



**Skills for Employment Investment Program (SEIP)**

**COMPETENCY-BASED LEARNING MATERIAL  
FOR  
INFORMATION SYSTEM SECURITY MANAGEMENT  
(STUDENT GUIDE)  
(IT SECTOR)**

**Finance Division, Ministry of Finance  
Government of the People's Republic of Bangladesh**

## Table of Contents

Copyright	3
How to Use this Competency-based Learning Material	4
List of Icons	5
Module 1: Interpret Fundamentals of Information System Governance and Security Management	6
Module 2: Manage Risks for Information Systems	39
Module 3: Perform infrastructure security	97
Module 4: Perform Application Software Security	198
Module 5: Perform Information Security Operations	234
Module 6: Interpret Information Systems Audit	270
Module 7: Perform Information Systems Security Testing	288

## Copyright

---

The Competency-based Learning Material (Student Guide) for Information System Security Management is a document, aligned to its applicable competency standard, for providing training consistent with the requirements of industry in order for individuals who graduated through the established standard via competency-based assessment to be suitably qualified for a relevant job.

This document is owned by the Finance Division of the Ministry of Finance of the People's Republic of Bangladesh, developed under the Skills for Employment Investment Program (SEIP).

Public and private institutions may use the information contained in this competency-based learning material for activities benefitting Bangladesh.

Other interested parties must obtain permission from the owner of this document for reproduction of information in any manner, in whole or in part, of this Competency-based Learning Material, in English or other language.

This document is available from:

*Skills for Employment Investment Program (SEIP) Project  
Finance Division  
Ministry of Finance  
Probashi Kallyan Bhaban (Level – 16)  
71-72 Old Elephant Road  
Eskaton Garden, Dhaka 1000  
Telephone: +8802 551 38598-9 (PABX), +8802 551 38753-5  
Facsimile: +8802 551 38752  
Website: [www.seip-fd.gov.bd](http://www.seip-fd.gov.bd)*

## How to Use this Competency-based Learning Material

---

Welcome to the competency-based learning material for **Information System Security Management** for use in IT works. These modules contain training materials and learning activities for you to complete in order to become competent and qualified as a merchandiser.

There are Seven (7) modules that make up this course which comprises the skills, knowledge and attitudes required to become a skilled worker including:

1. Interpret Basics of Information System Governance and Security Management
2. Manage risks for information system
3. Perform infrastructure security
4. Perform application software security
5. Perform Information security operations
6. Interpret Information Systems Audit
7. Perform Information Systems Security Testing

As a learner, you will be required to complete a series of activities in order to achieve each learning outcome of the module. These activities may be completed as part of structured classroom activities or simulated workplace demonstrations.

These activities will also require you to complete associated learning and practice activities in order to gain the skills and knowledge needed to achieve the learning outcomes. You should refer to **Learning Activity** pages of each module to know the sequence of learning tasks and the appropriate resources to use for each task.


This page will serve as the road map towards the achievement of competence. If you read the **Information Sheets**, these will give you an understanding of the work, and why things are done the way they are. Once you have finished reading the Information Sheets, you will then be required to complete the **Self-Check Quizzes**.

The self-check quizzes follow the Information Sheets in this learning guide. Completing the self-check quizzes will help you know how you are progressing. To check your knowledge after completion of the Self-Check Quizzes, you can review the **Answer Key** at the end of each module.

You are required to complete all activities as directed in the **Learning Activity and Information Sheet**. This is where you will apply your newly acquired knowledge while developing new skills. When working, high emphasis should be laid on safety requirements. You will be encouraged to raise relevant queries or ask the facilitator for assistance as required.

When you have completed all the tasks required in this learning guide, formal assessment will be scheduled to officially evaluate if you have achieved competency of the specified learning outcomes and are ready for the next task.

## List of Icons

Icon Name	Icon
Module content	
Learning outcomes	
Performance criteria	
Contents	
Assessment criteria	
Resources required	
Information sheet	
Self-check Quiz	
Answer key	
Activity	
Video reference	
Learner job sheet	
Assessment plan	
Review of competency	

## Module 1: Interpret Fundamentals of Information System Governance and Security Management

---



**MODULE CONTENT** module covers

**Module Descriptor:** This unit covers the knowledge, skills and attitudes required to interpret fundamentals of information system governance and security management. It specifically includes determining requirements of information system security management (ISSM) and interpreting Information System Security Management and governance.

**Nominal Duration:** 20 hours



**LEARNING OUTCOMES:**

Upon completion of the module, the trainee should be able to:

- 1.1 Determine requirements of Information System Security Management (ISSM)
- 1.2 Interpret Information System Security Management and governance



**PERFORMANCE CRITERIA:**

1. Fundamental terminologies of information security are interpreted.
2. Information security threats and attack vectors are recognized.
3. Security control requirements are identified.
4. Tools used for ISSM are listed.
5. Information warfare is defined.
6. Information System governance is interpreted.
7. Cyber law and ethics are interpreted.



## Learning Outcome 1.1 Determine requirements of Information System Security Management (ISSM)



### Contents:

- Organizational policies and national regulations
- Information Systems audit standard, Guideline and code of ethics.
- Types of audit and assessments
- Elements of audit plan
- Risk based audit plan



### Assessment criteria:

- 1 Fundamental terminology of information security is interpreted
- 2 Information security threats and attack vectors are recognized
- 3 Security controls requirements are identified.
- 4 Tools used for ISSM are listed and explained.
- 5 Information warfare is defined.



### Resources required:

Students/trainees must be provided with the following resources:

- Workplace (actual or simulated)
- Network devices, required tools, equipment's and materials.



### LEARNING ACTIVITY 1.1

Learning Activity	Resources/Special Instructions/References
Determine requirements of Information System Security Management.	<ul style="list-style-type: none"> <li>▪ Information Sheet: 1.1</li> <li>▪ Self-Check: 1.1</li> <li>▪ Answer Key: 1.1</li> </ul>



## Information sheet 1.1

Learning Objective: to determine requirements of Information System Security Management.

### Information

Information is processed, organized and structured data. It provides context for data and enables decision making process. For example, a single customer's sale at a restaurant is data – this becomes information when the business is able to identify the most popular or least popular dish.

### Information Vs Data

Data can be described as unprocessed facts and figures. Plain collected data as raw facts cannot help in decision-making. However, data is the raw material that is organized, structured, and interpreted to create useful information systems.

Data is defined as 'groups of non-random symbols in the form of text, images, voice representing quantities, action and objects'.

Information is interpreted data; created from organized, structured, and processed data in a particular context.

According to **Davis and Olson** –

"Information is a data that has been processed into a form that is meaningful to recipient and is of real or perceived value in the current or the prospective action or decision of recipient."



### Information Security

Information security means protecting information and information system from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.

### Information System Security Management

Information system security management is a systematic and structured approach to managing information so that it remains secure.

The core principles of information security-

**Confidentiality-** is keeping sensitive information protected.

**Integrity-** is keeping information intact and valid.

**Availability-** is keeping information available and accessible.

### Asset

An asset is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information.

### Threat



A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorized party.

Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental.

Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

### **Vulnerability**

A vulnerability is an organizational flaw that can be exploited by a threat to destroy, damage or compromise an asset.

we are most likely to encounter a vulnerability in our software, due to their complexity and the frequency with which they are updated. These weaknesses, known as bugs, can be used by criminal hackers to access sensitive information.

Vulnerabilities don't only refer to technological flaws, though. They can be physical weaknesses, such as a broken lock that lets unauthorized parties into a restricted part of your premises, or poorly written (or non-existent) processes that could lead to employees exposing information.

Other vulnerabilities include inherent human weaknesses, such as our susceptibility to phishing emails; structural flaws in the premises, such as a leaky pipe near a power outlet; and communication errors, such as employees' sending information to the wrong person.

### **Risk**

Risk is the potential for loss, damage or destruction of assets or data. It is the possibility of something bad happening.

### **Exploitation**

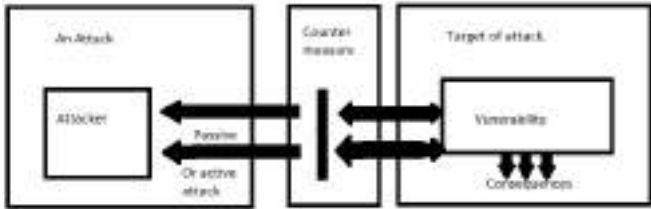
Exploitation is a piece of programmed software or script which can allow hackers to take control over a system, exploiting its vulnerabilities. Hackers normally use vulnerability scanners like Nessus, Nexpose, OpenVAS, etc. to find these vulnerabilities.

### **Attack**

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations.

### **Types of attack**

An attack can be active or passive. An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources



## **Security**

Security is the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

### **Security of an Information System**

Information system security refers to the way the system is defended against unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

There are two major aspects of information system security –

- Security of the information technology used – securing the system from malicious cyber-attacks that tend to break into the system and to access critical private information or gain control of the internal systems.
- Security of data – ensuring the integrity of data when critical issues, arise such as natural disasters, computer/server malfunction, physical theft etc. Generally an off-site backup of data is kept for such problems.

Guaranteeing effective information security has the following key aspects –

- Preventing the unauthorized individuals or systems from accessing the information.
- Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
- Ensuring that the computing systems, the security controls used to protect it and the communication channels used to access it, functioning correctly all the time, thus making information available in all situations.
- Ensuring that the data, transactions, communications or documents are genuine.
- Ensuring the integrity of a transaction by validating that both parties involved are genuine, by incorporating authentication features such as "digital signatures".
- Ensuring that once a transaction takes place, none of the parties can deny it, either having received a transaction, or having sent a transaction. This is called 'non-repudiation'.
- Safeguarding data and communications stored and shared in network systems.

### **The three-pillar approach to cyber security: Data and information protection**

#### **Confidentiality**

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need.

This component is often associated with secrecy and the use of encryption. Confidentiality in this context means that the data is only available to authorized parties. When information has been kept confidential it means that it has not been compromised by other parties; confidential data are not disclosed to people who do not require them or who should not have access to them. Ensuring confidentiality means that information is organized in terms of who needs to have access, as well as the sensitivity of the data. A breach of confidentiality may take place through different means, for instance hacking or social engineering.

**Integrity:** Data integrity refers to the certainty that the data is not tampered with or degraded during or after submission. It is the certainty that the data has not been subject to unauthorized modification, either intentional or unintentional. There are two points during the transmission process during which the integrity could be compromised: during the upload or transmission of data or during the storage of the document in the database or collection.

**Availability:** This means that the information is available to authorized users when it is needed. For a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels. Systems defined as critical (power generation, medical equipment, safety systems) often have extreme requirements related to availability. These systems must be resilient against cyber threats, and have safeguards against power outages, hardware failures and other events that might impact the system availability.

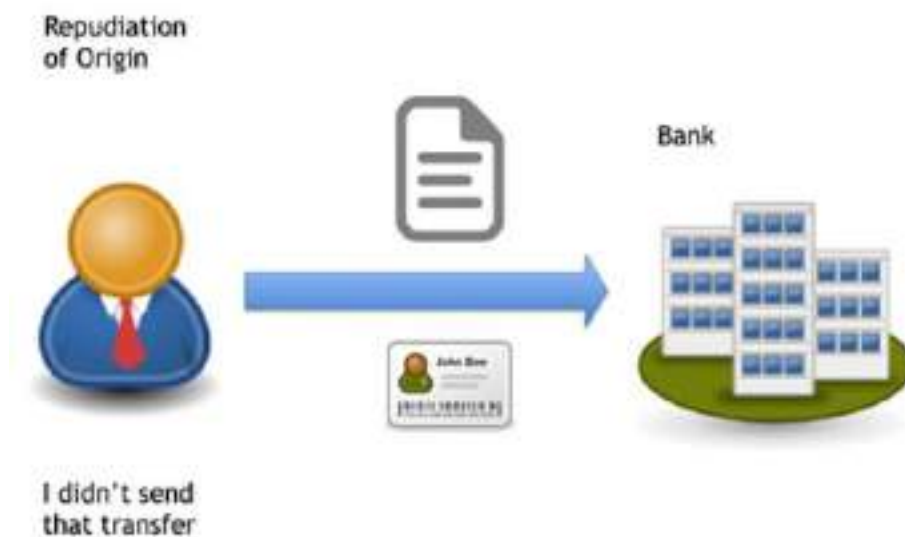
### Data Authenticity

Digital data can be assumed to be authentic if it is provable that it has not been corrupted after its creation. Data authenticity also means that a digital object is indeed what it claims to be or what it is claimed to be.

### Non-repudiation

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

Non-repudiation refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated contract. The term is often seen in a legal setting when the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated".



In computer security, the payload is the part of the private user text which could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data. In computing and telecommunications, the payload is the part of transmitted data that is the actual intended message. Headers and metadata are sent only to enable payload delivery. In the context of a computer virus or worm, the payload is the portion of the malware which performs malicious action.

## **Doxxing**

Doxxing is a type of cyber-attack that involves discovering the real identity of an Internet user. The attacker then reveals that person's details so others can target them with malicious attacks. Doxxing is analyzing information posted online by the victim in order to identify and later harass that person. It is the malicious identification and online publication of information about an individual. It can include Personally Identified Information (PII) or other sensitive, private, or damaging content about the individual or the individual's family members.

## **Bot**

A bot, short for "robot", is a type of software application or script that performs automated tasks on command. Bad bots perform malicious tasks that allow an attacker to remotely take control over an affected computer. Once infected, these machines may also be referred to as zombies.

## **Security threats**

In computer security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.

## **Types of security threats**

- Malware.
  - Malware is malicious software such as spyware, ransomware, viruses and worms.
- Emotet.
- Denial of Service.
- Man in the Middle.
- Phishing.
- SQL Injection.
- Password Attacks.
- The Internet of Things.

## **The most common threat to information security in an organization**

- **Phishing Attacks**

The biggest, most damaging and most widespread threat facing small businesses are phishing attacks. Phishing accounts for 90% of all breaches that organizations face, they've grown 65% over the last year, and they account for over \$12 billion in business losses. Phishing attacks occur when an attacker pretends to be a trusted contact, and entices a user to click a malicious link, download a malicious file, or give them access to sensitive information, account details or credentials.

Phishing attacks have grown much more sophisticated in recent years, with attackers becoming more convincing in pretending to be legitimate business contacts. There has also been a rise in Business Email Compromise, which involves bad actors using phishing campaigns to steal business email account passwords from high level executives, and then using these accounts to fraudulently request payments from employees.

Part of what makes phishing attacks so damaging is that they're very difficult to combat. They use social engineering to target humans within a business, rather than targeting technological weaknesses. However, there are technological defences against phishing attacks.

- **Malware Attacks**

Malware is the second big threat facing small businesses. It encompasses a variety of cyber threats such as trojans and viruses. Malware is a varied term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices.

These attacks are particularly damaging for small businesses because they can cripple devices, which requires expensive repairs or replacements to fix. They can also give attackers a back door to access data, which can put customers and employees at risk. Small businesses are more likely to employ people who use their own devices for work, as it helps to save time and cost. This, however, increases their likelihood of suffering from a malware attack, as personal devices are much more likely to be at risk from malicious downloads.

Business can prevent malware attacks by having strong technological defences in place. Endpoint Protection solutions protect devices from malware downloads and give admins a central control panel to manage devices and ensure all users' security is up to date. Web Security is also important, stopping users from visiting malicious webpages and downloading malicious software.

- **Ransomware**

Ransomware is one of the most common cyber-attacks, hitting thousands of businesses every year. These attacks have only become more common,, as they are one of the most lucrative forms of attacks. Ransomware involves encrypting company data so that it cannot be used or accessed, and then forcing the company to pay a ransom to unlock the data. This leaves businesses with a tough choice – to pay the ransom and potentially lose huge sums of money, or cripple their services with a loss of data.

Small businesses are especially at risk from these types of attack. In 2021, 71% of ransomware attacks targeted small businesses, with an average ransom demand of \$116,000. Attackers know that smaller businesses are much more likely to pay a ransom, as their data is often not backed-up and they need to be up and running as soon as possible. The healthcare sector is particularly badly hit by this type of attack, as locking patient medical records and appointment times can damage a business to a point where it has no choice but to close, unless a ransom has been paid.

To prevent these attacks, businesses need to have strong Endpoint Protection in place across all business devices. These will help to stop ransomware attacks from being able to effectively encrypt data. Endpoint protection solution SentinelOne even provides a 'ransomware rollback' feature, which allows organizations to very quickly detect and mitigate against ransomware attacks.

- **Weak Passwords**

Another big threat facing small businesses is employees using weak or easily guessed passwords. Many small businesses use multiple cloud based services, that require different accounts. These services often can contain sensitive data and financial information. Using easily guessed passwords, or using the same passwords for multiple accounts, can cause this data to become compromised.

Small businesses are often at risk from compromises that come from employees using weak passwords, due to an overall lack of awareness about the damage they can cause. An average of 19% of enterprise professionals use easily guessed passwords or share passwords across accounts.

To ensure that employees are using strong passwords, users should consider Business Password Management technologies. These platforms help employees to manage passwords for all their accounts, suggesting strong passwords that cannot be easily cracked. Businesses should also consider implementing Multi-Factor Authentication technologies. These ensure that users need more than just a password to have access to business accounts. This includes having multiple verification steps, such as a passcode sent to a mobile device. These security controls help to prevent attackers from accessing business accounts, even if they do correctly guess a password.

- **Insider Threats**

The final major threat facing small businesses is the insider threat. An insider threat is a risk to an organization that is caused by the actions of employees, former employees, business contractors or associates. These actors can access critical data about your company, and they can cause harmful effects through greed or malice, or simply through ignorance and carelessness. Verizon found that 25% of data breaches were caused by insider threats.

This is a growing problem and can put employees and customers at risk, or cause the company financial damage. Within small businesses, insider threats are growing as more employees have access to multiple accounts, that hold more data. Research has found that 62% of employees have reported having access to accounts that they probably didn't need to.

To block insider threats, small businesses need to ensure that they have a strong culture of security awareness within their organization. This will help to stop insider threats caused by ignorance, and help employees to spot early on when an attacker has compromised, or is attempting to compromise company data.

### **Cloud computing threats**

The high volume of data flowing between organizations and cloud service providers generates opportunities for accidental and malicious leaks of sensitive data to untrusted 3rd parties. Human error, insider threats, malware, weak credentials and criminal activity contribute to most cloud service data breaches.

## **Main Cloud Security Issues and Threats in 2021**

- Misconfiguration. Misconfigurations of cloud security settings are a leading cause of cloud data breaches.
- Unauthorized Access.
- Insecure Interfaces/APIs.
- Hijacking of Accounts.
- Lack of Visibility.
- External Sharing of Data.
- Malicious Insiders.
- Cyberattacks.

### **Advanced Persistent Threat (APT)**

An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data. It is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

### **Mobile Application Security Threats.**

Application-based threats happen when people download apps that look legitimate but actually skim data from their device. Examples are spyware and malware that steal personal and business information without people realizing it's happening.

Mobile security threats include everything from mobile forms of malware and spyware to the potential for unauthorized access to a device's data, particularly in the case of accidental loss or theft of the device.

### **Different Types of Mobile Security Threats**

Mobile security threats are commonly thought of as a single, all-encompassing threat. But the truth is, there are different types of mobile security threats that organizations need to take steps to protect themselves from:

#### **Mobile Application Security Threats**

Application-based threats happen when people download apps that look legitimate but actually skim data from their device. Examples are spyware and malware that steal personal and business information without people realizing it's happening.

#### **Web-Based Mobile Security Threats**

Web-based threats are subtle and tend to go unnoticed. They happen when people visit affected sites that seem fine on the front-end but, in reality, automatically download malicious content onto devices.

#### **Mobile Network Security Threats**

Network-based threats are especially common and risky because cybercriminals can steal unencrypted data while people use public WiFi networks.

#### **Mobile Device Security Threats**



Physical threats to mobile devices most commonly refer to the loss or theft of a device. Because hackers have direct access to the hardware where private data is stored, this threat is especially dangerous to enterprises.

### **Botnet**

A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.” Each individual machine under the control of the bot-herder is known as a bot. They are also used to spread



bots to recruit more computers to the botnet.

### **Insider attack**

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

### **Attack vectors**

Attack vectors are the methods that adversaries use to breach or infiltrate your network. Attack vectors take many different forms, ranging from malware and ransomware, to man-in-the-middle attacks, compromised credentials, and phishing.

In general, attack vectors can be split into passive or active attacks:

#### **Passive Attack Vector Exploits**

Passive attack vector exploits are attempts to gain access or make use of information from the system but does not affect system resources, such as typosquatting, phishing and other social engineering based attacks.

#### **Active Attack Vector Exploits**

Active attack vector exploits are attempts to alter a system or affect its operation such as malware, exploiting unpatched vulnerabilities, email spoofing, man-in-the-middle attacks, domain hijacking and ransomware.

## **The Common Types of Attack Vectors?**

### **1. Compromised Credentials**

Username and passwords are still the most common type of access credential and continue to be exposed in data leaks, phishing scams and by malware. When lost, stolen or exposed, credentials give attackers unfettered access. This is why organizations are now investing in tools to continuously monitor for data exposures and leaked credentials. Password managers, two-factor authentication and biometrics can reduce the risk of leak credentials resulting in a security incident too.

### **2. Weak Credentials**

Weak passwords and reused passwords mean one data breach can result in many more. Teach your organization how to create a secure password, invest in a password manager or a single sign-on tool, and educate staff on their benefits.

### **3. Malicious Insiders**

Disgruntled employees can expose private information or provide information about company specific vulnerabilities.

### **4. Missing or Poor Encryption**

Common encryption methods like SSL certificates and DNSSEC can prevent man-in-the-middle attacks and protect the confidentiality of data being transmitted. Missing or poor encryption for data at rest can mean that sensitive data or credentials are exposed in the event of a data breach or data leak.

### **5. Misconfiguration**

Misconfiguration of cloud services, like Google Cloud Platform, Microsoft Azure, or AWS, or using default credentials can lead to data breaches and data leaks, check your S3 permissions or someone else will. Automate configuration management where possible to prevent configuration drift.

### **6. Ransomware**

Ransomware is a form of extortion where data is deleted or encrypted unless a ransom is paid, such as WannaCry. Minimize the impact of ransomware attacks by keeping your systems patched and backing up important data.

### **7. Phishing**

Phishing is a social engineering technique where the target is contacted by email, telephone or text message by someone who is posing to be a legitimate colleague or institution to trick them into providing sensitive data, credentials or personally identifiable information (PII). To minimize phishing, educate your staff on the importance of cybersecurity and prevent email spoofing and typosquatting.

### **8. Vulnerabilities**

New vulnerabilities are added to CVE every day and zero-day vulnerabilities are found just as often. If a developer has not released a patch for a zero-day vulnerability before an attack can exploit it, it can be hard to prevent.

### **9. Brute Force**

Brute force attacks are based on trial and error. Attackers may continuously try to gain access to your organization until one attack works. This could be by attacking weak passwords or encryption, phishing emails or sending infected email attachments containing a type of malware. Read our full post on brute force attacks.

### **10. Distributed Denial of Service (DDoS)**

DDoS are cyber attacks against networked resources like data centers, servers or websites and can limit the availability of a computer system. The attacker floods the network resource with messages which cause it to slow down or even crash, making it inaccessible to users. Potential mitigations include CDNs and proxies.

### **11. SQL Injections**

SQL stands for structured query language, a programming language used to communicate with databases. Many of the servers that store sensitive data use SQL to manage the data in their database. An SQL injection uses malicious SQL to get the server to expose information it otherwise wouldn't. This is a huge cyber risk if the database stores customer information, credit card numbers, credentials or other personally identifiable information (PII).

### **12. Trojans**

Trojan horses are malware that misleads users by pretending to be a legitimate program and are often spread via infected email attachments or fake software.

### **13. Cross-Site Scripting (XSS)**

XSS attacks involve injecting malicious code into a website but the website itself is not being attacked, rather it aims to impact the website's visitors. A common way attackers can deploy cross-site scripting attacks is by injecting malicious code into a comment e.g. embed a link to malicious JavaScript in a blog post's comment section.

### **14. Session Hijacking**

When you log into a service, it generally provides your computer with a session key or cookie so you don't need to log in again. This cookie can be hijacked by an attacker who uses it to gain access to sensitive information.

### **15. Man-in-the-Middle Attacks**

Public Wi-Fi networks can be exploited to perform man-in-the-middle attacks and intercept traffic that was supposed to go elsewhere, such as when you log into a secure system.

### **16. Third and Fourth-Party Vendors**

The rise in outsourcing means that your vendors pose a huge cybersecurity risk to your customer's data and your proprietary data. Some of the biggest data breaches were caused by third parties.

#### **Operating system attack**

In Operating Systems attacks, "attackers look for vulnerabilities in OS such that they can exploit through vulnerabilities and gain access to the target system or network". The vulnerabilities in the OS can be open ports and services as most of the operating systems install these services and ports by default.

#### **Misconfiguration Attacks**

Security misconfiguration vulnerabilities take place when an application component is vulnerable to attack as a result of insecure configuration option or misconfiguration.

Misconfiguration vulnerabilities are configuration weaknesses that might exist in software subsystems or components. For instance, web server software might ship with default user accounts that a cybercriminal could utilize to access the system, or the software might have a known set of standard configuration files or directories, which a cybercriminal could exploit.

Furthermore, software might have vulnerable services enabled, such as remote administration operations. Misconfiguration vulnerabilities cause your application to be vulnerable to attacks that target any component of the application stack.

For instance, the following types of attacks could exploit misconfiguration vulnerabilities:

- Code injection
- Credential stuffing/brute force
- Buffer overflow
- Cross-site scripting (XSS)
- Command injection
- Forceful browsing

### **Common Mistakes that Lead to Security Misconfiguration**

Failure to remove or disable unnecessary features—when you do not remove superfluous components, code samples or features, the application is left open to attack. Do not keep unnecessary ports open or unneeded services running. You should also make sure to delete accounts that are no longer needed.

Using default accounts and passwords—devices and programs, including web applications and network devices, come with a set of default credentials that provide initial access to owners. After gaining access, owners must change their passwords. Otherwise, attackers can use lists of common default credentials to brute-force the system and gain unauthorized access.

Defining error messages that reveal too much information—default server configurations should not provide too much information in error messages. For example, the error message should not provide detailed stack traces. This can expose sensitive information, like the used component versions, which attackers can use to search for exploitable flaws.

Using old software versions and missing updates—outdated software can leave systems exposed to known vulnerabilities, which may have already been patched. To ensure patches are effective, they must be applied on time.

Misconfigured upgrades—to be truly effective, upgrades must be properly configured. Whether the upgrade includes security patches or new functionality, it must be configured and enabled correctly. To avoid misconfiguration, review each update to see the exact change and adjust your configuration accordingly.

Misconfigured cloud systems—cloud providers are responsible for securing the underlying infrastructure. You are responsible for securing your own cloud resources, including workloads and data. A misconfigured cloud-based operating system, for example, can expose your virtual machines (VMs) or containers to attacks.

### **Application-layer attack**

An application-layer attack targets computers by deliberately causing a fault in a computer's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of an application, system or network.

### **Shrink-wrap code attack**

Shrink Wrap Code Attacks are attacks where an attacker tries to run default code in the victim's software. This default code (from off-the-shelf libraries and code) is often REM'd or placed in a comment line.

### **Security controls**

Security controls exist to reduce or mitigate the risk to those assets. They include any type of policy, procedure, technique, method, solution, plan, action, or device designed to help accomplish that goal. Recognizable examples include firewalls, surveillance systems, and antivirus software.

To ensure security Control we need to identify security control requirements like-

- Information assurance
- Information security management programs
- Threat modeling
- Enterprise information security architecture
- Network security zoning
- Information security policy
- Physical security
- Environmental Security
- Incident management process
- Vulnerability research
- Vulnerability assessment
- Penetration testing

### **Information assurance**

Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

### **Information security management programs**

An information security management system (ISMS) is a framework of policies and controls that manage security and risks systematically and across your entire enterprise—information security. These security controls can follow common security standards or be more focused on your industry.

### **Continuous improvement in information security**

While ISMS is designed to establish holistic information security management capabilities, digital transformation requires organizations to adopt ongoing improvements and evolution of their security policies and controls.

The structure and boundaries defined by an ISMS may apply only for a limited time frame and the workforce may struggle to adopt them in the initial stages. The challenge for organizations is to evolve these security control mechanisms as their risks, culture, and resources change.

According to ISO 27001, ISMS implementation follows a Plan-Do-Check-Act (PCDA) model for continuous improvement in ISM processes:

**Plan.** Identify the problems and collect useful information to evaluate security risk. Define the policies and processes that can be used to address problem root causes. Develop methods to establish continuous improvement in information security management capabilities.

**Do.** Implement the devised security policies and procedures. The implementation follows the ISO standards, but actual implementation is based on the resources available to your company.

**Check.** Monitor the effectiveness of ISMS policies and controls. Evaluate tangible outcomes as well as behavioral aspects associated with the ISM processes.

**Act.** Focus on continuous improvement. Document the results, share knowledge, and use a feedback loop to address future iterations of the PCDA model implementation of ISMS policies and controls.

### **Threat modeling**

Threat modeling is a structured process with these objectives: identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods.

Threat modeling works by identifying the types of threat agents that cause harm to an application or computer system. It adopts the perspective of malicious hackers to see how much damage they could do. When conducting threat modeling, organizations perform a thorough analysis of the software architecture, business context, and other artifacts (e.g., functional specifications, user documentation). This process enables a deeper understanding and discovery of important aspects of the system. Typically, organizations conduct threat modeling during the design stage (but it can occur at other stages) of a new application to help developers find vulnerabilities and become aware of the security implications of their design, code, and configuration decisions.

### **Enterprise information security architecture**

Enterprise information security architecture (EISA) is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that they align with the organization's core goals and strategic direction.

### **Network security zone**

A network security zone is an administrative name for a collection of systems that require the same access control policy. IP addresses are used to map systems into security zones. This requires that the IP addresses used in your multilevel secure network be predictably associated with a single system or group of systems with the same access control policy. A network security zone can contain a single IP address or any combination of IP addresses and subnetworks. All of the IP addresses in a security zone must have the same security label,

though all IP addresses with the same security label do not have to be in the same security zone.

### **Information security policy**

An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements.

ISPs should address all data, programs, systems, facilities, infrastructure, authorized users, third parties and fourth parties of an organization.

### **Purpose of an Information Security Policy**

An information security policy aims to enact protections and limit the distribution of data to only those with authorized access. Organizations create ISPs to:

- Establish a general approach to information security
- Document security measures and user access control policies
- Detect and minimize the impact of compromised information assets such as misuse of data, networks, mobile devices, computers and applications
- Protect the reputation of the organization
- Comply with legal and regulatory requirements like NIST, GDPR, HIPAA and FERPA
- Protect their customer's data, such as credit card numbers
- Provide effective mechanisms to respond to complaints and queries related to real or perceived cyber security risks such as phishing, malware and ransomware
- Limit access to key information technology assets to those who have an acceptable use

### **Physical security**

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events.

The physical security framework is made up of three main components: access control, surveillance and testing. The success of an organization's physical security program can often be attributed to how well each of these components is implemented, improved and maintained.

### **Environmental security**

Environmental security is the state of protection of vital interests of the individual, society, natural environment from threats resulting from anthropogenic and natural impacts on the environment.

### **Incident management process**

An incident management process is a set of procedures and actions taken to respond to and resolve critical incidents: how incidents are detected and communicated, who is responsible, what tools are used, and what steps are taken to resolve the incident

Five Steps of Incident Response

1. Preparation. Preparation is the key to effective incident response.

2. Detection and Reporting.
3. Triage and Analysis.
4. Containment and Neutralization.
5. Post-Incident Activity.

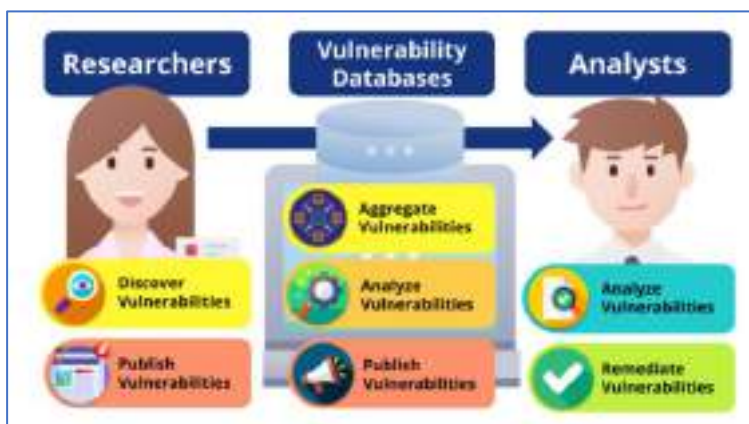
### Vulnerability research

Vulnerability research is the process where you research vulnerabilities and determine if any of them affects your organization's systems.

As you monitor your vulnerability sources, you must research the vulnerabilities that appear. Do any of them affect your organization's systems? Does a vulnerability affect a vendor in your supply chain, or a product your organization uses? If it does, what versions are susceptible to that vulnerability? Is an exploit available? Can you install a patch or upgrade to remediate it?

However, this stage of vulnerability intelligence (VI) is not so simple as vulnerability research can have different meanings and occur at different times depending on the role of the person performing it. The roles that can influence this are:

- Vulnerability researchers
- Vulnerability intelligence companies
- Security analysts at organizations



### Vulnerability Assessment

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Examples of threats that can be prevented by vulnerability assessment include:

SQL injection, XSS and other code injection attacks.

Escalation of privileges due to faulty authentication mechanisms.

Insecure defaults – software that ships with insecure settings, such as a guessable admin password.

There are several types of vulnerability assessments. These include:

**Host assessment** – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.



Network and wireless assessment – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.

**Database assessment** – The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization’s infrastructure.

**Application scans** – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

Vulnerability assessment: Security scanning process



### Penetration testing

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

The pen testing process can be broken down into five stages.



## Some Tools for Information System Security Management.

### MailCleaner

MailCleaner is a business anti-spam gateway installed between your mail infrastructure and the Internet. It offers professional protection against viruses and eliminates up to 99% of spam.

Main benefits of our anti spam services

While email is necessary for any corporate operations, it can also expose your company to a myriad of risks. This is because it offers virus, spyware, ransomware, cryptolocker, trojan and other harmful programs easy access to your business computers for phishing or extortion attack. This is where MailCleaner can help by stopping malware before it even reaches your employees' inboxes. Its spam filter server ensures that more than 99% of unwanted messages are blocked, analysing each message, so you only receive those that are important. If a harmful file is detected, MailCleaner will automatically send it to a quarantined zone where it cannot cause any more damage in the future.

### AdGuard

AdGuard is the best way to get rid of intrusive ads and online tracking, and to protect your computer from malware. Make your web surfing faster, safer and more comfortable with AdGuard.

Adguard will block ads in all browsers and in most applications. Quality of blocking will be similar to that we have in Adguard for Windows. As it is the case in Windows-version, Adguard for Android will use our anti-phishing database to protect you from phishing and malicious websites.

### Automated Vulnerability Detection System (AVDS)

Beyond Security Automated Vulnerability Detection System (AVDS) appliances create vulnerability data in Asset Export Information Source (AXIS) format. AXIS formatted files can be imported by XML files that can be imported.

### Cloudflare

Cloudflare secures and ensures the reliability of your external-facing resources such as websites, APIs, and applications. It protects your internal resources such as behind-the-firewall

applications, teams, and devices. And it is your platform for developing globally-scalable applications.

### **SiteLock**

SiteLock is a comprehensive website security tool for small and medium-sized businesses maintaining security on your websites and servers. SiteLock scans your websites for security-related issues like example malware, such as backdoor file Hacks, Trojan viruses, pharmaceutical hacks, redirect hacks, and many more. SiteLock automatically scans your website for malware to ensure they are not being spammed.

### **The Email Laundry**

Impersonation Detection To protect users from Impersonation type email attacks like CEO Fraud or Business Email Compromise The Email Laundry provides a range of methods to customers on its Full Stack Email security service to counter these attacks. Friendly Name filters to protect against social engineering impersonation attacks on mobile and desktop devices. Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud. Instant action from The Email Laundry Threat Intelligence Network and Security Analyst teams Protects against Newly Registered and Newly Observed Domains to catch the first email from a newly registered domain. Protects against Display name spoofing and attacks

## **PureVPN**

PureVPN is a Virtual Private Network (VPN) service that provides secured access using 256-bit encryption and anonymous, unrestricted browsing with IP address masking.

## **Anomaly Detection**

Anomaly detection, also called outlier detection, is the identification of unexpected events, observations, or items that differ significantly from the norm. Often applied to unlabeled data by data scientists in a process called unsupervised anomaly detection, any type of anomaly detection rests upon two basic assumptions:

Anomalies in data occur only very rarely

The features of data anomalies are significantly different from those of normal instances

Typically, anomalous data is linked to some sort of problem or rare event such as hacking, bank fraud, malfunctioning equipment, structural defects / infrastructure failures, or textual errors. For this reason, identifying actual anomalies rather than false positives or data noise is essential from a business perspective.

## **Firewall**

A firewall is a security device in the form of computer hardware or software. It can help protect your network by acting as an intermediary between your internal network and outside traffic. It monitors attempts to gain access to your operating system and blocks unwanted incoming traffic and unrecognized sources.

A firewall acts as a barrier or gatekeeper between your computer and another network like the internet. It works like a traffic controller, monitoring and filtering traffic that wants to gain access to your operating system.

A firewall can help protect your computer and data by managing your network traffic. It does this by blocking unsolicited and unwanted incoming network traffic. A firewall validates access by assessing this incoming traffic for anything malicious like hackers and malware that could infect your computer.

## **Access Rights Manager**

The Access Rights Manager keeps track of activities impacting the domain controllers operating on your network. It will alert you if any changes are made to records in the databases of AD. This is a crucial monitor because accessing Active Directory to change permissions is a strategy used by hackers and malware

## **Security Information and Event Management (SIEM)**

Security Information and Event Management (SIEM) is a set of tools and services offering a holistic view of an organization's information security. SIEM tools provide: Real-time visibility across an organization's information security systems. Event log management that consolidates data from numerous sources.

Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure. SIEM collects security data from network devices, servers, domain controllers, and more.

## **Identity Monitor**

Identity Monitor monitors your email domains for any exposure, protecting your credentials. Because reacting quickly to a potential leak is of critical importance, Identity Monitor will notify you instantly if your credentials appear in a data leak.

### **Server Configuration Monitor**

The SCM is a comprehensive tool that gives you complete visibility into your servers for extensive monitoring. It uses a really easy mechanism where instead of having you track changes it shows you the exact changes so that you can fix them. What's more, is that the logging of each change happens in an almost real-time basis which can be attributed to the use of agent-based monitoring. This allows you to detect problems early enough before they escalate.

### **Patch Manager**

The basis of the Patch Management service is the associated Asset Management module in the SuperOps platform. This detects all desktops and laptops connected to the monitored network. It then cans through those that run the Windows operating system and documents its software, creating an inventory.

Patch management is about keeping software on computers and network devices up to date and capable of resisting low-level cyber attacks. Any software is prone to technical vulnerabilities. Once discovered and shared publicly, these can rapidly be exploited by cyber criminals.

### **Access Rights Auditor**

Access Rights Auditor is a tool, designed to scan your Active Directory and file system, and evaluate possible security risks due to existing user access rights.

Active Directory and file servers are at the heart of nearly every IT infrastructure today; excessive user access rights can pose a significant risk to your organization's data. Accessing data on purpose or per accident over privileged users can harm your company, but with Access Rights Auditor you can analyze additional risk areas as expiration of passwords, direct user access, everyone access and more.

### **Information Warfare**

Information Warfare is any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions

#### **Defensive information warfare**

The term "defensive information warfare" (IW-D) is used here to refer to all actions taken to defend against information attacks, that is, attacks on decision makers, the information and information-based processes they rely on, and their means of communicating their decisions.

#### **Offensive information warfare**

Offensive information warfare seeks dominance over the enemy's information, computer information systems, and control systems using a myriad of tools. Attacks can be launched against the enemy's physical computer network, its supporting infrastructure, or a product of the network.

### **Individual Activity:**

- Determine requirements of Information System Security Management.



### **Self-check quiz 1.1**

Check your understanding by answering the following questions:

Write the correct answer for the following questions.

1. What is information?

2. What are the core principles of information security?

3. What is security Threat?

4. What is Vulnerability Assessment?

5. What is Penetration Testing?



## Learning outcome 1.2- Interpret Information System Security Management and governance



Contents:

- Cyber law and ethics
- Information System governance



Assessment criteria:

- 2.1. Information System governance is interpreted.
- 2.2. Cyber law and ethics are interpreted.



Resources required:

- Students/trainees must be provided with the following resources:
- Workplace (Actual or simulated), Server, Necessary software.



### LEARNING ACTIVITY 1.2

Learning Activity	Resources/Special Instructions/References
Recognize Information System Security Management and Governance	<ul style="list-style-type: none"> <li>▪ Information Sheets: 1.2</li> <li>▪ Self-Check: 1.2</li> <li>▪ Answer Key: 1.2</li> </ul>



## Information sheet 1.2

Learning objective: to Recognize Information System Security Management and Governance.

### Cyber Laws

Technology is constantly updating. This means that laws must also be constantly updated. Although U.S. law has remained the same for a long time, five laws were passed in 2014:

- National Cybersecurity Protection Act (NCPA).
- Cybersecurity Enhancement Act of 2014 (CEA).
- Federal Information System Modernization Act of 2014 (FISMA 2014).
- Cybersecurity Workforce Assessment Act (CWWA).
- Border Patrol Agent Pay Reform Act (BPAPRA).

Most of these laws were meant to update existing legislation. FISMA 2014 updated the framework for security controls. NCPA was meant for information sharing between the private sector and the government.

The CEA was one of the most important bills. It may affect private organizations. This is because it promotes developing voluntary cybersecurity standards. This law strengthens the informal mission of the National Institute of Standards and Technology (NIST). The CEA also covers areas once covered by the Federal Financial Institutions Examination Council (FFIEC).

Both the NIST and FFIEC were informal standards. The CEA is a law and more binding. This is particularly useful for resolving disputes resulting from cybercrimes. Businesses need to understand the rules of the CEA.

### Cyber law

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet.

Cyber Law is the legal issues that is, it is the standard rules and regulation (law) adopted by any government or organizations to control and minimize the computer crime and it is related to the use of internetworked information technology.

With the Computer and internet taking over every aspect of our life, there was a need for strong cyber law. Cyber laws supervise the digital circulation of information, software, information security, e-commerce, and monetary transactions. The Information Technology Act, 2000 addresses the gamut of new-age crimes.

The cyber law incorporates

1. The Intellectual Property Law
  - Copyright
  - Patent Right
  - Trademark
2. Privacy



3. Computer Crime Law
4. Digital Signature system
5. Freedom of Expression

The main issues that surround cyberethics are: Copyright/Downloading, Hacking and Cyberbullying. These three issues are increasing daily and mostly due to children using the internet improperly.

### **Copyright/Downloading**

This has become a major problem due to programs like Napster and LimeWire which allow users to download music, programs and videos for free. Many people, especially children, do not realize that this behavior has major consequences.

### **Hacking:**

Is the intentional damage that a person inflicts onto another computer or computer network. This can include stealing classified information, stealing passwords to get into a site and also changing a website without permission. Since the world is run on computers it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. Cybercitizenship.org gives a chilling example: "If a virus were to disable the computer network of a hospital, it could shut down medical instrumentation systems that control life support and monitoring functions-all of which could cost a patient his or her life." Children need to be aware of these extreme consequences.

### **Cyberbullying:**

Bullying does not only happen in real life anymore. Cyberbullying is growing and people are becoming aware of its effects on children. The Megan Meier case shed light on this issue that was thought of by many people as harmless bullying. This teenage girl was bullied on the internet through e-mail and Myspace which is said to ultimately lead to her suicide.

The Core issue of computer ethics incorporates

- Technological impact on society
- Plagiarism
- Intellectual property law
- Copyright
- Piracy
- Hacking
- Internet Pornography and adult sites
- Harassment and stalking

In Bangladesh, a draft Bill on Information and Communication Technology has been introduced in the Parliament.

The final report on the Law on Information Technology was approved by the Office of the Law Commission in its meeting dated 08.09.2002.

The Proposal:

Chapter VII on Penalties and Adjudication and Chapter IX on Offences includes some cybercrime provisions that prohibits attacks or unauthorized access to computers and computer systems.

**Chapter IX: Section 66.** Punishment for tampering with computer source documents

Whoever intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by any law for the time being in force, shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs, or with both.

Explanation- For the purpose of this section, “computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

**Section 67.** Hacking with computer system

- Whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any other person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of “hacking”.

**Section 68.** Punishment for hacking

- Whoever commits hacking shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs, or with both.

**information management policy**

An information management policy gives staff direction for creating, capturing and managing information assets (records, information and data) to satisfy business, legal and stakeholder requirements. It also assigns responsibilities across the agency.

An information management policy should be consistent with the principles, environment and strategic directions described in your agency's information governance framework.

The Building trust in the public record policy recommends that agencies update their information governance framework to include enterprise-wide information management.

Developing or updating your agency's information management policy should be part of implementing this governance framework.

An information management policy:

sets out your agency's expectations for fit for purposes information management practices, processes and systems that will support the management of information as an organisational asset

explains the benefits of good information management

outlines roles and responsibilities

proves commitment to meeting business, legislative and regulatory requirements  
contributes to an environment that values the integrity and accessibility of information assets to support the delivery of business outcomes.

When developing your information management policy, consider how it supports your agency's strategic objectives and intersects with other strategic documents.

How your information management policy integrates with other policy and governance documents can be influenced by the size and nature of your agency. It should be designed to best meet the size, nature and complexity of your agency's business. For example, a smaller agency may combine the information management policy with other governance documents. A larger agency, or one with a more complex information management environment, may have separate governance documents complemented by other policies on aspects of information management. This can be useful when different policy statements are directed at different audiences, to ensure they are aware of their specific requirements.

### **SOD segregation of duties**

Segregation of Duties (SOD) Segregation of Duties (SOD) is a basic building block of sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department.

Information systems managers, or IT managers, are responsible for the secure and effective operation of all computer systems, related applications, hardware and software that is used within a wide range of public and private sector organisations.

### **Business continuity plan (BCP)**

A key component of a business continuity plan (BCP) is a disaster recovery plan that contains strategies for handling IT disruptions to networks, servers, personal computers and mobile devices. The plan should cover how to reestablish office productivity and enterprise software so that key business needs can be met.

### **Disaster recovery plan**

A disaster recovery (DR) plan is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events.





## Answer keys

### Answer key 1.1

Write the correct answer for the following questions.

1. What is information?

Answer: Information is processed, organized and structured data. It provides context for data and enables decision making process. For example, a single customer's sale at a restaurant is data – this becomes information when the business is able to identify the most popular or least popular dish.

2. What are the core principles of information security?

Answer: The core principles of information security-

**Confidentiality-** is keeping sensitive information protected.

**Integrity-** is keeping information intact and valid.

**Availability-** is keeping information available and accessible.

3. What is security Threat?

Answer: In computer security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.

4. What is Vulnerability Assessment?

Answer: A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

5. What is Penetration Testing?

Answer: A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

## Answer key 1.2

Check your understanding by answering the following questions:

1. What is cyber law?

Answer: Cyber Law is the legal issues that is, it is the standard rules and regulation (law) adopted by any government or organizations to control and minimize the computer crime and it is related to the use of internetworked information technology.

2. What is Hacking?

Answer: What is the intentional damage that a person inflicts onto another computer or computer network. This can include stealing classified information, stealing passwords to get into a site and also changing a website without permission.

3. What do you mean by the term “Business continuity plan”?

Answer: A key component of a business continuity plan (BCP) is a disaster recovery plan that contains strategies for handling IT disruptions to networks, servers, personal computers and mobile devices. The plan should cover how to reestablish office productivity and enterprise software so that key business needs can be met.

4. Explain disaster recovery plan?

Answer: A disaster recovery (DR) plan is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events.

## Module 2: Manage Risks for Information Systems

---



### MODULE CONTENT

**Module Descriptor:** This unit covers the knowledge, skills, and attitudes required to manage risks for information systems. It specifically includes assessing Risks, implementing risk control, mitigating information system security risks, managing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) and Implementing backup and recovery management

**Nominal Duration:** 30 hours



### LEARNING OUTCOMES:

Upon completion of the module, the trainee should be able to:

- 2.1. Assess Risks
- 2.2. Implement risk control
- 2.3. Mitigate information system security risks
- 2.4. Manage Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
- 2.5. Implement backup and recovery management



### PERFORMANCE CRITERIA:

1. Risks for information system are identified as per Risk Identification procedure.
2. Risks areas at information system are interpreted.
3. Threats for information system security are assessed with appropriate risk assessment tool.
4. Information system security requirements checklist is developed.
5. Control management is performed for information system security risks.
6. Likelihood of risks are determined.
7. Impact of risks are analyzed.
8. Risks are determined and put into risk-level matrix.
9. Control of risks are recommended and applied.
10. Inherent and residual risks are analyzed.
11. Results are documented and communicated as per standard procedure.
12. Risk mitigation strategy is outlined.
13. Risk mitigation tools are determined.
14. Cost-benefit analysis is prepared following standard procedure.
15. Control category is determined and applied.

16. Business Continuity Plan (BCP) is interpreted.
17. Business Impact Analysis (BIA) is interpreted.
18. Business Impact Analysis is performed as per standard procedure.
19. Business Continuity Plan (BCP) is prepared as per industry standard.
20. Disaster Recovery Plan (DRP) is interpreted.
21. Disaster Recovery Plan (DRP) is prepared as per industry standard.
22. Backup and Storage management is interpreted.
23. Data retention is interpreted.
24. Backup management tools are described.
25. Backup is performed as per standard procedure.
26. Restore and recovery are performed.
27. Data destruction is interpreted.





## Learning Outcome 2.1 Assess Risks



Contents:

- Risks for information system
- Risks areas at information system.
- Threats for information system security
- Information system security requirements checklist



Assessment criteria:

1. Risks for information system are identified as per Risk Identification procedure.
2. Risks areas at information system are interpreted.
3. Threats for information system security are assessed with appropriate risk assessment tool.
4. Information system security requirements checklist is developed.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (actual or simulated)
- Network devices, required tools, equipments and materials.



### LEARNING ACTIVITY 2.1

Learning Activity	Resources/Special Instructions/References
Assess Risks	<ul style="list-style-type: none"> <li>▪ Information Sheet: 2.1</li> <li>▪ Self-Check: 2.1</li> <li>▪ Answer Key: 2.1</li> </ul>



## Information sheet 2.1

Learning Objective: to Assess Risks.

Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation.

IT risk assessment is a process of analysing potential threats and vulnerabilities to your IT systems to establish what loss you might expect to incur if certain events happen. Its objective is to help you achieve optimal security at a reasonable cost.

There are two prevailing methodologies for assessing the different types of IT risk: quantitative and qualitative risk analysis.

### **Quantitative IT risk assessment**

Quantitative assessment measures risk using monetary amounts. It uses mathematical formulas to give you the value of expected losses associated with a particular risk, based on:

- the asset values
- the frequency of risk occurrence
- the probability of associated loss

In an example of server failure, a quantitative assessment would involve looking at:

- the cost of a server or the revenue it generates
- how often does the server crash
- the estimated loss incurred each time it crashed

From these values, you can work out several key calculations:

- single loss expectancy - costs you would incur if the incident occurs once
- annual rate of occurrence - how many times a year you can expect this risk to occur
- annual loss expectancy - the total risk value over the course of a year

Find a formula to calculate annualised loss expectancy.

These monetary results could help you avoid spending too much time and money on reducing negligible risks. For example, if a threat is unlikely to happen or costs little or nothing to remedy, it probably presents a low risk to your business.

However, if a threat to your key IT systems is likely to happen, and could be expensive to fix or likely to affect your business adversely, you should consider it high risk.

You may want to use this risk information to carry out a cost/benefit analysis to determine what level of investment would make risk treatment worthwhile.

Keep in mind that quantitative measures of risk are only meaningful when you have good data. You may not always have the necessary historical data to work out probability and cost estimates on IT-related risks, since they can change very quickly.

### **Qualitative IT risk assessment**

Qualitative risk assessment is opinion-based. It relies on judgment to categorise risks based on probability and impact and uses a rating scale to describe the risks as:

- low - unlikely to occur or impact your business
- medium - possible to occur and impact
- high - likely to occur and impact your business significantly

For example, you might classify as 'high probability' something that you expect to happen several times a year. You do the same for cost/impact in whatever terms seem useful, for example:

- low - would lose up to half an hour of production
- medium - would cause complete shutdown for at least three days
- high - would cause irrevocable loss to the business

With your ratings determined, you can then create a risk assessment matrix to help you categorise the risk level for each risk event. This can, ultimately, help you decide which risks to mitigate using controls, and which to accept or transfer.

### Risk matrix

Probability	Harm severity			
	Negligible	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

### Assessing and Evaluating Risks

- Security/risk audits; identifying and prioritizing security risks due to theft, loss, unauthorized access, viruses, or improper disposal.
- To contract with outside vendors or not? Generally, the larger the firm, the larger the network, and the more points of entry for hackers (and more information that is valuable to hackers). Upper-level security requires a staff of specialists and sometimes an independent third party. For instance, Service Level Agreements (SLAs) for functions such as firewall effectiveness or IT uptime provide a form of insurance, although performance, service and loss prevention are more important than reimbursements.

### Examples of mitigating resource tools (not an endorsement):

- Audit My PC ([auditmypc.com](http://auditmypc.com))
- Microsoft Security Assessment Tool (MSAT) for security breaches caused by the Internet
- Microsoft Baseline Security Analyzer (MBSA) for workstations

– Center for Internet Security (cisecurity.org) has online benchmarks and scoring tools for assessing security.

### Implementing Security Measures

- Provide physical security as with any other asset, including building security and access codes, visual awareness, locking up servers in a separate room, and locking laptops to a desk or equivalent item.
- Establish written policies governing the custody and care of portable laptop and other computers.
- Ensure that all personnel are aware of the policies.
- Strictly define user permissions and restrictions so that users don't have any more rights or access to a program or system than they need, also known as the "least privilege" concept. Don't allow users to install or uninstall software. Excessive user rights and unauthorized devices can allow malware to do extra harm and lead to large losses of data.
- Apply security updates — Apply all software security updates to your computer. Once a software vulnerability is identified, most software companies issue software updates. For example, enabling Microsoft Windows Update will ensure that your operating system and Office software are secure from most common threats.

Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

Infection Methods

### Malware Actions

Malware on the basis of Infection Method are following:

**Virus** – They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

**Worms** – Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.

**Trojan** – The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

**Bots** –: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet.

#### **Malware on the basis of Actions:**

**Adware** – Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.

**Spyware** – It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection.

One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

**Ransomware** – It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.

**Scareware** – It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.

**Rootkits** – are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.

**Zombies** – They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

Theft of intellectual property means violation of intellectual property rights like copyrights, patents etc.

Identity theft means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.

Theft of equipment and information is increasing these days due to the mobile nature of devices and increasing information capacity.

Sabotage means destroying company's website to cause loss of confidence on part of its customer.

Information extortion means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

These are the old generation attacks that continue these days also with advancement every year. Apart from these there are many other threats. Below is the brief description of these new generation threats.

**Technology with weak security** – With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices

**Social media attacks** – In this cyber criminals identify and infect a cluster of websites that persons of a particular organization visit, to steal information.

**Mobile Malware** –There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes for Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus on the device.

**Outdated Security Software** – With new threats emerging everyday, updation in security software is a prerequisite to have a fully secured environment.

**Corporate data on personal devices** – These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.

**Social Engineering** – is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list, he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.

### **Risk Assessment Tools**

Risk assessment tools, sometimes called “risk assessment techniques,” are procedures or frameworks that can be used in the process of assessing and managing risks. There are many ways to assess risk, making risk assessment tools flexible and easy to use for a variety of jobs, industries, and needs.

#### **Most Commonly Used Risk Assessment Tools**

There are four commonly used risk assessment tools in different businesses. All of them are used often and are easily applicable to different situations. These tools are:

1. Risk matrix
2. Failure Mode and Effects Analysis (FMEA)
3. Decision Tree
4. Bowtie Model

### **Risk Matrix**

Likelihood		Very Likely	Likely	Unlikely	Highly Unlikely
Consequences	Fatality	High	High	High	Medium
	Major Injuries	High	High	Medium	Medium
	Minor Injuries	High	Medium	Medium	Low
	Negligible Injuries	Medium	Medium	Low	Low

A risk matrix is a visual representation of risks laid out in a diagram or a table, hence its alternate name as a risk diagram. Here, risks are divided and sorted based on their probability of happening and their effects or impact. A risk matrix is often used to help prioritize which risk to address first, what safety measures and risk mitigation plans to take, and how a certain task should be done. Risk matrices can come in any size and number of columns and rows, depending on the project and risks being discussed.

### FMEA

The Failure Mode and Effects Analysis (FMEA) risk assessment tool was first discovered in the 1940s by the US military to identify all possible issues or failures in a design, process, product, and service. This tool is often used during a product or service's design or proposal stage to actively study possible risks and discover their effects. FMEA has two parts to it:

- Failure Modes: the failures, problems, and issues that occur
- Effects Analysis: the analysis of the failures' effects

## Decision Tree



Risk Assessment Tool: Decision Tree

The decision tree risk assessment tool works by providing project managers a template to calculate and visualize the values of different results and the likelihood of achieving them. In some cases, a decision tree is also often used to help calculate the value of a project, product, or service.

To use this tool, one starts with one element, product, or service they want to evaluate, and then creates different branches from it with different goals. When carried out, the final product looks like a flowchart similar to a tree with different branches, hence the name.

## Bowtie Model



Risk Assessment Tool: Bowtie Model

The Bowtie Model risk assessment tool aims to show the causal links between different sources of risks and their consequences. The left side of the diagram shows what causes the risk, the right shows their potential outcomes, and then both sides meet in the middle with a single risk called "Event." The left and right sides of the Event are larger and wider as many sources may lead to different consequences, but still be centered around one risk. When drawn out, the model starts to look like a bowtie.

## Uses



Risk assessment tools are an essential part of performing risk assessments and risk management tasks. Not only do they make risk assessments easier, but they also help put different risks into perspective and help create contingency plans better.

Some things risk assessments tools can help with are:

- Creating and spreading awareness on different hazards and risks
  - Identifying who are most at risk of encountering or suffering from certain risks
  - Determining what control measures and programs are required for which risks and what need to be changed in existing rules
  - Preventing and mitigating injuries, fatalities, and illnesses
  - Meeting legal requirements on certain industry-specific tasks where applicable
- **Use antivirus software** — Antivirus software is a must. There are countless ways a computer can get a virus, and the range of harm can vary from slowing down the computer to stealing data from it. Antivirus companies constantly update virus definitions to defend computers against new threats, and for the most part these software updates are seamless to the user. Most antivirus software includes spyware, adware and email attachment protection. If not, they should be deployed along with antivirus software.

• Ensure that your computers and networks, especially wireless networks, are protected by a firewall. Secure your network and your computer so they are not visible to everyone on the Internet. Firewalls block outside access to the computer and are available in both hardware and software forms. Many standard and wireless routers come with a built-in firewall. They should be configured to block all non-Internet and e-mail traffic in and out of your network. Some software may require special configuration.

Firewall software should also be regularly updated. If that task is too daunting, you can simply buy a new router, which in some cases may be cheaper than hiring someone to update the software. If you are using a wireless router, disable SSID (Service Set Identifier) broadcasting and use strong passwords to secure access. For best protection, you should limit devices that can access your wireless network, using MAC (Media Access Control) addresses of the devices. There is also software for intrusion detection and prevention but the cost and complexity can be prohibitive for small businesses.

• Use strong passwords. It is convenient not to have to enter a username and password every time you start using the computer; however, not entering them makes it equally convenient to steal data off your computer without your knowledge. Usernames and passwords are the basic building blocks of security. Use a complex (or strong) password that cannot be guessed within the account lockout attempts. Passwords should be changed frequently. In addition, always use a password-protected screen-saver to prevent unauthorized access in your absence.

– Don't use passwords based on personal information that can be easily accessed or guessed; make them counter-intuitive.

– Don't use a complete password that can be found in any dictionary of any language.

– Use both lowercase and capital letters.

– Make passwords at least six characters long; use both lowercase and capital letters and a combination of letters, numbers and special characters such as <, } and ~.

– Misspell or "salt" words with special characters (e.g., "D@Wg&PoN1\$#0").

– Use different passwords on different systems.

– Use automated systems that change passwords at least every 90 days.

– Don't leave a password someplace for people to find, such as in your desk.

– Use screensaver passwords that lock out the screen after 15 to 30 minutes.

• Create backup copies of all important data and information on a regular basis. The frequency of backup

depends on: how often your data changes; and the impact on your business if you lose the data between the

last backup and the time of loss. Store and secure backup copies away from your office location and use encryption to protect any sensitive information about your firm and clients. Regular backups better ensure that critical data is not lost in the event of a cyber-attack or physical incident such as a fire or flood.

- Encrypt your client data to protect it from hackers and thieves. The following are three basic areas to be

considered:

**Hard-Drive Encryption** — Secures data in case you lose a computer or someone steals it. Hard-drive encryption locks down the computer after several unsuccessful login attempts. The most common technique for stealing data is to plug the hard drive into another computer (i.e., drive swapping), and almost all hard-drive encryption software prevents this kind of theft. Another reason to encrypt your hard drive is to prevent thieves from stealing your business data with hard-drive recovery software, which can happen when you recycle your computer.

- **Data Encryption** — If you use software that stores data in a detached database or other structured data formats, consider encrypting sensitive data like Social Security numbers, tax ID numbers, driver's license numbers, etc., on individual data element level. Most software programs are designed to be portable and scalable, but the downside of portability is that someone can walk away with the database or the backup of the database and read all of the sensitive information. When purchasing or designing software, ask vendors if the sensitive data can be encrypted in the individual data element level.

- **File Encryption** — E-mail has become the number one collaboration tool used to exchange files with sensitive data in them. Plain text e-mail and attachments can be read by people sniffing e-mail on the Internet cloud or by someone who can reach your computer. The common practice of leaving your computer unlocked and using the "remember my password" check-box means anyone who can get to your computer can read all of your e-mail, some of which may contain sensitive data about your business or clients. A good example of a low-cost and robust solution to that problem is Adobe PDF, which encrypts files with a password or phrase. In the standard version of Adobe Acrobat, you can lock your document with a password, and Adobe will use that password or phrase to encrypt the document. For added security, the password should be communicated over the phone.

- Remote Mobile Device Security enables a user to prevent access to protected files in the event a computer has been lost or stolen. Protected files are encrypted, and the application periodically authenticates the identity of the user. Some programs will track laptops when they are connected to the

**E-mail Digital Certificates** — File encryption protects attachments, but it does not help if you are exchanging sensitive data in the e-mail message body. One solution is to sign your e-mail with a digital certificate that encrypts the entire e-mail message so that only the intended recipient can read it. It also ensures the e-mail message has not been altered or manipulated. An e-mail digital certificate requires some preparation to set-up, and you have to maintain the subscription of your certificate. Digital certificates can be purchased from security identity management companies like Verisign, Thawte and GoDaddy, on annual, three- or five-year renewal terms.

