INFORMATION SYSTEM SECURITY AND AUDIT

The Guide provides Knowledge in the following Areas:

- Introduction to Information system
- Information system Vulnerabilities, threats and risks
- Information system Security Control and Governance
- Continuity of Computer Operations
- Audit

a 2022

FOREWORD

Cybercrime appears unstoppable, there are thousands of cybercrimes every year, ranging in cost from a few hundred dollars to the millions. From the report compiled by Z. Smith et.al (2021), since 2018, it is estimated that the cost of global cybercrime reached over $1 trillion. The estimated the monetary loss from cybercrime was approximately $945 billion, this average cost rose steadily from $300 billion in 2013 to $475 billion in 2014 to $522 billion in 2018.

what accounts for this increase is that cybercriminals are using more effective techniques, with cybercriminals "actively targeting non-financial organizations that include healthcare bodies, pharmaceutical companies, academia, medical research organizations, and local governments; this is mind boggling in the first glowing IT sector.

The risk of cybercrime to operations and profits continues to grow for many organizations. Global spending on cyber security, was expected to exceed $145 billion in 2020.

In the research for smith report a total of 1,500 companies were surveyed, only 4% claimed that they did not experience any sort of cyber incident in 2019.The damage from malware and spyware represented the highest cost to organizations, closely followed by data breaches. Affected companies said the biggest non-monetary loss was in productivity and lost work hours.
Despite this, it was found that most organizations do not have plans in place to reduce the effect of security incidents on their operations. From the report slightly more than half of the surveyed organization said they do not have plans to both prevent and respond to a cyber-incident. Out of the 951 organizations that had a response plan, only 32% said the plan was actually effective.

While many cyber-attacks can be managed in house, major incidents often require contracting with outside consultants at high rates, forming a significant portion of the cost of a large-scale incident. From the report Only 213 out of 1,332 surveyed companies reported that they dealt with cyber incidents without third-party support. Typically, they relied on cyber security organizations or response teams to help with ***CONTAINMENT, RECOVERY AND REMEDIATION,*** in most of these cases, consultants were used to assist in *containment, recovery and remediation*.
Cyber-attacks range from minor attacks that are easily handled in house to major breaches that require a coordinated response involving leadership throughout the organization, lawyers, public relations specialists, and cyber experts, many of whom must be brought in as consultants.

On December 14, 2021, Google asked its 2.6 billion Chrome users to update the browser urgently to fix a "critical" bug that was being exploited by hackers.
As cyber-attacks have become more prevalent, so have the consultants who can help remediate a major attack or breach that would otherwise overwhelm a victim organization. Many consulting firms provide cyber services, these consultancies continue to expand to meet demand for their services, with the shortage of qualified experts driving daily rates per consultant into the thousands of dollars. Fees paid to consulting firms are likely to be a significant component of the overall cost of responding to a major incident, for example the U.K.'s National Health Service spent a total of £73 million on IT support in response to the WannaCry attack, much of which went to outside consultants.

From a report compiled by Communications Authority of Kenya, National Kenya Computer Incident Response Team/Coordination (KE-CIRT/CC), in period July - September 2021, the National KE-CIRT/CC detected 143,040,599 cyber threat events, which was a 268.883% increase from the 38,776,699 threat events detected in the previous period, April - June 2021. This increase in cyber threat events detected is attributed to the significant increase in targeted attacks at critical systems and services; increased activity by ransom ware groups; adoption of more sophisticated tools by cyber threat actors; increased targeted attacks at Internet of Things (IoT) devices; increased exploits of third-party mobile application vulnerabilities; increased targeted attacks at unsecured infrastructure; and increased adoption of botnet and Distributed Denial of Service (DDoS) attack techniques. This is illustrated in the table below.

	Threats Detected	April-June 2021	July – September 2021
1	Malware	23,053,190	70,501,144
2	DDOS/Botnet	11,272,402	49,816,062
3	Web Application Attacks	2,564,173	478,123
4	System Vulnerabilities	1,886,934	22,245,270
	Totals	38,776,699	143,040,599

While opening Cyber Security Strategy 2022 – 2026 workshop in Naivasha in june 2022, interior and National Government Coordination Cabinet Secretary (CS), Dr. Fred Matiang`i, called on all players in the cyber space to work together in securing the cyber space. The minister said most of the private and government businesses are now being transacted on the cyber space which predisposes these businesses to cybercrime. He said the increase in technology and growth of the same has soared transactions from 1.9trillion 10 years ago to over 6.8trillion in 2022, indicating an urgent need to protect this space.

He further observed that the *Huduma Namba program* that was challenged in court was actually meant to protect individual data by putting it in a central place instead of it being scattered all over the place which make such data unsecure.

Cybercriminals find Africa an attractive scene to stage the attacks because many firms have yet to invest adequately in anti-hacking measures. Various reports indicate that various African countries, Kenyan among them, have in the recent past witnessed a surge in cases of cyber attacks.

“It’s alarming to think that Kenyan businesses are dealing with almost 540 more weekly cyber-attacks than their peers across the globe,” Pankaj Bhula, Check Point’s Regional Director for Africa told Digital Business.“This signals an urgent need for Kenya’s businesses to take a proactive approach to cybersecurity solutions, while focusing on companywide education on security hygiene to keep users and the business safe online.

When a small business owner is faced with the responsibilities of production economics, financial reports and marketing all at the same time, cybersecurity can often appear complicated and, at times, unnecessary. However, this disregard for IT security is being exploited by cybercriminals.

Companies and agencies need to do more to prevent cyber incidents from occurring. And they also need to do more to speed up service restoration, address business disruptions, and repair damage to employee morale and customer trust.

Bernard Mokua
Lecturer in Information system security and Control

Chapter One
INTRODUCTION TO INFORMATION SYSTEMS

System is a set of interacting or interdependent components forming an integrated whole or a set of elements (often called *'components')* and relationships which are different from relationships of the set or its elements to other elements or sets.

Data consists of the raw facts representing events occurring in the organization before they are organized into an understandable and useful form for humans.

Information is data that has been processed in such a way as to be meaningful to the person who receives it. It provides context for data and enables decision making processes.

Uses of Information

Businesses and other organizations need information for many purposes: we have summarized the five main uses in the table below.

- ***Planning***

To plan properly, a business needs to know what resources it has (e.g. cash, people, machinery and equipment, property, customers). At the planning stage, information is important as a key ingredient in decision-making.

- ***Recording***

Information about each transaction or event is needed. Just as importantly, information needs to be recorded so that the business can be properly managed.

- ***Controlling***

Once a business has produced its plan it needs to monitor progress against the plan - and control resources to do so. So information is needed to help identify whether things are going better or worse than expected, and to spot ways in which corrective action can be taken

- ***Measuring***

Performance must be measured for a business to be successful. Information is used as the main way of measuring performance. For example, this can be done by collecting and analysing information on sales, costs and profits

- ***Decision-making***

i. Strategic information**:** used to help plan the objectives of the business as a whole and to measure how well those objectives are being achieved. Examples of strategic information include:
- Profitability of each part of the business
- Size, growth and competitive structure of the markets in which a business operates

ii.Tactical Information: this is used to decide how the resources of the business should be employed. Examples include:
- Information about business productivity (e.g. units produced per employee; staff turnover)

iii. Operational: Information: this information is used to make sure that specific operational tasks are carried out as planned/intended (i.e. things are done properly).

For example, a production manager will want information about the extent and results of quality control checks that are being carried out in the manufacturing process.

An Information System (IS) can be any organized combination of people, hardware, software, communications networks, data resources, and policies and procedures that stores, retrieves, transforms, and disseminates information in an organization.

An important factor of computer based information system is ***precision,*** *which may not apply to other types of systems.*

Information system

An information system is a combination of software, hardware, and telecommunication networks to collect useful data, especially in an organisation. Many businesses use information technology to complete and manage their operations, interact with their consumers, and stay ahead of their competition

Components of information systems

An information system is described as having five components.

Computer hardware

This is the physical technology that works with information. Hardware can be as small as a smartphone that fits in a pocket or as large as a supercomputer that fills a building.

Computer software

Software can be divided into two types: system software and application software.

Telecommunications

This component connects the hardware together to form a network. Connections can be through wires, such as Ethernet cables or fibre optics, or wireless, such as through Wi-Fi.

Databases /Data

A database is a place where data is collected and from which it can be retrieved by querying it using one or more specific criteria. A data warehouse contains all of the data in whatever form that an organization needs.

Human resources and procedures

the people that are needed to run the system and the procedures they follow so that the knowledge in the huge databases and data warehouses can be turned into learning that can interpret what has happened in the past and guide future action.

Computer security

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

Cyber space

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers i.e. concept describing a widespread interconnected digital technology.

Cyberspace is an embodied switched network for moving information traffic further characterized by varying degrees of access, navigation, information- activity, augmentation (and trust), and these characteristics can be taken into account sufficiently for drawing legal conclusions.

The control of cyberspace is thus important not only because of the actions of individual participants but because the infrastructure of cyberspace is now fundamental to the functioning of national and international security systems, trade networks, emergency services, basic communications, and other public and private.

Securing Cyber Space

Increased connectivity of people and devices to the Internet and to each other has created an ever-expanding attack surface that extends throughout the world. As a result, cyberspace has become the most active threat domain in the world and the most dynamic threat to the Homeland.
The huge increase in the use of digital technologies throughout the COVID-19 pandemic has led to far greater numbers of connected devices, increasing the attack surface for cyber criminals.

Cyber space security

Focus on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Chapter Two
INFORMATION SYSTEM VULNERIBILITIES, THREATS AND RISKS

Before computer automation, data about individuals or organizations were maintained and secured as paper records dispersed in separate business or organizational units. Information systems concentrate data in computer files that can potentially be accessed by large numbers of people and by groups outside of the organization.

When large amounts of data are stored in electronic form they are vulnerable to many more kinds of threats than when they exist in manual form. Through communications networks, information systems in different locations can be interconnected. The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network.

All *risks, threats, and vulnerabilities* are measured for their potential capability to compromise one or all of the AIC principles

2.1. VULNERIBILITY

A vulnerability, in information technology (IT), is a flaw in code or design that creates a potential point of security compromise for an endpoint or network. Vulnerabilities create possible attack vectors, through which an intruder could run code or access a target system's memory.

The exposure of an information resource is the harm, loss, or damage that can result if a threat compromises that resource. An information resource's vulnerability is the possibility that the system will be harmed by a threat.

Hence a software, hardware, or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment.

Vulnerability characterizes the absence or weakness of a safeguard that could be exploited. Without strong safeguards, valuable data could be lost, destroyed, or could fall into the wrong hands, revealing important trade secrets or information that violates personal privacy.

One of the biggest causes of cyber and information security vulnerabilities is that systems and software are not regularly updated.

E.g.: a service running on a server, unpatched applications or operating system software, unrestricted modem dial-in access, an open port on a firewall, lack of physical security etc.

The four main types of vulnerabilities in information security are

- Network Vulnerabilities. These are issues with a network’s hardware or software that expose it to possible intrusion by an outside party. Examples include insecure Wi-Fi access points and poorly-configured firewalls.
- Operating System Vulnerabilities. These are vulnerabilities within a particular operating system that hackers may exploit to gain access to an asset the OS is installed on—or to cause damage.

Examples include default superuser accounts that may exist in some OS installs and hidden backdoor programs.

- Human Vulnerabilities. The weakest link in many cybersecurity architectures is the human element. User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.
- Process Vulnerabilities. Some vulnerabilities can be created by specific process controls (or a lack thereof). One example would be the use of weak passwords (which may also fall under human vulnerabilities)

Network vulnerabilities

Large public networks such as the Internet are more vulnerable than internal networks because they are virtually open to anyone. The Internet is so huge that when abuses do occur, they can have an enormously widespread impact. When the Internet becomes part of the corporate network, the organization's information systems are even more vulnerable to actions from outsiders.

Computers that are constantly connected to the Internet by cable modems or Digital Subscriber Line (DSL) are more open to penetration by outsiders because they use fixed Internet addresses where they can be easily identified. (With dial-up service, a temporary Internet address is assigned for each session.) A fixed Internet address creates a fixed target for hackers.

Telephone service based on Internet technology can be more vulnerable than the switched voice network if it does not run over a secure private network. Most Voice over IP (VoIP) traffic over the public Internet is not encrypted, so anyone linked to a network can listen in on conversations. Hackers can intercept conversations to obtain credit card and other confidential personal information or shut down voice service by flooding servers supporting VoIP with bogus traffic.

Vulnerability has also increased from widespread use of e-mail and instant messaging (IM). E-mail can contain attachments that serve as springboards for malicious software or unauthorized access to internal corporate systems. Employees may use e-mail messages to transmit valuable trade secrets, financial data, or confidential customer information to unauthorized recipients. Popular instant messaging applications for consumers do not use a secure layer for text messages, so they can be intercepted and read by outsiders during transmission over the public Internet. IM activity over the Internet can in some cases be used as a back door to an otherwise secure network

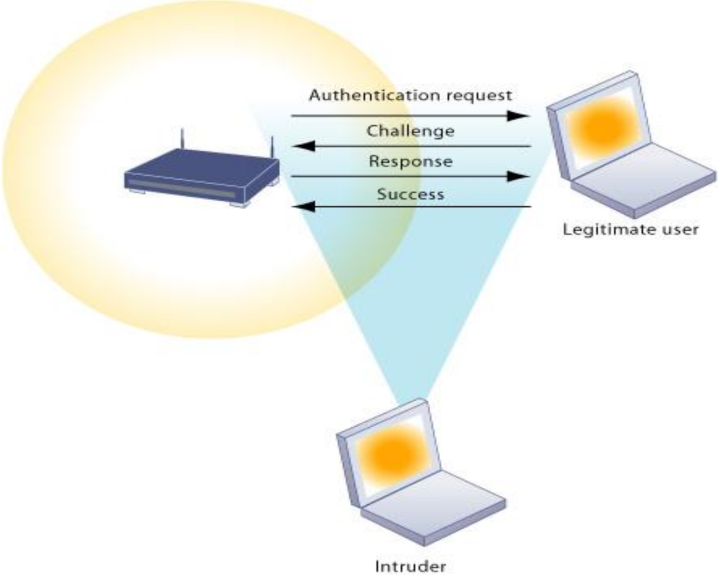
WIRELESS SECURITY CHALLENGES

Wireless networks using radio-based technology are even more vulnerable to penetration because radio frequency bands are easy to scan. Although the range of Wireless Fidelity (Wi- Fi) networks is only several hundred feet, it can be extended up to one-fourth of a mile using external antennae. Local area networks (LANs) that use the 802.11b (Wi-Fi) standard can be easily penetrated by outsiders armed with laptops, wireless cards, external antennae, and freeware hacking software. Hackers use these tools to detect unprotected networks, monitor network traffic, and in some cases, gain access to the Internet or to corporate networks.

Wireless networks in many locations do not have basic protections against war driving, in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.

Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

Intruders can also use the information they have gleaned about Internet Protocol (IP) addresses and SSIDs to set up rogue access points on a different radio channel in physical locations close to users to force a user's radio NIC to associate with the rogue access point. Once this association occurs, hackers using the rogue access point can capture the names and passwords of unsuspecting users.

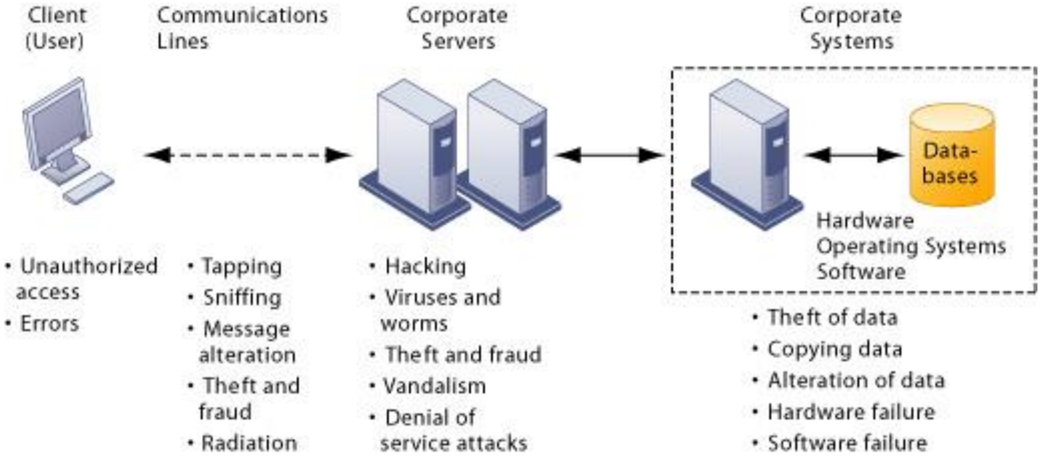


An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. These crimes target the confidentiality, integrity, or availability (known as the "CIA triad") of resources possessed by an application, its creators, and its users.

The figure below illustrates the most common threats against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions.

