ASP4134 - Audit Sistem Informasi

(week 6)

Reza R Pratama

Confidential. Terbatas untuk mahasiswa PKN STAN

ASP4134 - Audit Sistem Informasi

Protection of Information Assets

Confidential. Terbatas untuk mahasiswa PKN STAN

AGENDA

- Lecture Protection of Information Assets

ASP4134 - Audit Sistem Informasi

Key objectives:

1. memahami kerangka **konsep audit tata kelola** teknologi informasi berdasarkan standar tata Kelola
2. menyusun **program audit tata kelola** sistem informasi
3. menyusun **laporan audit tata kelola** sistem informasi
4. melaksanakan **pengauditan atas pengoperasian dan pemeliharaan** atas sistem informasi
5. melakukan **audit atas perolehan, pengembangan, dan implementasi sistem informasi**
6. melakukan **pengauditan atas keamanan informasi** Here we are
7. menggunakan **Teknik Audit Berbantuan Komputer** dalam pengujian pengendalian dan pengujian substantif
8. menjelaskan dampak kelemahan **pengendalian umum dan pengendalian aplikasi** terhadap peluang terjadinya kecurangan dan kesalahan saji pada laporan keuangan

Last Week Recap

Information systems (IS) operations and business resilience are important to provide assurance to users and management that the expected **level of service** will be delivered.

Service level expectations are derived from the organization's **business objectives**.

IT service delivery includes **IS operations**, **IT services,** and management of IS and the groups responsible for supporting them.

Disruptions are also an often-unavoidable factor of doing business.

Preparation is key to being able to continue business operations while protecting people, assets and reputation.

Employing **business resiliency tactics** helps organizations address these issues and limit the impact.

Part A vs Part B Topics

Part A: Information Asset Security and Control

1. Information Asset Security Frameworks, Standards, & Guidelines
2. Privacy Principles
3. Physical Access and Environmental Controls
4. Identity and Access Management
5. Network and End-point Security
6. Data Classification
7. Data Encryption and Encryption-related Techniques
8. Public Key Infrastructure (PKI)
9. Web-based Communication Technologies
10. Virtualized Environments
11. Mobile, Wireless, and Internet-of-Things (IOT) Devices

Part B: Security Event Management

1. Security Awareness Training and Programs
2. Information System Attack Methods and Techniques
3. Security Testing Tools and Techniques
4. Security Monitoring Tools and Techniques
5. Incident Response Management
6. Evidence Collection and Forensics

Part A: Information Asset Security and Control

It's about **building protection correctly** before testing, monitoring, or responding to incidents

No	Topics	Brief Explanation
1	Security Frameworks	***Rules before tools*:** protection must be structured and intentional
2	Privacy Principles	***Respect the citizen*:** personal data must be handled with care and purpose
3	Physical & Environmental Controls	***Protect the buildings***: no digital security works if the room burns
4	Identity & Access Management	**Only the right people** get the keys
5	Network & Endpoint Security	**Defend the walls** and houses
6	Data Classification	Not all valuables need the same lock
7	Encryption	Even if stolen, it stays unreadable
8	Public Key Infrastructure (PKI)	Trust needs a trusted third party
9	Web-based Technologies	Public-facing systems need extra caution
10	Virtualized Environments	Shared buildings need strong separation
11	Mobile, Wireless & IoT	Assets now move beyond the city walls

You cannot protect what you do not recognize -> Identified? Ownership is set? What's the risk?
Over protection wastes resources; under protection creates risk

Information Asset Security and Control

ASP4134 - Audit Sistem Informasi

Cyber World Today



2018

British Airways

- Personal details such as birth names, addresses, and payment card details of 400,000+ customers were leaked.
- British Airways was fined £20 million for this incident.



2020

Marriott International

- The passport information, payment card details, and names of 334 million customers were leaked, partly due to outdated systems.
- Marriott International settled a $52 million lawsuit.



2022

Advanced Computer Software Group

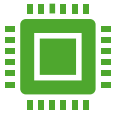
- Medical records and phone numbers for 79,904 people were leaked due to weak security policies.
- Government officials fined the organisation £3.07 million.



2023

23andMe

- Over 7 million users' sensitive data, such as names, addresses, health records, and DNA data, was leaked due to poor security policies.
- 23andMe was fined £2.31 million by government officials.



2024

SK Telecom

- Poorly configured servers led to the personal data of approximately 27 million users being leaked.
- SK Telecom were fined $97 million by government officials.

Security Triad

Confidentiality is about protecting data from **unauthorized access or disclosure**. This ensures that sensitive information is only viewable by individuals or systems that have been explicitly granted permission.



Integrity ensures that data is **accurate, consistent, and trustworthy** throughout its entire lifecycle. It means preventing unauthorized, unintentional, or malicious modification or destruction of information.

Availability ensures that authorized users have **reliable and timely access** to data, services, and resources when they need them. This pillar focuses on maintaining the functionality of the hardware, network, and systems that store and process the information.

Information Asset Security Policies, Frameworks, Standards and Guidelines



Policies and procedures provide the basis for maintaining proper operation and control



An information security *policy* is a set of rules, directives and practices designed to ensure the protection of information assets.



IS Policy Objectives

Confidentiality, Integrity, Availability, Information security guidance, Monitoring Governance, Compliance, Privacy

Issue-Specific Information Security Policies

Policy	Policy Description
Acceptable use policy	Outlines the constraints an employee must accept to use an organizational system and/or network
Change control policy	Refers to guidelines for the formal process for making changes to IT, software development and information security processes
Access control policy	Outlines access controls to an organization's data and information systems (IS) and the steps users need to follow to gain access
Incident response policy	Provides an organized approach to how the organization manages, remediates and recovers from information security incidents
Identity and access management (IAM) policy	Typically deals with the authorization of systems and applications to the right employees and how employees, contractors and third parties are authenticated by systems to comply with security standards
Remote access policy	Outlines acceptable methods of remotely and securely connecting to internal organizational networks
Bring your own device (BYOD) policy	Outlines the requirements that employees be allowed to use personal devices to access organizational infrastructure and the steps required to reduce the risk of exposure from employee-owned assets.

Information Asset Security Policies, Frameworks, Standards and Guidelines

Information Security Procedures

- are the **step-by-step** tasks that should be performed to achieve a certain objective
- address aspects like how to install operating systems (OSs), configure security mechanisms, set up new user accounts, assign computer privileges, audit activities, destroy data and report incidents.

Information Security Guidelines

- is a **description** of a particular way of accomplishing something that is less prescriptive than a procedure
- serve as recommendations to users when specific standards do not apply and assist in the implementation of the standard

Information Asset Security Policies, Frameworks, Standards and Guidelines

A **baseline** is a minimum level of security that a system, network or device must adhere to.

- For example, an organization might specify that all computer systems comply with a minimum trusted computer system evaluation criteria command and control (C2) standard.

Topics	Objective	Recommendations
Environment/ inventory	Establish and maintain an inventory.	Users are expected to follow standards for managing computers connected to the network and to have registered network addresses. The operating system (OS) and owner should be included along with the data provided.
Malware	Install antivirus software with automatic updating.	Antivirus software with an automatic DAT file should be updated at regular intervals, no less than weekly.
Passwords	Recognize the importance of passwords.	Users must use only strong passwords. The IT department should provide password guidance. Departmental accounts are created for workgroups to prevent/avoid password sharing.
Patching	Make it automatic; the less work necessary, the less chance for compromise.	Each machine should be configured for automatic OS and basic software patching. A process should be established that works for the department and minimizes disruptions at inconvenient times. Workstations should be more automated to give system administrators the time to attend to servers as required to minimize the impact on services offered.
Minimizing services offered by systems	Eliminate unnecessary services to reduce security risk and save time in the long run.	To improve basic security and minimize effort to maintain systems, workstations should offer only needed services. Many OSs are installed with services turned on. Removing services reduces a workstation's chances of being compromised and minimizes security risk.

Information Security Frameworks and Standards

Framework	Description
International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27001	ISO/IEC 27001 is an international standard on information security which specifies procedures for the development and maintenance of an information security management system in an organization. ISO/IEC 27001 provides best practices that can be adopted in information security management. It addresses organizational, people, physical and technological controls holistically.
Zachman Framework	The Zachman Framework is a model for classifying and developing enterprise architectures. Developed by John Zachman, it can be used to proactively model organizational functions, processes and elements. It is typically employed in the management of organizational change.
The Open Group Architecture Framework (TOGAF)	TOGAF is an enterprise architecture framework that is used to define business objectives and align them with architecture objectives. It ensures the adoption and application of consistent standards and methodologies by enterprise architecture professionals.
Sherwood Applied Business Security Architecture (SABSA)	SABSA is a model and methodology for the development of risk-driven and opportunity-focused information security enterprise architectures and service management to support critical business functions and processes. It consists of a life cycle starting with strategy planning, design, implementation and managing and measuring components.
COBIT	COBIT is an IT governance framework specifying the best approaches and procedures in the governance of enterprise IT to help organizations to minimize their IT risk while ensuring efficiency in the use of available resources.
NIST Cybersecurity Framework (CSF)	The NIST CSF consists of standards, guidelines and best practices that assist organizations in improving their management of cybersecurity risk. The framework is designed to be flexible and can be integrated with the existing security processes and procedures in an organization. It can be used in any industry or sector.
Information Technology Infrastructure Library (ITIL)	ITIL is a framework that promotes the standardization of IT service management in an organization. It seeks to standardize the processes of selecting, planning, delivering and maintaining the overall IT life cycle within the organization. Such standardization is expected to improve efficiency and IT service delivery.

Framework	Description
The Center for Internet Security (CIS) Critical Security Controls (CSC)	The CIS CSC provides technical security and operational controls that can be applied to any environment. It does not address risk management and focuses solely on reducing risk and increasing resilience for technical infrastructures. Controls include inventory, data protection, log management, malware and penetration testing. CIS controls link with existing risk management frameworks to help remediate identified risk and are critical especially for organizations lacking technical information security information
Payment Card Industry Data Security Standard (PCI DSS)	The PCI DSS standard was developed by major credit card companies for enhancing payment account data security. PCI DSS requirements apply to organizations with environments where cardholder data and/or sensitive authentication data are stored, processed or transmitted, as well as organizations with environments that can impact the security of the cardholder data environment. The standard's requirements extend to organizations that outsource their payment environments or payment operations to third parties.
Security, Trust, Assurance and Risk (STAR)	The STAR program was developed by the Cloud Security Alliance (CSA) as an assurance framework for cloud service providers (CSPs). It combines principles of transparency, rigorous auditing processes and harmonization of standards that reference cloud security. STAR provides organizations with cloud-specific structures for implementation of their information security programs. It consists of voluntary self-assessments, attestations and certifications that allow CSPs to validate their cloud security postures and demonstrate commitment to best practices.
Cloud Control Matrix (CCM)	The CCM was developed by the CSA and is composed of 197 control objectives in 17 domains, covering all key aspects of cloud technology. It is widely used for the systematic assessment of cloud implementation and provides guidance to both consumers and CSPs on which security controls should be implemented in the cloud supply chain. It is generally considered a de facto standard for cloud security assurance and compliance and has been mapped to other industry-accepted security standards, such as the ISO 27001/27002, PCI DSS and NIST CSF. Thus, it provides a way to align security practices with those that already exist in other domains.

Information Asset Security Policies, Frameworks, Standards and Guidelines

Frameworks	• High-level structure • Organizes control areas • Used for governance and audit alignment	THE MAP
Standards	• Mandatory requirements • Must be complied with	THE RULES
Guidelines	• Recommended practices • Flexible, context-based	THE ADVICES
Procedures	• Step-by-step execution • Operational level	THE DAILY INSTRUCTION



SECURING THE PHYSICAL & LOGICAL ACCESS

Physical and Environmental Controls

Security of information assets **requires physical** and **environmental** security.

