THE 3 TYPES OF SECURITY CONTROLS (EXPERT EXPLAINS)

TYPES OF SECURITY CONTROLS

	CONTROL FUNCTIONS		
	PREVENTATIVE	DETECTIVE	CORRECTIVE
PHYSICAL CONTROLS	• Fences • Gates • Locks	• CCTV • Surveillance Cameras	• Repair physical damage • Re-issue access cards
TECHNICAL CONTROLS	• Firewall • IPS • MFA • Antivirus	• IDS • Honeypots	• Vulnerability patching • Reboot a system • Quarantine a virus
ADMINISTRATIVE CONTROLS	• Hiring & termination policies • Separation of duties • Data classification	• Review access rights • Audit logs and unauthorized changes	• Implement a business continuity plan • Have an incident response plan

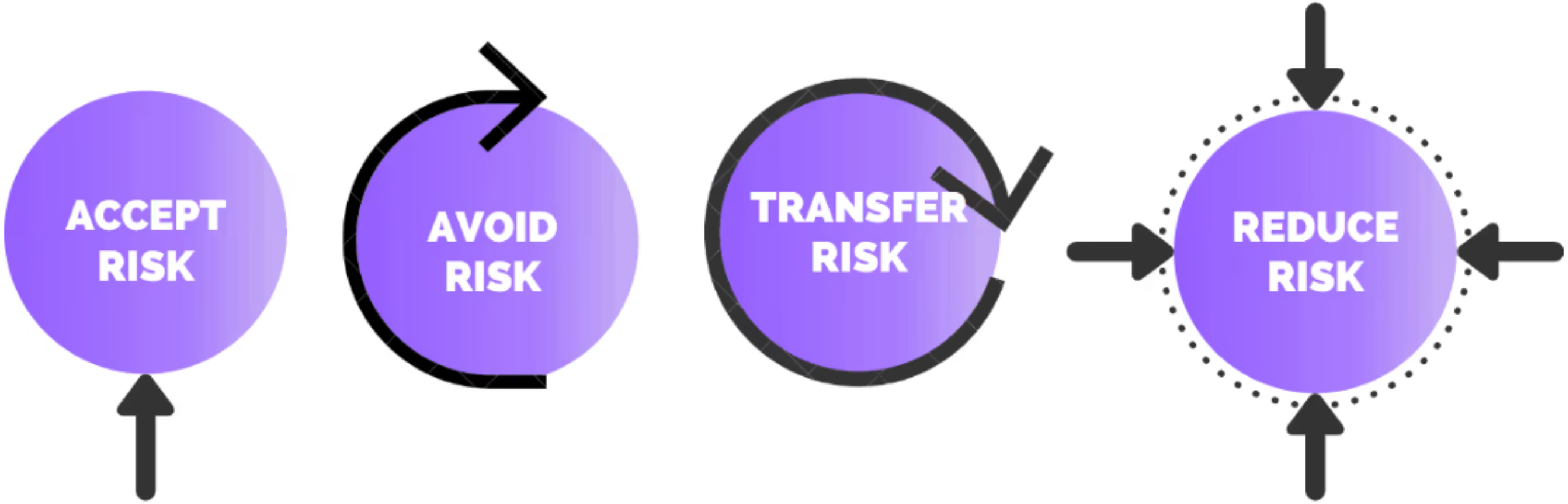
Contents

TECHNICAL CONTROLS
ADMINISTRATIVE CONTROLS
PHYSICAL CONTROLS

WHAT IS A SECURITY CONTROL?

Security Controls Explained

- Security controls are countermeasures or safeguards used to **reduce the chances that a threat will exploit a vulnerability**.
- For example, implementing company-wide security awareness training to **minimize the risk of a social engineering attack** on your network, people, and information systems.



The act of reducing risk is also called **risk mitigation**.

Mitigating Risk

- While it's next to **impossible to prevent all threats**, mitigation seeks to decrease the risk by reducing the chances that a threat will exploit a vulnerability.
- Risk mitigation is achieved by **implementing different types of security controls** depending on:

   1. The goal of the countermeasure or safeguard.
   2. The level to which the risk needs to be minimized.
   3. The severity of damage the threat can inflict.