In the multitier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter messages without authorization.

Radiation can disrupt a network at various points as well. Intruders can launch denial of service attacks or malicious software to disrupt the operation of Web sites. Those capable of penetrating corporate systems can destroy or alter corporate data stored in databases or files.



Contemporary security challenges and vulnerabilities
The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

Hackers and Cyber vandalism
A hacker is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term cracker is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker are used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use.

Hacker activities have broadened beyond mere system intrusion to include theft of goods and information, as well as system damage and cyber vandalism, the intentional disruption, defacement, or even destruction of a Web site or corporate information system.

2.2. THREAT

A threat is any potential danger to information or systems. A threat is a possibility that someone (person, s/w) would identify and exploit the vulnerability.

The entity that takes advantage of vulnerability is referred to as a threat agent. E.g.: A threat agent could be an intruder accessing the network through a port on the firewall

Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant financial losses. Information security damages can range from small losses to entire information system destruction. The effects of various threats vary considerably: some affect the confidentiality or integrity of **data** while others affect the **availability of a system.**

Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge. To improve our understanding of security threats, we propose a security threat classification model which allows us to study the threats class impact instead of a threat impact as a threat varies over time.

Examples of Access Control Threats

Denial of Service (DoS/DdoS)

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

The purpose of DoS attacks is to force the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service

Types of DoS Attacks

A DoS attack can be perpetrated in a number of ways. There are five basic types of attack:

- Consumption of computational resources, such as bandwidth, disk space, or CPU time;
- Disruption of configuration information, such as routing information;
- Disruption of state information, such as unsolicited resetting of TCP sessions;
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Countermeasures

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software.
- Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
- Follow good security practices for distributing your email address.
-

Buffer Overflows

A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

Buffer Overflow Techniques

- *Stack Buffer Overflow*
  - A stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside of the intended data structure; usually a fixed length buffer.

  - Stack buffer overflow bugs are caused when a program writes more data to a buffer located on the stack than there was actually allocated for that buffer. This almost always results in corruption of adjacent data on the stack, and in cases where the overflow was triggered by mistake, will often cause the program to crash or operate incorrectly.
  - A technically inclined and malicious user may exploit stack-based buffer overflows to manipulate the program

- *Heap Buffer Overflow*
  - A heap overflow is another type of buffer overflow that occurs in the heap data area. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.
  - Exploitation goes as follows: If an application copies data without first checking to see if it fits into the chunk (blocks of data in the heap), the attacker could supply the application with a piece of data that is too large, overwriting heap management information (metadata) of the next chunk. This allows an attacker to overwrite an arbitrary memory location with four bytes of data. In most environments, this may allow the attacker control over the program execution.

Countermeasure

- Choice of programming language
- Use of safe libraries
- Stack-smashing protection which refers to various techniques for detecting buffer overflows on stack-allocated variables. The most common implementation being StackGuard, and SSP
- Executable space protection which is the marking of memory regions as non-executable, such that an attempt to execute machine code in these regions will cause an exception. It makes use of hardware features such as the NX bit (Non Execute bit).
- Address space layout randomization: A technique which involves arranging the positions of key data areas, usually including the base of the executable and position of libraries, heap, and stack, randomly in a process' address space.

Spoofing/Masquerading

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Popular Spoofing Techniques

- *Man-in-the-middle attack (MITM):* An attack in which an attacker is able to read, insert and modify at will messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims
- *IP address Spoofing* : refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
- *URL spoofing*: A Spoofed URL describes one website that poses as another
- *Phishing* :An attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

- *Referrer spoofing*:It is the sending of incorrect referrer information along with an HTTP request, sometimes with the aim of gaining unauthorized access to a web site. It can also be used because of privacy concerns, as an alternative to sending no referrer at all.
- *Spoofing of file-sharing Networks*: Polluting the file-sharing networks where record labels share files that are mislabeled, distorted or empty to discourage downloading from these sources.
- *Caller ID spoofing* :This allows callers to lie about their identity, and present false names and numbers, which could of course be used as a tool to defraud or harass
- *E-mail address spoofing:*A technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message by changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields.
- *Login spoofing* : A technique used to obtain a user's password. The user is presented with an ordinary looking login prompt for username and password, which is actually a malicious program, usually called a Trojan horse under the control of the attacker. When the username and password are entered, this information is logged or in some way passed along to the attacker, breaching security.

Countermeasures

- Be skeptical of e-mails indicating that you need to make changes to your accounts or warnings indicating that accounts will be terminated without you doing some type of activity online.
- Call the legitimate company to find out if this is a fraudulent message.
- Review the address bar to see if the domain name is correct.
- When submitting any type of financial information or credential data, an SSL connection should be set up, which is indicated in the address bar and a closed-padlock icon in the browser at the bottom-right corner.

Shoulder Surfing

- Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is particularly effective in crowded places because it's relatively easy to observe someone as they:
  - Fill out a form
  - Enter their PIN at an automated teller machine or a POS Terminal
  - Use a calling card at a public pay phone
  - Enter passwords at a cybercafe, public and university libraries, or airport kiosks.
  - Enter a digit code for a rented locker in a public place such as a swimming pool or airport.

Object Reuse

Object reuse issues pertain to reassigning to a subject media that previously contained one or more objects.

The sensitive information that may be left by a process should be securely cleared before allowing another process the opportunity to access the object. This ensures that information not intended for this individual or any other subject is not disclosed.

For media that holds confidential information, more extreme methods should be taken to ensure that the files are actually gone, not just their pointers.

Countermeasures

- Sensitive data should be classified by the data owners.
- How the data is stored and accessed should also be strictly controlled and audited by software controls.
- Before allowing one subject to use media that was previously used, the media should be erased or degaussed. If media holds sensitive information and cannot be purged, there should be steps on how to properly destroy it so that there is no way for others to obtain this information.

Data Remanence

Data remanence is the residual representation of data that has been in some way been nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium.

Data remanence may make inadvertent disclosure of sensitive information possible, should the storage media be released into an uncontrolled environment.

Counter measures

- Methods to Countermeasure
  - Overwriting
    - A common method used to counter data remanence is to overwrite the storage medium with new data. This is often called a wiping or shredding a file or disk. The simplest overwrite technique writes the same data everywhere -- often just a pattern of all zeros. At a minimum, this will prevent the data from being retrieved simply by reading from the medium again, and thus is often used for clearing.
  - Degaussing
    - Degaussing is the removal or reduction of a magnetic field. Applied to magnetic media, degaussing may purge an entire media element quickly and effectively
    - Degaussing often renders hard disks inoperable, as it erases low-level formatting which is only done at the factory, during manufacture.
  - Encryption
    - Encrypting data before it is stored on the medium may mitigate concerns about data remanence.
    - Encryption may be done on a file-by-file basis, or on the whole disk.
  - Physical destruction
    - Physical destruction of the data storage medium is generally considered the most certain way to counter data remanence, although also at the highest cost.

Backdoor/Trapdoor

A backdoor is a malicious computer program or particular means that provide the attacker with unauthorized remote access to a compromised system exploiting vulnerabilities of installed software and bypassing normal authentication.

A backdoor works in background and hides from the user. It is very similar to a virus and therefore is quite difficult to detect and completely disable.

A backdoor is one of the most dangerous parasite types, as it allows a malicious person to perform any possible actions on a compromised computer. The attacker can use a backdoor to:

- spy on a user,
- manage files,
- install additional software or dangerous threats,

  - control the entire system including any present applications or hardware devices,
  - shutdown or reboot a computer or
  - attack other hosts.

Countermeasure

- Powerful antivirus and anti-spyware products

Dictionary Attacks

Dictionary attacks are launched by programs which are fed with a lists (dictionaries) of commonly used words or combinations of characters, and then compares these values to capture passwords. Once the right combination of characters is identified, the attacker can use this password to authenticate herself as a legitimate user.
Sometimes the attacker can even capture the password file using this kind of activity.

Countermeasures

To properly protect an environment against dictionary and other password attacks, the following practices should be followed:

- Do not allow passwords to be sent in cleartext.
- Encrypt the passwords with encryption algorithms or hashing functions.
- Employ one-time password tokens.
- Use hard-to-guess passwords.
- Rotate passwords frequently.
- Employ an IDS to detect suspicious behavior.
- Use dictionary cracking tools to find weak passwords chosen by users.
- Use special characters, numbers, and upper- and lowercase letters within the password.
- Protect password files.

Bruteforce Attacks

- Brute force is defined as “trying every possible combination until the correct one is identified.”
- The most effective way to uncover passwords is through a hybrid attack, which combines a dictionary attack and a brute force attack
- A brute force attack is also known as an exhaustive attack.
- These are usually used for wardialing in hopes of finding a modem that can be exploited to gain unauthorized access.

Countermeasures

For phone brute force attacks, auditing and monitoring of this type of activity should be in place to uncover patterns that could indicate a war dialing attack:

- Perform brute force attacks to find weaknesses and hanging modems.
- Make sure only necessary phone numbers are made public.
- Provide stringent access control methods that would make brute force attacks less successful.
- Monitor and audit for such activity.
- Employ an IDS to watch for suspicious activity.
- Set lockout thresholds.

Social Engineering

Social engineering is a collection of techniques used for manipulation of the natural human tendency to trust in order to obtain information that will allow a hacker to gain unauthorized access to a valued system and the information that resides on that system.

Forms of a Social engineering attack

- Physical: the workplace, the phone, your trash, and even on-line
- Psychological: Persuasion
- Reverse Social Engineering

Countermeasures

- Having proper security policies in place which addresses both physical and psychological aspects of the attack
- Providing proper training to employees, helpdesk personnel

Other threats can affect hardware, software, and the information you store include:

- Viruses are designed so that they can be easily transmitted from one computer or system to another. Often sent as email attachments, viruses corrupt and co-opt data, interfere with your security settings, generate spam, and may even delete content.
- Computer worms are similar; they spread from one computer to the next by sending themselves to all of the user's contacts and subsequently to all contacts' contacts.
- Trojans. These malicious pieces of software insert themselves into a legitimate program. Often, people voluntarily let trojans into their systems in email messages from a person or an advertiser they trust. As soon as the accompanying attachment is open, your system becomes vulnerable to the malware within.
- Bogus security software that tricks users into believing that their system has been infected with a virus. The accompanying security software that the threat actor provides to fix the problem causes it.
- The adware tracks your browsing habits and causes particular advertisements to pop up. Although this is common and often something you may even agree to, adware is sometimes imposed upon you without your consent.
- Spyware is an intrusion that may steal sensitive data such as passwords and credit card numbers from your internal systems.
- Phishing attacks are social engineering infiltrations whose goal is to obtain sensitive data: passwords and credit card numbers incorrectly. Via emails or links coming from trusted companies and financial institutions, the hacker causes malware to be downloaded and installed.
- SQL injections are network threats that involve using malicious code to infiltrate cyber vulnerabilities in data systems. As a result, data can be stolen, changed, or destroyed.
- Man-in-the-middle attacks involve a third party intercepting and exploiting communications between two entities that should remain private. Eavesdropping occurs, but information can be changed or misrepresented by the intruder, causing inaccuracy and even security breaches.

- Rootkit tools gain remote access to systems without permission and can lead to the installation of malware and the stealing of passwords and other data.

2.3. RISK

Risk is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact. Reducing vulnerability and/or threat reduces the risk.
Risk is the probability of loss of asset, exposure to threat, and potential damage from a cyberattack. It is basically the meeting point of threat and vulnerability.

E.g.: If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.

- Exposure

An exposure is an instance of being exposed to losses from a threat agent.
Vulnerability exposes an organization to possible damages.
E.g.:If password management is weak and password rules are not enforced, the company is exposed to the possibility of having users' passwords captured and used in an unauthorized manner.

- Countermeasure or Safeguard

It is an application or a software configuration or hardware configuration or a procedure that mitigates the risk.

E.g.: strong password management, a security guard, access control mechanisms within an operating system, the implementation of basic input/output system (BIOS) passwords, and security-awareness training.

The Relation between the Security Elements

Example 1

If a company has antivirus software but does not keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks.
The threat is that a virus will show up in the environment and disrupt productivity.
The likelihood of a virus showing up in the environment and causing damage is the risk.
If a virus infiltrates the company's environment, then vulnerability has been exploited and the company is exposed to loss.
The countermeasures in this situation are to update the signatures and install the antivirus software on all computers
Threat Agent gives rise to Threat exploits Vulnerability leads to Risk can damage Assets and causes an Exposure can be counter measured by Safeguard directly effects Threat Agent

Example 2
Target: A bank contains money.
Threat: There are individuals who want, or need, additional money.
Vulnerability: The bank uses software that has a security flaw.
Exposure: 20% of the bank's assets are affected by this flaw.

Exploit: By running a small snippet of code (malware), the software can be accessed illegally.

Threat Agent: There are hackers who have learned how to use this malware to control the bank's software.

Exploitation: The hackers access the software using the malware and steal money.

Impact: The bank loses monetary assets, reputation, and future business.

Risk: The likelihood that a hacker will exploit the bank's software vulnerability and impact the bank's reputation and monetary resources.

Examples: Timeline chronicles ~ some cyber incidents out of 200 cyber incidents targeting financial institutions since 2007

- Beanstalk Farms cryptocurrency theft

On April 17, 2022, the decentralised finance platform Beanstalk Farms lost $180 million in a cryptocurrency heist.

- TransUnion SA data breach

March 17 2022 Credit bureau TransUnion SA suffered a cyber attack which saw around three million customer's data stolen by a criminal third party.

- Moscow Stock Exchange and Sberbank cyber attack

On February 28, 2022, the Moscow Stock Exchange and Sberbank, Russia’s largest lender, were hit by DDoS attacks that took their websites offline.

- Aon ransomware attack

On February 25, 2022, global insurance and reinsurance broker, Aon was hit by a ransomware attack, causing limited disruption to a number of their services.

- OCBC phishing scam

On December 23, 2021, around 790 banking customers of Singporean bank OCBC were targeted in a phishing scam resulting in a loss of at least $13.7 million.

- AscendEX hot wallet breach

On December 12, 2021, crypto exchange AscendEX lost $77.7 million in a breach of its hot wallet.

- BadgerDAO DeFi protocol hack

On December 2, 2021, decentralied finance ("DeFi") protocol BadgerDAO was hit by a cyber attack in which hackers stole $120.3 million in crypto.

- Ecuadorian Pichincha Bank disrupted by cyber attack

On October 10, 2021, Pichincha Bank in Ecuador was hit by a cyber attack that disrupted customers' access to bank services, including their online and mobile app tools.

- Taiwanese DeFi Platform hit by cyber attack

On August 30, 2021, Cream Finance, a Taiwanese decentralised finance platform, lost over $29 million in cryptocurrency assets to hackers.

- FBI Attributes Loss of $4 billion to Cybercrime

On March 17, 2021, the FBI released its Internet Crime Report 2020 which stated that American victims reported $4.2 billion in losses as a result of cybercrime and internet fraud to the FBI last year.

- Indonesian Fintech Data Breach

On October 31, Indonesian fintech company Cermati reported 2.9 million users' information was leaked and sold in a hacker forum.

- Payments Processor Juspay Data Leak

On August 18, 2020, payments processor Juspay's was hacked through a compromised server, resulting in the leak of over 100 million debit and credit card users.

- Finance Sector RDoS Campaign

On August 17, Akamai, a global content delivery network, reported an ongoing campaign of RDoS (Ransom DDoS) attacks targeting the financial sector and other businesses.

- NetWalker Ransomware Attacks

On August 4, 2020, McAfee reported that ransomware-as-a-service (RaaS) provider NetWalker had made $25 million over the previous five months through ransomware attacks.

- Norfund Business Email Compromise

On May 13, Norfund, Norway's state investment fund, was subject to a $10 million heist that involved business email compromise.

- South Korean and US Payment Card Leak

On April 9, 2020, a cache of 400,000 payment card records from banks in South Korea and the U.S. were uploaded to a well-known underground marketplace.

- Cardplanet Fraud

On November 13, 2019, the United States charged a Russian man for running ‘Cardplanet,’ a card trading platform worth almost $20 million USD that buys and sells stolen payment card details.

- Bank of Valletta

On February 13 2019, the Bank of Valletta (BOV), Malta’s largest and oldest bank, shut down operations after an attempted theft of €13 million.

- Bancomext Attempted SWIFT Heist

On January 9, 2018, attackers attempted to use fraudulent SWIFT transactions to steal $110 million from Bancomext, Mexico’s state-owned trade bank, but the money was ultimately recovered.
Costa Rican Financial Institution Attempted Theft
In January 2018, attackers attempted to steal $19 million from a private Costa Rican financial institution.

- Standard Bank Theft

On May 15, 2016, attackers stole $19 million from South Africa’s Standard Bank by making 14,000 withdrawals over 3 hours from 1,700 ATMs across Japan.
Guatemalan Financial Institution Theft
In December 2015, attackers stole $16 million from a Guatemalan financial institution.