The IS auditor needs to **evaluate applicable controls**.

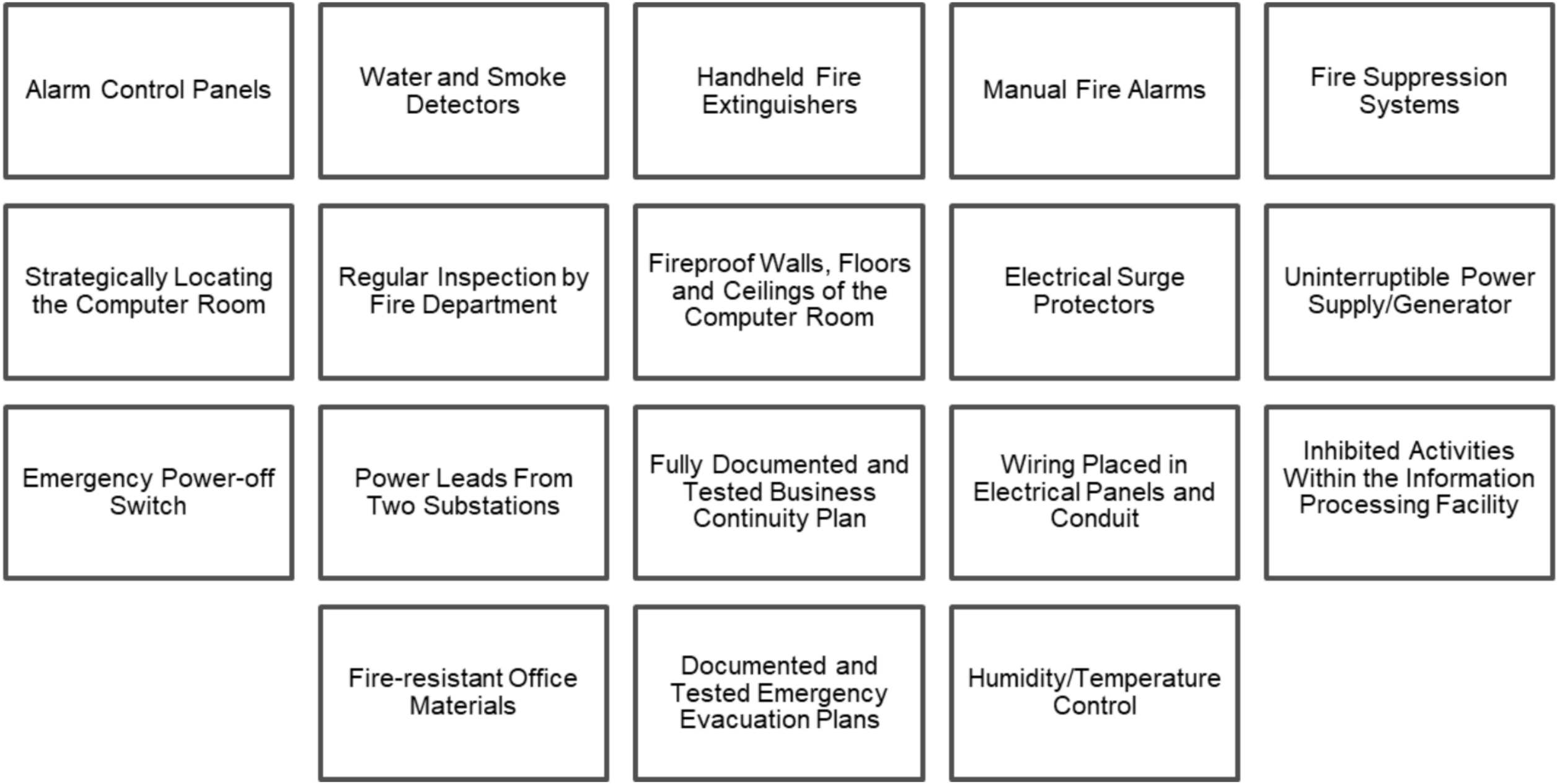
In many organizations, physical and environmental controls are **designed and implemented** by **facility management** and not by the **information security manager** or **IT**.

Most IT assets require environmental controls for things like **temperature**, **humidity** and **power**.

The IS auditor needs to assess these controls to provide assurance.

Remember what we covered in week 5 about business resilience





Controls for Environmental Exposures

Bolting door locks

Combination door locks (cipher locks)

Electronic door locks

Biometric door locks

Manual logging

Electronic logging

Identification badges (photo IDs)

Video cameras

Security guards

Controlled visitor access

Deadman doors

Computer workstation locks

A controlled single-entry point

An alarm system

Secured report/document distribution carts

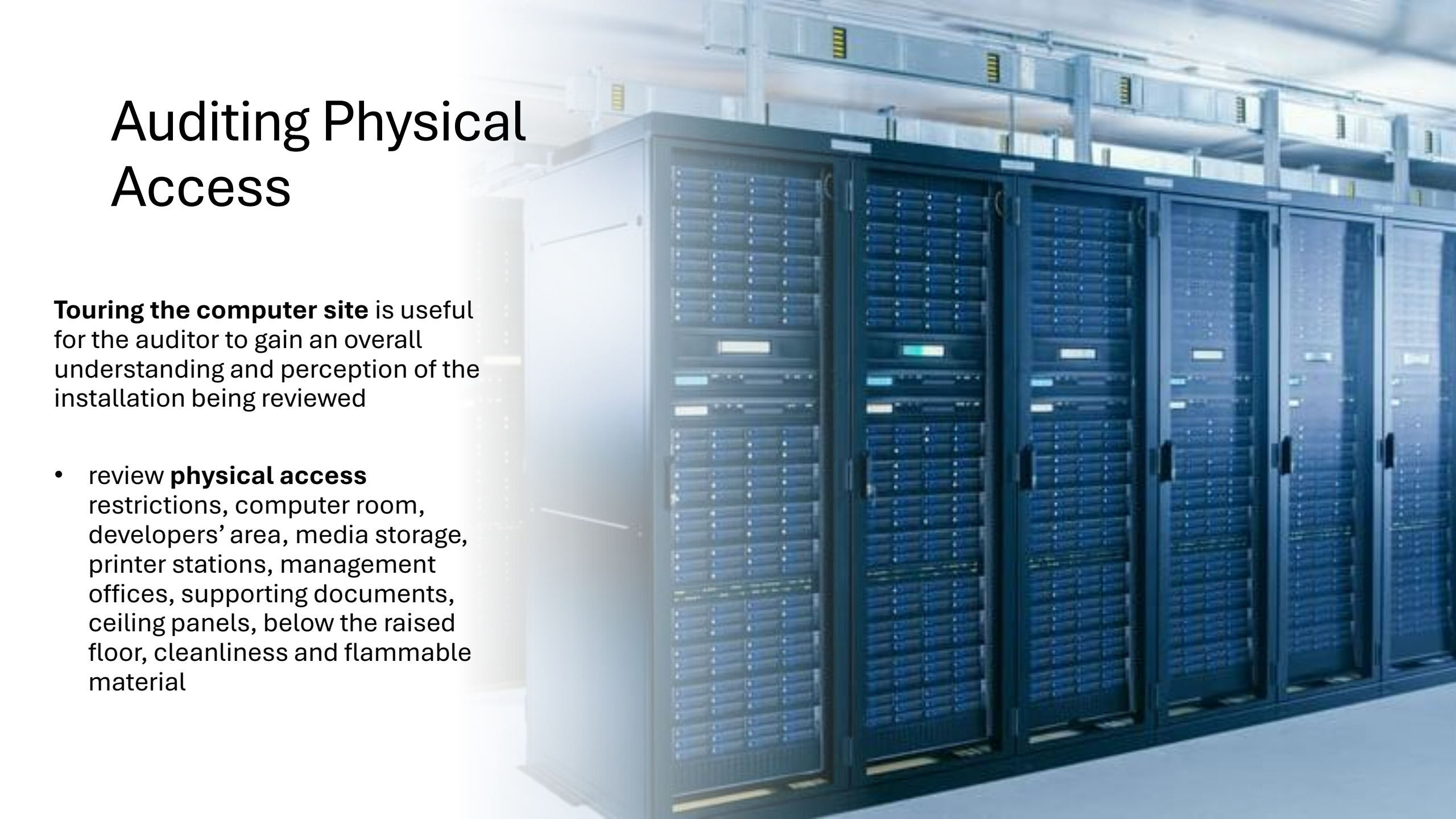
lightning

Physical Access Controls

Auditing Physical Access

Touring the computer site is useful for the auditor to gain an overall understanding and perception of the installation being reviewed

- review **physical access** restrictions, computer room, developers' area, media storage, printer stations, management offices, supporting documents, ceiling panels, below the raised floor, cleanliness and flammable material



Auditing Physical Access



Evaluate paths of **physical entry**

- All entry doors, Emergency exit doors, Glass windows and walls, Movable walls and modular cubicles, Areas above suspended ceilings and beneath raised floors, Ventilation systems, Areas behind curtains or fake walls

Terra Drone Fire Tragedy (Dec 2025): A Case Study in IT Physical Control Failure

- **What Happened:** A major fire occurred at the Terra Drone office building in Kemayoran, Jakarta, in December 2025.
- **The Cost:** The tragedy resulted in **22 fatalities**, primarily due to smoke inhalation/being trapped. It caused a total loss of the physical building, IT infrastructure, and stored assets.
- **The Suspected Cause:** Initial reports indicated the fire likely originated from **Lithium Batteries (drones)** being charged or stored in the facility (acting as a warehouse/service area) on the ground floor.



Terra Drone Fire Tragedy (Dec 2025): A Case Study in IT Physical Control Failure

A. High-Risk Asset Management Failure:

Risk: Lithium batteries are known *high-risk assets* requiring specialized storage and charging protocols (temperaturecontrol, ventilation).

Failure: These specialized controls were apparently absent or ineffective in the mixed-use building environment.



B. Fire Suppression System Deficiency:

The existing fire suppression methods (e.g., standard APAR) were **inadequate** for a massive Lithium-ion fire (which requires specific chemical or clean-agent suppression, not water).

Identity and Access Management

1. **Identification** (*Who are you?) :* Identification is the process of claiming an identity, typically via a user ID or account.
2. **Authentication** (*Prove it!*) Authentication verifies that the claimed identity is valid. (something you know, you have, or you are)
3. **Authorization** (*What Are You Allowed to Do?*) Authorization defines what actions and resources an authenticated user is permitted to access. Key principles: Least privilege - Role-based access.

Authentication Services • Single sign-on (SSO) • Federated identity management (FIM) • Multifactor authentication (MFA) • Biometric authentication • Adaptive authentication • Session management	**Authorization Services** • Rule-based access control • Role-based access control (RBAC) • Attribute-based access control • Privileged access management • Remote authorization
User Management • Provisioning • Deprovisioning • Self-service • Credential management • Delegated administration	**Central User Repository** • Directory services • Identity providers (IdPs) • Data synchronization • Identity stores • Directory federation • Virtual directory

Identification and authentication (I&A) is a **critical** building block of information security because it is needed for most **types** of **access control** and is necessary for establishing user accountability.

For most systems, I&A is the **first line of defense** because it prevents **unauthorized access** (or unauthorized processes) to a computer system or an information asset.

Logical access can be implemented in various ways.

The IS auditor should be aware of the **strengths and weaknesses of various architectures** along with the risk associated with the different architectures and how it may be addressed.