WHAT ARE THE GOALS OF SECURITY CONTROLS?

Security Control Goals

- The overall purpose of implementing security controls as previously mentioned is to help **reduce risks in an organization**.
- In other words, the primary goal of implementing security controls is to **prevent or reduce the impact of a security incident**.
- The effective implementation of a security control is based on its classification in relation to the **security incident**.

Security Control Goals

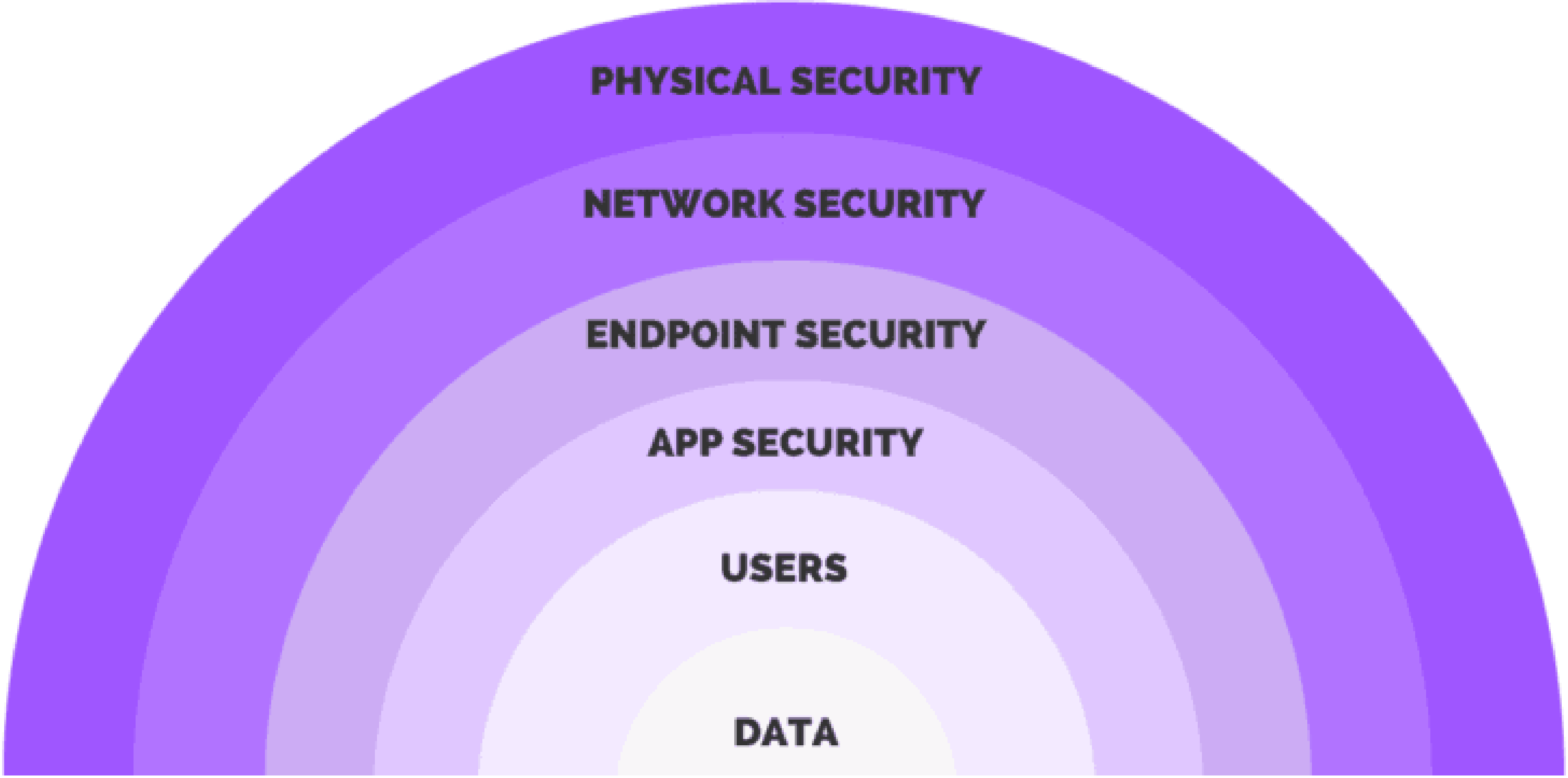
- The common classifications types are listed below along with their corresponding description:

    1. Preventive controls attempt to prevent an incident from occurring.
    2. Detective controls attempt to detect incidents after they have occurred.
    3. Corrective controls attempt to reverse the impact of an incident.
    4. Deterrent controls attempt to discourage individuals from causing an incident.
    5. Compensating controls are alternative controls used when a primary control is not feasible.

- An organization that places a high priority on reducing risk usually has a risk profile, which illustrates the potential cost of a negatively impacting risk and the human resources required to implement the control(s).

Layering Security Controls

- Layering is an approach that combines multiple security controls to develop what's called a **defense-in-depth strategy**.
- Defense-in-depth is a common strategy used in cyber security whereby **multiple layers of controls are implemented**.



PHYSICAL SECURITY

NETWORK SECURITY

ENDPOINT SECURITY

APP SECURITY

USERS

DATA

UNDERSTANDING THE BASICS OF RISKS & THREATS

Risks

- Risks in cyber security are the **likelihood that a threat will exploit a vulnerability** resulting in a loss.
- Losses could be information, financial, damage to reputation, and even **harm customer trust**.

Threats

- Threats are any event with the potential to compromise the **confidentiality**, **integrity**, and **availability** (CIA) of information.
- Threats come from outside an organization and from anywhere in the world **connected to the internet**.
- Insiders such as a **disgruntled employee** with too much access, or a **malicious insider** also pose a threat to businesses.
- For example, an employee clicking on a phishing email that installs malware **does not mean the employee intended to cause harm**.
- Finally, threats may also take the form of a **natural disaster** or be a manmade risk such as a **new malware variant**.

Vulnerabilities

- Vulnerabilities are a weakness or flaw in the software, hardware, or organizational processes, which when compromised by a threat, can result in a security incident.

Security Incidents

- Security incidents are an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- Now that we have a better understanding of basic risk concepts let's explore how security controls are implemented.

TECHNICAL SECURITY CONTROLS

Technical Controls

- At the most basic level, technical controls, also known as logic controls, use technology to reduce vulnerabilities in hardware and software. Automated software tools are installed and configured to protect these assets.
- Examples of technical controls include:
    - **Encryption**
    - **Anti-Virus And Anti-Malware Software**
    - **Firewalls**
    - **Security Information And Event Management (SIEM)**
    - **Intrusion Detection Systems (IDS)**
    - **Intrusion Prevention Systems (IPS)**

Implementing Technical Controls

- **Below are two common examples of technical control types**:
  - **Access Control Lists (ACL)** – Network traffic filters that can control incoming or outgoing traffic. ACLs are common in routers or firewalls, but they can also be configured in any device that runs in the network, from hosts, network devices, and servers.
  - **Configuration Rules** – Instructional codes that guide the execution of the system when information is passing through it. Network equipment vendors have proprietary configuration rules that manage the operation of their ACL objects.

ADMINISTRATIVE SECURITY CONTROLS

Administrative Controls

- Administrative security controls refer to **policies**, **procedures**, or **guidelines** that define personnel or business practices in accordance with the organization’s security goals.
- During the onboarding process, you may be instructed to **review and acknowledge the security policy** of the organization.
- By acknowledging that you have read the policies of the organization as a new hire, **you are then accountable to adhere to the corporate policy** of the organization.

Implementing Administrative Controls

- In order to implement the administrative controls, additional security controls are necessary for continuous monitoring and enforcement.
- The processes that monitor and enforce the administrative controls are:
  - **Management controls**: The security controls that focus on the management of risk and the management of information system security.
  - **Operational controls**: The security controls that are primarily implemented and executed by people (as opposed to systems).