- Bank of the West DDoS Attack

On Christmas Eve 2013, Bank of the West was the victim of a DDoS attack used to disguise $900,000 in fraudulent transfers out of accounts belonging to Ascent Builders, a Californian construction firm.

- Postbank Heist

From January 1-3 2020, hackers targeted Postbank, a division of the South African Post Office, breaching the organization's IT system and siphoning off cash into dummy accounts.

Risk Management Practices

A risk management team should have the ability and follow the best practices, some of them which include:

- Establishing a risk acceptance level as provided by senior management
- Documenting risk assessment processes and procedures
- Establishing proper procedures for identifying and mitigating risks
- Getting support from senior management for appropriate resource and fund allocation
- Defining contingency plans where assessments indicate that they are necessary

- Ensure that security-awareness training is provided for all staff members associated with information assets.
- Strive to establish improvement (or risk mitigation) in specific areas when necessary
- Should map legal and regulation compliancy requirements to control and implement requirements
- Develop metrics and performance indicators to be able to measure and manage various types of risks
- Identify and assess new risks as the environment and company changes
- Integrate IRM and the organization's change control process to ensure that changes do not introduce new vulnerabilities

Ways to deal with Risk

There are four basic ways of dealing with risks:

- Transfer it: If a company's total or residual risk is too high and it purchases an insurance then it is transfer of risk to the insurance company
- Reject it: If a company is in denial about its risk or ignore it, it is rejecting the risk
- Reduce it: If a company implements countermeasures, it is reducing the risk
- Accept it: If a company understands the risk and decides not to implement any kind of countermeasures it is accepting the risk. And this is actually what all computer systems boil down to. There is no way to mitigate the risk if the system is going to connect to the internet. Having only one user without any networking with others computer systems is the closet you can ever get to not having any risks.

Risk Assessment/Analysis

Risk analysis is a method of identifying vulnerabilities and threat and assessing the possible damage to determine where to implement security safeguards

Why Risk Analysis?

- ✓ To ensure that security is cost effective, relevant, timely, and responsive to threat.
- ✓ To provide a cost/benefit comparison, this compares the annualized cost of safeguards to the potential cost of loss.
- ✓ Help integrate the security program objectives with the company's business objectives and requirements
- ✓ To provide an economic balance between the impact of the threat and the cost of the countermeasure.

Analyze the risk

There are two approaches of analyzing risk

- ✓ Quantitative Approach
- ✓ Qualitative Approach

A Quantitative Approach to Risk Analysis

Quantitative analysis uses risk calculations that attempt to predict the level of monetary losses and percentage of chance for each type of threat.

Quantitative risk analysis also provides concrete probability percentages when determining the likelihood of threats.

Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.

Sample Steps for a Quantitative Risk Analysis

Step 1: Assign Value to Assets- For each asset, answer the following questions to determine its value

- What is the value of this asset to the company?
- How much does it cost to maintain?
- How much does it make in profits for the company?
- How much would it be worth to the competition?
- How much would it cost to re-create or recover?
- How much did it cost to acquire or develop?
- How much liability are you under pertaining to the protection of this asset?

Step 2: Estimate Potential Loss per Threat- To estimate potential losses posed by threats, answer the following questions:

- What physical damage could the threat cause and how much would that cost?
- How much loss of productivity could the threat cause and how much would that cost?
- What is the value lost if confidential information is disclosed?
- What is the cost of recovering from this threat?
- What is the value lost if critical devices were to fail?
- What is the single loss expectancy (SLE) for each asset, and each threat?

Step 3: Perform a Threat Analysis- Take the following steps to perform a threat analysis

- Gather information about the likelihood of each threat taking place from people in each department, past records, and official security resources that provide this type of data.
- Calculate the annualized rate of occurrence (ARO), which is how many times the threat can take place in a 12-month period.

Step 4: Derive the Overall Loss Potential per Threat-To derive the overall loss potential per threat, do the following:

- Combine potential loss and probability.
- Calculate the annualized loss expectancy (ALE) per threat by using the information calculated in the first three steps.
- Choose remedial measures to counteract each threat.
- Carry out cost/benefit analysis on the identified countermeasures.

Step 5: Reduce, Transfer, or Accept the Risk- For each risk, you can choose whether to reduce, transfer, or accept the risk:

Risk reduction methods

- Install security controls and components.
- Improve procedures.
- Alter environment.
- Provide early detection methods to catch the threat as it's happening and reduce the possible damage it can cause.

  - Produce a contingency plan of how business can continue if a specific threat takes place, reducing further damages of the threat.
  - Erect barriers to the threat.
  - Carry out security-awareness training.

Risk transfer- Buy insurance to transfer some of the risk, for example.

Risk acceptance- Live with the risks and spend no more money toward protection.

Quantitative Risk Analysis Metrics

- Single loss expectancy (SLE) - The amount of loss due to a single occurrence of a threat.
- Annualized loss expectancy (ALE) - The estimated loss per annum.
- Exposure factor (EF) - Represents the percentage of loss a realized threat could have on a certain asset.
- Annualized rate of occurrence (ARO) – It is the value that represents the estimated frequency of a specific threat taking place within a one-year timeframe. It can range from 0.0 to 1.0.

Results of a Quantitative Risk Analysis

The following is a short list of what generally is expected from the results of a risk analysis

- Monetary values assigned to assets
- Comprehensive list of all possible and significant threats
- Probability of the occurrence rate of each threat
- Loss potential the company can endure per threat in a 12-month time span
- Recommended safeguards, countermeasures, and actions analysis.

A Qualitative Approach to Risk Analysis

- In Qualitative approach, we walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures.
- The Qualitative analysis techniques include judgment, best practices, intuition, and experience.
- Qualitative Risk Analysis Techniques
- Delphi -A group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result to a particular threat will be. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

The risk analysis team will determine the best technique for the threats that need to be assessed and the culture of the company and individuals involved with the analysis.

Chapter three

INFORMATION SYSTEM SECURITY CONTROLS

Computer systems play such a critical role in business, government, and daily life that firms need to make security and control a top priority.

Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

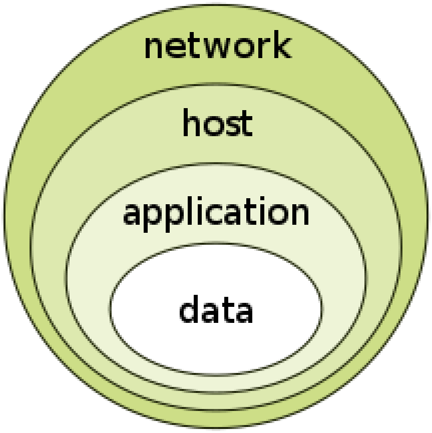
Controls consist of all the **methods, policies, and organizational procedures** that ensure the safety of the organization's assets, the accuracy and reliability of its accounting records, and operational adherence to management standards.

Information security is often used synonymously with IT security, but strictly speaking it goes beyond that. Information security encompasses everything that protects a company's information assets against threats (e.g., cyberattacks, sabotage, espionage, and natural disasters) and the resulting harm to its business or reputation.

It is a process of securing your personal data from unauthorized access, usage, revelation, interruption, modification, or deletion of data.

Information security must protect information throughout its lifespan, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest.

To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms.



The building up, layering on, and overlapping of security measures is called "defense in depth. In contrast to a metal chain, which is famously only as strong as its weakest link, the defense in depth strategy aims at a structure where, should one defensive measure fail, other measures will continue to provide protection

A very important component of information security is Cyber security.

Cyber security is how you protect against computer program, network and system attacks. Cyber security is not a one-and-done solution; it's a framework that evolves and adapts to a situation and includes oversight, prevention, and maintenance. Effective cyber security reduces the risk of a cyber-attack through the deliberate exploitation of systems, networks and technologies.

Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers. while you need to make sure that your data can't be accessed by unauthorized users, you also need to ensure that it *can* be accessed by those who have the proper permissions.

Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to, and getting to the data should not take an inordinate amount of time.

If, for example, there is a power outage and there is no disaster recovery system in place to help users regain access to critical systems, availability will be compromised. Also, a natural disaster like a flood or even a severe snowstorm may prevent users from getting to the office, which can interrupt the availability of their workstations and other devices that provide business-critical information or applications. Availability can also be compromised through deliberate acts of sabotage, such as the use of denial-of-service (DoS) attacks or ransomware.

To ensure availability, organizations can use redundant networks, servers, and applications. These can be programmed to become available when the primary system has been disrupted or broken. You can also enhance availability by staying on top of upgrades to software packages and security systems. In this way, you make it less likely for an application to malfunction or for a relatively new threat to infiltrate your system. Backups and full disaster recovery plans also help a company regain availability soon after a negative event.

Integrity

Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.

For example, if your company provides information about senior managers on your website, this information needs to have integrity. If it is inaccurate, those visiting the website for information may feel your organization is not trustworthy. Someone with a vested interest in damaging the reputation of your organization may try to hack your website and alter the descriptions, photographs, or titles of the executives to hurt their reputation or that of the company as a whole.

Compromising integrity is often done intentionally. An attacker may bypass an intrusion detection system (IDS), change file configurations to allow unauthorized access, or alter the logs kept by the system to hide the attack. Integrity may also be violated by accident. Someone may accidentally enter the wrong code or make another kind of careless mistake. Also, if the company's security policies, protections, and procedures are inadequate, integrity can be violated without any one person in the organization accountable for the blame.

To protect the integrity of your data, you can use hashing, encryption, digital certificates, or digital signatures. For websites, you can employ trustworthy certificate authorities (CAs) that verify the authenticity of your website so visitors know they are getting the site they intended to visit.

A method for verifying integrity is non-repudiation, which refers to when something cannot be repudiated or denied. For example, if employees in your company use digital signatures when sending emails, the fact that the email came from them cannot be denied. Also, the recipient cannot deny that they received the email from the sender.

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.
Maintaining data in its correct state and preventing it from being improperly modified, either by accident or maliciously.

Confidentiality
Data is confidential when only those people who are authorized to access it can do so; to ensure confidentiality, you need to be able to identify who is trying to access data and block attempts by those without authorization.

Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data—whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

For example, those who work with an organization’s finances should be able to access the spreadsheets, bank accounts, and other information related to the flow of money. However, the vast majority of other employees—and perhaps even certain executives—may not be granted access. To ensure these policies are followed, stringent restrictions have to be in place to limit who can see what.

There are several ways confidentiality can be compromised. This may involve direct attacks aimed at gaining access to systems the attacker does not have the rights to see. It can also involve an attacker making a direct attempt to infiltrate an application or database so they can take data or alter it.

These direct attacks may use techniques such as man-in-the-middle (MITM) attacks, where an attacker positions themselves in the stream of information to intercept data and then either steal or alter it. Some attackers engage in other types of network spying to gain access to credentials. In some cases, the attacker will try to gain more system privileges to obtain the next level of clearance.

However, not all violations of confidentiality are intentional. Human error or insufficient security controls may be to blame as well. For example, someone may fail to protect their password—either to a workstation or to log in to a restricted area. Users may share their credentials with someone else, or they may allow someone to see their login while they enter it. In other situations, a user may not properly encrypt a communication, allowing an attacker to intercept their information. Also, a thief may steal hardware, whether an entire computer or a device used in the login process and use it to access confidential information.

To fight against confidentiality breaches, you can classify and label restricted data, enable access control policies, encrypt data, and use multi-factor authentication (MFA) systems. It is also advisable to ensure that all in the organization have the training and knowledge they need to recognize the dangers and avoid them.

Ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of confidentiality should prevail while data resides on systems and devices within the network, as it is transmitted and once it reaches its destination.

CONTROLS

Controlling who has access to a system and the breadth of access a user has is vital to ensure the **security of systems** and **data** on the systems

Data is the **new oil** for any company. It is the most valuable asset in the digital world. Most digital giants like Amazon, Google, and Facebook etc. that monopolize on data are perhaps the most powerful companies in the world, prompting ongoing conversations about Data Protection regulations and digital privacy.
Kenya in this case has digital giants like Safaricom, Metropol Credit Reference Bureau among other companies who are processing huge amounts of data county-wide.

Data security is one of the most daunting tasks for IT and information security professionals. Each year, companies of all sizes spend a sizable portion of their IT security budgets protecting their organizations from hacker's intent on gaining access to data through brute force, exploiting vulnerabilities or social engineering.

Example 1: Report of the Kenyan Banking Sector Innovation Survey 2021,

- From the financial institutions that responded to the survey, 8 percent indicated that they had spent more than Ksh.**200 million in 2021**, on secure software development and database related activities, this is an increase from 4 percent in 2020.
- Cyber-risk (data privacy and data security risk) turned out to be the key risk for institutions in their innovation endeavors.

Example 2: How Often the Banks Updates/Patches their Software an extract from report on Challenges of cyber threats in Kenyan banking sector, J. Nyawanga (2015)
The results in showed that 70.7% or the respondents expressed that they update/patch their software between 0-6 months, 24.4% or the respondents expressed that they update/patch their software between 12-24 months and 4.9% of the respondents expressed that they update/patch their software within a period of more than 24 months.

Data

Data can be created, stored, destroyed, processed, transmitted, used, corrupted, lost, stolen etc. Whichever form the information takes it should be always appropriately protected.

- Data Classification

After identifying the information to be protected, it is necessary to classify the data and organize it according to its sensitivity to loss, disclosure or unavailability.

The primary purpose of data classification is to indicate the protection level of confidentiality, Integrity and Availability required for each type of dataset.

Data classification helps to ensure that the data is protected in the most cost-effective manner.

Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.

- Data Classification Procedures

The following outlines the necessary steps for a proper classification program:

- ✓ Define classification levels.
- ✓ Specify the criteria that will determine how data is classified.
- ✓ Have the data owner indicate the classification of the data she is responsible for.
- ✓ Identify the data custodian who will be responsible for maintaining data and its security level.
- ✓ Indicate the security controls, or protection mechanisms, that are required for each classification level.
- ✓ Document any exceptions to the previous classification issues.
- ✓ Indicate the methods that can be used to transfer custody of the information to a different data owner.
- ✓ Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
- ✓ Indicate termination procedures for declassifying the data.
- ✓ Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels.

- Classification Controls

The type of control implemented per classification depends upon the level of protection that management and the security team have determined is needed. Some of the controls are:

- ✓ Strict and granular access control for all levels of sensitive data and programs
- ✓ Encryption of data while stored and while in transmission
- ✓ Auditing and monitoring (determine what level of auditing is required and how long logs are to be retained)
- ✓ Separation of duties (determine whether two or more people need to be involved in accessing sensitive information to protect against fraudulent activities; if so, define and document procedures)
- ✓ Periodic reviews (review classification levels, and the data and programs that adhere to them, to ensure that they are still in alignment with business needs; data or applications may also need to be reclassified or declassified, depending upon the situation)

- ✓ Backup and recovery procedures (define and document)
- ✓ Change control procedures (define and document)
- ✓ File and file system access permissions (define and document)

Information system security controls

Information system security is the protection of information systems against unauthorized access to modify 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.

Information system security controls are measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems.

It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information.

These security controls are intended to help protect the **availability, confidentiality, and integrity** of data and networks, and are typically implemented after an information security risk assessment.

Information system Security Controls can be classified into three categories:

- Administrative Controls
- Technical control
- Physical controls

Administrative Controls

Administrative controls define the human factors of security. It involves all levels of personnel within an organization and determines which users have access to what resources and information.

Examples of Administrative Controls

- Security policy
- Monitoring and supervising
- Separation of duties
- Job rotation
- Information classification
- Personnel procedures
- Investigations
- Testing
- Security-awareness and training

Policy and Procedures

- A security policy is a high-level plan that states management’s intent pertaining to how security should be practiced within an organization, what actions are acceptable, and what level of risk the company is willing to accept. This policy is derived from the laws, regulations, and business objectives that shape and restrict the company.

- The security policy provides direction for each employee and department regarding how security should be implemented and followed, and the repercussions for noncompliance. Procedures, guidelines, and standards provide the details that support and enforce the company's security policy.

Personnel Controls

- Personnel controls indicate how employees are expected to interact with security mechanisms, and address noncompliance issues pertaining to these expectations.
- Change of Status: These controls indicate what security actions should be taken when an employee is hired, terminated, suspended, moved into another department, or promoted.
- Separation of duties: The separation of duties should be enforced so that no one individual can carry out a critical task alone that could prove to be detrimental to the company.

  Example: A bank teller who has to get supervisory approval to cash checks over $2000 is an example of separation of duties. For a security breach to occur, it would require collusion, which means that more than one person would need to commit fraud, and their efforts would need to be concerted. The use of separation of duties drastically reduces the probability of security breaches and fraud.
- Rotation of duties means that people rotate jobs so that they know how to fulfill the obligations of more than one position. Another benefit of rotation of duties is that if an individual attempts to commit fraud within his position, detection is more likely to happen if there is another employee who knows what tasks should be performed in that position and how they should be performed.