Identity and Access Management

Some of the common I&A vulnerabilities that may be exploited to gain unauthorized system access include:

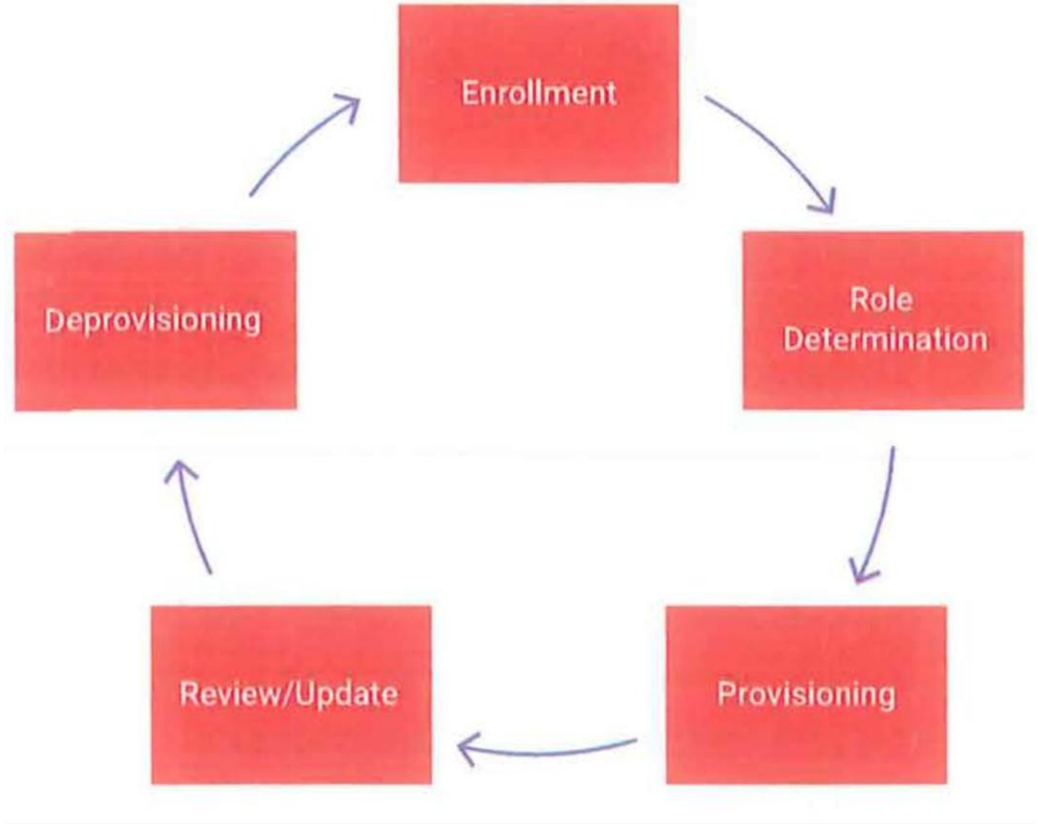
- **Weak authentication** methods (e.g., no enforcement of password minimum length, complexity and change frequency)
- Use of **simple** or easily guessed **passwords**
- The potential for users to **bypass the authentication** mechanism
- The lack of **confidentiality and integrity** for the stored authentication information
- The lack of **encryption** for authentication and protection of information transmitted over a network
- The user's lack of knowledge about the **risk** associated with sharing authentication elements (e.g., passwords and security tokens)



Identity and Access Management

- An identity and access management (IAM) framework consists of **policies**, **procedures**, **processes** and **technologies** that enable the management of identity and access information in an organization.

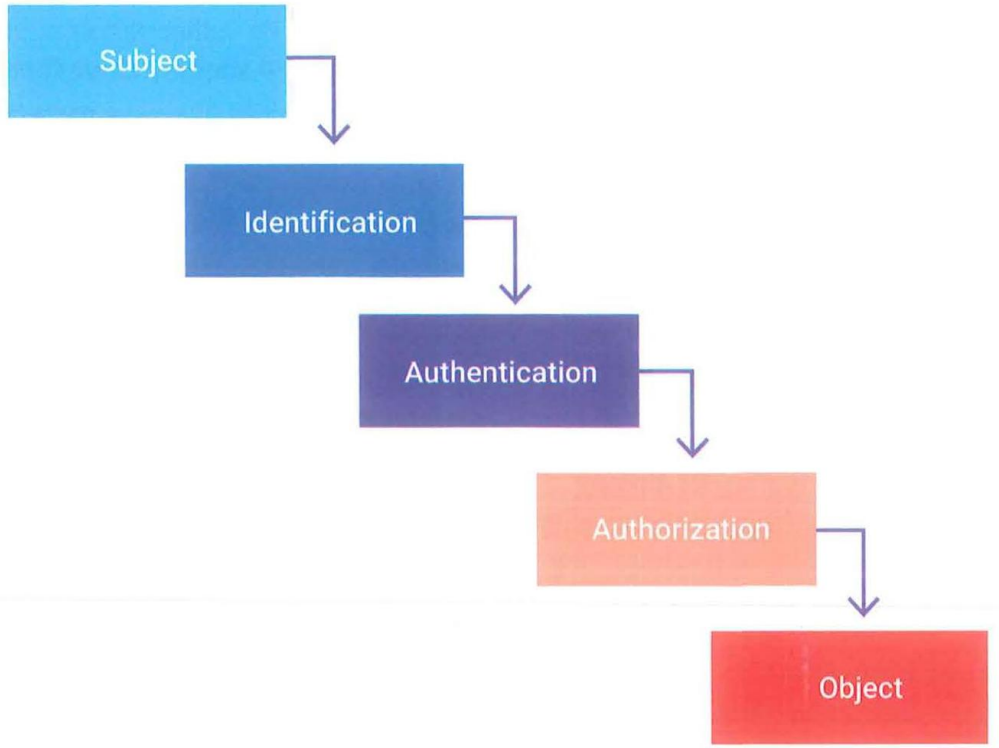
- Identity life cycle management is the process of **creating** and **maintaining** a **digital identity** for every human or non-human entity on a network



Identity and Access Management

- User accountability requires the **linking** of **activities** on a computer system to **specific individuals** and, therefore, requires the system to **identify users**.

- Authentication is the process of **proving** that subjects are who or what they claim to be; it verifies a **subject's identity**.
  - Types: Password, Multifactor, Adaptive, Token-based, Certificate-based, Biometric, Lightweight Directory Access Protocol (LDAP) and Smart card



Key Concepts of IAM	Identified Gaps and Security Concerns	Good Practices/Recommendations
Identify creation and access request	Authorized approval not in place	• The required authority (e.g., the user's manager, the resource owner or the security officer) should authorize the user for access to be granted.
	Privileged access granted without analyzing the need	• To justify its need, privileged access should be provided after approval is issued at two levels—the reporting manager level; and the reporting manager's manager or application, database or server owner level.
	Group shared access	• To justify its need, group shared access should be provided after approval is issued at two levels—the reporting manager level; and the reporting manager's manager or application, database or server owner level. • The principle of least privilege (POLP) should be applied. • The number of servers on which the account can exist should be limited. • The list of users sharing the account should be preapproved. • Account owners should maintain and publish a list of users who have access to the shared account. • The logging activities for shared accounts should be validated. • Passwords should be changed on a regular basis and whenever an employee leaves the organization or changes roles. The frequency should be defined in the process document. • If it is found that someone obtains unauthorized access, the password must be changed immediately.

Single Sign-On (SSO) Authentication

SSO allows users to access multiple apps and services with one set of login credentials.
SSO advantages include:

- **Multiple passwords** are **no** longer required
- Improves an administrator's ability to **manage users**' accounts and authorizations to all associated systems.
- reduces **administrative overhead** in resetting forgotten passwords
- **reduces** the **time** users take to **log into** multiple applications and platforms.

• Limitations:

- Not all Operating Systems **support** SSO
- The **costs** associated with SSO development can be significant
- The centralized nature of SSO presents the possibility of a **single point of failure** and total compromise of an organization's information assets

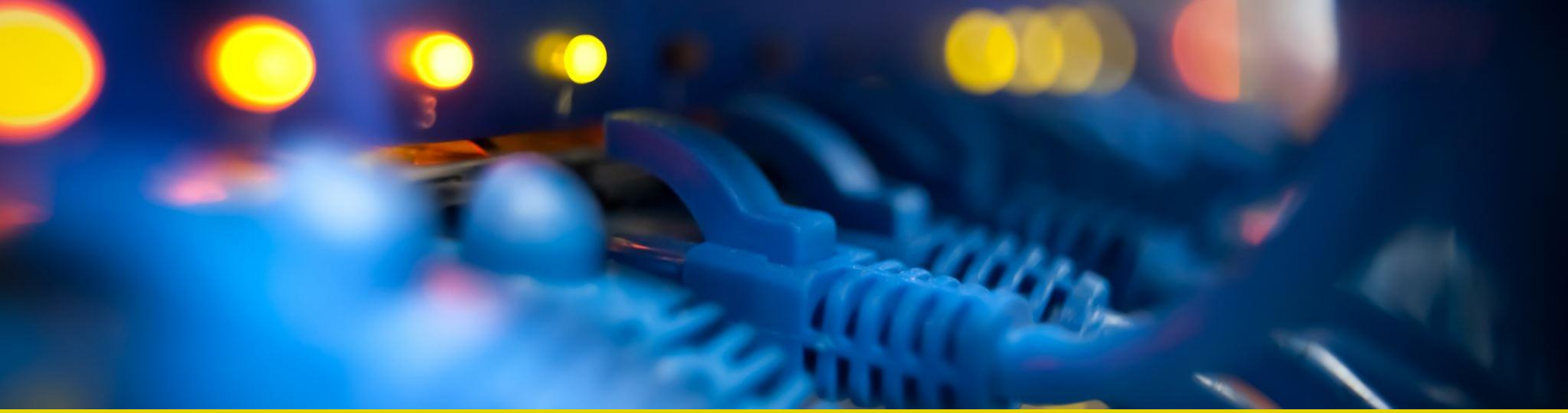
Information Security and External Parties

- Any access to the organization's information processing facilities and processing and communication of information by external parties should be **controlled**.
- Controls should be agreed to and defined in an **agreement** with the external patty.
- Organizations should have the **right to audit** the implementation and operation of the resulting security controls.
- Such agreements can help **reduce the risk** associated with external parties.

Auditing Logical Access

When evaluating logical access controls the IS auditor should:

- Obtain a general understanding of the **security risks** facing information processing
- Document and evaluate **controls** over potential access paths into the system
- **Test controls** over access paths to determine whether they are functioning and effective
- **Evaluate** the access control environment to determine if the **control objectives** are achieved
- Evaluate the **security environment** to assess its adequacy



SECURING THE NETWORK

Network and Endpoint Security

- Enterprises can effectively prevent and detect most attacks on their networks by employing **perimeter** security controls.
- Firewalls and IDSs provide protection and critical alert information at **borders** between trusted and untrusted networks.
- The proper **implementation** and **maintenance** of firewalls and IDSs is critical to a successful, in-depth security program.