**E-mail Spam Filter** — E-mail scams not only hamper office productivity but are also a big security threat. Often the scam appears to be from someone you know or some legitimate

organization, but it has a virus or spyware attached to it, or it directs you to a website that can infect your computer. Hackers are constantly developing new techniques to fool end-users and spam filters, so be sure to use e-mail spam filtering services from a reputable company that is constantly investing in improving their spam filter engines.

- **Internet Usage** — There are some simple best practices when using the Internet on your work computer. Never download free movies, music and software unless the vendor and product are reputable (e.g., Adobe Acrobat). Most of these sites are not well maintained and are a breeding ground for computer viruses and spyware. Limit your Internet usage to legitimate websites only. Many illegitimate websites, foreign and domestic, exploit software weaknesses to install spyware on your computer. Don't let anyone play online games on your work computer, as many viruses are downloaded unknowingly that way.

- Erase or destroy all data on hard drives when recycling them. The Environmental Protection Agency has been known to fine enterprises \$200,000 for not having documented proper computer disposal. An audit trail of serial-numbered inventory of equipment, and certification that personal data has been destroyed, will go a long way toward helping the firm meet the burden of proof in the event of investigation or litigation. This function can be outsourced to an external service provider. More information can be found on major vendor sites such as dell.com, hp.com, or ibm.com.

- Be prepared for emergencies. Create a contingency plan for continuing business operations (at an alternate location if necessary) and for recovering from an emergency. Test or review the plan annually.

### **Personnel**

- Conduct regular computer security awareness training for all computer users, including executives, IT staff and others with privileged access. Training sessions should enhance awareness of all risks, including social engineering and web application attacks. Tools alone cannot fully protect a firm from all computer and data security threats. Users need to also educate themselves on best practices. Many training organizations offer training classes, and there are many resources on the Internet to help educate users security-related topics.

- Test training results. One way to test awareness is by "inoculation," in which all users are sent phishing e-mail that is benign. Those who err are then educated or lose their user rights.

- Who is responsible for safeguarding information at your firm? Someone with the firm should take ownership of this responsibility.

- Ensure that security requirements are addressed by the firm's policies and procedures. Develop specific policies governing the custody and care of mobile devices and other computers. Ensure that all personnel are aware of the policies.

- Institute internal controls and background checks for key personnel.

**Individual Activity:**

- *Prepare risk matrix.*
- *Identify and assess Risk.*



**Self-check quiz 2.1**

Check your understanding by answering the following questions:

Write the correct answer for the following questions.

1. What is IT risk assessment?

Answer:

2. How Quantitative IT risk assessment Conducted?

Answer:

3. What is Virus?

Answer:

4. What are Bots?

Answer:

5. What is Ransomware?

Answer:



## **Learning outcome 2.2- Implement risk control**



Contents:

- Control management for information system security risks.
- Likelihood of risks
- Impact of risks.
- Risks determination
- Risk-level matrix.
- Inherent and residual risks



Assessment criteria:

1. Control management is performed for information system security risks.
2. Likelihood of risks are determined.
3. Impact of risks are analyzed.
4. Risks are determined and put into risk-level matrix.
5. Control of risks are recommended and applied.
6. Inherent and residual risks are analyzed.
7. Results are documented and communicated as per standard procedure.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (Actual or simulated), Server, Necessary software.



### **LEARNING ACTIVITY 2.2**

Learning Activity	Resources/Special Instructions/References
Implement risk control	<ul style="list-style-type: none"> <li>▪ Information Sheets: 2.2</li> <li>▪ Self-Check: 2.2</li> <li>▪ Answer Key: 2.2</li> </ul>



## Information sheet 2.2

Learning objective: to Implement risk control

Companies must adopt risk control strategies when securing their IT environment to identify and neutralize potential cyberthreats before breach incidents occur. The top risk control strategies in information security revolve around identifying and patching potential vulnerabilities, hunting for threats, and rapid incident response should a cyber attack breach perimeter defences.

Every organization is unique, so the risks they each face are not the same. In order to make a plan of action to protect your business, you need to first understand where the threats against you are. Once you know those risks and gaps, you can start to identify the likelihood of them occurring and the impact they could have on your organization.

Because of this, an information security risk assessment forms the cornerstone of any cybersecurity policy. Clear risk knowledge is crucial when making risk-based decisions for your company. Without full knowledge of where, how, and why a threat could occur, you won't be able to stop it. That's why understanding likelihood and impact for any given threat are both important factors in the risk assessment process.

Start thinking about your risks by reviewing the basic threat likelihood/impact formula below.

### **Keep It Simple**

You don't need a complex system in order to improve or support your organization's security environment. However, your organization's leaders need tools that show them where to spend time and resources in order to reduce potential risks to the company. That's how risk assessments can shed light on the key factors in this decision-making process.

A better understanding of the system also helps out other members of your staff. Members of the IT department need to know what products and processes to put into place in order to limit potential risks. The more knowledge they have, the better they can work with leadership to determine and address security concerns. Sharing the risk assessment results with members of the IT team will help them understand where they'll get the most from efforts to reduce risks.

Formula to Determine Risk Likelihood and Impact

The standard described in NIST SP 800-53 implies that a realistic assessment of risk requires an understanding of these areas:

### **Threats to an organization**

Potential vulnerabilities within the organization

Likelihood and impacts of successfully exploiting the vulnerabilities with those threats

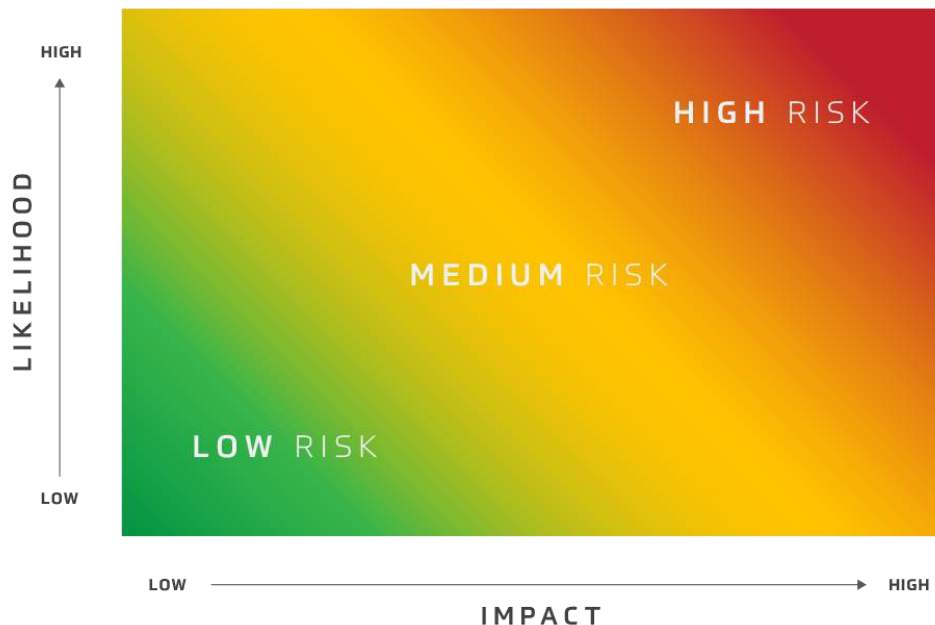
For handling the most basic level of risk assessment, risk managers can follow this simple formula:

$Risk = (Threat \times Vulnerabilities) \times Impact$

The first part of the formula (Threats x Vulnerabilities) identifies the likelihood of a risk. For example, if there's a known security flaw in older versions of software you use, there's the threat of hackers exploiting that particular vulnerability to compromise your system. But if you've applied the latest software patches that fix the problem, then the vulnerability cannot be exploited, and the threat has been eliminated.

Impact measures how much disruption you'll face if the threat actually occurs. Combining likelihood and impact produces a residual risk rating of Low, Medium or High. Each organization's residual risk rating may differ based on the likelihood and impact that each control deficiency introduces.

You could also represent this concept with a simple chart like this one:



For example, let's consider the risk of a hacker getting access to a folder containing all of your public-facing marketing materials. That event may have a medium likelihood, but it has a very low impact. Those materials are already publicly available on your website, etc., so unauthorized access to them does no harm. That risk gets a Low rating.

But the formula changes if the risk is an employee in the Accounts Payable department clicking a phishing link. There's at least a medium likelihood of one of those employees making this mistake. and the impact would be very high if a hacker got access to a user account that controls financial transactions. That risk gets a High rating.

Keep in mind that a very High impact rating could make a risk a top priority, even if it has a low likelihood. If a breach could shut down a hospital's life-support equipment, for example, that risk obviously deserves serious consideration on your priority list.

#### Drilling Down on Specific Residual Risk

Now that you know the formulas for determining likelihood and impact during a risk assessment, it's time to focus on specific risks.

**1. Inherent risk** – This is the risk level and exposure your system faces without taking into account any mitigating measures or controls that are actively in place. Where is your system at its weakest when no other security measures are in place to protect them? Which risks deserve the highest rating based on their likelihood and potential impact?

**2. Residual risk** – An area with a higher likelihood and impact of a threat on the organization, from an inherent risk level, may need additional controls to reduce the level of risk to an acceptable level. After you apply those controls, you are left with what we call "residual risk." If the residual risk level after mitigating controls is still higher than you prefer, then additional risk management measures and techniques should be introduced.

Mitigating measures you may apply include:

**Avoidance** – Elimination of the cause of the risk. You could, for example, prevent employees from accessing certain parts of your system on mobile devices.

**Mitigation** – Reduction of the probability of a risk's occurrence or of its impact. Adding multifactor authentication, for example, greatly reduces the probability of a hacker getting into a user's account.

**Transfer** – Sharing of risk with partners, such as through insurance or other ventures.

**Acceptance** – Formal acknowledgement of the presence of risk with a commitment to monitor it.

Finding Help When You Need It Reading through how to determine likelihood and impact can help you understand first steps in your risk assessment process. But you'll probably still need help from cybersecurity consultants to carry out a full assessment. These experts look over a number of key factors you may not have considered.

Cybersecurity consultants analyze your organization's structure, policies, standards, technology, architecture, controls, and more to determine the likelihood and impact of potential risks. They will also review your current controls and evaluate their effectiveness.

For example, a financial management company turned to Pratum when it realized that investors were choosing portfolio managers based, in part, on a company's strength of cybersecurity. The management firm asked Pratum's consultants to take a deep dive into its administrative, physical and technical controls. Pratum guided the company in developing a clear summary of its high and moderate risks along with recommendations for remediation.

Consultants also assess any gaps between your current security posture and where you want your organization to be. A core part of that process will be determining accountability and assigning risk ownership at the appropriate level and to the appropriate team. It's important to have the right security measures in the right hands.

#### **End Goal: An Acceptable Level of Risk**

The end goal is to get to a level of risk that is satisfactory to your management team. It's important to evaluate and be aware of the risk in your environment so you can implement appropriate controls to mitigate this risk and secure sensitive information. Evaluating risk means understanding the biggest factors of any security threat, likelihood and impact.

#### **Determining risk level:**

In accordance with policy IT-19, Institutional Data Access, Business Owners (as defined in IT-16, Roles and Responsibilities for Information Security Policy) will assess institutional risks and threats to the data for which they are responsible. This risk analysis is then used by Business Owners to classify systems (endpoints, servers, applications) into one of three risk categories:

#### **Low Risk**

System processes and/or stores public data  
System is easily recoverable and reproducible  
System provides an informational / non-critical service

#### **Moderate Risk**

System processes and/or stores non-public or internal-use data  
System is internally trusted by other networked systems  
System provides a normal or important service

#### **High Risk**

System processes and/or stores confidential or restricted data



System is highly trusted by UI networked systems

System provides a critical or campus-wide service

Risk Analysis must take into consideration the sensitivity of data processed and stored by the system, as well as the likelihood and impact of potential threat events. We use a simple methodology to translate these probabilities into risk levels and an overall system risk level.

### Threat Event Assessment

Risk assessment is the compilation of risks associated with various potential threat events. A "threat event" is any event which may cause a loss of confidentiality, integrity, or availability of the system and the data it stores and/or processes.

Although there may be hundreds of potential threat events related to a system, they can be generally organized into three main categories:

#### Loss of Confidentiality:

The system and its data is compromised by external hackers

The system and its data is released publicly without approval

The system and its data erroneously publishes data on public-facing portions of the system (i.e. web page) without authorization

#### Loss of Integrity:

The system and its data can no longer be trusted

The system and its data is not complete or incorrect

#### Loss of Availability:

The system and its data no longer exists (e.g. hard drive failure, system destroyed)

The system and its data no longer responds to valid queries from the user or users (system fault)

The system and its data cannot be retrieved by an authorized user (e.g. Denial of Service Attack)

These threat event categories can then be used to calculate their associated risk level, as well as the overall risk of the system:

SYSTEM:			
Threat Event	Likelihood	Impact	Risk Level
1. Loss of Confidentiality			
2. Loss of Integrity			
3. Loss of Availability			
		OVERALL RISK:	

### Calculating Risk Levels

Risk levels are calculated as the product of the LIKELIHOOD and IMPACT (to the University) of a potential threat event / threat event category:

		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood ↑	Very Likely	Low	Moderate	High	High	High
	Likely	Low	Moderate	Moderate	High	High
	Possible	Low	Low	Moderate	Moderate	High
	Unlikely	Low	Low	Moderate	Moderate	Moderate
	Very Unlikely	Low	Low	Low	Moderate	Moderate

For example, a threat event where the likelihood is "unlikely" and the impact is "moderate" equals an assessed risk of "Moderate":

		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood ↑	Very Likely	Low	Moderate	High	High	High
	Likely	Low	Moderate	Moderate	High	High
	Possible	Low	Low	Moderate	Moderate	High
	Unlikely	Low	Low	Moderate	Moderate	Moderate
	Very Unlikely	Low	Low	Low	Moderate	Moderate

As a general rule, networked systems that process data protected by federal or state regulation (HIPAA, FERPA, FISMA, ITAR, et. al.) or industry standards (PCI-DSS) are considered high-risk systems. This is because the likelihood of compromise is (at a minimum) possible, while the impact (due to regulatory or industry standard violation) is considered a severe loss of confidentiality.

The risk level for each threat event category is then calculated. The overall risk level for the system is equal to the HIGHEST risk level for any risk event. For example:

SYSTEM: IT Admin Laptop			
Threat Event	Likelihood	Impact	Risk Level
1. Loss of Confidentiality	Possible	Severe	HIGH
2. Loss of Integrity	Unlikely	Minor	LOW
3. Loss of Availability	Possible	Significant	MODERATE
OVERALL RISK:			HIGH

Because one of the risk events was rated as "High Risk", the overall risk level for the system is High.

### Inherent risk

Inherent risk refers to the amount of risk that exists absent any controls at all. This includes all risks to an organization before the organization implements any countermeasures.

For example, in the accounting world, an inherent risk might be management using its own judgment for key estimates included in financial statements — judgments made without following any specific procedure, or without requiring any documentation to show why management picked the estimate it did. In cybersecurity, an inherent risk might be the threat of data theft when the company uses no encryption or no security in its web browsers.

### **Residual risk**

Residual risk is the risk that remains after your organization has implemented all the security controls, policies, and procedures you believe are appropriate to take. Put another way, residual risk can affect your business even after taking all the security measures.

Residual risk refers to those risks that remain even after applying all the controls you intend to use. For example, suppose you implement a password policy that requires employees to use complex passwords. You decide to make the policy stricter by asking employees to change these passwords every week.

While the residual risk of hackers guessing the password would be low, the residual risk of employees using new passwords that vary only slightly from the old — or perhaps jotting them down on a post-it note — would be high. You now have to decide the amount and type of residual risk you're willing to accept.

**Individual Activity:**

- *Carry out Server and device security control.*



Self-check quiz 2.2

Check your understanding by answering the following questions:

1. What are the categories of the risk?

Answer:

2. How can you calculate risk level?

Answer:

3. What is Residual risk?

**Answer:**



## Learning outcome 2.3 – Mitigate information system security risks



Contents:

- Risk mitigation strategy.
- Risk mitigation tools.
- Cost-benefit analysis.
- Control category.



Assessment criteria:

1. Risk mitigation strategy is outlined.
2. Risk mitigation tools are determined.
3. Cost-benefit analysis is prepared following standard procedure.
4. Control category is determined and applied.



Resources required:

Students/trainees must be provided with the following resources:

Workplace (actual or simulated), class room, trainee handbook and Operating system



### **LEARNING ACTIVITY 2.3**

Learning Activity	Resources/Special Instructions/References
Mitigate information system security risks	<ul style="list-style-type: none"> <li>▪ Information Sheets: 2.3</li> <li>▪ Self-Check: 2.3</li> <li>▪ Answer Key: 2.3</li> </ul>



## Information sheet 2.3

Learning Objective: to mitigate information system security risks

Risk mitigation is a strategy to prepare for and lessen the effects of threats faced by a business. Comparable to risk reduction, risk mitigation takes steps to reduce the negative effects of threats and disasters on business continuity (BC). Threats that might put a business at risk include cyberattacks, weather events and other causes of physical or virtual damage. Risk mitigation is one element of risk management and its implementation will differ by organization.

Risk mitigation involves the use of security policies and processes to reduce the overall risk or impact of a cybersecurity threat. In regard to cybersecurity, risk mitigation can be separated into three elements: prevention, detection, and remediation. As cybercriminals' techniques rise in sophistication, your organization's cybersecurity risk mitigation strategies will have to adapt to maintain the upper hand.

### **Risk mitigation strategies**

Proactive cybersecurity risk mitigation is quickly becoming the only option for organizations as the likelihood of experiencing a cyber attack is all but guaranteed. Here are some strategies for mitigating cybersecurity incidents across your IT ecosystem:

#### **1. Conduct a risk assessment to determine vulnerabilities**

The first step in a cybersecurity risk mitigation strategy should be to conduct a cybersecurity risk assessment, which can help uncover potential gaps in your organization's security controls. A risk assessment can offer insight into the assets that need to be protected and the security controls currently in place, and conducting one can help your organization's IT security team identify areas of vulnerability that could be potentially exploited, and subsequently prioritize which steps should be taken first. Cybersecurity ratings are a great way to gain a real-time look at your organization's cybersecurity posture, including that of your third- and fourth-party vendors.

#### **2. Establish network access controls**

Once you have assessed your assets and identified high-priority problem areas, the next step is to establish network access controls to help mitigate the risk of insider threats. Many organizations are turning to security systems such as zero trust, which assesses trust and user access privileges on an as-needed basis depending on each user's specific job function. This helps minimize both the likelihood and impact of threats or attacks that occur due to employee negligence or a simple lack of awareness of cybersecurity best practices. Additionally, as the number of connected devices on a network increases, endpoint security will also become a growing concern.

#### **3. Implement firewalls and antivirus software**

Another important cybersecurity risk mitigation strategy involves the installation of security solutions such as firewalls and antivirus software. These technological defenses offer an additional barrier to your computer or network. Firewalls act as a buffer between the outside world and your network and gives your organization greater control over incoming and outgoing traffic. Similarly, antivirus software searches your device and/or network to identify any potentially malicious threats.

#### **4. Create a patch management schedule**

Many software providers release patches consistently, and today's cybercriminals are aware of that. As such, they can quickly determine how to exploit a patch almost as soon as it is released. Organizations should be aware of the typical patch release schedule among their service or software providers to create an effective patch management schedule that can help your organization's IT security team stay ahead of attackers.

## 5. Continuously monitor network traffic

Proactive action is one of the most effective strategies for mitigating cybersecurity risk. With roughly 2,200 attacks occurring every day, the only way to truly stay ahead of cybercriminals is to continuously monitor network traffic, as well as your organization's cybersecurity posture. To truly enable real-time threat detection and cybersecurity risk mitigation, consider tools that allow you to gain a comprehensive view of your entire IT ecosystem at any point in time. This will allow your IT security team to more actively identify new threats and determine the optimal path to remediation.

## 6. Build an incident response plan

Ensuring that everyone, including both the IT security team and non-technical employees, knows what they're responsible for in the event of a data breach or attack can make it easier to have resources in place and ready to go. This is known as an incident response plan, and it is one of the most critical components to mitigating cyber risk in your organization's evolving network environments. Threats can come from anywhere and they are continuously growing in sophistication, meaning it's becoming increasingly impossible to be 100% prepared for data breaches. An incident response plan helps your organization do as much as possible to remain proactively prepared so your team can move quickly and efficiently to remediate any issues.

### 1. Workscope



[Workscope](#) provides a platform where organizations can map, manage and improve the user-end computing industry. This platform provides a real-time contextual view of the spreadsheet which you have typed. These spreadsheets help users to understand the business process of companies. Whether you want to demonstrate operational resilience or understand the time and materiality associated with the making of spreadsheets, Workspace is the software for you. Workspace can provide solutions to all the spreadsheet-related problems without changing any business management services or manual intervention.

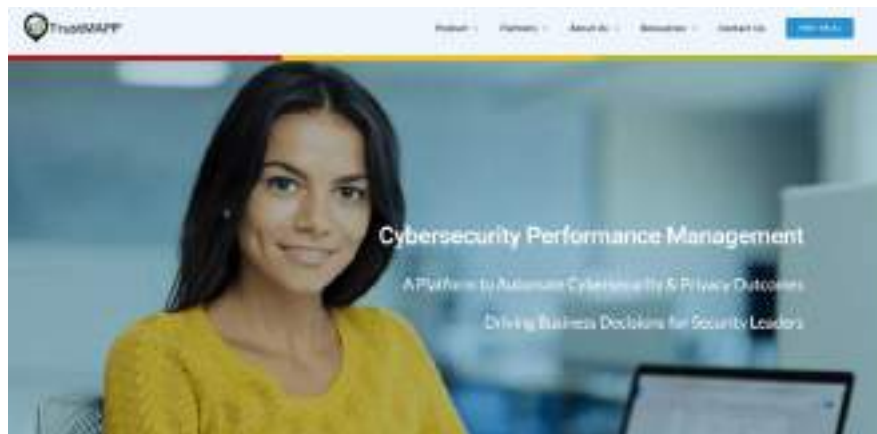
#### Key Features:

Without manual overhead, you can discover opportunities. You can automate the discovery services and pinpoint the most effective opportunities and manage the necessities.

End-to-end tracking of data maps relationships between sources of data and spreadsheets. This helps to understand the data risks, data dependencies, and data sources.

Automatic checking of data makes it for users and managers to maintain compliance. You can access an unlimited number of models, without any fees. Identify and analyze before you migrate to new versions of Microsoft Office for business processes. Workscope provides the tools to minimize disruption in the business schedule. Error checking is automatic to avoid risks and develop the spreadsheet quality with the help of productivity tools.

## 2. TrustMAPP



[TrustMAPP](#) platform provides the necessary tools and support needed to upgrade cybersecurity discussion into the wider business. The TrustMAPP Cybersecurity Performance Management system is used by companies that empower IT, security leaders, to identify and communicate with the executive stakeholders. TrustMAPP helps IT, leaders, to get a clear vision for how the cybersecurity system adds value to the companies.

Key Features:

TrustMAPP provides Turnkey Assessments which helps in an easier workflow. These are easier to build templates for your companies.

This platform provides real-time results as soon as the assessments are performed.

Complete budgetary guidance is provided by TrustMAPP to guide your redemption efforts and expenses.

TrustMAPP gives project management tools, also known as redemption tools to keep a check on your team's progress.

## 3. TeamSuccess

### Build a Successful Software Development Team

✓ Each project and team is unique. Try to find root causes, iterate, and experiment. Adopt a mindset of continuous improvement.

Team Flexibility	Purpose & Team Values
<ul style="list-style-type: none"><li>Is your team open to exploring different ways of doing things?</li><li>Do you achieve goals together, by using the talents and strengths of all your team members?</li><li>Does your team share responsibility for team development?</li><li>Is there a "no-blame culture"? Do you all feel safe to report issues or potential risks?</li></ul>	<ul style="list-style-type: none"><li>Are you committed to a common purpose? Do you all know what your team's work is and why it is important?</li><li>Are your team goals clear, challenging, agreed on and relevant to the purpose of the company?</li><li>Do you have clearly defined strategies for achieving goals, which you all agree on?</li><li>Are individual roles and responsibilities clear? And their relationship to your team's purpose and goals understood?</li></ul>



[TeamSuccess](#) is an easy-to-use risk management tool that empowers companies to control risks associated with the business. The system software of TeamSuccess enables managers to make team members agree to each risk and monitor risk continuously.

Key Features:

Each risk is monitored cautiously and the responsibility depends on every team member.

Provides tools that help in the management and maintenance of privacy of users' data.

Every employee is responsible to maintain compliance and contribute to the company's management system.



#### 4. Tanium Reveal

Tanium Reveal helps to search and monitor data across any number of endpoints. It eliminates data movement and improves data-handling services. Tanium Reveal helps to unify teams across companies' data management services. Tanium Reveal reduces IT infrastructure and helps improve efficiencies through risk inventory.

Key Features:

The Tanium Reveal platform aligns teams with complete, high-quality data services across the globe.

This platform helps to control the entire IT estate and departments within seconds with minimal impact on network services.

Tanium Reveal provides clear visibility into every endpoint and helps to manage and check accurate and real-time visibility.

#### 5. STREAM Integrated Risk Manager



[STREAM Integrated Risk Manager](#) platform provides an insight into IT operational risk which helps companies to make proper strategic decisions. Through a centralization system, STREAM reduces manual processes, eliminates risks in business, and builds stakeholders' positions.

STREAM Integrated Risk Manager is designed to meet the complex risk management needs of the leading companies. It is practical and easy to implement and delivers values within weeks.

Key Features:

This platform helps see all the factors involving risk to your organization and update automatically as they change.

STREAM Integrated Risk Manager uses configurable quantitative and qualitative assessments and determines the significance of each risk involved.

The Test for Tolerance is high in STREAM Integrated Risk Manager and helps to compare the risk profiles against companies' risk tolerance services.

You can check the best practices by planning your responses and laying out pre-configured data catalogs making details of the best practices to eliminate threats.

ROI-based security investments improve maturity readiness. It analyses the security investment needs and provides solutions.

## 6. SafePaaS



[SafePaaS](#) is a leading company that provides cybersecurity and risk management tools to help organizations efficiently monitor the real controls and manage risks against the company. Its risk management services enable companies to control IT investments and turn cybersecurity risk management obstacles into optimum business performance. SafePaaS is the one place solution for secure and trusted information management in wider applications.

Key Features:

AccessPaaS is a trusted access platform that allows you to improve performance by reducing costs.

ProcessPaaS ensures secure collaboration in the Cloud and On-Premise apps.

ARCPaaS is used for monitoring the datasheet attached. It includes an Audit Manager for automation.

This platform monitors Ent The enterprise Risk involved and reduces frequency and severity of loss occasions.



## 7. Reciprocity

[Reciprocity](#) offers optimal solutions to elevate a company's compliance program to the highest infosec level. The Clio cloud-based solutions stand perfectly with the GRC program. Using the GRC program you can continuously monitor and customize audit management needs. ZenGRC acts as a central platform to guide your company throughout the whole management system.

Key Features:

The automatic nature used by this platform reduces manual effort and helps in the efficient management of the system.

Risk management tools that are bolted on helps to secure the privacy of the user information.

It provides risk visibility and reports are shown on the company's dashboard.

Provides simplified and shortened audit management systems to increase the working capabilities.

## 8. LogicGate Risk Cloud



[LogicGate Risk Cloud](#) is a cloud-based form that offers risk management applications that helps businesses to govern their processes. It combines high-level intent with easy services to create a proper view of the risk programs involved.

Key Features:

Dozens of GRC applications are available on this platform to choose from. You can also build your personalized applications.

All your data is stored in one platform which provides better insights and it's easy to find the right data at the right time.

The manual processes are automated which eliminates duplicate values and checks them. The platform provides flexible connections for data points from various applications.

This GRC platform is built by GRC experts and customer service is top-rated and considered as prior for the company.

## 9. Fastpath Assure



[Fastpath Assure](#) is a cloud-based platform that can track, inform and mitigate access risks involved and shows in the dashboard. It comes with a pre-configured combination of duties set specifically for ERP/CRM systems. Using Fastpath Assure clients can easily see what access users have, generate reports, and record sign-offs. The automated process can cut off audit time from weeks to hours.

### Key Features:

The tools provided by Fastpath Assure are very easy to use and provide real-time results.

It gives fast solutions to your issues offering automated solutions.

The work time of Fastpath Assure is really saving and one can use it to cut off audit time as needed.

Cost-benefit analysis (CBA) is a method used to evaluate a project by comparing its losses and gains — essentially a quantified and qualified list of pros and cons. CBA is a useful way to assess business projects because it reduces the evaluation complexity to a single price figure. As you can imagine, this makes CBA an invaluable tool when it comes to explaining the intricacies and selling the value of a robust cyber security strategy to key stakeholders.

### Applying a Cost-Benefit Analysis to Your Risk Assessment

Remember, applying a CBA to your risk assessment is all about determining the risks you are willing to accept and comparing the costs of those risks against the benefits. This involves thinking about the direct and indirect risks you face, as well as the direct and indirect costs that could arise as a result of taking these risks. Examples of each include:

Direct costs: Ransom payments, or expenditure associated with identifying, mitigating and quarantining a threat.

Indirect costs: Downtime, operational disruption, reputational damage, time and internal resources, and legal and non-compliance fees.

It's helpful to think about both direct and indirect factors when applying a CBA to your risk management strategy. For instance, you might compare:

The cost of business income disruption (direct) and lost productivity (indirect) due to a ransomware attack vs the cost of preventing a data breach by investing in an endpoint security system.

The cost of operational disruption (direct) and a decrease in future revenues (indirect) vs the cost of preventing an attack by investing in building an in-house team.

Much of a CBA involves coming up with options that you could undertake to achieve your project's objectives — so you'll want to keep breaking things down and playing with various risks, costs and outcomes. For instance, you might look at the costs vs benefits of factors like:

Varying timescales for executing the strategy, or different components of the strategy.

Various budgets for the project. The NIST Cyber Security Framework and the Gordon-Loeb Model can be helpful here — for example, they reason that organisations should generally spend less than 37% of the expected loss from a cyber security breach on the preventative/strategic budget.

The costs of outsourcing cyber security services vs achieving them in-house.

The potential costs of protecting individual data assets and vulnerabilities vs the cost of these assets being breached.

Strategising effectively is all about placing risk within the context of your own business and its unique appetite for risk. However, you'll probably start to see a pattern emerge: preventative cyber security measures usually more than pay for themselves — particularly if approached in a cost-effective way.

Pro tip: To really highlight a cyber security strategy's value to stakeholders, you might also find it helpful to include a 'do nothing' or 'do minimum' option.

### Doing More with Less

At the end of the day, you should always be looking for the most effective way to deliver the outcomes you need. There is generally a cost/benefit trade-off between investment and risk. However, not all investments are equally costly.

For example, endpoint security systems partnered with managed detection response (MDR) services, such as those we offer at Six Degrees, are a great paired solution that delivers increased security and agility at limited cost. MDR and endpoint is also an ideal response to the challenges created by remote working and remote access that are likely to define much of 2021 and beyond.

In addition to delivering on-demand talent, working with a service provider enables you to:

Develop a more flexible, iterative and future-proof approach to cyber security.

Gain access to insider threat intelligence and risk insights.

Stay focused on core business competencies.

Pro tip: Full protection is never guaranteed. In the unfortunate event of an attack or failure, savvy management and effective response can significantly reduce the impact on your business — another instance of the benefit outweighing the cost.

### Preventative Action Can Be Cheaper

Risk management is all about managing uncertainties. When it comes to preventing costly attacks, there's significant value to be found in investing upfront in order to avoid paying a higher price later.

Ultimately, cyber security is a journey, not a destination. Any investment you make should be agile and flexible enough to meet both current and future demands. Six Degrees offers the capabilities and expertise you need to ensure business continuity in 2021 and beyond.



## Self-check quiz 2.3

Check your understanding by answering the following questions:

Write the appropriate/correct answer of the following:

1. What is risk mitigation?

Answer:

2. Write down the Risk mitigation strategies

Answer:

3. Write down the name of three risk mitigation tools

Answer:



## Learning outcome 2.4 Manage Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)



Contents:

- Business Continuity Plan (BCP)
- Business Impact Analysis (BIA)
- Disaster Recovery Plan (DRP)



Assessment criteria:

1. Business Continuity Plan (BCP) is interpreted.
2. Business Impact Analysis (BIA) is interpreted.
3. Business Impact Analysis is performed as per standard procedure.
4. Business Continuity Plan (BCP) is prepared as per industry standard.
5. Disaster Recovery Plan (DRP) is interpreted.
6. Disaster Recovery Plan (DRP) is prepared as per industry standard.



Resources required:

- Students/trainees must be provided with the following resources:
- Workplace (actual or simulated), class room, trainee handbook and Data center



### LEARNING ACTIVITY 2.4

Learning Activity	Resources/Special Instructions/References
Interpret data center security and operations	<ul style="list-style-type: none"> <li>▪ Information Sheets: 2.4</li> <li>▪ Self-Check: 2.4</li> <li>▪ Answer Key: 2.4</li> </ul>



## Information sheet 2.4

Learning Objective: to manage Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

### Business Continuity Plan

This involves the development of a Business Continuity Plan (BCP) designed to ensure the recovery of critical business activities from natural or man-made failures or disasters to an acceptable level within a predefined time frame, thereby minimising the impact of losses to the organisation. Implementing a BCP is essential for every business.

Business continuity planning involves the following five major processes:



### Critical Business Activities Identification

It is crucial to understand where a company needs to focus on in order to recover in case of an incident. The first step in business continuity planning is to identify the most critical business activities to your company's survival. You need to have a good understanding of your business, including its objective, products, services, resources, facilities, suppliers, customers, and their interdependencies.

Critical business activities are those that must be present to sustain the continuity of business, where failing to performing them would lead to:



- Major revenue losses;
- Failure to meet regulatory or contractual requirements;
- Compromise of operational efficiency, or
- Loss of customer / damage of reputation.

Once the critical activities are identified, you should perform analysis on each of them to determine the priority and objective on the recovery of critical business activities based on their importance to the company's achievement of strategic goals. Typical questions to be considered include:

- What are the operational, financial and other competitive impacts to the company if the activities are not functioned?
- How quickly do the activities need to be back in production for your company to survive?
- How much data and financial losses can you afford?

For each of the critical business activity identified, it is also necessary to find out all the supporting resources needed to perform the activity and the effect on the business of the unavailability of the resources. Listed below are the areas of resources you should consider:

- People;
- Information technology (service, application, network, data);
- Data and voice communication;
- Paper-based documents and records;
- Physical infrastructure, key equipment and facilities; and
- External services / products dependencies.

### **Business Continuity Risk Assessment**

A disaster could happen to any company – no matter the business size. Risk assessment on critical business activities should be conducted, identifying possible risks and assessing the likelihood and impact of disruptive events. It is vital that you understand the disruptions that would be disastrous to the running of your business. Different disaster scenarios should be considered, some common threats include:

- Natural disaster, such as earthquake, fire, typhoon, flood;
- Loss of key equipment / information system / facility;
- Disruption of external telecommunications services;
- Utility outage, such as failure of power supply;
- Loss of life, disease, health & safety issues; and
- Terrorism & cyber attack.

Risk assessment against different threats may result in different outcomes. Some may require no action, while some require continuity planning to be developed and supported with additional resources. This will help a company to explore the possible effects of disaster incidents. After that, risks can be prioritised against objectives relevant to the organisation, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

### **Business Continuity Plan Development**

Business Continuity Plan (BCP) allows you to prepare for the worst situation that would keep your business from being operational and to minimise service disruption as well as financial loss. The plan only needs to include the business activities that are most critical to keep your company up and running.

Based on the results from the analysis made on critical business activities and possible risks, you can start developing business continuity and recovery strategies. The selection of strategy may depend upon the criticality of business activities, cost, time for recovery and security.

Listed below are the typical items included in a BCP:

- Individual roles and responsibilities;

- Conditions for its activation;
- Processes to be followed;
- Escalation plan;
- Emergency procedure to handle incident;
- Temporary operational procedure;
- Resumption procedure;
- Fallback procedure; and
- Maintenance schedule and process for testing the plan.

For a small company, a BCP may be simply a printed manual stored safely away from main working location, with emergency contact information, location of offsite data backup storage media, copies of insurance contracts, and other critical material necessary for survival of the business.

The purchase of suitable insurance may be considered as part of the overall business continuity process to recoup losses from risks that cannot be completely prevented or controlled. The decision to obtain insurance should be based on the likelihood and degree of loss identified. Please note that insurance should not be treated as a substitute for an effective BCP since it does not deal with the recovery of business.

Before the plan is put into practice, testing should be conducted to ensure it is effective. Testing may include simulations, business process test, technical recovery and resumption testing, recovery processes testing at alternate site, supplier facilities and services testing etc.

### **Plan Approval and Implementation**

Once a Business Continuity Plan (BCP) is developed, it is important that endorsement should be sought for approval and support.

Points to note during the implementation of BCP:

- BCP should be documented and disseminated to all staff to follow before, during and after disruptive event occurred.
- Awareness training and education for staff should be conducted to help them understanding the business continuity processes and their individual responsibilities and actions to be taken when the plan is invoked. This is to ensure the processes would be carried out effectively.
- Copies of BCP should be stored at remote location and kept updated with the same level of security protection as at the main site.
- Other material necessary to execute the BCP and for organisational survival should also be stored at the remote location, such as offsite data backup storage media and copies of insurance contracts.
- A company may also need to have pre-arrangement with external parties to ensure timely resumption of operations, such as facilities access and telecommunication systems.

### **Regular Review and Ongoing Maintenance**

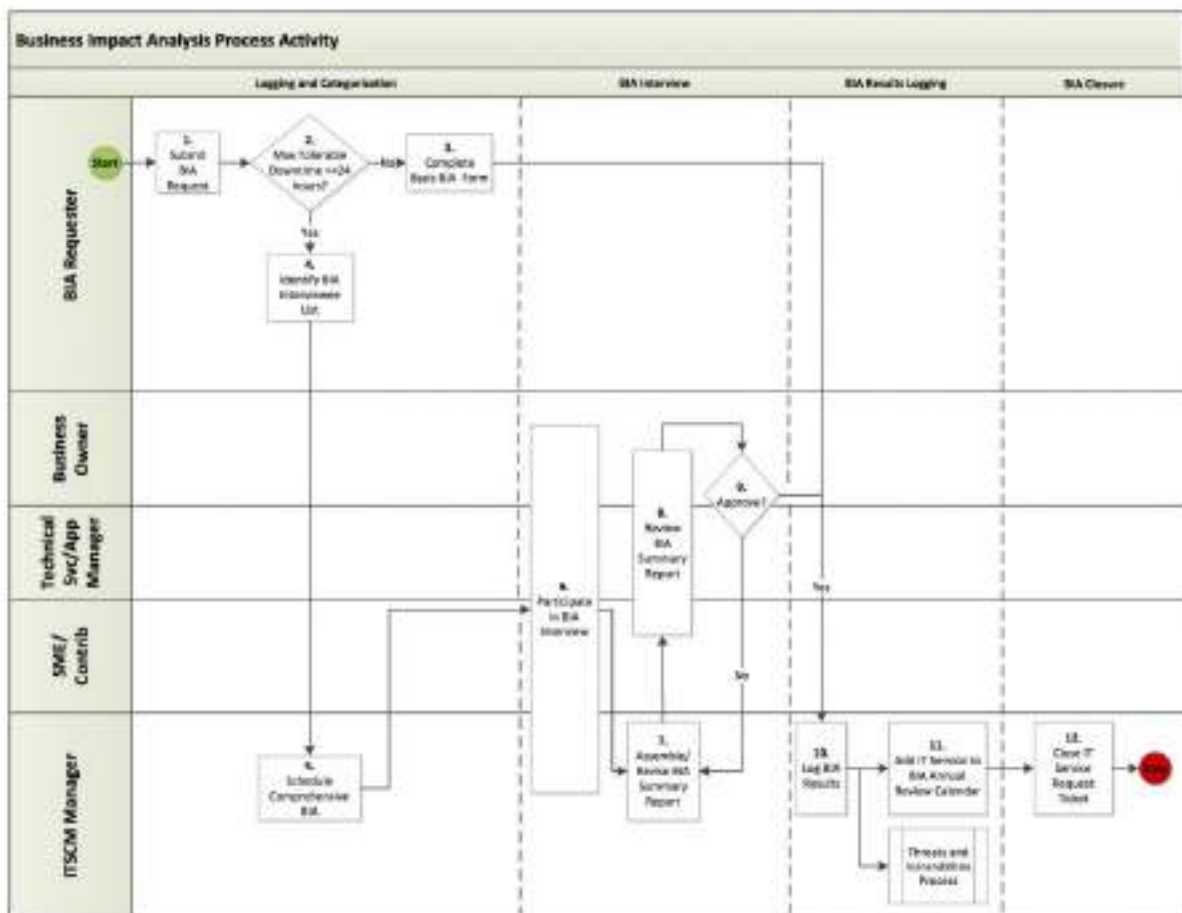
In order to validate the business continuity arrangements, testing, review and ongoing maintenance should be conducted regularly to ensure they are up-to-date and effective.

Points to note during the implementation of BCP:

- Regular review, testing & verification of documented Business Continuity Plan (BCP) and the technical solutions should be conducted regularly, say annually.
- When any new or major change in business requirements / environment are identified, the existing procedures should be updated as appropriate.
- Procedures should be included within the organisation's change management programme to ensure that business continuity matters are always addressed appropriately.
- BCP and the test results should also be subject to independent audit and review.

## Business Impact Analysis (BIA)

A business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organization's business continuance plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. The result is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, UCSF may be able to continue more or less normally if one of the cafes on campus has to close, but would come to a complete halt if the information systems crash.



As part of a disaster recovery plan, a BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, staff and data, and so on. A BIA report quantifies the importance of business components and may suggest appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts in areas such as safety, finances, marketing, business reputation, legal compliance and quality assurance and in this case IT resiliency. Where possible, impact is expressed monetarily for purposes of comparison. For example, UCSF may spend three times as much on recruiting potential students, faculty and staff in the wake of a disaster to rebuild customer confidence. The BIA should assess a disaster's impact over time and help to establish recovery strategies, priorities, and requirements for resources and time.

## **BIA versus Risk Assessment**

Business impact analysis and risk assessment are two important steps in a business continuity plan. A BIA often takes place prior to a risk assessment. In particular UC San Francisco's IT Business Continuity Team will focus its BIA efforts on the effects or consequences of the interruption to critical IT business functions and attempts to quantify the financial and non-financial costs associated with a disaster. The business impact assessment looks at the parts of the organization that are most crucial. A BIA can serve as a starting point for a disaster recovery strategy and examine recovery time objectives (RTOs) and recovery point objectives (RPOs), and resources and materials needed for business continuance.

A risk assessment identifies potential hazards such as a hurricane, earthquake, fire, supplier failure, utility outage, IT or network availability or cyber-attack and evaluates areas of vulnerability should the hazard occurs. Assets put at risk include people, property, supply chain, information technology, business reputation and contract obligations. Points of weakness that make an asset more prone to harm are reviewed. A mitigation strategy may be developed to reduce the probability that a hazard will have a significant impact.

During the risk assessment phase, the BIA findings may be examined against various hazard scenarios, and potential disruptions may be prioritized based on the hazard's probability and the likelihood of adverse impact to business operations. A BIA may be used to justify investments in prevention and mitigation, as well as disaster recovery strategies.

UCSF has a department that manages continuity for the campus (Office of Emergency Management – OEM) who are conducting separate BIAs and risk assessments for the business side of our campus. You may be in contact with OEM regarding the UCReady project or wish to contact OEM for more information. The IT Business Continuity Team specializes in IT resiliency and thus a BIA conducted by IT Business Continuity will focus on IT assets owned or managed by the interviewee.

A disaster recovery plan (DRP), disaster recovery implementation plan, or IT disaster recovery plan is a recorded policy and/or process that is designed to assist an organization in executing recovery processes in response to a disaster to protect business IT infrastructure and more generally promote recovery.

The purpose of a disaster recovery plan is to comprehensively explain the consistent actions that must be taken before, during, and after a natural or man-made disaster so that the entire team can take those actions. A disaster recovery plan should address both man-made disasters that are intentional, such as fallout from terrorism or hacking, or accidental, such as an equipment failure.

Organizations of all sizes generate and manage massive amounts of data, much of it mission critical. The impact of corruption or data loss from human error, hardware failure, malware, or hacking can be substantial. Therefore, it is essential to create a disaster recovery plan for the restoration of business data from a data backup image.

It is most effective to develop an information technology (IT) disaster recovery plan in conjunction with the business continuity plan (BCP). A business continuity plan is a complete organizational plan that consists of five components:

1. Business resumption plan
2. Occupant emergency plan
3. Continuity of operations plan

#### 4. Incident management plan (IMP)

#### 5. Disaster recovery plan

Generally, components one through three do not touch upon IT infrastructure at all. The incident management plan typically establishes procedures and a structure to address cyber attacks against IT systems during normal times, so it does not deal with the IT infrastructure during disaster recovery. For this reason, the disaster recovery plan is the only component of the BCP of interest to IT.

Among the first steps in developing such a strategy is business impact analysis, during which the team should develop IT priorities and recovery time objectives. The team should time technology recovery strategies for restoring applications, hardware, and data to meet business recovery needs.

Every situation is unique and there is no single correct way to develop a disaster recovery plan. However, there are three principal goals of disaster recovery that form the core of most DRPs:

prevention, including proper backups, generators, and surge protectors

detection of new potential threats, a natural byproduct of routine inspections

correction, which might include holding a “lessons learned” brainstorming session and securing proper insurance policies

What should a disaster recovery plan include?

Although specific disaster recovery plan formats may vary, the structure of a disaster recovery plan should include several features:

#### **Goals**

A statement of goals will outline what the organization wants to achieve during or after a disaster, including the recovery time objective (RTO) and the recovery point objective (RPO). The recovery point objective refers to how much data (in terms of the most recent changes) the company is willing to lose after a disaster occurs. For example, an RPO might be to lose no more than one hour of data, which means data backups must occur at least every hour to meet this objective.

Recovery time objective or RTO refers to the acceptable downtime after an outage before business processes and systems must be restored to operation. For example, the business must be able to return to operations within 4 hours in order to avoid unacceptable impacts to business continuity.

#### **Personnel**

Every disaster recovery plan must detail the personnel who are responsible for the execution of the DR plan, and make provisions for individual people becoming unavailable.

#### **IT inventory**

An updated IT inventory must list the details about all hardware and software assets, as well as any cloud services necessary for the company’s operation, including whether or not they are business critical, and whether they are owned, leased, or used as a service.

#### **Backup procedures**

The DRP must set forth how each data resource is backed up – exactly where, on which devices and in which folders, and how the team should recover each resource from backup.

## **Disaster recovery procedures**

These specific procedures, distinct from backup procedures, should detail all emergency responses, including last-minute backups, mitigation procedures, limitation of damages, and eradication of cybersecurity threats.

## **Disaster recovery sites**

Any robust disaster recovery plan should designate a hot disaster recovery site. Located remotely, all data can be frequently backed up to or replicated at a hot disaster recovery site — an alternative data center holding all critical systems. This way, when disaster strikes, operations can be instantly switched over to the hot site.

## **Restoration procedures**

Finally, follow best practices to ensure a disaster recovery plan includes detailed restoration procedures for recovering from a loss of full systems operations. In other words, every detail to get each aspect of the business back online should be in the plan, even if you start with a disaster recovery plan template. Here are some procedures to consider at each step.

Include not just objectives such as the results of risk analysis and RPOs, RTOs, and SLAs, but also a structured approach for meeting these goals. The DRP must address each type of downtime and disaster with a step-by-step plan, including data loss, flooding, natural disasters, power outages, ransomware, server failure, site-wide outages, and other issues. Be sure to enrich any IT disaster recovery plan template with these critical details.

Create a list of IT staff including contact information, roles, and responsibilities. Ensure each team member is familiar with the company disaster recovery plan before it is needed so that individual team members have the necessary access levels and passwords to meet their responsibilities. Always designate alternates for any emergency, even if you think your team can't be affected.

Address business continuity planning and disaster recovery by providing details about mission-critical applications in your DRP. Include accountable parties for both troubleshooting any issues and ensuring operations are running smoothly. If your organization will use cloud backup services or disaster recovery services, vendor name and contact information, and a list of authorized employees who can request support during a disaster should be in the plan; ideally the vendor and organizational contacts should know of each other.

Media communication best practices are also part of a robust disaster recovery and business continuity plan. A designated public relations contact and media plan are particularly useful to high profile organizations, enterprises, and users who need 24/7 availability, such as government agencies or healthcare providers. Look for disaster recovery plan examples in your industry or vertical for specific best practices and language.

Beyond the clear benefit of improved business continuity under any circumstances, having a company disaster recovery plan can help an organization in several other important ways.

## **Cost-efficiency**

Disaster recovery plans include various components that improve cost-efficiency. The most important elements include prevention, detection, and correction, as discussed above. Preventative measures reduce the risks from man-made disasters. Detection measures are designed to quickly identify problems when they do happen, and corrective measures restore lost data and enable a rapid resumption of operations.

Achieving cost-efficiency goals demands regular maintenance of IT systems in their optimal condition, high-level analysis of potential threats, and implementation of innovative cybersecurity solutions. Keeping software updated and systems optimally maintained saves time and is more cost-effective. Adopting cloud-based data management as a part of disaster recovery planning can further reduce the costs of backups and maintenance.

### **Increased productivity**

Designating specific roles and responsibilities along with accountability as a disaster recovery plan demands increases effectiveness and productivity in your team. It also ensures redundancies in personnel for key tasks, improving sick day productivity, and reducing the costs of turnover.

### **Improved customer retention**

Customers do not easily forgive failures or downtime, especially if they result in loss of sensitive data. Disaster recovery planning helps organizations meet and maintain a higher quality of service in every situation. Reducing the risks your customers face from data loss and downtime ensures they receive better service from you during and after a disaster, shoring up their loyalty.

### **Compliance**

Enterprise business users, financial markets, healthcare patients, and government entities, all rely on availability, uptime, and the disaster recovery plans of important organizations. These organizations in turn rely on their DRPs to stay compliant with industry regulations such as HIPAA and FINRA.

### **Scalability**

Planning disaster recovery allows businesses to identify innovative solutions to reduce the costs of archive maintenance, backups, and recovery. Cloud-based data storage and related technologies enhance and simplify the process and add flexibility and scalability.

The disaster recovery planning process can reduce the risk of human error, eliminate superfluous hardware, and streamline the entire IT process. In this way, the planning process itself becomes one of the advantages of disaster recovery planning, streamlining the business, and rendering it more profitable and resilient before anything ever goes wrong.

There are several steps in the development of a disaster recovery plan. Although these may vary somewhat based on the organization, here are the basic disaster recovery plan steps:

#### **Risk assessment**

First, perform a risk assessment and business impact analysis (BIA) that addresses many potential disasters. Analyze each functional area of the organization to determine possible consequences from middle of the road scenarios to “worst-case” situations, such as total loss of the main building. Robust disaster recovery plans set goals by evaluating risks up front, as part of the larger business continuity plan, to allow critical business operations to continue for customers and users as IT addresses the event and its fallout.

Consider infrastructure and geographical risk factors in your risk analysis. For example, the ability of employees to access the data center in case of a natural disaster, whether or not you use cloud backup, and whether you have a single site or multiple sites are all relevant here. Be sure to include this information, even if you’re working from a sample disaster recovery plan.

#### **Evaluate critical needs**

Next, establish priorities for operations and processing by evaluating the critical needs of each department. Prepare written agreements for selected alternatives, and include details specifying all special security procedures, availability, cost, duration, guarantee of compatibility, hours of operation, what constitutes an emergency, non-mainframe resource requirements, system testing, termination conditions, a procedure notifying users of system changes, personnel requirements, specs on required processing hardware and other equipment, a service extension negotiation process, and other contractual issues.

Set disaster recovery plan objectives

Create a list of mission-critical operations to plan for business continuity, and then determine which data, applications, equipment, or user accesses are necessary to support those functions. Based on the cost of downtime, determine each function's recovery time objective (RTO). This is the target amount of time in hours, minutes, or seconds an operation or application can be offline without an unacceptable business impact.

Determine the recovery point objective (RPO), or the point in time back to which you must recover the application. This is essentially the amount of data the organization can afford to lose.

Assess any service level agreements (SLAs) that your organization has promised to users, executives, or other stakeholders.

Collect data and create the written document

Collect data for your plan using pre-formatted forms as needed. Data to collect in this stage may include:

- lists (critical contact information list, backup employee position listing, master vendor list, master call list, notification checklist)
- inventories (communications equipment, data center computer hardware, documentation, forms, insurance policies, microcomputer hardware and software, office equipment, off-site storage location equipment, workgroup hardware, etc.)
- schedules for software and data files backup/retention
- procedures for system restore/recovery
- temporary disaster recovery locations
- other documentation, inventories, lists, and materials

Organize and use the collected data in your written, documented plan.

### **Test and revise**

Next, develop criteria and procedures for testing the plan. This is essential to ensure the organization has adopted compatible, feasible backup procedures and facilities, and to identify areas that should be modified. It also allows the team to be trained, and proves the value of the DRP and ability of the organization to withstand disasters.

Finally, test the plan based on the criteria and procedures. Conduct an initial dry run or structured walk-through test and correct any problems, ideally outside normal operational hours. Types of business disaster recovery plan tests include: disaster recovery plan checklist tests, full interruption tests, parallel tests, and simulation tests.

### **The right strategies and tools help implement a disaster recovery plan.**

Traditional on-premises recovery strategies



The IT team should develop disaster recovery strategies for IT applications, systems, and data. This includes desktops, data, networks, connectivity, servers, wireless devices, and laptops. Identify IT resources that support time-sensitive business processes and functions so their recovery times match.

Information technology systems require connectivity, data, hardware, and software. The entire system may fail due to a single component, so recovery strategies should anticipate the loss of one or more of these system components:

- Secure, climate-controlled computer room environment with backup power supply
- Connectivity to a service provider
- Hardware such as desktop and laptop computers, networks, wireless devices and peripherals, and servers
- Software applications such as electronic mail, electronic data interchange, enterprise resource management, and office productivity

### **Data and restoration**

For business applications that cannot tolerate downtime, actual parallel computing, data mirroring, or multiple data center synchronization is possible yet costly. Other solutions for mission critical business applications and sensitive data include cloud backup and cloud-native disaster recovery, which reduce the need for expensive hardware and IT infrastructure.

### **Internal recovery strategies**

Some enterprises store data at multiple facilities and configure hardware to run similar applications from data center to data center when needed. Assuming off-site data backup or data mirroring are taking place, processing can continue and data can be restored at an alternate site under these circumstances. However, this is a costly solution, and one that demands an internal solution that is itself infallible.

### **Cloud-based disaster recovery strategies**

Cloud-based vendors offer Disaster recovery as a service (DRaaS), which are essentially “hot sites” for IT disaster recovery hosted in the cloud. DRaaS leverages the cloud to provide fully configured recovery sites that mirror the applications in the local data center. This allows users a more immediate response, allowing them the ability to recover critical applications in the cloud, keeping them ready for use at the time of a disaster.

Vendors can host and manage applications, data security services, and data streams, enabling access to information via web browser at the primary business site or other sites. These vendors can typically enhance cybersecurity because their ongoing monitoring for outages offers data filtering and detection of malware threats. If the vendor detects an outage at the client site, they hold all client data automatically until the system is restored. In this sense, the cloud is essential to security planning and disaster recovery.



## Self-check quiz 2.4

Check your understanding by answering the following questions:

Write the appropriate/correct answer of the following:

1. What is Business Continuity Plan?

Answer

2. Write down the process of Business Continuity Plan.

Answer

3. Which things we need to consider during Business Continuity Risk Assessment?

Answer:

4. Which items we need to include During Business Continuity Plan?

Answer:

5. What are the components of business continuity plan?

Answer:



## Learning outcome 2.5 – Implement backup and recovery management



Contents:

- Backup and Storage management
- Data retention.
- Backup management tools.
- Restore and recovery management.
- Data destruction.



Assessment criteria:

1. Backup and Storage management is interpreted.
2. Data retention is interpreted.
3. Backup management tools are described.
4. Backup is performed as per standard procedure.
5. Restore and recovery are performed.
6. Data destruction is interpreted.



Resources required:

- Students/trainees must be provided with the following resources:
- Workplace (actual or simulated), class room, trainee handbook and Data center



### LEARNING ACTIVITY 2.5

Learning Activity	Resources/Special Instructions/References
Implement backup and recovery management	<ul style="list-style-type: none"> <li>▪ Information Sheets: 2.5</li> <li>▪ Self-Check: 2.5</li> <li>▪ Answer Key: 2.5</li> </ul>



## Information sheet 2.5

Learning Objective: to implement backup and recovery management

A backup is a copy of production data, created and retained for the sole purpose of recovering deleted or corrupted data. With growing business and regulatory demands for data storage, retention, and availability, organizations are faced with the task of backing up an ever-increasing amount of data. This task becomes more challenging as demand for consistent backup and quick restore of data increases throughout the enterprise — which may be spread over multiple sites. Moreover, organizations need to accomplish backup at a lower cost with minimum resources.

Organizations must ensure that the right data is in the right place at the right time. Evaluating backup technologies, recovery, and retention requirements for data and applications is an essential step to ensure successful implementation of the backup and recovery solution. The solution must facilitate easy recovery and retrieval from backups and archives as required by the business.

Typically backup data means all necessary data for the workloads your server is running. This can include documents, media files, configuration files, machine images, operating systems, and registry files. Essentially, any data that you want to preserve can be stored as backup data.

### **Data backup includes several important concepts:**

- Backup solutions and tools—while it is possible to back up data manually, to ensure systems are backed up regularly and consistently, most organizations use a technology solution to back up their data.
- Backup administrator—every organization should designate an employee responsible for backups. That employee should ensure backup systems are set up correctly, test them periodically and ensure that critical data is actually backed up.
- Backup scope and schedule—an organization must decide on a backup policy, specifying which files and systems are important enough to be backed up, and how frequently data should be backed up.
- Recovery Point Objective (RPO)—RPO is the amount of data an organization is willing to lose if a disaster occurs, and is determined by the frequency of backup. If systems are backed up once per day, the RPO is 24 hours. The lower the RPO, the more data storage, compute and network resources are required to achieve frequent backups.
- Recovery Time Objective (RTO)—RTO is the time it takes for an organization to restore data or systems from backup and resume normal operations. For large data volumes and/or backups stored off-premises, copying data and restoring systems can take time, and robust technical solutions are needed to ensure a low RTO.

### **The Importance of a Disaster Recovery Plan: Alarming Statistics**

To understand the potential impact of disasters on businesses, and the importance of having a data backup strategy as part of a complete disaster recovery plan, consider the following statistics:

- Cost of downtime—according to Gartner, the average cost of downtime to a business is \$5,600 per minute.

- Survival rate—another Gartner study found only 6% of companies affected by a disaster that did not have disaster recovery in place survived and continued to operate more than two years after the disaster.
- Causes of data loss—the most common causes of data loss are hardware/system failure (31%), human error (29%) and viruses, and malware of ransomware (29%).

## **Data Backup Options**

There are many ways to backup your file. Choosing the right option can help ensure that you are creating the best data backup plan for your needs. Below are six of the most common techniques or technologies:

1. Removable media
2. Redundancy
3. External hard drive
4. Hardware appliances
5. Backup software
6. Cloud backup services

### **Removable Media**

A simple option is to backup files on removable media such as CDs, DVDs, newer Blu-Ray disks, or USB flash drives. This can be practical for smaller environments, but for larger data volumes, you'll need to back up to multiple disks, which can complicate recovery. Also, you need to make sure you store your backups in a separate location, otherwise they may also be lost in a disaster. Tape backups also fall into this category.

### **Redundancy**

You can set up an additional hard drive that is a replica of a sensitive system's drive at a specific point in time, or an entire redundant system. For example, another email server that is on standby, backing up your main email server. Redundancy is a powerful technique but is complex to manage. It requires frequent replication between cloned systems, and it's only useful against the failure of a specific system unless the redundant systems are in a remote site.

### **External Hard Drive**

You can deploy a high-volume external hard drive in your network, and use archive software to save changes to local files to that hard drive. Archive software allows you to restore files from the external hardware with an RPO of only a few minutes. However, as your data volumes grow, one external drive will not be enough, or the RPO will substantially grow. Using an external drive necessitates having it deployed on the local network, which is risky.

### **Hardware Appliances**

Many vendors provide complete backup appliances, typically deployed as a 19" rack-mounted device. Backup appliances come with large storage capacity and pre-integrated backup software. You install backup agents on the systems you need to back up, define your backup schedule and policy, and the data starts streaming to the backup device. As with other options, try to place the backup device isolated from the local network and if possible, in a remote site.

### **Backup Software**

Software-based backup solutions are more complex to deploy and configure than hardware appliances, but offer greater flexibility. They allow you to define which systems and data you'd like to back up, allocate backups to the storage device of your choice, and automatically manage the backup process.

### **Cloud Backup Services**

Many vendors and cloud providers offer Backup as a Service (BaaS) solutions, where you can push local data to a public or private cloud and in case of disaster, recover data back from the cloud. BaaS solutions are easy to use and have the strong advantage that data is saved in a remote location. However, if using a public cloud, you need to ensure compliance with relevant regulations and standards, and consider that over time, data storage costs in the cloud will be much higher than the cost of deploying similar storage on-premises.

### **What Is a 3-2-1 Backup Strategy?**

A 3-2-1 backup strategy is a method for ensuring that your data is adequately duplicated and reliably recoverable. In this strategy, three copies of your data are created on at least two different storage media and at least one copy is stored remotely:

- Three copies of data—your three copies include your original data and two duplicates. This ensures that a lost backup or corrupted media do not affect recoverability.
- Two different storage types—reduces the risk of failures related to a specific medium by using two different technologies. Common choices include internal and external hard drives, removable media, or cloud storage.
- One copy off-site—eliminates the risk associated with a single point of failure. Offsite duplicates are needed for robust disaster and data backup recovery strategies and can allow for failover during local outages.

This strategy is considered a best practice by most information security experts and government authorities. It protects against both accidents and malicious threats, such as ransomware, and ensures reliable data backup and restoration.

### **Server Backup: Backing Up Critical Business Systems**

The easiest way to backup a server is with a server backup solution. These solutions can come in the form of software or appliances.

Server backup solutions are typically designed to help you backup server data to another local server, a cloud server, or a hybrid system. In particular, backup to hybrid systems is becoming more popular. This is because hybrid systems enable you to optimize resources, support easy multi-region duplication, and can enable faster recovery and failover.

In general, server backup solutions should include the following features:

- Support for diverse file types—should not include any file types. In particular, solutions should support documents, spreadsheets, media, and configuration files.
- Backup location—you should be able to specify backup locations. The solution should support backup to a variety of locations and media, including on and off-site resources.
- Scheduling and automation—in addition to enabling manual backups, solutions should support backup automation through scheduling. This helps ensure that you always have a recent backup and that backups are created in a consistent manner.