Supervisory Structure

Management must construct a supervisory structure which enforces management members to be responsible for employees and take a vested interest in their activities. If an employee is caught hacking into a server that holds customer credit card information, that employee and her supervisor will face the consequences?

Job Rotation

Job Rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give him or her a breath of exposure to the entire operation.

Job rotation is also practiced to allow qualified employees to gain more insights into the processes of a company and to increase job satisfaction through job variation.
Separation of Duties

Separation of duties (SoD)

Is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers.

SoD in basic terms that is no single individuals should have controls over two or more phases of a transaction or operation, so that a deliberate fraud is more difficult to occur because it requires collusion of two or more individuals or parties.

With the concept of SoD, business critical duties can be categorized into four types of functions, authorization, custody, record keeping and reconciliation. In a perfect system, no one person should handle more than one type of function.

Least Privilege

The principle of least privilege, also known as the principle of minimal privilege or just least privilege, requires that in a particular abstraction layer of a computing environment every module (such as a process, a user or a program on the basis of the layer we are considering) must be able to access only such information and resources that are necessary to its legitimate purpose.

Testing

- This control states that all security controls, mechanisms, and procedures are tested on a periodic basis to ensure that they properly support the security policy, goals, and objectives set for them.
- The testing can be a drill to test reactions to a physical attack or disruption of the network, a penetration test of the firewalls and perimeter network to uncover vulnerabilities, a query to employees to gauge their knowledge, or a review of the procedures and standards to make sure they still align with business or technology changes that have been implemented.

Security-Awareness Training

- This control helps users/employees understand hot to properly access resources, why access controls are in place and the ramification for not using the access controls properly.

Policies, procedures, practices and organizational structures put in place to reduce risks are referred to as internal controls.

TECHNICAL CONTROLS

Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network.

Implementing and maintaining access control mechanisms

Access controls are security features that control how users and systems communicate and interact with other systems and resources.

Access is the flow of information between a subject and an object.

A *subject* is an active entity that requests access to an object or the data within an object. E.g.: user, program, process etc.

An *object* is a passive entity that contains the information. E.g.: Computer, Database, File, Program etc.

Access Control Challenges

- Various types of users need different levels of access - Internal users, contractors, outsiders, partners, etc.
- Resources have different classification levels- Confidential, internal use only, private, public, etc.
- Diverse identity data must be kept on different types of users - Credentials, personal data, contact information, work-related data, digital certificates, cognitive passwords, etc.
- The corporate environment is continually changing- Business environment needs, resource access needs, employee roles, actual employees, etc.

Access Control Principles

- Principle of Least Privilege: States that if nothing has been specifically configured for an individual or the groups, he/she belongs to, the user should not be able to access that resource i.e. default no access
- Separation of Duties
- Need to know : It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties

Identification, Authentication and Authorization

Identification describes a method of ensuring that a subject is the entity it claims to be. E.g.: A user name or an account no.
Authentication is the method of proving the subjects identity. E.g.: Password, Passphrase, PIN
Authorization is the method of controlling the access of objects by the subject. E.g.: A user cannot delete a particular file after logging into the system

Identification

When issuing identification values to users or subjects, ensure that

- Each value should be unique, for user accountability
- A standard naming scheme should be followed
- The values should be non-descriptive of the users position or task
- The values should not be shared between the users.

Authentication Methods

Biometrics

- Verifies an individual’s identity by analyzing a unique personal attribute or behavior
- It is the most effective and accurate method for verifying identification.
- It is the most expensive authentication mechanism
- Types of Biometric Systems
  - *Finger Print*- are based on the ridge endings, bifurcation exhibited by the friction edges and some minutiae of the finger
  - *Palm Scan*- are based on the creases, ridges, and grooves that are unique in each individuals palm
  - Hand Geometry- are based on the shape (length, width) of a persons hand and fingers
  - *Retina Scan*- is based on the blood vessel pattern of the retina on the backside of the eyeball.
  - *Iris Scan*- is based on the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas and furrows.
  - *Signature Dynamics*- is based on electrical signals generated due to physical motion of the hand during signing a document
  - *Keyboard Dynamics*- is based on electrical signals generated while the user types in the keys (passphrase) on the keyboard.
  - *Voice Print*- based on human voice
  - *Facial Scan*- based on the different bone structures, nose ridges, eye widths, forehead sizes and chin shapes of the face.

Passwords

- It is the most form of system identification and authentication mechanism
- A password is a protected string of characters that is used to authenticate an individual
- Password Management
    - Password should be properly guaranteed, updated, and kept secret to provide and effective security
    - Passwords generators can be used to generate passwords that are uncomplicated, pronounceable, non-dictionary words.
    - If the user chooses his passwords, the system should enforce certain password requirement like insisting to use special char, no of char, case sensitivity etc.)

Access Control Technologies

Single Sign-On

- SSO is a technology that allows a user to enter credentials one time and be able to access all resources in primary and secondary network domains

Kerberos

- Kerberos is an authentication protocol that works in a C/S model and is based on symmetric key cryptography
- It is widely used in UNIX systems and also the default authentication method for windows 2k and 2k3 and is the de-facto standard for heterogeneous networks.

Kerberos Components

- Key Distribution Center (KDC)
- Secret Keys are the keys shared between principle and KDC generally using symmetric key cryptography algorithm that are used to authenticate the principles and communicate securely
- Principles are users, applications or any network services
- A ticket is a token generated by KDC and given to a principle when one principle need to authenticate another principle
- Realm is a set of principles. A KDC can be responsible for one or more realms. Realms allow an administrator to logically group resources and users.
- Session Keys are the keys shared between the principles that will enable them communicate security

SESAME

- SESAME (Secure European Systems for Applications in a Multi-vendor Environment) is a SSO technology that was developed to extend Kerberos functionality and improve upon its weakness.
- SESAME uses a symmetric and asymmetric cryptographic technique to protect exchanges of data and to authenticate subjects to network resources.
- SESAME uses digitally signed privileged Attribute Certificates (PAC) to authenticate subjects to objects. PAC contains the subject’s identity, access capabilities for the object, access time period, and life time of the PAC

Security Domain

- A domain is a set of resources that are available to a subject.

- A security domain refers to the set the resources working under the same security policy and managed by the same group.
- Domains can be architected in a hierarchical manner that dictates the relationship between the different domains and the ways in which subjects within the different domains can communicate.
- Subjects can access resources in domains of equal or lower trust levels.

Thin Clients

- Thin clients are diskless computers that are sometimes called as dumb terminals.
- It is based on C/S technology where a user is supposed to logon to a remote server to use the computing and network resources.
- When the user starts the client, it runs a short list of instructions and then points itself to a server that will actually download the operating system, or interactive operating software, to the terminal. This enforces a strict type of access control, because the computer cannot do anything on its own until it authenticates to a centralized server, and then the server gives the computer its operating system, profile, and functionality.
- Thin-client technology provides another type of SSO access for users, because users authenticate only to the central server or mainframe, which then provides them access to all authorized and necessary resources.

Access Control Models

- An access control model is a framework that dictates how subjects access objects.
- It uses access control technologies and security mechanisms to enforce the rules and objectives of the model.
- There are three main types of access control models:
    - Discretionary,
    - Mandatory, and
    - Nondiscretionary (also called role-based).

Discretionary Access Control

- The control of access is based on the discretion (wish) of the owner
- A system that uses DAC enables the owner of the resource to specify which subjects can access specific resources
- The most common implementation of DAC is through ACL's which are dictated and set by the owners and enforced by the OS.
- Examples: Unix, Linux, Windows access control is based on DAC
- DAC systems grant or deny access based on the identity of the subject. The identity can be user identity or a group identity (Identity based access control)

Mandatory Access Control

- This model is very structured and strict and is based on a security label (also known as sensitivity label) attached to all objects
- The subjects are given security clearance by classifying the subjects as secret, top secret, confidential etc.) and the objects are also classified similarly
- The clearance and the classification data is stored in the security labels, which are bound to the specific subject and object.

- This model is used and is suitable for military systems where classifications and confidentiality is of at most important

Non-Discretionary or Role Based Access Control

- A RBAC is based on user roles and uses a centrally administered set of controls to determine how subjects and objects interact.
- The RBAC approach simplifies the access control administration
- It is a best system for a company that has high employee turnover.

Access Control Administration

Access control administration can be done in two ways.

- Centralized
- Decentralized

Centralized Access Control

- Here one entity (dept or an individual) is responsible for overseeing access to all corporate resources.
- This type of administration provides a consistent and uniform method of controlling users access rights.

Decentralized Access Control

- A decentralized access control administration method gives control of access to the people closer to the resources
- In this approach, it is often the functional manager who assigns access control rights to employees.
- Changes can happen faster through this type of administration because not just one entity is making changes for the whole organization.
- There is a possibility for conflicts to arise that may not benefit the organization as because different managers and departments can practice security and access control in different ways.

Access Control Monitoring

Access Control Monitoring is a method of keeping track of who attempts to access specific network resources

The ACM system can fall into two categories: Intrusion Prevention System (IPS) and Intrusion Detection System (IDS)

Intrusion Detection Systems

Basic Concepts

Intrusion detection is the process of detecting an unauthorized use of, or attack upon, a computer, network, or a telecommunication infrastructure.

IDS are designed to aid in mitigating the damage that can be caused by hacking, or breaking into sensitive computer and network systems.

Common Functions of an IDS

- Watch for attacks
- Parse audit logs

- Protect system files
- Alert administrators during attacks
- Expose a hackers technique
- Illustrate which vulnerabilities need to be addressed
- Help track down individual hackers

IDS Types

- Network-Based IDS: A network-based IDS (NIDS) uses sensors, which are either host computers with the necessary software installed or dedicated appliances—each with its network interface card (NIC) in promiscuous mode. The NIC driver captures all traffic and passes it to an analyzer to look for specific types of patterns.
- Host-Based IDS: A host-based IDS (HIDS) can be installed on individual workstations and/or servers and watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.

Intrusion Prevention System

The traditional IDS only detects that something bad may be taking place and sends an alert. The goal of an IPS is to detect this activity and not allow the traffic to gain access to the target in the first place. An IPS is a preventative and proactive technology, whereas an IDS is a detective and after-the-fact technology.

PHYSICAL CONTROL

Is the protection of personnel, data, hardware, etc., from physical threats that could harm, damage, or disrupt business operations or impact the confidentiality, integrity, or availability of systems and/or data.

Physical Control Components

Network Segregation

- Network segregation can be carried out through physical and logical means. A section of the network may contain web servers, routers, and switches, and yet another network portion may have employee workstations.
- Each area would have the necessary physical controls to ensure that only the permitted individuals have access into and out of those sections.

Perimeter Security

- Perimeter security can also encompass closed-circuit TVs that scan the parking lots and waiting areas, fences surrounding a building, lighting of walkways and parking areas, motion detectors, sensors, alarms, and the location and visual appearance of a building. These are examples of perimeter security mechanisms that provide physical access control by providing protection for individuals, facilities, and the components within facilities.

Computer Controls

- Each computer can have physical controls installed and configured, such as locks on the cover so that the internal parts cannot be stolen, the removal of the floppy and CD-ROM drives to prevent copying of confidential information, or implementation of a protection device that reduces the electrical emissions to thwart attempts to gather information through airwaves.

Work Area Separation

- Some environments might dictate that only particular individuals can access certain areas of the facility.

Data Backups

Another essential tool for information security is a comprehensive backup plan for the entire organization. Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up.

Cabling

- There are different types of cabling that can be used to carry information throughout a network.
- Some cable types have sheaths that protect the data from being affected by the electrical interference of other devices that emit electrical signals.
- Some types of cable have protection material around each individual wire to ensure that there is no crosstalk between the different wires.
- All cables need to be routed throughout the facility in a manner that is not in people's way or that could be exposed to any danger of being cut, burnt, crimped, or eavesdropped upon.

Control Zone

- It is a specific area that surrounds and protects network devices that emit electrical signals. These electrical signals can travel a certain distance and can be contained by a specially made material, which is used to construct the control zone.
- The control zone is used to resist penetration attempts and disallow sensitive information to "escape" through the airwaves.
- A control zone is used to ensure that confidential information is contained and to hinder intruders from accessing information through the airwaves.
- Companies that have very sensitive information would likely protect that information by creating control zones around the systems that are processing that information

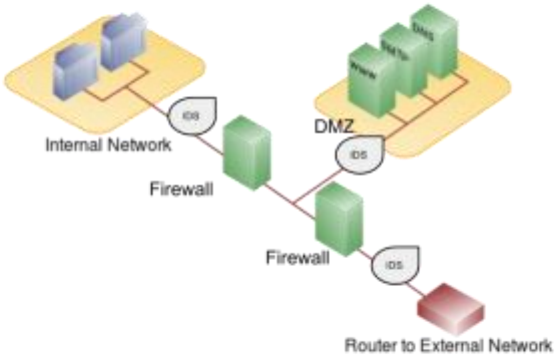
Locked doors

It may seem obvious, but all the security in the world is useless if an intruder can simply walk in and physically remove a computing device. High-value information assets should be secured in a location with limited access.

Firewalls

A firewall is use to increase security on its network is a firewall and can exist as hardware or software (or both). A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive to a computer.

A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization. This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer.



Examples of Physical Control

- Fences, Locks, Badge system, Security guard, Biometric system, Mantrap doors, Lighting, Motion detectors, Closed-circuit TVs, Alarms and Backups

Evolution of information from office to a battle field

As government and civilian organizations continue to increase their dependency on networked computers that control communications, infrastructures, and weapons systems, the vulnerabilities of exploitation, manipulation, and corruption likewise increase.

The debate surrounding the changing nature of conflict in the modern era continues with the introduction of a new element, the cyber dimension. Cyber warfare represents a fundamental transformation in the very nature of the concept of conflict itself, not only changing the weapons of modern conflict, but radically shifting the nature of the wartime battlefield.

Over the past decade, the entire global cyber space has turned into a battlefield. The raging war — with no end in sight — is affecting everyone using internet-based services and technologies. Operators of critical infrastructure from energy companies, to banks, and to telecommunications providers are under an unrelenting onslaught

Cyber Warfare

Cyber warfare is usually defined as a cyber-attack or series of attacks that target a country. It has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.Cyber warfare typically involves a nation-state perpetrating cyber-attacks on another, but in some cases, the attacks are carried out by terrorist organizations or non-state actors seeking to further the goal of a hostile nation.

Cyber warfare is one of the newest elements in contemporary warfare, however, this new advancement is continuously evolving and it can be challenging, at times, to stay abreast of all the new developments. In an age when individuals voluntarily transmit and receive copious amounts of personal data, exploiting electronic devices to alter or obtain information has become a crucial new tactic of conflict known as the 'fifth dimension battlefield, after air, sea, land and outer space' and has, arguably, become vital in achieving states' success today.

There is no clear set date of when cyber warfare began but a key milestone was in Kosovo in 1999. Whilst Vietnam was the world's first TV war, Kosovo became its first cyber war (Geers, 2008). NATO Kosovo operation was a major challenge in the history of the Atlantic alliance. For the first time, a defensive alliance launched a military campaign to avoid a humanitarian tragedy outside its own borders

And despite many challenges, including the use of cyber warfare, NATO prevailed. Numerous pro-Serbian hackers attacked NATO's internet infrastructure with the goal to disrupt military operations Whilst some states declared the cyber-attacks had no impact on their overall war effort, the U.K. admitted to having lost at least some database information, these attacks where the first sign of things to come and the potential power cyberware would have.

The cyber domain is unique in that it is all new, manmade and subject to even more rapid technological evolution than other domains. More importantly, the non-existent boundaries in cyberspace create an environment where states can simultaneously be allies and adversaries.

As such,cyberspace has become gradually well-defined in a military context by a variety of state governments. However, cyber-attacks are not just restricted to local governments but can also rapidly spread worldwide without the need of human capital, as "cyber warfare has no borders and is able to attack multiple destinations simultaneously" .The U.S. Department of Defence termed cyberspace a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers".

7 Types of Cyber Warfare Attacks

Here are some of the main types of cyber warfare attacks.

- Espionage

Refers to monitoring other countries to steal secrets.

- Sabotage

Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

- Denial-of-service (DoS) Attacks

DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests.

- Electrical Power Grid

Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm

- Propaganda Attacks

Attempts to control the minds and thoughts of people living in or fighting for a target country.

- Economic Disruption

Attackers can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

- Surprise Attacks

The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses. This can be done to prepare the ground for a physical attack in the context of hybrid warfare.

Chapter four
INFORMATION SYSTEM SECURITY MANAGEMENT SYSTEM

An information security management system defines policies, methods, processes, and tools to ensure sustainable information security in companies and government agencies. This includes the introduction of specific procedures and the implementation of organizational and technical measures that must be continuously controlled, monitored, and improved.

The goal is to ensure, beyond the IT department, an appropriate level of protection for the confidentiality, availability, and integrity of information within the entire organization or the defined scope. Thus, the ISMS provides the basis for systematic implementation of information security within a company and for compliance with security standards. Potential threats relating to information security are identified, analyzed, and mitigated, making them controllable.

