Security Management

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

- **Penetration Tests:** Penetration tests (also known as pen tests) are designed to identify exploitable vulnerabilities in a company's computer network. After conducting a pen test, the testers report their findings to the company's security manager so solutions and patches can be developed.
- **Vulnerability Management:** Network vulnerabilities allow threats such as spyware and malware to gain entry into a company's network. The more applications a company deploys, the more vulnerabilities it creates for itself. Security management professionals must identify a company's primary threat vectors so that they can be addressed.
- **Endpoint Security:** Endpoint security involves protecting an organization's computer network by protecting the remote devices that are bridged to it, such as laptops, smartphones and tablets. Security managers must help an organization understand the need to engineer proper security for wireless technologies.
- **Phishing and Identity Theft:** Phishing is a tactic used by criminals to steal someone's identity. The most common phishing campaigns involve convincing fraudulent emails in which the sender purports to be a legitimate company.
- **Disaster recovery** is an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber attack, or even business disruptions related to the COVID-19 pandemic. A variety of disaster recovery (DR) methods can be part of a disaster recovery plan.

Information Technology (IT) policy - To regulate the use of technology resources
Acceptable Use Policy - A policy that defines proper and improper use of IT resources

What is Remote Access

- ability for an authorized person to access a computer or network from a geographical distance through a network connection.
- enables users to connect to the systems they need when they are physically far away. This is especially important for employees who work at branch offices, are traveling or telecommute.

A **remote access strategy** gives organizations the flexibility to hire the best talent regardless of location, remove silos and promote collaboration between teams, offices and locations.

What are privileged accounts?

Standard user accounts have a limited set of privileges, such as for internet browsing, accessing certain types of applications (e.g., MS Office, etc.), and for accessing a limited array of resources, which is often defined by role-based access policies.

Guest user accounts possess fewer privileges than standard user accounts, as they are usually restricted to just basic application access and internet browsing.

A **privileged account** is considered to be any account that provides access and privileges beyond those of non-privileged accounts. A privileged user is any user currently leveraging privileged access, such as through a privileged account. Because of their elevated capabilities and access, privileged users/privileged accounts pose considerably larger risks than non-privileged accounts / non-privileged users.

Types of Remote Access

Cable broadband shares bandwidth across many users and, as a result, upstream data rates can be slow during high-usage hours in areas with many subscribers.

DSL (Digital Subscriber Line) broadband provides high-speed networking over a telephone network using broadband modem tech. However, DSL only works over a limited physical distance and may not be available in some areas if the local telephone infrastructure doesn't support DSL technology.

Cellular internet services can be accessed by mobile devices via a wireless connection from any location where a cellular network is available.

Types of Remote Access

Satellite internet services use telecommunications satellites to provide users internet access in areas where land-based internet access isn't available, as well as for temporary mobile installations.

Fiber optics broadband technology enables users to transfer large amounts of data quickly and seamlessly.

What is VPN?

A **virtual private network** (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

Desktop Sharing

- refers to the technologies that allow remote access of your computer or mobile device by another user on a separate device. Typically, the other user deploys a VNC (Virtual Networking Client) to view or even control your desktop from a remote location. You may also have heard desktop sharing being referred to as ‘screen sharing’ or ‘remote support’.