- Backup management—you should be able to manage the lifecycle of backups, including number stored and length of time kept. Ideally, solutions also enable easy export of backups for transfer to external resources or for use in migration.
- Partition selection—partitions are isolated segments of a storage resource and are often used to separate data within a system. Solutions should enable you to independently backup data and restore partitions.
- Data compression—to minimize the storage needed for numerous backups, solutions should compress backup data. This compression needs to be lossless and maintain the integrity of all data.
- Backup type selection—you should be able to create a variety of backup types, including full, differential, and incremental backups. Differential backups create a backup of changes since the last full backup while incremental records the changes since the last incremental backup. These types can help you reduce the size of your backups and speed backup time.
- Scaling—backup abilities should not be limited by the volume of data on your servers. Solutions should scale as your data does and support backups of any size.

### **Backup Storage Technology**

Whichever technique you use to backup, at the end of the day, data must be stored somewhere. The storage technology used to hold your backup data is very significant:

The more cost-effective it is, the more data it is able to store, and the faster the storage and retrieval over a network, the lower your RPO and RTO will be.

The more reliable the storage technology, the safer your backups will be.

Below, you'll find a review of backup storage technologies and their unique advantages.

### **Network Shares and NAS**

You can set up centralized storage such as Network Attached Storage (NAS ), Storage Area Network (SAN), or regular hard disks mounted as a network share using Network File System (NFS) protocol. This is a convenient option for making large storage available to local devices for backup. However, it is susceptible to disasters affecting your entire data center, such as natural disasters or cyberattacks.

### **Tape Backup**

Modern tape technology such as Linear Tape-Open 8 (LTO-8) can store up to 9 TB of data on a single tape. You can then ship the tape to a distant location, preferably at least 100 miles away from your primary location. Tape backups have been used for decades, but their obvious downside is the extremely high RTO and RPO due to the need to physically ship the tapes to and from a backup location. They also require a tape drive and an autoloader to perform backup and recovery, and this equipment is expensive.

### **Cloud-Based Object Storage**

When using cloud providers, you have access to a variety of storage services. Cloud providers charge a flat price per Gigabyte, but costs can start to add up for frequent access. There are multiple tools that let you backup data to S3 automatically, both from within the cloud and from on-premise machines.

### **Data retention**

Data retention, also called records retention, is the continued storage of an organisation's data for compliance or business reasons. The General Data Protection Regulation (GDPR) does not specify time limits for retention. However, the general principle is that data should only be kept for as long as it is needed. This is reflected in Article 5(1)(e) GDPR, also known as the storage limitation principle. This principle provides that even if personal data is collected fairly and lawfully, it cannot be kept longer than required to fulfil the purposes for which it was collected. Personal data may be kept for longer periods where it is archived in the public interest or for scientific or historical research, provided the data is appropriately anonymised or encrypted. Therefore, the onus is on the organisation to understand what data it holds, why it holds it, and where it no longer has an appropriate use for the data, whether it should be erased or anonymised.

### **Data Retention Policies and Procedures**

Putting in place retention policies and procedures can enable organisations to only retain data necessary for the purposes for which it is collected. Retention policies state what type of information is held by the organisation, what it is used for, and how long it should be retained. These policies establish standard retention periods for different categories of data the organisation holds and is extremely beneficial in maintaining GDPR compliance. In deciding on retention periods, organisations should consider any legal obligations imposed on them for retention, limitation periods for claims, organisational needs, and the quality of the data held. Any decision on retention periods should be proportionate. This means retention periods should appropriately balance the organisation's needs against the impact of retention on individuals concerned.

Retention procedures ensure that data is destroyed appropriately and securely per the retention policies. This could be done in different ways depending on the organisation. A good example would be introducing an automated system which flags records for review or deletion after a set time limit. Retention policies could also include procedures for data sharing between two organisations including what happens when the data is no longer needed. This could contain procedures for the recipient returning all shared data to the supplier without keeping any copies. It could also include all organisations involved deleting any copies of any data shared between them where it is no longer needed.

### **Data retention in AWS**

There are four main practical considerations when designing data retention flows in AWS:

Moving or expiring data. How can data be moved to cheaper storage tiers, and how can it be deleted? This addresses cost concerns and, sometimes, regulatory requirements.

Encryption and access. How is data encrypted, and how is access controlled? Beyond security best practices, some regulatory frameworks prescribe specific encryption and access controls.

Querying and modification. How can you find and modify individual records if required? This addresses business needs, and privacy regulation requirements.

Backups and redundancy. How much data needs to be backed up, how durable do backups need to be, and how can backups be automated? This is sometimes a regulatory consideration, but most often, it will be about business continuity, disaster recovery, and auditing.

Typically, you restore and recover a database or subset of a database in the following cases:



A media failure has damaged some or all control files or datafiles.

You want to recover the database to a point before a user error, such as a dropped table, occurred.

If you want to restore a version of the database for testing purposes, then run the DUPLICATE rather than the RESTORE command.

#### Generic Procedure for Media Recovery

The basic procedure for performing restore and recovery with RMAN is as follows:

- Determine which database files require recovery.
- Place the database in the state appropriate for the type of recovery that you are performing. For example, if you are recovering all data files, then mount the database. If you are recovering a single table space or data file, then you can keep the database open and take the table space or data file offline.
- Restore the necessary files using the RESTORE command.
- Recover the restored files using the RECOVER command.

Place the database in its normal state. For example, open the database if it is closed, or bring all recovered files online if they are offline.

Because so many possible restore and recover scenarios exist, the actual recovery procedure that you should follow differs from case to case.

Note that if you use Oracle Enterprise Manager, then you can use the Recovery wizard instead of running the RESTORE and RECOVER commands through the RMAN command-line interface. You can perform the following RMAN restore and recovery tasks through the Recovery wizard:

- restore and recover the entire database to the current or a noncurrent time
- restore and recover tablespaces or datafiles to the latest time or from the latest backup or an older backup
- restore the control file from a controlfile autobackup when the database is in the NOMOUNT state and there are no backup configurations which use a recovery catalog
- restore archived logs by time, by SCN, or by log sequence.
- recover datablocks by using a corruption list, datafiles, or tablespace

## Differences Among Restore and Recovery Scenarios

Before performing recovery, identify the conditions under which you will perform the recovery. The recovery procedure differs depending on whether:

- The current control file is available
- You are using a recovery catalog
- The restore host is the same as the original target host
- The restored database files are named the same as the target database files
- The target database runs in an Oracle Real Application Clusters configuration
- You want to recover to the current time or to a noncurrent time
- You are recovering the whole database
- You have a backup made after the most recent RESETLOGS
- You are recovering whole datafiles rather than a limited number of corrupt data blocks



## Self-check quiz 2.5

Check your understanding by answering the following questions:

Write the appropriate/correct answer of the following:

1. Write some way by which you back your data.

Answer:

2. What is Data Retention?

Answer:

3. What are the differences among Restore and Recovery Scenarios?

Answer:

<b>LEARNER JOB SHEET 1</b>			
<b>Qualification:</b>	Information System Security Management		
<b>Learning unit:</b>	Perform data backup and recovery		
<b>Learner name:</b>			
<b>Personal protective equipment (PPE):</b>			
<b>Materials:</b>			
<b>Tools and equipment:</b>			
<b>Performance criteria:</b>	<ol style="list-style-type: none"> <li>1. Backup and Storage management is interpreted.</li> <li>2. Data retention is interpreted.</li> <li>3. Backup management tools are described.</li> <li>4. Backup is performed as per standard procedure.</li> <li>5. Restore and recovery are performed.</li> <li>6. Data destruction is interpreted.</li> </ol>		
<b>Measurement:</b>			
<b>Notes:</b>			
<b>Procedure:</b>	<ol style="list-style-type: none"> <li>1. Collect PPE, tools, equipment and materials</li> <li>2. Check the usability of PPE, tools, equipment and materials.</li> <li>3. Identify what to back up</li> <li>4. Select backup media</li> <li>5. Back up your data</li> <li>6. Store it safely</li> <li>7. Check that it works</li> <li>8. Report to the authority</li> </ol>		
<b>Learner signature:</b>		<b>Date:</b>	
<b>Assessor signature:</b>		<b>Date:</b>	
<b>Quality Assurer signature:</b>		<b>Date:</b>	
<b>Assessor remarks:</b>			
<b>Feedback:</b>			



## Answer keys

### Answer key 2.1

1. Answer:

IT risk assessment is a process of analysing potential threats and vulnerabilities to your IT systems to establish what loss you might expect to incur if certain events happen. Its objective is to help you achieve optimal security at a reasonable cost.

2. Answer:

Quantitative assessment measures risk using monetary amounts. It uses mathematical formulas to give you the value of expected losses associated with a particular risk, based on:

- the asset values
- the frequency of risk occurrence
- the probability of associated loss

3. Answer:

Virus – They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

4. Answer:

Bots can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet

5. Answer:

Ransomware It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange

### Answer key 2.2

1. Answer:

1. Low Risk
2. Moderate Risk
3. High Risk

2. Answer:

Risk levels are calculated as the product of the LIKELIHOOD and IMPACT (to the University) of a potential threat event / threat event category:

		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood ↑	Very Likely	Low	Moderate	High	High	High
	Likely	Low	Moderate	Moderate	High	High
	Possible	Low	Low	Moderate	Moderate	High
	Unlikely	Low	Low	Moderate	Moderate	Moderate
	Very Unlikely	Low	Low	Low	Moderate	Moderate

3. Answer:

Residual risk is the risk that remains after your organization has implemented all the security controls, policies, and procedures you believe are appropriate to take. Put another way, residual risk can affect your business even after taking all the security measures.

Answer key 2.3

1. Answer:

Risk mitigation is a strategy to prepare for and lessen the effects of threats faced by a business. Comparable to risk reduction, risk mitigation takes steps to reduce the negative effects of threats and disasters on business continuity (BC). Threats that might put a business at risk include cyberattacks, weather events and other causes of physical or virtual damage

2. Answer:

Some strategies for mitigating cybersecurity incidents across your IT ecosystem:

1. Conduct a risk assessment to determine vulnerabilities
2. Establish network access controls
3. Implement firewalls and antivirus software
4. Create a patch management schedule
5. Continuously monitor network traffic
6. Build an incident response plan

3. Answer

1. Tanium Reveal
2. TeamSuccess
3. TrustMAPP

## Answer key 2.4

### 1. Answer:

This involves the development of a Business Continuity Plan (BCP) designed to ensure the recovery of critical business activities from natural or man-made failures or disasters to an acceptable level within a predefined time frame, thereby minimising the impact of losses to the organisation. Implementing a BCP is essential for every business

### 2. Answer:

Business continuity planning involves the following five major processes:



### 3. Answer:

During Business Continuity Risk Assessment Different disaster scenarios should be considered, some common threats include:

- Natural disaster, such as earthquake, fire, typhoon, flood;
- Loss of key equipment / information system / facility;
- Disruption of external telecommunications services;
- Utility outage, such as failure of power supply;
- Loss of life, disease, health & safety issues; and
- Terrorism & cyber attack.

4. Answer:

During Business Continuity Plan below are the typical items included in a BCP:

- Individual roles and responsibilities;
- Conditions for its activation;
- Processes to be followed;
- Escalation plan;
- Emergency procedure to handle incident;

5. Answer:

Components of business continuity plan:

1. Business resumption plan
2. Occupant emergency plan
3. Continuity of operations plan
4. Incident management plan (IMP)
5. Disaster recovery plan

Answer key 2.5

1. Answer:

- Answer: Removable media
- Redundancy
- External hard drive
- Hardware appliances

2. Answer:

Answer: Data retention, also called records retention, is the continued storage of an organisation's data for compliance or business reasons. Retention procedures ensure that data is destroyed appropriately and securely per the retention policies. This could be done in different ways depending on the organisation

3. Answer:

Before performing recovery, identify the conditions under which you will perform the recovery. The recovery procedure differs depending on whether:

- The current control file is available
- You are using a recovery catalog
- The restore host is the same as the original target host
- The restored database files are named the same as the target database files
- The target database runs in an Oracle Real Application Clusters configuration



## Module 3: Perform infrastructure security

---



### MODULE CONTENT

**Module Descriptor:** This module covers the knowledge, skills, and attitudes required to executing Network security, carrying out Server and device security control, ensuring system (OS) security and interpreting data center security and operations. It specifically includes information sheets, job sheets, self-checking, answer keys and assessment plan

**Nominal Duration: 50 hours**



### LEARNING OUTCOMES:

Upon completion of the module, the trainee should be able to:

- 3.1 Execute Network security
- 3.2 Carry out Server and device security control
- 3.3 Ensure system (OS) security
- 3.4 Interpret data center security and operations



### PERFORMANCE CRITERIA:

1. Network audit is performed.
2. Firewall is configured following standard procedure.
3. Router is configured as per standard procedure.
4. Switch is configured as per standard procedure.
5. Network load balancing is performed.
6. IP addresses are configured according to workplace requirement.
7. Network devices are hardened following standard procedure.
8. Network based intruders are detected and prevented following standard procedure.
9. Cryptography is applied as per standard procedure.
10. Device hardening is performed for server.
11. Logs are analyzed as per standard procedure.
12. Identity and access management configurations are audited following standard procedure.
13. Password management is checked and performed following client's requirements.
14. Host and network based intruders are detected and prevented following standard procedure.

15. File and service auditing are performed following standard procedure.
16. Hardening of operating system is performed.
17. System security is audited.
18. Identity is set and access management is performed as per standard procedure.
19. OS Configuration management is performed as per client's requirement.
20. OS default Firewall/ Intrusion detection and prevention system are configured by following standard.
21. Web services and browsing security is configured as per standard procedure.
22. Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) are described.
23. Data Leak/Loss Prevention (DLP) is interpreted.
24. Data center architecture is explained.
25. Data center components are described.
26. Data center network security is interpreted.
27. Environmental security is interpreted.



### **Learning Outcome 3.1 Execute Network security**



Contents:

- Network audit
- Firewall configuration.
- Router configuration.
- Switch configuration.
- Network load balancing.
- IP addresses configuration.
- Network devices.
- Network based intruders.
- Cryptography



Assessment criteria:

1. Network audit is performed.
2. Firewall is configured following standard procedure.
3. Router is configured as per standard procedure.
4. Switch is configured as per standard procedure.
5. Network load balancing is performed.
6. IP addresses are configured according to workplace requirement.
7. Network devices are hardened following standard procedure.
8. Network based intruders are detected and prevented following standard procedure.
9. Cryptography is applied as per standard procedure.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (actual or simulated)
- Network devices, required tools, equipments and materials.



### LEARNING ACTIVITY 3.1

Learning Activity	Resources/Special Instructions/References
Execute Network security	<ul style="list-style-type: none"> <li>▪ Information Sheet: 3.1</li> <li>▪ Self-Check: 3.1</li> <li>▪ Answer Key: 3.1</li> </ul>



### Information sheet 3.1

Learning Objective: to execute network security.

#### The security of network infrastructure devices

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and network administrators to implement the following recommendations to better secure their network infrastructure:

- Segment and segregate networks and functions.
- Limit unnecessary lateral communications.
- Harden network devices.
- Secure access to infrastructure devices.
- Perform out-of-band (OoB) network management.
- Validate integrity of hardware and software.

#### Network Audit

Network auditing is the process of mapping and inventorying your network in terms of hardware and software. It's a fairly complex task that involves manually identifying network elements. In some cases, network auditing tools can provide automation support to identify the devices and services connected to the network. In addition to hardware and software, auditing should include security documentation such as user accounts and groups as well as permissions.

#### Network Audit vs Network Assessment

What's the difference between a network audit and assessment? While network audits inventory hardware devices, software, and services at each location, network assessments serve a completely different purpose.

Network assessments are used to examine your IT infrastructure and identify any potential areas for improvement or concern. They touch on topics such as bandwidth bottlenecks, network security flaws, and under and over-utilized resources.

Especially, network assessment can help organizations remedy networking issues that have been plaguing their networks, applications, dampening performance, or causing additional risks and security concerns. Assessment reports are used for specific recommendations on how to improve network performance, increase network security, and reduce costs – all with the goal of maximizing the IT infrastructure and underlying network.

I will do a deep dive into network assessments and best practices in a follow-up blog article soon. Make sure to sign-up for our newsletter and follow us on LinkedIn for the latest articles.

### **When Do You Need a Network Audit?**

There are many reasons why you should consider an audit. Typically, it's timed around important technology decisions or business requirements. Here's just a few potential reasons why your business might consider a network audit.

#### **1) Outdated & Incomplete Inventories**

When was the last time that you and your team performed an audit? A lot can change overtime – mergers and acquisitions, new and existing application demands on the network, budget forecasting and capital expenses, and turnover within IT and especially network infrastructure.

#### **2) Upgrades & Refreshes**

There's a tendency for network admins to fall into an operational state where their main priority is the day-to-day operations. I like to call keeping the lights on. However, networks need to be upgraded and refreshed from time-to-time. This is especially true when upgrading your networking technology. This includes performing an audit to identify which hardware and software need to be replaced or upgraded.

#### **3) Troubleshooting & Resolution**

It's probably the last thing that IT or a Network Administrator wants to hear is – we're experiencing a major network outage, we can't connect to the internet, or latency issues are having an impact on applications, clients, users, and partners. In this scenario, it's needed on an emergency basis as a way of troubleshooting the network.

#### **4) Regulatory & Compliance Standards**

For many industries including financial and healthcare, regulatory and compliance standards are an important reason to initiate a network audit. This includes adhering to HIPAA, SOC1, SOC2, FedRAMP, PCI, FISMA, NIST, and other critical standards for compliance. It may be used by internal or external auditors to assess the compliance of the organization as a whole.

### **What's Included in a Network Audit?**

Here are several key focus areas that should be included within your network auditing process. Unfortunately, some of the tasks will require manual resources to complete. Yet, others can be accomplished with the use of today's advanced network auditing and analysis tools.

#### **Inventory Creation**

The best place to start your network audit is in building an inventory of your existing network. This includes detailing the devices that are running on your network at each location. It's important to include both physical and virtual network infrastructure associated with each location.

Another important part of the process is to identify the services and service providers at each location. This includes taking note of the telecom carriers, ISPs, and network providers you are using at each location along with contract expiration and pricing or rates.

### **Identifying Obsolescence**

You've created a comprehensive inventory of your devices and services at each location, the next step is to determine if any devices are obsolete, outdated, or nearing end-of-life. This includes hardware such as routers, switches, and firewalls. It may also include software, licenses, versioning, and support.

### **Network Architecture**

Most Network Architects and Engineers really enjoy this step in the auditing process. This is where they get to create their masterpiece – the creation of network diagrams. Some professionals use Microsoft Visio while others rely on tools like SolarWinds, Intermapper, Lucidchart, Edraw Max, and LANFlow.

Network diagrams are simply used to define the various connections and relationships that exist between locations and devices within the network. It provides a visual representation of the network.

### **Network Security**

Last but not least, network security plays an exceptionally large role in the auditing process. Some clients may choose to briefly touch on cybersecurity while others create detailed project scopes entirely on the subject.

### **How to Perform a Network Audit?**

We've discussed why network audits are important, when you should consider an audit, and how they relate to assessments. Let's now discuss how to perform a network audit. There are three stages involved in performing an audit – planning your audit, performing the audit, and post-audit activities.

### **Planning Your Network Audit**

The first rule of successful planning is preparation, right? If you do not plan properly, you may end up with delays and project outcomes you're not exactly satisfied with at its conclusion. Here's a couple of things you should consider when planning your network audit.

### **Get Buy-In from Stakeholders**

First and foremost, get buy-in from all stakeholders. That's right. This is critical to almost all IT related projects. There are usually two major stakeholders involved in network audits – Management Teams and the Technical Team.

Even if you have approval from Management, make sure to check-in and involve the Technical Team from the very beginning of your audit. They have access and insight into critical parts of the IT environment relating directly to the network.

### **Networking Tools**

Make sure that you have a plan for which tools you will be using to audit your network. You may be comfortable with a certain networking tool but if it's been a while, make sure to reach out to your peers and colleagues for advice on networking tools. Here are a few network auditing tools that are highly recommended by IT professionals.

## **Access to Devices**

Do you have access to all the devices? Whether you use a tool or not, you need access via SNMP, Telnet and/or SSH. Make sure to document the necessary credentials – community strings, usernames, and passwords for gaining access. This is especially true for SNMP as you may find that the network devices have not been enabled for SNMP.

## **Saving Data & Accessibility**

Where will you be accessing and saving data relating to the network audit? A personal laptop, desktop or hard drive? This can be a security concern and misplaced, highly-sensitive information can create increased risks and network vulnerabilities. You may also need a computer that can process and store large amounts of data.

## **Performing Your Network Audit**

You're ready to start your network audit but unsure where to start. To find a good starting point for your network, start by collecting the information that will be most relevant to the purpose of the audit. As an example, you may want to analyze and troubleshoot potential devices and locations that could be causing the issue. If you're interested in upgrading your network, you may want to review hardware lifecycles, services, and contract expiration.

## **Network Discovery Tool**

Here are some tools that we recommend when performing a network audit –Solarwinds, NetformX, Wireshark and Nessus. There are many out there, but we tend to gravitate towards the ones mentioned above.

If using an automated tool to perform your network audit, you can start by configuring basic settings such as the SNMP community strings (v1 or v2c) or usernames/passwords (v3), Telnet/SSH usernames/passwords, and enable passwords.

You will be able to use a seed device to initiate a crawl of network devices. It will start with the seed device and hop to other devices on the network using retrieved information from the seed device. You can also configure IP addresses and subnet ranges for the tool to probe.

Network discovery tools can take several hours or even days to create inventories of your network. Many of these tools will create inventories, diagrams, and documents for network audits. These will be used in the post-audit phase of the process.

## **Post Network Audit Action Items**

Running networking tools and creating inventories are great, but what do you do with the results from your audit? There are two outcomes that you should have at the end of your network audit – network audit report and audit recommendations.

## **Network Audit Report**

A network audit report simply keeps everything organized and is used to make sense of the information collected during the audit. As mentioned, many of these networking tools provide automated reports that address issues from a business and operational perspective rather than a technical point of view.

## **Audit Recommendations**

As a result of the audit report, you should have specific actionable data to examine and make recommendations on. This includes the discovery of obsolete devices, outdated software

versions, and underutilized network services. It can also be used to make quick-fix recommendations when troubleshooting network issues.

## **Firewall**

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

### **Types of Firewalls**

- **Packet filtering**  
A small amount of data is analyzed and distributed according to the filter's standards.
- **Proxy service**  
Network security system that protects while filtering messages at the application layer.
- **Stateful inspection**  
Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW)**  
Deep packet inspection Firewall with application-level inspection.

### **Firewall configuration**

Firewall configuration involves configuring domain names and Internet Protocol (IP) addresses and completing several other actions to keep firewalls secure. Firewall policy configuration is based on network types called "profiles" that can be set up with security rules to prevent cyber attacks.

### **A basic guide to configure a firewall in 5 steps: create zones, configure settings, and review firewall rules.**

As the first line of defense against online attackers, your firewall is a critical part of your network security. Configuring a firewall can be an intimidating project, but breaking it down into simpler tasks can make the work much more manageable. The following steps will help you understand the major steps involved in firewall configuration.

There are many suitable firewall models that can be used to protect your network. You can consult a HIPAA security expert or PCI security expert to learn more about your options. The following steps are critical, regardless of the firewall model you choose. This guide assumes that you are using a business grade firewall that supports multiple internal networks (or zones) and performs stateful packet inspection.

Due to the technical nature of firewalls, a detailed step-by-step guide is beyond the scope of this blog post. However, I will provide some direction to help illustrate the process so you can understand how to configure a firewall in 5 steps.

### **Step 1: Secure your firewall**

If an attacker is able to gain administrative access to your firewall it is "game over" for your network security. Therefore, securing your firewall is the first and most important step of this process. Never put a firewall into production that is not properly secured by at least the following configuration actions:

Securing a firewall is the vital first step to ensure only authorized administrators have access to it. This includes actions such as:

1. Update with the latest firmware
2. Never putting firewalls into production without appropriate configurations in place
3. Deleting, disabling, or renaming default accounts and changing default passwords
4. Use unique, secure passwords
5. Never using shared user accounts. If a firewall will be managed by multiple administrators, additional admin accounts must have limited privileges based on individual responsibilities
6. Disabling the Simple Network Management Protocol (SNMP), which collects and organizes information about devices on IP networks, or configuring it for secure usage
7. Restricting outgoing and incoming network traffic for specific applications or the Transmission Control Protocol (TCP)

## **Step 2: Architect your firewall zones and IP addresses**

In order to protect the valuable assets on your network, you should first identify what the assets are (for example, payment card data or patient data). Then plan out your network structure so that these assets can be grouped together and placed into networks (or zones) based on similar sensitivity level and function.

For example, all of your servers that provide services over the internet (web servers, email servers, virtual private network (VPN) servers, etc.) should be placed into a dedicated zone that will allow limited inbound traffic from the internet (this zone is often called a demilitarized zone or DMZ). Servers that should not be accessed directly from the internet, such as database servers, must be placed in internal server zones instead. Likewise, workstations, point of sale devices, and voice over Internet protocol (VOIP) systems can usually be placed in internal network zones.

Generally speaking, the more zones you create, the more secure your network. But keep in mind that managing more zones requires additional time and resources, so you need to be careful when deciding how many network zones you want to use.

If you are using IP version 4, Internal IP addresses should be used for all of your internal networks. Network address translation (NAT) must be configured to allow internal devices to communicate on the Internet when necessary.

Once you have designed your network zone structure and established the corresponding IP address scheme, you are ready to create your firewall zones and assign them to your firewall interfaces or sub-interfaces. As you build out your network infrastructure, switches that support virtual LANs (VLANs) should be used to maintain level-2 separation between the networks.

## **Step 3: Configure Access Control Lists (ACLs)**

Now that you have established your network zones and assigned them to interfaces, you should determine exactly which traffic needs to be able to flow into and out of each zone.

This traffic will be permitted using firewall rules called access control lists (ACLs), which are applied to each interface or subinterface on the firewall. Make your ACLs specific to the exact source and/or destination IP addresses and port numbers whenever possible. At the end of every access control list, make sure there is a “deny all” rule to filter out all unapproved traffic. Apply both inbound and outbound ACLs to each interface and subinterface on your firewall so that only approved traffic is allowed into and out of each zone.

Whenever possible, it is generally advised to disable your firewall administration interfaces (including both secure shell (SSH) and web interfaces) from public access. This will help to protect your firewall configuration from outside threats. Make sure to disable all unencrypted protocols for firewall management, including Telnet and HTTP connections.



#### **Step 4: Configure your other firewall services and logging**

If your firewall is also capable of acting as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion prevention system (IPS), etc., then go ahead and configure the services you wish to use. Disable all the extra services that you don't intend to use.

To fulfill PCI DSS requirements, configure your firewall to report to your logging server, and make sure that enough detail is included to satisfy requirement 10.2 through 10.3 of the PCI DSS.

#### **Step 5: Test your firewall configuration**

In a test environment, verify that your firewall works as intended. Don't forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations. Testing your firewall should include both vulnerability scanning and penetration testing.

Once you have finished testing your firewall, your firewall should be ready for production. Always remember to keep a backup of your firewall configuration saved in a secure place so that all of your hard work is not lost in the event of a hardware failure.

#### **Manage Firewall Continually**

Firewall management and monitoring are critical to ensuring that the firewall continues to function as intended. This includes monitoring logs, performing vulnerability scans, and regularly reviewing rules. It is also important to document processes and manage the configuration continually and diligently to ensure ongoing protection of the network.

#### **Router**

A router is a physical or virtual appliance that passes information between two or more packet-switched computer networks. A router inspects a given data packet's destination Internet Protocol address (IP address), calculates the best way for it to reach its destination and then forwards it accordingly.

#### **Router Configuration:**

1. Connect the router to the modem.
2. Connect the computer to the router.
3. Go to the router's default IP address in a browser.
4. Sign in with the default username and password.
5. Open the Wireless settings.
6. Name your network.
7. Set an encryption type and passphrase.
8. Save your changes.

#### **Before you configuring router first of all you have to-**

##### **Check your Internet connection**

If you don't have a good internet connection, the router setup experience will be frustrating. The simplest method is to connect a computer to the modem or gateway device supplied by your Internet service provider (ISP). If your computer detects an Internet connection, you're ready to set up the router.

##### **Gather documentation**

Here's another "seems obvious" step—but one that will save you aggravation when you're in the middle of setup. Keep an eye out for stickers or slips of paper that might include important setup information, like the router's default username and password.

## **Check for an app**

Many router manufacturers provide mobile apps or web dashboard that can be used for both setup and management. With a smartphone app, you may not have to connect the router to a computer to configure it. Check the documentation that came with your router to see if an app is available.

## **Install and extend antennas**

If the router has antennas and they're separate from the router box, you'll need to install them. In addition, you should extend the antennas before beginning the setup process.

## **Router setup steps**

### **Step 1: Decide where to place the router**

The best place for a wireless business router is in an open area of the workplace, as you'll benefit from even coverage. However, sometimes it's not easy to find a space out in the open because you must connect the router to a broadband gateway from your ISP (Internet service provider), which is usually attached to a cable near an outside wall.

### **Step 2: Connect to the Internet**

Attach the router to a cable - or choose a mesh router

To solve the "long-distance" problem when connecting a router, you can use a CAT5e or CAT6 cable to connect the router to the ISP gateway's Ethernet port. Another option is to run Ethernet cables through the walls of your office to the chosen central location for the router.

Yet another option is to install a mesh network with a router. A mesh network allows you to place multiple Wi-Fi transmitters across your home or office, all on one network. Unlike extenders, which can be used with any wireless router, mesh networks require a router with this capability built-in.

No matter which option you choose, you'll use a basic Ethernet cable, plugged into the router's wide-area network (WAN) or Internet port. The Internet port is typically set apart from other ports by a different color.

Check the router's LED lights

Your router's LED lights tell you if you've successfully made an active Internet connection. If you don't see lights confirming such a connection, make sure you've plugged the cable into the correct port.

Test the connection with a device

Confirm that your router has a working connection by plugging a laptop computer into one of the device ports on the back of the router. If all goes well, you should be able to begin a wired connection, just as you did when confirming an active Internet connection.

### **Step 3: Configure the wireless router gateway**

In some cases, ISPs offer customers gateways with built-in routers. In most cases, these combined devices are not built for business environments, nor do they have extra ports, security, and other options that allow you to add services and expand networks as the business grows.

If you have a gateway with an integrated router, you'll have to configure the gateway to disable the router and pass the WAN IP address—the unique Internet protocol address that the Internet provider assigns to your account—and all network traffic through to your new router.

If you don't take this step, you may run into conflicts that prevent devices from working properly. You may need to contact your ISP for help with this step.

#### **Step 4: Connect gateway to router**

First, turn off the gateway. If there is already an Ethernet cable plugged into the gateway's local-area network (LAN) port, unplug the cable and plug it into your router's WAN port. Turn the gateway back on and wait a few minutes for it to boot up. Plug in the router's power supply and turn it on, again waiting a few minutes.

#### **Step 5: Use app or web dashboard**

The easiest way to continue with router setup is to use a mobile app if the router maker provided one. If there is no app, or you'd rather use the router's web-based dashboard, connect the router to a computer via an Ethernet cable.

You might find the router's IP address printed on the back of device itself; if not, type 192.168.1.1, a common router address, into the browser search bar.

#### **Step 6: Create a username and password**

To configure the router, you'll need to log in, using its default admin name and password. You can usually find this information printed on the router itself, or in an accompanying user manual. Next, enter the required credentials. Once you're in, you should immediately create a new username and password. The defaults are usually something like "admin" and "password1234," which are obviously not secure—so make sure to change them at the first opportunity.

#### **Step 7: Update the router's firmware**

Your router may need an update of the "firmware," or software that operates it. Update it as soon as possible, since the new firmware might fix bugs or offer new security protections.

Some routers may download new firmware automatically, but many do not. You may need to check for updates through the app or the browser interface.

#### **Step 8: Create a Wi-Fi password**

Just as most routers come with preassigned admin usernames and passwords, most also come with preset Wi-Fi usernames and passwords. You'll likely be prompted to change the Wi-Fi username and password, but even if you don't see such a prompt, plan to do so quickly.

#### **Step 9: Use auto-configuration tools where possible**

If your router is equipped with auto-install features, rely on them to help complete setup. For example, you should be able to use auto-configuration to manage IP addresses with the Dynamic Host Configuration Protocol (DHCP), which automatically assigns IP addresses to devices. You can always change these addresses later.

#### **Step 10: Set up security**

Many router manufactures provide security functionality to safeguard network and user privacy. You can login into the web dashboard and enabling added security features such as firewall, web filtering, and access controls to protect yourself from malicious traffic. You can also set up virtual private networks (VPNs) for privacy.

#### **Connect to your network wirelessly, or via ethernet.**

Note: An ethernet cable works a bit better, because your router will disconnect your from the wireless network for a moment while it switches channels.

### **Find your router configuration page.**

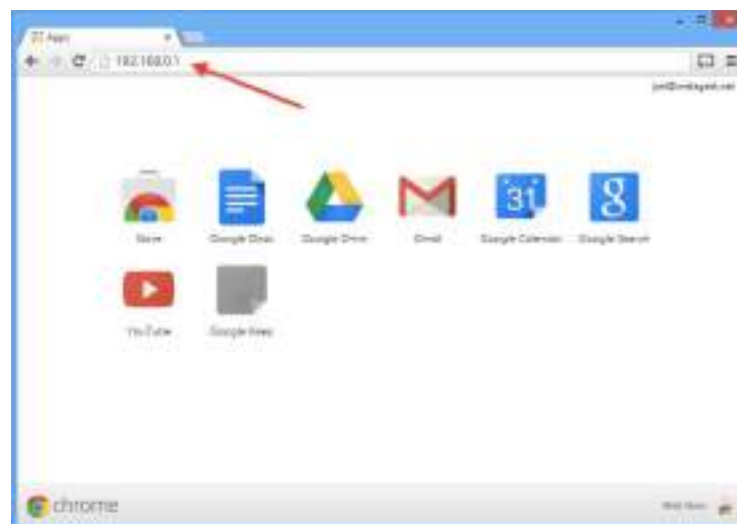
Access the router configuration page by typing the router's **IP address** in to the address bar, and pressing **enter**.

IP Address	Typical For
192.168.0.1	D-Link, Netgear, and others. Try this IP first.
192.168.1.1	Linksys, Belkin, TP-Link, and others
192.168.15.1	Clear/ClearWire
192.168.100.1	Virgin Media Superhub
192.168.1.254	TP-Link
10.0.1.1	This is pretty rare.

Note: Even though there are a few more possible addresses, it doesn't take long to see the pattern. Try changing the second to last number if none of those work.

### Wait a minute... what's an IP Address?

Glad you asked! Each router hosts a tiny webpage that you access to configure it. Just like a website has an address (such as [www.metageek.com](http://www.metageek.com)), your router has an address. Since it's a home Wi-Fi router, it doesn't need a name reserved for it, so it's just a numerical address. Typing in the address in the address bar on your browser will take you to the configuration page for your router.



### 3. Log in with the username and password.

Visualize Your Wi-Fi Landscape with in SSID. SSID shows you exactly how your network is configured, how neighboring Wi-Fi networks are impacting yours, and gives suggestions for fast, secure Wi-Fi.



Most routers require a username and password. The default username is usually *admin*. The default password is usually on a sticker on the router, or printed on the paper manual or packaging. If you can't figure it out, Google the model number of your router and "password" together.



#### 4. Find the Wireless Settings page.

On the D-Link router that we used, the wireless settings page was easy to find. Usually, you can locate it along the top or the left side, but it depends on the router. In some cases, it's hidden in



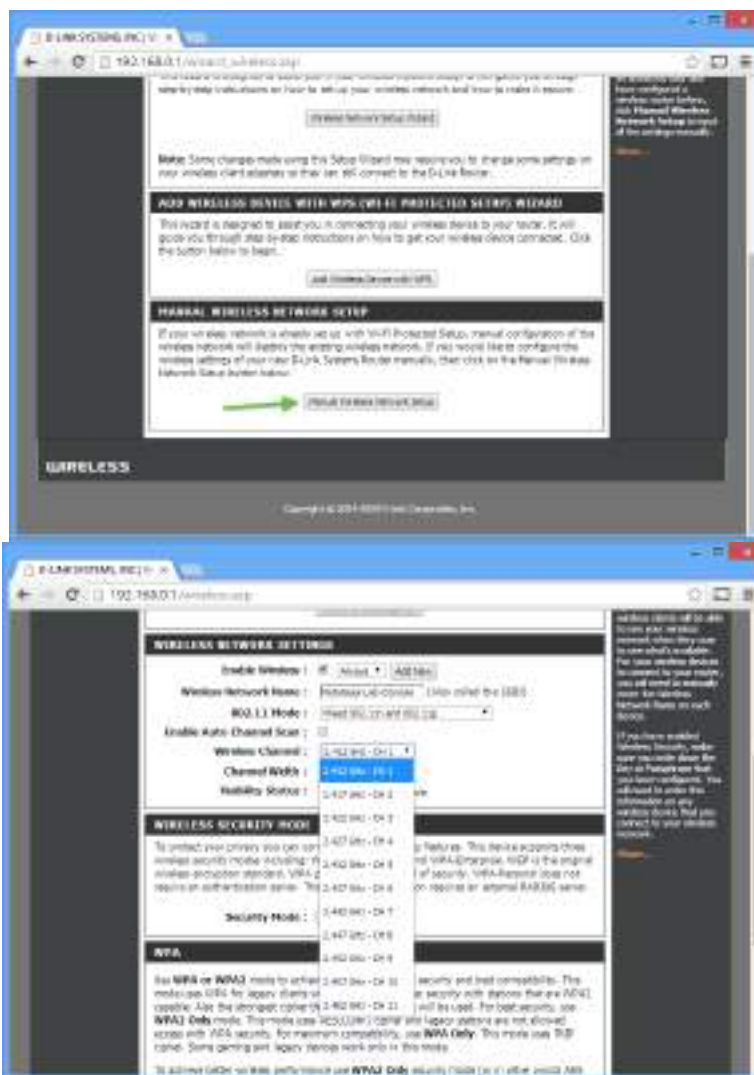
another menu.

### 5. Set the new channel, usually with a dropdown menu.

1, 6, and 11 are the only three channels that don't overlap on the 2.4 GHz band, and while putting your Wi-Fi network on the same channel as another network in the same band isn't ideal, it is always a better idea to share a channel than to overlap.

This is also a really good time to make sure that you are using WPA2 for security, and 20 MHz channels only (not 40 MHz or "bonded" channels).

In the 5 GHz band, almost any channel is a good choice except for DFS channels. Therefore we recommend using channels 36-48, or 149-165. We recommend using 40 MHz wide channels in the 5 GHz band.



Click *Save Settings* or *Apply Settings* to save the changes.

### 6. Your router will now reboot.

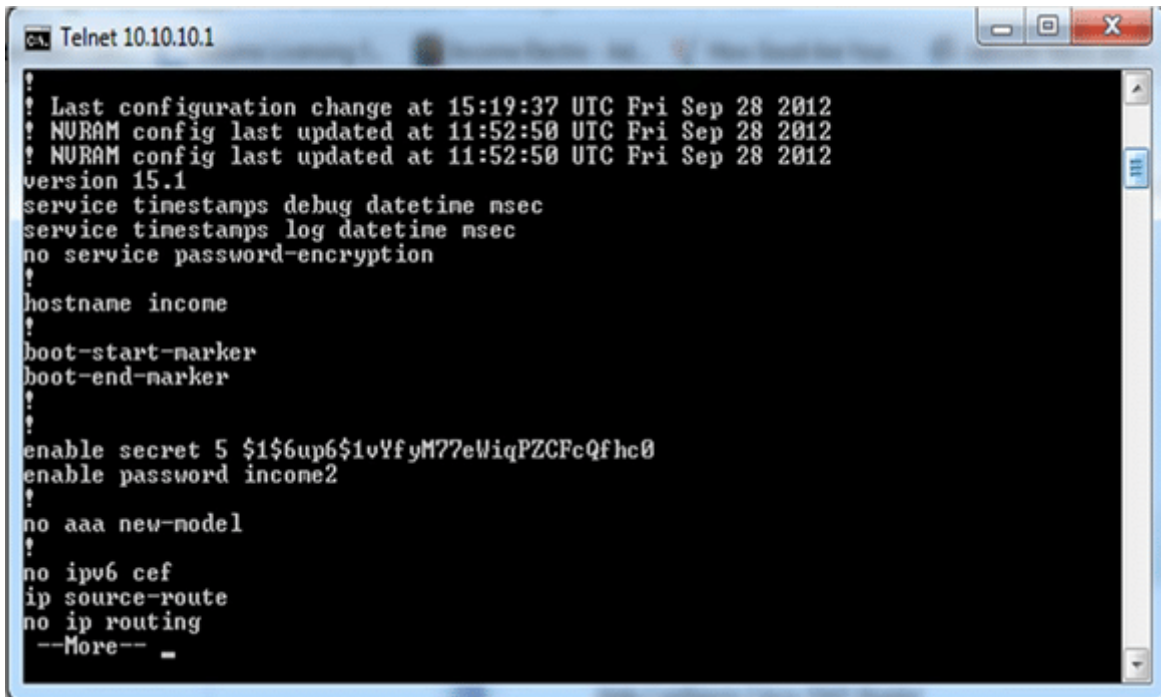
If you are connected wirelessly, it might take a moment for the channel to switch and for your computer to reconnect. Restart in SSID to verify that the changes have been applied.

## Default Router Configuration

Whenever we boot our Router first, there is always some default configuration that exists into it. The **show running-config** command is used to see the starting configuration of the router. The details are very lengthy. Here, I have given an example of a few of the important lines shown by the router, when we enter the show running-config command into the router with the help of two screenshots.

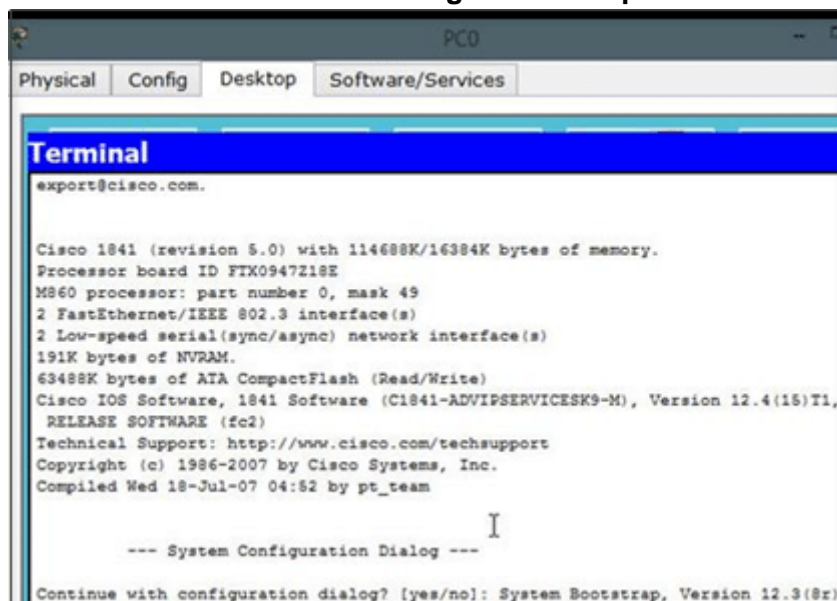
**Router#** show running-config

### Default Router configuration Output-1



```
Telnet 10.10.10.1
?
? Last configuration change at 15:19:37 UTC Fri Sep 28 2012
? NVRAM config last updated at 11:52:50 UTC Fri Sep 28 2012
? NVRAM config last updated at 11:52:50 UTC Fri Sep 28 2012
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
?
hostname income
?
boot-start-marker
boot-end-marker
?
?
enable secret 5 $1$6up6$1vYfyM7?eWiqPZCFcQfhc8
enable password income2
?
no aaa new-model
?
no ipv6 cef
ip source-route
no ip routing
--More-- _
```

### Default Router configuration Output-2



```
PC0
Physical Config Desktop Software/Services
Terminal
export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947218E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

I
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: System Bootstrap, Version 12.3(8r)
```

In the above default configuration details, we can see that all the interfaces are down and there are no IP addresses and not any route are allocated to any port or interface of the router.

**#1)** Now we need to configure the router with some basic parameters like enabling hostname, password and enabling the terminal for configuration.

**#2)** For performing configuration on the router from the remote end using the console port we need to enable the configure terminal mode.

**#3)** By using telnet, we can login into the router with the username and password from the remote end system.

telnet router name or IP address

**Example:**

Telnet 10.180.196.42

Login: Router1 (specify login id, here login id is Router1)

Password: \*\*\*\*\*

Router> enable

**#4)** The understanding will become better with the help of the following.

**Example:**

Router> enable

Router# configure terminal

Router(config)# <— Now router is in configuration mode. The configuration can be done.

**#5)** Now define the hostname ( router name ) and password.

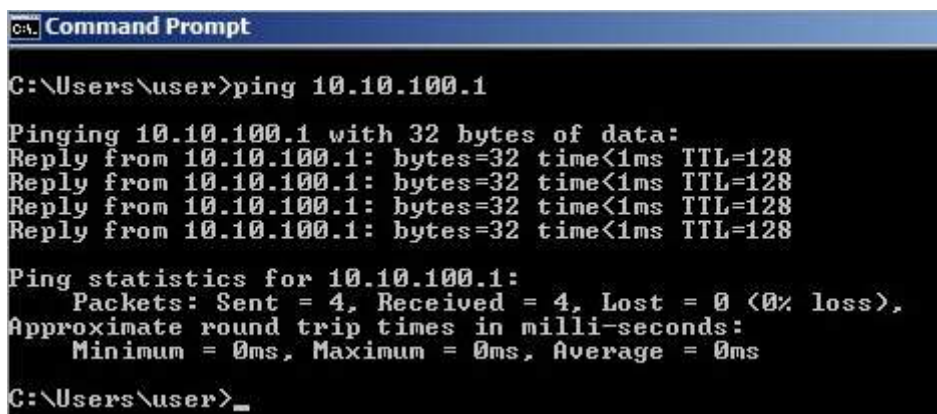
Router(config)# hostname Router X

Router(config)# exit

**#6)** To find out from the remote end if the far end IP of the router, switch or any other host is reachable or not, we use “Ping” command. It is one of the important commands and can be used locally on your PC as well to check the IP reachability.

**RouterX# ping 10.10.100.1**

**Ping Command Output**



```
C:\Users\user>ping 10.10.100.1

Pinging 10.10.100.1 with 32 bytes of data:
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128
Reply from 10.10.100.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>_
```

*[image source]*

The above output shows that the ping is successful and the IP is reachable. It is also used to check the loopback interface.

If in case we don't get any response then it means that we are not reaching up to the IP due to some reason.



## Configuration of Gigabit Ethernet Interfaces

The next task is to configure those ports and interfaces on which the connection with other network devices has been physically made. There are various types of interfaces like fast Ethernet, Ethernet and Gigabit Ethernet that are available on the router.

In WAN connectivity or WLAN, the gigabit interface is used, as it is of high bandwidth and high-speed link.

Thus understanding the configuration of this interface is very crucial. Please find below some points, which we should keep in mind while configuring the gigabit interfaces.

**1)** The first step is to go to the config mode of the router and then enter on which port or slot of gigabit Ethernet you are going to perform the configuration.

***RouterX (config)# interface gigabitethernet 0/1***

RouterX (config-if)# Now the user is at the gigabit interface 0/1 and it can further configure the IP address and subnet mask etc.

**2)** Ideally, in the router, all the interface ports are in the downstate i.e inactive. To make them in an active state or “up” the following command is used.

***RouterX (config-if)# no shutdown***

**3)** Similarly, we can define the IP address and subnet mask to other gigabit and fast Ethernet ports as well by following the above steps, one by one.

**4)** To check our configuration on interfaces, we can run one show command as given below:

***RouterX# show up in brief***

**5)** To save our configuration we use the write command.

***RouterX# write then enter will save the configuration.***

**The below figure represents the configuration in the command line on a Gigabit Ethernet interface:**



[image source]

## Configuration of Loopback Interface

Defining the loopback IP address is very crucial as it provides default routing statistics.

**1)** The first step is to go to the configuration mode and add the interface with the type number on which you are going to define the address.

### Example:

RouterX (config)# interface loopback 1  
While (1 denotes the type number)

**2)** Now assign the IP address and subnet mask for loopback.  
RouterX (config-if)# ip address 172.148.1.1 255.255.255.240

**3)** Now the next command is  
RouterX (config-if)# exit —> the configuration has been saved and by using the exit command we step out from the loopback interface.  
RouterX (config)# —> Returns to the simple configuration mode.

## Configuration of Command-Line Access

The commands under this category are used to provide only limited access of Routers to the users or we can say that the access of routers is managed by a remote user or administrator.

**#1)** The first command is line console| tty | vty ] line number.

This command denotes the type of the line and console terminal used for accessing the Router.

**Example:**

```
RouterX (config)# line console 0  
RouterX (config-line) #
```

**#2)** The next step is to assign a password for access.

**Example:**

```
RouterX (config-line)# password abc123!
```

**#3)** The login command is used to verify if the password is enabled or not to login into the Router.

```
RouterX (config-line)# login
```

**#4)** For denoting the virtual terminal for remote access, the following command is used – line console vty line number.

**Example:**

```
RouterX (config-line)# line vty 0 6 (6 denotes that 6 virtual telnet options are available)
```

**#5)** To exit from this command-line access the end command is used.

**Example:**

```
RouterX (config-line)# end  
Router#
```

## **Configuration of Static Routes**

Routing the data packets from the source to the destination end is the basic feature of Routers. The static route provisions the predefined set of routes to reach the destination in the network.

**The procedure to configure static routes is as follows:**

1. ip route {destination host IP address | subnet mask | source interface IP address}
2. end
3. Show ip route will show the routes defined in the router and we can also verify this command from our routing configuration.

**Example of defining static IP route is:**

```
RouterX (config)# ip route 10.180.146.4 255.255.255.252 10.180.146.29
```

```
RouterX (config)# ip route 10.180.146.28 255.255.255.252 10.180.146.5
```

```
RouterX (config)# end
```

The above example of defining IP route explains that the router will float all the IP packets of the destination address 10.180.146.4 and of subnet mask 255.255.255.252 on the Gigabit Ethernet interface 0/1 to a destined device with the IP address 10.180.146.29.

In reverse routing, all the IP packets with the destination address 10.180.146.28 will be destined to the device having interface IP 10.180.146.5.

## **Configuration of Dynamic Routes**

In this type of routing protocol, the routers will gather the routing information dynamically. Thus the routes can be changed on the basis of the kind of service, topology and network traffic.

The Cisco and ZTE routers use various kinds of dynamic routing protocols, but the most popularly ones are Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP).

## RIP Configuration

**The steps of configuring RIP on routers are as follows:**

1) Firstly go to the configure terminal mode.

```
Router> configure terminal  
RouterX (config)#
```

2) Now enable the RIP protocol on the router.

**For this, the command is as below:**

```
RouterX (config)# router rip
```

3) Now the RIP protocol on the router is enabled. Thus we can assign the IP address range and version to the router for those network addresses which are using RIP routing as shown below.

4) Next for disabling the routes of the subnet used for automatic summation, we use the following commands:

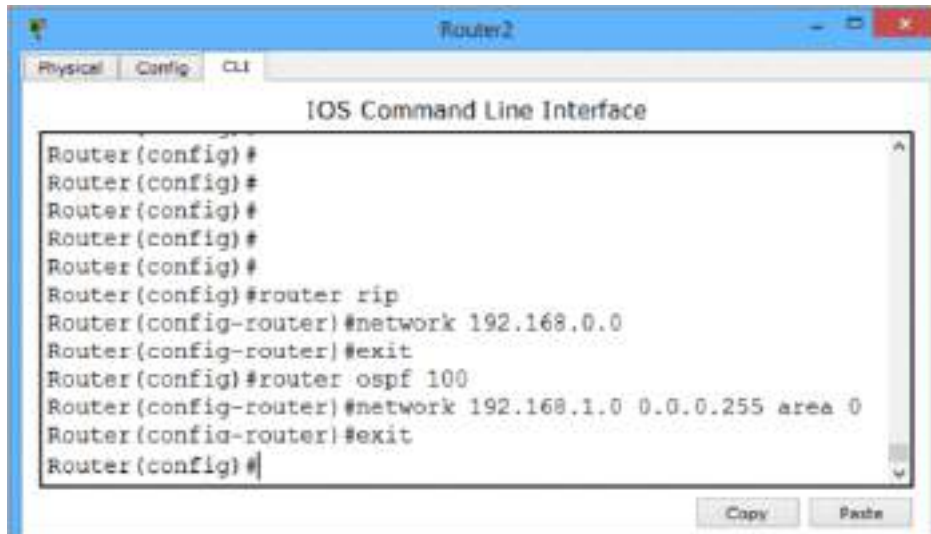
```
RouterX (config-router)# no auto-summary
```

5) The last step is to save the configuration and exit from the router configuration mode.

To verify the configuration, we use **the show running-config** command and the output will appear similar to as shown in the below figure.

```
RouterX# show running-config
```

## RIP Configuration



```
Router2
Physical | Config | CLI
IOS Command Line Interface
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#exit
Router(config)#router ospf 100
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
```

## EIGRP Protocol Configuration

The process is as follows:

#1) Firstly, go to router configuration mode and enable the EIGRP on the router.

The command is as shown below:

RouterX (config)# router eigrp 203 → The number here specifies the auto-generated system number which locates the router to the other EIGRP using routers.

2) Now assign the range of the network IP's on which EIGRP is applied as follows:

3) The last step is to save the configuration and exit from the router configuration mode.

To verify the configuration, we use **show running-config** command and the output will appear similar to as how it is shown in the below figure:

Router# show running-config

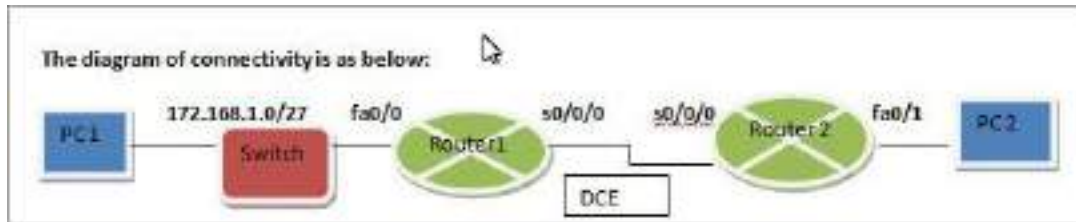
```
Router_A>en
Router_A#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_A(config)#router eigrp 10
Router_A(config-router)#network 10.0.0.0
Router_A(config-router)#network 20.0.0.0
Router_A(config-router)#end
Router_A#
%SYS-5-CONFIG_I: Configured from console by console
```

[[image source](#)]

Thus from the above set of examples, we have learned various commands that are commonly used for basic configuration and show configuration purposes in the routers.

Now let's make our understanding better with the help of an example of a simple router network and software configuration in them.

### Router Connectivity Diagram



### Addressing Table:

Device name	Interface	IP address	Subnet mask
R1	Fa0/0	172.148.1.1	255.255.255.224
R1	S0/0/0	172.148.2.1	255.255.255.224
R2	Fa0/1	172.148.3.1	255.255.255.224
R2	S0/0/0	172.148.2.2	255.255.255.224
PC1	NA	172.148.1.10	255.255.255.224
PC2	na	172.148.3.10	255.255.255.224

For any network to be operational, it is very important to do the IP planning of the network properly. Thus we are prepared with the IP addresses to be allocated to the interfaces on Router1 and Router2. All the physical network cabling should be done in accordance with the plan.

### The steps of the configuration are as follows:

- 1) Firstly set up a hyper terminal connection with Router1 and enable the execution mode.  
Router> enable  
Router#
- 2) Next is to go to the configure terminal mode.  
Router# configure terminal  
Router (config)#
- 3) Next step is to assign a hostname to the router.  
Router (config)# hostname R1  
R1 (config)# Now configuration will take place on Router1.
- 4) Disable the DNS loopback.  
R1 config)# no ip domain-loopback
- 5) Now configure the password to the router.
- 6) Also, configure a password for virtual terminals.
- 7) Next is the configuration of interfaces with the Network IP addresses.
- 8) When we configure the serial interface, we will also set the clock rate to 64000.

Here, please make a mark that the serial interface will not come in up state until the serial interface on Router2 is also configured and made up.

Now save the configuration that has been done on Router1.

```
R1# write running-config startup-config
```

```
Building configuration.....
```

```
[OK]
```

```
R1#
```

9) Now the steps for configuration of Router2 for assigning hostname, configuring a password for the router and virtual terminals and disabling the DNS loop are same as in the case of Router1.

**See below as how the output of the above commands will appear on the command line with the help of a similar example:**

```
HQ(config)#interface fa0/0
HQ(config-if)#ip address 172.16.0.1 255.255.254.0
HQ(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
o up

HQ(config-if)#interface s0/0/0
HQ(config-if)#ip address 192.168.1.17 255.255.255.252
HQ(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial10/0/0, changed state to down
HQ(config-if)#interface s0/0/1
HQ(config-if)#ip address 192.168.1.21 255.255.255.252
HQ(config-if)#clock rate 64000
HQ(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial10/0/1, changed state to down
HQ(config-if)#interface loopback0

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

HQ(config-if)#ip address 209.165.200.225 255.255.255.252
```

10) The next step is to manually configure the host device PC1 and PC2 with the IP's 172.148.1.10 and 172.148.3.10 and with the subnet mask 255.255.255.224 respectively.

11) Now finally it's time to validate our configuration by using the show ip route command and show ip interface brief command in router 1 and router 2.

### Show IP route output

```
R1# show ip route
```

**The output will appear in the command line as much similar as shown in the below screenshot:**

```

Dynamips(0): R1, Console port
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, D - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
R1#

```

**Show IP interface brief command output**

R1# show ip int brief

If you want to see how it will appear in the command line, then please take a look at the below screenshot:

```

Dynamips(0): R1, Console port
R1#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
FastEthernet0/0    192.168.1.150  YES NVRAM    up            up
FastEthernet0/1    unassigned      YES NVRAM    administrativ down down
Serial1/0          unassigned      YES NVRAM    administrativ down down
Serial1/1          unassigned      YES NVRAM    administrativ down down
Serial1/2          unassigned      YES NVRAM    administrativ down down
Serial1/3          unassigned      YES NVRAM    administrativ down down
FastEthernet3/0    unassigned      YES NVRAM    administrativ down down
FastEthernet3/1    unassigned      YES NVRAM    administrativ down down
SSLVPN-VIF0       unassigned      NO  unset     up            up
R1#

```

From the above-detailed output of show commands, our configuration has been checked and found OK.

**Home Router Configuration Vs Company Set-up Routers**

Enlisted below is the comparison between home routers and business purpose routers.

**Home Routers**

The routers which are used for home purposes are less expensive than the business purpose routers. The installation of routers for home use is easy and the maintenance cost is also less as they only need to cover a limited area for operation, and not the WAN regions.

The trend of using routers for home purposes like accessing the Internet for multiple users at a time, entertainment like watching online movies, gaming, and controlling the settings at home like light, temperature, on and off operations of home appliances etc. when we are not at the home is very common these days.

Thus it is essential for us to understand the process of configuration of home usable routers. The steps are not as long as that is of Business purpose routers.

**Please find below the generic process of installation and configuration:**



**#1) Setting the hardware:** We need a desktop PC to make a connection with the router and two network cables. By using the first network cable, connect the WAN port of the router to the modem or DSL through which the Internet connection is going to be provided. Now by using the second network cable, connect the LAN port of the router to the PC's network port.

Now, switch on the power supply of router, PC and the modem by using the power adapter. This sums up the hardware installation part.

**#2) To access the Web Interface:** For accessing the router's web interface we need to know the router's login IP address, password, and the router's URL. This information can be extracted from the manual of the router.

Usually, the default IP address is the default URL for accessing the router, and it will be like 192.168.x.1 where x can be 0,1,2,10 Or 11. For D-link routers, it will use the default IP as 192.168.0.1 or 198.168.1.1. Mostly the default username is admin and the default password is admin, password or 1234.

With all these data, in the address browser of the PC from which the router is connected, type the default IP of the router and then the login ID and password, and now you will enter into the web interface of the router.

**#3) Basic Router Settings:** Through the web interface we can make the basic settings in the router. Though there are different types of parameters based on the type of router, some of the generic parameters are explained here in short.

The first parameter is the Wizard, here we can set the Wi-Fi network name and password and can modify the default password that is used to log in the device to make it a more secure one for personal use.

Next are the router's wireless settings, where we can make the settings for the network. In the LAN settings part, we will assign the IP to the router and also allocate the IP address and subnet mask to the client's connected with the router.

In case, if the router's settings get deleted or if altered by chance or by some virus, then we can restore the default settings or the basic settings by going to system tool of the router. Here, we can keep the backup of the router's configuration and save it in a file format.

**#4) Router's hard Reset option:** If in case the router is malfunctioning or if it is hung for a long time or if unable to login into it, then we can use the hard reset button of the router that is found at the bottom portion of the router.

As the reset button is very tiny, we can use a small pin to push the button for about 10-15 seconds to do the hard reset. By doing this action, the router will go back to its default settings in the way in which it was while purchasing it.

In this way, the configuration of a home router is concluded and now it is ready to use to access the internet or share the Internet services among the users present at home.

## **Switch Configuration using Cisco Switch Commands**

Before we begin, get to know what hardware you're using, fire up your CLI and download PuTTY.

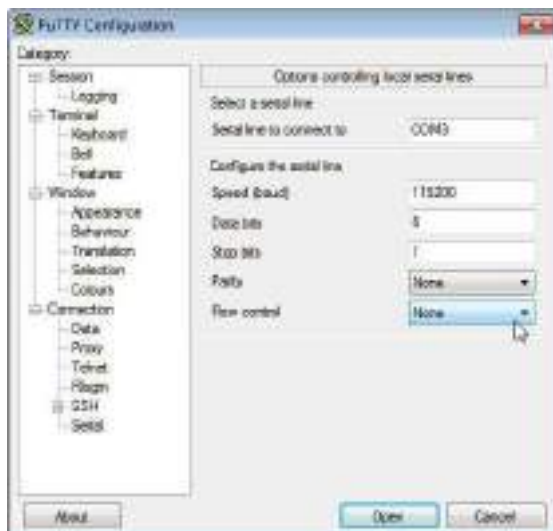
The first step is to check what hardware you're using before you begin. If you're using a Cisco switch you need to know what model you have. You also want to check the physical state of the device and verify that none of the cables are damaged. You can turn the router on to make sure there is no damage to the lighting/indicators.

Now that you've made sure the device is in working order you're ready to start configuring. In this guide, we're going to perform a **Cisco switch configuration** through the **command-line interface** (CLI) with the open-source SSH/Telnet client PuTTY (although you can use another tool if you prefer). If for any reason putty is not an option for your setup, you can get similar results with a PuTTY alternative.