The goal of an ISMS is to **minimize risk and ensure business continuity** by proactively limiting the impact of a security breach.

The Difference between Information Security and IT Security?

Unlike IT security, information security refers not only to the security of the technology used, but also to organizational issues such as access authorizations and responsibilities. Accordingly, information security is not the sole responsibility of the IT department, but must be implemented in all areas of the company, starting with management.

The Protection Goals of Information Security?

According to the international ISO 27000 family of standards, the protection goals of information security comprise three main aspects:

- Confidentiality: Confidential information may only be viewed and disclosed by authorized persons. Access to this information must therefore be appropriately secured. Confidentiality is violated if an attacker is able to eavesdrop on communications, for example.
- Integrity: Information must be protected from undetected manipulation in order to preserve its accuracy and completeness. Integrity is violated if, for example, an attacker is able to modify research data without detection.
- Availability: Information, services, or resources must be available and usable for legitimate users at all times. Availability can be disrupted, for example, by a DDoS attack that deliberately overloads systems.

An information security officer appointed by top management acts as the point of contact for all information security issues. He/she must be integrated into the ISMS process and work closely with IT managers, for example, when selecting new IT components or applications.

Security frameworks and standards

A security framework is a compilation of state-mandated and international cyber security policies and processes to protect critical infrastructure. It includes precise instructions for companies to handle the personal information stored in systems to ensure their decreased vulnerability to security-related risks.

Compliance and regulatory frameworks are sets of guidelines and best practices. Organizations follow these guidelines to meet regulatory requirements, improve processes, strengthen security, and achieve other business objectives.

While security standards offer insight into recommended controls and guidelines go over the security measures that are ideally put in place on a network and are mandatory for compliance in some cases, a framework has security best practices that companies should follow to get the best results for implementing

Information security compliance standards

Cyber security compliance is the organizational risk management method aligned with pre-defined security measures & controls on how data confidentiality is ensured by its administrational procedures.

Companies are encouraged to implement a systematic risk governance approach that adheres to regulatory authorities, laws, and industry-relevant units established controls to meet data management and protection requirements.

Significance of cyber security compliance

It’s important to acknowledge cybersecurity compliance isn’t solely a collection of strict and mandatory requirements coming from regulatory bodies — it’s consequential to overall business success.

Any company is at risk of becoming a victim of a cyber attack. Especially, small enterprises tend to make themselves a low-hanging fruit for criminals as it’s popular to assume that if you are insignificant in size, potential threats will pass by. However, hesitation to invest in a strong cyber security posture exposes vulnerabilities that interest hostile actors.

CYBER SECURITY FRAMEWORK

Cyber security frameworks are sets of documents describing guidelines, standards, and best practices designed for cyber security risk management. The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit.

But much like a framework in the “real world” consists of a structure that supports a building or other large object, the cyber security framework provides foundation, structure, and support to an organization’s security methodologies and efforts.

Why Do We Need Cyber Security Frameworks?

Cyber security frameworks help teams address cyber security challenges, providing a strategic, well-thought plan to protect its data, infrastructure, and information systems. The frameworks offer guidance, helping IT security leaders manage their organization’s cyber risks more intelligently.

Companies can adapt and adjust an existing framework to meet their own needs or create one internally.

Bottom line, businesses are increasingly expected to abide by standard cyber security practices, and using these frameworks makes compliance easier and smarter. The proper framework will suit the needs of many different-sized businesses regardless of which of the countless industries they are part of.

Frameworks help companies follow the correct security procedures, which not only keeps the organization safe but fosters consumer trust.

Cyber Security Frameworks

When it comes to picking a cyber-security framework, you have an ample selection to choose from. Here are the frameworks recognized today as some of the better ones in the industry. Naturally, your choice depends on your organization’s security needs.
Companies turn to cyber security frameworks for guidance. The right framework, instituted correctly, lets IT security teams intelligently manage their companies’ cyber risks. Companies can either customize an existing framework or develop one in-house.

1. The NIST Cyber Security Framework.
The NIST Framework for Improving Critical Infrastructure Cybersecurity, or the “NIST cybersecurity framework” .The NIST was designed to protect America’s critical infrastructure (e.g., dams, power plants) from cyberattacks.
NIST is a set of voluntary security standards that private sector companies can use to find, identify, and respond to cyberattacks. The framework also features guidelines to help organizations prevent and recover from cyberattacks. There are five functions or best practices associated with NIST: Identify, Protect, Detect, Respond and Recover

2. The Center for Internet Security Critical Security Controls (CIS).
If you want your company to start small and gradually work its way up, you must go with CIS. This framework was developed in the late 2000s to protect companies from cyber threats. It’s made up of 20 controls regularly updated by security professionals from many fields (academia, government, industrial). The framework begins with basics, moves on to foundational, then finishes with organizational.

3. The International Standards Organization (ISO) frameworks
ISO/IEC 27001 is the international standard for information security and for creating an ISMS.
ISO/IEC 27001, the international standard for an information security management system (ISMS), is the most commonly used IT security compliance standard.
The standard also encourages a holistic approach to information security that involves many parts of the organization beyond IT, including senior management, business continuity, physical security, and human resources.
To become ISO 27001 certified, an organization requires an ISMS that identifies the organizational assets and provides the following assessment:

- the risks the information assets face;
- the steps taken to protect the information assets;
- a plan of action in case a security breach happens; and
- identification of individuals responsible for each step of the information security process.

The goal of an ISMS isn't necessarily to maximize information security, but rather to reach an organization's desired level of information security
Implementing ISMS
There are various ways to set up an ISMS. Most organizations either follow a plan-do-check-act process or study the ISO 27001 international security standard which effectively details the requirements for an ISMS.
The following steps illustrate how an ISMS should be implemented:

- Define the scope and objectives. Determine which assets need protection and the reasons behind protecting them.
- Identify assets. Identify the assets that are going to be protected. This can be achieved by creating an inventory of business-critical assets including hardware, software, services, information, databases and physical locations by using a business process map.
- Recognize the risks. Once the assets are identified, their risk factors should be analyzed and scored by assessing the legal requirements or compliance guidelines. Organizations should also weigh the effects of the identified risks. For example, they could question the amount of impact it would create if the confidentiality, availability or integrity of information assets is breached, or the probability of that breach's occurrence.
- Identify mitigation measures. An effective ISMS not only identifies risk factors but also provides satisfactory measures to effectively mitigate and combat them. An effective mitigation measure would be to set up a policy or rule that doesn't permit employees to store customer data on their laptops.
- Make improvements. All the previous measures should be monitored, audited and checked repeatedly for effectiveness. If the monitoring reveals any deficiencies or new risk management factors, then restart the ISMS process from scratch.

4.The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization, established in the United States, dedicated to providing guidance to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting.

COSO's member organizations were the American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (IMA), and the Institute of Internal Auditors (IIA).

COSO, the Committee of Sponsoring Organizations, is an advisory group that designs frameworks to help organizations with risk management issues.

COSO has established a common internal control model against which companies and organizations may assess their control systems.

The COSO framework involves several key concepts:

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is affected by people. It’s not merely policy, manuals, and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity’s management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories

Information Technology Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) is sometimes referred to as the ITIL foundation or the ITIL framework

The Information Technology Infrastructure Library (ITIL) is a set of practices. Its primary purpose is to provide a systematic approach to IT service management (ITSM).

Overview and Benefits

ITIL provides a systematic and professional approach to the management of IT service provision. Adopting its guidance offers users a huge range of benefits that include:

- ✓ reduced costs;
- ✓ improved IT services through the use of proven best practice processes;
- ✓ improved customer satisfaction through a more professional approach to service delivery;
- ✓ standards and guidance;
- ✓ improved productivity;

COBIT

COBIT stands for Control Objectives for Information and Related Technology. It is a framework created by the ISACA (Information Systems Audit and Control Association. ISACA stands for Information Systems Audit and Control Association. It develops controls and guidance for information governance, security, control, and audit professionals.

This international association focuses on IT governance, providing benchmarks and governance tools for organizations that employ information systems.

Control Objectives for Information and Related Technologies, more popularly known as COBIT, is a framework that aims to help organizations that are looking to develop, implement, monitor, and improve IT governance and information management.

The COBIT framework provides a common language for IT professionals, compliance auditors, and business executives. They can communicate with each other on the same IT goals, controls, objectives and outcomes.

The COBIT business orientation includes linking business goals with its IT infrastructure by providing various maturity models and metrics that measure the achievement while identifying associated business responsibilities of IT processes. The main focus of COBIT 4.1 was illustrated with a process-based model subdivided into four specific domains, including:

- Planning & Organization
- Delivering and Support
- Acquiring & Implementation
- Monitoring & Evaluating

Chapter Five

INFORMATION SECURITY GOVERNANCE

IS governance providing strategic direction, ensures objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security programme.

Information Security Governance

IT security governance is the system by which an organization directs and controls IT security. IT security governance should not be confused with IT security management. IT security management is concerned with making decisions to mitigate risks; governance determines who is authorized to make decisions. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Management recommends security strategies. Governance ensures that security strategies are aligned with business objectives and consistent with regulations.

Enterprise security governance results from the duty of care owed by leadership towards fiduciary requirements. This position is based on judicial rationale and reasonable standards of care .The five general governance areas are:

- Govern the operations of the organization and protect its critical assets
- Protect the organization's market share and stock price (perhaps not appropriate for education)
- Govern the conduct of employees (educational AUP and other policies that may apply to use of technology resources, data handling, etc.)
- Protect the reputation of the organization
- Ensure compliance requirements are met

"Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business."

Characteristics of effective security governance

The eleven characteristics of effective security governance are critical for an effective enterprise information security information program. They are:

- ✓ It is an institution-wide issue
- ✓ Leaders are accountable
- ✓ It is viewed as an institutional requirement (cost of doing business)
- ✓ It is risk-based
- ✓ Roles, responsibilities and segregation of duties are defined
- ✓ It is addressed and enforced in policy
- ✓ Adequate resources are committed
- ✓ Staff are aware and trained
- ✓ A development life cycle is required
- ✓ It is planned, managed, measureable and measured
- ✓ It is reviewed and audited

The following principles describe preferred behavior to guide governance decision making :

- Responsibility: Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
- Strategy: The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.
- Acquisition: IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
- Performance: IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.
- Conformance: IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
- Human Behavior: IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the 'people in the process'.

Outcomes of effective information security governance should include:

- Strategic alignment of information security with institutional objectives
- Risk management - identify, manage, and mitigate risks
- Resource management
- Performance measurement - defining, reporting, and using information security governance metrics
- Value delivery by optimizing information security investment

Defining the Information Security Program (so as to define what needs to be governed)

Activities of an information security program directly support/trace to an institutional risk management plan. In other words, the information security program is targeted to managing institutional risk. An effective information security program requires the development and maintenance of:

- A long-term information security strategy
- An overarching institutional security plan
- Security policies, procedures, and other artifacts
- The system architecture and supporting documentation

Information Security Governance Best Practices

- Information security activities should be governed based on relevant requirements, including laws, regulations, and organizational policies.
- Senior managers should be actively involved in establishing information security governance framework and the act of governing the agency's implementation of information security. Information security responsibilities must be assigned and carried out by appropriately trained individuals.
- Individuals responsible for information security within the agency should be held accountable for their actions or lack of actions.
- Information security priorities should be communicated to stakeholders of all levels within an organization to ensure a successful implementation of an information security program.

- Information security activities must be integrated into other management activities of the enterprise, including strategic planning, capital planning, and enterprise architecture.
- Information security organization structure should be appropriate for the organization it supports and should evolve with the organization, if the organization undergoes change.
- Information security managers should continuously monitor the performance of the security program/effort for which they are responsible, using available tools and information.
- Information discovered through monitoring should be used as an input into management decisions about priorities and funding allocation to effect the improvement of security posture and the overall performance of the organization.

Benefits of information security governance

- Increased predictability and reduced uncertainty of business operations
- Protection from the potential for civil and legal liability
- Structure to optimize the allocation of resources
- Assurance of security policy compliance
- Foundation for effective risk management.
- A level of assurance that critical decisions are not based on faulty information
- Accountability for safeguarding information

Security Governance

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

Security governance is a process for overseeing the cybersecurity teams who are responsible for mitigating business risks. Security governance leaders make the decisions that allow risks to be prioritized so that security efforts are focused on business priorities rather than their own

Information Security Governance or ISG, is a subset discipline of Corporate Governance focused on information Security systems and their performance and risk management. It includes: Security Policies, Procedures, Standards, Guidelines, and Baselines

- Policies

A security policy is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization.

Types of Policies

Regulatory: This type of policy ensures that the organization is following standards set by specific industry regulations. This policy type is very detailed and specific to a type of industry. This is used in financial institutions, health care facilities, public utilities, and other government-regulated industries. E.g.: TRAI.

Advisory: This type of policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical information, handle financial transactions, or process confidential information.

Informative: This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations.

Types of Security Policies

- Organizational

Management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out.

Provides scope and direction for all future security activities within the organization

This policy must address relative laws, regulations, and liability issues and how they are to be satisfied. It also describes the amount of risk senior management is willing to accept.

Characteristics

- Business objectives should drive the policy's creation, implementation, and enforcement. The policy should not dictate business objectives.
- It should be an easily understood document that is used as a reference point for all employees and management.
- It should be developed and used to integrate security into all business functions and processes.
- It should be derived from and support all legislation and regulation applicable to the company.
- It should be reviewed and modified as a company changes, such as through adoption of a new business model, merger with another company, or change of ownership.
- Each iteration of the policy should be dated and under version control.
- The units and individuals who are governed by the policy must have access to the applicable portions and not be expected to have to read all policy material to find direction and answers

- Issue-specific

Addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues

E.g.: An e-mail policy might state that management can read any employee's e-mail messages that reside on the mail server, but not when they reside on the user's workstation

- System-specific

System-specific presents the management's decisions that are specific to the actual computers, networks, applications and data.

This type of policy may provide an approved software list, which contains a list of applications that may be installed on individual workstations.

E.g.: This policy may describe how databases are to be used and protected, how computers are to be locked down, and how firewalls, IDSs, and scanners are to be employed.

- Standards

Standards refer to mandatory activities, actions, rules, or regulations.

Standards can give a policy its support and reinforcement in direction.

Standards could be internal, or externally mandated (government laws and regulations).

- Procedures

Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal.

E.g.: we can write procedures on how to install operating systems, configure security mechanisms, implement access control lists, set up new user accounts, assign computer privileges, audit activities, destroy material, report incidents, and much more.

Procedures are considered the lowest level in the policy chain because they are closest to the computers and users (compared to policies) and provide detailed steps for configuration and installation issues.

Procedures spell out how the policy, standards, and guidelines will actually be implemented in an operating environment.

If a policy states that all individuals who access confidential information must be properly authenticated, the supporting procedures will explain the steps for this to happen by defining the access criteria for authorization, how access control mechanisms are implemented and configured, and how access activities are audited

- Baselines

A baseline can refer to a point in time that is used as a comparison for future changes. Once risks have been mitigated, and security put in place, a baseline is formally reviewed and agreed upon, after which all further comparisons and development are measured against it.

A baseline results in a consistent reference point.

Baselines are also used to define the minimum level of protection that is required.

In security, specific baselines can be defined per system type, which indicates the necessary settings and the level of protection that is being provided. For example, a company may stipulate that all accounting systems must meet an Evaluation Assurance Level (EAL) 4 baseline.

- Guidelines

Guidelines are recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply.

Guidelines can deal with the methodologies of technology, personnel, or physical security.

Putting It All Together

A policy might state that access to confidential data must be audited. A supporting guideline could further explain that audits should contain sufficient information to allow for reconciliation with prior reviews. Supporting procedures would outline the necessary steps to configure, implement, and maintain this type of auditing.

policies are strategical(long term) while standards, guidelines and procedures are tactical(medium term).

Chapter Six
SECURITY AWARENESS, TRAINING, AND EDUCATION

Security awareness training is a formal process for educating employees and third-party stakeholders, like contractors and business partners, with the information they need to protect themselves and their organization's assets from loss or harm.
The primary and foremost objective of any awareness program is to educate users on their responsibility to protect the confidentiality, availability and integrity of their organization's information.

What are the four elements of security education?
An effective security system comprises of four elements: Protection, Detection, Verification & Reaction. These are the essential principles for effective security on any site, whether it's a small independent business with a single site, or a large multinational

Benefits of security training:

- ✓ Training for Avoiding Blunders. ...
- ✓ Training Increases Security Measures. ...
- ✓ Training Assures Educated Staff to Start Defiance. ...
- ✓ Training Saves Organizational Reputation. ...
- ✓ Training & Knowledge Boosts Morale. ...
- ✓ Training Saves Precious Time & Money. ...
- ✓ Training Gives You Peace of Mind.