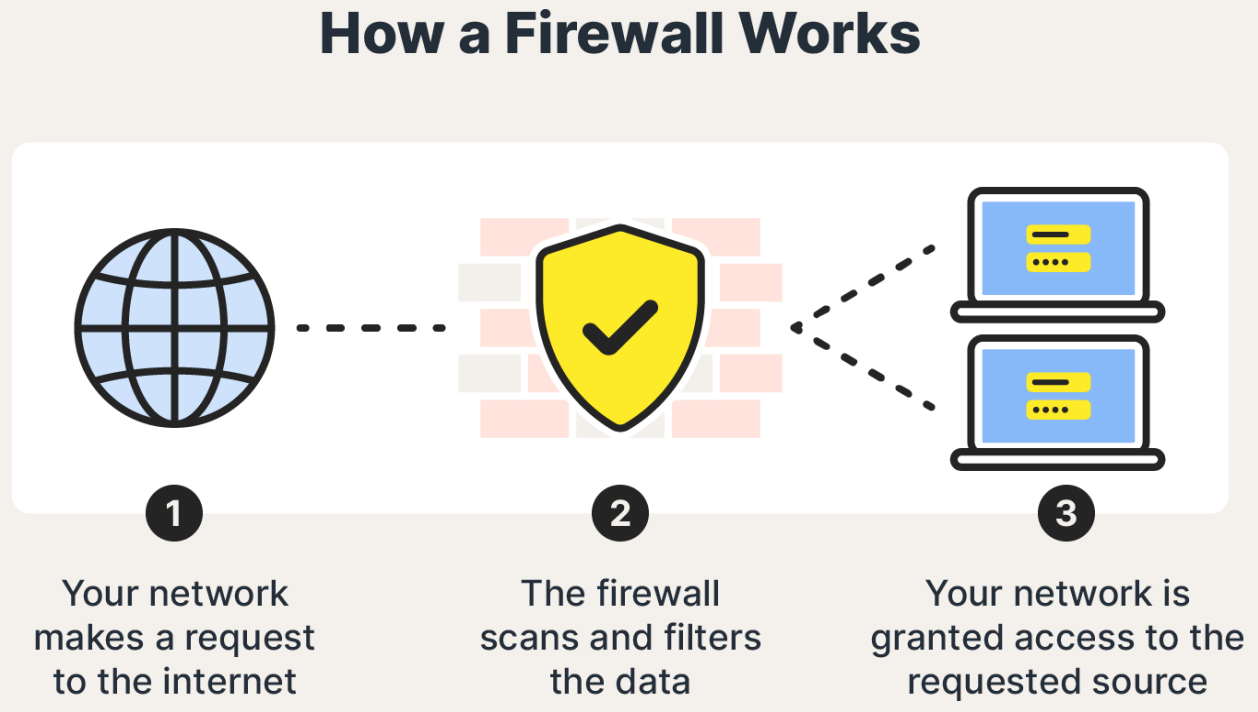
Firewalls

Firewalls are hardware or software to control the type of networking traffic flowing in and out.

E.g: Palo Alto Networks PA Series, Cisco Firepower, Fortinet FortiGate, Check Point Quantum Security Gateways and SonicWall NSa Series

Firewall types
- Router packet filtering
- Application firewall systems
- Stateful inspection
- Next Generation Firewalls
- Web Application Firewall

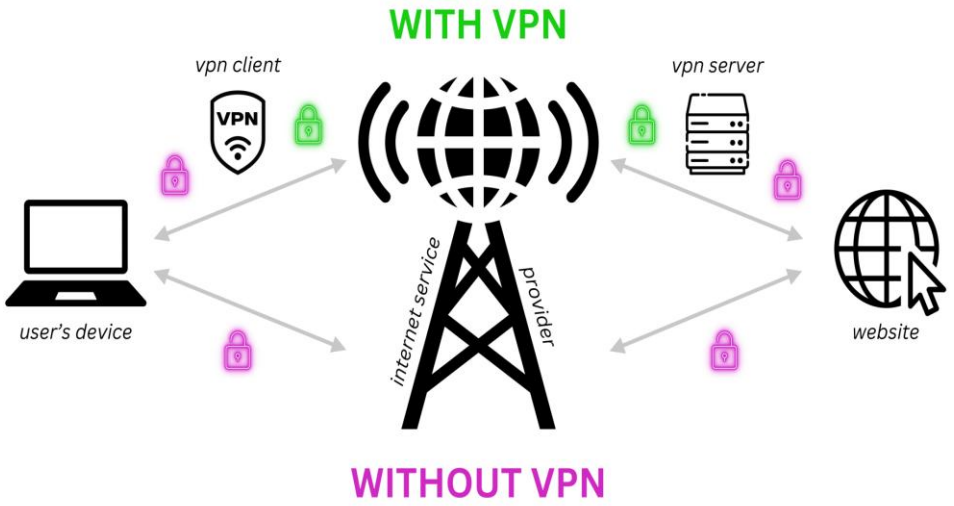
Examples of firewall implementations
- Screened-host firewall
- Dual-homed firewall
- Demilitarized zone (DMZ)



Virtual Private Networks (VPN)

A VPN extends the corporate network securely with encrypted packets sent out via virtual connections over the public Internet to remote offices and workers, salespeople and business partners.

The impact on the business transmitting data through public networks and the accompanying risk are significant.



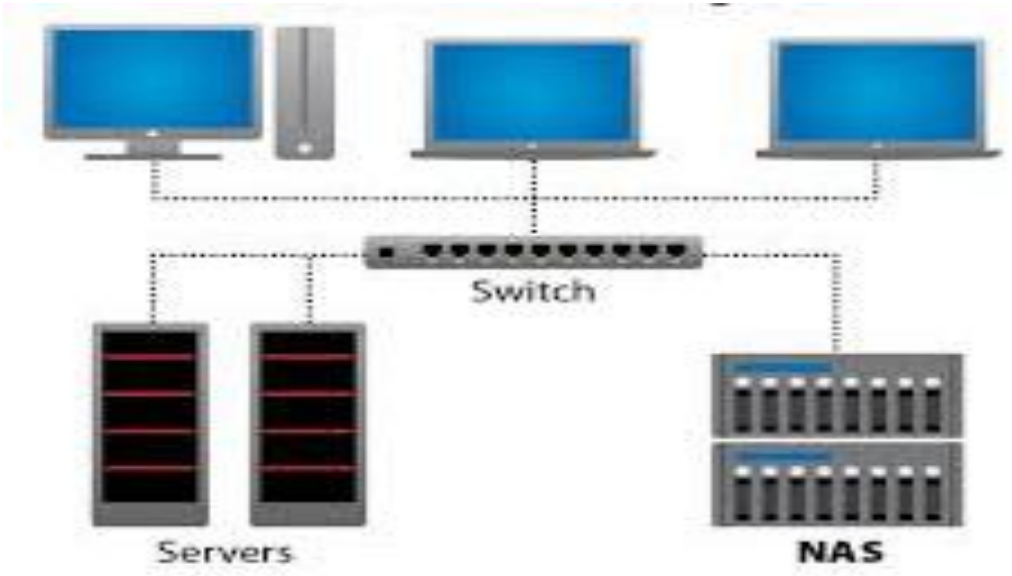
VPN Best Practices

- Establish a VPN policy
- Select a standards-based VPN
- Implement a VPN with strong cryptograph
- Implement strong authentication
- Monitor and log VPN usage

Network Attached Storage (NAS)

NAS consists of a centralized file server that enables multiple users to store and share files over communication networks.
The IS auditor should be aware that NASs are subject to vulnerabilities such as:

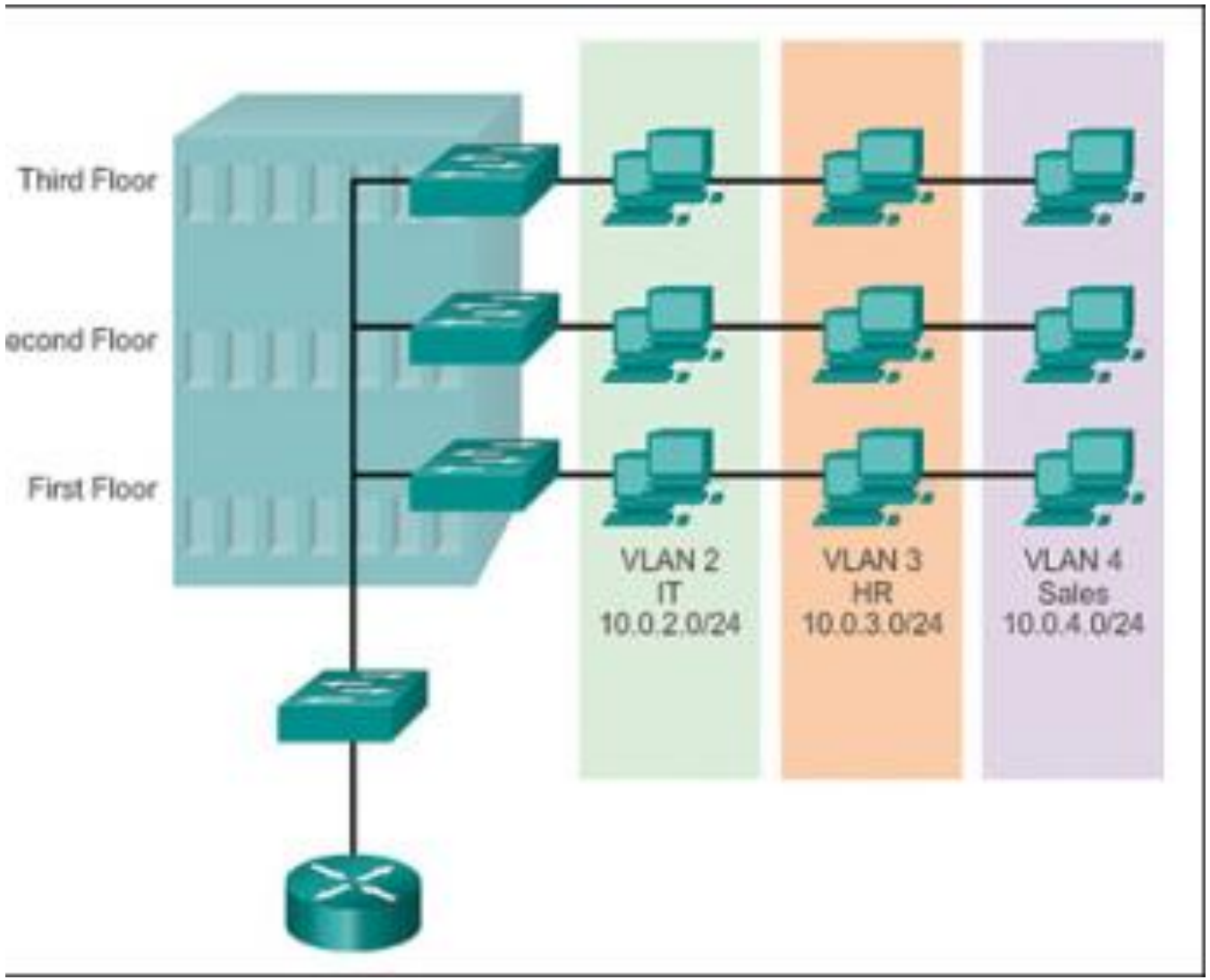
- Unsecure network configurations
- Unsecure passwords
- Insufficient authentication
- Leakage from other network devices
- Exposure to malware
- Command injection



Network Segmentation

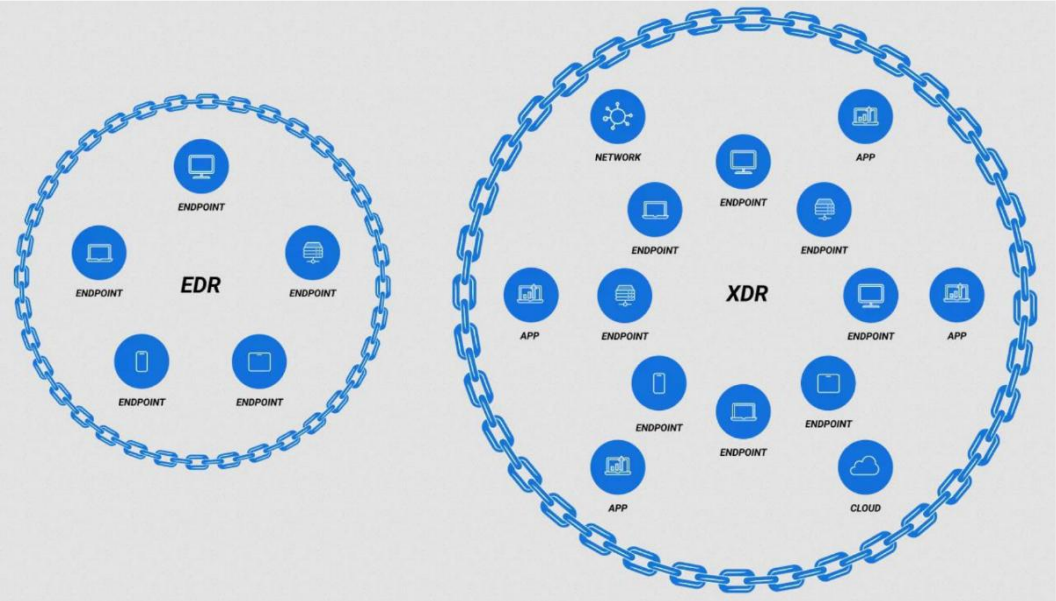
Network segmentation is splitting a network into smaller parts to improve network performance and security.