## Connect the Switch to PuTTY

To start configuration, you want to connect the switch console to PuTTY. You can do this by doing the following:

1. Connect the switch to PuTTY with a 9-pin serial cable.
2. Now open PuTTY and the PuTTY Configuration window will display. Go to the **Connection type** settings and check the **Serial** option (shown below).

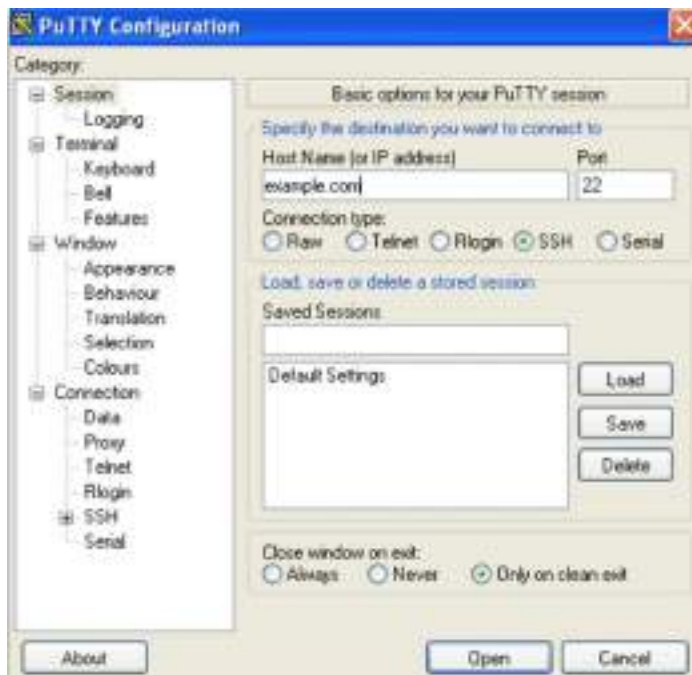


3. Go to the **Category** list section on the left-hand side and select the **Serial** option.
4. When the options controlling local serial lines page displays enter the COM port your network is connected to in the **Serial line to connect to** box e.g. **COM1**.
5. Next, enter the digital transmission speed of your switch model. For 300 and 500 Series Managed Switches, this is **115200**.
6. Go to the **Data bits** field and enter **8**.
7. Now go to the **Stops bits** field and enter **1**.
8. Click on the **Parity** drop-down menu and select the **None** option.
9. Go to the **Flow Control** drop-down menu and select the **None** option.

## Save Your Settings and Start the PuTTY CLI

To save your PuTTY settings for your next session do the following:

Click on the **Session** option from the **Category list** on the left-hand side of the page.



1. Go to the **Saved Session** field and enter a name for your settings e.g. **Comparitech**.
2. Click the **Save** button to store the settings.
3. Press the **Open** button at the bottom of the page to launch the CLI.

The following message will display in the command prompt:

**Switch>**

2. Enter Privileged EXEC Mode and Set a Hostname for the Switch

Type in the enable command to enter privileged EXEC mode (you don't need a password at this stage because you're under the default configurations which don't have one!):

**Enable**

Next, enter Global Configuration Mode and enter the following command:

```
Switch# configure terminal  
Switch(config)#
```

You can make the switch easier to locate in the network by assigning a hostname. Enter the following command to assign a hostname:

```
Switch(config)# hostname access-switch1  
access-switch1(config)#1
```

3. Assign a Password to the Switch

Once you've assigned a hostname you will want to create a password to control who has access to the privileged EXEC mode (to prevent everyone from being able to log in). To assign an administrator password to enter the following command:

```
access-switch1(config)# enable secret COMPARI7ECH
```

Remember to pick a strong password so that it's harder to figure out.

#### 4. Configure Telnet and Console Access Passwords

The next step is to configure passwords for Telnet and console access. Configuring passwords for these is important because it makes your switch more secure. If someone without authorization gains telnet access then it puts your network at serious risk. You can configure passwords by entering the following lines (See the top paragraph for Telnet and the bottom paragraph for Console access).

##### Telnet

```
access-switch1(config)# line vty 0 15
```

```
access-switch1(config-line)# password COMPARI7ECH
```

```
access-switch1(config-line)# login
```

```
access-switch1(config-line)# exit
```

```
access-switch1(config)#
```

##### Console

```
access-switch1(config)# line console 0
```

```
access-switch1(config-line)# password COMPARI7ECH
```

```
access-switch1(config-line)# login
```

```
access-switch1(config-line)# exit
```

```
access-switch1(config)#
```

#### 5. Configure IP Addresses with Telnet Access

The next step is to decide which IP addresses will have access to Telnet, and add them with the PuTTY CLI. To select permitted IP's enter the following command (replace the listed IPs with the IPs of the components you want to grant permission to):

```
access-switch1(config)# ip access-list standard TELNET-ACCESS
```

```
access-switch1(config-std-nacl)# permit 216.174.200.21
```

```
access-switch1(config-std-nacl)# permit 216.174.200.21
```

```
access-switch1(config-std-nacl)# exit
```

You can also configure your network's access control lists (ACLs) to virtual terminal (VTY) lines. ACLs ensure that only the administrator can connect to the router through Telnet.

```
access-switch1(config)# line vty 0 15
access-switch1(config-line)# access-class TELNET-ACCESS in
access-switch1(config-line)# exit
access-switch1(config)#
```

#### 6. Configure a Network Management IP address (or Management Interface)

Next, you need to configure a network management IP address. Switches don't come with an IP address by default, meaning that you can't connect to it with Telnet or SSH. To solve this problem you can select a virtual LAN(VLAN) on the switch and create a virtual interface with an IP address. You can do this by entering the following command:

```
access-switch1(config)# interface vlan 1
access-switch1(config-if)# ip address 10.1.1.200 255.255.255.0
access-switch1(config-if)# exit
access-switch1(config)#
```

The new IP management address is located in VLAN1, which other computers will now use to connect.

#### 7. Assign a Default Gateway to the Switch

At this stage, you want to assign a default gateway to the switch. The default gateway is essentially the address of the router that the switch will be communicating with. If you don't configure a default gateway then VLAN1 will be unable to send traffic to another network. To assign the default gateway, enter the command below (change the IP address to that of your router).

```
access-switch1(config)# ip default-gateway 10.1.1.254
```

#### 8. Disable Unused Open Ports

As a best practice, it is a good idea to disable any unused open ports on the switch. Cyber-criminals often use unsecured ports as a way to breach a network. Closing these ports down reduces the number of entry points into your network and makes your switch more secure. Enter the range of ports you want to close by entering the following command (you would change 0/25-48 to the ports that you want to close):

```
access-switch1(config)# interface range fe 0/25-48
access-switch1(config-if-range)# shutdown
access-switch1(config-if-range)# exit
access-switch1(config)#
```

#### 9. Save Your System Configuration Settings

Once you've finished configuring the router it's time to save your system configuration. Saving the configuration will make sure that your settings are the same when you open up your next session. To save enter the following command:

```
access-switch1(config)# exit  
access-switch1# wr
```

Always remember to save any changes to your settings before closing the CLI.

## 10. Configure NetFlow to Manage Your Cisco Switch (Optional)

It is also a good idea to use a network traffic analyzer to monitor network traffic. As a Cisco device, your switch will have the communication protocol NetFlow. However, it must be configured first. You can configure NetFlow by completing the four steps below. Before we begin, enter Global Configuration Mode by executing the following command:

### **Switch# configure terminal**

Create a flow record

1. The first step is to create a flow record (you can change the name). You can do this by entering the following command:

```
#flow record Comparitechrecord
```

2. After you've entered the previous command you need to set the IPv4 source address, IPv4 destination address, IPv4 protocol, transport source-port, transport destination-port, IPv4 tos, interface input, and interface output. You can do this by entering the following command:
3. **Switch# match ipv4 source address**
- 4.
5. **Switch# match ipv4 destination address**
- 6.
7. **Switch# match ipv4 protocol**
- 8.
9. **Switch# match transport source-port**
- 10.
11. **Switch# match transport destination-port**
- 12.
13. **Switch# match ipv4 tos**
- 14.
15. **Switch# match interface input**
16. **Switch# collect interface output**
17. To finish configuring the flow record and define the type of data you're going to collect, enter the following switch configuration commands:
18. **Switch# collect interface output**
- 19.
20. **Switch# collect counter bytes**
- 21.
22. **Switch# collect counter packets**
- 23.
24. **Switch# collect timestamp sys-uptime first**

25.

**Switch# collect timestamp sys-uptime last**

Create the Flow Exporter

1. You must now create the flow exporter to store the information that you want to export to an external network analyzer. The first step is to name the flow exporter:  
**Switch# flow exporter Comparitechexport**
2. Enter the IP address of the server your network analyzer is on (Change the IP address):  
**Switch# destination 117.156.45.241**
3. Configure the interface that you want to export packets with:  
**Switch# destination source gigabitEthernet 0/1**
4. Configure the port that the software agent will use to listen for network packets:  
**Switch# transport UDP 2055**
5. Set the type of protocol data that you're going to export by entering this command:  
**Switch# export-protocol netflow-v9**
6. To make sure there are no gaps in when flow data is sent enter the following command:  
**Switch# template data timeout 60**

Create a Flow Monitor

1. Once you've configured the flow exporter it is time to create the flow monitor. Create the flow monitor with the following command:<  
**Switch# flow monitor Comparitechmonitor**
2. Associate the flow monitor with the flow record and exporter we configured earlier:  
**Switch# record Comparitechrecord**  
**Switch# exporter Comparitechexport**
3. To make sure that flow information is collected and normalized without a delay, enter the following command:  
**Switch# cache timeout active 60**  
**Switch# cache timeout inactive 15**
4. Enter the exit command:  
**Switch# exit**
5. You need to input the interfaces that will collect the NetFlow data. If this is an ethernet interface you would enter the following:  
**Switch# interface gigabitEthernet 0/1**
6. Use the following command to configure NetFlow on multiple interfaces (the input command will still collect data in both directions):  
  
**Switch# ip flow monitor Comparitechmonitor input**
7. If you want to collect NetFlow data on only one interface then you must use the input and output command. So you would enter the following:  
  
**Switch# ip flow monitor Comparitechmonitor input**  
**Switch# ip flow monitor Comparitechmonitor output**

8. Exit configuration mode by entering the following command:

**Switch# exit**

9. Save your settings to finish.

Configure a Cisco Switch for Peace of Mind!

Completing simple tasks like configuring passwords and creating network access lists controls who can access the switch can enable you to stay secure online. Incomplete or incorrect configurations are a vulnerability that attackers can exploit.

Configuring a Cisco switch is only half the battle, you also have to regularly monitor its status. Any performance issues with your switch can have a substantial impact on your users.

Using a network monitoring tool and network analyzer can help you to monitor switches remotely and review performance concerns. Taking the time out of your day to configure a switch and assign strong passwords gives you peace of mind so that you can communicate safely online.

Cisco Switch Configuration & Commands FAQs

How to configure a trunk port on a Cisco 2960 switch?



To configure a trunk port on a Cisco 2960 switch:

1. Enter configuration mode:

```
configure terminal
```

2. Specify the port to use:

```
interface <interface-id>
```

3. Configure the port as a Layer 2 trunk:

```
switchport mode {dynamic {auto | desirable} | trunk}
```

These options mean:

- **dynamic auto** – The Default. Creates a trunk link if the neighboring interface is set to trunk or desirable mode.
- **dynamic desirable** – Creates a trunk link if the neighboring interface is set to trunk, desirable, or auto mode.
- **trunk** – Sets the interface in permanent trunking mode.

4. Specify a default VLAN to use for back up. This is optional:

```
switchport access vlan <vlan-id>
```

5. Specify the native VLAN:

```
switchport trunk native vlan <vlan-id>
```

6. Exit the config mode:

```
end
```

Set a static IP on a Cisco switch

A problem with the GUI interface of Cisco switches makes it impossible to assign a static IP address to an interface. Follow these steps for a workaround:

1. Create a text file on your PC. It doesn't matter where you save it or what you call it, but make sure you remember where it is. Substitute real values for the tokens shown in angle brackets (<>) below. The text in the file should be:

```
Config t
Interface <VLAN ID>
No ip address DHCP
Y
No ip address <old IP address>
IP address <new IP address> <subnet mask>
Exit
IP default-gateway <gateway IP address>
```

2. Access the admin menu of the switch for Switch Management.

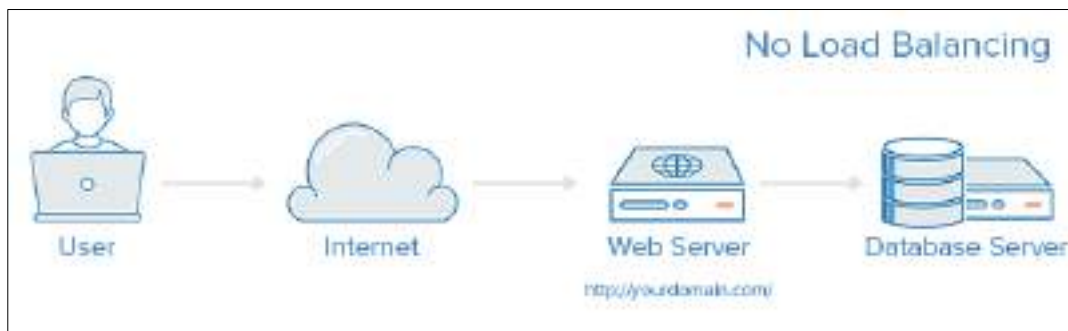
3. In the menu, click on Administration, then File Management, and then select File Operations.
4. In the File Operations screen, set the following:
  - Operation Type: Update File
  - Destination File Type: Running Configuration
  - Copy Method: HTTP/HTTPS
  - File Name: (Browse to select the file you created on your PC).
5. Click on Apply.

These steps will create a static IP address, which you can check by going from the main menu to IP Configuration > IPv4 Interface.

## Load Balancing

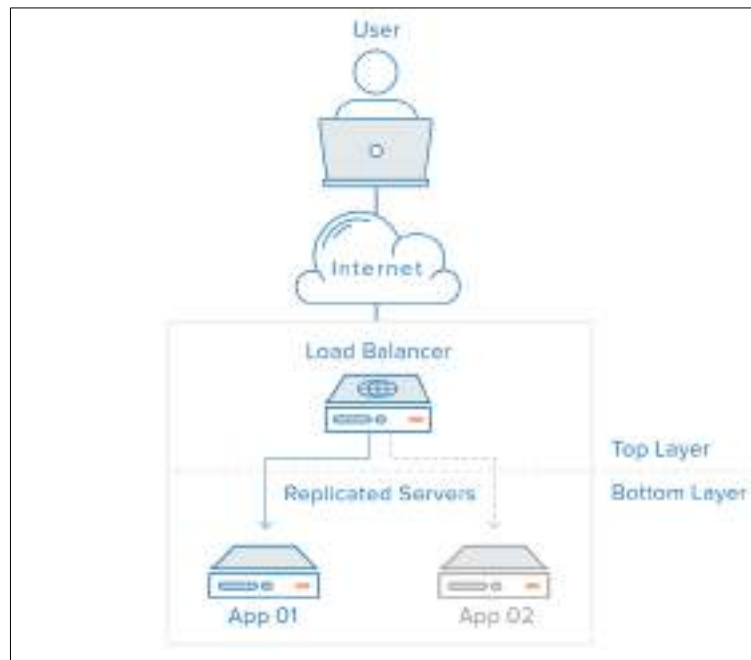
Load balancing is a key component of highly-available infrastructures commonly used to improve the performance and reliability of web sites, applications, databases and other services by distributing the workload across multiple servers.

A web infrastructure with no load balancing might look something like the following:



In this example, the user connects directly to the web server, at [yourdomain.com](http://yourdomain.com). If this single web server goes down, the user will no longer be able to access the website. In addition, if many users try to access the server simultaneously and it is unable to handle the load, they may experience slow load times or may be unable to connect at all.

This single point of failure can be mitigated by introducing a load balancer and at least one additional web server on the backend. Typically, all of the backend servers will supply identical content so that users receive consistent content regardless of which server responds.



In the example illustrated above, the user accesses the load balancer, which forwards the user's request to a backend server, which then responds directly to the user's request. In this scenario, the single point of failure is now the load balancer itself. This can be mitigated by introducing a second load balancer, but before we discuss that, let's explore how load balancers work.

### What kind of traffic can load balancers handle?

Load balancer administrators create forwarding rules for four main types of traffic:

- **HTTP** — Standard HTTP balancing directs requests based on standard HTTP mechanisms. The Load Balancer sets the X-Forwarded-For, X-Forwarded-Proto, and X-Forwarded-Port headers to give the backends information about the original request.
- **HTTPS** — HTTPS balancing functions the same as HTTP balancing, with the addition of encryption. Encryption is handled in one of two ways: either with SSL passthrough which maintains encryption all the way to the backend or with SSL termination which places the decryption burden on the load balancer but sends the traffic unencrypted to the back end.
- **TCP** — For applications that do not use HTTP or HTTPS, TCP traffic can also be balanced. For example, traffic to a database cluster could be spread across all of the servers.
- **UDP** — More recently, some load balancers have added support for load balancing core internet protocols like DNS and syslogd that use UDP.

These forwarding rules will define the protocol and port on the load balancer itself and map them to the protocol and port the load balancer will use to route the traffic to on the backend.

Load balancers choose which server to forward a request to based on a combination of two factors. They will first ensure that any server they can choose is actually responding appropriately to requests and then use a pre-configured rule to select from among that healthy pool.

### Health Checks

Load balancers should only forward traffic to “healthy” backend servers. To monitor the health of a backend server, health checks regularly attempt to connect to backend servers using the protocol and port defined by the forwarding rules to ensure that servers are listening. If a server fails a health check, and therefore is unable to serve requests, it is automatically removed from the pool, and traffic will not be forwarded to it until it responds to the health checks again.

### Load Balancing Algorithms

The load balancing algorithm that is used determines which of the healthy servers on the backend will be selected. A few of the commonly used algorithms are:

**Round Robin** — Round Robin means servers will be selected sequentially. The load balancer will select the first server on its list for the first request, then move down the list in order, starting over at the top when it reaches the end.

**Least Connections** — Least Connections means the load balancer will select the server with the least connections and is recommended when traffic results in longer sessions.

**Source** — With the Source algorithm, the load balancer will select which server to use based on a hash of the source IP of the request, such as the visitor’s IP address. This method ensures that a particular user will consistently connect to the same server.

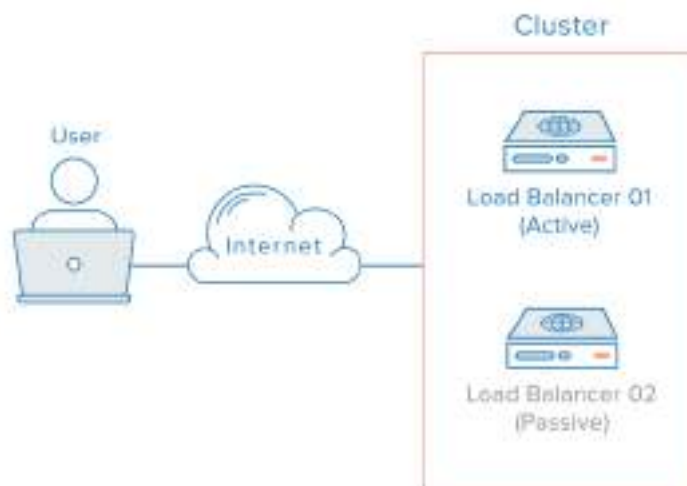
The algorithms available to administrators vary depending on the specific load balancing technology in use.

How do load balancers handle state?

Some applications require that a user continues to connect to the same backend server. A Source algorithm creates an affinity based on client IP information. Another way to achieve this at the web application level is through **sticky sessions**, where the load balancer sets a cookie and all of the requests from that session are directed to the same physical server.

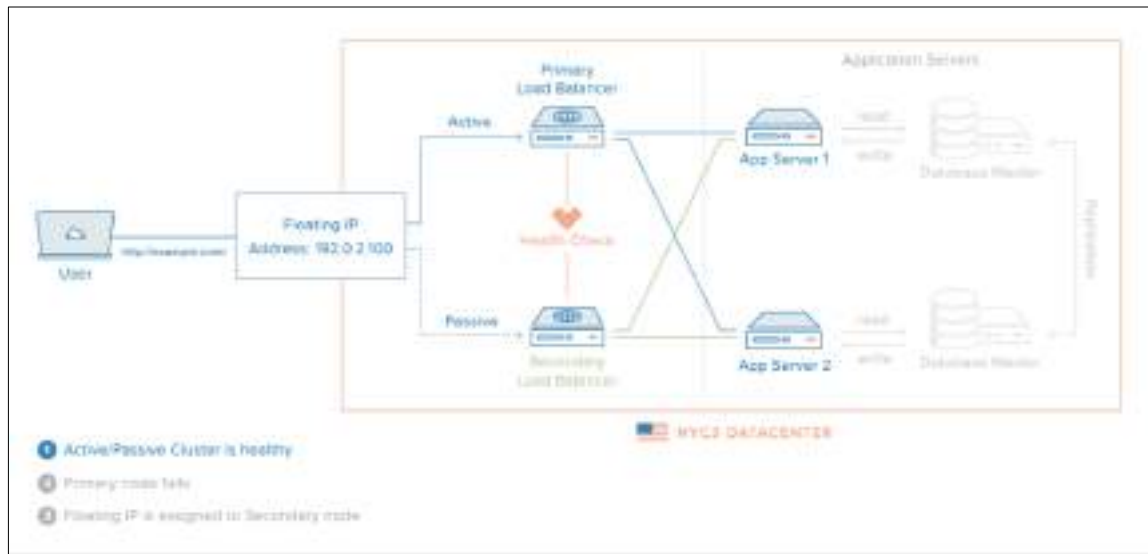
### Redundant Load Balancers

To remove the load balancer as a single point of failure, a second load balancer can be connected to the first to form a cluster, where each one monitors the others’ health. Each one is equally capable of failure detection and recovery.



In the event the main load balancer fails, DNS must take users to the to the second load balancer. Because DNS changes can take a considerable amount of time to be propagated on the Internet and to make this failover automatic, many administrators will use systems that allow for flexible IP address remapping, such as Reserved IPs. On demand IP address remapping eliminates the propagation and caching issues inherent in DNS changes by providing a static IP address that can be easily remapped when needed. The domain name can remain associated with the same IP address, while the IP address itself is moved between servers.

This is how a highly available infrastructure using Reserved IPs might look:



Hardening network devices reduces the risk of unauthorized access into a network's infrastructure. Vulnerabilities in device management and configurations present weaknesses for a malicious cyber actor to exploit in order to gain presence and maintain persistence within a network

#### Harden Network Devices

A fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. Government agencies, organizations, and vendors supply a wide range of guidance to administrators—including benchmarks and best practices—on how to harden network devices. Administrators should implement the following recommendations in conjunction with laws, regulations, site security policies, standards, and industry best practices.

#### To harden network devices you have to follow

- Disable unencrypted remote admin protocols used to manage network infrastructure (e.g., Telnet, File Transfer Protocol [FTP]).
- Disable unnecessary services (e.g., discovery protocols, source routing, Hypertext Transfer Protocol [HTTP], Simple Network Management Protocol [SNMP], Bootstrap Protocol).
- Use SNMPv3 (or subsequent version), but do not use SNMP community strings.
- Secure access to the console, auxiliary, and virtual terminal lines.
- Implement robust password policies, and use the strongest password encryption available.
- Protect routers and switches by controlling access lists for remote administration.
- Restrict physical access to routers and switches.
- Back up configurations and store them offline. Use the latest version of the network device operating system and keep it updated with all patches.
- Periodically test security configurations against security requirements.
- Protect configuration files with encryption or access controls when sending, storing, and backing up files.

#### IP Configuration: Configure IP Address and Network Settings

Companies with advanced network configurations can configure multiple IP addresses on the B Series Appliance's ethernet ports. Using multiple ports can enhance security or enable connections over non-standard networks. For example, if employees are restricted from accessing the internet but need to provide off-network support, using one port for your internal private network and another for the public internet allows users worldwide to access systems without breaching your network security policies.

NIC teaming combines your system's physical network interface controllers (NICs) into a single logical interface. NIC teaming operates in "Active-Backup" mode. One of the NICs is used to carry all network traffic. If the link on that NIC is lost for any reason, the other NIC becomes active. Before activating NIC teaming, please ensure that both NICs are connected to the same network segment (subnet) and that you have IP addresses configured on only one of the existing NICs.

Although multiple IP addresses can be assigned to each NIC, do not configure either NIC such that it has an IP address that is in the same subnet as an IP address on the other NIC. In this scenario, packet loss occurs with packets originating from the IP on the NIC that does not have the default gateway. Consider the following example configuration:

- eth0 is configured with the default gateway of 192.168.1.1
- eth0 is assigned with 192.168.1.5
- eth1 is assigned with 192.168.1.10
- Both eth0 and eth1 are connected to the same subnet switch

Given this configuration, traffic from both NICs are sent to the default gateway (192.168.1.1) regardless of which NIC received traffic. Switches configured with dynamic ARP send packets randomly to either eth0 (192.168.1.5) or eth1 (192.168.1.10), not both. When eth0 receives these packets from the switch destined for eth1, eth0 drops the packets. Some switches are configured with static ARP. These switches drop all packets received from eth1 since this NIC does not have the default gateway and is not present in the static ARP table of the gateway. If you wish to configure redundant NICs on the same subnet, use NIC teaming.

By default, Dynamic Host Configuration Protocol (DHCP) is enabled for your B Series Appliance. DHCP is a network protocol that uses a DHCP server to control the distribution of network parameters, such as IP addresses, allowing systems to automatically request these parameters. This reduces the need to manually configure settings. In this case,



when checked, an IP address is obtained from the DHCP server and is removed from the pool of available IP addresses.

Click **Show Details** to view and verify transmission and reception statistics for each ethernet port on the B Series Appliance.



Under the Global Network Configuration section, configure the hostname.

Assign a default gateway, selecting which ethernet port to use. Enter an IP address for one or more DNS servers. If DHCP is enabled, the DHCP lease provides you with a default gateway as well as a listing of DNS servers in order of preference. Any statically configured DNS servers listed in the Custom DNS Servers field are attempted to be reached first, followed by DNS servers received from DHCP. In the event that these local DNS servers are unavailable, the Fallback to OpenDNS Servers option enables the B Series Appliance to use publicly available DNS servers from OpenDNS.

Allow your B Series Appliance to respond to pings if you wish to be able to test if the host is functioning. Set the hostname or IP address for a Network Time Protocol (NTP) server with



which you wish your B Series Appliance to synchronize.

Two settings are available in the Port Number Settings area: Server Listen Ports and Default URL Ports. When configuring these, keep in mind that connections made to valid ports may be rejected by network restrictions set in /appliance > Security > Appliance Administration and in /login > Management > Security. The opposite is also true: connections made to invalid ports are rejected even if such connections satisfy network restrictions.

The Server Listen Ports section allows you to configure ports for the B Series Appliance to listen on. You may specify up to 15 comma-separated ports for HTTP and 15 comma-separated ports for HTTPS. Each port may appear only once in any field, and it may appear in only one field, not both. The B Series Appliance responds to HTTP connections made to any of the ports listed in the HTTP field, and the B Series Appliance responds to HTTPS connections made to any of the ports in the HTTPS field. You cannot change the built-in listen ports (80 and 443).

To access the B Series Appliance on a given port using a browser requires that you enter the port in the URL of the browser (e.g., support.example.com:8200). Clients downloaded from the B Series Appliance attempt connections to the ports listed on the /login > Status > Information page under Client Software Is Built to Attempt. These ports are not configurable from /login or /appliance.

Default URL Ports are used when generating URLs that point back to the B Series Appliance, such as session keys generated from the representative console. When the default ports are blocked on the network (or can be expected to fail for any other reason), you can change the default URL ports to have generated URLs spawn with the ports that you specify. Whatever

The screenshot shows a web-based configuration page for an IP address. The title bar reads "IP :: Edit 10.10.28.250". The form contains the following elements: an "Enabled" checkbox which is checked; a "Network Port" dropdown menu set to "eth0"; an "IP Address" text input field containing "10.10.28.250"; a "Subnet Mask" text input field containing "255.255.252.0"; a "Primary" checkbox which is unchecked; an "Access Type" dropdown menu set to "Allow Both"; and a "Save Changes" button. Below the form is a "Delete" button and a warning message: "WARNING: Changes to the network settings should be made ONLY when the device is not in use by other users!".

ports you enter should also be listed in the Server Listen Ports; otherwise, the default ports are not connected. For example, if you enter 8080 in the Default URL Port field, make sure 8080 is also in the HTTP or HTTPS Listen Port field. Unlike the listen port fields, you cannot enter more than one port in either of the URL port fields. You cannot enter the same port in both fields.

When adding or editing an IP address, choose whether that IP should be enabled or disabled. Select the network port on which you would like this IP to function. The IP Address field sets an address to which your B Series Appliance can respond, while Subnet Mask enables to communicate with other devices.

When editing an IP address that is on the same subnet as another IP address for this B Series Appliance, choose if this IP address should be Primary. When this box is checked, the B Series Appliance designates this IP address to be the primary or originating IP address for the subnet. This helps, for example, to ensure that any network traffic originating from the B Series Appliance on that subnet matches and complies with defined firewall rules.



From Access Type, you can restrict access over this IP to the public site or customer client. Use Allow Both to allow access for both the public site and customer client.

### **Network Intrusion Detection System (NIDS)**

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

### **Classification of Intrusion Detection System:**

**IDS are classified into 5 types:**

#### **Network Intrusion Detection System (NIDS):**

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

#### **Host Intrusion Detection System (HIDS):**

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

#### **Protocol-based Intrusion Detection System (PIDS):**

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

#### **Application Protocol-based Intrusion Detection System (APIDS):**

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would

monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

### **Hybrid Intrusion Detection System :**

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

### **Detection Method of IDS:**

#### **Signature-based Method:**

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

### **Anomaly-based Method:**

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

### **Comparison of IDS with Firewalls:**

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

### **Cryptography**

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

### **Cryptography techniques**

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

### **Modern cryptography concerns itself with the following four objectives:**

**Confidentiality.** The information cannot be understood by anyone for whom it was unintended.

**Integrity.** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

**Non-repudiation.** The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.

**Authentication.** The sender and receiver can confirm each other's identity and the origin/destination of the information.

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems and not discussing sensitive procedures with outsiders.

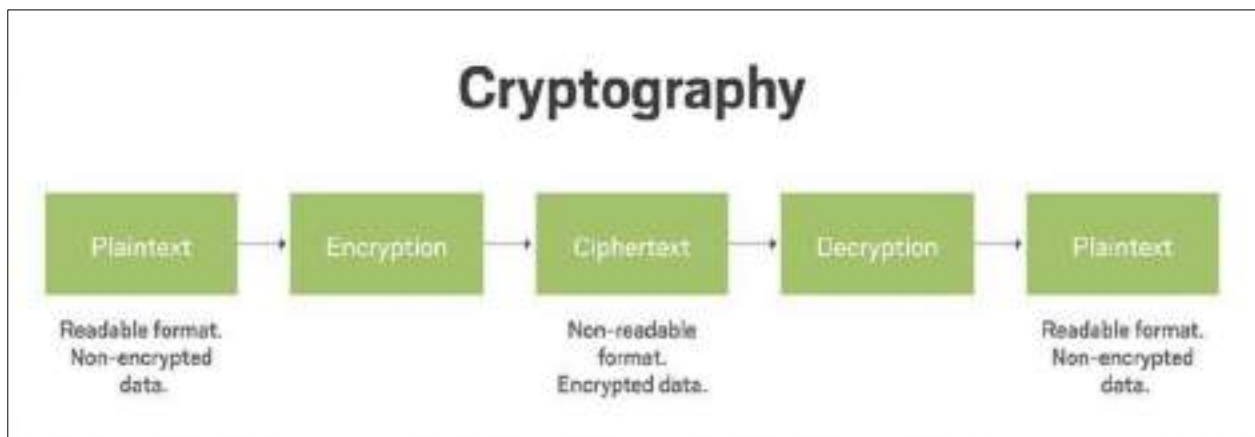


Image displaying cryptography steps and functions.

Cryptography is the process of encrypting and decrypting data.

Cryptographic algorithms

Cryptosystems use a set of procedures known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices and applications.

A cipher suite uses one algorithm for encryption, another algorithm for message authentication and another for key exchange. This process, embedded in protocols and written in software that runs on operating systems (OSes) and networked computer systems, involves:

- public and private key generation for data encryption/decryption
- digital signing and verification for message authentication
- key exchange

#### **Individual Activity:**

- *Identify Network Devices.*
- *Perform subnetting.*



### **Self-check quiz 3.1**

Check your understanding by answering the following questions:

Write the correct answer for the following questions.

1. What is Network Audit?

2. When Do You Need a Network Audit?

3. What is Firewall?

4. Write down the steps of firewall configuration.

Answer:

5. What kind of traffic can load balancers handle?



### Learning outcome 3.2 - Carry out Server and device security control



Contents:

- Device hardening procedure.
- Analyzing Logs.
- Identity and access management configurations.
- Password management.
- Host and network based intruders
- File and service auditing.



Assessment criteria:

1. Device hardening is performed for server.
2. Logs are analyzed as per standard procedure.
3. Identity and access management configurations are audited following standard procedure.
4. Password management is checked and performed following client's requirements.
5. Host and network based intruders are detected and prevented following standard procedure.
6. File and service auditing are performed following standard procedure.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (Actual or simulated), Server, Necessary software.



### **LEARNING ACTIVITY 3.2**

Learning Activity	Resources/Special Instructions/References
Carry out Server and device security control	<ul style="list-style-type: none"> <li>▪ Information Sheets: 3.2</li> <li>▪ Self-Check: 3.2</li> <li>▪ Answer Key: 3.2</li> </ul>



## Information sheet 3.2

Learning objective: to identify the types of garments.

### **System Hardening**

System hardening is the process of securing a server or computer system by minimizing its attack surface, or surface of vulnerability, and potential attack vectors. It's a form of cyberattack protection that involves closing system loopholes that cyberattackers frequently use to exploit the system and gain access to users' sensitive data.

One official definition of system hardening, according to the National Institute of Standards and Technology (NIST), is that it's "a process intended to eliminate a means of attack by patching vulnerabilities and turning off non-essential services."

Part of the system hardening elimination process involves deleting or disabling needless system applications, permissions, ports, user accounts, and other features so that attackers have fewer opportunities to gain access to a mission-critical or critical-infrastructure computer system's sensitive information.

But at its core, system hardening is a method for protecting a system against attacks perpetrated by cybercriminals. It involves securing a computer system's software mainly but also its firmware and other system elements to reduce vulnerabilities and a potential compromise of the entire system.

Now you know why system hardening exists, but you might be wondering about its practical purpose and why businesses and organizations implement system hardening practices.

The basic purpose of implementing system hardening techniques and practices is to simply minimize the number of potential entryways an attacker could use to access your system and to do so from inception. This is oftentimes referred to as following a secure-by-design philosophy.

### **Types of system hardening**

System hardening involves securing not only a computer's software applications, including the operating system, but also its firmware, databases, networks, and other critical elements of a given computer system that an attacker could exploit.

#### **There are five main types of system hardening:**

1. Server hardening
2. Software application hardening
3. Operating system hardening
4. Database hardening
5. Network hardening

It's important to note that the types of system hardening are broad enough to be universal and translate well across different server and computer system configurations; however, the methods and tools used to practically achieve a hardened or secure-by-design state vary widely.

But for now, let's review the purpose of each type of system hardening.

## Server hardening

Server hardening is a general system hardening process that involves securing the data, ports, components, functions, and permissions of a server using advanced security measures at the hardware, firmware, and software layers.

### **These general server security measures include, but are not limited to:**

Keeping a server's operating system patched and updated

Regularly updating third-party software essential to the operation of the server and removing third-party software that doesn't conform to established cybersecurity standards

Using strong and more complex passwords and developing strong password policies for users

Locking user accounts if a certain number of failed login attempts are registered and removing needless accounts

Disabling USB ports at boot

### **Implementing multi-factor authentication**

Using self-encrypting drives or AES encryption to conceal and protect sensitive information

Using firmware resilience technology, memory encryption, antivirus and firewall protection, and advanced cybersecurity suites specific to your operating system, such as Titanium Linux

### **Software application hardening**

Software application hardening, or just application hardening, involves updating or implementing additional security measures to protect both standard and third-party applications installed on your server.

Unlike server hardening, which focuses more broadly on securing the entire server system by design, application hardening focuses on the server's applications, specifically, including, for example, a spreadsheet program, a web browser, or a custom software application used for a variety of reasons.

At a basic level, application hardening involves updating existing or implementing new application code to further secure a server and implementing additional software-based security measures.

### **Examples of application hardening include, but are not limited to:**

- Patching standard and third-party applications automatically
- Using firewalls
- Using antivirus, malware, and spyware protection applications
- Using software-based data encryption
- Using CPUs that support Intel Software Guard Extensions (SGX)
- Using an application like LastPass to manage and encrypt passwords for improved password storage, organization, and safekeeping
- Establishing an intrusion prevention system (IPS) or intrusion detection system (IDS)

### **Database hardening**



Database hardening involves securing both the contents of a digital database and the database management system (DBMS), which is the database application users interact with to store and analyze information within a database.

Database hardening mainly involves three processes:

1. Controlling for and limiting user privileges and access
2. Disabling unnecessary database services and functions
3. Securing or encrypting database information and resources

**Types of database hardening techniques include:**

- Restricting administrators and administrative privileges and functions
- Encrypting in-transit and at-rest database information
- Adhering to a role-based access control (RBAC) policy
- Regularly updating and patching database software, or the DBMS
- Turning off needless database services and functions
- Locking database accounts if suspicious login activity is detected
- Enforcing strong and more complex database passwords

### **Network hardening**

Network hardening involves securing the basic communication infrastructure of multiple servers and computer systems operating within a given network.

Two of the main ways that network hardening is achieved are through establishing an intrusion prevention system or intrusion detection system, which are usually software-based. These applications automatically monitor and report suspicious activity in a given network and help administrators prevent unauthorized access to the network.

Network hardening techniques include properly configuring and securing network firewalls, auditing network rules and network access privileges, disabling certain network protocols and unused or unnecessary network ports, encrypting network traffic, and disabling network services and devices not currently in use or never in use.

Using these techniques in combination with an intrusion prevention or intrusion detection system reduces the network's overall attack surface, and thus, bolsters its resistance to network-based attacks.

### **harden my system**

System hardening is a dynamic and variable process. One of the best ways to begin or expand upon the system hardening process is to follow a system hardening checklist or a system hardening standard, such as those published by the NIST or CIS Center.

Generally, how you harden your system depends on your server's configuration, operating system, software applications, hardware, among other variables.

The system hardening standards and guidelines published by the NIST and CIS Center for Internet Security, for example, discuss system hardening techniques specific to Microsoft Windows, Unix, and Linux.

So, if you're curious about how to begin the system hardening process, reading the NIST's Special Publication 800-123 and the CIS Center for Internet Security's free benchmark PDFs is

a good place to start. You can then, if necessary, consult with an experienced cybersecurity professional on how to move forward with implementing these standards' recommended processes and best practices within your business or organization.

There are some common and transferrable system hardening practices of which you should be aware, however. We've put a few best practices in the checklist below.

**A good system hardening checklist usually contains the following action items:**

1. Have users create strong passwords and change them regularly
2. Remove or disable all superfluous drivers, services, and software
3. Set system updates to install automatically
4. Limit unauthorized or unauthenticated user access to the system
5. Document all errors, warnings, and suspicious activity

Log analysis is the process of reviewing computer-generated event logs to proactively identify bugs, security threats, factors affecting system or application performance, or other risks. Log analysis can also be used more broadly to ensure compliance with regulations or review user behavior.

A log is a comprehensive file that captures activity within the operating system, software applications or devices. Logs automatically document any information designated by the system administrators, including: messages, error reports, file requests, file transfers and sign-in/out requests. The activity is also time-stamped, which helps IT professionals and developers establish an audit trail in the event of a system failure, breach or other outlying event.

**Why Is Log Analysis Important?**

In some cases, log analysis is critical for compliance since organizations must adhere to specific regulations that dictate how data is archived and analyzed. It can also help predict the useful lifespan of hardware and software. In addition, log analysis can help IT teams amplify four key factors that help deliver greater business value and customer-centric solutions: agility, efficiency, resilience and customer value.

Log analysis can unlock many additional benefits for the business. These include:

**Improved Troubleshooting**

Organizations that regularly review and analyze logs are typically able to identify errors more quickly. With an advanced log analysis tool, the business may even be able to pinpoint problems before they occur, which greatly reduces the time and cost of remediation.

Logs also help the log analyzer review the events leading up to the error, which may make the issue easier to troubleshoot and prevent in the future.

**Enhanced Cybersecurity**

Effective log analysis dramatically strengthens the organization's cybersecurity capabilities. Regular review and analysis of logs helps organizations more quickly detect anomalies, contain threats and prioritize responses.

**Improved Customer Experience**

Log analysis helps businesses ensure that all customer-facing applications and tools are fully operational and secure. The consistent and proactive review of log events helps the organization quickly identify disruptions or even prevent such issues — improving satisfaction and reducing turnover.

### **Agility:**

Organizations can predict the useful life span of hardware and software and help businesses prepare for scale and agility, thus providing a competitive edge in the marketplace.

Log analysis is typically done within a log management system, a software solution that gathers, sorts and stores log data and event logs from a variety of sources.

Log management platforms allow the IT team and security professionals to establish a single point from which to access all relevant endpoint, network and application data. Typically, logs are searchable, which means the log analyzer can easily access the data they need to make decisions about network health, resource allocation or security. Traditional log management uses indexing, which can slow down search and analysis. Modern log management uses index-free search; it's less expensive, faster and can create gains of 50-100x in required disk space.

### **Log analysis typically includes:**

**Ingestion:** Installing a log collector to gather data from a variety of sources, including the OS, applications, servers, hosts and each endpoint, across the network infrastructure.

**Centralization:** Aggregating all log data in a single location as well as a standardized format regardless of the log source. This helps simplify the analysis process and increase the speed at which data can be applied throughout the business.

**Search and analysis:** Leveraging a combination of AI/ML-enabled log analytics and human resources to review and analyze known errors, suspicious activity or other anomalies within the system. Given the vast amount of data available within the log, it is important to automate as much of the log analysis process as possible. It is also recommended to create a graphical representation of data, through knowledge graphing or other techniques, to help the IT team visualize each log entry, its timing and interrelations.

**Monitoring and alerts:** The log management system should leverage advanced log analytics to continuously monitor the log for any log event that requires attention or human intervention. The system can be programmed to automatically issue alerts when certain events take place or certain conditions are or are not met.

**Reporting:** Finally, the LMS should provide a streamlined report of all events as well as an intuitive interface that the log analyzer can leverage to get additional information from the log.

### **Log Analysis Methods**

Given the massive amount of data being created in today's digital world, it has become impossible for IT professionals to manually manage and analyze logs across a sprawling tech environment. As such, they require an advanced log management system and techniques that automate key aspects of the data collection, formatting and analysis processes.

These techniques include:

#### **Normalization**

Normalization is a data management technique that ensures all data and attributes, such as IP addresses and timestamps, within the transaction log are formatted in a consistent way.

### **Pattern recognition**

Pattern recognition refers to filtering events based on a pattern book in order to separate routine events from anomalies.

### **Classification and tagging**

Classification and tagging is the process of tagging events with key words and classifying them by group so that similar or related events can be reviewed together.

### **Correlation analysis**

Correlation analysis is a technique that gathers log data from several different sources and reviews the information as a whole using log analytics.

### **Artificial ignorance**

Artificial ignorance refers to the active disregard for entries that are not material to system health or performance.

### **Identity and access management (IAM)**

Identity and access management involve defining controls, both procedural and technical, that show a user's identity and the access level they are granted or denied to the enterprise IT systems. This can cover everything from defining which staff members have admin rights, to what actions should require admin rights – such as downloading new applications to a work desktop, or changing system preferences. It also includes identification factors such as single sign-on (SSO) systems and multi-factor authentication, with privilege access management acting as an overlay to the authentication schemes. The Identity profile data must always be stored securely and can typically be linked to an existing active directory domain.

### **An IAM Security Audit in AWS**

AWS Identity and Access Management (IAM) is a service within AWS' cloud infrastructure that provides access control across all other services within AWS and including IAM itself. IAM allows you to create users, roles and policies that can be assigned to folks within your organisation or other services within AWS to perform specific functions.

Given that IAM essentially acts as the gatekeeper to access control for all AWS resources, it is imperative that the security of IAM itself must be considered when verifying the security of your cloud infrastructure.

### **Step by Step Auditing AWS IAM**

1. Creating the user that will be used to perform the Audit
2. Configuring a profile for the audit
3. Enumerating AWS IAM resource information for the Audit
4. Enumerate IAM Account Password Policy
5. Enumerating IAM user information using a credential report
6. Enumerating groups and policies attached to them
7. Enumerating directly attached policies to users
8. Enumerating roles and the policies attached to them

### **Creating the user that will be used to perform the Audit**

To begin the audit, an AWS IAM user with IAM ReadOnly permissions is required. This can easily be achieved by logging into the AWS console and creating a user. Of course, if you already have a user with administrative privilege, you can use that user to continue, however, it would be a security best practice to create a user for this activity and use it periodically to perform the audit.

**Step 1:** Navigate to <https://console.aws.amazon.com/iamv2/home?#/users> and click on the "Add users" button. Give it a name. We are using the name "iamauditor"

**Add user** 1 2 3 4 5

**Set user details**

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[Add another user](#)

**Select AWS access type**

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type\*  **Access key - Programmatic access**  
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

**Password - AWS Management Console access**  
Enables a password that allows users to sign-in to the AWS Management Console.

**Step 2:** Click “Next: Permissions” to go to the permissions page where we will create an IAM user group and attach the "IAMReadOnlyAccess" permission to the group instead of to the user. The name of the group we are creating is “iamauditors”

**Add user** 1 2 3 4 5

▼ **Set permissions**

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Add user to group**

[Create group](#) [Refresh](#)

Search  Showing 4 results

Group ▼ Attached policies

Click on “Create Group” to create the new group and have it selected in the Add user page.



**Step 3:** Click on “Next: Tags” to add tags to the user being created. Tags allow us to add attributes that can be used to filter and manage properties based on their functions. In this case, we are adding 3 tags “createdBy”, “createdFor” and “createdDate”.

### Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#).

Key	Value (optional)	Remove
<input type="text" value="createdBy"/>	<input type="text" value="rly2"/>	<input type="button" value="✕"/>
<input type="text" value="createdFor"/>	<input type="text" value="Performing IAM Audit"/>	<input type="button" value="✕"/>
<input type="text" value="createdDate"/>	<input type="text" value="14th Jan 2022"/>	<input type="button" value="✕"/>
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 47 more tags.

**Step 4:** The last page offers you a review of the user being created. Click on the “Create user” button to create the user that we will be using for the audit.

## Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

### User details

User name	iamauditor
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

### Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	iamauditors

### Tags

The new user will receive the following tags

Key	Value
createdBy	HYAZ
createdFor	Performing IAM Audit
createdDate	14th Jan 2022

Cancel

Previous

Create user

**Step 5:** Download and save the CSV file containing the user credentials. We will be configuring these credentials on our system next.

Download .csv

User	Access key ID	Secret access key
iamauditor	AKIAQLEO3HKNTJAGE7LSM	***** Show

## Configuring a profile for the audit

In this section we will configure the credentials that we obtained of the new user locally on our system and use AWS CLI commands to perform the audit.

**Step 1:** Skip this step, if you already have the AWS CLI installed. Else download and install the AWS CLI for your operating system from <https://aws.amazon.com/cli/>.

**Step 2:** You can configure a new profile using the following command. Enter the information from the CSV when prompted. We can provide any region (us-east-1 for example) since IAM is a global service.

```
aws configure --profile iamauditor
```

```
kloudle-rnd:$>
kloudle-rnd:$> aws configure --profile iamauditor
AWS Access Key ID [None]: AKIAQLE03KKMJAGE7L5M
AWS Secret Access Key [None]:
Default region name [None]: us-east-1
Default output format [None]: json
kloudle-rnd:$>
```

**Step 3:** Export the profile you just created to the “AWS\_PROFILE” environment variable so that we don't have to specify it every time on the command line. Confirm your account is set up using the following command:

```
export AWS_PROFILE=iamauditor
```

```
aws sts get-caller-identity
```

```
kloudle-rnd:$>
kloudle-rnd:$> export AWS_PROFILE=iamauditor
kloudle-rnd:$>
kloudle-rnd:$> aws sts get-caller-identity
{
  "UserId": "AIDAQLE03KKMCV4AYMBEZ",
  "Account": " ",
  "Arn": "arn:aws:iam:: :user/iamauditor"
}
kloudle-rnd:$>
```

We are now ready to begin the audit.

## Enumerating AWS IAM resource information for the Audit

We need to enumerate information about the following resources:

1. **IAM Account Password Policy**
2. **Users**
3. **User Groups**
4. **Roles**
5. **Policies**

For each of these resources we will perform additional steps to identify and answer security related questions.

## Enumerate IAM Account Password Policy



A password policy enforces users to set up and operate their accounts in adherence to rules that the organization requires. For example, a password policy prevents users from reusing their last 3 passwords.

In the case of AWS IAM, you can use the following command to obtain the current password policy that is enforced

```
aws iam get-account-password-policy
```

```
kloudle-rnd:$> aws iam get-account-password-policy
{
  "PasswordPolicy": {
    "MinimumPasswordLength": 16,
    "RequireSymbols": true,
    "RequireNumbers": false,
    "RequireUppercaseCharacters": true,
    "RequireLowercaseCharacters": true,
    "AllowUsersToChangePassword": false,
    "ExpirePasswords": false,
    "PasswordReusePrevention": 22,
    "HardExpiry": true
  }
}
kloudle-rnd:$>
```

Based on how secure you want the user passwords to be, you can verify if the password policy meets your requirement or not.

If you receive an error (*NoSuchEntity*), it means that the password policy was never created and this audit check can be considered a failure. However, a default AWS password policy does exist which enforces the following conditions on the password:

- **Minimum password length of 8 characters and a maximum length of 128 characters**
- **Minimum of three of the following mix of character types: *uppercase, lowercase, numbers, and ! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } | ' symbols***
- **Not be identical to your AWS account name or email address**

### Enumerating IAM user information using a credential report

AWS IAM provides a pretty neat feature that allows us to create an attribute snapshot of the users within IAM that can be used to answer a multitude of security questions.

**Step 1:** Generate an IAM security credential report using the following commands

```
aws iam generate-credential-report
```

```
kloudle-rnd:~$> aws iam generate-credential-report
{
  "State": "COMPLETE"
}
kloudle-rnd:~$>
```

**Step 2:** Download the credential report after a minute or so of running the previous command. If “State”: “COMPLETE” is printed as shown in the previous screenshot, you can go ahead and run the next command to download the report instead of waiting.

```
aws iam get-credential-report --query "Content" | cut -d '"' -f 2 | base64 -d > iam-credential-report.csv
```

This sequence of commands will take the response from the AWS IAM *get-credential-report* command and extract only the Base64 part and decode it with the help of the *base64* command.

The report is saved in the *iam-credential-report.csv* file.

**Step 3:** Open the file in a text editor like VSCode or since it's a comma separated value file, you can open it in MS Excel or LibreOffice (or equivalent). The screenshot below shows the file in CSV preview mode in Visual Studio Code.

User	Arn	User_creation_time	Password_enabled	Password_last_used	Password_last_changed
root	arn:aws:iam::root	2007-09-23T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs	arn:aws:logs::root	2014-04-06T00:00:00.000Z	False		
aws-logs-2018-01	arn:aws:logs::root:aws-logs-2018-01	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-02	arn:aws:logs::root:aws-logs-2018-02	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-03	arn:aws:logs::root:aws-logs-2018-03	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-04	arn:aws:logs::root:aws-logs-2018-04	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-05	arn:aws:logs::root:aws-logs-2018-05	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-06	arn:aws:logs::root:aws-logs-2018-06	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-07	arn:aws:logs::root:aws-logs-2018-07	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-08	arn:aws:logs::root:aws-logs-2018-08	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-09	arn:aws:logs::root:aws-logs-2018-09	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-10	arn:aws:logs::root:aws-logs-2018-10	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-11	arn:aws:logs::root:aws-logs-2018-11	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2018-12	arn:aws:logs::root:aws-logs-2018-12	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-01	arn:aws:logs::root:aws-logs-2019-01	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-02	arn:aws:logs::root:aws-logs-2019-02	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-03	arn:aws:logs::root:aws-logs-2019-03	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-04	arn:aws:logs::root:aws-logs-2019-04	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-05	arn:aws:logs::root:aws-logs-2019-05	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-06	arn:aws:logs::root:aws-logs-2019-06	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-07	arn:aws:logs::root:aws-logs-2019-07	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-08	arn:aws:logs::root:aws-logs-2019-08	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-09	arn:aws:logs::root:aws-logs-2019-09	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-10	arn:aws:logs::root:aws-logs-2019-10	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-11	arn:aws:logs::root:aws-logs-2019-11	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2019-12	arn:aws:logs::root:aws-logs-2019-12	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-01	arn:aws:logs::root:aws-logs-2020-01	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-02	arn:aws:logs::root:aws-logs-2020-02	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-03	arn:aws:logs::root:aws-logs-2020-03	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-04	arn:aws:logs::root:aws-logs-2020-04	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-05	arn:aws:logs::root:aws-logs-2020-05	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-06	arn:aws:logs::root:aws-logs-2020-06	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-07	arn:aws:logs::root:aws-logs-2020-07	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-08	arn:aws:logs::root:aws-logs-2020-08	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-09	arn:aws:logs::root:aws-logs-2020-09	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-10	arn:aws:logs::root:aws-logs-2020-10	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-11	arn:aws:logs::root:aws-logs-2020-11	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z
aws-logs-2020-12	arn:aws:logs::root:aws-logs-2020-12	2017-04-06T00:00:00.000Z	True	2020-11-11T00:00:00.000Z	2020-11-11T00:00:00.000Z

**Step 4:** Using the credential report, answer the following set of questions for your AWS account:

1. Do you know all the users that are listed in the report? Are there any unfamiliar users?
2. Are there any users whose password is enabled AND the password last used value is over 90 days? Why does a user exist who has not logged into AWS in the last 90 days? Is this user required?
3. Are there any users whose password is enabled AND the password last changed value is over 90 days? Why hasn't this user rotated their password as a security best practice?
4. Are there any users whose password is enabled AND who do not have 2 factor authentication enabled? The value for the "Mfa\_active" column will be False for these users.

5. Are there any users who have Access keys? The columns “Access\_key\_1\_active” or “Access\_key\_2\_active” will be True. In case both the columns are True, then the user has 2 active Access Keys. Are there any such users with both keys active? Why?
6. Which users have not used their Access Key in the last 90 days? This can be obtained from the values of the “Access\_key\_1\_last\_user\_date” and “Access\_key\_2\_last\_user\_date” columns.
7. Which users have not rotated their Active key in the last 90 days? This can be obtained from the values of the “Access\_key\_1\_last\_rotated” and “Access\_key\_1\_last\_rotated” columns.

The answers to these questions will enable you to remove unnecessary users and unused keys from your AWS IAM thereby reducing your attack footprint.

### Enumerating groups and policies attached to them

As we saw while creating a new user, it is recommended to add a user to a group and assign the group the permissions you want the user to have. In this section, we will enumerate the various user groups within IAM, identify what users are present in each group and check what effective permissions the users have because of policies attached to the group.

**Step 1:** Run the following command to get a list of groups:

aws iam list-groups

```
kloudle-rnd:~$
kloudle-rnd:~$ aws iam list-groups
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "admins",
      "GroupId": "AGPAQLE03K0MCFD3BPTU5",
      "CreateDate": "2020-08-08T00:00:00Z",
      "LastModifiedDate": "2020-08-08T00:00:00Z"
    },
    {
      "Path": "/",
      "GroupName": "dev",
      "GroupId": "AGPAQLE03K0M0303TFRW",
      "CreateDate": "2020-08-08T00:00:00Z",
      "LastModifiedDate": "2020-08-08T00:00:00Z"
    },
    {
      "Path": "/",
      "GroupName": "dev_read_only",
      "GroupId": "AGPAQLE03K0MLFB7XNEK6",
      "CreateDate": "2020-08-08T00:00:00Z",
      "LastModifiedDate": "2020-08-08T00:00:00Z"
    },
    {
      "Path": "/",
      "GroupName": "iamauditors",
      "GroupId": "AGPAQLE03K0M1KK563SNF",
      "CreateDate": "2020-08-08T00:00:00Z",
      "LastModifiedDate": "2020-08-08T00:00:00Z"
    },
    {
      "Path": "/",
      "GroupName": "root",
      "GroupId": "AGPAQLE03K0M9U2D4QBE7",
      "CreateDate": "2020-08-08T00:00:00Z",
      "LastModifiedDate": "2020-08-08T00:00:00Z"
    }
  ]
}
```

Do you recognise all of the groups listed in the output of the above command? Are all of them required and relevant to your business?

**Step 2:** For each of the groups, enumerate the policies that are attached to the group. Three kinds of policies can be attached to a group (and to a user directly) - AWS Managed Policies, Customer Managed Policies and an Inline Policy. The following commands will list Inline policies and Managed (AWS and Customer) policies that are attached to the group:

```
aws iam list-group-policies --group-name <groupname>
```

```
aws iam list-attached-group-policies --group-name <groupname>
```

```
kloudle-rnd:$>
kloudle-rnd:$> aws iam list-group-policies --group-name dev
{
  "PolicyNames": [
    "dev_custom_policy"
  ]
}
kloudle-rnd:$>
kloudle-rnd:$> aws iam list-attached-group-policies --group-name dev
{
  "AttachedPolicies": [
    {
      "PolicyName": "ReadOnlyAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/ReadOnlyAccess"
    },
    {
      "PolicyName": "PowerUserAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/PowerUserAccess"
    }
  ]
}
kloudle-rnd:$>
```

**Step 3:** For each user, obtain a list of the groups that the user belongs to. Run the following commands to fetch a list of all users and the next command to get all the groups to which the provided user belongs:

```
aws iam list-users --query "Users[].UserName"
```

```
aws iam list-groups-for-user --user-name <username-here>
```

```

kcloudle-rnd:~$ aws iam list-groups-for-user --user-name just-a-test-user
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "ec2fullcontrol",
      "GroupId": "AGPAOLE03KKMCKXT4EFT0",
      "CreateDate": "2021-10-26T20:14:39+00:00",
      "LastModifiedDate": "2021-10-26T20:14:39+00:00"
    },
    {
      "Path": "/",
      "GroupName": "dev",
      "GroupId": "AGPAOLE03KKM0303TFRMM",
      "CreateDate": "2021-10-26T20:14:39+00:00",
      "LastModifiedDate": "2021-10-26T20:14:39+00:00"
    }
  ]
}
kcloudle-rnd:~$

```

Now that we have users, the groups that they belong to and the policies attached to those groups, we can expand the policies and examine them if any of them give extra privileges to the groups and indirectly to the user within those groups.

**Step 4:** Run the following command to fetch the actual policy definition by providing the policy name in the command. The policy names were obtained from Step 2.

**Step 4.1:** For AWS and Customer Managed Policies that have been created, obtain the attached policy ARN and the policy version number.

```
aws iam list-attached-group-policies --group-name <groupname>
```

```
aws iam get-policy --policy-arn <policy-arn>
```

```

kcloudle-rnd:~$ aws iam list-attached-group-policies --group-name dev
{
  "AttachedPolicies": [
    {
      "PolicyName": "ReadOnlyAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/ReadOnlyAccess"
    },
    {
      "PolicyName": "PowerUserAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/PowerUserAccess"
    }
  ]
}
kcloudle-rnd:~$ aws iam get-policy --policy-arn "arn:aws:iam::aws:policy/ReadOnlyAccess"
{
  "Policy": {
    "PolicyName": "ReadOnlyAccess",
    "PolicyId": "AMPRIILL3WAF5B6DC0VYQ",
    "Arn": "arn:aws:iam::aws:policy/ReadOnlyAccess",
    "Path": "/",
    "DefaultVersionId": "v012",
    "AttachmentCount": 6,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "Description": "Provides read-only access to AWS services and resources.",
    "CreateDate": "2015-02-06T18:39:48+00:00",
    "UpdateDate": "2021-10-26T20:14:39+00:00",
    "Tags": []
  }
}
kcloudle-rnd:~$

```

Next, obtain the policy document using the version number and the `get-policy-version` IAM command.

```
aws iam get-policy-version --policy-arn <policy-arn> --version-id <version>
```

```
kloudle-rnd:~$ aws iam get-policy-version --policy-arn "arn:aws:iam::aws:policy/ReadOnlyAccess" --version-id v82
{
  "PolicyVersion": {
    "Document": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": [
            "a4b:Get*",
            "a4b:List*",
            "a4b:Search*",
            "access-analyzer:GetAccessPreview",
            "access-analyzer:GetAnalyzedResource",
            "access-analyzer:GetAnalyzer",
            "access-analyzer:GetArchiveRule",
            "access-analyzer:GetFinding",
            "access-analyzer:GetGeneratedPolicy",
            "access-analyzer:ListAccessPreviewFindings",
            "access-analyzer:ListAccessPreviews",
            "access-analyzer:ListAnalyzedResources",
            "access-analyzer:ListAnalyzers",
            "access-analyzer:ListArchiveRules",
            "access-analyzer:ListFindings",
            "access-analyzer:ListPolicyGenerations",
            "access-analyzer:ListTagsForResource",
            "access-analyzer:ValidatePolicy",

```

Review the *Action* and *Resource* section of the policy to determine privileges and identify if any of the policies are overprivileged.

**Step 4.2:** For inline policies, you can use the following command

```
aws iam get-group-policy --group-name <groupname> --policy-name <custom-policy-name>
```

```
kloudle-rnd:~$ aws iam get-group-policy --group-name dev --policy-name dev_custom_policy
{
  "GroupName": "dev",
  "PolicyName": "dev_custom_policy",
  "PolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
          "iam:CreateInstanceProfile",
          "iam:UntagRole",
          "iam:PutRolePermissionsBoundary",
          "iam:TagRole",
          "iam:RemoveRoleFromInstanceProfile",
          "iam:CreateRole",
          "iam:TagMFADevice",
          "iam:AttachRolePolicy",
          "iam:CreateVirtualMFADevice",
          "iam:PutRolePolicy",
          "iam:TagSAMLProvider",
          "iam:CreateAccessKey",
          "iam:PassRole",
          "iam:DetachRolePolicy",
          "iam>DeleteRolePolicy",
          "iam:EnableMFADevice",

```

Verify the Action and Resource section of the policy and identify any untoward extraneous permissions.

Based on the group that these policies are attached to, verify if these sets of permissions are required or not by the business and the teams that use this AWS account.

### Enumerating directly attached policies to users

Although it's a recommended practice to attach policies to groups and assign users to specific groups based on the attached policies, it is still possible to directly attach a policy to a user.

Use the following steps to identify which users have directly attached policies and what these policies contain.