MGMT & Operational Controls

- For example, a security policy is a management control, but its security requirements are implemented by people (operational controls) and systems (technical controls).
- **The security control to monitor and enforce** could be in the form of a web content filter, which can enforce the policy and log simultaneously.
- The remediation of a phishing attack is another example that **employs a combination of management and operation controls**.
- Security controls to help thwart phishing, besides the management control of the acceptable use policy itself, include operational controls, such as **training users not to fall for phishing scams**, and technical controls that **monitor emails and web site usage** for signs of phishing activity.

PHYSICAL
SECURITY CONTROLS

Physical Controls

- Physical controls are the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material.
- Examples of physical controls are:
  - **Closed-circuit surveillance cameras**
  - **Motion or thermal alarm systems**
  - **Security guards**
  - **Picture IDs**
  - **Locked and dead-bolted steel doors**
  - **Biometrics (includes fingerprint, voice, face, iris, handwriting, etc.)**

PREVENTATIVE CONTROLS

Preventative Controls

- Examples of preventative controls include:
  - **Hardening** - The process of reducing security exposure and tightening security controls.
  - **Security Awareness Training** - The process of providing formal cybersecurity education to your workforce about a variety of information security threats and your company's policies and procedures for addressing them.
  - **Security Guards** - A person employed by a public or private party to protect an organization's assets. Security guards are frequently positioned as the first line of defense for businesses against external threats, intrusion and vulnerabilities to the property and its dwellers.

Preventative Controls

- **Change Management** - The methods and manners in which a company describes and implements change within both its internal and external processes. This includes preparing and supporting employees, establishing the necessary steps for change, and monitoring pre- and post-change activities to ensure successful implementation.
- **Account Disablement Policy** - A policy that defines what to do with user access accounts for employees who leave voluntarily, immediate terminations, or on a leave of absence.

DETECTIVE CONTROLS

Detective Controls

- Examples of detective controls include:
  - **Log Monitoring** - Log monitoring is a diagnostic method used to analyze real-time events or stored data to ensure application availability and to access the impact of the change in state of an application's performance.
  - **SIEM** - Security Information and Event Management (SIEM) is a set of tools and services offering a holistic view of an organization's information security by of operational logs from various systems.
  - **Trend Analysis** - The practice of gathering information and attempting to identify a pattern in the information gathered from an application's log output. The output of the trend analysis is usually in a graph or table form.

Detective Controls

- **Security Audit** - A measurement that focuses on cyber security standards, guidelines, and procedures; as well as the implementation of these controls. The security audit is usually conducted by trained 3rd party entities, or by internal resources in preparation for an external audit.
- **Video Surveillance** - A system that is capable of capturing digital images and videos that can be compressed, stored or sent over communication networks for onsite or remote monitoring.
- **Motion Detection** - A device that utilizes a sensor to detect nearby motion. Such a device is often integrated as a component of a surveillance system that automatically performs a task or alerts a monitoring analyst of detected movement.

CORRECTIVE CONTROLS

Corrective Controls

- Examples of detective controls include:
  - **Intrusion Prevention System (IPS)** - A network security technology that monitors network traffic to detect anomalies in traffic flow. IPS security systems intercept network traffic and can quickly prevent malicious activity by dropping packets or resetting connections.
  - **Backups And System Recovery** - A network security technology that monitors network traffic to detect anomalies in traffic flow. IPS security systems intercept network traffic and can quickly prevent malicious activity by dropping packets or resetting connections.