What are the 3 main steps to implementing security awareness?
We've put together a list of three steps to implement robust cyber security awareness in your business to ensure you're on the right path.
Step 1: Assess current levels of cyber awareness. ...
Step 2: Implement cyber security policies. ...
Step 3: Ensure staff are trained in security awareness best practices.
There are four primary types of security training: basic security awareness training, technical security training, security management training, and compliance training.

Security Awareness

Awareness refers to having knowledge of a situation or fact. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.” Examples of awareness activities include anti-phishing posters placed in common areas; discussions of stronger passwords at staff meetings; or informational videos distributed via email.

Awareness is a basic necessity, but training is the difference maker when it comes to truly safeguarding an organization's sensitive information. And delivering information security training one time per year is simply not enough. You should plan to spread awareness and training activities across the year to provide greater persistence. Because cyber threats are constantly changing, the awareness and training program must be agile enough to provide information regarding the latest threats.

Security Education

You don't need to give everyone a formal security education to establish a successful security program. Awareness and training, however, are integral to a security-minded business culture.

For security to be successful and effective, senior management on down to the rest of the staff needs to be fully aware of the importance of enterprise and information security.

All employees should understand the underlying significance of security and the specific security related requirements expected out of them.

The controls and procedures of a security program should reflect the nature of the data being processed.

The security program should be developed in a fashion that makes sense for the different cultures and environments.

The security program should communicate the what, how, and why of security to its employees.

Security-awareness training should be comprehensive, tailored for specific groups, and organization-wide with a goal that each employee understands the importance of security to the company as a whole and to each individual.

Expected responsibilities and acceptable behaviours need to be clarified, and noncompliance repercussions, which could range from a warning to dismissal, need to be explained before being invoked.

Different Types of Security Awareness Trainings

There are usually at least three separate audiences for a security-awareness program: management, staff, and technical employees. Each type of awareness training needs to be geared toward the individual audience to ensure that each group understands its particular responsibilities, liabilities, and expectations.

- Members of management would benefit the most from a short, focused security awareness orientation that discusses corporate assets and financial gains and losses pertaining to security.
- Mid-management would benefit from a more detailed explanation of the policies, procedures, standards, and guidelines and how they map to the individual departments for which they are responsible.
- The technical departments must receive a different presentation that aligns more to their daily tasks. They should receive a more in-depth training to discuss technical configurations, incident handling, and indications of different types of security compromises so they can be properly recognized.

Employees should not try to combat an attacker or address fraudulent activities by themselves instead they should be told to report these issues to upper management, and upper management should determine how to handle the situation.

Specialized Training Programs

Different roles require different types of training (firewall administration, risk management, policy development, IDSs, and so on). A skilled staff is one of the most critical components to the security of a company, and not enough companies are spending the funds and energy necessary to give their staffs proper levels of security education.

Ethics

Ethics is the field of study concerned with questions of value, that is,judgments about what type of human behavior is "good" or "bad" in any given situation. Ethics are the standards, values, morals, principles, etc.,on which to base one's decisions or actions; often, there is no clear "right" or "wrong" answer.

A cyber-security specialist

Education

Like most other careers in cyber security, most jobs falling under the cyber security specialist category require some form of formal education. However, since cyber security specialist jobs can fall across a wide spectrum of job descriptions and responsibilities, it is possible to obtain a specialist job after completing many levels of cyber security education such as a cyber-security associate's degree, a bachelor's degree, or a master's degree.

Additionally, much of the cyber security specialist workforce found employment after completing a related degree such as computer science, engineering, or mathematics and/or by having closely-related work experience.

Industry certifications and clearances

As is the norm in many other cyber security career paths, obtaining the proper industry certifications and/or clearances is an important step in career preparation.

It makes sense to start thinking about what kinds of certifications are required by an employer, or what kinds of certifications make job applicants competitive within the field. To get an idea of some of the kinds of cyber security certifications available, here are a few examples:

- The Certified Information Systems Security Professional (CISSP) is a more advanced certification designed for cyber security professionals with at least five years of work experience. The certification covers topics such as architecture, engineering, and management.
- The Certified Ethical Hacker (CEH) certification is also considered a more advanced cert because it generally requires that applicants have multiple years of work experience. The goal of an ethical hacker certification is to be able to understand how cyber-attacks unfold in order to improve threat assessment and mitigation skills.

Information system Auditor certification

It is known as Certified Information Systems Auditor (CISA) .

CISA is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems**.**

Eligibility is established at the time of exam registration and is good for twelve (12) months (365 days).

Exam registration and payment are required before you can schedule and take an exam. You will forfeit your fees if you do not schedule and take the exam during your 12-month eligibility period.

Chapter Seven
CONTINUITY PLANNING FOR COMPUTER OPERATIONS

7.0. Emergency Preparedness Planning

In a recent survey, half the risk managers surveyed reported that their organizations had experienced natural or human disasters.Disaster can strike at any time, although most people think of disasters as naturally occurring events such as hurricanes or earthquakes, other events or conditions can have disastrous effects.
Despite the need, many risk managers fail to prepare adequately for emergencies.

- Why Plan for Emergencies

The growing dependence on technology and the increasingly complex hazards of various manufacturing operations and processes increase the frequency, immediacy, and severity of disasters—both natural and technological—and contribute to the difficulty of recovery.
In today’s business climate, it is more important than ever to have a well-considered, comprehensive Emergency Preparedness Plan in place and ready to be activated.

- Emergency Preparedness Plan

An Emergency Preparedness Plan (or EPP) is the development, documentation, testing, evaluation, and implementation of policies, procedures, organizational structure, information, and resources that an entity can use to assess potential hazards, develop and prepare an appropriate response to each hazard, and develop and prepare strategies for recovery.

While Emergency Preparedness objectives may differ from one organization to another, they are almost always directed toward protection of people, protection of property, and preparation for the organization to resume productive operations as soon as possible.
Pre-planning allows for better prevention, better response, and better recovery. Should a disaster strike, the actions taken in the first minutes and hours can make all the difference to how soon—or if—normal operations can be resumed.

Without a plan, people will spend the initial precious minutes of an emergency situation frantically trying to decide what to do, who should do it, and what to tackle first. With a comprehensive plan in place, an organized, prioritized, practiced response can begin immediately, thus mitigating damage and perhaps even preventing loss of life.
Another study showed that companies with disaster recovery plans experience an average disruption of four to six hours, whereas companies without such plans experience average disruptions of ten hours.

Although developing and implementing an effective Emergency Preparedness Plan can be costly and time-consuming, these costs are insignificant when compared to the potential losses a Company must bear in the event of a major catastrophe.
An Emergency Preparedness Plan generally encompasses three areas:

✓ Emergency Preparedness- is the process of developing and defining roles and responsibilities, procedures, and resources for the Plan.

- ✓ Emergency Response - is the process of implementing the organization’s policies, procedures, and actions to stabilize and control an emergency as it occurs and throughout its duration.
- ✓ Emergency Recovery - is the process of implementing the organization’s policies, procedures, and actions to resume the organization’s normal operation.

7.1. Continuity Planning for Computer Operations

- ▪ Roles and Responsibilities
- ✓ Management must be involved at all levels to provide commitment, input, decisions,and approval.
- ✓ Technical support personnel will be needed to provide the hardware, software, anddata requirements, to help plan the recovery process, and to assist with testing.
- ✓ One or more staff members may be dedicated to the development of the businessimpact analysis, disaster recovery plans, ongoing Plan maintenance, and periodictesting.
- ▪ Business Impact Analysis

An effective business impact analysis (BIA) will establish a clear picture of the critical functions or services that are dependent on computer automation that must be restored following an emergency

In a business impact analysis, you will define and prioritize critical functions of the business, establish recovery time-frame requirements, and determine the computer automation necessary to support the critical functions. Thus, you can develop specific mitigation and disaster recovery plans appropriate to support the critical function requirements.

An effective business impact analysis (BIA) can

- ✓ define and prioritize the critical functions or services that are dependent on computer
- ✓ automation that must be restored following an emergency
- ✓ establish recovery time-frame requirements
- ✓ determine the computer automation necessary to support the critical functions
- ✓ obtain management’s commitment to providing the resources needed to accomplish
- ✓ disaster recovery, or confirm management’s acceptance of the risk of not planning for disaster recovery.

- ▪ Develop Plans Specific to Your Needs

Depending on the size and complexity of your organization, one plan may cover all of your automation processes, or you may need separate plans for special needs

Determine the extent of planning needed for your organization. Depending on the size and complexity of your organization, one Plan may cover all of your automation processes. Separate Plans may be required for

- ✓ hardware (such as a distributed system or network communications environment)
- ✓ software (such as the operating platform, application software, and data repositories)
- ✓ Types of data repositories, such as hierarchical databases or relational databases, if they are handled by specialized units.

- Preparedness
  Prevention and protection are the best and most economical strategies for emergency preparedness. Effective protection of automation hardware, software, and data repositories prevents disasters and significantly reduces the impact of potential disasters.

  - ✓ Hardware protection measures (surge protectors, battery backups, uninterruptable power supplies [UPS], physical security, and environmental control)
  - ✓ Software protection measures (make backup copies of critical software and data on a regular basis, and store them off-site, along with equipment configuration files, current recovery plans, and documentation)

Continuity of operations planning process

Continuity of operations planning involves more than planning for a move offsite if a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in case of disruptions, either long or short term in duration. The continuity planning process is covered in six steps:

Step 1 - Identify Mission- or Business-Critical Functions

Step 2 - Identify Resources that support Critical Functions

Step 3 - Anticipate Potential Contingencies or Disasters

Step 4 - Select Continuity Of Operations Planning Strategies

Step 5 - Document Continuity Of Operations Strategies

Step 6 - Test and Revise Strategies

Step 1 - Identify Mission- or Business-Critical Functions

Because the development of the business plan will be used to support the continuity of operations planning process, it is necessary, not only to identify critical missions and business processes, but also to set priorities and time criticalities for them.

Functional Activities Listing-The process continues by developing a list of all functions performed by the office in support of the mission. In parallel with this listing, it is also necessary to identify those functions that require support from IT Systems, and the extent of that dependency (i.e., is the function totally dependent on IT System support, is only some portion that can be quantified dependent on such support, or could the function be performed manually with little or no loss of efficiency). Any special requirements affecting the performance of the function or relating to the information involved should also be noted. These could include the sensitivity of data, or whether there is a specific timeframe when data is more critical than other times.

Criticality Determination- The next part of the process is to compare the functional activities against the criticality determinations and corresponding time frames. The result is a prioritized list of essential activities, based on criticality, and reflected in terms of the maximum time frame that these essential functions are not performed before the office fails to accomplish its mission. It can be further modified to identify specific systems, applications, and/or databases if a function is supported by more than one, or if a given system, application, or database is more critical to the effective completion of a given function.

Step 2 - Identify Resources that support Critical Functions

After critical missions and business functions are identified, supporting resources should be identified, as well as the timeframes in which each resource is used, and the effect of unavailable resources on the missions. It is important to note that the Continuity of Operations Plan (COOP) resources inventory must consist of only those physical resources and support services necessary for an office to perform the essential parts of its mission.

The COOP does not plan for the immediate or even eventual replacement of all existing resources at an alternate site. Rather, it is intended to implement a viable and effective office in an alternate location for an undetermined period of time to perform only those functions essential to the mission.

Step 3 - Anticipate Potential Contingencies or Disasters

Although it is impossible to anticipate everything that can go wrong, this step involves identifying a likely range of problems. Developing scenarios can help an organization to prepare a plan that addresses a wide range of possible mishaps. Scenarios should include small and large disruptions that require both short-term (contingency) and long-term (continuity) solutions.

Step 4 - Select Continuity of Operations Planning Strategies

This step considers the use of contingency and continuity plans to recover needed resources. When alternative strategies are evaluated, current controls for preventing and minimizing losses should be considered. A contingency planning strategy normally consists of five parts:

- Prevention refers to those measures taken to forestall a disruption of service (e.g., preventive maintenance, virus prevention, etc.).
- Response encompasses the initial actions taken to protect lives and limit damage.
- Resumption refers to the steps taken to continue support for critical functions.
- Recovery concerns the re-activation of a greater scope of business processes and services beyond the most time-sensitive processes.
- Restoration is the return to normal operations.

The longer it takes to restore normal operations, the longer the organization will have to operate in the resumption or recovery mode. The selection of a strategy needs to be based on practical considerations, including feasibility and cost.

Step 5 - Document Continuity of Operations Strategies

With continuity of operations strategies well defined, the next step is to create the COOP itself. The COOP needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a continuity of operations event, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan.

Step 6 - Test and Revise Strategy.

A COOP should be tested in order to train personnel, and to keep the plan in step with changes to the environment. The extent and frequency of testing will vary among organizations and systems. There are several types of testing:

Review - This is a simple test to check the accuracy of the COOP. For instance, a reviewer can check the accuracy of contact telephone numbers, building and room numbers, and whether the listed individuals are still in the organization.

Analysis - An analysis may be performed on the entire plan or parts of it. The analyst may mentally follow the strategies in the COOP and look for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to detect missing or unworkable pieces of the plan.

Simulation & Test - Simulation and test consists of various types and scope of exercises designed to test and evaluates the COOP. In the Structured Walk-through, a disaster scenario is established, and the teams "walk-through"their assigned tasks. This is a role-playing activity that requires the participation of at least the team leaders and their alternates. A Tactical Exercise is a simulated exercise, conducted in a "war game" format. All members of the continuity organization are required to participate and perform their tasks and procedures under announced or surprise conditions. The exercise monitor provides information throughout the exercise to simulate events following an actual disaster.

Recovery

Develop plans for the recovery of automated processes and communication networks connecting all data processing environments. A good plan will identify:

- ✓ assumptions
- ✓ recovery location(s)
- ✓ recovery and management teams
- ✓ notification and contact lists
- ✓ response procedures
- ✓ recovery processes
- ✓ minimum recovery requirements
- ✓ functions or services to be recovered
- ✓ Develop an ongoing process for testing and maintaining the Plan.
- ✓ Request that management of the areas or functions supported by the Plan review and approve the Plan, in order to ensure its consistency with their expectations.

Continuity Planning for Computer Operations

The activities include the following listed below:

a. Software and Network Protection

Inventory Controls

- ✓ Maintain a current inventory of all hardware and upgrades.
- ✓ Create a master log of DIP switch and jumper settings.
- ✓ Create a master log of miscellaneous cables, gateways, wire frames, and other equipment.
- ✓ Maintain a current inventory of all software and upgrades.
- ✓ Create a master log of software service packs, fixes, and order of installation.

- ✓ Log the configuration settings used for the installation of hardware and software.
- ✓ Store warranties, manuals, installation booklets, and other paperwork away from computer.
- ✓ Store original copies of software and upgrades away from computer.

Saving and Restoring Documents

- ✓ Make a copy first, then store originals and use the copy.
- ✓ Obtain as much RAM as you can afford on clients and servers.
- ✓ Enable “full auto saves” versus “fast saves,” for easier restorations.
- ✓ Enable “make back-up copy” whenever offered, to protect originals.
- ✓ Name and save documents immediately, to place working document into hard disk space.
- ✓ Re-save documents often, especially after many revisions.
- ✓ Copy documents onto sets of “copied” diskettes. If one fails, there is a second copy.
- ✓ Make regular “mini” backups of “my documents” or similar files.

Software and Data Duplication

- ✓ Use automated software to conduct daily incremental backups.
- ✓ Use automated software to conduct weekly full backups to be sure that all resources are covered.
- ✓ Rotate backups through a set cycle.
- ✓ Maintain at least three copies in rotation, with at least one copy stored off-site.
- ✓ Replace backup media at 80 percent recommended use, to avoid bad sectors,etc.

Storage of Software and Data Backup Place backups in U.L.-listed records containers.

- ✓ Store containers off-site at a location that is accessible 24 hours a day, 7 days a week.
- ✓ Ensure that off-site storage is environmentally conditioned and secured, allowing only authorized acces s.
- ✓ Ensure that off-site storage is far enough away so that it will not be affected byan area-wide disaster that may involve the company location.
- ✓ Clearly mark containers that have critical backups and documentation (e.g.,use red containers).
- ✓ Rotate off-site backups.
- ✓ Use off-site backups when performing disaster recovery exercises.

Virus Protection

- ✓ Install virus protection software for network servers.
- ✓ Install virus protection software for client computers.
- ✓ Run background checking portion of virus software at all times.
- ✓ Automatically scan all disks, removal disks, and tapes at least weekly,(preferably nightly).
- ✓ Automatically scan all client computer hard disks at least weekly (preferablydaily at logon).
- ✓ Automatically update virus protection software at least monthly.
- ✓ Scan all diskettes, removable media, CDs, and DVDs before use.
- ✓ Before using input from the Internet or electronic mail, load it to diskette and scan.
- ✓ Develop procedures for handling viruses, in order to limit their impact should they enter the system.