**Step 1:** Enumerate the list of users and check if any of them have a policy directly attached to them

**Step 1.1:** Run the following command to list all managed (AWS and Customer) policies that have been directly attached to the user

```
aws iam list-attached-user-policies --user-name <username>
```

```
kcloudle-rnd:~$ aws iam list-attached-user-policies --user-name just-a-test-user
{
  "AttachedPolicies": [
    {
      "PolicyName": "AmazonEC2FullAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2FullAccess"
    },
    {
      "PolicyName": "IAMFullAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMFullAccess"
    },
    {
      "PolicyName": "IAMUserChangePassword",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMUserChangePassword"
    },
    {
      "PolicyName": "demo6546456464",
      "PolicyArn": "arn:aws:iam:::policy/demo6546456464"
    }
  ]
}
kcloudle-rnd:~$
```

Next, obtain the policy document using the version number and the *get-policy-version* IAM command.

```
aws iam get-policy-version --policy-arn <policy-arn> --version-id <version>
```

Review the *Action* and *Resource* section of the policy to determine privileges and identify if any of the policies are overprivileged.

**Step 1.2:** Run the following command to list inline policies attached directly to the user

```
aws iam list-user-policies --user-name <username>
```

```
kloudle-rnd:$>
kloudle-rnd:$> aws iam list-user-policies --user-name just-a-test-user
{
  "PolicyNames": [
    "S3ListAll"
  ]
}
kloudle-rnd:$>
```

You can then use the following command to list the policy document of the attached inline policy to the user.

```
aws iam get-user-policy --user-name <username> --policy-name <policy-name>
```

```
kloudle-rnd:$> aws iam get-user-policy --user-name just-a-test-user --policy-name S3ListAll
{
  "UserName": "just-a-test-user",
  "PolicyName": "S3ListAll",
  "PolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
          "s3:ListStorageLensConfigurations",
          "s3:ListAccessPointsForObjectLambda",
          "s3:ListBucketMultipartUploads",
          "s3:ListAllMyBuckets",
          "s3:ListAccessPoints",
          "s3:ListJobs",
          "s3:ListBucketVersions",
          "s3:ListBucket",
          "s3:ListMultiRegionAccessPoints",
          "s3:ListMultipartUploadParts"
        ],
        "Resource": "*"
      }
    ]
  }
}
kloudle-rnd:$>
```

Verify the Action and Resource section of the policy and identify any untoward extraneous permissions.

Based on the user that these policies are attached to, verify if these sets of permissions are required or not by the business and the teams that use this AWS account.



## Enumerating roles and the policies attached to them

Just like AWS IAM users are used to administer and manage cloud resources, AWS IAM Roles are used to provide different resources, say EC2 instances, the ability to interact with other services, say S3. These roles can be assigned permissions via policies based on their functions, but more often than not, roles end up with higher privileges.

In this section we will enumerate the roles and their policies as part of the audit

**Step 1:** Enumerate all the roles within your AWS account using the following commands. This can be a fairly large list.

```
aws iam list-roles
```

```
kloudle-rnd:~$> aws iam list-roles
{
  "Roles": [
    {
      "Path": "/service-role/",
      "RoleName": "aws-codestar-service-role",
      "RoleId": "AROAQLE03KKMANL373GDF",
      "Arn": "arn:aws:iam:::role/service-role/aws-codestar-service-role",
      "CreateDate": "2021-07-08T05:39:57+00:00",
      "AssumeRolePolicyDocument": {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Principal": {
              "Service": "codestar.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
          }
        ]
      },
      "MaxSessionDuration": 3600
    },
    {
      "Path": "/",
      "RoleName": "aws-elasticbeanstalk-ec2-role",
      "RoleId": "AROAQLE03KKMNFJMLYYK",
      "Arn": "arn:aws:iam:::role/aws-elasticbeanstalk-ec2-role",
      "CreateDate": "2021-08-03T11:26:49+00:00",
      "AssumeRolePolicyDocument": {
        "Version": "2008-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Principal": {
              "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
          }
        ]
      }
    }
  ]
}
```

You can use the query parameter, you can only extract the RoleName so that it is easier to fetch the policy in the next step. You can do this using the following command:

```
aws iam list-roles --query "Roles[].RoleName"
```

```
kloudle-rnd:~$> aws iam list-roles --query "Roles[].RoleName"
[
  "aws-codestar-service-role",
  "aws-elasticbeanstalk-ec2-role",
  "aws-elasticbeanstalk-service-role",
  "AWSCodePipelineServiceRole-us-east-2-service-check-demo",
  "AWSEKSClusterPolicy",
  "AWSServiceRoleForAccessAnalyzer",
  "AWSServiceRoleForAmazonEKS",
  "AWSServiceRoleForAmazonEKSFargate",
  "AWSServiceRoleForAmazonEKSNodegroup",
  "AWSServiceRoleForAmazonElasticsearchService",
  "AWSServiceRoleForAmazonGuardDuty",
  "AWSServiceRoleForAmazonInspector",
  "AWSServiceRoleForAmazonInspector2",
  "AWSServiceRoleForAmazonSSM",
  "AWSServiceRoleForAmazonWorkLink",
  "AWSServiceRoleForAPIGateway",
  "AWSServiceRoleForAutoScaling",
  "AWSServiceRoleForECS",

```

From the list of existing roles, their names should give you an idea of what these roles are being used for. However, it is important to look at their attached policies as well to identify any role that has been maliciously created perhaps.

**Step 2:** For each of these roles, their attached policies need to be enumerated. Both Managed (AWS and Customer) and inline policy statements.

This can be done using the following commands:

```
aws iam list-role-policies --role-name <role-name>
```

```
aws iam list-attached-role-policies --role-name <role-name>
```

```
kloudle-rnd:~$> aws iam list-attached-role-policies --role-name custom-ec2-role-2
{
  "AttachedPolicies": [
    {
      "PolicyName": "AdministratorAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
    }
  ]
}
kloudle-rnd:~$>
```

**Step 3:** The last step is to fetch the policy document itself. You can use the following commands to list the policy document of the policy attached to the role by first fetching the active version of the policy in use.

```
aws iam get-policy --policy-arn <policy-arn>
```

```
aws iam get-policy-version --version-id <policy-version> --policy-arn <policy-arn>
```

```
kcloudle-rnd:~$  
kcloudle-rnd:~$ aws iam get-policy --policy-arn "arn:aws:iam::aws:policy/AdministratorAccess"  
{  
  "Policy": {  
    "PolicyName": "AdministratorAccess",  
    "PolicyId": "ANPAI1M8CKSKIEE64ZLYK",  
    "Arn": "arn:aws:iam::aws:policy/AdministratorAccess",  
    "Path": "/",  
    "DefaultVersionId": "v1",  
    "AttachmentCount": 4,  
    "PermissionsBoundaryUsageCount": 0,  
    "IsAttachable": true,  
    "Description": "Provides full access to AWS services and resources.",  
    "CreateDate": "2015-02-06T18:39:46+08:00",  
    "UpdateDate": "2015-02-06T18:39:46+08:00",  
    "Tags": []  
  }  
}  
kcloudle-rnd:~$ aws iam get-policy-version --version-id v1 --policy-arn "arn:aws:iam::aws:policy/AdministratorAccess"  
{  
  "PolicyVersion": {  
    "Document": {  
      "Version": "2012-10-17",  
      "Statement": [  
        {  
          "Effect": "Allow",  
          "Action": "*",  
          "Resource": "*"   
        }  
      ]  
    },  
    "VersionId": "v1",  
    "IsDefaultVersion": true,  
    "CreateDate": "2015-02-06T18:39:46+08:00"  
  }  
}  
kcloudle-rnd:~$
```

Based on the policy statement you can determine if the policy is over privileged for the role that is attached to.

A Strong Password is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

### A Strong Password should -

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#\$\$%^&\*()\_+)=)
- Strong Passwords do not -
- Spell a word or series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc.

## **The following are several recommendations for maintaining a Strong Password:**

### **Do not share your password with anyone for any reason**

Passwords should not be shared with anyone, including any students, faculty or staff. In situations where someone requires access to another individual's protected resources, delegation of permission options should be explored. For example, Microsoft Exchange calendar will allow a user to delegate control of his or her calendar to another user without sharing any passwords. This type of solution is encouraged. Passwords should not be shared even for the purpose of computer repair. An alternative to doing this is to create a new account with an appropriate level of access for the repair person.

### **Change your password upon indication of compromise**

If you suspect someone has compromised your account, change your password immediately. Be sure to change your password from a computer you do not typically use (e.g. university cluster computer). After resetting your password, report the incident to your local departmental administrator and/or the Information Security Office at iso-ir@andrew.cmu.edu.

### **Consider using a passphrase instead of a password**

A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember. For example, the passphrase "My passw0rd is \$uper str0ng!" is 28 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.

### **Do not write your password down or store it in an insecure manner**

As a general rule, you should avoid writing down your password. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed (see Guidelines for Data Protection). Using a password manager to store your passwords is not recommended unless the password manager leverages strong encryption and requires authentication prior to use. The ISO has vetted some password managers that meets these requirements.

### **Avoid reusing a password**

When changing an account password, you should avoid reusing a previous password. If a user account was previously compromised, either knowingly or unknowingly, reusing a password could allow that user account to, once again, become compromised. Similarly, if a password was shared for some reason, reusing that password could allow someone unauthorized access to your account.

### **Avoid using the same password for multiple accounts**

While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more sensitive accounts such as your Andrew account or your online banking account. These passwords should differ from the password you use for instant messaging, webmail and other web-based accounts.

### **Do not use automatic logon functionality**

Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

The following are Guidelines for individuals responsible for provisioning and support of user accounts:

### **Enforce strong passwords**

Many systems and applications include functionality that prevents a user from setting a password that does not meet certain criteria. Functionality such as this should be leveraged to ensure only Strong Passwords are being set.

### **Require a change of initial or “first-time” passwords**

Forcing a user to change their initial password helps ensure that only that user knows his or her password. Depending on what process is being used to create and distribute the password to the user, this practice can also help mitigate the risk of the initial password being guessed or intercepted during transmission to the user. This guidance also applies to situations where a password must be manually reset.

### **Force expiration of initial or “first-time” passwords**

In certain situations, a user may be issued a new account and not access that account for a period of time. As mentioned previously, initial passwords have a higher risk of being guessed or intercepted depending on what process is being used to create and distribute passwords. Forcing an initial password to expire after a period of time (e.g. 72 hours) helps mitigate this risk. This may also be a sign that the account is not necessary.

### **Do not use Restricted data for initial or “first-time” passwords**

The Guidelines for Data Classification defines Restricted data in its data classification scheme. Restricted data includes, but is not limited to, social security number, name, date of birth, etc. This type of data should not be used wholly or in part to formulate an initial password. See Appendix A for a more comprehensive list of data types.

### **Always verify a user’s identity before resetting a password**

A user’s identity should always be validated prior to resetting a password. If the request is in-person, photo identification is a sufficient means of doing this. If the request is by phone, validating an identity is much more difficult. One method of doing this is to request a video conference with the user (e.g. Skype) to match the individual with their photo id. However, this can be a cumbersome process. Another option is to have the person’s manager call and confirm the request. For obvious reasons, this would not work for student requests. If available, a self-service password reset solution that prompts a user with a series of customized questions is an effective approach to addressing password resets.

### **Never ask for a user’s password**

As stated above, individual user account passwords should not be shared on any reason. A natural correlation to this guidance is to never ask others for their passwords. Once again, delegation of permission is one alternative to asking a user for their password. Some applications include functionality that allows an administrator to impersonate another user, without entering that user’s password, while still tying actions back to the administrator’s user account. This is also an acceptable alternative. In computer repair situations, requesting that a user create a temporarily account on their system is one alternative.

The following are several additional Guidelines for individuals responsible for the design and implementation of systems and applications:

**Change default account passwords**

Default accounts are often the source of unauthorized access by a malicious user. When possible, they should be disabled completely. If the account cannot be disabled, the default passwords should be changed immediately upon installation and configuration of the system or application.

## **Implement strict controls for system-level and shared service account passwords**

Shared service accounts typically provide an elevated level of access to a system. System-level accounts, such as root and Administrator, provide complete control over a system. This makes these types of accounts highly susceptible to malicious activity. As a result, a more lengthy and complex password should be implemented. System-level and shared service accounts are typically critical to the operation of a system or application. Because of this, these passwords are often known by more than one administrator. Passwords should be changed anytime someone with knowledge of the password changes job responsibilities or terminates employment. Use of accounts such as root and Administrator should also be limited as much as possible. Alternatives should be explored such as using sudo in place of root and creating unique accounts for Windows administration instead of using default accounts.

## **Do not use the same password for multiple administrator accounts**

Using the same password for multiple accounts can simplify administration of systems and applications. However, this practice can also have a chain effect allowing an attacker to break into multiple systems as a result of compromising a single account password.

## **Do not allow passwords to be transmitted in plain-text**

Passwords transmitted in plain-text can be easily intercepted by someone with malicious intent. Protocols such as FTP, HTTP, SMTP and Telnet all natively transmit data (including your password) in plain-text. Secure alternatives include transmitting passwords via an encrypted tunnel (e.g. IPSec, SSH or SSL), using a one-way hash or implementing a ticket based authentication scheme such as Kerberos. Contact the Information Security Office at iso@andrew.cmu.edu if you would like an assessment of your application's authentication controls.

## **Do not store passwords in easily reversible form**

Passwords should not be stored or transmitted using weak encryption or hashing algorithms. For example, the DES encryption algorithm and the MD-4 hash algorithm both have known security weaknesses that could allow protected data to be deciphered. Encryption algorithms such as 3DES or AES and hashing algorithms such as SHA-1 or SHA-256 are stronger alternatives to the previously mentioned algorithms. Contact the Information Security Office at iso@andrew.cmu.edu if you have questions related to the use of a specific encryption and hashing algorithm.

## **Implement automated notification of a password change or reset**

When a password is changed or reset, an email should be automatically sent to the owner of that user account. This provides a user with a confirmation that the change or reset was successful and also alerts a user if his or her password to unknowingly changed or reset.

The following are additional Guidelines for system or service accounts - those not designed to be used by humans:

Where possible, service accounts should be randomly generated, long (  $\geq$  15 characters), and follow the same complexity requirements for strong passwords above.

Service accounts in Microsoft Active Directory with a Service Principal Name (SPN) should be randomly generated, long (  $\geq$  28 characters), and follow the same complexity requirements for strong passwords above. The longer length mitigates weak encryption ciphers. If software compatibility requires setting a shorter password, please contact the Information Security Office (iso@andrew.cmu.edu) to discuss compensating controls.

## **Intrusion Detection**

If a firewall is like having a security guard at your office door, checking the credentials of everyone coming and going, then an intrusion-detection system (IDS) is like having a network of sensors that tells you when someone has broken in, where they are and what they're doing.

Firewalls work only at the point of entry to the network, and they work only with packets as they pass in and out of the network. Once an attacker has breached the firewall, he can roam at will through the network. That's where intrusion detection is important.

There are a number of approaches that can be used for detecting intruders. Many experts advise using a combination of methods rather than relying on any single mechanism.

### **Host-Based Detection**

Perhaps the most famous IDS is Tripwire, a program written in 1992 by Eugene Spafford and Gene Kim. Tripwire exemplifies the host-based agent approach to intrusion detection: Installed on a host, it checks to see what has changed on the system, verifying that key files haven't been modified.

The agent is initially installed against a pristine host installation and records important system file attributes, including hashes of the files. The agent software then periodically compares the current state of those files to the stored attributes and reports any suspicious changes.

Another host-based approach monitors all packets as they enter and exit the host, essentially taking a personal firewall approach. Receipt of a suspicious packet triggers an alarm. Other commercial host-based products include Cupertino, Calif.-based Symantec Corp.'s Intruder Alert and Issaquah, Wash.-based CyberSafe Corp.'s Centrax.

Network-based intrusion-detection systems scrutinize all packets on a network segment, flagging those that look suspicious. A network IDS searches for attack signatures - indicators that the packets represent an intrusion. Signatures might be based on actual packet contents and are checked by comparing bits to known patterns of attacks. For example, the system might look for patterns that match attempts to modify system files.

Other network attacks are protocol-based. Attackers often seek weaknesses in a network by probing for active but poorly administered Web, file or other servers. These port attack signatures are identified by watching for attempts to connect to network ports associated with services that are often vulnerable.

An attack with a header signature uses malformed or illogical TCP/IP packet headers. For example, an attacker might try to send a packet that simultaneously requests to close and open a TCP connection; such a packet might cause a denial-of-service event for some systems.

Commercial network-based systems include Cisco Systems Inc.'s Secure Intrusion Detection System (formerly known as Cisco NetRanger), Atlanta-based Internet Security System Inc.'s RealSecure and Symantec's NetProwler.

### **What You Know, What They Do**

Detection systems can also be categorized as knowledge- or behavior-based. Most commercially available systems are knowledge-based, matching signatures of known attacks against changes in systems or streams of packets on a network. Such systems are reliable and generate few false positives, but they can detect intruders using only attacks they already know



about. They're often helpless against new attacks, so they must be continually updated with new knowledge about new attacks.

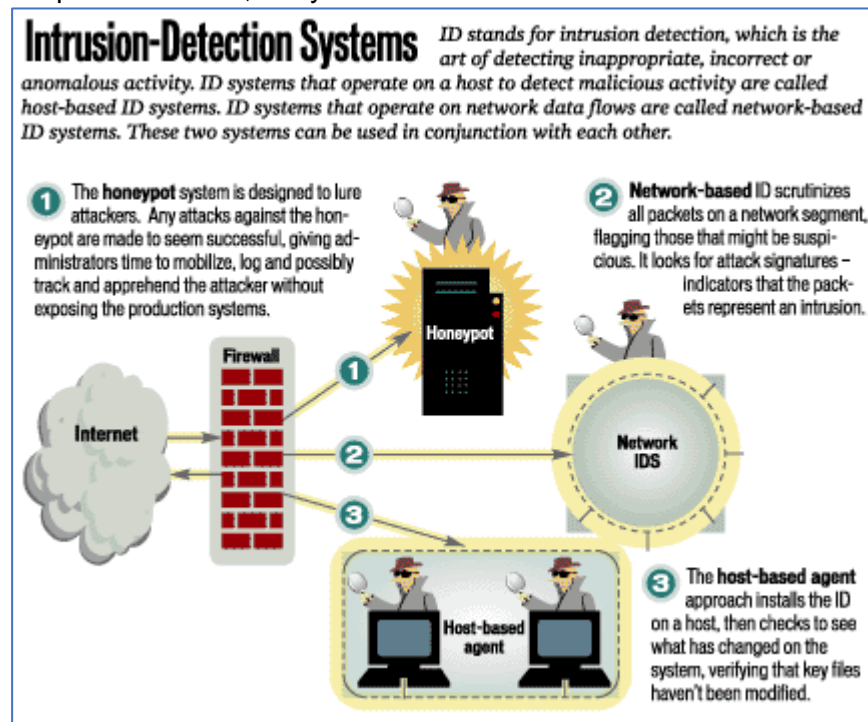
A behavior-based IDS instead looks at actions, attempting to identify attacks by monitoring system or network activity and flagging any activity that doesn't seem to fit in. Such activities may trigger an alarm - often a false alarm. Though false positives are common with a behavior-based IDS, so is the ability to detect a previously unreported attack.

Another intrusion-detection tool is the "honeypot," a completely separate system designed to offer an attractive nuisance to attackers. One manager of a prominent Web site often uses a honeypot to handle all inbound requests. Any attacks against the honeypot are made to seem successful, giving administrators time to mobilize, log and track the attacker without ever exposing production systems.

Intrusion detection requires considerable planning. As with virus detection, host-based intrusion detection that monitors system and file changes must be installed on pristine systems. Otherwise, there's always the chance that the system has already been compromised prior to installation of the IDS.

It's even more important to have a clear procedure in place for dealing with intrusions. It's not always best to simply pull the plug once you know that an intrusion is under way.

Depending on what systems or networks have been compromised and what you want to happen to the attackers, it's often preferable to keep the attackers in the system and contact a law enforcement agency to try to catch them. Such a decision shouldn't be made in haste; a set of intrusion response policies and procedures should be prepared well in advance. You want to keep intruders out, but you also want to discover and locate them when they succeed.



## File auditing

File Auditing monitors changes – and attempted changes - to file or folder permissions, usually documenting what permissions have been changed, the object path, the user making the assignment, and other identifiable factors like machine name, IP address, etc.

In any enterprise using file servers to store and share data, auditing is important to ensure data security. You can monitor multiple file servers in your domain. In this article, you will see how to track who accesses files on Windows File Servers in your organization, using Windows Server's built-in auditing. At the end of the article, you will also see how to do it effortlessly through Lepide File Server Auditor (part of Lepide Data Security Platform).

Here are the steps to track who read a file on Windows File Server.

- Step 1 – Set 'Audit Object Access' audit policy
- Step 2 – Set auditing on the files that you want to track
- Step 3 – Track who reads the file in Windows Event Viewer

### Step 1 – Set 'Audit Object Access' audit policy

Follow these steps one by one to enable "Audit object access" audit policy:

1. Launch "Group Policy Management" console. For that, on the primary "Domain Controller", or on the system where "Administration Tools" is installed, type "gpmc.msc" in the "Run" dialog box, and click "OK".
2. After you have opened the "Group Policy Management" window, you will have to create a new GPO, or edit an existing one.
3. To edit an existing GPO, in the left-pane, right-click on the default or a user-created GPO, and click "Edit" on the context menu. This action opens the Editor window of Group Policy Management Editor.

**Note:** If you want to track multiple folders, you will have to configure audit for every folder individually.

4. Navigate to "Security" tab.

**Note:** It is suggested to create a new GPO, link it to the domain, and edit it.

5. In the "Group Policy Management Editor" window, you have to set the appropriate audit policy.
6. To audit file accesses, you have to set "Audit object access" policy. For that, navigate to "Computer Configuration" → "Windows Settings" → "Security Settings" → "Local Policies" → "Audit Policy". All the available policies under "Audit Policy" are displayed in the right panel.

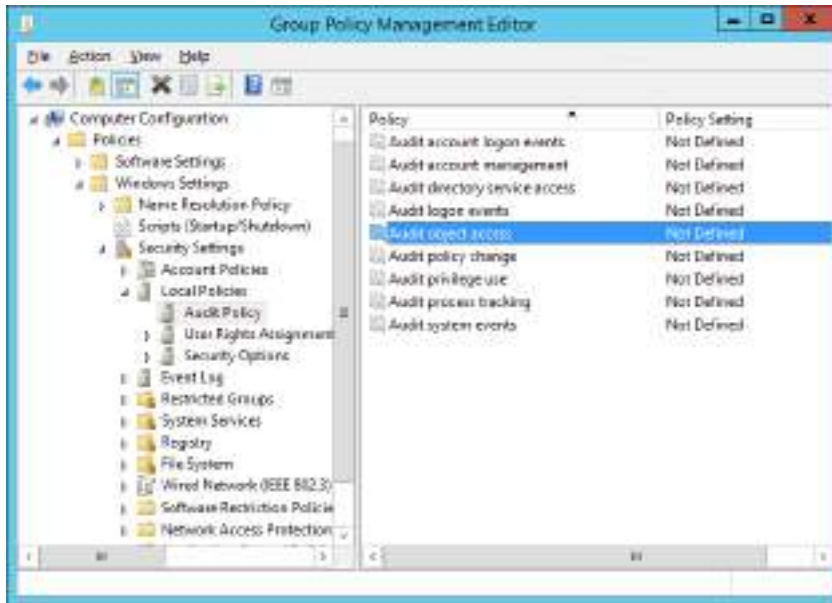


Figure 1: “Audit Object Access” policy

7. Double-click “Audit object access” policy to open its “Properties”.

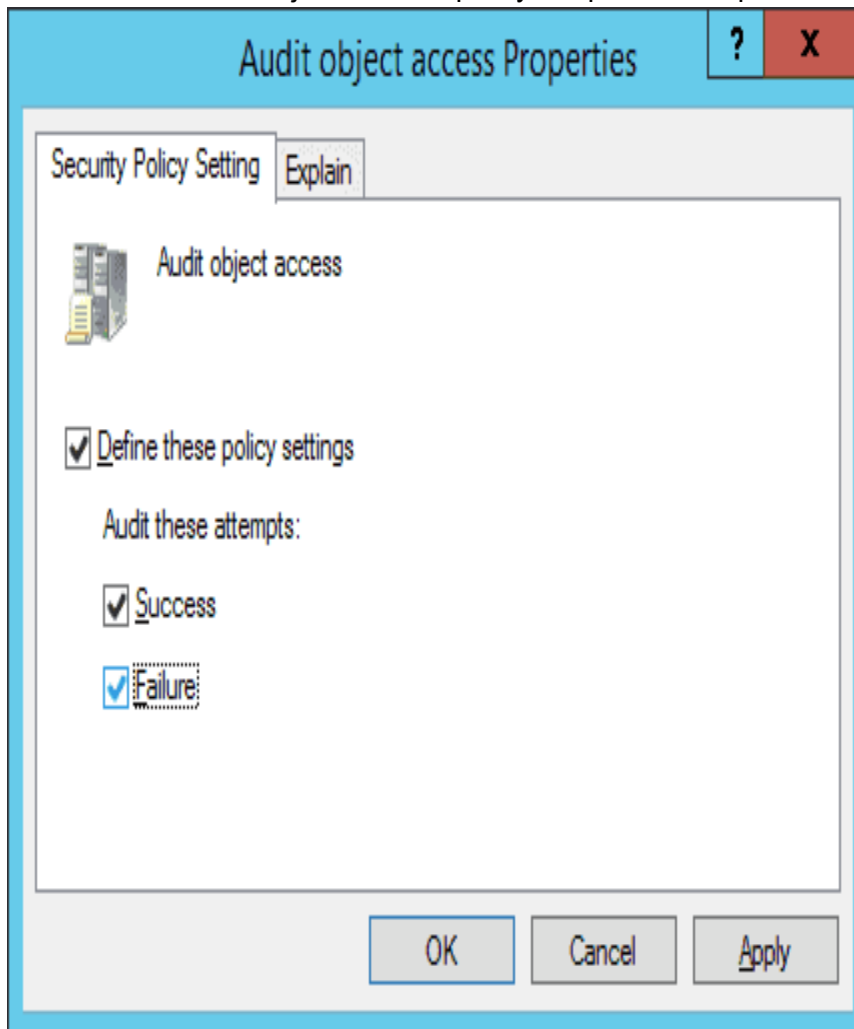


Figure 2: Properties of Audit Object Access Policy

8. On this window, click “Define these policy settings” checkbox. Then, you get two options to audit – “Success” and “Failure”. The former lets you audit successful

attempts made to access the objects, whereas the latter lets you audit failed attempts.

9. Select any one or both the options as per requirement. It is recommended to select both options. In our case, we have selected both the options because we want to audit both the successful and the failed attempts.
10. Click “Apply” and “OK” to close the window.
11. To immediately update the Group Policy instead of waiting for it to auto update, run the following command in the “Command Prompt”:

Gpupdate /force

## Step 2 – Set auditing on the files that you want to track

After configuring GPO, you have to set auditing on each file individually, or on folders that contain the files. Here are the steps:

1. Open “Windows Explorer” and navigate to the file or folder that you want to audit.
2. Right-click the file and select “Properties” from the context menu. The file’s properties window appears on the screen.  
**Note:** If you want to track multiple files, put them into one, two or more folders to enable their auditing easily. Doing this saves you from repeating these steps for each file.
3. By default, “General” tab of “Properties” window appears on the screen. Go to “Security” tab.

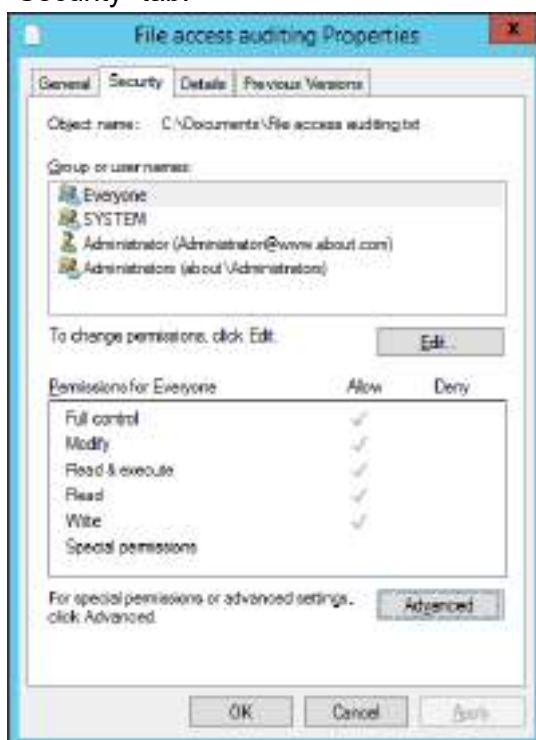
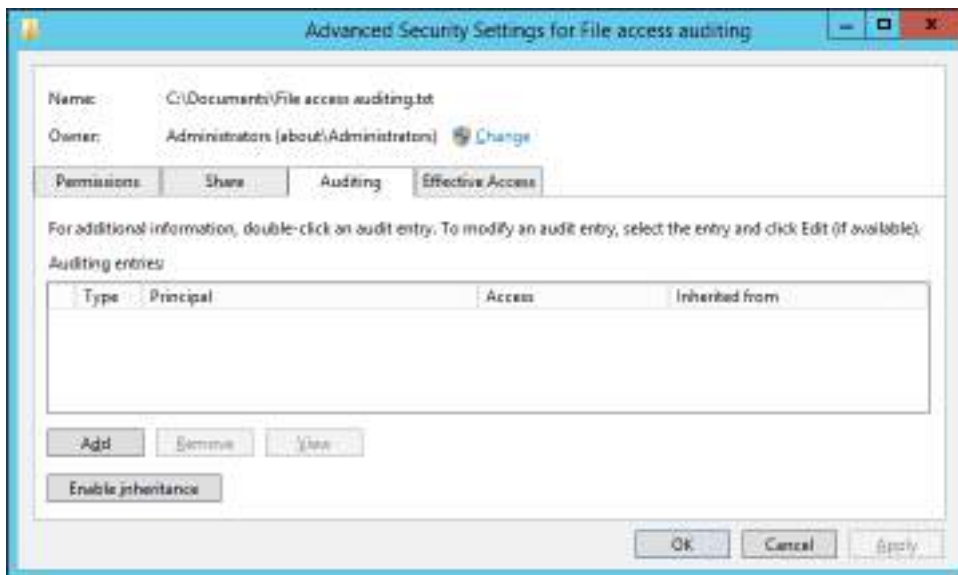


Figure 3 Auditing tab of “Advanced Security Settings”

4. On “Security” tab, click “Advanced” to access “Advanced Security Settings for” window appears on the screen.

- In “Advanced Security Settings for” window, go to “Auditing” tab.  
Figure 4: Select User, Computer, Service Account, or Group



- On this tab, you have to create a new audit entry. For that, click “Add”. The “Auditing Entry for” window appears on the screen.
- In “Auditing Entry for” window, at first, select users whose actions you want to audit. Click “Select a Principal”, to open “Select User, Computer, Service Account, or Group” dialog box.
- Here, choose users to audit. If you want to audit all users’ activities, enter “Everyone” in the “Enter the object name to select” field, and click “Check Names”. In our case, we enter “Everyone”.

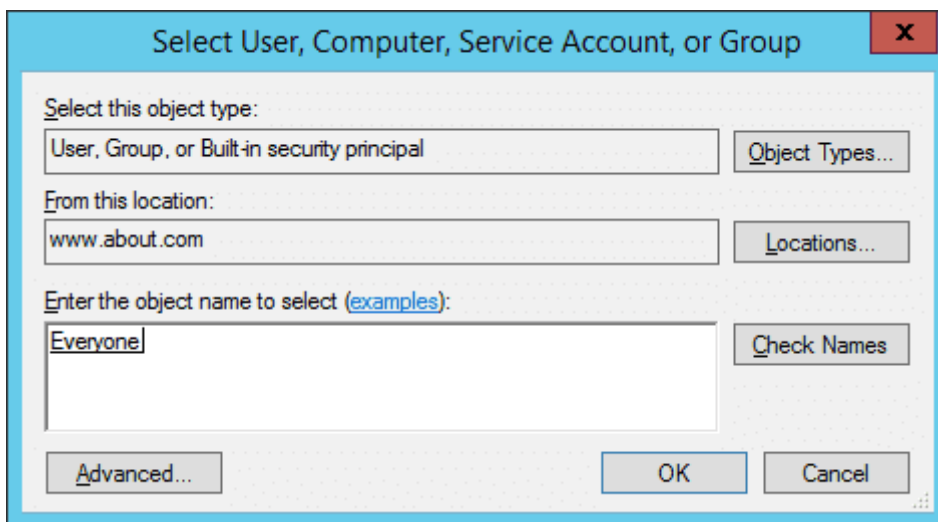


Figure 5: “Auditing Entry” window of the file

- Click “OK” to close the dialog box.
- Three options are available in the “Type” picklist: “Success”, “Fail”, and “All”. We select “All” option because we want to audit both successful and failed attempts.

11. In “Permissions” section, you can select all activities that you want to audit. In the case to audit file read, select “Traverse Folder/Execute File”, “List Folder/Read data”, “Read attributes”, and “Read extended attributes” permissions.

**NOTE:** If you want to audit all the activities, select the “Full Control” checkbox.

12. Click “OK” to close “Auditing Entry for File Access auditing” window.

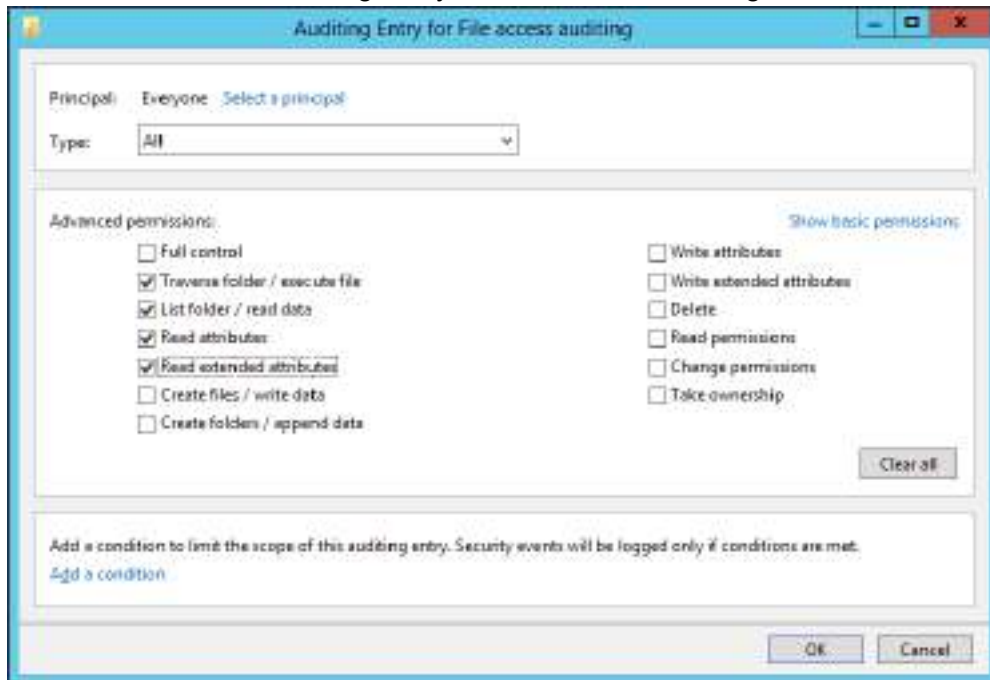


Figure 6: The file access event

13. Back in the “Advanced security settings” window, now you see the new audit entry.
14. Click “Apply” and “OK” to close the window.
15. Click “Apply” and “OK” to close file properties.

### Step 3 – Track who reads the file in Windows Event Viewer

To see who reads the file, open “Windows Event Viewer”, and navigate to “Windows Logs” → “Security”. There is a “Filter Current Log” option in the right pane to find the relevant events.

If anyone opens the file, event ID 4656 and 4663 will be logged. For example, in our case, someone opened the file (File access auditing.txt), and as shown in the following image, a file access event (ID 4663) was logged. You can see who accessed the file in “Account Name” field and access time in “Logged” field.

In the below image, you can see file’s name (C:\Users\Administrator\Documents\New Text Document.txt), which is visible after you scroll down the side bar, under the “Object Name” field.

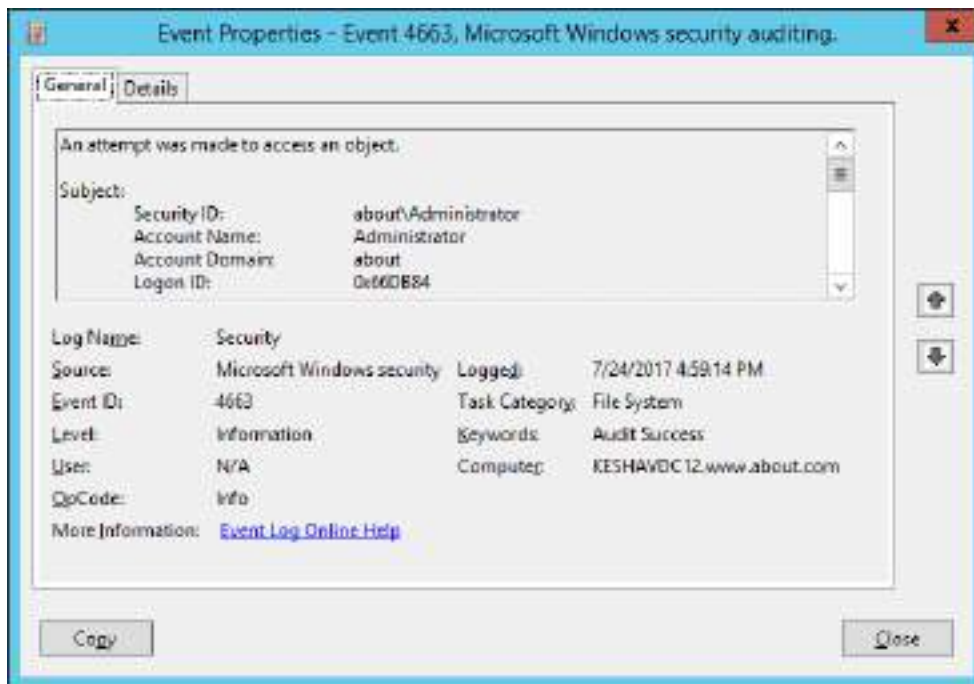


Figure 7: Name of the file in the Event 4663

**Individual Activity:**

- *Carry out Server and device security control.*



**Self-check quiz 3.2**

Check your understanding by answering the following questions:

1. What is System Hardening?

Answer:

2. Write down the techniques of database hardening.

Answer:

3. What is normalization?

Answer:

4. What are the recommendations for maintaining a Strong Password?

Answer:





### Learning outcome 3.3 – Ensure system (OS) security



Contents:

- Hardening of operating system.
- System security Auditing.
- Access management.
- OS Configuration management
- OS default Firewall/ Intrusion detection and prevention system.
- Configuration of web services and browsing security.
- Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)
- Data Leak/Loss Prevention (DLP)



Assessment criteria:

1. Hardening of operating system is performed.
2. System security is audited.
3. Identity is set and access management is performed as per standard procedure.
4. OS Configuration management is performed as per client's requirement.
5. OS default Firewall/ Intrusion detection and prevention system are configured by following standard.
6. Web services and browsing security is configured as per standard procedure.
7. Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) are described.
8. Data Leak/Loss Prevention (DLP) is interpreted.



Resources required:

- Students/trainees must be provided with the following resources:
- Workplace (actual or simulated), class room, trainee handbook and Operating system



### **LEARNING ACTIVITY 3.3**

Learning Activity	Resources/Special Instructions/References
Ensure system (OS) security	<ul style="list-style-type: none"> <li>▪ Information Sheets: 3.3</li> <li>▪ Self-Check: 3.3</li> <li>▪ Answer Key: 3.3</li> </ul>



### Information sheet 3.3

Learning Objective: to List out production process of garments

#### **Operating system hardening**

Operating system hardening involves patching and implementing advanced security measures to secure a server's operating system (OS). One of the best ways to achieve a hardened state for the operating system is to have updates, patches, and service packs installed automatically.

OS hardening is like application hardening in that the OS is technically a form of software. But unlike application hardening's focus on securing standard and third-party applications, OS hardening secures the base software that gives permissions to those applications to do certain things on your server.

Oftentimes, operating system developers, such as Microsoft and Linux, do a fine and consistent job of releasing OS updates and reminding users to install these updates. These frequent updates - and we've all ignored them - can actually help keep your system secure and resilient to cyberattacks.

#### **Other examples of operating system hardening include:**

- Removing unnecessary drivers
- Encrypting the HDD or SSD that stores and hosts your OS
- Enabling and configuring Secure Boot
- Limiting and authenticating system access permissions
- Limiting or eliminating the creation and logging in of user accounts

#### **System security Auditing**

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to an established set of criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.

Security audits are often used to determine compliance with regulations such as the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act and the California Security Breach Information Act that specify how organizations must deal with information.

These audits are one of three main types of security diagnostics, along with vulnerability assessments and penetration testing. Security audits measure an information system's performance against a list of criteria. A vulnerability assessment is a comprehensive study of an information system, seeking potential security weaknesses. Penetration testing is a covert approach in which a security expert tests to see if a system can withstand a specific attack. Each approach has inherent strengths and using two or more in conjunction may be the most effective approach.

Organizations should construct a security audit plan that is repeatable and updateable. Stakeholders must be included in the process for the best outcome.

## Why do a security audit?

There are several reasons to do a security audit. They include these six goals:

1. Identify security problems and gaps, as well as system weaknesses.
2. Establish a security baseline that future audits can be compared with.
3. Comply with internal organization security policies.
4. Comply with external regulatory requirements.
5. Determine if security training is adequate.
6. Identify unnecessary resources.

Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reasons.

IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.

Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.

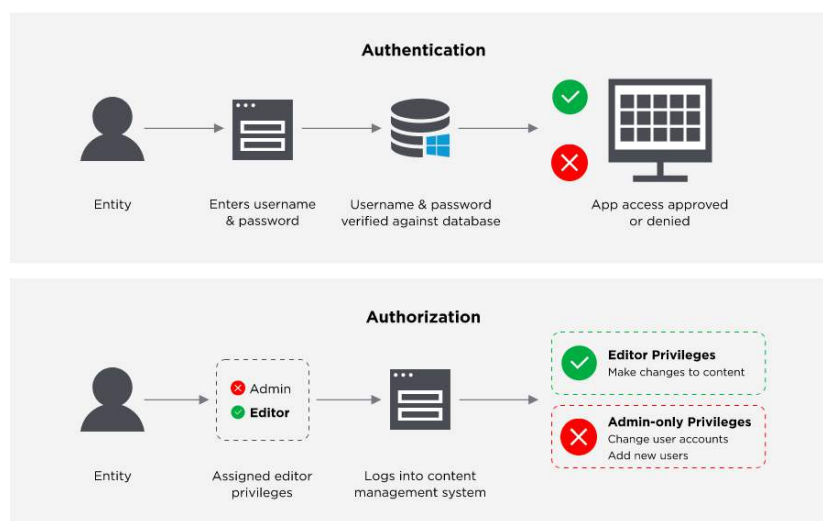
## 5 keys to success when implementing Identity and Access Management

1. Embed the program in the company.
2. Create a long-term roadmap for IAM implementation.
3. Decide on build vs buy.
4. Define IAM roles and responsibilities.
5. Make user experience your top priority.

## Identity management solutions generally perform two tasks:

IAM confirms that the user, software, or hardware is who they say they are by authenticating their credentials against a database. IAM cloud identity tools are more secure and flexible than traditional username and password solutions.

Identity access management systems grant only the appropriate level of access. Instead of a username and password allowing access to an entire software suite, IAM allows for narrow slices of access to be portioned out, i.e. editor, viewer, and commenter in a content management system.



Configuration management is a process for maintaining computer systems, servers, and software in a desired, consistent state. It's a way to make sure that a system performs as it's expected to as changes are made over time.

### **Intrusion detection system (IDS)**

An IDS is either a hardware device or software application that uses known intrusion signatures to detect and analyze both inbound and outbound network traffic for abnormal activities.

This is done through:

- System file comparisons against malware signatures.
- Scanning processes that detect signs of harmful patterns.
- Monitoring user behavior to detect malicious intent.
- Monitoring system settings and configurations.

Upon detecting a security policy violation, virus or configuration error, an IDS is able to kick an offending user off the network and send an alert to security personnel.

Despite its benefits, including in-depth network traffic analysis and attack detection, an IDS has inherent drawbacks. Because it uses previously known intrusion signatures to locate attacks, newly discovered (i.e., zero-day) threats can remain undetected.

Furthermore, an IDS only detects ongoing attacks, not incoming assaults. To block these, an intrusion prevention system is required.

### **Intrusion prevention system (IPS)**

An IPS complements an IDS configuration by proactively inspecting a system's incoming traffic to weed out malicious requests. A typical IPS configuration uses web application firewalls and traffic filtering solutions to secure applications.

An IPS prevents attacks by dropping malicious packets, blocking offending IPs and alerting security personnel to potential threats. Such a system usually uses a preexisting database for signature recognition and can be programmed to recognize attacks based on traffic and behavioral anomalies.

While being effective at blocking known attack vectors, some IPS systems come with limitations. These are commonly caused by an overreliance on predefined rules, making them susceptible to false positives.

Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of your network to detect and stop potential incidents.

An Intrusion Detection and Prevention (IDP) policy lets you selectively enforce various attack detection and prevention techniques on the network traffic passing through your security device. Security devices offer the same set of IDP signatures that are available on Juniper Networks

IDP Series Intrusion Detection and Prevention Appliances to secure networks against attacks. The basic IDP configuration involves the following tasks:

- Download and install the IDP license.
- Download and install the signature database—You must download and install the IDP signature database. The signature databases are available as a security package on the Juniper Networks website. This database includes attack object and attack object groups that you can use in IDP policies to match traffic against known attacks.
- Configure recommended policy as the IDP policy—Juniper Networks provides predefined policy templates to use as a starting point for creating your own policies. Each template is a set of rules of a specific rulebase type that you can copy and then update according to your requirements.
- Enable a security policy for IDP inspection—For transit traffic to pass through IDP inspection, you configure a security policy and enable IDP application services on all traffic that you want to inspect.

### Securing Web Services

Because of its nature (loosely coupled connections) and its use of open access (mainly HTTP), SOA implemented by Web services adds a new set of requirements to the security landscape. Web services security includes several aspects:

- Authentication—Verifying that the user is who she claims to be. A user's identity is verified based on the credentials presented by that user, such as:
  1. Something one has, for example, credentials issued by a trusted authority such as a passport (real world) or a smart card (IT world).
  2. Something one knows, for example, a shared secret such as a password.
  3. Something one is, for example, biometric information.
- Using a combination of several types of credentials is referred to as "strong" authentication, for example using an ATM card (something one has) with a PIN or password (something one knows).
- Authorization (or Access Control)—Granting access to specific resources based on an authenticated user's entitlements. Entitlements are defined by one or several attributes. An attribute is the property or characteristic of a user, for example, if "Marc" is the user, "conference speaker" is the attribute.
- Confidentiality, privacy—Keeping information secret. Accesses a message, for example a Web service request or an email, as well as the identity of the sending and receiving parties in a confidential manner. Confidentiality and privacy can be achieved by encrypting the content of a message and obfuscating the sending and receiving parties' identities.
- Integrity, non repudiation—Making sure that a message remains unaltered during transit by having the sender digitally sign the message. A digital signature is used to validate the signature and provides non-repudiation. The timestamp in the signature prevents anyone from replaying this message after the expiration.

#### Web Service Security Requirements

The following summarize the Web service security requirements:

- Transport-level security to protect the communication channel between the Web service consumer and the Web service provider, with transport-level authentication by requiring username, SAML, or JWT tokens.
- Transport-level security with message-level authentication by requiring username or SAML tokens.

- Message-level security to ensure confidentiality by digitally encrypting message parts; integrity using digital signatures; and authentication by requiring username, X.509, or SAML tokens.

### **Endpoint detection and response (EDR)**

Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. The term was suggested by Anton Chuvakin at Gartner to describe emerging security systems that detect and investigate suspicious activities on hosts and endpoints, employing a high degree of automation to enable security teams to quickly identify and respond to threats.

The primary functions of an EDR security system are to:

- Monitor and collect activity data from endpoints that could indicate a threat
- Analyze this data to identify threat patterns
- Automatically respond to identified threats to remove or contain them, and notify security personnel
- Forensics and analysis tools to research identified threats and search for suspicious activities

### **Extended Detection and Response (XDR)**

According to analyst firm Gartner, Extended Detection and Response (XDR) is “a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components.”

XDR enables an enterprise to go beyond typical detective controls by providing a holistic and yet simpler view of threats across the entire technology landscape. XDR delivers real-time actionable threat information to security operations for better, faster outcomes.

Extended Detection and Response (XDR) primary advantages are:

- Improved protection, detection, and response capabilities
- Improved productivity of operational security personnel
- Lower total cost of ownership for effective detection and response of security threats

### **Data loss prevention (DLP)**

Data loss prevention (DLP) -- sometimes referred to as data leak prevention, information loss prevention and extrusion prevention -- is a strategy for preventing individuals from accessing sensitive information who do not need it. It also ensures that employees do not send sensitive or critical information outside the corporate network.



### Self-check quiz 3.3

Check your understanding by answering the following questions:

Write the appropriate/correct answer of the following:

1. What is Operating system hardening?

2. What do you mean by System security Auditing?

3. Why do a security audit?





### Learning outcome 3.4 – Interpret data center security and operations



Contents:

- Data center architecture.
- Data center components.
- Data center network security.
- Environmental security



Assessment criteria:

1. Data center architecture is explained.
2. Data center components are described.
3. Data center network security is interpreted.
4. Environmental security is interpreted.



Resources required:

Students/trainees must be provided with the following resources:

Workplace (actual or simulated), class room, trainee handbook and Data center



### **LEARNING ACTIVITY 3.4**

Learning Activity	Resources/Special Instructions/References
Interpret data center security and operations	<ul style="list-style-type: none"> <li>▪ Information Sheets: 3.4</li> <li>▪ Self-Check: 3.4</li> <li>▪ Answer Key: 3.4</li> </ul>



## Information sheet 3.4

Learning Objective: to Interpret data center security and operations

Data architecture is a framework for how IT infrastructure supports your data strategy. The goal of any data architecture is to show the company's infrastructure how data is acquired, transported, stored, queried, and secured. A data architecture is the foundation of any data strategy.

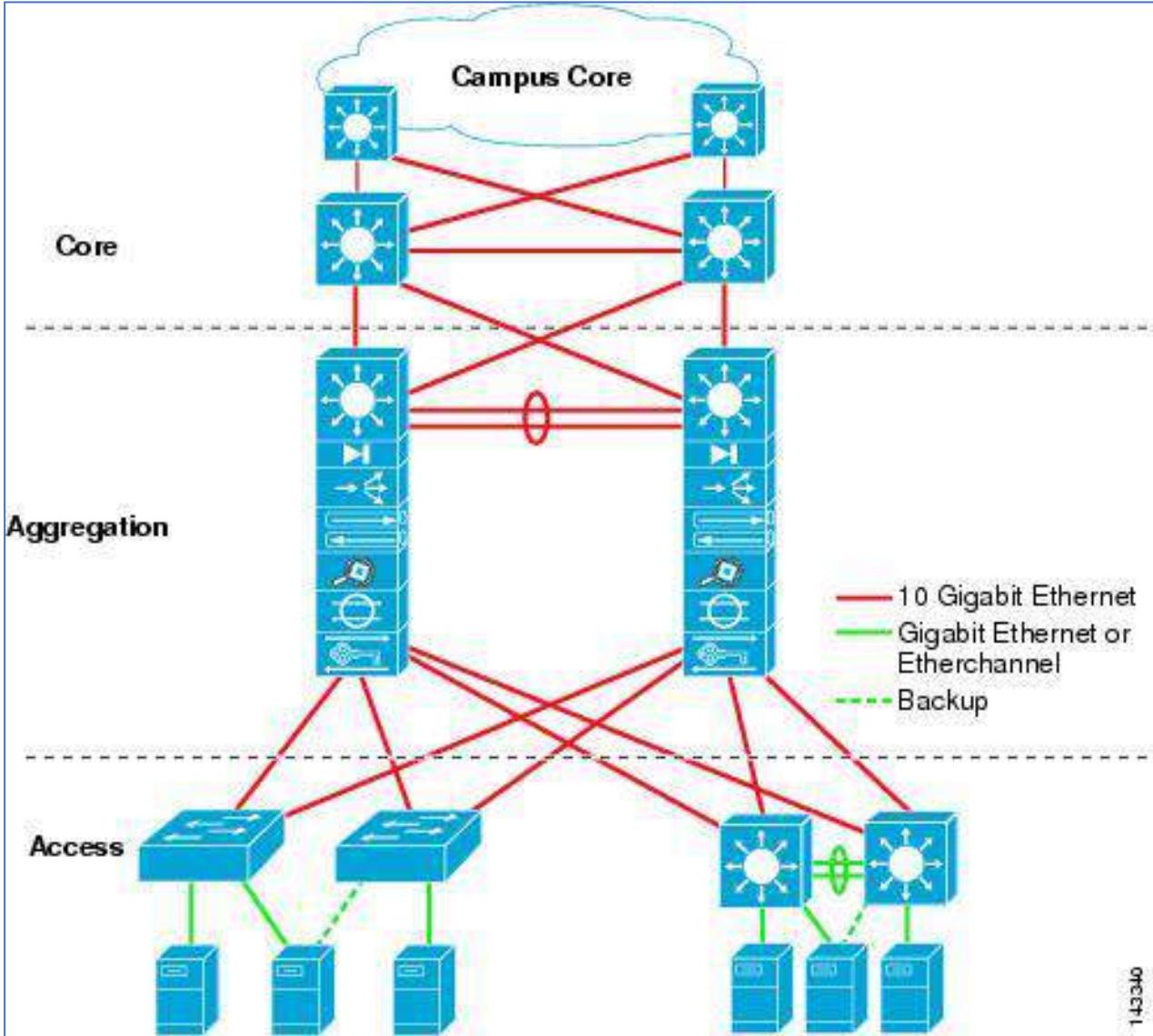
### **Data Center Architecture Overview**

The data center is home to the computational power, storage, and applications necessary to support an enterprise business. The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered.

Another important aspect of the data center design is flexibility in quickly deploying and supporting new services. Designing a flexible architecture that has the ability to support new applications in a short time frame can result in a significant competitive advantage. Such a design requires solid initial planning and thoughtful consideration in the areas of port density, access layer uplink bandwidth, true server capacity, and oversubscription, to name just a few.

The data center network design is based on a proven *layered* approach, which has been tested and improved over the past several years in some of the largest data center implementations in the world. The layered approach is the basic foundation of the data center design that seeks to improve scalability, performance, flexibility, resiliency, and maintenance. [Figure 1-1](#) shows the basic layered design.

Figure 1-1 Basic Layered Design



The layers of the data center design are the *core*, *aggregation*, and *access* layers. These layers are referred to extensively throughout this guide and are briefly described as follows:

- **Core layer**—Provides the high-speed packet switching backplane for all flows going in and out of the data center. The core layer provides connectivity to multiple aggregation modules and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as OSPF or EIGRP, and load balances traffic between the campus core and aggregation layers using Cisco Express Forwarding-based hashing algorithms.
- **Aggregation layer modules**—Provide important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy. Server-to-server multi-tier traffic flows through the aggregation layer and can use services, such as firewall and server load balancing, to optimize and secure applications. The smaller icons within the aggregation layer switch in [Figure 1-1](#) represent the integrated service modules. These modules provide services, such as content switching, firewall, SSL offload, intrusion detection, network analysis, and more.
- **Access layer**—Where the servers physically attach to the network. The server components consist of 1RU servers, blade servers with integral switches, blade servers with pass-through cabling, clustered servers, and mainframes with OSA adapters. The access layer network infrastructure consists of modular switches, fixed configuration 1 or 2RU switches, and integral blade server switches. Switches provide both Layer 2 and Layer 3 topologies, fulfilling the various server broadcast domain or administrative requirements.

This chapter defines the framework on which the recommended data center architecture is based and introduces the primary data center design models: the *multi-tier* and *server cluster* models.

### Data Center Design Models

The *multi-tier* model is the most common design in the enterprise. It is based on the web, application, and database layered design supporting commerce and enterprise business ERP and CRM solutions. This type of design supports many web service architectures, such as those based on Microsoft .NET or Java 2 Enterprise Edition. These web service application environments are used by ERP and CRM solutions from Siebel and Oracle, to name a few. The multi-tier model relies on security and application optimization services to be provided in the network.

The *server cluster* model has grown out of the university and scientific community to emerge across enterprise business verticals including financial, manufacturing, and entertainment. The server cluster model is most commonly associated with high-performance computing (HPC), parallel computing, and high-throughput computing (HTC) environments, but can also be associated with grid/utility computing. These designs are typically based on customized, and sometimes proprietary, application architectures that are built to serve particular business objectives.

[Chapter 2 "Data Center Multi-Tier Model Design,"](#) provides an overview of the multi-tier model, and [Chapter 3 "Server Cluster Designs with Ethernet,"](#) provides an overview of the server

cluster model. Later chapters of this guide address the design aspects of these models in greater detail.

### Multi-Tier Model

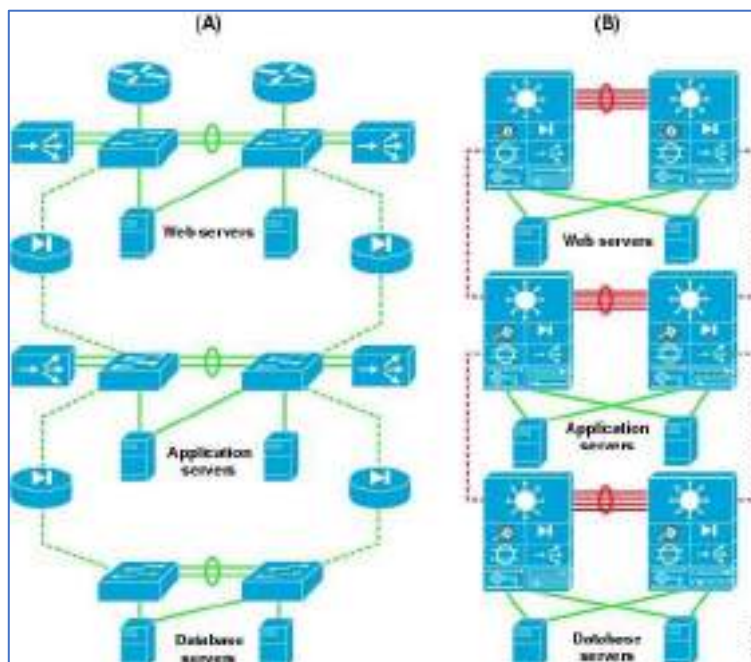
The multi-tier data center model is dominated by HTTP-based applications in a multi-tier approach. The multi-tier approach includes web, application, and database tiers of servers. Today, most web-based applications are built as multi-tier applications. The multi-tier model uses software that runs as separate processes on the same machine using interprocess communication (IPC), or on different machines with communications over the network. Typically, the following three tiers are used:

- Web-server
- Application
- Database

Multi-tier server farms built with processes running on separate machines can provide improved resiliency and security. Resiliency is improved because a server can be taken out of service while the same function is still provided by another server belonging to the same application tier. Security is improved because an attacker can compromise a web server without gaining access to the application or database servers. Web and application servers can coexist on a common physical server; the database typically remains separate.

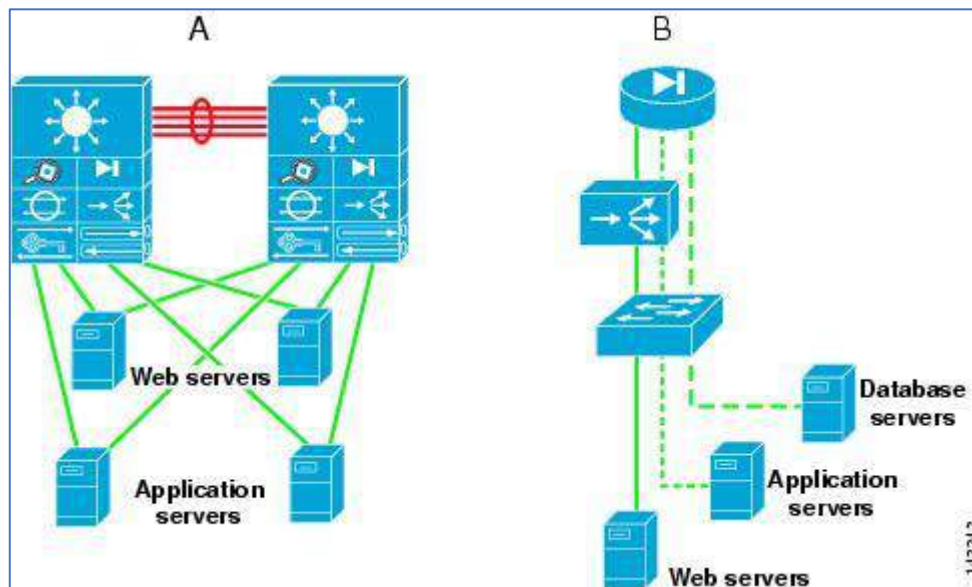
Resiliency is achieved by load balancing the network traffic between the tiers, and security is achieved by placing firewalls between the tiers. You can achieve segregation between the tiers by deploying a separate infrastructure composed of aggregation and access switches, or by using VLANs

**Figure 1-2 Physical Segregation in a Server Farm with Appliances (A) and Service Modules (B)**



The design shown in [Figure 1-3](#) uses VLANs to segregate the server farms. The left side of the illustration (A) shows the physical topology, and the right side (B) shows the VLAN allocation across the service modules, firewall, load balancer, and switch. The firewall and load balancer, which are VLAN-aware, enforce the VLAN segregation between the server farms. Note that not all of the VLANs require load balancing. For example, the database in the example sends traffic directly to the firewall.

**Figure 1-3 Logical Segregation in a Server Farm with VLANs**



Physical segregation improves performance because each tier of servers is connected to dedicated hardware. The advantage of using logical segregation with VLANs is the reduced complexity of the server farm. The choice of physical segregation or logical segregation depends on your specific network performance requirements and traffic patterns.