DETERRENT CONTROLS

Deterrent Controls

- Deterrent controls reduce the likelihood of a deliberate attack and is usually in the form of a tangible object or person.
- Example of deterrent controls include:
  - **Cable Locks**
  - **Hardware Locks**
  - **Video surveillance & guards**

DIFFERENCE BETWEEN PREVENTATIVE AND DETECTIVE CONTROLS

Preventative VS Detective Controls

- **A preventive control** is designed to be implemented prior to a threat event and reduce and/or avoid the likelihood and potential impact of a successful threat event.
- **A detective control** is designed to detect errors and locate attacks against information systems that have already occurred.
- The routine analysis of the detective control output provides input to further enhance the preventative control.
- The goal of continuous analysis is to **prevent errors and irregularities** from occurring in the first place.

COMPENSATING CONTROLS

Compensating Controls

- An alternative method that is put in place to satisfy the requirement for a security measure that cannot be readily implemented due to financial, infrastructure, or simply impractical to implement at the present time.
- The compensating control should meet the following criteria:
    - **Meet the intent of the original control requirement**
    - **Provide a similar level of assurance**

Compensating Controls

- Examples of compensating controls include:
  - **Time-based One Time-Password (TOTP)** – A temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors. Providing a new hire with a TOTP until authentication is fully delivered is an example of a compensating control.
  - **Encryption** – Database security applications, e-mail encryption and other tools. An organization cannot encrypt all electronic data in a PCI assessment. To compensate, they may use other existing tools to implement encryption.

PERFORMING A SECURITY CONTROL ASSESSMENT

Security Control Assessment

- A Security Control Assessment is a **critical component** to measure the state and performance of an organization's security controls.
- The testing and/or evaluation of the **management**, **operational**, and **technical security controls** in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Testing of security controls is also a critical component of the overall governance of an organization's **Information Security Management System**.

Security Control Assessment

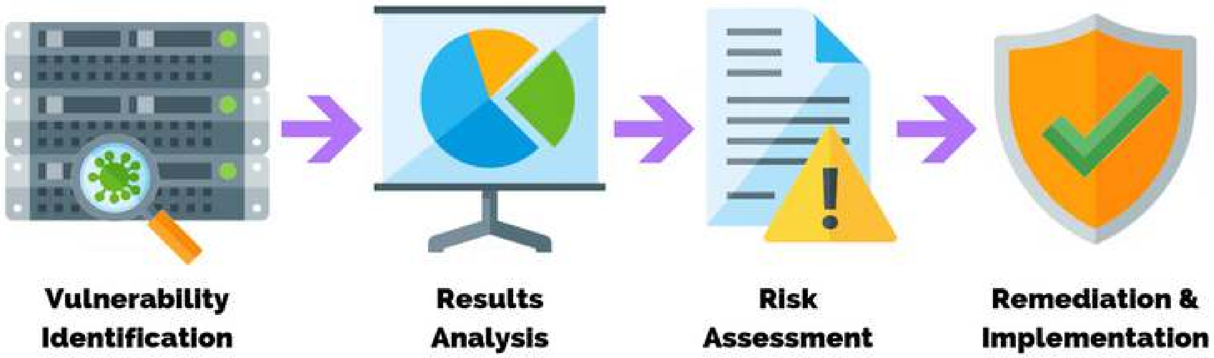
- Depending upon the organization type, regulatory requirements **mandate consistent and continuous assessments**, whereas, non-public organizations are not held to regulatory requirements.
- Today, it is not only best practice to monitor security controls, but **a necessary requirement in order to keep systems secure** and free from target practice of hackers, looking to penetrate any network that has weak security at the perimeter and internally.
- Examples of security assessments include:
    - **Risk Assessments**
    - **Vulnerability Assessment**
    - **Penetration Testing**

Risk Assessments

- A risk assessment involves many steps and forms the backbone of your overall risk management plan.
- Risk assessments are important because they are used to identify assets or areas that present the **highest risk**, **vulnerability**, or **exposure** to the enterprise.
- It then identifies the risks that could affect those assets.

Vulnerability Assessments

- A vulnerability assessment refers to the process of identifying risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem.
- Vulnerability assessments are a critical component of the vulnerability management and IT risk management lifecycles, helping protect systems and data from unauthorized access and data breaches.
- Vulnerability assessments typically leverage tools like vulnerability scanners to identify threats and flaws within an organization's IT infrastructure that represents potential vulnerabilities or risk exposures.