Software and Hardware Compatibles

- ✓ Develop software and hardware certification procedures.
- ✓ Always pre-test new software and hardware on non- critical PCs.
- ✓ Test, re-test, and test again, until there are no apparent conflicts.
- ✓ Develop a contingency fall-back plan before installation of changes to critical systems.
- ✓ Be ready for client and server "crashes," and have backup drives ready"online."

b. Computer Networks

- ✓ Use encryption on E-mail, documents, teleconferencing, and Internet phone, when working with sensitive data.
- ✓ Block, or severely restrict access to, files, modems, printers, and faxes fromInternet users.
- ✓ Use "Caller ID" services to identify hackers and password-cracker programs.
- ✓ Lock out hackers and password-cracker programs after three attempts.
- ✓ Change passwords at least quarterly, and require new passwords of 8 to 64 alphanumeric characters.
- ✓ Use private and public key encryption services whenever possible.
- ✓ Intranets, LANS, and WANS
- ✓ Carefully control access to software, data files, printers, modems, and faxeswithin an Intranet.
- ✓ Change passwords at least quarterly, and require new passwords of 8 to 64alphanumeric characters.
- ✓ Set company-wide system and user policies, and update them daily.
- ✓ Disable access by temporary or terminated employees, vendors, andcustomers.

c. Hardware Protection Hard Drive Maintenance and Upkeep

- ✓ Always make a full backup before performing hard drive maintenance.
- ✓ Clean out temporary files regularly.
- ✓ Clean out the "trash can" or "recycle" bin at least weekly.
- ✓ Clean out "trash cans" or "deleted items" folders in electronic mail programs.
- ✓ Archive and clean out calendar information at least twice per year.
- ✓ Run compression utilities for various programs that use "data bases," at least weekly.
- ✓ Run basic "scan disk" (or similar software) at least weekly on all machines, or at startup.
- ✓ Run thorough "scan disk" (or similar software) at least twice a year to mark
- ✓ defective sectors.
- ✓ Run a hard disk defragmentation program at least monthly, to increase computer efficiency.

Hardware Duplication

- ✓ Contract for hot site, warm site, cold site, or mobile unit vendor services.
- ✓ Contract with hardware vendors for quick shipment of critical equipment.
- ✓ Check software contracts/licenses for clauses pertaining to use at alternate location during emergencies.
- ✓ Create a contingency plan for the purchase, installation, and certification of replacement equipment.
- ✓ Determine the excess cost associated with "Rush" manufacturing, installation, and certification.

Duplicate Servers

- ✓ Determine the cost of purchasing and installing a true duplicate server.

- ✓ Determine the cost of upgrading the “back-up” server to full server.
- ✓ Determine the cost of duplicate software, including license fees for multiple users and sites.
- ✓ Determine the cost to maintain “exact” duplicate servers, including all overhead expenses.
- ✓ Locate servers in separate areas, fire divisions, or buildings.

d. Facilities, Environmental Controls, and Security

Main and Emergency Power

Include but not limited to the following:

- ✓ Ensure that power panels are fed from separate trunk lines.
- ✓ Ensure that power panels are easily accessible.
- ✓ Ensure that power to critical equipment is distributed from separate power panels.
- ✓ Ensure that panels, circuit breakers, and UPS rating exceed the total wattage of all attached equipment.
- ✓ Verify that all critical communication equipment is protected by noise-shielded and surge-protection devices.
- ✓ Verify that all critical equipment is powered by an Uninterruptable Power Supply (UPS).
- ✓ Ensure that the UPS is “network aware” and capable of starting the shutdown process.
- ✓ Use backup emergency generators for “No Down Time” applications.
- ✓ Ensure that emergency systems shut-down procedures are documented; include procedures for an ordered systems shut-down.
- ✓ Ensure that emergency room power down is available in the room and at a remote location.

Detection and Suppression Systems

- ✓ Ensure that fixed fire detection, alarm, and fire suppression systems are installed and maintained according to requirements, and manufacturers’ specifications.
- ✓ Install wet or pre-action sprinkler systems in all areas.
- ✓ Install fire alarm signals in all areas.
- ✓ Verify that fire alarm systems transmit signals to a 24-hour monitoring station.
- ✓ Install smoke detectors below the raised floors, on ceilings, and above suspended ceilings.
- ✓ Install a water detection system if flooding is a potential hazard under raised floors.
- ✓ Test all detection, alarms, and suppression equipment on a regular basis.
- ✓ Provide regular training in the use of fire extinguishers to employees.
- ✓ Install illuminated exit signs and post evacuation routes in all areas.
- ✓ Practice evacuation drills regularly.

Security Controls

- ✓ Limit access to computer areas (use ID cards, key pads, door locks, and guard stations).
- ✓ Limit access to computer systems (use BIOS passwords, client and network passwords).
- ✓ Secure and limit access to location of keys, passwords, combination lock numbers, etc.
- ✓ Install burglary/intrusion alarm systems, closed-circuit TV monitoring, guard services, and sign-in and sign-out sheets.
- ✓ Use “power on” locks on computers.
- ✓ Keep computers, especially laptop equipment, out of sight; lock computers on or in desks, cabinets, or in a storage room.
- ✓ Change combinations and passwords quarterly, or when personnel changes occur.

Chapter eight
INFORMATION SYSTEMS AUDIT

8.1. Introduction

An Information Technology or information systems audit is the examination and evaluation of an organization's information technology infrastructure, applications, data use and management, policies, procedures and operational processes against recognized standards or established policies.

The purpose of an information systems audit is to establish whether information systems are safeguarding corporate assets, maintaining the integrity of stored and communicated data, supporting corporate objectives effectively, and operating efficiently.

Audit represents a complex activity for assessing an information system in order to set forth a qualified opinion regarding the conformity between the system and the regulating standards, as well as over the information system's capacity of achieving the organization's strategic objectives.

Information systems have to be auditable by design. This means that every transaction can be traced to the total figures it affects, and each total figure can be traced back to the transactions which gave rise to it. In other words, a audit trail must exist, making it possible to establish where each transaction originated and how it was processed. Transaction logs provide a basic audit trail.

The four major objectives of information system audit

i. Asset safeguarding –'assets' which include the following five types of assets:

- Data objects in their widest sense, (i.e., external and internal, structured and non- structured, graphics, sound, system documentation etc).
- Application system is understood to be the sum of manual and programmed procedures.
- Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.
- Resources to house and support information systems, supplies etc.
- Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

ii. Effective and efficient use of resources

- Effectiveness - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- Efficiency - concerns the provision of information through the optimal (most productive and economical) usage of resources.
- Confidentiality - concerns protection of sensitive information from unauthorized disclosure.
- Integrity - relates to the accuracy and completeness of information as well as to its validity in accordance with the business' set of values and expectations.
- Availability - relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.
- Compliance - deals with complying with those laws, regulations and contractual arrangements to which the business process is subject;
- Reliability of information

iii. Reliability and integrity of information.

iv**.** Compliance with significant policies, procedures, laws and regulations.

There are three types of information system audits:

- audit carried out in support of a financial statements audit,
- audit to evaluate compliance to applicable laws, policies and standards related to IT,
- an IT audit can also be a performance (or value-for-money) audit.

Benefits of an IT Audit

- Reduce Risk. Risk reduction is the most important and significant benefit of an IT audit. ...
- Strengthen Controls.
- Comply with Regulation.
- Facilitate Communication.
- Improve Governance.

8.2. Conducting Information Systems Audit

IS auditors primarily concentrate on evaluating information system controls, on the assumption that if a system has adequate controls that are consistently applied, then the information produced by it is also reliable. They perform both scheduled and unscheduled audits.

Phases of the Audit Process

The audit process includes the following steps or phases:

- o Planning.
- o Definition of audit objectives and scope.
- o Evidence collection and evaluation.
- o Documentation and reporting.

(a) Planning

i. Preliminary assessment and information gathering.

Although concentrated at the beginning of an audit, planning is an iterative process performed throughout the audit. This is because the results of preliminary assessments provide the basis for determining the extent and type of subsequent testing. If auditors obtain evidence that specific control procedures are ineffective, they may find it necessary to reevaluate their earlier conclusions and other planning decisions made based on those conclusions.

ii. Understanding the organization.

The IT auditor has to gather knowledge and inputs on the following aspects of the entity to be audited:

- ✓ Organizational function and the operating environment

  This should include a general understanding of the various business practices and functions relating to the auditee, the types of information systems supporting the activity, as well as the environment it is operating. Understanding the organization helps decide what to audit, at what frequency, when, how and to what extent.

- ✓ Organizational Structure
  The IT auditor needs to obtain an understanding of the organizational hierarchy as well as the structure and hierarchy of the IT department.
- ✓ Criticality of IT systems
  IT systems can be categorized as Mission Critical Systems and Support Systems. Mission Critical Systems are those whose failure would have very serious impact on the organization. Support Systems are those that support management decision making, the absence of which may not result in as serious an impact as Mission Critical Systems.

iii. Nature and extent of Risks affecting the systems
The auditor can gather the required information by:

- Reading background material including organization publications, annual reports and independent audit/analytical reports
- Reviewing long-term strategic plans
- Interviewing key personnel to understand business issues
- Visiting key organization facilities

The extent of the knowledge of the organization and its processes required by the auditor will be determined by the nature of the organization and the level of detail at which the audit work is being performed. Knowledge of the organization should include the business, financial and inherent risks facing the organization. It should also include the extent to which the organization relies on outsourcing to meet its objectives. The auditor should use this information in identifying potential problems, formulating the objectives and scope of the work.

(b) Risk assessment to define audit objective and scope

The steps that can be followed for a risk-based approach to making an audit plan are:

- ▪ Inventory the information systems in use in the organization and categorise them.
- ▪ Determine which of the systems impact critical functions or assets.
- ▪ Assess what risks affect these systems and the severity of impact on the business.
- ▪ Based on the above assessment decide the audit priority, resources, schedule and frequency.

There are many risk assessment methodologies available from which the IT auditor may choose. These range from simple classifications of high, medium and low based on the judgement to complex and apparently scientific calculations to provide a numeric risk rating.

Elements of controls that should be considered when evaluating control strength are classified as Preventive, Detective and Corrective with the following characteristics.

Preventive

- ✓ Monitor both operation and inputs
- ✓ Attempt to predict potential problems before they occur and make adjustments
- ✓ Prevent an error, omission or malicious act from occurring

Detective

- ✓ Use controls that detect and report the occurrence of an error, omission or malicious act.

Corrective

- ✓ Minimise the impact of a threat
- ✓ Resolve problems discovered by detective controls

- ✓ Identify the cause of a problem
- ✓ Correct errors arising from a problem
- ✓ Modify the processing systems to minimize future occurrence of the problem.

The auditor should ordinarily make a preliminary evaluation of the controls and develop the audit plan on the basis of this evaluation. Based on the assessments of inherent and control risks, including the preliminary evaluation of computer-based controls, the auditor should identify the general control techniques that appear most likely to be effective and that therefore should be tested to determine if they are in fact operating effectively. By relying on these preliminary assessments to plan audit tests, the auditor can avoid expending resources on testing controls that clearly are not effective. Although it is essential to set out audit objectives clearly for commencement of detailed audit it is necessary to understand that during the course of the audit these objectives could undergo modifications or further elaborations.

The following is an illustrative list of some of the common audit objectives for an IT audit:

- ✓ Review of the controls of the IT systems to gain assurance about their adequacy and effectiveness.
- ✓ Evaluation of the performance of a system or a specific programme.
- ✓ Review of the security of the IT systems.
- ✓ Examine the system development process and the procedures followed at various stages involved therein.

Audit objectives and scope could cover more than just one aspect of the above mentioned areas. For example, review of system security could cover merely one of the following aspects or a combination of these:

- ✓ Firewall security
- ✓ Physical access security
- ✓ Passwords
- ✓ Security settings
- ✓ User rights etc.

Scope defines the boundaries of the audit. Determining the scope of the audit is a part of audit planning and addresses such aspects as the period and number of locations to be covered and the extent of substantive testing depending on risk levels and control weaknesses.

(c) Evidence collection and evaluation

Competent, relevant and reasonable evidence should be obtained to support the auditor’s judgement and conclusions regarding the organization, programme, activity or function under audit. Data collection techniques should be carefully chosen. The auditors should have a sound understanding of techniques and procedures chosen.

i. Types of Audit Evidence.

When planning the IT audit work, the auditor should take into account the type of the audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. The types of audit evidence, which the auditor should consider using, include:

- Observed process and existence of physical items
- Documentary audit evidence (including electronic records)
- Analysis (including IT enabled analysis)

Physical evidence is obtained by observing. Physical verification is the inspection or count by the auditor of a tangible asset. The auditor can physically inspect for the presence of computers, terminals, printers etc. The computer Centre should be visited for the visual verification of the presence of water and smoke detectors, fire extinguishers etc. Physical access controls are designed to protect the organization from unauthorized access.

The following methods are generally employed for collection of audit evidence.

- Interviews

Auditors can use interviews to obtain both qualitative and quantitative information during evidence collection work. System analysts and programmers can be interviewed to obtain a better understanding of the functions and controls embedded within the system. Data entry staff can be interviewed to determine how they correct input data that the application system identifies as inaccurate or incomplete. Users of an application system can be interviewed to determine their perceptions of how the system has affected the quality of their working life. Operations staff can be interviewed to determine whether any application system seem to consume abnormal amounts of resources when they are executed.

- Questionnaires

Questionnaires have been used traditionally to evaluate controls within systems. Auditors can also use questionnaires to flag areas of system weakness during evidence collection. Similarly, questionnaires can be used to identify areas within an information system where potential inefficiencies exist. Some general guidelines of questionnaires need to be kept in view. Questions must be specific. Must be used a language which is commensurate with the understanding of the intended person. Leading questions, presumptuous questions and leading questions must be avoided.

3- Flowcharts

Control flowcharts show that controls exist in a system and where these controls exist in the system. They have three major audit purposes:

- Analytical Procedures

Analytical procedures use comparisons and relationships to determine whether account balances appear reasonable. Analytical procedures should be performed early in the audit to aid in deciding which accounts do not need further verification, where other evidence can be reduced and which audit areas should be more thoroughly investigated..

Tools of evidence collection

With increased necessity for certification of systems, there is also an increase in the availability of tools which the IT auditors can use.

- Generalized Audit Software

Generalized audit software provides the means to gain access to and manipulate data maintained on computer storage media. IDEA is a commonly used example of generalized audit software. They provide a number of functions such as file access, file re- organization, selection and extraction of data, various data analysis function and reporting functions. They are used to examine the existence, accuracy, completeness, consistency and timeliness of data the quality of processes embedded within an application system analytical review to monitor key audit indicators such as trend analysis.

- Industry specific audit software

Industry specific audit software is designed to provide high level commands that invoke common audit functions needed within a particular industry. To be more specific they provide industry specific logic.

- Utility Software

This software performs frequently used functions such as copy, sort, disc search, disc format etc.

- Specialized Audit Software

This is software written to fulfil a specific set of audit tasks. Most well developed systems have embedded audit modules, which essentially comprise routines that throw up alerts as well as information to ensure continued dependence on controls.

- Concurrent Auditing Tools

Concurrent Auditing techniques are used to collect audit evidence at the same time as an application system undertakes processing of its data.

(d) Documentation and Reporting

Auditors should adequately document the audit evidence in working papers, including the basis and extent of the planning, work performed and the findings of the audit Documentation includes a record of:

- The planning and preparation of the audit scope and objectives
- The audit programme
- The evidence collected on the basis of which conclusions are arrived at.
- All work papers including general file pertaining to the organization and system
- Points discussed in interviews clearly stating the topic of discussion, person interviewed, position and designation, time and place.
- Observations as the auditor watched the performance of work. The observations may include the place and time, the reason for observation and the people involved.
- Reports and data obtained from the system directly by the auditor or provided by the audited staff. The auditor should ensure that these reports carry the source of the report, the date and time and the conditions covered.
- At various points in the documentation the auditor may add his comments and clarifications on the concerns, doubts and need for additional information. The auditor should come back to these comments later and add remarks and references on how and where these were resolved.

The draft and final reports of the audit should form part of the audit documentation.

i. Structure of the report.

The report should be timely, complete, accurate, objective, convincing, and as clear and concise as the subject permits. The report can be broadly structured under the following headings:

- Introduction

A brief introduction to the IT Audit being taken up would be the starting point of the report. The report must briefly give details of the system highlighting application and operating software environment and hardware resources required to run the system. The volume of data, the complexity of processing and other details should also be highlighted so that the reader can gain a clear idea about the system to appreciate subsequent audit findings. The criticality of the system must be assessed and mentioned, as many of the audit observations gain their seriousness from the criticality of the system. If the data flow is complex, a flow chart may be annexed to the report.

- Objectives, Scope and Methodology

Knowledge of the objectives of the audit, as well as of the audit scope and methodology for achieving the objectives, is needed by readers to understand the purpose of the audit, judge the merits of the audit work and what is reported, and understand significant limitations.

In reporting the audit's objectives, auditors should explain the aspects of performance examined.