Business security and performance requirements can influence the security design and mechanisms used. For example, the use of wire-speed ACLs might be preferred over the use of physical firewalls. Non-intrusive security devices that provide detection and correlation, such as the Cisco Monitoring, Analysis, and Response System (MARS) combined with Route Triggered Black Holes (RTBH) and Cisco Intrusion Protection System (IPS) might meet security requirements. Cisco Guard can also be deployed as a primary defense against distributed denial of service (DDoS) attacks. For more details on security design in the data center, refer to *Server Farm Security in the Business Ready Data Center*

### Server Cluster Model

In the modern data center environment, clusters of servers are used for many purposes, including high availability, load balancing, and increased computational power. This guide focuses on the high performance form of clusters, which includes many forms. All clusters have the common goal of combining multiple CPUs to appear as a unified high performance system using special software and high-speed network interconnects. Server clusters have historically

been associated with university research, scientific laboratories, and military research for unique applications, such as the following:

- Meteorology (weather simulation)
- Seismology (seismic analysis)
- Military research (weapons, warfare)

Server clusters are now in the enterprise because the benefits of clustering technology are now being applied to a broader range of applications. The following applications in the enterprise are driving this requirement:

- Financial trending analysis—Real-time bond price analysis and historical trending
- Film animation—Rendering of artist multi-gigabyte files
- Manufacturing—Automotive design modeling and aerodynamics
- Search engines—Quick parallel lookup plus content insertion

In the enterprise, developers are increasingly requesting higher bandwidth and lower latency for a growing number of applications. The time-to-market implications related to these applications can result in a tremendous competitive advantage. For example, the cluster performance can directly affect getting a film to market for the holiday season or providing financial management customers with historical trending information during a market shift.

### **Data center**

Data center infrastructure is composed of the physical elements that can be found within a data center. In essence, data center physical infrastructure can be classified as the IT hardware and supporting hardware (like cooling and air quality systems) found within the walls of the facility.

The components of data centers allow for the efficient processing, storage, and distribution of large amounts of data. These components include:

#### **Servers.**

Servers are pieces of hardware or software that provide functionality to a data center. They are connected to networks to make data accessible to computers. Servers are typically housed in server racks.

#### **Networking.**

Networking equipment enables the storage and processing of applications and data through switching, routing, load balancing, analytics, etc.

#### **Storage.**

Data center storage consists of technologies, software, and devices that allow for the storing of data and applications within a data center.

#### **Software.**

Software is the non-physical component of a computer system that comprises the programs, procedures, and routines involved in the efficient operation of a computer system.

#### **Cabling infrastructure.**

The foundation of data centers lies within the cabling infrastructure as it enables the power and data transmissions that are critical to operations. Failure to properly manage these systems can lead to serious issues such as downtime and large expenses.

#### **Power infrastructure.**

Physical infrastructure such as rack PDUs, remote power panels, busways, floor PDUs, and UPSs are necessary to provide power to IT equipment. Backup power is usually supplied by a fuel generator to minimize downtime.

#### **Cooling infrastructure.**

Data center cooling equipment such as computer room air conditioning (CRAC) and computer room air handler (CRAH) units are designed to always keep the facility at an ideal temperature and to prevent critical IT equipment from overheating.

#### **Physical security.**

Data centers may include alarms, electronic door locks, biometric scanners, and other safety measures to protect the data and assets inside.

#### **Network security infrastructure**

Businesses can keep the data center protected from malicious inbound network traffic by setting up a strong security perimeter or firewall between external traffic and the internal network. IT managers can further structure the network infrastructure to strengthen the security in a data center by partitioning it into segments and isolating each segment from the others. With a segmented network infrastructure, a security breach in one segment does not necessarily compromise the entire network.

#### **Backbone network data center**

Image result for backbone data center network

A backbone or core network is a part of a computer network which interconnects networks, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas.

#### **zoning in data center**

Constructing a data center facility needs zoning approval. Data centers consume a lot of power and water (for cooling) and have come under the scrutiny of environmental groups. Zoning is an area of law, which dictates how the property can be constructed and used.

#### **Data center environment**

A modern data center houses an organization's data systems in a well-protected physical and storage infrastructure along with servers, storage subsystems, networking switches, routers, firewalls, cabling and physical racks.

#### **Data Center Environmental Standards and Concerns**

- Temperature Control. As it turns out, heat may not be the ferocious data center threat it's made out to be.
- Humidity Control. Data centers work hard to combat heat.
- Static Electricity Monitoring.
- Fire Suppression.
- Physical Security Systems.





### Self-check quiz 3.4

Check your understanding by answering the following questions:

Write the appropriate/correct answer of the following:

1. What is data center?

Answer:

2. Which term we need to concern during establishment of data center environment?

Answer:



## Answer keys

### Answer key: 3.1

#### 1. Answer:

Network auditing is the process of mapping and inventorying your network in terms of hardware and software. It's a fairly complex task that involves manually identifying network elements. In some cases, network auditing tools can provide automation support to identify the devices and services connected to the network.

#### 2. Answer:

There are many reasons why you should consider an audit. Typically, it's timed around important technology decisions or business requirements. Here's just a few potential reasons why your business might consider a network audit.

- 1) Outdated & Incomplete Inventories
- 2) Upgrades & Refreshes
- 3) Troubleshooting & Resolution
- 4) Regulatory & Compliance Standards

#### 3. Answer:

Answer: A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

#### 4. Answer:

Answer:

Step 1: Secure your firewall

Step 2: Architect your firewall zones and IP addresses

Step 3: Configure Access Control Lists (ACLs)

Step 4: Configure your other firewall services and logging

Step 5: Test your firewall configuration

#### 5. Answer:

Load balancer administrators create forwarding rules for four main types of traffic:

**HTTP** — Standard HTTP balancing directs requests based on standard HTTP mechanisms. The Load Balancer sets the X-Forwarded-For, X-Forwarded-Proto, and X-Forwarded-Port headers to give the backends information about the original request.

**HTTPS** — HTTPS balancing functions the same as HTTP balancing, with the addition of encryption. Encryption is handled in one of two ways: either with SSL passthrough which maintains encryption all the way to the backend or with SSL termination which places the decryption burden on the load balancer but sends the traffic unencrypted to the back end.

TCP — For applications that do not use HTTP or HTTPS, TCP traffic can also be balanced. For example, traffic to a database cluster could be spread across all of the servers.

UDP — More recently, some load balancers have added support for load balancing core internet protocols like DNS and syslogd that use UDP.

### Answer key 3.2

Check your understanding by answering the following questions:

1. Answer:

System hardening is the process of securing a server or computer system by minimizing its attack surface, or surface of vulnerability, and potential attack vectors. It's a form of cyberattack protection that involves closing system loopholes that cyberattackers frequently use to exploit the system and gain access to users' sensitive data

2. Answer:

Types of database hardening techniques include:

- Restricting administrators and administrative privileges and functions
- Encrypting in-transit and at-rest database information
- Adhering to a role-based access control (RBAC) policy
- Regularly updating and patching database software, or the DBMS
- Turning off needless database services and functions
- Locking database accounts if suspicious login activity is detected
- Enforcing strong and more complex database passwords

3. Answer:

Normalization is a data management technique that ensures all data and attributes, such as IP addresses and timestamps, within the transaction log are formatted in a consistent way.

4. Answer:

The recommendations for maintaining a Strong Password?

- Do not share your password with anyone for any reason
- Change your password upon indication of compromise
- Consider using a passphrase instead of a password
- Do not write your password down or store it in an insecure manner
- Avoid reusing a password
- Avoid using the same password for multiple accounts
- Do not use automatic logon functionality
- Enforce strong passwords
- Require a change of initial or "first-time" passwords
- Force expiration of initial or "first-time" passwords
- Do not use Restricted data for initial or "first-time" passwords
- Always verify a user's identity before resetting a password
- Never ask for a user's password
- Change default account passwords

### Answer key 3.3

1. Answer:

Operating system hardening involves patching and implementing advanced security measures to secure a server's operating system (OS). One of the best ways to achieve a hardened state for the operating system is to have updates, patches, and service packs installed automatically.

2. Answer:

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to an established set of criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.

3. Answer:

There are several reasons to do a security audit. They include these six goals:

1. Identify security problems and gaps, as well as system weaknesses.
2. Establish a security baseline that future audits can be compared with.
3. Comply with internal organization security policies.
4. Comply with external regulatory requirements.
5. Determine if security training is adequate.
6. Identify unnecessary resources.

### Answer key 3.4

1. Answer:

Answer: The data center is home to the computational power, storage, and applications necessary to support an enterprise business. The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered

2. Answer:

Answer: Data Center Environmental Standards and Concerns

- Temperature Control. As it turns out, heat may not be the ferocious data center threat it's made out to be.
- Humidity Control. Data centers work hard to combat heat.
- Static Electricity Monitoring.
- Fire Suppression.
- Physical Security Systems.

LEARNER JOB SHEET 2			
<b>Qualification:</b>	Information System Security Management		
<b>Learning unit:</b>	Configure Firewall		
<b>Learner name:</b>			
<b>Personal protective equipment (PPE):</b>			
<b>Materials:</b>			
<b>Tools and equipment:</b>			
<b>Performance criteria:</b>	Firewall is configured following standard procedure		
<b>Measurement:</b>			
<b>Notes:</b>			
<b>Procedure:</b>	<ol style="list-style-type: none"> <li>1. Secure your firewall</li> <li>2. Architect your firewall zones and IP addresses</li> <li>3. Configure Access Control Lists (ACLs)</li> <li>4. Configure your other firewall services and logging</li> <li>5. Test your firewall configuration</li> </ol>		
<b>Learner signature:</b>		<b>Date:</b>	
<b>Assessor signature:</b>		<b>Date:</b>	
<b>Quality Assurer signature:</b>		<b>Date:</b>	
<b>Assessor remarks:</b>			
<b>Feedback:</b>			

## Module 4: Perform Application Software Security

---



### MODULE CONTENT

#### Module Descriptor:

This module covers the knowledge, skills, and attitudes required to Perform Application Software security. It specifically includes maintaining security operations management, performing incidents management and interpreting security threats Intelligence management.

**Nominal Duration: 40 hours**



#### LEARNING OUTCOMES:

Upon completion of the module, the trainee should be able to:

- 4.1 Maintain Security operations management
- 4.2 Perform Incidents Management
- 4.3 Interpret Security Threat Intelligence Management



#### PERFORMANCE CRITERIA:

1. Capacity management is evaluated.
2. Change management is determined.
3. problem management process is identified and followed.
4. Incidents Management is interpreted.
5. Security incident management process is interpreted.
6. Security incidents are analyzed.
7. Learnt lessons from particular incident are documented.
8. Documents are prepared as per standard procedure.
9. Security Threat Intelligence is interpreted.
10. MITRE Attack is interpreted.
11. Security threat is mitigated as per standard procedure.
12. Cyber kill chain is interpreted.



## **Learning Outcome 4.1 Maintain Security operations management**



Contents:

- Capacity management
- Change management
- Problem management



Assessment criteria:

1. Capacity management is evaluated.
2. Change management is determined.
3. Problem management process is identified and followed.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (actual or simulated)
- Network devices, required tools, equipments and materials.



### **LEARNING ACTIVITY 4.1**

Learning Activity	Resources/Special Instructions/References
Maintain Security operations management	<ul style="list-style-type: none"> <li>▪ Information Sheet: 4.1</li> <li>▪ Self-Check: 4.1</li> <li>▪ Answer Key: 4.1</li> </ul>



## Information sheet 4.1

Learning Objective: to maintain Security operations management.

Capacity Management is the continuous and iterative process that monitors, analyses, and evaluates the performance and capacity of the IT infrastructure and, with the data obtained, it optimizes the service or submits an RFC to Change Management. All the information obtained in these activities, and that generated by Capacity Management using that information, is stored and recorded in the Capacity Database (CDB) available with the IT Manager.



### 1. Monitoring

The main objective is to ensure that the performance of the IT infrastructure matches the requirements of the SLAs. As well as technical aspects, monitoring needs to include details of licenses and other administrative information.

### 2. Analysis and Evaluation

The data collected needs to be analyzed to assess whether corrective action needs to be taken, such as requesting an increase in capacity or better Demand Management.

### 3. Optimization and changes

If it is decided that capacity needs to be increased, an RFC will be raised and sent to Change Management to set in train the whole process involved in implementing the change. Capacity Management will lend its support throughout the process and it will be jointly responsible, together with Change Management and Release Management for ensuring that the change requested meets the envisaged objectives. In the case where a simple rationalization of demand will be enough to resolve the deficiencies or non-compliances with SLAs, Capacity Management itself will be responsible for managing this sub-process.

### 4. Capacity Database

The CDB must cover all the business, financial, technical, and service information received and generated by Capacity Management in relation to the capacity of the infrastructure and its elements. Ideally, the CDB must be interrelated with the CMDB so that the CMDB is able to give a complete image of the systems and applications and includes all the information about



their capacity. However, this does not mean that the two databases cannot be “physically independent”.

Capacity management tools measure the volumes, speeds, latencies and efficiency of the movement of data as it is processed by an organization's applications. All facets of data's journey through the IT infrastructure must be monitored, so capacity management must be able to examine the operations of all the hardware and software in an environment and capture critical information about data flow.

Measurement and analysis tools must be able to observe the individual performances of IT assets, as well as how these assets interact. A comprehensive capacity management process should be able to monitor and measure the following IT elements:

- Servers
- End-user devices
- Networks and related communications devices
- Storage systems and storage network devices
- Cloud services

Whether capacity management is achieved via software, hardware or manual means -- or a combination of any of those -- it relies on the interception of data movement metrics and the internal processes of individual components. Most IT hardware products ship with applications that can extract basic performance information. While the information is useful, it usually is limited and may only pertain to a few performance factors. To get more detailed statistics, an admin would typically run a software utility program designed to address specific functionalities of a components. For example, IOmeter is a free, open source utility originally developed by Intel that provides details about processing by servers, clusters of servers or individual end-user computers. One of the key metrics that IOmeter provides is IOPS -- input/output operations per second -- which is a basic measure of the transfer rate of data during processing.

Emulation programs are also effective tools for capacity management. These programs mimic application programs such as database management systems (DBMSes) to determine how a system is likely to perform under similar loads in production environments. Application emulators typically include their own sets of test data to help ensure accurate and consistent results across disparate equipment.

Another approach to capacity management involves the use of hardware-based monitoring devices. Generally, these management systems focus on network performance and can provide comprehensive information on most aspects of data movement. The components of these systems vary, but a basic configuration will include control devices -- typically servers with specialized software -- and network TAPS, or network Test Access Points, devices that physically hook into particular elements of a network to capture information about data traffic as it occurs.

### **Components of capacity management**

Capacity management could have a fairly narrow scope, providing high-level information on a variety of infrastructure components or, perhaps, providing detail metrics related to one segment of the computing environment. The trend, however, is to gather as much information as possible and then to attempt to correlate those measurements into an application-centric picture that focuses on the performance and requirements of mission-critical applications across the environment, rather than how individual components are performing.

Still, to achieve that application-centric view of capacity management, virtually all elements of the IT infrastructure must be monitored and the definition of capacity must be broad enough to consider the impact an application will have on processing power, memory, storage capacity and speed for all physical and software components comprising an infrastructure.

Performance -- or throughput -- is a key metric in capacity management as it may point to processing bottlenecks that affect overall application processing performance. The central processor unit (CPU) in servers and other connected devices, such as routers, storage and controllers, should be monitored to ensure that their processing capabilities are not frequently "pinning" at or near 100%. An overtaxed processor would be a candidate for upgrading.

Memory is also a factor in capacity management. Servers and other devices use their installed memory to run applications and process data -- if too little memory is installed, processing will slow down. It's relatively easy to determine if a server has adequate memory resources, but it's also important to monitor other devices in the environment to ensure that insufficient memory doesn't turn them into processing bottlenecks.

Physical space is what is most commonly associated with capacity management, with the focus generally on storage space for applications and data. Storage systems that are near capacity will have longer response times, as it takes longer to locate specific data when drives -- hard disk or solid-state -- are full or nearly full. As with processor and memory measurements, it's important to monitor space usage in devices other than servers and end-user PCs that may have installed storage that's used for caching data.

### **Capacity management in networking**

Managing the capacity of IT networks can be a complex process given the number of different networking elements that can be found in an enterprise environment.

The number and type of networks being monitored is likely to vary as well. In addition to the wired and wireless Ethernet-based network infrastructure that connects servers to storage, end-user devices, networking gear, etc., comprehensive network capacity management must also consider dedicated storage networks based on Fibre Channel technologies; the FC networks are likely to be physically isolated from other data networks and will require different tools for monitoring and management.

External networking should also be monitored. Again, different tools will be required to track traffic and performance for network connections to remote offices and users, the internet and to cloud services.

The networking devices that should be monitored include network interface cards (NICs), network switches, network routers, storage network interfaces (e.g., host bus adapters), storage network switches and optical network devices.

Although capacity management for networks doesn't directly address security, it can be a good method of keeping track of network access, which can help inform security procedures.

### **Benefits of capacity management**

Capacity management provides many benefits to an IT organization and is a factor in overall management of a computing infrastructure.

In addition to ensuring that systems are performing at adequate levels to achieve a company's goals, capacity management can often realize cost savings by avoiding over-provisioning of hardware and software resources. It can also help save money and time by identifying extraneous activities like backing up unused data or maintaining idle servers.

Good capacity management can also result in more-effective purchasing to accommodate future growth by being able to more accurately anticipate needs and, thus, make purchases when prices may be lower.

By constantly monitoring equipment and processing, problems that might have hindered production may be avoided, such as bottlenecks or imminent equipment failures.

Change management is a key information security component of maintaining high availability systems. Change management involves requesting, approving, validating, and logging changes to systems. This process can bring significant benefits to an organization. Namely, it can strengthen the decision making ability of an organization by training personnel to fully think on and evaluate changes before they are made and it provides a knowledge base of past changes and the lessons learned from situations.

Information security can be divided into three sections: confidentiality, integrity, and availability, often called the CIA triad. Availability is extremely important. After all, if the data is not available to authorized users when they need it, of what use is it? High availability is another term that describes a system that is accessible to users 24x7 with minimal scheduled downtime.

An often mentioned method for obtaining high availability include hardware redundancy such as active/passive firewalls, clustered servers, network load balancing, and round robin DNS. Redundancy is an excellent aspect that high availability networks must have. However, another important factor in achieving high availability is a change management policy.

Any change has the potential to create new vulnerabilities or reduce the availability of systems. Of course, the process of maintaining systems and managing business objectives requires change. Therefore, organizations must determine how to balance the need for change with the minimization of risk. The answer is through change management. This starts with a change management policy that then leads into a change management program hereby change management is implemented throughout the company.

Let's first define change management and describe what a change management system looks like. Change management is the process whereby changes are requested, approved, validated, and logged to reduce the risk of a change compromising the availability of systems or creating new vulnerabilities. Validation also takes place after a change has been made. The system needs to be tested to determine if the change produced the desired result. Change management approvers should thoroughly consider the impact of changes and notify users and others about the change. It is advantageous to schedule the changes during standard downtimes to minimize the potential impact to system availability.

Moving along with the description laid out for us, the first element of change management is approval Change management systems require changes to be requested in a system and then approved by an authorized individual such as a supervisor, manager, data owner, or by multiple persons. The process of requesting a change and approving a change validates the actions taken since multiple people consider the decision and actions before they are approved.

The last element is logging. Logging produces some ancillary benefits to change management. Change management logging is a positive step towards knowledge management and it can aid personnel in reversing any damaging changes that may occur.

Change management can assist in knowledge management objectives because the rational behind changes along with those who implemented them are stored in the system. If a similar event comes along, such as a server error or a new project, the system can be queried to determine a course of action and the persons involved can be contacted for further information or involvement in future projects or troubleshooting.

Change management also gives an organization the ability to reverse damaging changes because it keeps a log of the actions taken. Not all changes achieve the desired outcome. In such situations, it is imperative that the organization have a method of reversing the changes to bring the system back into a functioning state. Change management accomplishes this by enabling users to view the log of actions taken so that these actions can be undone.

So what kinds of actions should be managed in a change management system? The CISSP common body of knowledge asserts that change management systems should manage changes related to the entire life cycle of a system including design, development, testing, evaluation, implementation, distribution, and ongoing maintenance.

The next question is what changes in these categories should be logged? This important question that has to be determined on a case-by-case basis by organizational decision makers. The greatest amount of benefits from a change management system will be realized by tracking even minor changes but this is a determination you will have to make.

Lastly, consider implementing change management metrics and integrating them with other security metrics you track so that you can ensure change management goals are met.

### **Problem management**

Problem management isn't just about finding and fixing incidents, but identifying and understanding the underlying causes of an incident as well as identifying the best method to eliminate that root cause. Moreover, pinpointing the cause has no value to an organization if it's a cut-off process completed by a siloed team, so problem management should be constant and widely practiced across multiple teams, including IT, security, and software developers. An incident may be over once the service is up and running again, but until the underlying causes and contributing factors are addressed, the problem remains.

### **Problem management vs. incident management**

ITIL defines a problem as a cause, or potential cause, of one or more incidents. The behaviors behind effective incident management and effective problem management are often similar and overlapping, but there are still key differences. For example, rolling back a recently deploy may get the service operating again and end the incident, but the underlying problem remains.

That said, we believe that problem management and incident management practices are becoming increasingly intertwined. During the times between incidents, IT teams can focus their efforts on problem investigations that lead to improvements and better service quality. This is how problem management becomes the most valuable to the organization.

### **Problem management and change management**

Change management is the process of planning, tracking, and releasing changes without service disruption or downtime.

When a change does cause disruption or downtime, that change is analyzed during incident and problem management processes.

### **Problem management and knowledge management**

Knowledge management creates a repository of solutions and documentation for common procedures and even incident workarounds. When used together, a healthy knowledge management practice can enable faster incident resolution and fewer incidents altogether.

### **Problem management and service request management**

Service request management is the practice of processing a request from a user for something to be provided, such as access to applications, software enhancements, and information. It can sometimes be difficult to distinguish a service request from an incident. In fact, the two were not

distinguished and both lumped into the category “incidents” until the release of ITIL V3 in 2007. ITIL now defines an incident as ‘an unplanned interruption to an IT service or reduction in the quality of an IT service.’ It defines a service request as “a formal request from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a workstation for a new user.”

### **The problem management process**

At Atlassian, we advocate bringing the problem and incident management processes closer together.

When problem management is a heavy, siloed, and separate process, companies can end up creating a dumping ground of problems. This backlog is where problem issues go to die in some teams. It's best to get problems in front of the teams that can handle and do valuable investigations.

That all being said, it's good to understand the main steps that contribute to a problem management process. Such as:

1. **Problem detection** - Proactively find problems so they can be fixed, or identify workarounds before future incidents happen.
2. **Categorization and prioritization** - Track and assess known problems to keep teams organized and working on the most relevant and high-value problems.
3. **Investigation and diagnosis** - Identify the underlying contributing causes of the problem and the best course of action for remediation.
4. **Create a known error record** - In ITIL, a known error is “a problem that has a documented root cause and a workaround.” Recording this information leads to less downtime if the problem triggers an incident. This is typically stored in a document called a known error database.
5. **Create a workaround, if necessary** - A workaround is a temporary solution for reducing the impact of problems and keeping them from becoming incidents. These aren't ideal, but they can limit business impact and avoid a customer-facing incident if the problem can't be easily identified and eliminated.
6. **Resolve and close the problem** - A closed problem is one that has been eliminated and can no longer cause another incident.

### Individual Activity:

- 



### Self-check quiz 4.1

Check your understanding by answering the following questions:

Write the correct answer for the following questions.

1. What is capacity Management?  
Answer:

2. What is capacity Management?  
Answer:

3. What are the problem management process?  
Answer:



## Learning outcome 4.2 - Perform Incidents Management



Contents:

- Incidents Management.
- Security incident management process.
- Security incidents.



Assessment criteria:

1. Incidents Management is interpreted.
2. Security incident management process is interpreted.
3. Security incidents are analyzed.
4. Learnt lessons from particular incident are documented.
5. Documents are prepared as per standard procedure.



Resources required:

- Students/trainees must be provided with the following resources:
- Workplace (Actual or simulated), Server, Necessary software.



### **LEARNING ACTIVITY 4.2**

Learning Activity	Resources/Special Instructions/References
Perform Incidents Management	<ul style="list-style-type: none"> <li>▪ Information Sheets: 4.2</li> <li>▪ Self-Check: 4.2</li> <li>▪ Answer Key: 4.2</li> </ul>



## Information sheet 4.2

Learning objective: to Perform Incidents Management

### **Incident**

An incident is an unexpected disruption to a service. It disturbs the normal operation thus affecting end user's productivity. An Incident may be caused due to an asset that is not functioning properly or network failure. Examples of Incidents include printer issue, wifi connectivity issue, application lock issue, email service issue, laptop crash, AD authentication error, file sharing issue etc

### **Security incident management**

Security incident management is the process of identifying, managing, recording and analyzing security threats or incidents in real-time. It seeks to give a robust and comprehensive view of any security issues within an IT infrastructure. A security incident can be anything from an active threat to an attempted intrusion to a successful compromise or data breach. Policy violations and unauthorized access to data such as health, financial, social security numbers, and personally identifiable records are all examples of security incidents.

### **The cybersecurity incident management process**

As cybersecurity threats continue to grow in volume and sophistication, organizations are adopting practices that allow them to rapidly identify, respond to, and mitigate these types of incidents while becoming more resilient and protecting against future incidents.

Security incident management utilizes a combination of appliances, software systems, and human-driven investigation and analysis. The security incident management process typically starts with an alert that an incident has occurred and engagement of the incident response team. From there, incident responders will investigate and analyze the incident to determine its scope, assess damages, and develop a plan for mitigation.

This means that a multi-faceted strategy for security incident management must be implemented to ensure the IT environment is truly secure. The ISO/IEC Standard 27035 outlines a five-step process for security incident management, including:

1. Prepare for handling incidents.
2. Identify potential security incidents through monitoring and report all incidents.
3. Assess identified incidents to determine the appropriate next steps for mitigating the risk.
4. Respond to the incident by containing, investigating, and resolving it (based on outcome of step 3).
5. Learn and document key takeaways from every incident.

Problem management is the process of identifying and managing the causes of incidents on an IT service. It is a core component of ITSM frameworks.

The closer you get to real incident experts, the less you actually hear the question: "What caused the incident?" Sure, you'll hear it plenty from executives, and customers, and the press. But the experts know better.



Because the answer to “what caused the incident” is often dry and non-helpful: a rewritten config file, a corrupted database entry.

But what were the contributing causes behind the thing that caused the incident? What were the factors that led up to the incident? How is it possible that a config file could be rewritten? What conditions create a corrupted database entry? These are the questions you hear experts ask. And they’re at the heart of problem management.

### **Best Practices for Security Incident Management**

Organizations of all sizes and types need to plan for the security incident management process. Implement these best practices to develop a comprehensive security incident management plan:

Develop a security incident management plan and supporting policies that include guidance on how incidents are detected, reported, assessed, and responded to. Have a checklist ready for a set of actions based on the threat. Continuously update security incident management procedures as necessary, particularly with lessons learned from prior incidents.

Establish an incident response team (sometimes called a CSIRT) including clearly defined roles and responsibilities. Your incident response team should include functional roles within the IT/security department as well as representation for other departments such as legal, communications, finance, and business management or operations.

Develop a comprehensive training program for every activity necessary within the set of security incident management procedures. Practice your security incident management plan with test scenarios on a consistent basis and make refinements as need be.

After any security incident, perform a post-incident analysis to learn from your successes and failures and make adjustments to your security program and incident management process where needed.

In some situations, collecting evidence and analyzing forensics is a necessary component of incident response. For these circumstances, you’ll want the following in place:

A policy for evidence collection to ensure it is correct and sufficient – or, when applicable, will be accepted in the court of law.

The ability to employ forensics as needed for analysis, reporting, and investigation.

Team members who have experience and training in forensics and functional techniques.

A strong security incident management process is imperative for reducing recovery costs, potential liabilities, and damage to the victim organization. Organizations should evaluate and select a suite of tools to improve visibility, alerting, and actionability with regard to security incidents.

**There is a five-step process for incident management in cybersecurity given by the ISO/IEC Standard 27035. They are as follows.**

#### **Step-1**

The process of incident management starts with an alert that reports an incident that took place. Then comes the engagement of the incident response team (IRT). Prepare for handling incidents.

#### **Step-2**

Identification of potential security incidents by monitoring and report all incidents.

**Step-3**

Assessment of identified incidents to determine the appropriate next steps for mitigating the risk.

**Step-4**

Respond to the incident by containing, investigating, and resolving it (based on the outcome of step 3).

**Step-5**

Learn and document key takeaways from every incident.

**Some tips for security incident management:**

Each and every organization needs to have a good and matured plan for the security incident management process, implementing the best process is very useful to make a comprehensive security incident management plan.

Create a security incident management plan with supporting policies including proper guidance on how incidents are detected, reported, assessed, and responded. It should have a checklist ready. The checklist will be containing actions based on the threat. The security incident management plan has to be continuously updated with security incident management procedures as necessary, particularly with lessons learned from prior incidents.

Creating an Incident Response Team (IRT) which will work on clearly defined roles and responsibilities. The IRT will also include functional roles like finance, legal, communication, and operations.

Always create regular training and mock drills for security incident management procedures. This improves the functionality of the IRT and also keep them on their toes.

Always perform a post-incident analysis after any security incident to learn from any success and failure and make necessary adjustments to the program and incident management processes when needed.

**Necessary part of incident response:**

Always make a habit of collecting evidence and analyze forensics which is a necessary part of incident response. For these circumstances, the following things are needed.

1. A well-defined policy to collect evidence to ensure that it is correct and very much sufficient to make it admissible in the Court of Law.
2. It is also importantly needed to have the ability to employ forensics as needed for analysis, reporting, and investigation.
3. The personnel of the IRT must be trained in cyber forensics, functional techniques and would also have some knowledge in the legal and governance.

**Individual Activity:**

- *Identify and listed some incident considering security issue.*

**Self-check quiz 4.2**

Check your understanding by answering the following questions:

1. What is incident?

Answer:

2. Write down the five-step process for security incident management, including:

Answer:



### Learning outcome 4.3 – Ensure system (OS) security



Contents:

1. Security Threat Intelligence
2. MITRE Attack.
3. Security threat.
4. Cyber kill chain



Assessment criteria:

1. Security Threat Intelligence is interpreted.
2. MITRE Attack is interpreted.
3. Security threat is mitigated as per standard procedure.
4. Cyber kill chain is interpreted.



Resources required:

Students/trainees must be provided with the following resources:

Workplace (actual or simulated), class room, trainee handbook and Operating system



### **LEARNING ACTIVITY 4.3**

Learning Activity	Resources/Special Instructions/References
Ensure system (OS) security	<ul style="list-style-type: none"> <li>▪ Information Sheets: 4.3</li> <li>▪ Self-Check: 4.3</li> <li>▪ Answer Key: 4.3</li> </ul>



## Information sheet 4.3

Learning Objective: to interpret Security Threat Intelligence Management

### Threat intelligence

Threat intelligence, also known as cyber threat intelligence (CTI), is information gathered from a range of sources about current or potential attacks against an organization. The information is analyzed, refined and organized and then used to minimize and mitigate cybersecurity risks.

The main purpose of threat intelligence is to show organizations the various risks they face from external threats, such as zero-day threats and advanced persistent threats (APTs). Threat intelligence includes in-depth information and context about specific threats, such as who is attacking, their capabilities and motivation, and the indicators of compromise (IOCs). With this information, organizations can make informed decisions about how to defend against the most damaging attacks.

Why is threat intelligence important?

In a military, business or security context, intelligence is information that provides an organization with decision support and possibly a strategic advantage. Threat intelligence is a part of a bigger security intelligence strategy. It includes information related to protecting an organization from external and inside threats, as well as the processes, policies and tools used to gather and analyze that information.

Threat intelligence provides better insight into the threat landscape and threat actors, along with their latest tactics, techniques and procedures. It enables organizations to be proactive in configuring its security controls to detect and prevent advanced attacks and zero-day threats. Many of these adjustments can be automated so security stays aligned with the latest intelligence in real time.

Benefit From Threat Intelligence?

Everyone! Cyber threat intelligence is widely imagined to be the domain of elite analysts. In reality, it adds value across security functions for organizations of all sizes.

When threat intelligence is treated as a separate function within a broader security paradigm rather than an essential component that augments every other function, the result is that many of the people who would benefit the most from threat intelligence don't have access to it when they need it.

Security operations teams are routinely unable to process the alerts they receive — threat intelligence integrates with the security solutions you already use, helping automatically prioritize and filter alerts and other threats. Vulnerability management teams can more accurately prioritize the most important vulnerabilities with access to the external insights and context provided by threat intelligence. And fraud prevention, risk analysis, and other high-level security processes are enriched by the understanding of the current threat landscape that threat intelligence provides, including key insights on threat actors, their tactics, techniques, and procedures, and more from data sources across the web.

Look at our section on use cases below for a deeper look at how every security role can benefit from threat intelligence.

## **The Threat Intelligence Lifecycle**

So, how does cyber threat intelligence get produced? Raw data is not the same thing as intelligence — cyber threat intelligence is the finished product that comes out of a six-part cycle of data collection, processing, and analysis. This process is a cycle because new questions and gaps in knowledge are identified during the course of developing intelligence, leading to new collection requirements being set. An effective intelligence program is iterative, becoming more refined over time.

To maximize the value of the threat intelligence you produce, it's critical that you identify your use cases and define your objectives before doing anything else.

### **1. Planning and Direction**

The first step to producing actionable threat intelligence is to ask the right question.

The questions that best drive the creation of actionable threat intelligence focus on a single fact, event, or activity — broad, open-ended questions should usually be avoided.

Prioritize your intelligence objectives based on factors like how closely they adhere to your organization's core values, how big of an impact the resulting decision will have, and how time sensitive the decision is.

One important guiding factor at this stage is understanding who will consume and benefit from the finished product — will the intelligence go to a team of analysts with technical expertise who need a quick report on a new exploit, or to an executive that's looking for a broad overview of trends to inform their security investment decisions for the next quarter?

### **2. Collection**

The next step is to gather raw data that fulfills the requirements set in the first stage. It's best to collect data from a wide range of sources — internal ones like network event logs and records of past incident responses, and external ones from the open web, the dark web, and technical sources.

Threat data is usually thought of as lists of IoCs, such as malicious IP addresses, domains, and file hashes, but it can also include vulnerability information, such as the personally identifiable information of customers, raw code from paste sites, and text from news sources or social media.

### **3. Processing**

Once all the raw data has been collected, you need to sort it, organizing it with metadata tags and filtering out redundant information or false positives and negatives.

Today, even small organizations collect data on the order of millions of log events and hundreds of thousands of indicators every day. It's too much for human analysts to process efficiently — data collection and processing has to be automated to begin making any sense of it.

Solutions like SIEMs are a good place to start because they make it relatively easy to structure data with correlation rules that can be set up for a few different use cases, but they can only take in a limited number of data types.

If you're collecting unstructured data from many different internal and external sources, you'll need a more robust solution. Recorded Future uses machine learning and natural language processing to parse text from millions of unstructured documents across seven different languages and classify them using language-independent ontologies and events, enabling

analysts to perform powerful and intuitive searches that go beyond bare keywords and simple correlation rules.

#### **4. Analysis**

The next step is to make sense of the processed data. The goal of analysis is to search for potential security issues and notify the relevant teams in a format that fulfills the intelligence requirements outlined in the planning and direction stage.

Threat intelligence can take many forms depending on the initial objectives and the intended audience, but the idea is to get the data into a format that the audience will understand. This can range from simple threat lists to peer-reviewed reports.

#### **5. Dissemination**

The finished product is then distributed to its intended consumers. For threat intelligence to be actionable, it has to get to the right people at the right time.

It also needs to be tracked so that there is continuity between one intelligence cycle and the next and the learning is not lost. Use ticketing systems that integrate with your other security systems to track each step of the intelligence cycle — each time a new intelligence request comes up, tickets can be submitted, written up, reviewed, and fulfilled by multiple people across different teams, all in one place.

#### **6. Feedback**

The final step is when the intelligence cycle comes full circle, making it closely related to the initial planning and direction phase. After receiving the finished intelligence product, whoever made the initial request reviews it and determines whether their questions were answered. This drives the objectives and procedures of the next intelligence cycle, again making documentation and continuity essential.

### **The Types of Threat Intelligence**

As demonstrated by the threat intelligence lifecycle, the final product will look different depending on the initial intelligence requirements, sources of information, and intended audience. It can be helpful to break down threat intelligence into a few categories based on these criteria.

Threat intelligence is often broken down into three subcategories:

- Strategic — Broader trends typically meant for a non-technical audience
- Tactical — Outlines of the tactics, techniques, and procedures of threat actors for a more technical audience
- Operational — Technical details about specific attacks and campaigns

#### **Strategic Threat Intelligence**

Strategic threat intelligence provides a broad overview of an organization's threat landscape. It's intended to inform high-level decisions made by executives and other decision makers at an organization — as such, the content is generally less technical and is presented through reports or briefings. Good strategic intelligence should provide insight into areas like the risks associated with certain lines of action, broad patterns in threat actor tactics and targets, and geopolitical events and trends.

Common sources of information for strategic threat intelligence include:



- Policy documents from nation-states or nongovernmental organizations
- News from local and national media, industry- and subject-specific publications, or other subject-matter experts
- White papers, research reports, and other content produced by security organizations

Producing strong strategic threat intelligence starts with asking focused, specific questions to set the intelligence requirements. It also takes analysts with expertise outside of typical cybersecurity skills — in particular, a strong understanding of sociopolitical and business concepts.

Although the final product is non-technical, producing effective strategic intelligence takes deep research through massive volumes of data, often across multiple languages. That can make the initial collection and processing of data too difficult to perform manually, even for those rarified analysts who possess the right language skills, technical background, and tradecraft. A threat intelligence solution that automates data collection and processing helps reduce this burden and allows analysts who do not have as much expertise to work more effectively.

### **Tactical Threat Intelligence**

Tactical threat intelligence outlines the tactics, techniques, and procedures (TTPs) of threat actors. It should help defenders understand, in specific terms, how their organization might be attacked and the best ways to defend against or mitigate those attacks. It usually includes technical context, and is used by personnel directly involved in the defense of an organization, such as system architects, administrators, and security staff.

Reports produced by security vendors are often the easiest way to get tactical threat intelligence. Look for information in reports about the attack vectors, tools, and infrastructure that attackers are using, including specifics about what vulnerabilities are being targeted and what exploits attackers are leveraging, as well as what strategies and tools that they may be using to avoid or delay detection.

Tactical threat intelligence should be used to inform improvements to existing security controls and processes and speed up incident response. Because many of the questions answered by tactical intelligence are unique to your organization, and need to be answered on a short deadline — for example, “Is this critical vulnerability being exploited by threat actors targeting my industry present in my systems?” — having a threat intelligence solution that integrates data from within your own network is crucial.

### **Operational Threat Intelligence**

Operational intelligence is knowledge about cyber attacks, events, or campaigns. It gives specialized insights that help incident response teams understand the nature, intent, and timing of specific attacks.

Because this usually includes technical information — information like what attack vector is being used, what vulnerabilities are being exploited, or what command and control domains are being employed — this kind of intelligence is also referred to as technical threat intelligence. A common source of technical information is threat data feeds, which usually focus on a single type of indicator, like malware hashes or suspicious domains.

But if technical threat intelligence is strictly thought of as deriving from technical information like threat data feeds, then technical and operational threat intelligence are not totally synonymous — more like a Venn diagram with huge overlaps. Other sources of information on specific

attacks can come from closed sources like the interception of threat group communications, either through infiltration or breaking into those channels of communication.

Consequently, there are a few barriers to gathering this kind of intelligence:

**Access** — Threat groups may communicate over private and encrypted channels, or require some proof of identification. There are also language barriers with threat groups located in foreign countries.

**Noise** — It can be difficult or impossible to manually gather good intelligence from high-volume sources like chat rooms and social media.

**Obfuscation** — To avoid detection, threat groups might employ obfuscation tactics like using codenames.

Threat intelligence solutions that rely on machine learning processes for automated data collection on a large scale can overcome many of these issues when trying to develop effective operational threat intelligence. A solution that uses natural language processing, for example, will be able to gather information from foreign-language sources without needing human expertise to decipher it.

## **Machine Learning for Better Threat Intelligence**

Data processing takes place at a scale today that requires automation to be comprehensive. Combine data points from many different types of sources — including open, dark web, and technical sources — to form the most robust picture possible.

Recorded Future uses machine learning techniques in four ways to improve data collection and aggregation — to structure data into categories, to analyze text across multiple languages, to provide risk scores, and to generate predictive models.

### **1. To structure data into entities and events**

Ontology has to do with how we split concepts up and how we group them together. In data science, ontologies represent categories of entities based on their names, properties, and relationships to each other, making them easier to sort into hierarchies of sets. For example, Boston, London, and Gothenburg are all distinct entities that will also fall under the broader “city” entity.

If entities represent a way to sort physically distinct concepts, then events sort concepts over time. Recorded Future events are language independent — something like “John visited Paris,” “John took a trip to Paris,” “Джон прилетел в Париж,” and “John a visité Paris” are all recognized as the same event.

Ontologies and events enable powerful searches over categories, letting analysts focus on the bigger picture rather than having to manually sort through data themselves.

### **2. To structure text in multiple languages through natural language processing**

With natural language processing, entities and events are able to go beyond bare keywords, turning unstructured text from sources across different languages into a structured database.

The machine learning driving this process can separate advertising from primary content, classify text into categories like prose, data logs, or code, and disambiguate between entities with the same name (like “Apple” the company, and “apple” the fruit) by using contextual clues in the surrounding text.

This way, the system can parse text from millions of documents daily across seven different languages — a task that would require an impractically large and skilled team of human analysts to do. Saving time like this helps IT security teams work 32 percent more efficiently with Recorded Future.

### **3. To classify events and entities, helping human analysts prioritize alerts**

Machine learning and statistical methodology are used to further sort entities and events by importance — for example, by assigning risk scores to malicious entities.

Risk scores are calculated through two systems: one driven by rules based on human intuition and experience, and the other driven by machine learning trained on an already vetted dataset.

Classifiers like risk scores provide both a judgment (“this event is critical”) and context explaining the score (“because multiple sources confirm that this IP address is malicious”).

Automating how risks are classified saves analysts time sorting through false positives and deciding what to prioritize, helping IT security staff who use Recorded Future spend 34 percent less time compiling reports.

### **4. To forecast events and entity properties through predictive models**

Machine learning can also generate models that predict the future, oftentimes much more accurately than any human analysts, by drawing on the deep pools of data previously mined and categorized.

This is a particularly strong “law of large numbers” application of machine learning — as we continue to draw on more sources of data, these predictive models will become more and more accurate.

## **Threat Intelligence Use Cases**

The diverse use cases of threat intelligence make it an essential resource for cross-functional teams in any organization. Although it’s perhaps the most immediately valuable when it helps you prevent an attack, threat intelligence is also a useful part of triage, risk analysis, vulnerability management, and wide-scope decision making.

MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s attack lifecycle and the platforms they are known to target.

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of cybersecurity threats. They’re displayed in matrices that are arranged by attack stages, from initial system access to data theft or machine control. There are matrices for common desktop platforms—Linux, macOS and Windows, technologies like cloud, containers, network, ICS, and mobile platforms.

## Tactics in the ATT&CK Framework

ATT&CK stands for adversarial tactics, techniques, and common knowledge. The tactics are a modern way of looking at cyberattacks. Rather than looking at the results of an attack, aka an indicator of compromise (IoC), it identifies tactics that indicate an attack is in progress. Tactics are the “why” of an attack technique.

The Enterprise ATT&CK matrix (learn about all three matrices below) has 14 tactics:

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Command & Control
12. Collection
13. Exfiltration
14. Impact

What are Techniques in the ATT&CK Framework?

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	Inject, profile and hijack	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Command and Control
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Search History	Application Writer Discovery	Application Deployment Software	Account Collection	Data Compromise	Communication Through Removable Media
Hardware Addition	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Stow-Force	Browser Malware Discovery	Distributed Component Object Model	Clipboard Data	Data Exfiltration	Connection Away
Replicator Through Removable Media	Corrupted HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppCert DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	User Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local Systems	Exfiltration Over Command and Control Channel	Data Blocking

Figure 2: The Mitre Enterprise ATT&CK Matrix shows the tactics in an attack across the top, and individual techniques down each column.

## MITRE ATT&CK Framework

The second “T” in ATT&CK stands for techniques. Each tactic includes a set of techniques that have been seen used by malware and threat actors. Techniques represent the “how”—how attackers carry out a tactic in practice. For example, if the tactic is privilege escalation, the techniques will be various ways attackers carry out privilege escalation in real world attacks.

There are currently 185 techniques and 367 sub-techniques in the Enterprise ATT&CK matrix, and Mitre continuously adds more. Each technique has a four-digit code—for example, Abuse Elevation Control Mechanism is T1548.

Each technique contains specific information about how threat actors operate, such as the privileges required, the platforms on which the technology is commonly used, and how to detect commands or activities **associated with the technique**.

### **Common Knowledge in the ATT&CK Framework**

The “CK” at the end of ATT&CK stands for common knowledge. This is the documented use of tactics and techniques by adversaries. Essentially, common knowledge is the documentation of procedures. Those familiar with cybersecurity may be familiar with the term “tactics, techniques, and procedures,” or TTP. (The “CK” makes for a sexier acronym than “P”— always a must in government projects.)

### **Who is MITRE?**

MITRE is a government-funded research organization based in Bedford, MA, and McLean, VA. The company was spun out of MIT in 1958 and has been involved in a range of commercial and top secret projects for a range of agencies. These included the development of the FAA air traffic control system and the AWACS airborne radar system. MITRE has a substantial cybersecurity practice funded by the National Institute of Standards and Technology (NIST).

(Interestingly, MITRE is not an acronym, though some thought it stood for Massachusetts Institute of Technology Research and Engineering. The name is the creation of James McCormack, an early board member, who wanted a name that meant nothing, but sounded evocative.)

### **The Goal of MITRE ATT&CK**

The goal of the Mitre security initiative is to create a comprehensive list of known adversary tactics and techniques used during a cyberattack. Open to government, education, and commercial organizations, it should be able to collect a wide, and hopefully exhaustive, range of attack stages and sequences. MITRE ATT&CK is intended to create a standard taxonomy to make communications between organizations more specific.

ATT&CK was created out of a need to systematically categorize adversary behavior as part of conducting structured adversary emulation exercises within MITRE’s Fort Meade Experiment research environment.

### **The ATT&CK Matrices**

There are three matrices in the ATT&CK framework:

**Enterprise ATT&CK** – an adversary model that explains actions an attacker can take to operate inside a corporate network. It mainly focuses on post-compromise behavior. This matrix can help prioritize network defense, explaining the tactics, techniques, and procedures (TTPs) attackers use once inside the network.

**PRE-ATT&CK** – this matrix focuses on activities performed before an attack, largely outside the organization’s view. It helps security teams understand how attacker perform reconnaissance and select their point of entry, and makes it possible to more effectively monitor and identify attacker activities outside the boundaries of the corporate network.

**Mobile ATT&CK** – based on the NIST Mobile Threat Catalogue, this is a threat model describing tactics and techniques attackers can use to infiltrate mobile devices. These include “network-based effects”, attack methods which can be performed without direct access to the device.

### How Do You Use the ATT&CK Matrix?

The MITRE ATT&CK Matrix visually arranges all known tactics and techniques into an easy to understand format. Attack tactics are shown across the top, and individual techniques are listed down each column.

In the Enterprise ATT&CK matrix, an attack sequence would involve at least one technique per tactic, and a completed attack sequence would be built by moving from left (Initial Access) to right (Command and Control). It is possible for multiple techniques to be used for one tactic. For example, an attacker might try both an attachment and a link in a spear phishing exploit.

Figure 2: The Mitre Enterprise ATT&CK Matrix shows the tactics in an attack across the top, and individual techniques down each column.

It’s not necessary for an attacker to use all eleven tactics across the top of the matrix. Rather, the attacker will use the minimum number of tactics to achieve their objective, as it’s more efficient and provides less chance of discovery. In this attack (shown in Figure 3), the adversary performs Initial Access to the credentials of the CEO’s administrative assistant using a spear phishing link delivered in an email. Once they have the admin’s credentials, the attacker will look for a remote system in the Discovery stage.

Figure 3 shows an example attack with techniques from each tactical stage of the attack.

What is the MITRE ATT&CK Framework?

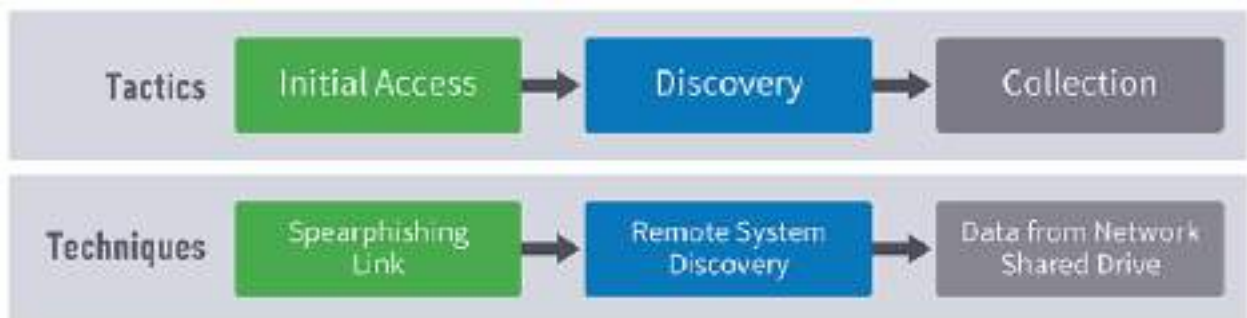


Figure 3: A simple attack to steal sensitive files from the CEO can be accomplished in three steps using three tactics and techniques.

Let’s assume that they’re after sensitive data in a Dropbox folder to which the admin also has access, so there is no need to escalate privileges. Collection, which is the last stage, is performed by downloading files from Dropbox to the attacker’s machine.

Note that if using behavior analytics, a security analyst might detect the attack in process by identifying anomalous user behavior. For example, let’s say the admin clicked a link that no one in the company has ever clicked before, then the admin accessed a particular Dropbox folder at an unusual time. During the final stage of the attack, the attacker’s computer accessed the Dropbox folder for the first time. With behavioral analytics, these activities would be flagged as suspicious user behavior.

## How Does MITRE ATT&CK Compare to Lockheed Martin's Cyber Kill Chain?

Lockheed Martin's Cyber Kill Chain® and ATT&CK resemble each other in that both are models that define the steps an attacker uses to achieve their goal. Lockheed Martin's Cyber Kill Chain identifies seven steps in an attack:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control
7. Actions on objectives

ATT&CK has ten steps that make up an attack chain:

1. Initial access
2. Execution
3. Persistence
4. Privilege escalation
5. Defense evasion
6. Credential access
7. Discovery
8. Lateral movement
9. Collection and exfiltration
10. Command and control

In addition to more granularity in the attack chain tactics, ATT&CK delineates the techniques that can be used in each stage, whereas Lockheed Martin's Cyber Kill Chain does not.

What Can Be Done with MITRE ATT&CK?

There are a number of ways an organization can use MITRE ATT&CK. Here are the primary use cases.

**Adversary Emulation** – ATT&CK can be used to create adversary emulation scenarios to test and verify defenses against common adversary techniques.

**Red Teaming** – ATT&CK can be used to create red team plans and organize operations to avoid certain defensive measures that may be in place within a network.

**Behavioral Analytics Development** – ATT&CK can be used to construct and test behavioral analytics to detect adversarial behavior within an environment.

**Defensive Gap Assessment** – ATT&CK can be used as a common behavior-focused adversary model to assess tools, monitoring, and mitigations of existing defenses within an organization's enterprise.

**SOC Maturity Assessment** – ATT&CK can be used as one measurement to determine how effective a SOC is at detecting, analyzing, and responding to intrusions.

**Cyber Threat Intelligence Enrichment** – ATT&CK is useful for understanding and documenting adversary group profiles from a behavioral perspective that is agnostic of the tools the group may use.

**Security Threat**

A security threat is a malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization. A security event refers to an occurrence during which company data or its network may have been exposed.

### Types of security threats

The NIST definition above states that a threat can be an event or a condition. An event, in this case, also includes natural disasters, fire, and power outage. It is a very general concept. In cybersecurity, it is more common to talk about threats such as viruses, trojan horses, denial of service attacks.

Phishing emails is a social engineering threat that can cause, e.g., loss of passwords, credit card numbers and other sensitive data. Threats to information assets can cause loss of confidentiality, integrity or availability of data. This is also known as the CIA triad.

The CIA triad, together with three other well known security concepts, is the basis for the STRIDE threat model. When listing possible threats, it is convenient to use an existing classification as a starting point. STRIDE is the most well-known classification, proposed by Microsoft in 1999. The name comes from the initial letters of the different categories, which also makes it easier to remember them.

Threat	Meaning/Example	Related Security Property
Spoofting identity	An example is to use someone else's password and authenticate as that person.	Authentication
Tampering with data	This includes e.g., modification of data. Either data at rest or data sent over a network.	Integrity
Repudiation	This means that users can deny having performed an action, e.g., sending or receiving data.	Non-repudiation
Information disclosure	This includes a user reading data without granted access, or eavesdropping a communication channel.	Confidentiality
Denial of service	This relates to the availability of a system	Availability
Elevation of privilege	In these types of threats, a less privileged user gets higher privileges. Normal users obtaining root privileges is the most typical and severe form of this	Authorization

### Examples of security threats

Recall that a threat is very general. It does not include how to realize it, or even if it is possible in the current system. Here are a few examples.

- A malicious user reads the files of other users.
- An attacker redirects queries made to a web server to his own web server.
- An attacker modifies the database.
- A remote attacker runs commands on the server.



Each of these examples can easily be mapped to a category in STRIDE. Other examples would be malware, trojans and worms.

### **Related terminology**

There are several other terms that are closely related, but that should not be confused by threat.

**Threat actor or threat agent.** This is the entity that carries out and realizes the threat. This is often instead called attacker or adversary when it is carried out by a person or a group. In that case it is also a deliberate action.

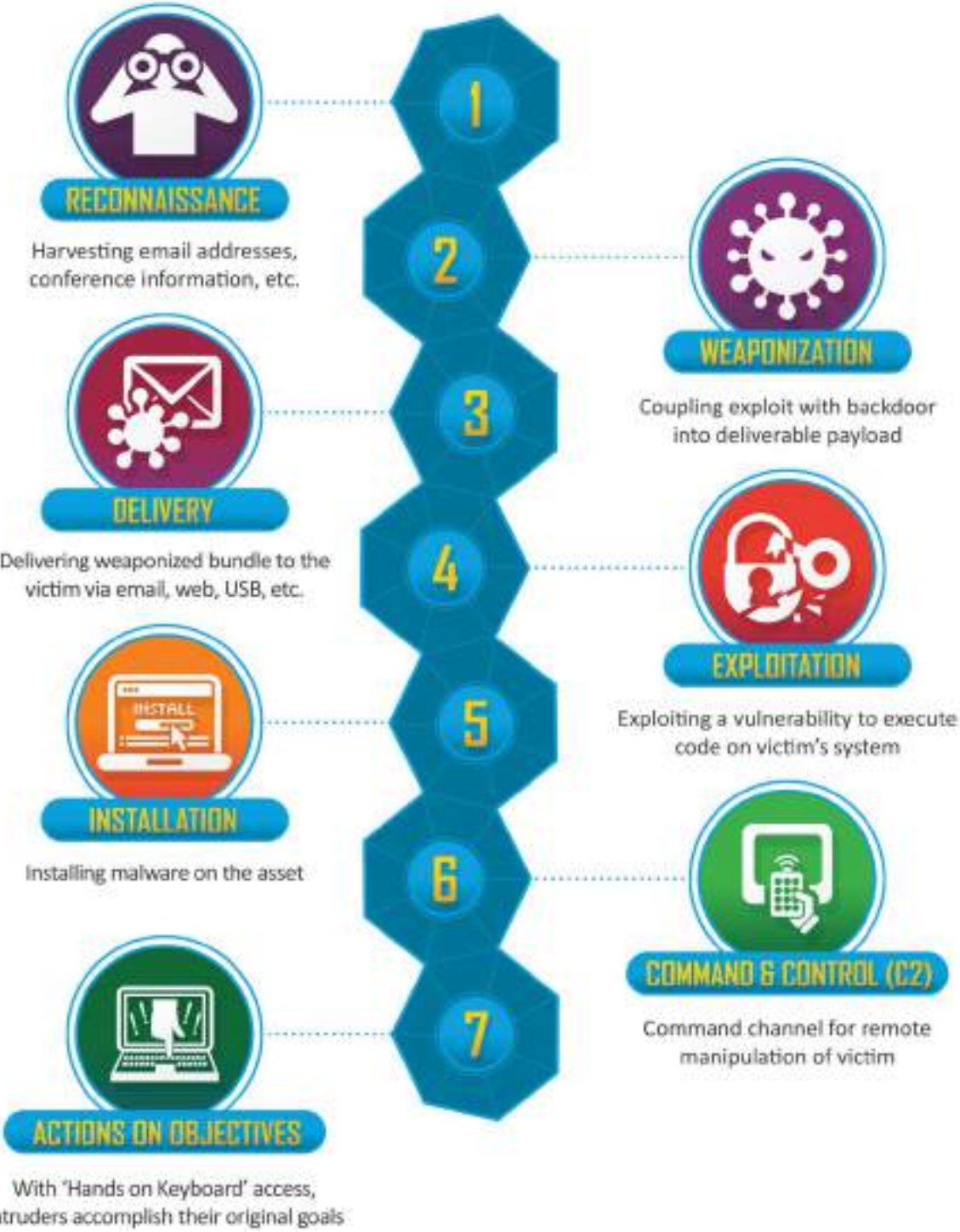
**Threat action.** This is the actual attack, or the realization of a threat. It can take advantage of a vulnerability, but in e.g., the case of natural disaster, it does not have to be an underlying vulnerability that causes the threat to be realized.

**Threat consequence.** This is the actual result when the threat is realized. RFC 4949 lists four main categories of consequences, namely “unauthorized disclosure”, “deception”, “disruption”, and “usurpation”.

The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).

Lockheed Martin derived the kill chain framework from a military model – originally established to identify, prepare to attack, engage, and destroy the target. Since its inception, the kill chain has evolved to better anticipate and recognize insider threats, social engineering, advanced ransomware and innovative attacks.

The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.



## **The Steps of the Cyber Security Kill Chain?**

### **Cyber kill chain model steps**

There are several other cyber kill chain models developed by other companies, but for the sake of simplicity, we're going to stick with the Lockheed Martin model, which is the best-known framework in the industry. We've included explanations as well as brief solutions for each one so you can better understand the process hackers take to breach a target.

#### **Step 1: Reconnaissance**

Like any form of traditional warfare, the most successful cyber attacks start with lots of information gathering. Reconnaissance is the first step in the cyber security kill chain and utilizes many different techniques, tools, and commonly used web browsing features including:

- Search engines
- Web archives
- Public cloud services
- Domain name registries
- WHOIS command
- Packet sniffers (Wireshark, tcpdump, WinDump, etc.)
- Network mapping (nmap)
- DIG command
- Ping
- Port scanners (Zenmap, TCP Port Scanner, etc.)

There is a wide range of tools and techniques used by hackers to gather information about their targets, each of which exposes different bits of data that can be used to find doors into your applications, networks, and databases which are increasingly becoming cloud based. It's important that you secure your sensitive data behind cloud-based SASE defenses, encryption and secure web pages in order to prevent attackers from stumbling on compromising information while browsing through your publicly-accessible assets, including apps and cloud services.

#### **Step 2: Weaponize**

Once an attacker has gathered enough information about their target, they'll choose one or several attack vectors to begin their intrusion into your space. An attack vector is a means for a hacker to gain unauthorized access to your systems and information. Attack vectors range from basic to highly technical, but the thing to keep in mind is that, for hackers, targets are often chosen by assessing cost vs. ROI.

Everything from processing power to time-to-value is a factor that attackers take into account. Typical hackers will flow like water to the path of least resistance, which is why it is so important to consider all possible entry points along the attack surface (all of the total points in which you are susceptible to an attack) and harden your security accordingly.

#### **The most common attack vectors include:**

- Weak or stolen credentials
- Remote access services (RDP, SSH, VPNs)
- Careless employees
- Insider attackers
- Poor or no encryption
- System misconfiguration
- Trust relationships between devices/systems

- Phishing (social engineering)
- Denial of service attacks
- Man-in-the-middle attacks (MITM)
- Trojans
- SQL injection attacks
- And many others

Remember: a hacker only needs one attack vector to be successful. Therefore, your security is only as strong as its weakest point and it's up to you to discover where those potential attack vectors are. Ransomware attacks continue to exploit remote access services to gain entry, make lateral movements, detect sensitive data for exfiltration, all before encrypting and making ransom requests.

So typically once an attacker is in, their next move is to find different ways to move laterally throughout your network or cloud resources and escalate their access privileges so their attack will gather the most valuable information, and they'll stay undetected for as long as possible. Preventing this kind of behavior requires adopting "Zero Trust" principles, which, when applied to security and networking architecture, consistently demands reaffirmation of identity as users move from area to area within networks or applications.

### **Step 3: Delivery**

Now that a hacker has gained access to your systems, they'll have the freedom they need to deliver the payload of whatever they have in store for you (malware, ransomware, spyware, etc.). They'll set up programs for all kinds of attacks, whether immediate, time-delayed or triggered by a certain action (logic bomb attack). Sometimes these attacks are a one-time move and other times hackers will establish a remote connection to your network that is constantly monitored and managed.

Malware detection with Next Gen SWGs to TLS decrypt and inspect web and cloud traffic are key components for preventing the delivery of these types of payloads. Increasingly attacks are cloud delivered with 68% of malware using cloud delivery versus web delivery. Running inline threat scanning services for web and cloud traffic along with accounting for the status of all endpoint devices is crucial in ensuring your company is not infected with any malicious software.

### **Step 4: Exploit**

Once the attacker's intended payload is delivered, the exploitation of a system begins, depending on the type of attack. As mentioned before, some attacks are delayed and others are dependent on a specific action taken by the target, known as a logic bomb. These programs sometimes include obfuscation features in order to hide their activity and origin in order to prevent detection.

Once the executable program is triggered, the hacker will be able to begin the attack as planned, which leads us to the next few steps, encompassing different types of exploitations.

### **Step 5: Install**

If a hacker sees the opportunity for future attacks, their next move is to install a backdoor for consistent access to the target's systems. This way they can move in and out of the target's network without running the risk of detection by reentering through other attack vectors. These kinds of backdoors can be established through rootkits and weak credentials, and so long as their behavior doesn't throw up any red flags to a security team (such as unusual login times or large data movements), these intrusions can be hard to detect. SASE architecture is uniting

security defenses to collect rich metadata on users, devices, apps, data, activity and other attributes to aid investigations and enhance anomaly detection.

### **Step 6: Callback**

Now that the programs and backdoors are installed, an attacker will take control of systems and execute whatever attack they have in store for you. Any actions taken here are solely for the purpose of maintaining control of their situation with the target, which can take all kinds of forms, such as planting ransomware, spyware, or other means for exfiltrating data in the future.

Unfortunately, once you learn of an intrusion and exfiltration, it is probably too late—the hackers have control of your system. That's why it's important to have safeguards that monitor and evaluate data movements for any suspicious activity. A machine is far more likely to detect and prevent malicious behavior faster than any network administrator.