Sometimes known as network partitioning or network isolation.

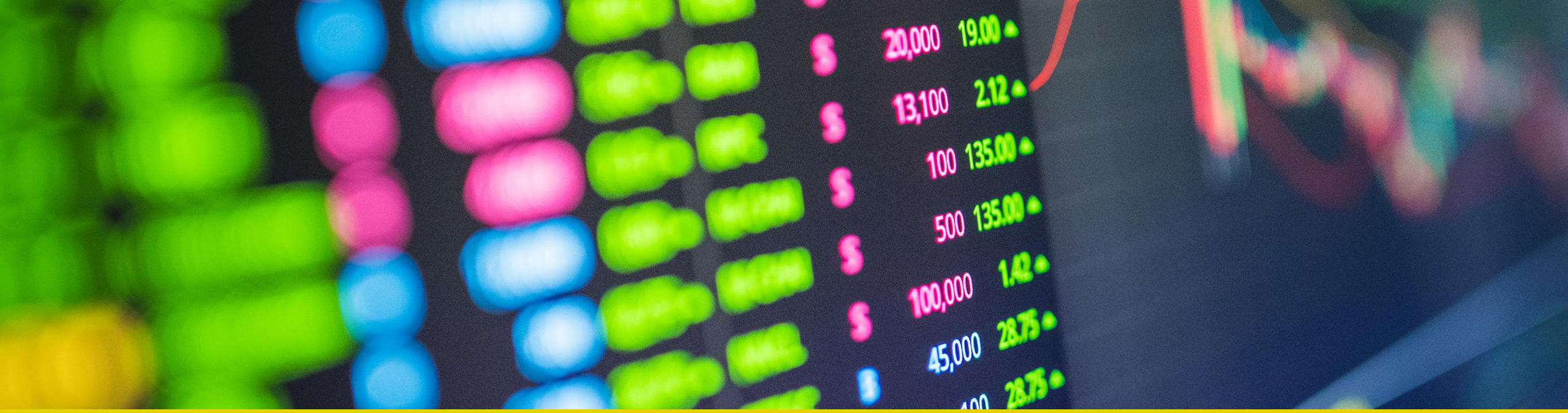


Endpoint Security

An **endpoint** refers to any a device that enables an employee to connect to the organizational network.



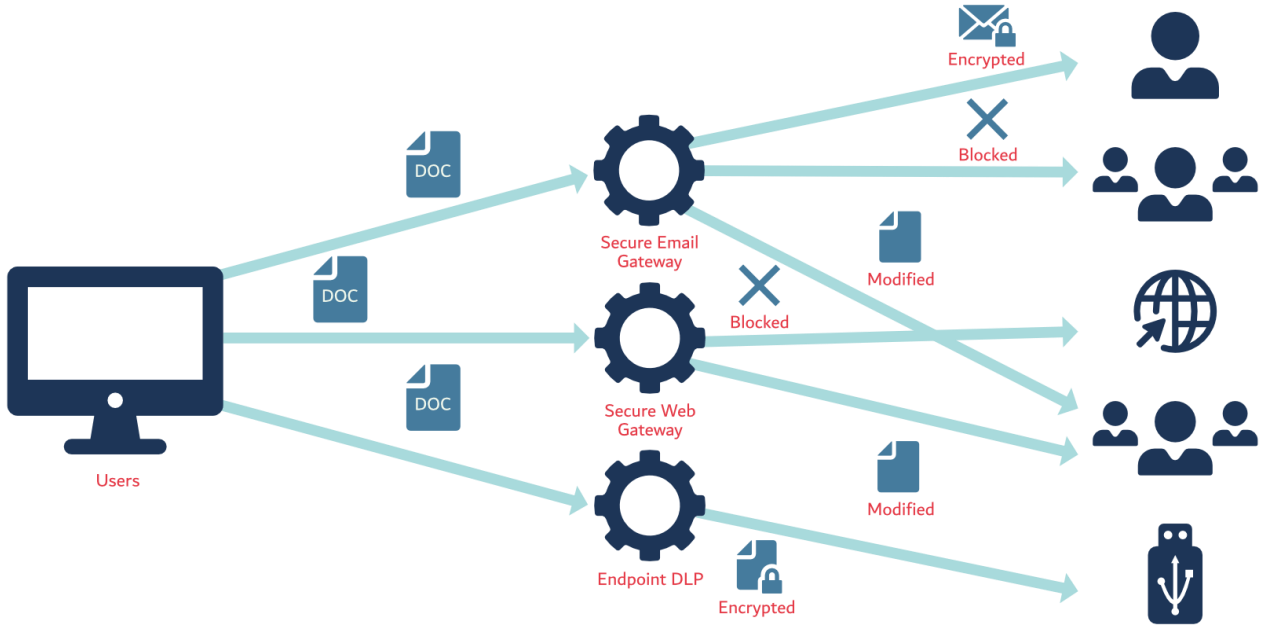
- Endpoint detection and response (EDR) refers to the application of various tools and technologies to continuously monitor the organization's endpoints for the purposes of detecting suspicious behavior and triggering automatic responses
- Extended detection and response (XDR) security takes a broader view of information security than EDR by integrating security across endpoints, cloud computing, email and other solutions.
- XDR provides extended visibility, analysis and response across endpoints, workloads, users and networks.



SECURING THE DATA

Data Loss Prevention

- DLP is a set of tools and processes that are implemented to prevent the loss or misuse of sensitive data or access by unauthorized users, especially those outside the organization.
- Sometimes referred to as data leakage prevention.
- DLP software classifies regulated, confidential and businesscritical data and identifies violations defined by organizations' DLP policies.



DLP Risks

Area of Risk	Causes of Data Loss
Technology	• Loss or theft of devices • Unencrypted data storage • Inheriting data from another system • Software vulnerabilities • Exploitation of vulnerabilities in a database development environment • Exploitation of unnecessary technology installed on the computer • Processing production data in the development environment • Failure to install patches and updates • Unsecure remote access tools • Faults in vendor products (software and/or hardware) • Insecure communication platforms • Inappropriate access rights to applications with sensitive data • Insecure transmission links between the organization and a third party • Poor system programming and/or design
Process	• Poor data governance oversight • Absence of data retention policy • Non-performance of risk assessments • Keeping or transmitting unencrypted data • Not assessing data sensitivity • Not enforcing principle of least privilege (POLP) and need to know • Poor incident response practices • Software setting misconfigurations • Poor data monitoring systems • Failure to close expired accounts
People	• Negligence • Unintentional data transmission • Lack of training and awareness; inadequate awareness • Poor accountability systems • Accidental deletion of files • Leaving sensitive data exposed • Emailing sensitive data without encryption • Sharing work devices • Poor employee supervisory systems • Data theft (selling corporate information) • Exposure of data due to blackmail via social engineering • Printing and copying sensitive data • Insider threats with malicious intent (hacking, fraud, sabotage) mainly due to discontent • Breach of trust among systems developers • Misuse or sharing of passwords • Copying data to remote systems (to support work effort)
Threat actors	• Malware propagation • Software corruption • Sabotage (mainly by malicious insiders)
Natural disasters	• Data loss due to fires, earthquakes and tornados • Liquid spillages • Power outages • High temperatures (overheating) and low humidity levels (overcooling/freezing)

DLP Controls

Area	Control
Governance	• Craft DLP policy, procedures and guidelines. • Classify data and assign sensitivity levels. • Perform data loss risk assessment regularly. • Regularly update data risk profiles to identify new threats. • Standardize the endpoints to make deployment more manageable. • Document all data loss incidents. • Periodically audit the organization for compliance with data protection requirements.
People	• Do not leave sensitive data exposed and unattended. • Prohibit copying sensitive data onto removable media. • Provide read-only access to sensitive information. • Incorporate data protection clauses in employment contracts. • Require data owner authorization prior to data exportation. • Train and develop employees in data protection.
DLP Solution Deployment	• Deploy DLP using a risk-based approach. • Fine-tune DLP policies to the organization's requirements. • Test the DLP implementation. • Encrypt data in transit and at rest.
IT Controls	• Closely monitor all sensitive data channels. • Prohibit unauthorized devices in the network. • Block files containing personal identity information. • Ensure all removable storage devices are configured for read-only. • Implement multilayered authorization and access controls. • Encrypt the data backup containing sensitive information. • Implement firewall and antivirus technologies.
Procurement	• Evaluate the DLP solution to check compatibility with the organization's data formats. • Choose a product that provides real-time reports regarding DLP policy violations.

Data Encryption

Encryption is **locking a message in a box** so only someone with a key can open it.

Encryption is the process of converting a plaintext message into a **secure coded form of text**, called ciphertext, which cannot be understood **without converting** it **back** via decryption (the reverse process) to plaintext.

Encryption generally is used to:

- **Protect data in transit over networks** from unauthorized interception and manipulation
- **Protect information stored on computers** from unauthorized viewing and manipulation
- Deter and detect **alterations** of data
- Verify **authenticity** of a transaction or document

Data Encryption

Key elements of encryption systems include:

- **Encryption algorithm**—A mathematically based function that
- encrypts/decrypts data
- **Encryption key**—A piece of information that is used by the encryption
- algorithm to make the encryption or decryption process unique.
- **Key length**—A predetermined length for the key

Types of encryption schemes:

- **Symmetric** – DES, 3DES, RC4, AES (DES replacement)
  Using one key called secret/private key
- **Asymmetric**– RSA, ECC, Diffie-Hellman
  Using two keys: Private and Public key