In reporting the scope of the audit, auditors should describe the depth and coverage of work conducted to accomplish the audit's objectives.

To report the methodology used, auditors should clearly explain the evidence gathering and analysis techniques used. This explanation should identify any significant assumptions made in conducting the audit; describe any comparative techniques applied and describe the criteria used.

- Findings

Auditors should report the significant findings developed in response to each audit objective. In reporting the findings, auditors should include sufficient, competent, and relevant information to promote adequate understanding of the matters reported and to provide convincing but fair presentations in proper perspective. Auditors should also report appropriate background information that readers need to understand the findings.

- Conclusions

Auditors should report conclusions as called for by the audit objectives. The strength of the auditors' conclusions depends on the persuasiveness of the evidence supporting the findings and the logic used to formulate the conclusions. Sweeping conclusions regarding absence of controls and risks thereon may be avoided, when they are not supported by substantive testing.

- Recommendations

Auditors should report recommendations when the potential for significant improvement in operations and performance is substantiated by the reported findings. Recommendations to effect compliance with laws and regulations and improve management controls should also be made when significant instances of noncompliance are noted or significant weaknesses in controls are found.

Auditors should also report the status of uncorrected significant findings and recommendations from prior audits that affect the objectives of the current audit. Constructive recommendations can encourage improvements. Recommendations are most constructive when they are directed at resolving the cause of identified problems, are action oriented and specific, are addressed to parties that have the authority to act, are feasible, and, to the extent practical, are cost-effective

- Noteworthy Accomplishments

Noteworthy management accomplishments identified during the audit, which were within the scope of the audit, can be included in the audit report along with deficiencies. Such information provides a more fair presentation of the situation by providing appropriate balance to the report.

- Limitations

It is important to mention in the audit report, limitations that were faced by audit.

8.3. AUDIT OF VARIOUS SECTIONS OF INFORMATION SYSTEMS

When performing IT Control Audit, both types of testing – compliance and substantive testing would be involved. Compliance testing determines if controls are being applied in the manner described in the program documentation or as described by the auditee.

IT controls can be classified in two broad categories:

a. General Controls
b. Application Controls

A. GENERAL CONTROLS

General controls include controls over data Centre operations, system software acquisition and maintenance, access security, and application system development and maintenance.

The IT auditor will focus on general controls that normally pertain to an entity's major computer facilities and systems supporting a number of different IT applications, such as major data processing installations or local area networks. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications i.e. application controls. Following are the major categories of general controls that an auditor should consider. The IT auditor may use the information for evaluating the practices adopted by auditee organization. In order to facilitate the auditor's evaluation, sample audit checklists in a tabular format have been summarised in the appendix of this manual.

General IT controls include:

- Organization and management controls (IT policies and standards).
- IT operational controls.
- Physical controls (access and environment).
- Logical access controls.
- program change controls.
- Business continuity and disaster recovery controls.

I. Organization and management controls (IT policies and standards).

Examples include IT policies, standards, and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, business continuity planning, IT project management, etc. General IT controls are concerned with the organization's IT infrastructure, including any IT related policies, procedures and working practices.

ii. IT Operations control

The roles of IT operations include the following:

- Capacity Planning: ensuring that the computer systems will continue to provide a satisfactory level of performance in the longer term. This will involve IT operation staff having to make estimates of future CPU requirements, disk storage capacity and network loads capacity.
- Performance Monitoring: monitoring the day to day performance of the system in terms of measures such as response time.
- Initial Program loading: booting up the systems, or installing new software.
- Media Management: includes the control of disks and tapes, CD ROMs, etc.
- Job Scheduling: a job is normally a process or sequence of batch processes which are run overnight or in background and which update files etc. Jobs are normally run periodically, either daily, weekly, monthly.
- Back-ups: backups of data and software should be carried out by IT operations staff on a regular basis.
- Network Monitoring and Administration: The IT operations function is given the responsibility for ensuring that communication links are maintained.

Risks

The risks associated with poorly controlled computer operations are:

- ✓ Applications not run correctly
- ✓ Loss or corruption of financial applications or the underlying data files: may result from improper or unauthorised use of system utilities.
- ✓ Delays and disruptions in processing. Wrong priorities may be given to jobs.
- ✓ Lack of backups and contingency planning increases the risk of being unable to continue processing following a disaster.
- ✓ Lack of system capacity. The system may be unable to process transactions in a timely manner because of overload, or lack of storage space preventing the posting of any new transactions.
- ✓ High amount of system downtime to fix faults.
- ✓ Users' problems remaining unresolved due to a poor help-desk function.

Audit Procedures

Service Level Agreements (SLA)

This allows users to specify and agree, preferably in writing, what levels of service, in terms of quantity and quality, they should receive. The structure and level of service specified in a SLA will depend upon the working practices and requirements of each organization.

A typical SLA would contain the following:

- ✓ General provisions including the scope of the agreement, its signatories, date of next review.
- ✓ Brief description of services
- ✓ Service hours
- ✓ Service availability (percentage availability, maximum number of service failures and the maximum downtime per failure);
- ✓ User support levels
- ✓ Performance (response times, turnaround times);
- ✓ Security
- ✓ Restrictions

The auditor should review any SLA to determine that they support the accurate and consistent processing

iii. Physical Control (Access and Environment)

- Control Objectives

The objective of physical and environmental controls is to prevent unauthorized access and interference to IT services. In meeting this objective, computer equipment and the information they contain and control should be protected from unauthorized users. They should also be protected from environmental damage, caused by fire, water (either actual water or excess humidity), earthquakes, electrical power surges or power shortages. The entity's IT security policy should include consideration of physical and environmental risks.

- Risks

Physical

- ✓ Accidental or intentional damage by staff.
- ✓ Theft of computers or their individual components.
- ✓ Power spikes or surges which may cause component damage and the loss or corruption of data.
- ✓ Copying or viewing of sensitive or confidential information.

Environmental

- ✓ Fire/water damage (or damage from other natural disasters).
- ✓ Power: Cuts, leading to loss of data in volatile storage (RAM).
- ✓ Spikes: leading to system failures, processing errors, damage to components of equipment.
- ✓ Failure of equipment due to temperature or humidity extremes (or just outside tolerances of a few degrees).
- ✓ Static electricity: can damage delicate electrical components. Computer chips (ROM, RAM and processor) are delicate and easily damaged by static electricity shocks.
- ✓ Others: e.g. Lightning strikes

- Audit Procedure

Physical access controls are specifically aimed at ensuring that only those who have been authorized by management have physical access to the computer systems. Physical access controls reduce the risk of unauthorized persons gaining access to the computer equipment.

The auditor should identify controls which would restrict access to the organization's site, the computer rooms, terminals, printers and data storage media. Common physical access controls include the use of locked doors, CCTV, intruder alarms, combination keypads and security guards.

iv. Logical Access Control

▪ Control Objectives

The objective of logical access controls is to protect the applications and underlying data files from unauthorized access, amendment or deletion. The objectives of limiting access are to ensure that:

- ✓ Users have only the access needed to perform their duties
- ✓ Access to very sensitive resources such as security software program, is limited to very few individuals, and
- ✓ Employees are restricted from performing incompatible functions or functions beyond their responsibility

Risks

• Users have the access to the areas other than related to the performance of their duties, causing threats to unauthorised access, amendment or deletion in the maintained data.

• Access to very sensitive resources such as security software program which may be of mission critical nature.

• Employees are not barred/ restrained from performing incompatible functions or functions beyond their responsibility.

Audit Procedure

Logical access controls can exist at both an installation and application level. Logical access controls usually depend on the in-built security facilities available under the operating system or hardware in use. Menu restrictions can be effective in controlling access to applications and system utilities. Systems may be able to control access by identifying each individual user through their unique login ids and then having a pre-defined profile of authorized menus for each.

v. Program Change Controls

▪ Control Objectives.

Even when the system development process has been completed and the new system is accepted, it is likely that it will have to be changed, maintained, or altered during its lifecycle. This change process may have an impact on the existing controls and may affect the underlying functionality of the system. Change controls are needed to gain assurance that the systems continue to do what they are supposed to do and the controls continue to operate as intended. Change refers to changes to both hardware and software. Hardware includes the computers, peripherals and networks. Software includes both the system software (operating system and any utilities) and individual applications.

▪ Risks

Change controls are put in place to ensure that all changes to systems configurations are authorised, tested, documented, controlled, the systems operate as intended.

- ✓ The risks associated with inadequate change controls are as follows:
- ✓ Unauthorised changes
- ✓ Implementation problems
- ✓ Erroneous processing and reporting
- ✓ User dissatisfaction

- ✓ Maintenance difficulties
- ✓ Use of unauthorised hardware and software

- ▪ Audit Procedure

It may be ensured in audit that the organization's procedures to control changes should include:

- ✓ Procedures for management authorization
- ✓ Thorough testing before amended software is used in the live environment
- ✓ Management review of the effects of any changes
- ✓ Maintenance of adequate records
- ✓ The preparation of fallback plans
- ✓ The establishment of procedures for making emergency changes

B. **AUDIT OF APPLICATION CONTROLS**.

Application Controls

Application controls pertain to specific computer applications. They include controls that help to ensure the proper authorization, completeness, accuracy, and validity of transactions, maintenance, and other types of data input.

Application controls are particular to an application and may have a direct impact on the processing of individual transactions. These controls are used to provide assurance that all transactions are valid, authorized, and complete and recorded. Before getting on to evaluation of application controls, it will be necessary for an auditor to secure a reasonable understanding of the system. Application controls may be divided into:

- ▪ Input controls
- ▪ Processing controls
- ▪ Output controls
- ▪ Master/Standing Data File controls.

i. Input Controls.

- ▪ Control Objectives

The objective of Input control is to ensure that the procedures and controls reasonably guarantee that:

- ✓ The data received for processing are genuine, complete, not previously processed, accurate and properly authorized.
- ✓ Data are entered accurately and without duplication.

Input control is extremely important as the most important source of error or fraud in computerized systems is incorrect or fraudulent input. Controls over input are vital to the integrity of the system.

- ▪ Risks
- ✓ Weak input control may increase the risk of:
- ✓ Entry of unauthorized data
- ✓ Data entered in to the application may be irrelevant
- ✓ Incomplete data entry
- ✓ Entry of duplicate/redundant data

- ▪ Audit Procedure

The aspects that the auditor should evaluate are:

- ✓ All prime input, including changes to standing data, is appropriately authorized.

- ✓ For on-line systems, the ability to enter data from a terminal is adequately restricted and controlled.
- ✓ If there is a method to prevent and detect duplicate processing of a source document.
- ✓ All authorized input has been submitted or, in an on-line system transmitted and there are procedures for ensuring correction and resubmission of rejected data.

Processing Controls

Processing controls ensure complete and accurate processing of input and generated data.

- ▪ Control Objectives

The objectives for processing controls are to ensure that:

- ✓ Transactions processing is accurate
- ✓ Transactions processing is complete
- ✓ Transactions are unique (i.e. No duplicates)
- ✓ All transactions are valid
- ✓ The computer processes are auditable.

- ▪ Risks

Weak process controls would lead to:

- ✓ Inaccurate processing of transactions leading to wrong outputs/results
- ✓ Some of the transactions being processed by the application may remain incomplete
- ✓ Allowing for duplicate entries or processing which may lead to duplicate payment in case of payment
- ✓ Unauthorized changes or amendments to the existing data
- ✓ Absence of audit trail rendering, sometimes, the application unauditable
- ✓

- ▪ Audit Procedure.

The auditor should ensure that there are controls to detect the incomplete or inaccurate processing of input data. Application processes may perform further validation of transactions by checking data for duplication and consistency with other information held by other parts of the system. Computerized systems should maintain a log of the transactions processed.

The transaction log should contain sufficient information to identify the source of each transaction. There should be procedures which allow identifying and reviewing all unclear transactions beyond a certain age

Output Controls

Output controls are incorporated to ensure that computer output is complete, accurate and correctly distributed.

- ▪ Audit Objectives

Output controls ensure that all output is:

- ✓ Produced and distributed on time
- ✓ Physically controlled at all times, depending on the confidentiality of the document
- ✓ Errors and exceptions are properly investigated and acted upon

- ▪ Risks

If output controls prevailing in the application are weak or are not appropriately designed these may lead to:

- ✓ Repeated errors in the output generated leading to loss of revenue, loss of creditability of the system as well as that of the organization.
- ✓ Non-availability of the data at the time when it is desired.
- ✓ Even sometimes, the information which may be of very confidential nature may go to the wrong hands.

- ▪ Audit Procedure

A combination of physical and logical controls may be used to protect the integrity of computer output. Output from one IT system may form the input to another system. Where this is the case the auditor should look for controls to ensure that outputs are accurately transferred from one processing stage to the next.

INFORMATION SYSTEMS AUDIT POLICY

a. General

A regular and proactive audit policy helps to manage and reduce risks to information systems, the data it manages, and the users it services. A security auditor is usually an external/independent third party (or at a minimum someone who is not operationally responsible for the area being audited), who evaluates systems for best practices and ensures compliance within an established set of requirements and controls.

b. Audit Scope

Considers the following when determining organizational audit scope:

•Security Vulnerabilities – Identifies security vulnerabilities using reputable outside sources, and assign risk rankings to newly discovered security vulnerabilities.

•Risk Evaluation – Identifies methods for evaluating vulnerabilities and assigning risk ratings to systems. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment.

•Automated Tools – Evaluates and recommends automated assessment tools and external resources that are suitable in identifying vulnerabilities including weak passwords, configuration issues, improper access controls, network penetration testing, and patch management issues.

•Administrative Safeguards – Defines protocols, policies, procedures, training plans and other administrative security controls useful to an auditor in comparing against a standard of operation.

•Penetration Testing – Evaluates whether penetration testing may be used to identify system vulnerabilities.

c. Audit Procedures

Access to audit tools shall be controlled and restricted to prevent possible misuse or compromise resources and log data. Audits shall be performed on a regular basis as defined by law, statute, or executive management protocol.

d. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of day to day operations.

e. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

f. Distribution
This policy is to be distributed to all staff.

g. Policy Version History

Version	Date	Description	Approved By
1.0	11/20/2016	Initial Policy	Drafted

ACCESS CONTROL ASSURANCE

Auditing is an activity where the users/subjects actions on the objects are monitored in order to verify that the sensitivity policies are enforced and can be used as an investigation tool.

Advantages of Auditing

- To track unauthorized activities performed by individuals.
- Detect intrusion.
- Reconstruct events and system conditions.
- Provide legal resource material and produce problem reports.

What to Audit

- System-level events
  System performance, Logon attempts (successful and unsuccessful), Logon ID, Date and time of each logon attempt, Lockouts of users and terminals, Use of administration utilities, Devices used, Functions performed and Requests to alter configuration files
- Application-level events
  Error messages, Files opened and closed, Modifications of files and Security violations within application
- User-level events
  Identification and authentication attempts, Files, services, and resources used and Security violations

Review of Audit Information

- Audit trails can be reviewed manually or through automated means.
- Types of audit reviews
  - Event oriented: done as and when an event occurs.
  - Periodic: done periodically to access the health of the system.
  - Real time: done with the help of automated tools as and when the audit information gets created.
- Audit trail analysis tools: These tools help in reducing/filtering the audit log information that is not necessary and provides only that information necessary for auditing.

Protecting Audit Data and Log Information

- Audit logs should be protected by implementing strict access control.
- The integrity of the data should be ensured with the use of digital signatures, message digest tools ,and strong access control.
- The confidentiality can be protected with encryption and access controls and can be stored on CD-ROM'S to prevent loss or modification of the data. The modification of logs is often called as scrubbing.

- Unauthorized access attempts to audit logs should be captured and reported

8.4. NETWORK AND INTERNET CONTROLS

- Control Objectives

The majority of systems encountered in medium to large scale organizations use either local or wide area networks to connect users.

- Risks

Where the organization's systems are connected to networks, there is potentially a greater risk of unauthorized access by unauthorized users which may lead to:

- ✓ Data loss - data may be intentionally deleted or lost in transmission;
- ✓ Data corruption - data can be corrupted by users or data errors can occur during transmission
- ✓ Fraud
- ✓ System unavailability
- ✓ Disclosure of confidential information
- ✓ Virus and worm infections - worm infections are specifically designed to spread over networks.

- Audit Procedure

Before carrying out a review of the organization's logical access and network controls, the auditor should review any technical material or publications on the organization's systems.

Controls which the auditor may encounter include:

- ✓ Network security policy: this may be a part of the overall IT security policy
- ✓ Network documentation: the organization should have copies of documentation describing the logical and physical layout of the network These are usually treated as confidential
- ✓ Logical access controls: these are especially important and the organization should ensure that logons, passwords and resource access permissions are in place
- ✓ The network should be controlled and administered by staff with the appropriate training and experience. Those staff should be monitored by management
- ✓ Certain network events should be automatically logged by the network operating system. The log should be periodically reviewed for unauthorized activities