### **Step 7: Persist**

Everything has led to this. This is the continuous execution stage where an attacker takes action on their target and may encrypt your data for ransom, exfiltrate your data for monetary gain, bring down your network via denial of service, or monitor your system behaviors for any other openings via spyware, to name just a few potential outcomes. Espionage and monitoring are leading actions in this last kill chain step where attackers keep a low profile and persist.

This is where real-time monitoring of data movement and suspicious behavior detection is crucial because attackers will move as quickly as possible to achieve their goals. There is never enough time to react to every possible anomaly within a large corporate structure so your role in prevention must be proactive instead of reactive.

### **Putting the Cyber Security Kill Chain Steps into Practice**

You should now have a rudimentary understanding of the common kill chain stages your company faces, and it's up to you to fill in the gaps in your security strategy. While these steps were originally developed with traditional, perimeter-focused security in mind, many of these steps are used by insider attackers as well, with techniques including privilege escalation, shoulder surfing, SQL injections, and many others.

There are all kinds of reasons for attacks, including financial, political—even just for fun and recognition. Understanding what motivations an attacker might have for targeting your company will help you plan for potential attack vectors.

When developing your defense strategies, it's important to look at all possible weak points, from your network to the cloud. The good news is that Netskope is uniquely positioned to take on all kinds of insider and outsider threats to your users, apps, data and cloud infrastructure. Learn more about how Netskope can help you prevent data loss and monitor abnormal movements of cloud data today.



### Self-check quiz 4.3

Check your understanding by answering the following questions:

Write the appropriate/correct answer of the following:

1. What is Threat intelligence

Answer:

2. Write down the categories of threat intelligence

Answer:

3. What are Tactics in the ATT&CK Framework?

Answer:

4. What is the MITRE ATT&CK Framework?

Answer:

5. What is the ATT&CK Matrices?

Answer:



## Answer keys

### Answer key 4.1

1. Answer:  
Capacity Management is the continuous and iterative process that monitors, analyses, and evaluates the performance and capacity of the IT infrastructure and, with the data obtained, it optimizes the service or submits an RFC to Change Management.
2. Answer:  
Problem management isn't just about finding and fixing incidents, but identifying and understanding the underlying causes of an incident as well as identifying the best method to eliminate that root cause. Moreover, pinpointing the cause has no value to an organization if it's a cut-off process completed by a siloed team, so problem management should be constant and widely practiced across multiple teams, including IT, security, and software developers.
3. Answer:  
problem management process. Such as:
  1. **Problem detection** - Proactively find problems so they can be fixed, or identify workarounds before future incidents happen.
  2. **Categorization and prioritization** - Track and assess known problems to keep teams organized and working on the most relevant and high-value problems.
  4. **Investigation and diagnosis** - Identify the underlying contributing causes of the problem and the best course of action for remediation.
  5. **Create a known error record** - In ITIL, a known error is "a problem that has a documented root cause and a workaround." Recording this information leads to less downtime if the problem triggers an incident. This is typically stored in a document called a known error database.
  6. **Create a workaround, if necessary** - A workaround is a temporary solution for reducing the impact of problems and keeping them from becoming incidents. These aren't ideal, but they can limit business impact and avoid a customer-facing incident if the problem can't be easily identified and eliminated.

**Resolve and close the problem** - A closed problem is one that has been eliminated and can no longer cause another incident

### Answer key: 4.2

1. Answer:  
An incident is an unexpected disruption to a service. It disturbs the normal operation thus affecting end user's productivity. An Incident may be caused due to an asset that is not functioning properly or network failure
2. Answer:  
  
The five-step process for security incident management, including:
  1. Prepare for handling incidents.
  2. Identify potential security incidents through monitoring and report all incidents.

3. Assess identified incidents to determine the appropriate next steps for mitigating the risk.
4. Respond to the incident by containing, investigating, and resolving it (based on outcome of step 3).
5. Learn and document key takeaways from every incident.

### Answer key 4.3

1. What is Threat intelligence

Answer: Threat intelligence, also known as cyber threat intelligence (CTI), is information gathered from a range of sources about current or potential attacks against an organization. The information is analyzed, refined and organized and then used to minimize and mitigate cybersecurity risks.

2. Write down the categories of threat intelligence

Answer: Threat intelligence is often broken down into three subcategories:

- Strategic — Broader trends typically meant for a non-technical audience
- Tactical — Outlines of the tactics, techniques, and procedures of threat actors for a more technical audience
- Operational — Technical details about specific attacks and campaigns

3. What are Tactics in the ATT&CK Framework?

Answer: ATT&CK stands for adversarial tactics, techniques, and common knowledge. The tactics are a modern way of looking at cyberattacks. Rather than looking at the results of an attack, aka an indicator of compromise (IoC), it identifies tactics that indicate an attack is in progress. Tactics are the “why” of an attack technique.

4. What is the MITRE ATT&CK Framework?

Answer: The second “T” in ATT&CK stands for techniques. Each tactic includes a set of techniques that have been seen used by malware and threat actors. Techniques represent the “how”—how attackers carry out a tactic in practice

5. What are the ATT&CK Matrices?

There are three matrices in the ATT&CK framework

1. Enterprise ATT&CK
2. PRE-ATT&CK
3. Mobile ATT&CK



<b>LEARNER JOB SHEET 3</b>			
<b>Qualification:</b>	Information System Security Management		
<b>Learning unit:</b>	Perform Incidents Management		
<b>Learner name:</b>			
<b>Personal protective equipment (PPE):</b>			
<b>Materials:</b>			
<b>Tools and equipment:</b>			
<b>Performance criteria:</b>	<ol style="list-style-type: none"> <li>1. Incidents Management is interpreted.</li> <li>2. Security incident management process is interpreted.</li> <li>3. Security incidents are analyzed.</li> <li>4. Learnt lessons from particular incident are documented.</li> <li>5. Documents are prepared as per standard procedure.</li> </ol>		
<b>Measurement:</b>			
<b>Notes:</b>			
<b>Procedure:</b>	<ol style="list-style-type: none"> <li>1. Collect PPE, tools, equipment and materials</li> <li>2. Check the usability of PPE, tools, equipment and materials.</li> <li>3. Identify potential security incident by monitoring.</li> <li>4. Assess identified incidents to determine the appropriate next steps for mitigating the risk</li> <li>5. Respond to the incident by containing, investigating, and resolving it</li> <li>6. Prepare report and document key takeaways from every incident</li> </ol>		
<b>Learner signature:</b>		<b>Date:</b>	
<b>Assessor signature:</b>		<b>Date:</b>	
<b>Quality Assurer signature:</b>		<b>Date:</b>	
<b>Assessor remarks:</b>			
<b>Feedback:</b>			

## Module 5: Perform Information Security Operations

---



**MODULE CONTENT** module covers

**Module Descriptor:** This module covers the knowledge, skills, and attitudes required to Perform Information security operations. It specifically includes analyzing business and system requirements, interpreting secure software architecture, performing security measures on software and interpreting database and container security

**Nominal Duration:** 60 hours



**LEARNING OUTCOMES:**

Upon completion of the module, the trainee should be able to:

1. Analyze business and system requirements
2. Interpret Secure software architecture
3. Perform security measures on software
4. Interpret Database and container security



**PERFORMANCE CRITERIA:**

1. Business requirements are interpreted.
2. Business requirement analysis is Performed.
3. Business requirement document is prepared and submitted as per workplace standard.
4. System requirements are interpreted as per business requirements.
5. System requirement analysis is performed.
6. Threat modeling is interpreted.
7. Threat modeling is performed.
8. Software security architecture is interpreted.
9. Software security core concepts are interpreted.
10. Secured coding practices are interpreted.
11. Code risks are interpreted.
12. Software security testing is performed using testing tools.
13. Software life cycle security is interpreted.
14. Database terminologies are interpreted.
15. Database security is interpreted.
16. Container is interpreted.
17. Container security is described.



## Learning Outcome 5.1 Analyze business and system requirements



Contents:

- Business requirements
- System requirements.



Assessment criteria:

1. Business requirements are interpreted.
2. Business requirement analysis is Performed.
3. Business requirement document is prepared and submitted as per workplace standard.
4. System requirements are interpreted as per business requirements.
5. System requirement analysis is performed.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (actual or simulated)
- Network devices, required tools, equipments and materials.



### LEARNING ACTIVITY 5.1

Learning Activity	Resources/Special Instructions/References
Analyze business and system requirements	<ul style="list-style-type: none"> <li>▪ Information Sheet: 5.1</li> <li>▪ Self-Check: 5.1</li> <li>▪ Answer Key: 5.1</li> </ul>



## Information sheet 5.1

Learning Objective: to analyze business and system requirements.

Business requirements are the critical activities of an enterprise that must be performed to meet the organizational objective(s) while remaining solution independent. A business requirements document (BRD) details the business solution for a project including the documentation of customer needs and expectations.

### **Business requirement analysis**

Business requirement analysis is a process in which the expectations and requirements of the users and stakeholders of a project or task are defined. The analysis of business needs is a comprehensive statement of what the outcome of a project or task should be.

This document contains a step-by-step procedure to record all requirements related to a project or task. Good requirements are defined in such a way that they can be documented and are useful and measurable

In general, the Business Requirements Analysis consist of three activities. The first is identifying the requirements of the various stakeholders.

Next is the analysis of the requirements. During that stage, they analyse whether the requirements are unambiguous, complete, and consistent. The final step is tracking and monitoring the requirements. That part of the process goes on for as long as the project does.

### **Functional and non-functional requirements**

In software development and systems engineering, functional requirements are different functions of a system or component. Functional requirements include calculations, technical details, processing, and other specific functionalities.

Non-functional requirements are generally quality requirements. Quality requirements can impose limitations to a design or implementation, for instance related to reliability or security.

The plan for functional requirements is recorded in the system design. The quality requirements are generally included in the system architecture plan.

### **Identifying requirements**

There are a number of proven methods for collecting information for the Business Requirements Analysis. Some of the most effective methods are explained below.

#### **Brainstorming**

In relatively little time, brainstorming can generate a lot of ideas on a certain topic. Try to have as many people from different disciplines as possible, but avoid groups larger than fifteen people to maintain focus. Use whiteboards or drawings to get ideas flowing.

#### **Interviews**

Interviewing people who are involved in a certain project is a very effective way of obtaining information that might not always be shared in a group setting. It's important that the right people with the right knowledge are interviewed. Ask the questions in an open format, so that respondents give complete answers.

#### **Prototyping**

If it's about the development of a new product or service, you can build a prototype. This makes it easier to visualise what the eventual design will look like. Prototypes often bring issues to light that have to be resolved before introducing the final design.

Business Requirements Analysis step-by-step plan

Identifying business requirements might sound simple, but a thorough analysis includes at least the following four steps:

## 1. Identify stakeholders

Learn everything about the stakeholders of the project, such as sponsors, end users, and others. It's essential to identify sponsors or investors who have decision-making power. Their ideas and needs will strongly influence the process.

## 2. Identify all requirements

Requirements are either known or unknown. Identify as many of them as you can. Collecting the needs is not easy; it requires a critical approach. It might seem simple to collect information from users and document it.

However, recording accurate and organised information is a challenge. Information about needs and requirements is exchanged in different ways, such as through email, interviews, phone calls, meetings, etc. Interpreting, documenting, and processing this information is quite time consuming.



There are also other techniques and requirements to be identified, such as flow charts, competition analyses, and user cases.

## 3. Classify company requirements

During this step of the business requirements analysis, requirements are organised, documented, and refined. The product of this step-by-step plan is considered to be a contract for the project or task to be carried out, concluded between the principal and the agent.

When developing software, the key is to document all functionality requirements of the end user in a very detailed way. Developers have to be able to grasp these requirements to be able to develop the new solution.

## 4. Analyse business requirements

Identify the [highest priorities](#) and determine which requirements are feasible, and which aren't. If problems arise with two requirements because of conflicts of interests or something else, those will have to be resolved. Try to predict the impact of the proposed changes as accurately as possible.

The final list must be clear, succinct, logical, feasible, and relevant to the project.

## 5. Document & monitor

Now that the business requirements are fully known, it's time to develop a rulebook. This document contains all information about stakeholders and their requirements, what they want to achieve, etc. It's also important that stakeholders are kept informed of project developments during the project.

The most common objectives of the BRD are:

To gain agreement with stakeholders

To provide a foundation to communicate to a technology service provider what the solution needs to do to satisfy the customer's and business' needs

To provide input into the next phase for this project

To describe what not how the customer/business needs will be met by the solution

The BRD is important because it is the foundation for all subsequent project deliverables, describing what inputs and outputs are associated with each process function. The process function delivers CTQs (critical to quality). CTQs deliver the voice of customer (VOC). The BRD describes what the system would look like from a business perspective.

Who Should Be Involved in the Creation of the BRD?

A number of teams and partners should create the BRD:

- Project core team
- Business partner(s)
- Process owner(s) or representatives
- Subject matter experts
- Change/project/product management, quality department and/or IT management as needed or available

## **Common Business Obligations for Information Security Requirements**

Organizations today, like yours, understand the need for security. Failure to meet those business obligations can result in operational problems, impacting your organization's ability to function, and could ultimately affect your bottom line. Here are the some common business obligations that you should keep in mind when determining your information security requirements:

### **1. Business Continuity**

The largest obligation that businesses have regarding their information security requirements is the ability to provide continuity for business services in the event that business-as-usual is interrupted by an event (such as the COVID-19 pandemic). Any information security requirements should take business continuity into account.

### **2. End-User Security**

End-user security is another important consideration. This includes end-user security awareness and training to limit end users' exploitability and the ability to remediate any disruptions to end users.

### **3. Risk Management**

Information security risks (threats and vulnerabilities) must be identified, defined, quantified, and managed. This includes the prioritization and rating of the risks to systems and data.

### **4. Security Awareness**

Your new information security program must raise the overall information security awareness of the organization, in order to ensure privacy and security issues are mitigated and given adequate respect and consideration.

### **5. Integration and Interoperability**

The security program you put in place will require well-defined and mature processes and controls that support information security, privacy, and compliance management obligations.

### **6. Data Protection**

The primary expectation is that sensitive or critical information is secured from unauthorized access and disclosure. However, this expectation drives more detailed expectations as well, such as proper access control, encryption, and threat management.

## **7. End-User Ease of Use**

Security controls must be easy for end-users, being sure not to impede their ability to complete their duties. If it impedes their abilities, they're less likely to comply.

## **8. Innovation**

The security strategy you implement must support innovative processes and enable the freedom to use new technologies.

## **9. Confidence and Assurance**

Security controls should support a high level of confidence and assurance to the organization that data is being protected by following industry standard best practices.

## **10. Governance Transparency**

There should be transparency related to security risks and capabilities, including communication of breach and security incident activity to senior management.

## **11. Project Management**

Security analysis and design must be integrated into project management processes, ensuring a risk-based approach is followed while not unduly limiting the ability to initiate or finish projects.

### **Common Regulatory Obligations for Information Security Requirements**

When it comes to your regulatory requirements for your information security considerations, it's important to note that many of these are mandated by either legislation or compliance obligations. Here are the top 8 regulatory obligations to consider:

#### **1. Personal Information Protection and Electronic Documents Act (PIPEDA)**

This regulatory requirement applies to private sector organizations that collect personal information in Canada to ensure the protection of personal information in the course of commercial business. See more.

#### **2. General Data Protection Regulation (GDPR)**

Applying to organizations operating within the EU and any organizations outside the EU who offer goods or services to businesses or individual customers in the EU, GDPR is the EU's data privacy and "right to be forgotten" regulation.

#### **3. Payment Card Industry Data Security Standard (PCI-DSS)**

This regulation applies to any organization that processes, transmits, or stores credit card information, to ensure that cardholder data is protected.

#### **4. Health Insurance Portability and Accountability Act (HIPAA)**

This regulation applies to the healthcare sector and protects the privacy of individually identifiable health information.

## **5. Health Information Technology for Economic and Clinical Health (HITECH)**

This regulation applies to the healthcare sector and widens the scope of privacy and security protections that are available under HIPAA.

## **6. Sarbanes Oxley Act (SOX)**

This regulation applies to public companies that have registered equity or debt securities within the US Securities and Exchange Commission (SEC), to guarantee data integrity against financial fraud, and improve the accuracy of corporate disclosures.

## **7. Gramm-Leach-Bliley Act (GLBA)**

Also known as the Financial Modernization Act of 1999, the Gramm-Leach-Bliley Act applies to the financial sector, and requires financial institutions, including banks and lenders, to explain how they're sharing and protecting the private information of their customers.

## **8. Federal Information Processing Standards (FIPS) 140-2**

This regulation is a Canadian and U.S. government standard that specifies various security requirements for encryption algorithms and document processing, including cryptographic modules.

### **Customer Obligations for Your Information Security Requirements**

Today, most of your customers expect some level of security to be put in place to protect their data. For many organizations, customer data privacy is arguably the biggest reason to develop a mature IT security program. Failing to meet customer requirements could tarnish your organization's reputation. Here are 3 customer obligations to keep in mind:

#### **1. Clear Communication with Business Customers**

Whether it's a B2B or partner relationship, organizations you do business with are expecting their data and their systems to be protected. Consider how your customer security requirements are communicated. Do you include customer security requirements in your Statement of Work (SOW) or Master Service Agreement (MSA)? Do you provide auditing processes or questionnaire-style surveys? Being able to provide clear communication around the customer's requirements will be one way that you can set your organization apart from your competitors.

#### **2. Know Your Business Customers' Security Requirements**

Organizations frequently have "best practices" or, in some cases, industry standard requirements that are placed on them. It's a good practice to understand if your customers are facing these, and what that implies for doing business with them. This will help you to ensure that your organization's information security requirements will match with theirs, and that your businesses are a good fit.

#### **3. Privacy Policy for Consumer Customers**

Consumer customers are customers that are actually consuming your products or services. They expect privacy. It's normal for consumers to expect that their personal information is protected, and they're more likely to buy from companies that they believe will protect that personal information. By putting strong information security requirements in place will only help you to increase your brand recognition as a company that takes consumer privacy seriously.

**Keep your organisation secure with robust information security by following the mandatory requirements and the associated information lifecycle stages explained below.**



Understand what information and ICT systems you need to protect

To implement the right security measures, you need to understand what information you have and how valuable it is.

A comprehensive inventory will assist you to determine what types of information and ICT systems your organisation has, including those that support business continuity and disaster recovery plans.

For each type of information or ICT system, you should record:

- how your organisation (and any providers or partners) uses, processes, shares, or stores it
- any relevant confidentiality, integrity, privacy, or legislative requirements
- how long you need to keep and protect the information
- the minimum level of system performance or information accessibility your organisation needs to function
- what destruction or disposal requirements apply.

### **Understand the value of your information**

You must understand the value, importance, and sensitivity of your information. This will determine the minimum requirements you need to protect it from harm.

Not all information should be treated equally. Some information is more valuable or sensitive, requiring a greater level of protection. The Business Impact Levels (BILs) is a tool that can be used to assess the value of your information and what impact might occur if your information is compromised.

Based on the value of your information and equipment, you will need to classify and assign protective markings to it that will inform your people on how to handle and protect the information from harm. All New Zealand Government agencies must do this in line with the New Zealand Government Security Classification System.

### **Assess the risks to your information security**

You need to think about the vulnerabilities and threats you face and their impact on your organisation. Consider the following questions to help you assess your organisation's risks.

#### **Where is your organisation vulnerable?**

Identify areas where your organisation might be vulnerable to security breaches (deliberate or accidental). Determine which vulnerabilities might be exploited and how this might be limited.

#### **What threats do you face?**

Identify and document the potential threats to your information security and ensure that this information is kept current. Ask yourself, 'Who would benefit from having access to our organisation's information and what information would they want?'

#### **What impact would a security breach have on your organisation?**

Assess how your organisation would be impacted if your information security is breached. Think about the confidentiality, integrity, and availability of your information.

You should also consider these additional questions during your risk assessment:

### **Have you included your supply chain risks?**

Supply chains are becoming deeper and the interconnections more complex. Make sure each part of your organisation's supply chain is included in your risk assessment. Check that your suppliers can articulate who and what they are connected to, and what dependencies they have.

### **Have you factored in the risks from collections of information?**

Collections of information (aggregated information) can be more valuable than the single pieces of information they're made up of, so your organisation might need extra security measures to protect them. Ask yourself, 'What could be deduced if the collection were breached?' Aggregated information includes collections of physical documents and collections of information stored in your ICT systems.

### **Is your existing security enough?**

Analyse your existing security measures. How well would they protect your information against the risks and effects you've identified? If information such as customer records, financial data, and intellectual property were stolen, could you quickly and accurately determine what was lost and be able to recover it? What action do you need to take to improve your security?

**Individual Activity:**

- *Identify* Business requirements.
- *Analyse and prepare* Business requirements document.

**Self-check quiz 5.1**

Check your understanding by answering the following questions:

Write the correct answer for the following questions.

1. What is Business Requirement?

Answer:

2. Why we need to analyse Business requirement?

Answer:

3. How can we identify Business?

Answer:

4. What are the common business obligations for Information Security Requirements?

Answer:

## Learning outcome 5.2 Interpret Secure software architecture



Contents:

- Threat modeling.
- Software security architecture.
- Software security core concepts
- Asset
- Threat agent
- Vulnerabilities



Assessment criteria:

- 1 Threat modeling is interpreted.
- 2 Threat modeling is performed.
- 3 Software security architecture is interpreted.
- 4 Software security core concepts are interpreted.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (Actual or simulated), Server, Necessary software.



### LEARNING ACTIVITY 5.2

Learning Activity	Resources/Special Instructions/References
Interpret Secure software architecture	<ul style="list-style-type: none"><li>▪ Information Sheets: 5.2</li><li>▪ Self-Check: 5.2</li><li>▪ Answer Key: 5.2</li></ul>



## Information sheet 5.2

Learning objective: to interpret Secure software architecture.

A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security.

Threat modelling can be applied to a wide range of things, including software, applications, systems, networks, distributed systems, Internet of Things (IoT) devices, and business processes.

A threat model typically includes:

Description of the subject to be modelled

Assumptions that can be checked or challenged in the future as the threat landscape changes

Potential threats to the system

Actions that can be taken to mitigate each threat

A way of validating the model and threats, and verification of success of actions taken

Threat modelling is a process for capturing, organizing, and analyzing all of this information. Applied to software, it enables informed decision-making about application security risks. In addition to producing a model, typical threat modelling efforts also produce a prioritized list of security improvements to the concept, requirements, design, or implementation of an application.

In 2020 a group of threat modelling practitioners, researchers and authors got together to write the Threat Modelling Manifesto in order to "...share a distilled version of our collective threat modelling knowledge in a way that should inform, educate, and inspire other practitioners to adopt threat modelling as well as improve security and privacy during development". The Manifesto contains values and principles connected to the practice and adoption of Threat Modelling, as well as identified patterns and anti-patterns to facilitate it.

### Objectives of Threat Modelling

Threat modelling is a family of activities for improving security by identifying threats, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device). Threat modelling is a planned activity for identifying and assessing application threats and vulnerabilities.

"Security architecture" is the term used to define the overall system required to protect an organization's IT infrastructure. Such a system includes the specifications, processes, and standard operating procedures (SOPs) involved in preventing, mitigating, and investigating different threats. Just as a building's architectural design instructs engineers how to build a structure, a security architecture defines how personnel should carry out security processes.

### The Components of a Security Architecture

A security architecture is related to existing security policies and guidelines, rather than a standalone system. As such, it consists of more than just firewalls, antivirus/antimalware programs, threat intelligence platforms, VPN software (note that VPNs can be considered part

of security architecture only if their aim is to protect users' privacy), and other security tools and applications that protect a company's network. A good security architecture is a combination of three components, namely:

- Tools
- Processes
- People

**A typical security architecture is quite long as it tackles the following areas:**

**Security protocols:** A security architecture defines in detail the tools and processes used in threat detection and prevention, as well as those used in incident response (the set of instructions that guides IT professionals in dealing with security breaches) and disaster recovery (a detailed plan that allows business processes to resume or continue despite a security incident). For instance, the security architecture might include specific requirements that security software vendors need to fulfill to win a bid. Incident response refers to

**Account creation and management:** The security architecture also includes a guide detailing user account creation, what access to grant to the particular user, and what restrictions to impose. A security architecture must protect the whole IT infrastructure. As such, it should detail who can access sensitive data and who cannot. An accounting staff in charge of payroll processing, for example, should have access to employee timesheets and the payroll management software. Another accounting staff who handles the company's taxes don't necessarily need the same access. Limiting access to tools that contain sensitive data effectively reduces risks.

**Security roles and their responsibilities:** Vital to any security architecture are the people who carry out every step within it. Who is responsible for the day-to-day operations of the security system? Who is in charge of maintaining specific applications and the whole network? Who are the end-users? Who will be the auditor of the overall security architecture? The answers to these questions should be part of the security architecture.

**Auditing the security architecture:** The IT security landscape is continually changing, so there is a need to assess an organization's security architecture regularly. The auditors must make sure that the current architecture is still in line with the business goals and, at the same time, meets its needs. After the assessment, they should make the necessary adjustments to the security architecture.

**Software security**

Software security is the concept of implementing mechanisms in the construction of security to help it remain functional (or resistant) to attacks. This means that a piece of software undergoes software security testing before going to market to check its ability to withstand malicious attacks.

The idea behind software security is building software that is secure from the get-go without having to add additional security elements to add additional layers of security (although in many cases this still happens). The next step is teaching users to use the software in the right manner to avoid being prone or open to attacks.

Software security is critical because a malware attack can cause extreme damage to any piece of software while compromising integrity, authentication, and availability. If programmers take this into account in the programming stage and not afterward, damage can be stopped before it begins.

**There are four main types of IT security that are important to understand when it comes to software security.**

**Network security** – The security between different devices located on the same network. In this case, both software security and hardware security are important. When securing a network, companies look to make sure that their network won't be used maliciously.

**End-point security** – In this situation, security is focused on the devices used. This means that laptops, phones, computers, tablets, etc. are secure (again, both software and hardware) to avoid unwanted users sneaking in. This often involves various methods of encryption, user controls, and of course, software security.

**Internet security** – This is what is commonly known as cybersecurity and deals with the transit and use of information. Cybersecurity attacks happen when information is intercepted and therefore various layers of encryption and authentication are typically used to stop these attacks.

**Cloud security** – Cloud security revolves around lowering software security risks within the cloud. Some of the concepts in cloud security overlap with the other forms of security listed here, in having to secure data transfers, and devices on the same network.

### **Asset**

An asset is any data, device or other component of an organisation's systems that is valuable – often because it contains sensitive data or can be used to access such information.

For example, an employee's desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets.

An organisation's most common assets are information assets. These are things such as databases and physical files – i.e. the sensitive data that you store.

A related concept is the 'information asset container', which is where that information is kept. In the case of databases, this would be the application that was used to create the database. For physical files, it would be the filing cabinet where the information resides.

### **Threat**

A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorised party.

Threats can be categorised as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental.

Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

### **Vulnerability**

A vulnerability is an organisational flaw that can be exploited by a threat to destroy, damage or compromise an asset.

You are most likely to encounter a vulnerability in your software, due to their complexity and the frequency with which they are updated. These weaknesses, known as bugs, can be used by criminal hackers to access sensitive information.

Vulnerabilities don't only refer to technological flaws, though. They can be physical weaknesses, such as a broken lock that lets unauthorised parties into a restricted part of your

premises, or poorly written (or non-existent) processes that could lead to employees exposing information.

Other vulnerabilities include inherent human weaknesses, such as our susceptibility to phishing emails; structural flaws in the premises, such as a leaky pipe near a power outlet; and communication errors, such as employees' sending information to the wrong person.

**Individual Activity:**

- *Interpret Threat Modelling.*



**Self-check quiz 5.2**

Check your understanding by answering the following questions:

1. What is Threat modelling?

Answer:

2. What is Asset?

Answer:

3. What is Threat?

Answer:

4. What is vulnerability?

Answer:





### Learning outcome 5.3 – Perform security measures on software



Contents:

- Secured coding
- Code risks
- Software security testing
- Software life cycle security



Assessment criteria:

- 1 Secured coding practices are interpreted.
- 2 Code risks are interpreted.
- 3 Software security testing is performed using testing tools.
- 4 Software life cycle security is interpreted.



Resources required:

Students/trainees must be provided with the following resources:

Workplace (actual or simulated), class room, trainee handbook and Operating system



### **LEARNING ACTIVITY 5.3**

Learning Activity	Resources/Special Instructions/References
Perform security measures on software	<ul style="list-style-type: none"><li>▪ Information Sheets: 5.3</li><li>▪ Self-Check: 5.3</li><li>▪ Answer Key: 5.3</li></ul>



## Information sheet 5.3

Learning Objective: to perform security measures on software

### Secure coding

Secure coding is a set of practices that applies security considerations to how software will be coded and encrypted to best defend against cyber attack or vulnerabilities. Defects, bugs, and logic flaws are the primary cause of commonly exploited software vulnerabilities, and security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. Secure coding standards introduce safeguards that reduce or eliminate the risk of leaving security vulnerabilities in code.

This is the most critical elements of the software development lifecycle and organizations must develop robust secure coding policies and procedures. It helps to mitigate the vulnerabilities and risks associated with the software product development process.

Secure code review is a manual or automated process that examines an application's source code. The goal of this examination is to identify any existing security flaws or vulnerabilities. Code review specifically looks for logic errors, examines spec implementation, and checks style guidelines, among other activities. Automated code review is a process in which a tool automatically reviews the source code of an application, using a predefined set of rules to look for inferior code. Automated review can find issues in source code faster than identifying them manually. Manual code review involves a human looking at source code, line by line, to find vulnerabilities. Manual code review helps to clarify the context of coding decisions. Automated tools are faster but they cannot take the developer's intentions and general business logic into consideration. Manual review is more strategic and looks at specific issues.

### Security Measures Every Project Manager Should Implement

#### 1. Install an Antivirus



harmful downloads.

First, you must invest on an effective antivirus. Free anti-viruses will only provide the basic level of protection. Go premium and choose a reliable solution provider that offer foolproof security to your projects and business. It acts as the first line of defense against security attacks and prevents them from causing damage to your sensitive data. It takes care of a variety of security threats such as malware, viruses, spyware and adware. Some even offer email protection and prevent

#### 2. Take Regular Backup of Your Data



If you are not taking regular backup of your data, you are risking your data. Make sure that you take frequent backups of your data. It will also help you to protect against one of the most common cyber attacks today, Ransomware. Even if a cyber attack targets your system, you

can easily restore and reclaim your data if you have a backup ready. You can also use a cloud storage to make copies of your data and store it there. Schedule regular backup to protect and keep your data safe otherwise you will have to regret later.

### Install a Firewall



Roland Cloutier, Chief Security Officer for ADP and board member of National Cyber Security Alliance said, “Firewalls are a must to protect your network.” One of the best ways to protect your network is to install a firewall. Although, it is an old technique to secure your network but it is very effective even today. It keeps your network secure by managing internet traffic coming in and going out of the network.

### 3. Use Complex Passwords



According to Microsoft’s password creation guidelines, you should never use any personal data, common words spelled backward and sequence of character and numbers as your password. Security experts suggest that you should use a password that is hard to guess and contains combination of numbers, upper and lower case letters and symbols to make it hack-proof. The ideal length of your passwords should be anywhere around 10-12 characters. If you follow the advice given above, you can

prevent your password from getting in wrong hands.

### 4. Use Encryption Software



Laptops have replaced desktops as the preferred device at workplaces. Just like mobile devices, portability factor puts laptop at a much higher risk of being stolen or lost. Security experts recommend that you use encryption software to encrypt your laptops. Roland Cloutier further suggests that you should never leave your laptop in the car, where it is a soft target for thieves.

### 5. Update Your Software



It is quite unfortunate to see many businesses still using old software and operating system. The problem with that approach is that it makes you more vulnerable to security attacks and many business owners do not realize it. As a project manager, you should ensure that you use good software but more importantly, you should keep them updated to the latest

versions. The advantage of using updated software is that it fixes many bugs and loopholes that a hacker can exploit and protect you from cyber-attacks.

## 6. Secure Mobile Devices



With the proliferation of mobile devices and an increase in their capabilities, they now contain a huge amount of data. You cannot count out the advantages of mobile devices such as portability but you should never ignore the risk attached to it either. They have become prime targets for hackers due to their popularity. Mobile devices are easier to get lost or stolen and securing them is much harder but the amount of data it holds these days forces you to take mobile security seriously. The best way to safeguard your mobile device is to take

advantage of advanced features such as remote wiping, two-way authentication and encryption.

## 7. Protect Wireless Networks



Wireless networks are at a greater risk of cyber attacks as compared to a wired network because of its open nature and comparatively weaker control. Therefore, it is important to pay extra attention towards securing your wireless networks. Use **WPA2** (Wi-Fi Protected Access Version 2) technology to secure your wireless network. If you are still using old technology such as **WEP** (Wired Equivalent Privacy), then switch immediately to latest wireless security because they are much more secure than their older counterparts. You can also add a layer of security by using complex **PSK** (Pre-Shared Key)



## 8. Keep an Eye on Suspicious Activity

Hackers are always one step ahead of the cyber security professionals. They somehow find a way to get inside the most secured system. Even with so many security measures to protect your data, you cannot afford to sit back and relax. As a project manager, you should be on your toes all the time keeping an eye out for suspicious activity in the network. Raise red flags as soon as you notice any suspicious activity and have a counter strategy to deal with such issues.

## 9. Educate Your Team



Probably the most ignored step on this list, most businesses rarely pay attention towards educating their employees about cyber security. Due to this, cyber security attacks are increasing on a daily basis. Despite establishing a secured infrastructure, you end up losing your data. This happens because your employees do not have adequate knowledge. Inform them about the latest

technology trends and security threats.

By educating your team members, you can eliminate the risks of malware and ransomware. Malware can enter your system through multiple channels but one of the most common among them is malicious links, which your employees click. Cyber attackers use social engineering to conduct ransomware attacks. You can easily prevent these common ransomware attacks from harming your systems by creating awareness among your employees. With little education, you can easily prevent that.

### **Code risk**

Code risk encompasses the probability of occurrence for uncertain events and their potential for loss within an organization. Risk management has become an important component of software development as organizations continue to implement more applications across a multiple technology, multi-tiered environment. Typically, software risk is viewed as a combination of robustness, performance efficiency, security and transactional risk propagated throughout the system.

### **Security Testing**

Security Testing is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders. The purpose of Security Tests is to identify all possible loopholes and weaknesses of the software system which might result in a loss of information, revenue, reputation at the hands of the employees or outsiders of the Organization.

### **Types of Security Testing:**

There are seven main types of security testing as per Open Source Security Testing methodology manual. They are explained as follows:

**Vulnerability Scanning:** This is done through automated software to scan a system against known vulnerability signatures.

**Security Scanning:** It involves identifying network and system weaknesses, and later provides solutions for reducing these risks. This scanning can be performed for both Manual and Automated scanning.

**Penetration testing:** This kind of testing simulates an attack from a malicious hacker. This testing involves analysis of a particular system to check for potential vulnerabilities to an external hacking attempt.

**Risk Assessment:** This testing involves analysis of security risks observed in the organization. Risks are classified as Low, Medium and High. This testing recommends controls and measures to reduce the risk.

**Security Auditing:** This is an internal inspection of Applications and Operating systems for security flaws. An audit can also be done via line by line inspection of code

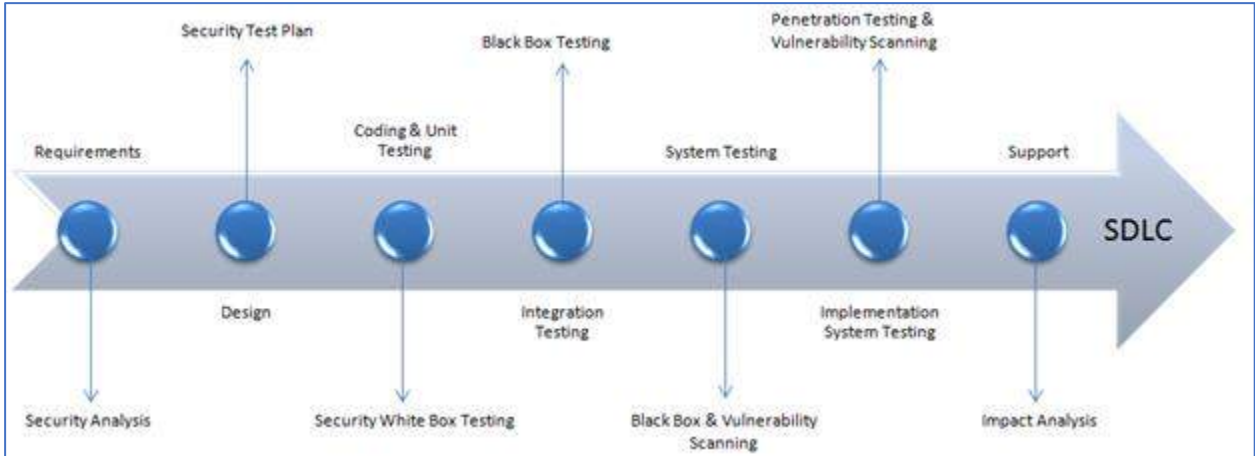
**Ethical hacking:** It's hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.

**Posture Assessment:** This combines Security scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.

**How to do Security Testing**

It is always agreed, that cost will be more if we postpone security testing after software implementation phase or after deployment. So, it is necessary to involve security testing in the SDLC life cycle in the earlier phases.

Let's look into the corresponding Security processes to be adopted for every phase in SDLC



SDLC Phases	Security Processes
Requirements	Security analysis for requirements and check abuse/misuse cases
Design	Security risks analysis for designing. Development of Test Plan including security tests
Coding and Unit Testing	Static and Dynamic Testing and Security White Box Testing
Integration Testing	Black Box Testing
System Testing	Black Box Testing and Vulnerability scanning
Implementation	Penetration Testing, Vulnerability Scanning
Support	Impact analysis of Patches

The test plan should include

- Security-related test cases or scenarios
- Test Data related to security testing
- Test Tools required for security testing
- Analysis of various tests outputs from different security tools

**Methodologies/ Approach / Techniques for Security Testing**

In security testing, different methodologies are followed, and they are as follows:

**Tiger Box:** This hacking is usually done on a laptop which has a collection of OSs and hacking tools. This testing helps penetration testers and security testers to conduct vulnerabilities assessment and attacks.

**Black Box:** Tester is authorized to do testing on everything about the network topology and the technology.

**Grey Box:** Partial information is given to the tester about the system, and it is a hybrid of white and black box models.

## **Security Testing Tool**

### **1) Acunetix**

Intuitive and easy to use, [Acunetix](#) by Invicti helps small to medium-sized organizations ensure their web applications are secure from costly data breaches. It does so by detecting a wide range of web security issues and helping security and development professionals act fast to resolve them.



#### **Features:**

- Advanced scanning for 7,000+ web vulnerabilities, including OWASP Top 10 such as SQLi and XSS
- Automated web asset discovery for identifying abandoned or forgotten websites
- Advanced crawler for the most complex web applications, incl. multi-form and password-protected areas
- Combined interactive and dynamic application security testing to discover vulnerabilities other tools miss
- Proof of exploit provided for many types of vulnerabilities
- DevOps automation through integrations with popular issue tracking and CI/CD tools

### **2) Owasp**

The Open Web Application Security Project (OWASP) is a worldwide non-profit organization focused on improving the security of software. The project has multiple tools to pen test various software environments and protocols. Flagship tools of the project include

- Zed Attack Proxy (ZAP – an integrated penetration testing tool)
- OWASP Dependency Check (it scans for project dependencies and checks against known vulnerabilities)
- OWASP Web Testing Environment Project (collection of security tools and documentation)

### **3) WireShark**

Wireshark is a network analysis tool previously known as Ethereal. It captures packets in real time and displays them in a human-readable format. Basically, it is a network packet analyzer which provides the minute details about your network protocols, decryption, packet information, etc. It is open source and can be used on Linux, Windows, OS X, Solaris, NetBSD, FreeBSD and many other systems. The information that is retrieved via this tool can be viewed through a GUI or the TTY mode TShark Utility.

### **4) W3af**

w3af is a web application attack and audit framework. It has three types of plugins; discovery, audit and attack that communicate with each other for any vulnerabilities in site, for example a discovery plugin in w3af looks for different url's to test for vulnerabilities and forward it to the audit plugin which then uses these URL's to search for vulnerabilities.

The Software Development Life Cycle (SDLC) is a systematic yet standardized approach to developing software applications. SDLC borrows elements heavily from general project management life cycle approaches, as evident from the similarity in the steps and phases involved.

### **Software Development Life Cycle (SDLC)**

The Software Development Life Cycle (SDLC) is a structured process that enables the production of high-quality, low-cost software, in the shortest possible production time. The goal of the SDLC is to produce superior software that meets and exceeds all customer expectations and demands.

Application security is an essential part of developing modern software. As the internet increases in complexity, attackers are turning more and more to known security flaws and vulnerabilities in programs themselves. To avoid data breaches, companies need to build security into all the phases of building, testing, and deploying their software.



One way to plan for this is to examine the software development lifecycle, or SDLC.

Five stages underlie a typical SDLC process:

1. Requirement gathering: Every application is developed to solve certain problems and offer utility to the user. When gathering requirements, the development team aims to understand the needs and goals of the customer and define the resources necessary to complete the project optimally.
2. Design: In this phase, the groundwork for the whole project is laid down. Some of the main details determined here include programming languages, architecture, platforms, user interface, communication protocols and security.



3. Development/build: This is the part where all the planning is put into action by developing the source code of the application, and all the features of the app, including user interface and security, are implemented.
4. Testing: One of the most crucial components of any SDLC process is testing the software for bugs, errors, performance and functionality. Any issues with the performance of the application discovered in this phase are generally rectified before deployment.
5. Deploy and maintain: The application is released for the use of the intended clients. It often involves getting the app approved by the Google Play Store or the App Store and making it available for download. Of course, highly specialized corporate apps are not released on smartphone app stores and are usually directly provided to the client. Now that we've considered SDLC in some detail, it's relatively easy to introduce SSDLC. After all, SSDLC is only a natural progression of SDLC, occurring in response to the rising importance of security in the modern application development landscape.



### Self-check quiz 5.3

Check your understanding by answering the following questions:

- Write the appropriate/correct answer of the following:

1. What is secure coding?

Answer:

2. What is security testing?

Answer

3. Write down the name of some security testing tools.

Answer:

4. What is Software Development Life Cycle (SDLC)?

Answer:



## Learning outcome 5.4 Interpret Database and container security



Contents:

- Database terminologies.
  - DBMS
  - Primary key
  - Foreign key
  - Normalization and de-normalization
  - Database clustering
  - Database backup
- Database security.
- Container security.



Assessment criteria:

- 1 Database terminologies are interpreted.
- 2 Database security is interpreted.
- 3 Container is interpreted.
- 4 Container security is described.



Resources required:

Students/trainees must be provided with the following resources:

Workplace (actual or simulated), class room, trainee handbook and Data center



### LEARNING ACTIVITY 5.4

Learning Activity	Resources/Special Instructions/References
Interpret Database and container security	<ul style="list-style-type: none"> <li>▪ Information Sheets: 5.4</li> <li>▪ Self-Check: 5.4</li> <li>▪ Answer Key: 5.4</li> </ul>



## Information sheet 5.4

Learning Objective: to interpret database and container security

### **Database**

A database is a named collection of tables. A database can also contain views, indexes, sequences, data types, operators, and functions. Other relational database products use the term catalog.

### **DBMS**

A database management system (or DBMS) is essentially nothing more than a computerized data-keeping system. Users of the system are given facilities to perform several kinds of operations on such a system for either manipulation of the data in the database or the management of the database structure itself.

### **Primary Key**

A primary key, also called a primary keyword, is a key in a relational database that is unique for each record. It is a unique identifier, such as a driver license number, telephone number (including area code), or vehicle identification number (VIN). A relational database must always have one and only one primary key.

### **Foreign Key**

A foreign key is a column or columns of data in one table that connects to the primary key data in the original table.

### **Normalization and Denormalization**

Normalization is used to remove redundant data from the database and to store non-redundant and consistent data into it. Denormalization is used to combine multiple table data into one so that it can be queried quickly

### **Database Cluster**

A database cluster is a collection of databases that is managed by a single instance of a running database server. After initialization, a database cluster will contain a database named postgres, which is meant as a default database for use by utilities, users and third party applications.

### **Database backup**

Database backup is the process of backing up the operational state, architecture and stored data of database software. It enables the creation of a duplicate instance or copy of a database in case the primary database crashes, is corrupted or is lost.

### **Command**

A command is a string that you send to the server in hopes of having the server do something useful. Some people use the word statement to mean command. The two words are very similar in meaning and, in practice, are interchangeable.

### **Query**

A query is a type of command that retrieves data from the server.

### **Table (relation, file, class)**

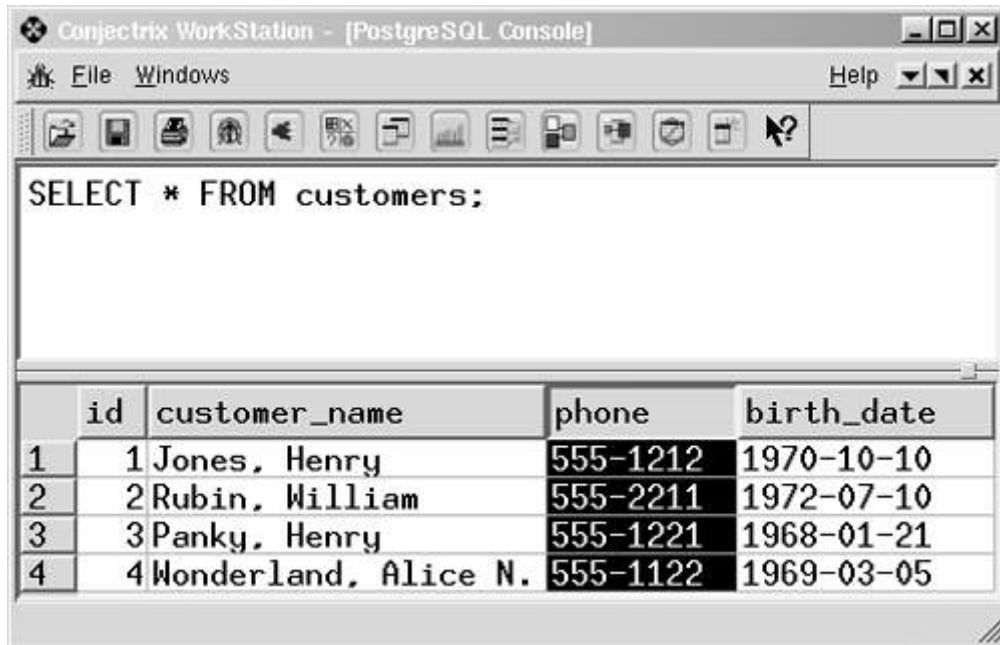
A table is a collection of rows. A table usually has a name, although some tables are temporary and exist only to carry out a command. All the rows in a table have the same shape (in other words, every row in a table contains the same set of columns). In other

database systems, you may see the terms relation, file, or even class?these are all equivalent to a table.

### Column (field, attribute)

A column is the smallest unit of storage in a relational database. A column represents one piece of information about an object. Every column has a name and a data type. Columns are grouped into rows, and rows are grouped into tables. In Figure 1.1, the shaded area depicts a single column.

**Figure 1.1. A column (highlighted).**



```
SELECT * FROM customers;
```

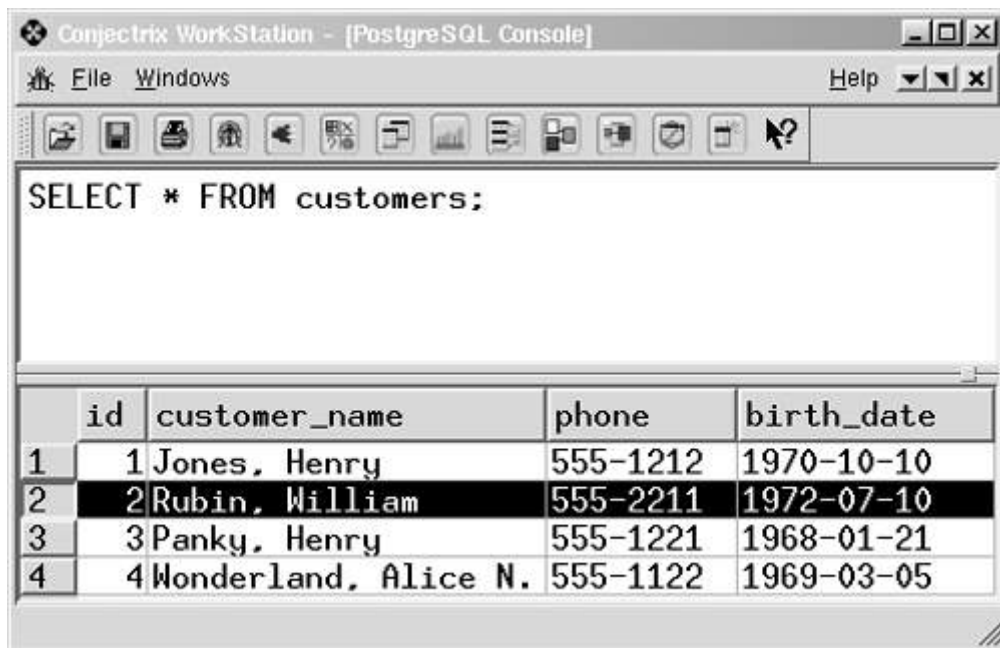
	id	customer_name	phone	birth_date
1	1	Jones, Henry	555-1212	1970-10-10
2	2	Rubin, William	555-2211	1972-07-10
3	3	Panky, Henry	555-1221	1968-01-21
4	4	Wonderland, Alice N.	555-1122	1969-03-05

The terms field and attribute have similar meanings.

### Row (record, tuple)

A row is a collection of column values. Every row in a table has the same shape (in other words, every row is composed of the same set of columns). If you are trying to model a real-world application, a row represents a real-world object. For example, if you are running an auto dealership, you might have a vehicles table. Each row in the vehicles table represents a car (or truck, or motorcycle, and so on). The kinds of information that you store are the same for all vehicles (that is, every car has a color, a vehicle ID, an engine, and so on). In Figure 1.2, the shaded area depicts a row.

**Figure 1.2. A row (highlighted).**



You may also see the terms record or tuple?these are equivalent to a row.

### View

A view is an alternative way to present a table (or tables). You might think of a view as a "virtual" table. A view is (usually) defined in terms of one or more tables. When you create a view, you are not storing more data, you are instead creating a different way of looking at existing data. A view is a useful way to give a name to a complex query that you may have to use repeatedly.

### Client/server

PostgreSQL is built around a client/server architecture. In a client/server product, there are at least two programs involved. One is a client and the other is a server. These programs may exist on the same host or on different hosts that are connected by some sort of network. The server offers a service; in the case of PostgreSQL, the server offers to store, retrieve, and change data. The client asks a server to perform work; a PostgreSQL client asks a PostgreSQL server to serve up relational data.

### Client

A client is an application that makes requests of the PostgreSQL server. Before a client application can talk to a server, it must connect to a postmaster (see postmaster) and establish its identity. Client applications provide a user interface and can be written in many languages. Chapters 8 through 17 will show you how to write a client application.

### Server

The PostgreSQL server is a program that services commands coming from client applications. The PostgreSQL server has no user interface?you can't talk to the server directly, you must use a client application.

### Postmaster

Because PostgreSQL is a client/server database, something has to listen for connection requests coming from a client application. That's what the postmaster does. When a connection request arrives, the postmaster creates a new server process in the host operating system.

### Transaction

A transaction is a collection of database operations that are treated as a unit. PostgreSQL guarantees that all the operations within a transaction complete or that none of them complete. This is an important property?it ensures that if something goes wrong in the middle of a transaction, changes made before the point of failure will not be reflected in the database. A transaction usually starts with a BEGIN command and ends with a COMMIT or ROLLBACK (see the next entries).

### **Commit**

A commit marks the successful end of a transaction. When you perform a commit, you are telling PostgreSQL that you have completed a unit of operation and that all the changes that you made to the database should become permanent.

### **Rollback**

A rollback marks the unsuccessful end of a transaction. When you roll back a transaction, you are telling PostgreSQL to discard any changes that you have made to the database (since the beginning of the transaction).

### **Index**

An index is a data structure that a database uses to reduce the amount of time it takes to perform certain operations. An index can also be used to ensure that duplicate values don't appear where they aren't wanted. I'll talk about indexes in Chapter 4, "Query Optimization."

### **Result set**

When you issue a query to a database, you get back a result set. The result set contains all the rows that satisfy your query. A result set may be empty.

## **Database security**

Database security refers to the various measures organizations take to ensure their databases are protected from internal and external threats. Database security includes protecting the database itself, the data it contains, its database management system, and the various applications that access it. Organizations must secure databases from deliberate attacks such as cyber security threats, as well as the misuse of data and databases from those who can access them.

It refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability. This article will focus primarily on confidentiality since it's the element that's compromised in most data breaches.

Database security must address and protect the following:

- The data in the database
- The database management system (DBMS)
- Any associated applications
- The physical database server and/or the virtual database server and the underlying hardware
- The computing and/or network infrastructure used to access the database

Database security is a complex and challenging endeavor that involves all aspects of information security technologies and practices. It's also naturally at odds with database usability. The more accessible and usable the database, the more vulnerable it is to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use.

## **Common threats and challenges**

Many software misconfigurations, vulnerabilities, or patterns of carelessness or misuse can result in breaches. The following are among the most common types or causes of database security attacks and their causes.

### **Insider threats**

- An insider threat is a security threat from any one of three sources with privileged access to the database:
- A malicious insider who intends to do harm
- A negligent insider who makes errors that make the database vulnerable to attack
- An infiltrator—an outsider who somehow obtains credentials via a scheme such as phishing or by gaining access to the credential database itself

Insider threats are among the most common causes of database security breaches and are often the result of allowing too many employees to hold privileged user access credentials.

### **Human error**

Accidents, weak passwords, password sharing, and other unwise or uninformed user behaviors continue to be the cause of nearly half (49%) of all reported data breaches.

### **Exploitation of database software vulnerabilities**

Hackers make their living by finding and targeting vulnerabilities in all kinds of software, including database management software. All major commercial database software vendors and open source database management platforms issue regular security patches to address these vulnerabilities, but failure to apply these patches in a timely fashion can increase your exposure.

### **SQL/NoSQL injection attacks**

A database-specific threat, these involve the insertion of arbitrary SQL or non-SQL attack strings into database queries served by web applications or HTTP headers. Organizations that don't follow secure web application coding practices and perform regular vulnerability testing are open to these attacks.

### **Buffer overflow exploitations**

Buffer overflow occurs when a process attempts to write more data to a fixed-length block of memory than it is allowed to hold. Attackers may use the excess data, stored in adjacent memory addresses, as a foundation from which to launch attacks.

### **Denial of service (DoS/DDoS) attacks**

In a denial of service (DoS) attack, the attacker deluges the target server—in this case the database server—with so many requests that the server can no longer fulfill legitimate requests from actual users, and, in many cases, the server becomes unstable or crashes.

### **Malware**

Malware is software written specifically to exploit vulnerabilities or otherwise cause damage to the database. Malware may arrive via any endpoint device connecting to the database's network.

### **Attacks on backups**

Organizations that fail to protect backup data with the same stringent controls used to protect the database itself can be vulnerable to attacks on backups.

**These threats are exacerbated by the following:**

**Growing data volumes:** Data capture, storage, and processing continues to grow exponentially across nearly all organizations. Any data security tools or practices need to be highly scalable to meet near and distant future needs.

**Infrastructure sprawl:** Network environments are becoming increasingly complex, particularly as businesses move workloads to multicloud or hybrid cloud architectures, making the choice, deployment, and management of security solutions ever more challenging.

**Increasingly stringent regulatory requirements:** The worldwide regulatory compliance landscape continues to grow in complexity, making adhering to all mandates more difficult.

**When evaluating database security in your environment to decide on your team's top priorities, consider each of the following areas:**

**Physical security:** Whether your database server is on-premise or in a cloud data center, it must be located within a secure, climate-controlled environment. (If your database server is in a cloud data center, your cloud provider will take care of this for you.)

**Administrative and network access controls:** The practical minimum number of users should have access to the database, and their permissions should be restricted to the minimum levels necessary for them to do their jobs. Likewise, network access should be limited to the minimum level of permissions necessary.

**End user account/device security:** Always be aware of who is accessing the database and when and how the data is being used. Data monitoring solutions can alert you if data activities are unusual or appear risky. All user devices connecting to the network housing the database should be physically secure (in the hands of the right user only) and subject to security controls at all times.

**Encryption:** ALL data—including data in the database, and credential data—should be protected with best-in-class encryption while at rest and in transit. All encryption keys should be handled in accordance with best-practice guidelines.

**Database software security:** Always use the latest version of your database management software, and apply all patches as soon as they are issued.

**Application/web server security:** Any application or web server that interacts with the database can be a channel for attack and should be subject to ongoing security testing and best practice management.

**Backup security:** All backups, copies, or images of the database must be subject to the same (or equally stringent) security controls as the database itself.

**Auditing:** Record all logins to the database server and operating system, and log all operations performed on sensitive data as well. Database security standard audits should be performed regularly.

**Container security**

Container security is the process of implementing security tools to provide a strong information security for any container-based system or workload, including both container image, the running container and everything in between.



The process of securing containers is continuous. It should be integrated into your development process, automated to remove the number of manual touch points, and extended into the maintenance and operation of the underlying infrastructure. This means protecting your build pipeline container images and runtime host, platform, and application layers. Implementing security as part of the continuous delivery life cycle means your business will mitigate risk and reduce vulnerabilities across an ever-growing attack surface.

When securing containers, the main concerns are:

- The security of the container host
- Container network traffic
- The security of your application within the container
- Malicious behavior within your application
- Securing your container management stack
- The foundation layers of your application
- The integrity of the build pipeline



#### **Self-check quiz 5.4**

Check your understanding by answering the following questions:

Write the appropriate/correct answer of the following:

1. What is database?

Answer:

2. What is Transaction?

Answer:

3. What is Database security

Answer:



## Answer keys

### Answer key: 5.1

1. Answer:

Business requirements are the critical activities of an enterprise that must be performed to meet the organizational objective(s) while remaining solution independent.

2. Answer:

Business requirement analysis is a process in which the expectations and requirements of the users and stakeholders of a project or task are defined. The analysis of business needs is a comprehensive statement of what the outcome of a project or task should be.

3. Answer:

Identifying business requirements might sound simple, but a thorough analysis includes at least the following four steps:

1. Identify stakeholders
2. Identify all requirements
3. Classify company requirements
4. Analyse business requirements
5. Document & monitor

4. Answer:

1. Business Continuity
2. End-User Security
3. Risk Management
4. Security Awareness
5. Integration and Interoperability
6. Data Protection
7. End-User Ease of Use
8. Innovation
9. Confidence and Assurance
10. Governance Transparency
11. Project Management

### Answer key: 5.2

1. Answer:

A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security.

2. Answer:

An asset is any data, device or other component of an organisation's systems that is valuable – often because it contains sensitive data or can be used to access such information.

3. Answer:

A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorised party.

4. Answer:

A vulnerability is an organisational flaw that can be exploited by a threat to destroy, damage or compromise an asset.

### **Answer key: 5.3**

1. Answer:

Secure coding is a set of practices that applies security considerations to how software will be coded and encrypted to best defend against cyber attack or vulnerabilities. This is one of the most critical elements of the software development lifecycle and organizations must develop robust secure coding policies and procedures. It helps to mitigate the vulnerabilities and risks associated with the software product development process.

2. Answer:

Security Testing is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders.

3. Answer:

1. Acunetix
2. Owasp
3. WireShark
4. W3af

4. Answer:

The Software Development Life Cycle (SDLC) is a structured process that enables the production of high-quality, low-cost software, in the shortest possible production time. The goal of the SDLC is to produce superior software that meets and exceeds all customer expectations and demands.

### **Answer key 5.4**

1. Answer:

A database is a named collection of tables. A database can also contain views, indexes, sequences, data types, operators, and functions. Other relational database products use the term catalog.

2. Answer:

A transaction is a collection of database operations that are treated as a unit. PostgreSQL guarantees that all the operations within a transaction complete or that none of them complete.

3. Answer:

Database security refers to the various measures organizations take to ensure their databases are protected from internal and external threats. Database security includes protecting the database itself, the data it contains, its database management system, and the various applications that access it

LEARNER JOB SHEET 4			
<b>Qualification:</b>	Information System Security Management		
<b>Learning unit:</b>	Perform security measures on software		
<b>Learner name:</b>			
<b>Personal protective equipment (PPE):</b>	Mask, Anti-static rist belt		
<b>Materials:</b>	Fabrics, Garments, Measuring tape, paper, pen, pencil		
<b>Tools and equipment:</b>			
<b>Performance criteria:</b>	<ol style="list-style-type: none"> <li>1. Secured coding practices are interpreted.</li> <li>2. Code risks are interpreted.</li> <li>3. Software security testing is performed using testing tools.</li> <li>4. Software life cycle security is interpreted.</li> </ol>		
<b>Measurement:</b>			
<b>Notes:</b>			
<b>Procedure:</b>	<ol style="list-style-type: none"> <li>1. Collect PPE, tools, equipment and materials</li> <li>2. Check the usability of PPE, tools, equipment and materials.</li> <li>3. Install an Antivirus</li> <li>4. Take Backup form Data</li> <li>5. Install a Firewall</li> <li>6. Use Complex Passwords</li> <li>7. Use Encryption Software</li> <li>8. Update Software</li> <li>9. Secure Mobile Devices</li> <li>10. Protect Wireless Networks</li> <li>11. Keep an Eye on Suspicious Activity</li> <li>12. Educate Your Team</li> </ol>		
<b>Learner signature:</b>		<b>Date:</b>	
<b>Assessor signature:</b>		<b>Date:</b>	
<b>Quality Assurer signature:</b>		<b>Date:</b>	
<b>Assessor remarks:</b>			
<b>Feedback:</b>			

## Module 6: Interpret Information Systems Audit

---



**MODULE CONTENT** module covers

**Module Descriptor:** This module covers the knowledge, skills, and attitudes required to interpret Information Systems Audit. It specifically includes planning Information system audit and interpreting audit for Information systems.

**Nominal Duration:** 40 hours



### **LEARNING OUTCOMES:**

Upon completion of the module, the trainee should be able to:

- 6.1 Plan information system audit
- 6.2 Interpret audit for Information systems



### **PERFORMANCE CRITERIA:**

1. Organizational policies and national regulations are interpreted.
2. Information Systems audit standard, guideline and code of ethics are interpreted.
3. Types of audit and assessments are described.
4. Elements of audit plan are identified.
5. Risk based audit plan is developed.
6. International standards for information system audit is described.
7. Information system governance, risk and compliance audit is interpreted.
8. Information system Procurement, Development and Implementation is interpreted.
9. Information system operations and maintenance audit is interpreted.
10. Information assets security audit is interpreted.



## Learning Outcome 6.1 Plan information system audit



### Contents:

- Organizational policies and national regulations
- Information Systems audit standard, Guideline and code of ethics.
- Types of audit and assessments
- Elements of audit plan
- Risk based audit plan



### Assessment criteria:

1. Organizational policies and national regulations are interpreted.
2. Information Systems audit standard, guideline and code of ethics are interpreted.
3. Types of audit and assessments are described.
4. Elements of audit plan are identified.
5. Risk based audit plan is developed.