FIND THE MESSAGE

D X G L W T

Key = shift +3

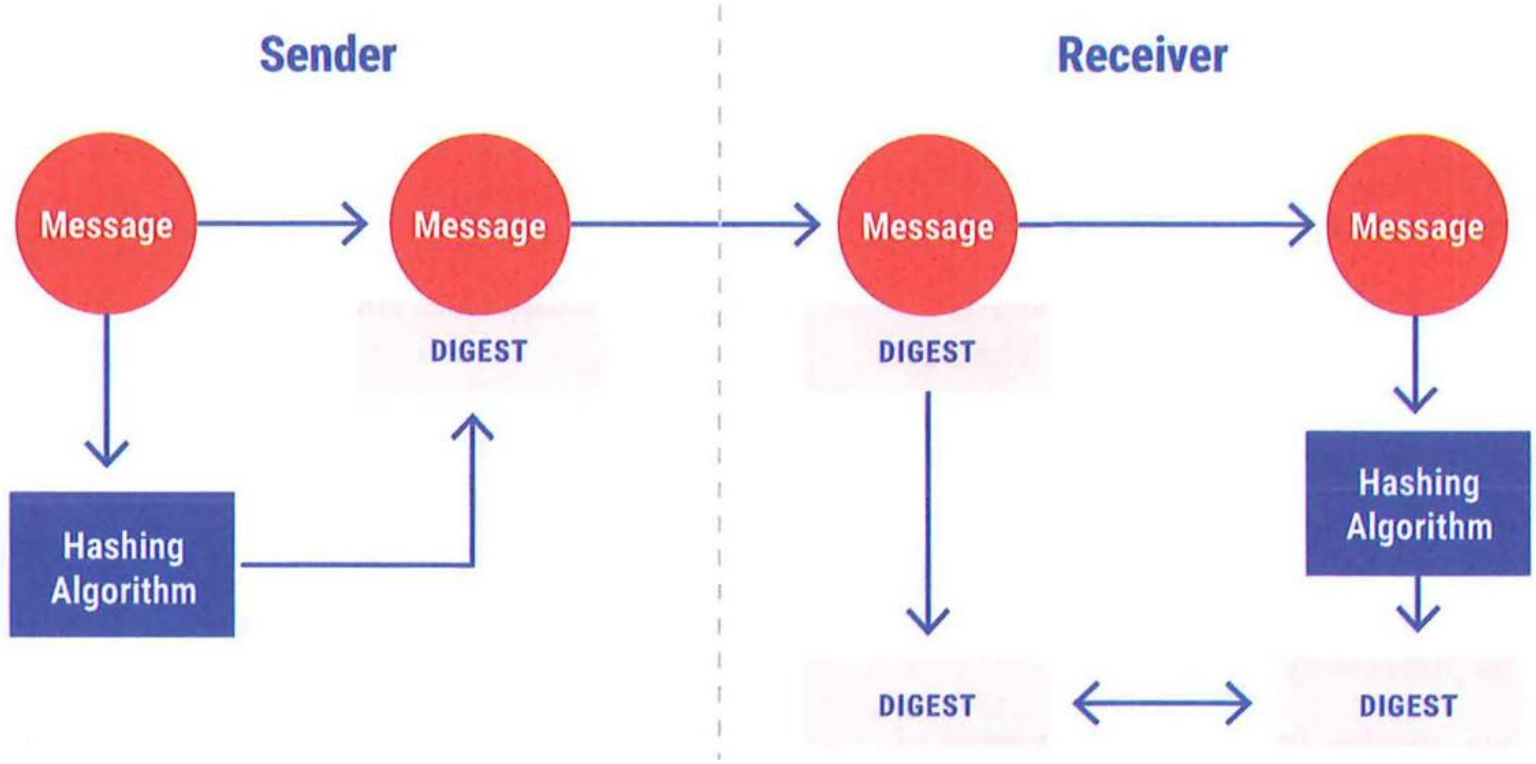
FIND THE MESSAGE

QXVkaXQgU2lzdGVtIEluZm9ybWFzaQ==

64

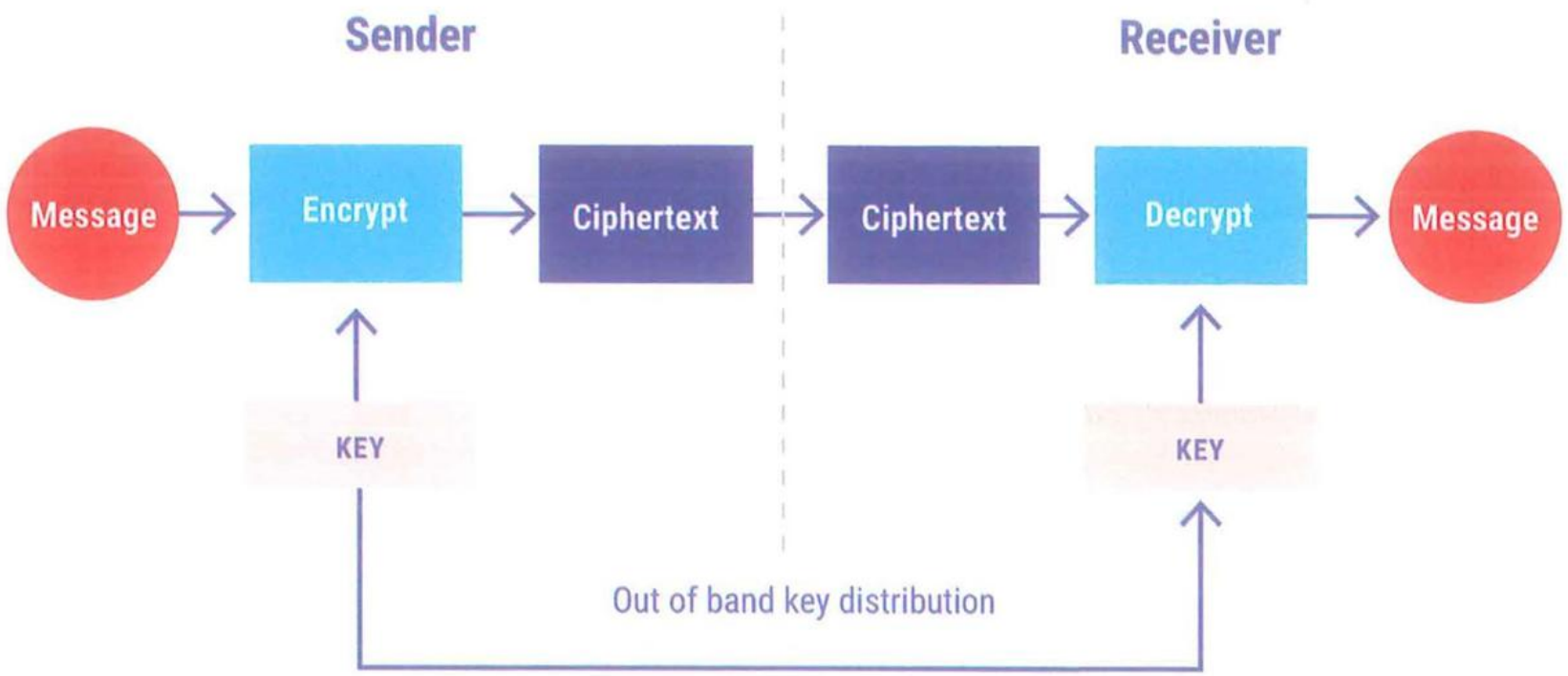
Hash functions

- A fixed length output
- As an integrity check tool – detects changes of even a single bit in a message



Symmetric Key Cryptographic Systems

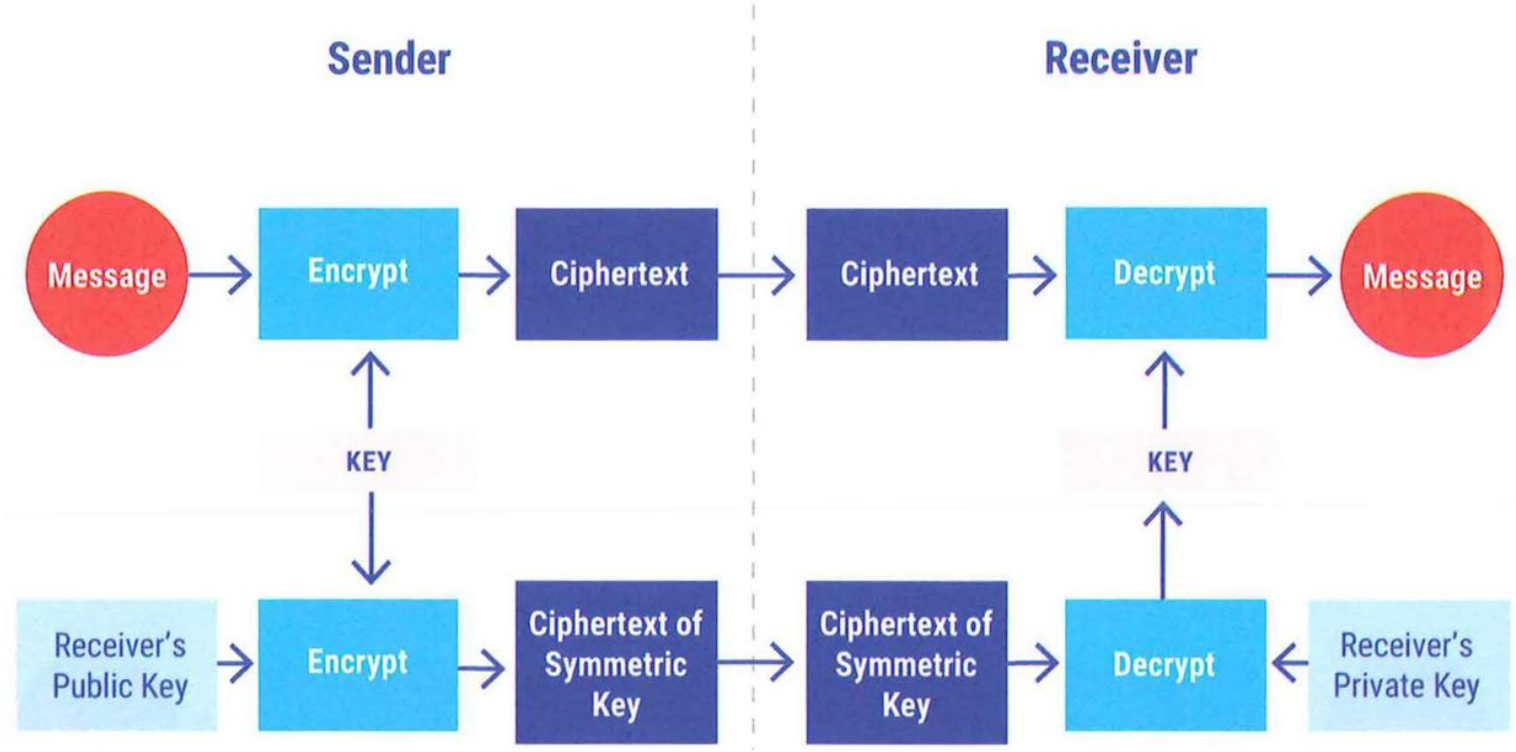
A symmetric encryption uses a secret key to encrypt the plaintext to the ciphertext and the same key to decrypt the ciphertext to the corresponding plaintext



Public (Asymmetric) Key Cryptographic Systems

Asymmetric encryption uses two keys:

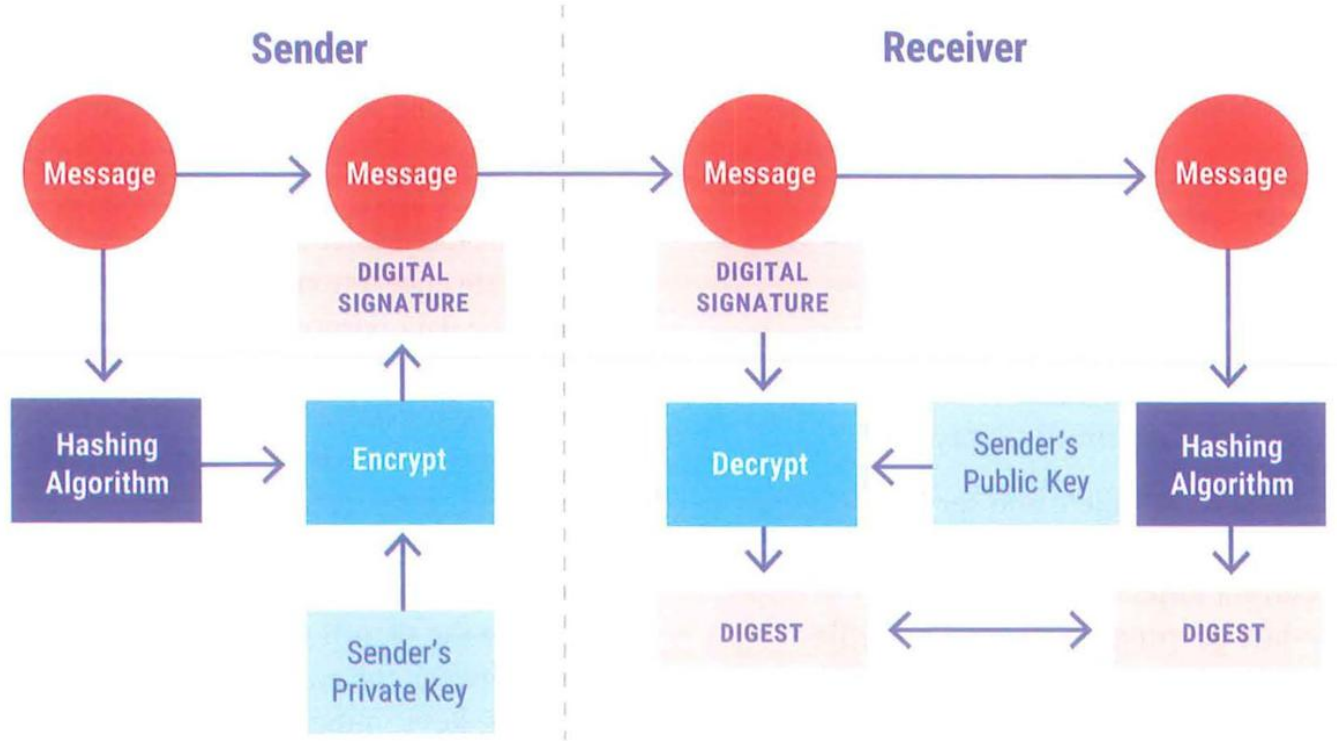
- Private key – kept private
- Public key – publicly open



Digital Signatures

Digital Signatures ensures:

- Data integrity
- Authentication
- Nonrepudiation



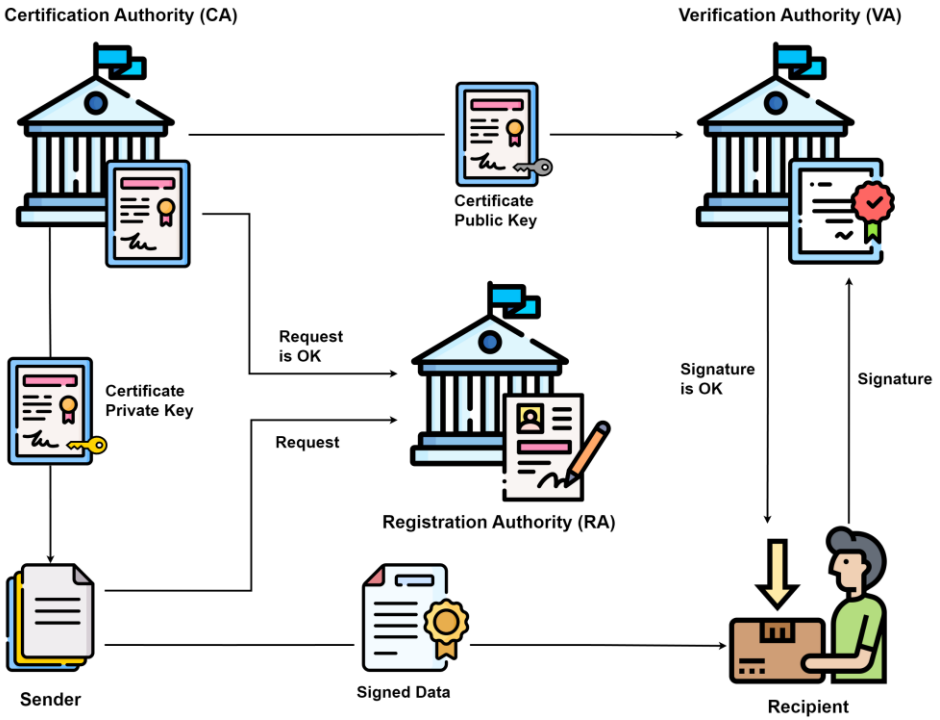
Nonrepudiation as an assurance that **a party cannot successfully deny having performed a specific action or having made a commitment.**

Encryption Audit Procedures

Encryption governance	• Verify that written encryption policies and procedures are in place. • Ascertain the presence of a data classification system. • Determine if encryption risk assessments are regularly carried out. • Verify that there is no duplication of encryption. • Verify that management has instituted controls to support encryption, such as dual control and separation of duties. • Verify that the organization complies with all data protection rules and regulations. • Verify the existence of an audit system associated with encryption.
Encryption design	• Verify that the process and the selection of an encryption algorithm are effective and efficient. • Review documentation from management attesting that the chosen algorithm ensures adequate protection. • Verify that management has implemented processes to ensure minimal effect on interfacing and other systems. • Determine if management has applied respected standards such Transport Layer Security (TLS) as part of its cryptographic system. • Check whether the cryptographic system in place is compatible with the applications. • Verify that the keys contain all the required properties, including the length, composition and management of the key according to policy. • Ascertain the difficulty of key generation and modification.
Key management	• Verify whether changes to the cryptographic system are adequately controlled. • Determine whether changes or updates to the cryptographic system are performed only by authorized individuals. • Verify that the key transmission is controlled according to a specific written procedure. • Determine if the creation, rotation and destruction of keys based on time is in accordance with policy or best industry standards. • Verify that users and operators do not handle keys.
Digital signatures	• Verify that private keys are never backed up, as backing up private keys increases exposure. • Determine whether the organization uses different key pairs for encryption and digital certificates.
Encryption algorithms	• Ascertain if management has considered the need for the complex mathematical equations. • Verify that the cost of deciphering does not exceed the value of the information the encryption system is supposed to protect.

Public Key Infrastructure

- Public key infrastructure (PKI) is a system for distributing public keys through digital certificates.
- A PKI is made up of policies, procedures, hardware, software and personnel required to create, manage, store, distribute and revoke public key certificates.



Certificate Authority (CA)

- Issues and signs certificates
- Establishes trust

Registration Authority (RA)

- Verifies identity before certificate issuance

Digital Certificates

- Bind public key to identity
- Have expiration dates

PKI – Management Practice

Area	Description
Key creation	Also known as key generation, creation is the process of generating keys for use in cryptographic processes through a device or program known as the key generator.
Key distribution	Key distribution is the process of transferring a key to a user or system. This process must be secure, and secure encryption technologies are often used for the purpose.
Key storage and custody	Keys must be stored securely on the computing device. Often, they are stored in a protected storage facility such as the Windows certificate store. Methods such as dual custody, split knowledge and custody generally require two or more people to share access to a key. It is crucial for the IS auditor to be aware that some keys may be placed under key escrow.
Key rotation	Keys are typically not meant to be used forever, as this increases the risk of them getting stolen or lost, or malfunctioning. To mitigate this risk, it is advisable that organizations retire old keys and implement new ones.
Key recovery and backup	Key recovery is a critical element in key management. Losing a private key often leads to losing data if the key is not placed in escrow. Key escrow enables the organization to safely store keys for later recovery. There is also a need to have a backup method in case the key malfunctions. PKIs typically offer inbuilt backup and recovery facilities.
Key destruction	A key can be suspended (placed on temporary hold), revoked (no reinstatement is possible), expired (inactive until renewed) or destroyed. Key destruction often happens at the end of the key lifecycle or after a compromise is detected on the key. The IS auditor should monitor the key destruction process to ensure that it is appropriate and secure.

PKI – Risk

- **Outdated protocols** – makes organization prone to security incidents
- **Weak cryptographic keys** – less than 2048 is vulnerable
- **Infrequent key rotation** – still use old key and never changed
- **Mismanaged certificates** – fail to properly manage, issue, renew or revoke digital certificates
- **Lack of automation** – management become complex and prone to error
- **Insufficient skills and resources** – ineffective management
- **Unclear certificate ownership** – makes certificate hard to manage
- **Lack of policies** – makes inconsistency in policy application
- **Limited visibility** – should be centralized
- **Poor private key management** – can result in private key compromise
- **Compromised root CA** – If the root CA is untrustworthy, the overall PKI cannot be trusted
- **Poor patch management** – makes PKI vulnerabilities increase

PKI- Audit Procedure

Audit Category	Audit Procedures
Certificate authority (CA)	• Determine whether the CA has an information security policy in place. • Evaluate the CA's physical controls. • Verify that the CA performs background checks on its personnel. • Determine whether the CA backs up audit logs. • Inspect how the CA performs key management throughout the entire key management life cycle. • Verify whether the CA systems are appropriately isolated.
Registration authority (RA)	• Verify whether enrollment of RAs is as specified in the CPS. • Verify that the role of the RA is restricted to the submission of details to the CA and no other roles are assigned. • Ascertain whether the RA onboarding and termination procedures are defined. • Determine whether communication channels between the CA and the RA are sufficiently secure for the certificates. • Verify that all activities of the RA are logged. • Verify that RA access to CA systems is based on multifactor authentication (MFA). • Inspect the previous audit reports undertaken on the RA operations and identify issues of noncompliance. • Verify the list of RA violations (if any) and corresponding actions taken by the CA.
Certificate	• Verify that the certificate information is published on the CA's website. • Ascertain whether certificate renewal is per the CPS. • Verify whether certificate suspension and revocation is per the CPS. • Ascertain the availability of a secure certificate distribution system.
Key management	• Check the hardware used to generate keys for Federal Information Processing Standards (FIPS) compliance. • Verify that the keys are distributed using secure mechanisms. • Determine the appropriateness of procedures available to address cases of key compromise. • Verify that the storage of the keys is secure and appropriate. • Verify whether the CA maintains key escrow. • Check on the availability and operation of key backup and archiving procedures. • Ascertain whether procedures for key destruction are appropriate and prevent data remaining.
Certificate policy (CP)	• Verify that the organization has an approved CP in place. • Ascertain whether the CP in place is current. • Determine whether the CP is being followed by all PKI parties, and document identified gaps.
Certificate practice statement (CPS)	• Check whether the CPS complies with applicable laws and regulations. • Verify that the CPS is available to relevant parties. • Ascertain whether responsibilities for maintaining the CPS are appropriately assigned. • Verify that the modification of the CPS follows defined processes and procedures. • Ascertain whether the CPS has a valid object identifier.
Certificate revocation list/ Online Certificate Status Protocol (CRL/OCSP)	• Verify whether the CRL or OCSP is in place. • Determine whether the CRL issued is digitally signed by the CA. • Verify that a secure mechanism for CRL distribution is in place. • Take a sample of CRL entries and verify that the revoked certificate remains on the CRL up to the end of the certificate's validity period. • Determine whether the OCSP response processes and procedures are automated. • Verify that the CRL and OCSP services comply with relevant industry standards and regulations.