Vulnerability Identification

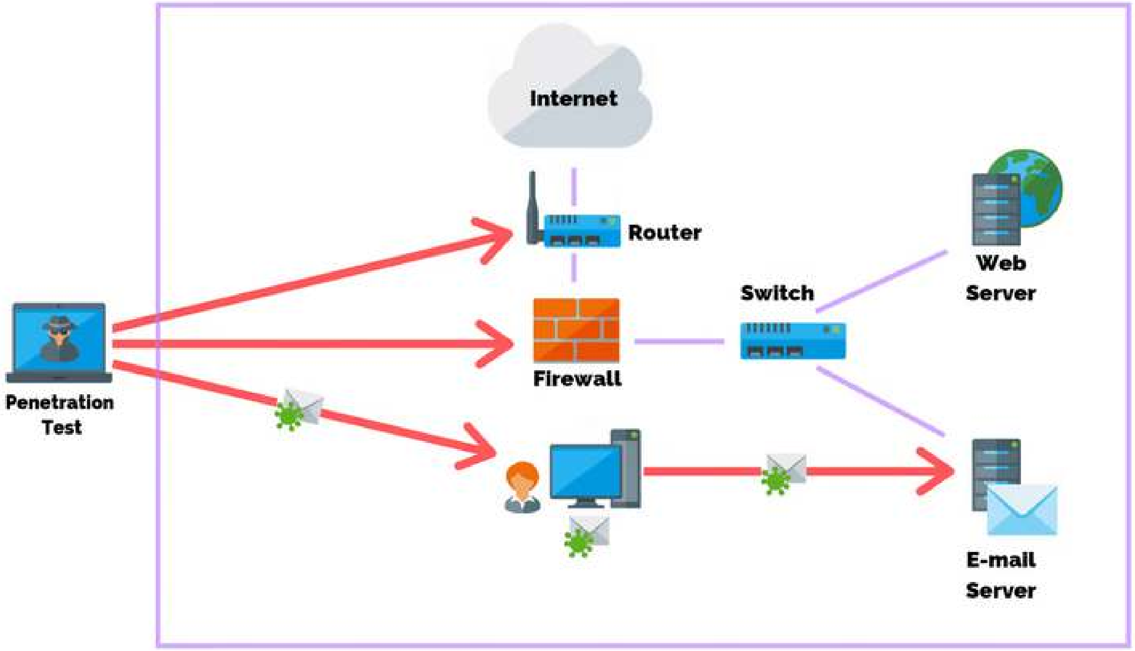
Results Analysis

Risk Assessment

Remediation & Implementation

Penetration Testing

- Penetration testing is a method for testing a web application, network, or computer system to **identify security vulnerabilities that could be exploited**.
- The primary objective for security as a whole is to **prevent unauthorized parties from accessing**, **changing**, or **exploiting** a network or system.
- It aims to do what a bad actor would do.



Penetration Testing

- The main reason penetration tests are crucial to an organization's security is that they help personnel learn **how to handle any type of break-in from a malicious entity**.
- Pen tests serve as a way to **examine** whether an organization's **security policies are genuinely effective**.
- They serve as a type of fire drill for organizations.
- Penetration tests can also provide solutions that will help organizations to not only prevent and detect attackers but also to **expel such an intruder from their system in an efficient way**.

CONCLUSION

Conclusion

- In this article, we have examined the three basic security controls – **technical**, **administrative**, and **physical**.
- A review of various critical sub controls was also reviewed – **deterrent**, **corrective**, and **compensating**.
- Although it is important for security professionals to understand the definition of the controls, they must also recognize that **the ultimate goal of implementing the controls is to strengthen their organization's defenses** in order to reduce risk.
- Information security must be treated as a program that **requires continuous monitoring in order to defend and protect** its most valuable assets.
- Remain vigilant by incorporating the controls listed in this article, and **you will be equipped to support and contribute to the success of your organization's risk management program**.