### Resources required:

Students/trainees must be provided with the following resources:

- Workplace (actual or simulated)
- Network devices, required tools, equipment's and materials.



### LEARNING ACTIVITY 6.1

Learning Activity	Resources/Special Instructions/References
Plan information system audit	<ul style="list-style-type: none"> <li>▪ Information Sheet: 6.1</li> <li>▪ Self-Check: 6.1</li> <li>▪ Answer Key: 6.1</li> </ul>



## Information sheet 6.1

Learning Objective: to plan information system audit.

### **Policies**

Policies are rules that are made by organizations, to achieve their aims and goals. Policies are made by individuals, groups, companies, and even governments to carry out their plans.

Organizational policies are rules and regulations employees must follow to keep business running smoothly. Some are intended to provide guidance and be helpful to employees. Others aim to protect the business from legal risk and warn employees not to do certain things.

An organization policy is a configuration of restrictions. You, as the organization policy administrator, define an organization policy, and you set that organization policy on organizations, folders, and projects in order to enforce the restrictions on that resource and its descendants.

### **Examples of workplace policies and procedures:**

#### **1. Code of conduct**

A code of conduct is a common policy found in most businesses. It is a set of rules that companies expect employees to follow. The rules establish the expected behavioural standards for all employees. A code of conduct policy may cover the following:

- Attendance and absence
- Employee behaviour
- Company values
- Break and mealtime policies
- Confidentiality
- Use of company property
- Use of social media
- Plagiarism
- Travel policies
- Conflicts of interest
- Client interaction
- Dress code
- Reporting misconduct

#### **2. Recruitment policy**

A recruitment policy outlines how the company hires new people. It outlines the hiring process and aims to promote consistency in the recruitment process. It's an important document for employees to access. It may cover the following things:

- Internal and external hiring preferences
- Equal opportunity and anti-discrimination
- Job description and advertisement templates
- Selection process and timeframe
- How to review resumes and cover letters
- The expected amount of short-listed applicants
- How to check references
- How to select a suitable candidate and offer the job



### **3. Internet and email policy**

This policy outlines how companies expect employees to use their email accounts and the internet. It helps to save time and promote efficiency. It also sets up procedures to minimise risk, which is especially important for secure networks. An internet and email policy may cover the following things:

- Internet access rules
- Appropriate online usage
- Controls on misuse of the internet
- Restrictions on web browsing
- A security protocol for online data
- Download rules
- Social networking rules
- Work email usage rules
- How to frame emails to colleagues
- Work email usage at home or outside the office

### **4. Mobile phone policy**

A mobile phone policy covers the rules of mobile phone usage in the workplace. It may cover personal mobile phone usage as well as work mobile phones. They provide employees with a comprehensive set of rules about when and how they are allowed to use their mobile phones. This sort of policy is set up to promote productivity and reduce distractions. It may cover the following:

- When you can use your personal mobile phone
- Where you can keep your personal mobile phone during office hours
- Rules surrounding personal phone calls
- How to use your work mobile phone
- What is and isn't acceptable use for you work mobile phone

### **5. Smoking policy**

A smoking policy covers a workplace's rules regarding smoking and tobacco use. Many companies do not allow smoking on their premises. It's important for employees to know where and when they can smoke, if applicable. A smoking policy may cover the following:

- Whether smoking is allowed
- Designated smoking areas
- Smoking breaks
- Smoking off-site

### **6. Drug and alcohol policy**

This type of policy covers a company's rules regarding drug and alcohol use. It may mention procedures for dealing with rule-breaking. It may also mention the procedure for dealing drug testing. A drug and alcohol policy is usually a strict list of rules that may cover the following:

- A company's tolerance to drug and alcohol use
- Drug testing rules
- Alcohol use rules (i.e., Friday drinks)
- Procedure for dealing with intoxicated individuals

### **7. Health and safety policy**

This type of policy covers a company's obligations under work health and safety laws. It is an important policy because it establishes how employees are protected. Such a policy may cover the following:

- Risk assessment
- Employee safety training
- First aid information
- Equipment maintenance
- Safe handling of materials and substances
- Supervision rules
- Delegation of authority
- Accident training
- Physical and mental health information
- Monitoring hazards
- Emergency procedures

## 8. Anti-discrimination and harassment policy

An anti-discrimination and harassment policy is important to promote a healthy and positive workplace for all employees. One of the key things to include in this policy is education. Education is one of the best ways to prevent discrimination and harassment. This type of policy may cover the following:

- Procedure for employee complaints
- Education and training for employees
- Provide a clear definition of discrimination and harassment
- Guidelines for dealing with discrimination and harassment
- How management expects to respond to complaints
- Confidentiality information

### Regulations

Regulations are rules that are made to make people comply and behave in a certain manner. A regulation has the effect of a law and is considered as a restriction that is imposed by authorities, to make people follow the desired code of conduct.

### Information security policy

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges. An information security policy makes it possible to coordinate and enforce a security program and communicate security measures to third parties and external auditors.

To be effective, an information security policy should:

- Cover end-to-end security processes across the organization
- Be enforceable and practical
- Be regularly updated in response to business needs and evolving threats
- Be focused on the business goals of your organization

### Information security policies can have the following benefits for an organization:

- **Facilitates data integrity, availability, and confidentiality** — effective information security policies standardize rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.
- **Protects sensitive data** — Information security policies prioritize the protection of intellectual property and sensitive data such as personally identifiable information (PII).
- **Minimizes the risk of security incidents** — An information security policy helps organizations define procedures for identifying and mitigating vulnerabilities and risks. It also details quick responses to minimize damage during a security incident.
- **Executes security programs across the organization** — Information security policies provide the framework for operationalizing procedures.
- **Provides a clear security statement to third parties** — Information security policies summarize the organization's security posture and explain how the organization protects IT resources and assets. They facilitate quick response to third-party requests for information by customers, partners, and auditors.
- **Helps comply with regulatory requirements** — Creating an information security policy can help organizations identify security gaps related to regulatory requirements and address them.

## **Elements of an Information Security Policy**

A security policy can be as broad as you want it to be, from everything related to IT security and the security of related physical assets, but enforceable in its full scope. The following list offers some important considerations when developing an information security policy.

### **1. Purpose**

First state the purpose of the policy, which may be to:

Create an overall approach to information security.

Detect and preempt information security breaches such as misuse of networks, data, applications, and computer systems.

Maintain the reputation of the organization, and uphold ethical and legal responsibilities.

Respect customer rights, including how to react to inquiries and complaints about non-compliance.

### **2. Audience**

Define the audience to whom the information security policy applies. You may also specify which audiences are out of the scope of the policy (for example, staff in another business unit which manages security separately may not be in the scope of the policy).

### **3. Information security objectives**

Guide your management team to agree on well-defined objectives for strategy and security. Information security focuses on three main objectives:

Confidentiality — Only individuals with authorization can should access data and information assets.

Integrity — Data should be intact, accurate and complete, and IT systems must be kept operational.

Availability — Users should be able to access information or systems when needed.

### **4. Authority and access control policy**

Hierarchical pattern — A senior manager may have the authority to decide what data can be shared and with whom. The security policy may have different terms for a senior manager vs. a junior employee. The policy should outline the level of authority over data and IT systems for each organizational role.

Network security policy — Users are only able to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens. You should monitor all systems and record all login attempts.

### **5. Data classification**

The policy should classify data into categories, which may include “top secret”, “secret”, “confidential”, and “public”. Your objective in classifying data is:

To ensure that sensitive data cannot be accessed by individuals with lower clearance levels

To protect highly important data, and avoid needless security measures for unimportant data

### **6. Data support and operations**

Data protection regulations — systems that store personal data, or other sensitive data — must be protected according to organizational standards, best practices, industry compliance standards, and relevant regulations. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection.

Data backup — Encrypt data backup according to industry best practices. Securely store backup media, or move backup to secure cloud storage.

Movement of data — Only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network.

### **7. Security awareness and behavior**

Share IT security policies with your staff. Conduct training sessions to inform employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification.

Social engineering — Place a special emphasis on the dangers of social engineering attacks (such as phishing emails). Make employees responsible for noticing, preventing and reporting such attacks.

Clean desk policy — Secure laptops with a cable lock. Shred documents that are no longer needed. Keep printer areas clean so documents do not fall into the wrong hands.

Acceptable Internet usage policy—define how the Internet should be restricted. Do you allow YouTube, social media websites, etc.? Block unwanted websites using a proxy.

### **8. Encryption policy**

Encryption involves encoding data to keep it inaccessible to or hidden from unauthorized parties. It helps protect data stored at rest and in transit between locations and ensure that sensitive, private, and proprietary data remains private. It can also improve the security of client-server communication. An encryption policy helps organizations define:

The devices and media the organization must encrypt

When encryption is mandatory

The minimum standards applicable to the chosen encryption software

### **9. Data backup policy**

A data backup policy defines rules and procedures for making backup copies of data. It is an integral component of overall data protection, business continuity, and disaster recovery strategy. Here are key functions of a data backup policy:

Identifies all information the organization needs to back up

Determines the frequency of backups, for example, when to perform an initial full backup and when to run incremental backups

Defines a storage location holding backup data

Lists all roles in charge of backup processes, for example, a backup administrator and members of the IT team

### **10. Responsibilities, rights, and duties of personnel**

Appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.

### **11. System hardening benchmarks**

The information security policy should reference security benchmarks the organization will use to harden mission critical systems, such as the Center for Information Security (CIS) benchmarks for Linux, Windows Server, AWS, and Kubernetes.

## **PHASE 1: Audit Planning**

In this phase we plan the information system coverage to comply with the audit objectives specified by the Client and ensure compliance to all Laws and Professional Standards. The first thing is to obtain an Audit Charter from the Client detailing the purpose of the audit, the management responsibility, authority and accountability of the Information Systems Audit function as follows:

1. **Responsibility:** The Audit Charter should define the mission, aims, goals and objectives of the Information System Audit. At this stage we also define the Key Performance Indicators and an Audit Evaluation process;
2. **Authority:** The Audit Charter should clearly specify the Authority assigned to the Information Systems Auditors with relation to the Risk Assessment work that will be carried out, right to access the Client's information, the scope and/or limitations to the scope, the Client's functions to be audited and the auditee expectations; and
3. **Accountability:** The Audit Charter should clearly define reporting lines, appraisals, assessment of compliance and agreed actions.

The Audit Charter should be approved and agreed upon by an appropriate level within the Client's Organization.

In addition to the Audit Charter, we should be able to obtain a written representation ("Letter of Representation") from the Client's Management acknowledging:

1. Their responsibility for the design and implementation of the Internal Control Systems affecting the IT Systems and processes
2. Their willingness to disclose to the Information Systems Auditor their knowledge of irregularities and/or illegal acts affecting their organisation pertaining to management and employees with significant roles within the internal audit department.
3. Their willingness to disclose to the IS Auditor the results of any risk assessment that a material misstatement may have occurred

## **PHASE 2 – Risk Assessment and Business Process Analysis**

Risk is the possibility of an act or event occurring that would have an adverse effect on the organisation and its information systems. Risk can also be the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets. It is ordinarily measured by a combination of effect and likelihood of occurrence.

More and more organisations are moving to a risk-based audit approach that can be adapted to develop and improve the continuous audit process. This approach is used to assess risk and to assist an IS auditor's decision to do either compliance testing or substantive testing. In a risk based audit approach, IS auditors are not just relying on risk. They are also relying on internal and operational controls as well as knowledge of the organisation. This type of risk assessment decision can help relate the cost/benefit analysis of the control to the known risk, allowing practical choices.

The process of quantifying risk is called Risk Assessment. Risk Assessment is useful in making decisions such as:

1. The area/business function to be audited
2. The nature, extent and timing of audit procedures
3. The amount of resources to be allocated to an audit

The following types of risks should be considered:

**Inherent Risk:** Inherent risk is the susceptibility of an audit area to error which could be material, individually or in combination with other errors, assuming that there were no related internal controls. In assessing the inherent risk, the IS auditor should consider both pervasive and detailed IS controls. This does not apply to circumstances where the IS auditor's assignment is related to pervasive IS controls only. A pervasive IS Control are general controls which are designed to manage and monitor the IS environment and which therefore affect all IS-related activities. Some of the pervasive IS Controls that an auditor may consider include:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management
- Pressures on IS management which may predispose them to conceal or misstate information (e.g. large business-critical project over-runs, and hacker activity)
- The nature of the organisation's business and systems (e.g., the plans for electronic commerce, the complexity of the systems, and the lack of integrated systems)
- Factors affecting the organisation's industry as a whole (e.g., changes in technology, and IS staff availability)
- The level of third party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers)
- Findings from and date of previous audits

A detailed Information Security control is a control over acquisition, implementation, delivery and support of Information Security systems and services. The Information Security auditor should consider, to the level appropriate for the audit area in question:

- The findings from and date of previous audits in this area
- The complexity of the systems involved
- The level of manual intervention required
- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, and payroll)
- The likelihood of activity peaks at certain times in the audit period
- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data)
- The integrity, experience and skills of the management and staff involved in applying the IS controls

**Control Risk:** Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied. The IS auditor should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

### **Types of Cybersecurity Audits and Assessments**

Here is a handy reference of standard cybersecurity assessment and audit terms:

**Controls (or Controls Library)** – A control is a rule or requirement that is designed to drive a specific objective. A controls library is simply a list of the controls. The business objective, and an established test for the control is often, but not always, included in the library.

**Cybersecurity Audit** – An audit is typically defined as an evaluation of performance against specifications, standards, controls, or guidelines. This is often a checklist exercise where there is an evaluation against a list of controls called the controls library. The effectiveness, comprehensiveness, and business appropriateness of those controls are not obvious.

**Cybersecurity Assessment** – Assessments come in many shapes and sizes, and typically deliver a much deeper evaluation of performance against, or adherence to, the controls. Assessments usually include some sort of impact measure or an interpretation of the effectiveness of the area being assessed. Assessments may include some degree of an audit but not always.

**Penetration Testing** – This is neither an audit or an assessment. It is a situational test that looks at one point in time. It is a trial to the controls, monitoring, processes, and technologies that protect an environment. It provides no measure but an anecdotal data point and a narrative. There is value in this exercise, however it is not a satisfactory replacement for audits or assessments.



### **Self-check quiz 6.1**

Check your understanding by answering the following questions:

Write the correct answer for the following questions.

1. What do you mean by Organizational policies?

Answer:

2. What is Information security policy?

Answer:

3. What are the elements of an Information Security Policy?

Answer:



## Learning outcome 6.2 Interpret audit for Information systems



Contents:

- International standards for information system audit
- Information system governance, risk and compliance audit
- Information system Procurement, Development and Implementation
- Information system operations and maintenance audit
- Information assets security audit



Assessment criteria:

1. International standards for information system audit is described.
2. Information system governance, risk and compliance audit is interpreted.
3. Information system Procurement, Development and Implementation is interpreted.
4. Information system operations and maintenance audit is interpreted.
5. Information assets security audit is interpreted.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (Actual or simulated), Server, Necessary software.



### **LEARNING ACTIVITY 6.2**

Learning Activity	Resources/Special Instructions/References
Interpret audit for Information systems	<ul style="list-style-type: none"> <li>▪ Information Sheets: 6.2</li> <li>▪ Self-Check: 6.2</li> <li>▪ Answer Key: 6.2</li> </ul>





## Information sheet 6.2

Learning objective: to interpret audit for information systems.

Information Systems Audit is a managerial, technical and organisational process to ensure proper utilization of Information Technology and systems to strategically align with the overall mission and goal of organisation. Information Systems Audit should not be viewed as controlling procedure, but as a means of leveraging maximum return on investments from IT investment and better dissemination of Information resources to the stakeholders.

The effectiveness of an information system's controls is evaluated through an information systems audit. An audit aims to establish whether information systems are safeguarding corporate assets, maintaining the integrity of stored and communicated data, supporting corporate objectives effectively, and operating efficiently. It is a part of a more general financial audit that verifies an organization's accounting records and financial statements. Information systems are designed so that every financial transaction can be traced. In other words, an audit trail must exist that can establish where each transaction originated and how it was processed. Aside from financial audits, operational audits are used to evaluate the effectiveness and efficiency of information systems operations, and technological audits verify that information technologies are appropriately chosen, configured, and implemented.

### **Auditing Standards for auditing Information Systems**

The specialized nature of Information Systems auditing and the professional skills and credibility necessary to perform such audits, require standards that would apply specifically to IS auditing. Standards, procedures and guidelines have been issued by various institutions, which discuss the way the auditor should go about auditing Information Systems. In line with such developments Supreme Audit Institution of India has declared a mission to adopt and evolve standards, guidelines and best practices for auditing in a computerized environment. This will lend credibility and clarity in conducting audit in computerized environment. The framework for the IS Auditing Standards provides multiple levels of guidance.

Standards provide a framework for all audits and auditors and define the mandatory requirements of the audit. They are broad statement of auditors' responsibilities and ensure that auditors have the competence, integrity, objectivity and independence in planning, conducting and reporting on their work.

Guidelines provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.

Procedures provide examples of procedures an IS audit or might follow in an audit engagement. It provides information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Guidelines and Procedures is to provide further information on how to comply with the IS Auditing Standards. While conducting Information System Audit the auditor should consider the issues of confidentiality, integrity and availability (CIA) and his work should be guided by international or respective national standards. These may include INTOSAI Auditing Standards, International Federation of Accountants (IFAC) Auditing Standards, International standards of professional audit institutions such as Information Systems Audit and Control Association (ISACA) and Institute of Internal auditors (IIA) and national auditing standards of Supreme Audit Institutions (SAI) member countries. Information Systems Audit and Control Association (ISACA) has laid down the following generic requirements for IS audit which are applicable to all categories of IS audits

1. The responsibility, authority and accountability of the information systems audit function are to be appropriately documented in an audit.

2. The information systems auditor is to be independent of the auditee in attitude and appearance.

3. The information systems auditor is to adhere to the 'Code of Professional Ethics'.

Due professional care and observance of applicable professional auditing standards are to be exercised.

4. The information systems auditor is to be technically competent, having the skills and knowledge

necessary to perform the auditor's work and has to maintain technical competence through continuing professional education.

5. The information systems auditor is to plan his work to address the audit objectives.

6. Information systems audit staff is to be appropriately supervised so as to ensure that audit objectives and applicable professional auditing standards are met. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of sufficient, reliable, relevant and useful evidence

7. The information systems auditor is to provide a report, in an appropriate form, to intended recipients upon the completion of audit work.

8. The information systems auditor follow-up action timely taken on previous relevant findings.

### **Information Systems Governance**

Information Systems Governance (ISG) can be defined as a set of rules allowing executives and stakeholders to determine how they will decide on the Information System management.

An important goal of information governance is to provide employees with data they can trust and easily access while making business decisions. In many organizations, responsibilities for data governance tasks are split among security, storage and database teams. Often, the need for a holistic approach to managing information does not become evident until a major event occurs, such as a lawsuit, compliance audit or corporate merger.

Information governance provides a wide range of benefits. It ensures the following:

- Whoever requires access to certain information can receive it;
- Underlying data is properly managed, stored and secured;
- Regulatory requirements are correctly observed, where necessary; and
- Risk management is in place to minimize any issues that might arise from incorrect use.



## Information governance challenges

Even a clear vision and strong management support don't guarantee information governance success. Organizations can experience a number of common issues when implementing information governance, including the following:

- **Compliance and regulatory issues.** An organization often requires information governance during a lawsuit or some other consequence of noncompliance. On such occasions, compliance teams must go through potentially millions of pages of documents -- and possibly even more rows of data -- in pursuit of information that has been requested for legal purposes. This process, also called electronic discovery (e-discovery), is daunting even when things are at their most orderly. It can become a nightmare if the organization's information is not well ordered and readily discoverable.

Organizations can mitigate this challenge using several strategies, such as the following:

- establishing a universal metadata taxonomy for consistent tagging of information;
  - developing a consistent retention management/defensible disposal policy and process; and
  - establishing a data classification program to rate all information assets according to their sensitivity.
- **Big data and machine learning.** Machine learning is increasingly essential in the enterprise, enabling the predictive and prescriptive analytics that are necessary to maintaining a competitive edge. But machine learning depends on big data -- large amounts of information about the particular domain being modeled for predictive use -- and it is often challenging to manage data of that magnitude.

Careful attention to the integrity of data sources and the merging and transformation of data from multiple sources is essential in this endeavor. Organizations should ensure that the big data underlying the analytics is as accurate and clean as possible, and strong governance policy can help ensure this.

- **Lifecycle management.** One major challenge of an information governance implementation is the need to manage data that underlies information assets throughout its lifecycle in multiple domains. As silos come down and information becomes more centralized in the enterprise, inconsistencies in its management can creep into existing processes, causing friction between groups. All groups using common information must agree about the process of refreshing, modifying and archiving that information. Achieving policies that encourage such agreement should be a responsibility of the governance officer and council.

## Information governance frameworks

Many types of organizations may have different goals and tasks, but the elements of information that are used to manage those activities are often similar. For this reason, it is possible to create frameworks to clarify an information governance plan that can be useful in organizing the effort, regardless of how customized the organization's handling of information may seem.

These information governance plan frameworks outline the who, what, when, where, why and how of company information. Frameworks are built from the answers to some central questions that apply to information of all types:

- What does this information mean?
- Who uses it?
- How is it created/where does it come from?
- What do users do with it?
- Who can access it?
- Why is it important?
- How long is it useful for?

- What other information depends upon this information?

Answering all of those questions for every information asset within the enterprise is a monumental task. Once an organization collects those the answers, however, a path to managing it becomes increasingly clear.

Frameworks are tailored to the organization's unique governance needs but should define the following areas:

**Policy.** The framework defines which wide-ranging, overall corporate policies and procedures are relevant to the information governance program as a whole, including the company's data security, records management, retention and disposal schedules, privacy and information sharing policies.

**Process.** The framework carefully defines how the policies are implemented.

**Roles and accountability.** Who does what is a key part of policy implementation and process. An accountability framework defines the information governance program's key roles, including what information governance responsibilities specific employees and departments will have as part of the program's implementation and integration. For example, who has ultimate responsibility for the management of specific bodies of information, particularly sensitive ones? What are the consequences of mismanagement in this area?

**Metrics.** Organizations can track information quality, access and lifecycle management by measuring activity, quality of outcomes and issues. Strong metrics make for strong process and effective risk management.

**Compliance.** A framework highlights legal and regulatory concerns to ensure that they are addressed and to specify how.

**Scope.** The framework establishes the extent of the information governance program, including clearly outlining its overall goals, what staff members will be involved in achieving these goals and the types of data the information governance program is designed to manage.

**Internal and external data management.** The information governance framework defines how employees and the organization manage specific data, with relevant sections including legal and regulatory compliance; acceptable content types; how personal information is managed; how information is stored, archived and disposed of; and how information is shared.

It is also essential to establish how the organization operates and shares information with stakeholders, partners and suppliers. The framework should define the policies and procedures for sharing information with third parties, how the information governance process influences contractual obligations and how the organization will determine whether third parties are meeting its information governance goals.

**Disaster recovery (DR) and business continuity (BC).** The framework should clearly outline company procedures in the event of a data breach, including how to report information losses and breaches, incident management specifics, DR processes, BC strategies, and auditing of these DR and BC processes.

**Continuous monitoring.** The framework should outline plans for quality assurance (QA) of information governance processes, including how the company will monitor information access and use, measure regulatory compliance adherence, maintain effective security, conduct risk assessments and periodically review the information governance program as a whole.

### **Laws, regulations and principles**

Information governance isn't just a matter of best practices; it is a matter of regulation in and of itself because it is so deeply intertwined with security, privacy and compliance concerns.

As technological innovations continue to expand business capabilities and corporate data volumes grow, regulations that put strict mandates on information governance processes have become the norm. This is especially true for data privacy and security, as personally identifiable information (PII) has become a big target for hackers and nefarious online actors. Privacy laws, such as the European Union's Data

Protection Directive, have started to expand in countries all over the world and create new information security (infosec) governance obligations for companies.

Many industries, including highly regulated sectors, such as energy and financial services, are subject to regulations that require records and electronic communications be retained for a minimum period of time. These regulations include mandates from federal agencies, such as the Securities and Exchange Commission (SEC), Department of Justice (DOJ) and Environmental Protection Agency (EPA), regarding response times for information requests. Regulatory reporting requirements also often mandate that companies provide an account of compliance, usually in the form of raw or summary data, with set frequency, such as annually.

Some examples of laws and regulations that information governance can address include the following:

**HIPAA.** The Health Insurance Portability and Accountability Act is a good example of regulatory requirements that can be addressed through effective information governance. It imposes strict compliance requirements of healthcare organizations to compel them to protect the privacy of patient medical information.

**GDPR.** The European Union's General Data Protection Regulation is another regulatory effort to preserve privacy -- in this case, that of consumers. GDPR calls for organizations to empower customers to control the amount of private information that a company can share. This is another area where information governance is critical and empowering.

**FCPA.** The Foreign Corrupt Practices Act addresses compliance, imposing rules on organizations to ensure the authenticity of the records they keep. The idea is that organizations will be able, if called upon, to produce evidence of information authenticity -- yet another process for information governance.

### **Information governance models**

In addition to frameworks, there are information governance models. Organizations can use these to assess the quality and effectiveness of an information governance program once they implement it.

The Information Governance Reference Model (IGRM) provides organizations with a means of communicating the processes, policies and responsibilities of an information governance program with its key stakeholders. Its goal is to establish a clear mapping of information management responsibilities within the organization and among its partner organizations.

The Information Governance Maturity Model (IGMM) is focused on best practices. It is built on the Generally Accepted Recordkeeping Principles, encouraging the implementation of processes that are not only compliant, but progressive, spurring the organization to greater efficiency, competitiveness and customer focus.

The Information Governance Implementation Model (IGIM) establishes common understanding of governance principles and policies among stakeholders, reducing risk and enhancing cooperation and broad uptake of processes.

**Individual Activity:**

- *Carry out information system audit.*

**Self-check quiz 6.2**

Check your understanding by answering the following questions:

- What is Information Systems Audit?  
Answer:
  
- What is information governance?  
Answer:



## Answer keys

### Answer key 6.1

1. Answer:

Organizational policies are rules and regulations employees must follow to keep business running smoothly. Some are intended to provide guidance and be helpful to employees. Others aim to protect the business from legal risk and warn employees not to do certain things.

2. Answer:

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges.

3. Answer:

The following list offers some important considerations when developing an information security policy:

- Purpose
- Audience
- Information security objectives
- Authority and access control policy
- Data classification
- Data support and operations
- Security awareness and behavior
- Encryption policy
- Data backup policy
- Responsibilities, rights, and duties of personnel
- System hardening benchmarks

### Answer key 6.2

1. Answer:

Information Systems Audit is a managerial, technical and organisational process to ensure proper utilization of Information Technology and systems to strategically align with the overall mission and goal of organisation. Information Systems Audit should not be viewed as controlling procedure, but as a means of leveraging maximum return on investments from IT investment and better dissemination of Information resources to the stakeholders.

2. Answer:

Information Systems Governance (ISG) can be defined as a set of rules allowing executives and stakeholders to determine how they will decide on the Information System management.

An important goal of information governance is to provide employees with data they can trust and easily access while making business decisions. In many organizations, responsibilities for data governance tasks are split among security, storage and database teams.

## Module 7: Perform Information Systems Security Testing

---



### MODULE CONTENT

**Module Descriptor:** This module covers the knowledge, skills, and attitudes required to perform Information System security testing. It specifically includes Performing Vulnerability Assessment and penetration testing.

**Nominal Duration:** 50 hours



### LEARNING OUTCOMES:

Upon completion of the module, the trainee should be able to:

- 7.1 Perform Vulnerability Assessment
- 7.2 Perform Penetration testing



### PERFORMANCE CRITERIA:

- 1 Reconnaissance is performed.
- 2 Scanning is completed as per industry standard.
- 3 Vulnerabilities are identified and documented.
- 4 Reporting is performed following standard procedure.
- 5 Vulnerability Assessment is performed.
- 6 Gaining access is performed.
- 7 Clearing track is performed following industry standard.
- 8 Reporting is performed following standard procedure.





## Learning Outcome 7.1 Perform Vulnerability Assessment



Contents:

- Reconnaissance
- Scanning
- Vulnerabilities.
- Reporting procedure



Assessment criteria:

1. Reconnaissance is performed.
2. Scanning is completed as per industry standard.
3. Vulnerabilities are identified and documented.
4. Reporting is performed following standard procedure.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (actual or simulated)
- Network devices, required tools, equipment's and materials.



### LEARNING ACTIVITY 7.1

Learning Activity	Resources/Special Instructions/References
Perform Vulnerability Assessment	<ul style="list-style-type: none"> <li>▪ Information Sheet: 7.1</li> <li>▪ Self-Check: 7.1</li> <li>▪ Answer Key: 7.1</li> </ul>



## Information sheet 7.1

Learning Objective: to perform Vulnerability assessment.

### **Vulnerability assessment**

A vulnerability assessment (or vulnerability testing) is the systematic evaluation of potential and existing threats and flaws in your organization's systems, networks, applications, hardware, and other parts of the IT ecosystem.

#### **The different types of vulnerability assessments**

Vulnerability assessments can help you find potential exploits before hackers start snooping, ensure your systems remain up to date and patched, create a proactive focus on information security, and ultimately help your organization maintain its reputation.

**There are various types of vulnerability assessments. They include:**

#### **Network-based assessment**

As the name suggests, this scan helps pinpoint possible flaws on wired and wireless networks.

#### **Database assessment**

This assessment involves locating security loopholes in a database to prevent malicious attacks, such as distributed denial-of-service (DDoS), SQL injection, brute force attacks, and other network vulnerabilities.

#### **Web application assessment**

This scan involves a careful evaluation of web applications and their source code to find any security holes. The process can be done manually or automated.

#### **Host-based assessment**

This type of assessment examines any possible weaknesses or threats in server workstations and other network hosts. It also involves a meticulous examination of ports and services.

#### **Wireless network assessment**

This scan validates whether an organization's wireless infrastructure is securely configured to prevent unauthorized access.

### **Steps to conducting a proper vulnerability assessment**

#### **1. Defining and planning the scope of testing**

Before you begin conducting a vulnerability assessment, you need to establish a methodology:

- Identify where your most sensitive data is stored.
- Uncover hidden sources of data.
- Identify which servers run mission-critical applications.
- Identify which systems and networks to access.

- Review all ports and processes and check for misconfigurations.
- Map out the entire IT infrastructure, digital assets, and any devices used.

The idea here is to streamline the entire process.

## 2. Vulnerability identification



Conduct a vulnerability scan of your IT infrastructure and make a complete list of the underlying security threats. To achieve this step you'll need to do an automated vulnerability scan as well as a manual penetration test to validate findings and reduce false positives.

## 3. Analysis

A scanning tool will provide you with a detailed report containing different risk ratings and scores for vulnerabilities.

Most tools use a CVSS (common vulnerability scoring system) to assign a numerical score. A careful analysis of these scores will tell you which vulnerabilities you'll need to deal with first. You can prioritize them based on factors such as severity, urgency, potential damage, and risk.

## 4. Treating the vulnerabilities

With the vulnerabilities identified and analyzed, the next step is to decide how you want to fix them. There are two ways to do this: remediation and mitigation.

Remediation involves fixing a vulnerability fully to prevent any exploitation. You can achieve it through the fresh installation of security tools, a product update, or something more involved.

The vulnerability remediation process is based on the priorities set during the analysis phase and requires the participation of all stakeholders.

When there's no proper fix or patch for an identified vulnerability, mitigation helps reduce the prospect of an attack. The option is used to buy time until remediation is possible.

Part of the mitigation process should include deploying additional tools to help reduce cybersecurity risks. For example, antivirus software can be used to identify and remove malware and other threats within your network. Reputable tools can accomplish this through a variety of measures, including real-time antivirus scanners, remote firewalls, and predictive artificial intelligence threat detection.

### Vulnerability Scanning

Depending on the part of the system you wish to scan, vulnerability scans are divided into two categories, external and internal. External scans encompass all publicly available resources, while internal scans target all internal assets that are inaccessible from the internet.

To add, depending on who is conducting the vulnerability scan, it can be classified as an in-house scan or as a 3rd party scan. Vulnerability scans are typically performed by qualified security staff and configured in various tools that are available as a paid software solution or in an open-source form.

### Step 1: Conduct Risk Identification and Analysis

Identifying risks for each asset and possible threats they face is a complex task. The most important thing is to structure the process well so that nothing important slips through the

cracks. Companies can accomplish this by structuring their asset registers with added columns for threats and vulnerabilities.

This way, you will have a centralized document with all the necessary information needed. After you assign threats and vulnerabilities to your assets, you can begin the analysis phase where you assign risks to assets by determining the impact and likelihood of each threat materializing.

Once complete, you can finally focus on prioritizing assets that have the highest risk assigned and those most critically affected by known weaknesses or vulnerabilities.

## **Step 2: Vulnerability Scanning Policies and Procedures**



In order to have a structured and successful scanning methodology, policies and procedures must exist in order to have a pre-determined course of action needed to be taken. This includes all aspects of vulnerability scanning.

For starters, the policy or a procedure should have an official owner that is responsible for everything that is written inside. The policy should also be approved by upper management before taking effect. Defining the frequency of scanning is also important due to compliance adherence.

From a technical perspective, everything regarding the vulnerability scan configuration and functionality should be emphasized and written down. The document should also include steps to be taken after the scan is complete.

The most important factors are the types of scans that will be conducted, the ways the scans will be performed, software solutions used, which vulnerabilities take precedence over others, and steps that need to be taken after the scan is complete.

## **Step 3: Identify the Types of Vulnerability Scans**



Vulnerability scanning is a process where vulnerability scanning software is used to identify security weaknesses in information systems. Vulnerability scanning can be performed by network administrators, information security analysts and all technical IT staff that are trained and assigned the function of conducting a vulnerability scan.

Most malicious hackers attempt to map a network by scanning the system and trying to find possible vulnerabilities to gain unauthorized access to information systems. If malicious hackers you are trying to defend against use vulnerability scanning techniques, you have no choice but to employ them as well in order to stay ahead of their game.

Depending on the software that is running on the system you need to scan and secure, you need to determine the type of scan to be performed in order to get the most benefits.



**The most common types of vulnerability scans include:**

### **Network Vulnerability Scans**

The most common type of vulnerability scan is a network based scan. This scan includes networks, their communication channels and the networking equipment used in an environment.

Some of the major software and hardware devices that are in the scope of a network scan are hubs, switches, routers, firewalls, clusters, and servers. A network scan will detect and classify all vulnerabilities that it finds on these devices.

### **Host Based Vulnerability Scans**

Host based scan is often misunderstood as being the same as a network scan. Far from the truth, host-based scans address vulnerabilities related to hosts on the network including computers, laptops and servers.

More specifically, this scan investigates the host configuration, its user directories, file systems, memory settings and other information that can be found on a host. This scan focuses more on the endpoints and their internal system setup and functionality.

The importance of a host-based scan is also often overlooked. If neglected, misconfigurations and dormant vulnerabilities that lie in endpoints can mean disaster for your company if a malicious hacker manages to penetrate past your perimeter. By neglecting host-based scans malicious actors are able to move laterally through the system with far more ease.

### **Wireless Based Vulnerability Scans**

In order to conduct a successful wireless vulnerability scan you need to know all the wireless devices that are in your network. Additionally, you need to map out the attributes for each device in order to know how to properly configure the scan.

The next step is to identify any rogue access points that might be in your network and isolate those unknown devices. It is important to remove these devices from your network as they might be listening in on your wireless traffic.

After all of the above, you can start testing your wireless access points and your wireless LAN infrastructure.

### **Application Based Vulnerability Scans**

This type of vulnerability scan is often forgotten and is in the shadows of an application penetration test. Nevertheless, if you are not conducting an application penetration test, scanning your applications for vulnerabilities should be very high on your priority list.

By choosing from a variety of application vulnerability scanning tools, you can automate your security tasks and increase the security of your applications. There is a variety of tools that you can use, both open-source and commercial in order to conduct a true application vulnerability scan.

### **Step 4: Configure the Scan**

Even though there are many vulnerability scanning vendors to choose from, the configuration of any scan can still be addressed by identifying general objectives and the type of system you want to scan.

To configure a vulnerability scan you must:

Add A List of Target IPs – The IP addresses where the target systems are hosted need to be inputted into the vulnerability scanning software in order for a scan to be performed.

Defining Port Range and Protocols – After adding the target IPs it is important to specify the port range you want to scan and which protocol you wish to use in the process.

Defining The Targets – In this step, you need to specify if your target IPs are databases, windows servers, applications, wireless devices etc. By making your scan more specific, you will get more accurate results.

Setting Up the Aggressiveness of The Scan, Time And Notifications – Defining how aggressive your scan will be can influence the performance of the devices you are going to scan. To avoid any downtime on the target systems, it is recommended to set up a scan to be executed at a certain time, usually non-business hours. Additionally, you can also setup to receive a notification when the scan is complete.

#### **Step 5: Perform the Scan**



After determining the type of scan you want to conduct, and after setting up the configuration of the scan, you can save the configuration and run as desired. Depending on the size of the target set and the intrusiveness of the scan, it can take minutes to hours for it to complete.

Each vulnerability scan can be divided into three phases:

- Scanning
- Enumeration
- Vulnerability Detection

In the scanning phase, the tool you are using will fingerprint the specified targets to gather basic information about them.

With this information, the tool will proceed to enumerate the targets and gather more detailed specifications such as ports and services that are up and running. Finally, after determining the service versions and configuration of each target IP, the network vulnerability scanning tool will proceed to map out vulnerabilities in the targets, if any are present.

#### **Step 6: Evaluate and Consider Possible Risks**



Risks associated with performing a vulnerability scan pertain mostly to the availability of the target system. If the links and connections cannot handle the traffic load generated by the scan, the remote target can shut down and become unavailable.

When performing a scan on critical systems and production systems, extra caution should be exercised, and the scan should be performed after hours when the traffic to the target is minimal, in order to avoid overload.

#### **Step 7: Interpret the Scan Results**



Having qualified staff members configuring, performing and analyzing the results of a vulnerability scan is most important. Knowledge of the scanned system is also important in order to properly prioritize remediation efforts. Even though each vulnerability scanning tool will prioritize vulnerabilities automatically, certain types of vulnerabilities should be given a priority.

For example, remote code execution vulnerabilities should take precedence over possible DDOS and encryption vulnerabilities. It's important to consider the likelihood and the effort needed in order for a hacker to exploit the found vulnerability.

If there is a public exploit available for a vulnerability that you found in your system, giving priority to that vulnerability should take precedence over other vulnerabilities found that are exploitable but with far more effort.

### **Step 8: Create A Remediation Process and Mitigation Plan**



After interpreting the results, information security staff should prioritize the mitigation of each vulnerability detected and work with IT staff in order to communicate mitigation actions. The Information security staff and IT staff need to communicate and work closely together in the vulnerability mitigation phase in order to make the process successful and fast.

Numerous follow-up scans are usually performed during the back and forth problem-solving between teams until all vulnerabilities that need to be mitigated no longer appear in the reports.

### **Vulnerability assessment reports**

A vital advantage for security professionals is the ability to come up with robust vulnerability assessment reports. A clear and concise vulnerability assessment report aids an organization's network security team in fixing and alleviating vulnerabilities, the risks they pose, and the possible occurrence of cyberattacks.

In this article, we will explore how to create a strong vulnerability assessment report and understand the aims of its creation. We will also provide you samples of best practices in making these reports to help your organization prepare for future threats and attacks.

The vulnerability assessment report is a part and most crucial step of vulnerability assessment. The findings of this assessment are all included in the vulnerability assessment report. When creating a report, it is necessary to understand the vulnerability assessment process. First, we need to explore the things that comprise vulnerability assessment and define its components to get real value from the vulnerability assessment report.

### **Vulnerability Assessment Report**

It is essential for an organization to come up with a strong and clear vulnerability assessment report in order for the readers to understand it quickly and take action immediately. The following tips can be of great help to an organization that's having a hard time creating an effective vulnerability assessment report:

#### **1. Compose a descriptive title**

The first and most important component is the title of the report. A strong title is a mix of where the vulnerability occurs, domain or endpoint, and the type of vulnerability. The report title should focus on the main point and be descriptive to the point that it quickly provides an organization's security team a clear idea of the report and its possible criticality.

## **2. Write a direct, clear and short description**

The security team, program owners and clients don't have to spend too much time on reading, so the description should be concise. A strong way to come up with a description is to provide and include links or references to credible sources that can aid others to understand, identify and solve the issues. This could be CVE references or an OWASP link. It is advisable to avoid referencing Wikipedia or other websites that are less trusted.

## **3. Include a severity assessment**

A strong vulnerability assessment report should have an honest severity assessment of the vulnerabilities. Security teams have other work to attend to, so it is essential to create an honest severity assessment to help them prioritize which issues to address first. This is to ensure that the major and crucial problems discovered are taken care of immediately.

Studying the CVSS (Common Vulnerability Scoring System) can definitely provide an organization with a general idea of the criticality of the vulnerabilities.

## **4. Provide clear steps of reproduction**

This is one of the most important parts of the vulnerability assessment report. This is written from the perspective of the attacker and includes a step-by-step guide to follow by the security team. It is best to attach proof-of-concept files, images or video links to aid in explaining the complicated steps. In order for the issue to be fixed in less time, make sure to include all the required steps and make them specific.

## **5. Describe the impact of the vulnerability**

The impact reflects the report's level of severity. A strong report describes and explains what the attacker can do by referring to the result of the attack. Also, provide what information can be accessed by these attackers and how this problem can affect all the system users. It is best to escalate the impact of vulnerability and give the security team a realistic scenario of how the issue can be exploited by future attackers.

## **6. Recommend mitigations**

Providing potential mitigations can help the security team save time from researching. However, this should be done if the root cause of the issue is very clear and the organization has a good idea of that certain vulnerability.

In writing a vulnerability assessment report, always remember that the readers are human, too. Make sure to write the report in a conversational tone and include references for complicated information. Because the concepts are complex and technical, the report should be written to be read by non-technical readers, too.

Miscommunications will happen, but it is possible to minimize these mistakes by providing an effective and comprehensive report. Keeping a vulnerability assessment report simple, concise and clear makes it stronger and so is the mitigation. Contact RSI Security today to get started.



**Individual Activity:**

- *Perform vulnerability assessment.*

**Self-check quiz 7.1**

Check your understanding by answering the following questions:

Write the correct answer for the following questions.

1. What is Vulnerability Assessment?

Answer:

2. Write down some types of vulnerability Assessment?

Answer:



## Learning outcome 7.2 Perform Penetration testing



Contents:

- Vulnerability Assessment
- Gaining access
- Clearing track



Assessment criteria:

- 1 Vulnerability Assessment is performed.
- 2 Gaining access is performed.
- 3 Clearing track is performed following industry standard.
- 4 Reporting is performed following standard procedure.



Resources required:

Students/trainees must be provided with the following resources:

- Workplace (Actual or simulated), Server, Necessary software.



### **LEARNING ACTIVITY 7.2**

Learning Activity	Resources/Special Instructions/References
Perform Penetration testing	<ul style="list-style-type: none"> <li>▪ Information Sheets: 7.2</li> <li>▪ Self-Check: 7.2</li> <li>▪ Answer Key: 7.2</li> </ul>



## Information sheet 7.2

Learning objective: to perform penetration testing.

### Penetration Test

Penetration Testing or Pen Testing is a type of Security Testing used to cover vulnerabilities, threats and risks that an attacker could exploit in software applications, networks or web applications. The purpose of penetration testing is to identify and test all possible security vulnerabilities that are present in the software application. Penetration testing is also called Pen Test.

Types of Penetration Testing:

The type of penetration test selected usually depends on the scope and whether the organization wants to simulate an attack by an employee, Network Admin (Internal Sources) or by External Sources. There are three types of Penetration testing and they are

- Black Box Testing
- White Box Penetration testing
- Grey Box Penetration Testing

Five Stages of Penetration Testing

#### 1. Planning and reconnaissance

The first stage involves:

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

#### 2. Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

Static analysis – Inspecting an application’s code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.

Dynamic analysis – Inspecting an application’s code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application’s performance.

#### 3. Gaining Access

This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target’s vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

#### 4. Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization’s most sensitive data.

## 5. Analysis

The results of the penetration test are then compiled into a report detailing:

Specific vulnerabilities that were exploited

Sensitive data that was accessed

The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

### Clearing Track:

No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

The prime task in penetration testing is to gather system information. There are two ways to gather information –

'One to one' or 'one to many' model with respect to host: A tester performs techniques in a linear way against either one target host or a logical grouping of target hosts (e.g. a subnet).

'Many to one' or 'many to many' model: The tester utilizes multiple hosts to execute information gathering techniques in a random, rate-limited, and in non-linear.

After you complete the preparation work, you're ready to do a pen test! Here you walk through the process of the penetration test and then look at the results of the assessment, as well as methods of prevention.

Always be absolutely careful when you're working on a live network in production. Even better is to use a lab to learn how to conduct a pen test prior to doing it on a live network. In the spirit of "measure twice and cut once," please make sure you are careful.

For this pen test you will be starting at the network edge externally and attempting to make your way inside via any weaknesses found outside the network perimeter. Here, you review each portion of the pen test so you can see a building block approach that you can adapt to future projects. Successful attacks might differ regarding your intentions and methods, but each successful attack essentially contain these actions, which happen in this order and which you'll mimic during a pen test:

**Infiltration.** Just gaining access is fairly easy and straightforward where those with access to hacking tools such as script kiddies can basically run attacks all day probing your defenses, looking for ways in and if they are lucky enough... get in. This means that an attacker had to be connected to the technology that they want to exploit. You want to make sure that you test and scan for vulnerabilities that disallow anyone who is unauthorized to connect to a network they don't belong to. This should at least minimize the amount of attacks just by who is able to sneak past and connect with this first level of security. Defense in depth should start to thwart an attack. Make sure that you disallow login access from devices that can be probed in this fashion. An access control list (ACL) can be configured on the device to tell it to only allow access from trusted IPs.

**Penetration.** Once access is gained, another level of access can be gained. This hop-by-hop strategy is used by more experienced hackers who can gain access (via malware as an example in the form of a Trojan horse) and then launch another attack or move to another segment of your network looking for more access or data. By attempting to spoof, connect, gain

access, raise, and escalate privilege, assume the roles of other systems, and get in the middle of conversations, the attacker is able to potentially do a vast amount of damage. An attacker could have run an advanced persistent threat test (APT) and conducted eavesdropping that may have provided them more passwords or data. By running tools such as Burp Suite, Nessus, and Wireshark you can assess these vectors and ensure that access is limited in this area.

**Exploit.** At this stage, the hacker builds upon the previous level where access and access to data is actually achieved or granted and something of value can be garnished from the attack. Exploit is when the attacker has conducted the attack to gain and assume control; however, the next step would be to actually do the exploit. Steal data, take credentials, lie in wait for an APT, and do what they do. You can conduct similar attacks to see whether tools can flag these types of attacks taking place and how the security team can better monitor (and respond) to them.

**Conduct an advanced persistent threat.** The final level of this multilevel attack is the APT. To gain access, maintain it, have the ability to move around, and eventually gain access to valuable data while being undetected is the most valuable attack of them all.

**Exfiltration.** If they're able to do the previous steps and vanish without a trace, they have been highly successful in their attack.

You want to do the same as a pen tester and see whether you can set up ways to identify whether someone has been in the system without your knowledge. In the scenario with Company X, finish your pen test with an exfil and see whether any systems picked up a trace of your ability to access.

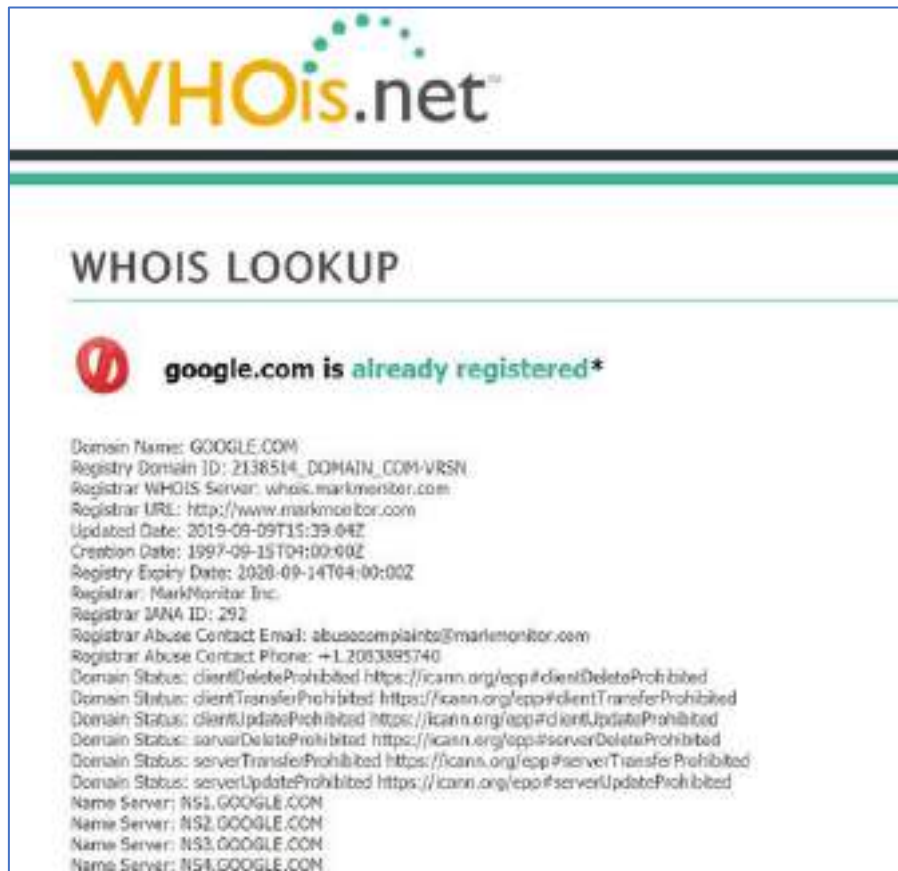
Company X, a technology company publicly traded on the market, is a medium to large sized company with approximately 10,000 employees.

The target will be data held internally, such as trade secrets on new technology development (research and development) that may be awaiting patents, sales data, or marketing information that has yet to be released to the public. You know the name of the company, and you want to launch a pen test to see whether you can find where this data may be located and/or saved. Here are the steps (and remember to document what you do and what you find as you go):

Find out where the data is stored. For the example of Company X, you'd do some preemptive reconnaissance work. You discover that the corporate data center and its mirror are in Colorado and Texas.

With location information in hand, track down the phone numbers at the main site and start probing from spoofed phone numbers. You can simply call the help desk and claim to be an internal resource looking to open a ticket and gain helpful information, such as source IPs (so you can get an actual IP address range for the internal network) and some other target information.

To gain access externally, use the WHOIS database for the DNS and locate a public IP address that you may be able to scan. The following image shows an example of looking up public information to gain some valuable insight when trying to find an attack vector. Here, if you run a search on a domain, you may be able to find their name servers that may be located



on their network. Not all companies do this, but this might provide a clue.

Doing a WHOIS search to gain intel

Run a ping to get the IP address from the domain name.

```
Command Prompt

(c) 2016 Microsoft Corporation. All rights reserved.

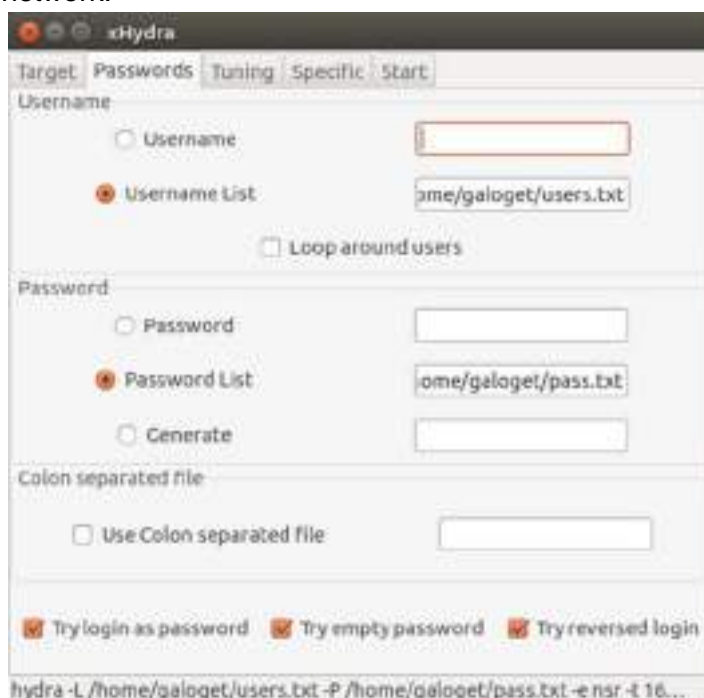
C:\Users\rshimonski>ping -a NS1.google.com

Pinging NS1.google.com [216.239.32.10] with 32 bytes of data:
Reply from 216.239.32.10: bytes=32 time=24ms TTL=45
Reply from 216.239.32.10: bytes=32 time=26ms TTL=45
Reply from 216.239.32.10: bytes=32 time=25ms TTL=45
Reply from 216.239.32.10: bytes=32 time=24ms TTL=45

Ping statistics for 216.239.32.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 26ms, Average = 24ms
```

Pinging at a command prompt to get an IP address or range to scan

Start to run Nmap or another tool against that IP. The goal is to find a public IP address or range to scan with your network mapper, such as Kali or Nmap, which can help to give you some access into the network.



Once in, find a way to access your targets. The target in this case is internally held data. Some of the easiest and most common ways to get the data are these:

Deploy a piece of malware into the network via email or other means. When users click it, you can gain access to their machine via a Trojan horse and from there you can control it like a zombie to do more reconnaissance work.

Brute-force attack a router (as an example) on the edge of a network you're scanning to see whether you can gain access by password cracking. In this scenario, say a router is left with HTTP configured and you can probe it with Kali's xhydra, shown below. Using this tool, you can find the router's username and password and can now enter and gain access.

Using Kali (Xhydra) to crack a router password

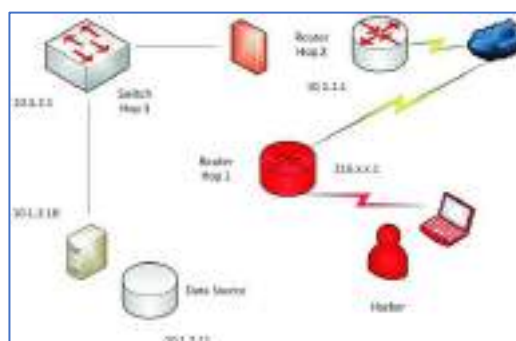
Once access is gained, get console access and then telnet or SSH to the device. The goal here is to use the device as a springboard into the next target that you identify.

When you have console access, look at the routing table, ARP table, configuration, and other items to develop a manual map of what can be seen.

Start to scan, map, and identify the rest of the network looking for assets. In the following image, a manual map has been created to reflect the pen tester's expectations from this first router hop.

A network map with IP addressing

Begin an APT, a long-term engagement. At this point in the test, you have done enough to begin an APT. You can lie dormant inside the network and remain undetected for the purpose of continuing research and removing more information. From moving from one device to another a Unix server has been found (which looks like a dual node cluster) at 10.1.2.10 and 10.1.2.11. Here the pen tester has probed ports and found a possible database port open that I may be able to gain access to.



Get out. You have successfully gained access using tools from basic identification of a possible entry point, built a map, and found a potential database that you can continue to manipulate to get more (hopefully valuable) data. At this point, you have proved enough that this pen test was successful and can disconnect from the system or get out by shutting down the tool or connection to the system.

Next steps to take after your penetration test

Although it may look like this hack took about five minutes to do, it can take much longer than that. It may take a week to get valuable information that allows you to probe a perimeter network with a public IP address. It may take days to crack a router if it is even set up to answer to non-specified IPs it doesn't know. It can take a long time to get to the next hop, which you may not be able to reach as well.

After you get through these edge devices, you may have a firewall that tracks your movement or flags you as a threat. Host intrusion detection system (IDS) applications such as Tripwire may flag your probes of a critical database system that required priority protection.

This attack may take a long time (for many reasons) for anyone to perform when coming from the outside in. Many hacks come from the inside because, when there is an avenue inside to take, it reduces time and effort just in gaining access. Can it be done? Absolutely, and that is why you do [vulnerability assessments](#) and pen tests to find and close every single one of the holes you identified.

What would detection look like if you are caught in the system mimicking a hacker? Well, because you're performing a test, you would likely have given notice that you would be in the system. However, if running a test undetected, you stand the same chance any hacker would in being caught in a system and either terminated (your connection) or left alone based on the protocols of the incident response team.

## **Penetration Testing Report or VAPT Report**

A Penetration Testing report is a document that contains a detailed analysis of the vulnerabilities uncovered during the security test. It records the weaknesses, the threat they pose, and possible remedial steps. The Pentest Report gives you a complete overview of vulnerabilities with a POC (Proof of Concept) and remediation to fix those vulnerabilities on priority. It also gives a score against each found issue and how much it can impact your application/website.

### **To create a powerful penetration testing report**

#### **1. Detailed outline of uncovered vulnerabilities**

The first and the most important component of an ideal pentesting report is an outline of all the vulnerabilities uncovered in VAPT and documentation on the basis of findings. Regardless of where the vulnerability lies in the application, a proper birds-eye view of the vulnerabilities gives your security and executive team a clear idea of the situation and the path ahead. A too technical or detailed approach will leave you and your team perplexed. In a good penetration testing report, you should also expect to see an explanation of where these vulnerabilities lie and how an attacker can manipulate them, preferably in laymen's language.

#### **2. Executive Summary & CVSS Score**

Not all stakeholders are security professionals. Keeping this in mind you must provide an executive summary of the pentesting report for the decision-makers. The executive summary does not cover technical details or terminology but the overview of the major findings is explained in layman's terms. The executive summary should be short, crisp, and well-formatted.

#### **3. Assessment of the business impact**



The next important component you should expect in a VAPT report is a detailed outline of the impact of the uncovered vulnerabilities on your business. By default, the numerical scoring assigned is mapped around Common Vulnerability Scoring System (CVSS). However, these scores often fail to take into account the severity of the vulnerabilities. Therefore, a pentester should employ more sophisticated ways to assign the scores. For example, a scoring system that assigns both comparable scores (low/medium/high/critical) and an explanation regarding the extent of severity each vulnerability possesses for the business, will bring the desired precision.

#### **4. Insight into Exploitation difficulty**

It is also important to mention the time period for which the pentester was exploiting the website unnoticed. The report should document how difficult it was to exploit the security loopholes. If it was easy for the pentester, it can be far easier for a hacker. It will also help you understand what you were doing wrong before, and rectify them.

#### **5. Technical Risks Briefing**

The vulnerability risk rating (or CVSS score) is a straightforward way to indicate the severity of a vulnerability. It provides a quick understanding of the vulnerabilities at just a glance.

However, when it comes to eradicating those vulnerabilities, just a rating or score won't be substantial. Thus, when drafting a penetration testing report you must provide an explanation of the highlighted vulnerabilities and technical risks. This briefing when coupled with contextualization adds even more weight to the report.

#### **6. Remediation**

Without remedial advice, a pentest report is just a document containing a list of vulnerabilities. Without proper remediation or suggestions for mitigation, your website or network will continue to stay unsafe. Some VAPT service providers do not include the remediation steps in their reports, stay away from them!

Instead, look for a VAPT service provider that provides proper remediation steps along with the list of vulnerabilities in the pentesting report. Remediation advice varies for different vulnerabilities. For example, for some vulnerabilities, only installing a security patch will be enough whereas for others intervention of a development team might be required to rectify code vulnerabilities. In either situation, remediation steps provided by the VAPT service company come in handy.

#### **7. Strategic Recommendations**

Strategic recommendations are often overlooked by most VAPT service providers. But they are crucial and can define your organization's outlook on security and shape your security strategies. Security is not just a destination, but a journey. In the absence of a defined security strategy, one-time security fixes can only do so much to protect your organization. Strategic recommendations from security experts will prove to be invaluable for your business, hence, look for a service provider that will give strategic recommendations to improve the working and security of your business.

**Individual Activity:**

- *Perform penetration testing.*

**Self-check quiz 7.2**

Check your understanding by answering the following questions:

1. What is Penetration Testing?

Answer:

2. What are the types of penetration testing?

Answer:

3. What is VAPT Report?

Answer:



## Answer keys

### Answer key 7.1

1. Answer:

A vulnerability assessment (or vulnerability testing) is the systematic evaluation of potential and existing threats and flaws in your organization's systems, networks, applications, hardware, and other parts of the IT ecosystem

2. Answer:

- Database assessment
- Web application assessment
- Host-based assessment
- Wireless network assessment

### Answer key 7.2

1. Answer:

Penetration Testing or Pen Testing is a type of Security Testing used to cover vulnerabilities, threats and risks that an attacker could exploit in software applications, networks or web applications.

2. Answer:

- Black Box Testing
- White Box Penetration testing
- Grey Box Penetration Testing

3. Answer:

A Penetration Testing report is a document that contains a detailed analysis of the vulnerabilities uncovered during the security test. It records the weaknesses, the threat they pose, and possible remedial steps.

<b>LEARNER JOB SHEET 5</b>			
<b>Qualification:</b>	Information System Security Management		
<b>Learning unit:</b>	Perform Vulnerability assessment		
<b>Learner name:</b>			
<b>Personal protective equipment (PPE):</b>			
<b>Materials:</b>			
<b>Tools and equipment:</b>			
<b>Performance criteria:</b>	<ol style="list-style-type: none"> <li>1. Vulnerability Assessment is performed.</li> <li>2. Gaining access is performed.</li> <li>3. Clearing track is performed following industry standard.</li> <li>4. Reporting is performed following standard procedure.</li> </ol>		
<b>Measurement:</b>			
<b>Notes:</b>	<ul style="list-style-type: none"> <li>• Identify where your most sensitive data is stored.</li> <li>• Uncover hidden sources of data.</li> <li>• Identify which servers run mission-critical applications.</li> <li>• Identify which systems and networks to access.</li> <li>• Review all ports and processes and check for misconfigurations.</li> <li>• Map out the entire IT infrastructure, digital assets, and any devices used</li> </ul>		
<b>Procedure:</b>	<ol style="list-style-type: none"> <li>1. Collect PPE, tools, equipment and materials</li> <li>2. Check the usability of PPE, tools, equipment and materials.</li> <li>3. Defining and planning the scope of testing</li> <li>4. Identify Vulnerability</li> <li>5. Analyse Data</li> <li>6. Perform Treating for the vulnerabilities</li> <li>7. Prepare VAPT report</li> </ol>		
<b>Learner signature:</b>		<b>Date:</b>	
<b>Assessor signature:</b>		<b>Date:</b>	
<b>Quality Assurer signature:</b>		<b>Date:</b>	
<b>Assessor remarks:</b>			
<b>Feedback:</b>			