SECURING THE DISTRIBUTION

Web-based Communication Technologies

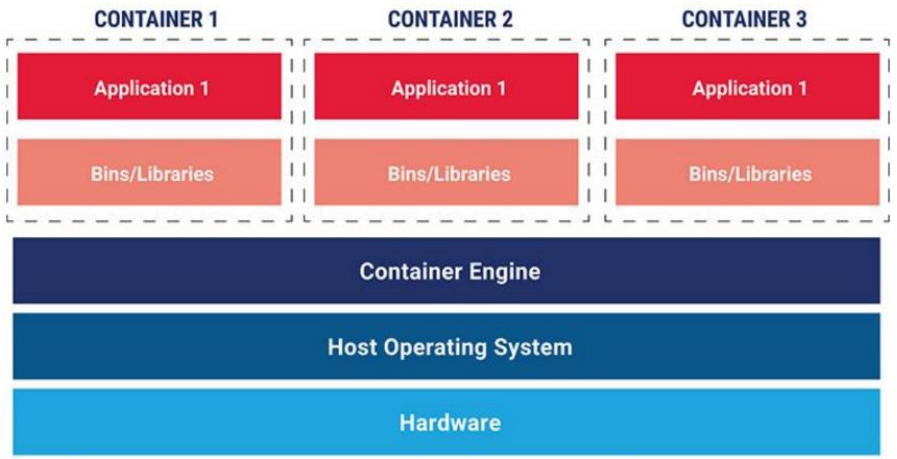
Web-based communication technologies define how data is exchanged between:

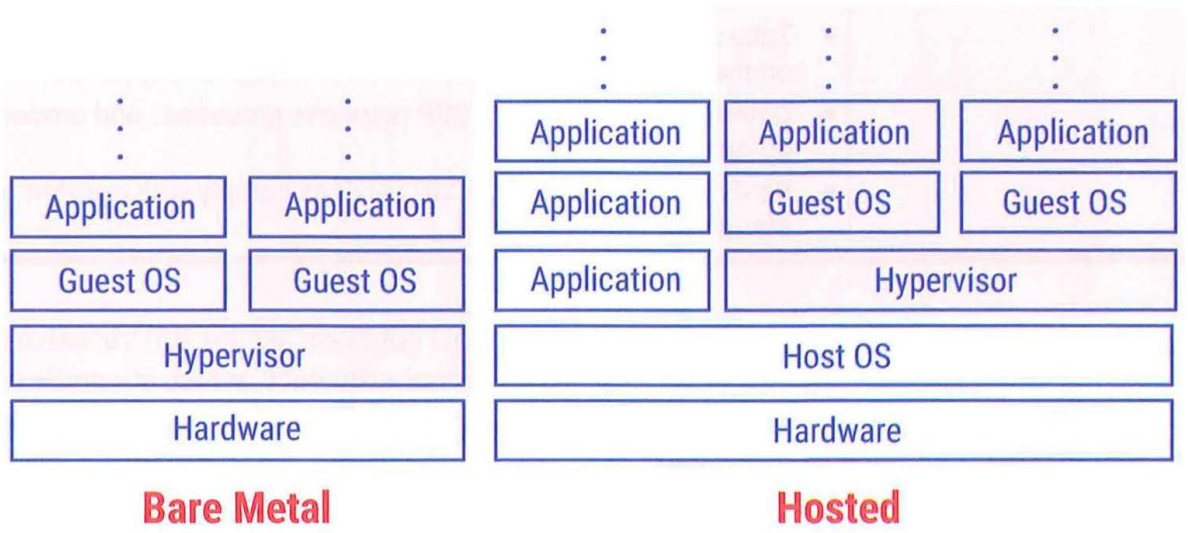
- Users and systems
- Systems and systems
- Internal and external parties

HTTP vs HTTPS (No encryption vs Encryption)
API (Application Program Interface) enables system-to-system communication

Cloud and Virtualized Environments

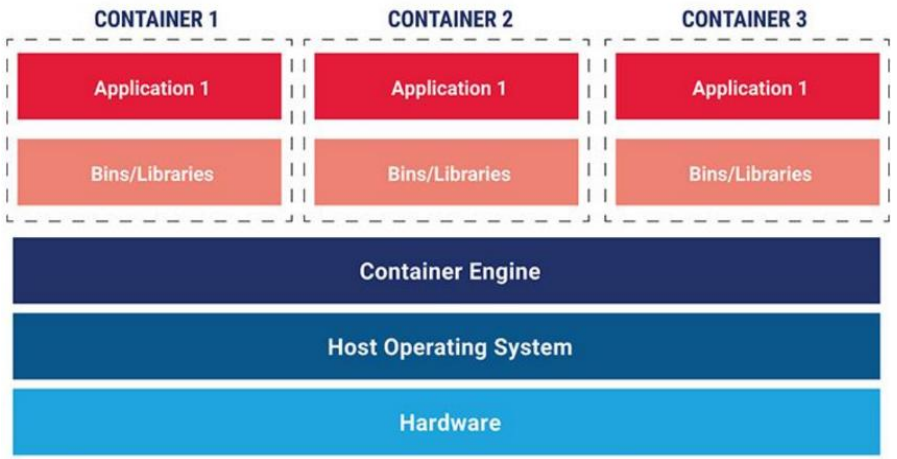
Virtualization is a broad concept and generally refers to the transformation of physical technologies into virtual resources.

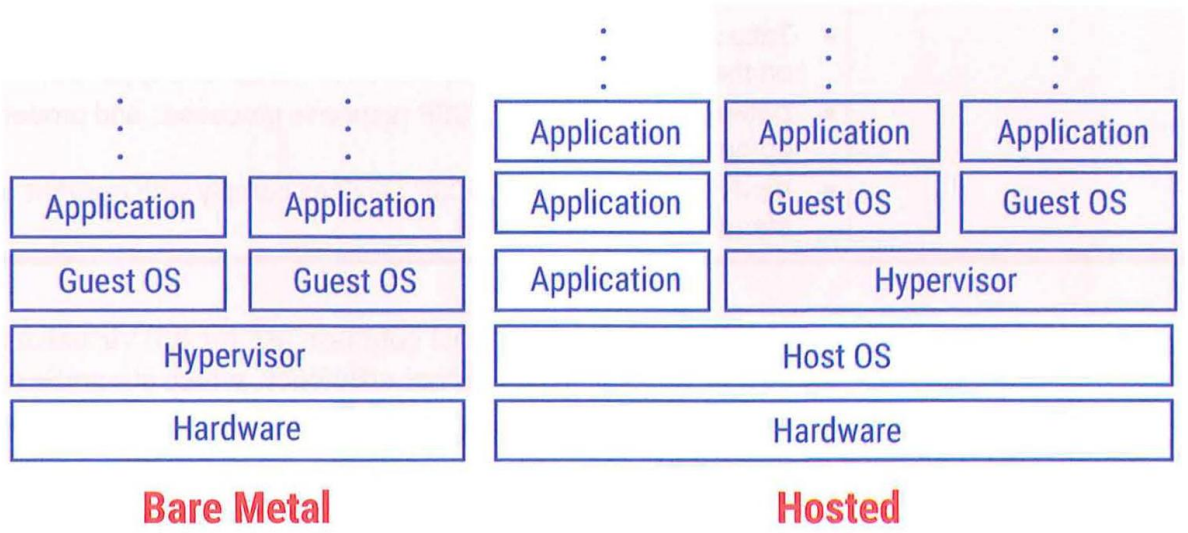




Cloud and Virtualized Environments

Virtualization is a broad concept and generally refers to the transformation of physical technologies into virtual resources.





Cloud and Virtualized Environments- Risk

- Insufficient identity, credentials, access and key management
- Insecure interfaces and APIs
- Misconfiguration and inadequate change control
- Lack of cloud security architecture and strategy
- Insecure software development
- Unsecured third-party resources
- System vulnerabilities
- Accidental cloud data disclosure
- Misconfiguration and exploitation of serverless and container workloads
- Organized crime, hackers and APTs
- Cloud storage data exfiltration

Mobile, Wireless and Internet of Things Devices

- Portable and wireless devices present a **ubiquitous** threat to an enterprise's information assets and must be properly controlled.
- **Policies, procedures and additional protection** mechanisms must be put into place to ensure that data is protected.
- Mobile computing refers to devices that are **transported** or **moved** during normal use.
- Common mobile devices include **tablets**, **smartphones**, **laptops**, **USB storage devices**, **digital cameras** and similar technologies.

Mobile, Wireless and IoT Devices

Vulnerability	Threat	Risk
Information travels across wireless networks that are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, enterprise reputation, adherence to regulation or legal action
Mobility provides users with the opportunity to leave enterprise boundaries and thereby eliminates many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware that it can bring into the enterprise network.	Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data
Bluetooth technology is very convenient for many users to have hands-free conversations, but it is often left on and then is discoverable.	Hackers can discover the device and launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information
Unencrypted information is stored on the device.	In the event that a malicious outsider intercepts data in transit or steals a device or if an employee loses the device, the data is readable and usable.	Exposure of sensitive data, resulting in damage to the enterprise, customers or employees
Lost data may affect employee productivity.	Mobile devices may be lost or stolen due to their portability. Data on mobile devices is not always backed up.	Workers dependent on mobile devices being unable to work due to broken, lost or stolen devices and data not backed up
The device has no authentication requirements applied.	In the event that the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the enterprise and liability and regulation issues
The enterprise is not managing the device.	If no mobile device strategy exists, employees may choose to bring in their own unsecured devices.	Data leakage, malware propagation or unknown data loss in the case of device loss or theft
The device allows for installation of unsigned third-party applications.	Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.	Malware propagation, data leakage or intrusion on the enterprise network

Bring Your Own Device

BYOD is a policy that allows employees to bring their own personal mobile devices to work and use them to **connect** to the organization's **network**, to **business resources** and/or the **Internet**.

Some specific BYOD-related risk is:

- **Access controls** and **controls over device** security
- Ability to eliminate **sensitive enterprise data** on termination of employment or loss of the device
- **Management issues** related to supporting many different types of devices, OSs and applications
- Ensuring that employee-owned BYOD devices are **properly backed up** at all time

Audit Procedures for Mobile Device

Audit Area	Audit Procedures
Governance	• Verify that a security policy exists for mobile devices. • Verify that mobile devices have protective features enabled. • Verify that the policy prohibits users to carry mobile devices to sensitive areas. • Ascertain whether mobile devices have been subjected to risk assessments and periodic audits.
Patch management	• Ascertain whether device software is up to date. • Verify whether mobile antivirus software is up to date. • Verify that all mobile applications are up to date. • Verify procedures for testing and approving patches and determine whether they are secure.
Configuration and change management	• Determine whether mobile device gateways are running the latest approved software. • Verify that Bluetooth functionality is disabled when not in use. • Determine whether mobile operating systems (OSs) are appropriately patched. • Evaluate whether effective change management processes exist for mobile devices.
Device management	• Verify that the mobile device is not connected to unknown removal media. • Determine the effectiveness of device security controls around data protection. • Verify that there are no unmanaged devices on the network. • Verify whether remote wiping/locking on mobile devices is enabled. • Evaluate controls in place for life cycle device management for both organization-owned mobile devices and BYOD. • Verify that cameras are always covered when not in use. • Verify that location services are disabled when not required.
Bring Your Own Device (BYOD)	• Verify whether a BYOD policy is in place. • Evaluate controls in place to manage personally owned mobile devices. • Verify that BYOD procedures are in place for installing applications.
Security monitoring	• Determine whether an asset management process is in place for monitoring and tracking of mobile devices. • Evaluate whether security monitoring systems, including log reviews, are in place. • Verify whether there are rules for downloading software onto mobile devices. • Determine whether mobile devices are subject to a centralized mobile device management (MDM) system.
Disaster recovery/business continuity (DR/BC)	• Evaluate DR/BC processes to restore mobile devices and continue operations in case of disaster. • Verify that the DR/BC plan for mobile devices is tested regularly.
Awareness training	• Determine whether an awareness program on securing mobile devices is in place. • Verify that the training programs on mobile device security are in place. • Specify the types of information that can be stored on mobile devices. • Evaluate whether the training educates users not to open unknown links and attachments.
Encryption	• Verify whether sensitive data is properly secured while at rest and in transit. • Verify that mobile device users connect to the organization using secure channels such as Transport Layer Security (TLS), virtual private network (VPN), etc.

Information Security in Real Life

Not all cyber security risks come from malware, viruses, or software vulnerabilities. One of the most grievous risks is a bit more obvious.

Keeping passwords on post-it notes or in notepad files might be one of the most easy to recognize vulnerabilities.



NO HOMEWORK!

HAPPY HOLIDAY!