Global Certification Course in Introduction to IT Compliance and Regulations

Security Policies and Procedures

Access Control:
Access control is the process of regulating who can view or use resources in a computing environment. It involves defining and managing access rights for users or groups of users to specific resources. This could include restricting access to certain files, databases, or applications based on user roles or permissions.

Antivirus Software:
Antivirus software is a program designed to detect, prevent, and remove malicious software (malware) from a computer or network. It scans files and programs for known patterns of malicious code and can quarantine or delete infected files to protect the system from potential threats.

Authentication:
Authentication is the process of verifying the identity of a user or system. It ensures that the entity trying to access a resource is who they claim to be. Common authentication methods include passwords, biometrics, smart cards, and tokens.

Authorization:
Authorization is the process of granting or denying access to resources based on a user's identity and permissions. Once a user is authenticated, authorization determines what actions or resources the user is allowed to access. This helps enforce security policies and prevent unauthorized access.

Backups:
Backups are copies of data that are stored separately from the original data to protect against loss or corruption. Regular backups are essential for data protection and disaster recovery. They can be stored on external drives, cloud services, or tapes to ensure data integrity.

Bring Your Own Device (BYOD):
Bring Your Own Device (BYOD) is a policy that allows employees to use their personal devices, such as smartphones, laptops, or tablets, for work purposes. BYOD can increase productivity and flexibility but also poses security risks if not properly managed.

Business Continuity Plan (BCP):
A Business Continuity Plan (BCP) is a documented strategy outlining how an organization will continue operating during and after a disruptive event. It includes procedures for disaster recovery, data backup, and crisis management to minimize downtime and ensure business resilience.

Compliance:
Compliance refers to adhering to laws, regulations, industry standards, and internal policies related to information security and privacy. It involves implementing controls and measures to meet legal requirements and protect sensitive data from unauthorized access or misuse.

Data Encryption:
Data encryption is the process of converting plain text data into a coded format to prevent unauthorized access. Encrypted data can only be read by those with the appropriate decryption key, ensuring confidentiality and data security, especially during transmission over networks.

Data Loss Prevention (DLP):
Data Loss Prevention (DLP) is a set of technologies and policies designed to prevent the unauthorized disclosure of sensitive information. DLP solutions monitor, detect, and block the transmission of confidential data to unauthorized users or devices to mitigate data breaches.

Firewall:
A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between trusted internal networks and untrusted external networks, preventing unauthorized access and protecting against cyber threats.

Incident Response Plan:
An Incident Response Plan is a documented set of procedures outlining how an organization will respond to and manage security incidents. It includes steps for identifying, containing, eradicating, and recovering from security breaches to minimize damage and restore normal operations.

Information Security:
Information security refers to the protection of data from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing security controls, policies, and procedures to safeguard sensitive information and ensure confidentiality, integrity, and availability.

Internet of Things (IoT):
The Internet of Things (IoT) refers to a network of interconnected devices, sensors, and objects that can communicate and exchange data over the internet. IoT devices collect and transmit information for various applications, but they also pose security challenges due to their vulnerability to cyber attacks.

Malware:
Malware is a type of malicious software designed to disrupt, damage, or gain unauthorized access to a computer system. Common types of malware include viruses, worms, Trojans, ransomware, and spyware. Antivirus software and security measures are used to protect against malware attacks.

Network Security:
Network security involves the protection of network infrastructure, devices, and data from unauthorized access or cyber threats. It includes implementing security protocols, firewalls, intrusion detection systems, and encryption to secure network communications and prevent network breaches.

Penetration Testing:
Penetration testing, also known as pen testing or ethical hacking, is a simulated cyber attack conducted to evaluate the security of a system or network. Certified ethical hackers attempt to exploit vulnerabilities to identify weaknesses and recommend security improvements to enhance defenses.

Phishing:
Phishing is a social engineering technique used by cyber criminals to deceive users into revealing sensitive information, such as usernames, passwords, or financial details. Phishing attacks often involve fraudulent emails, websites, or messages impersonating trusted entities to trick victims into sharing confidential data.

Physical Security:
Physical security refers to measures designed to protect physical assets, facilities, and personnel from unauthorized access, theft, vandalism, or damage. Physical security controls may include access control systems, surveillance cameras, locks, alarms, and security guards to secure physical spaces.

Ransomware:
Ransomware is a type of malware that encrypts a victim's files or locks their computer until a ransom is paid. Cyber criminals demand payment in exchange for decrypting the data or restoring access to the system. Regular backups and security measures are crucial to prevent ransomware attacks.

Risk Assessment:
Risk assessment is the process of identifying, analyzing, and evaluating potential risks and vulnerabilities in an organization's information systems. It helps assess the likelihood and impact of threats, prioritize security controls, and develop strategies to mitigate risks and enhance security posture.

Security Awareness Training:
Security awareness training is an educational program designed to raise awareness and educate employees about information security best practices. It covers topics such as phishing, password security, data protection, and social engineering to help users recognize and respond to security threats.

Security Incident:
A security incident is an event that compromises the confidentiality, integrity, or availability of an organization's information assets. Security incidents can include data breaches, unauthorized access, malware infections, or system outages that require investigation, containment, and remediation.

Security Policies:
Security policies are formal documents that outline an organization's rules, guidelines, and procedures for protecting information assets and ensuring compliance with security requirements. They define roles and responsibilities, establish security controls, and enforce best practices to mitigate security risks.

Security Procedures:
Security procedures are detailed instructions that describe how security policies are implemented and enforced within an organization. They provide step-by-step guidance on security tasks, such as access control, incident response, data backup, and encryption, to ensure consistent security practices.

Social Engineering:
Social engineering is a psychological manipulation technique used by cyber attackers to deceive individuals into divulging confidential information or performing actions that compromise security. Common social engineering tactics include pretexting, phishing, baiting, and tailgating to exploit human vulnerabilities.

Two-Factor Authentication (2FA):
Two-Factor Authentication (2FA) is a security method that requires users to provide two forms of identification to access a system or application. It typically combines something the user knows (e.g., a password) with something they have (e.g., a verification code) to enhance authentication security.

Vulnerability Management:
Vulnerability management is the practice of identifying, assessing, and mitigating security vulnerabilities in an organization's systems and networks. It involves scanning for weaknesses, prioritizing patches, and implementing controls to reduce the risk of exploitation by cyber threats.

Zero-Day Attack:
A zero-day attack is a cyber attack that exploits a previously unknown vulnerability in software or hardware before a patch or fix is available. Zero-day attacks are difficult to detect and defend against because security vendors have not had time to develop countermeasures, making them highly dangerous.