**IS Notes**

**Ayesha Altaf**

**CHAPTER 3**

1. **Difference between laws and ethics?**

Laws are formal, legally binding rules and regulations enforced by a governing authority, while ethics are moral principles and values that guide individual behavior and decision-making. Laws are mandatory and violators can face legal consequences, while ethics are voluntary and based on personal beliefs about what is right or wrong.

* **Laws** are rules that mandate or prohibit certain behavior;
* **ethics**, which define socially acceptable behaviors.

The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not.

* Ethics in turn are based on cultural mores.
* Some ethical standards are universal.

1. **What is liability?**

Liability refers to legal responsibility or obligation for one's actions or debts. It means that an individual or entity can be held accountable or legally responsible for any harm, damage, or financial obligations resulting from their actions or negligence.

1. **What is Civil Law?**

Civil law comprises a wide variety of Laws that govern the nation and state and deal with the relationship and conflict between organizational entities and peoples.

* Civil law is the part of the country's set law that is concerned with the private affairs of the citizens.
* Civil law is the system of rules that helps solve problems and disagreements between people or organizations by deciding who should get compensation or how to make things right, rather than punishing someone like in criminal law.

1. **What is Criminal Law?**

Criminal law is the set of rules and punishments that deal with actions that are considered crimes, like theft or assault. It's about holding people accountable for breaking these rules, and if found guilty, they can face penalties like fines or jail time.

1. **What is public Law?**

Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

1. **What is private Law?**

Private law encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations.

1. **Cybersecurity laws of Pakistan.**

Cybersecurity laws in Pakistan are designed to protect computer systems, data, and online activities. They include:

* **Prevention of Electronic Crimes Act (PECA):** This law criminalizes activities like hacking, cyberbullying, and online harassment.
* **Data Protection Laws:** These laws regulate how personal data is collected and used online.
* **Telecommunication Laws:** They govern the use of communication networks and ensure data privacy.
* **National Response Center for Cyber Crime (NR3C):** This agency is responsible for investigating and preventing cybercrimes in Pakistan.

These laws aim to safeguard digital activities and punish cybercriminals.

**CHAPTER 04**

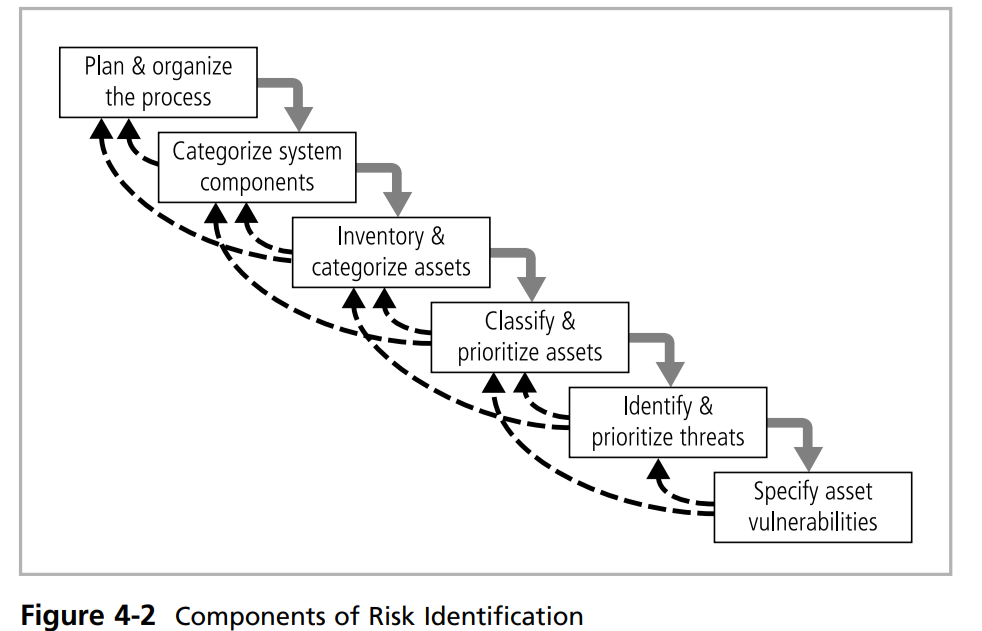
1. **What is risk management?**

Risk management in information security is the process of identifying, assessing, and minimizing potential threats and vulnerabilities that could harm or compromise a company's sensitive data or technology systems. It involves taking steps to protect against security breaches and data breaches.

* Risk identification
* Risk assessment.
* Risk Control

1. **What is risk identification?**

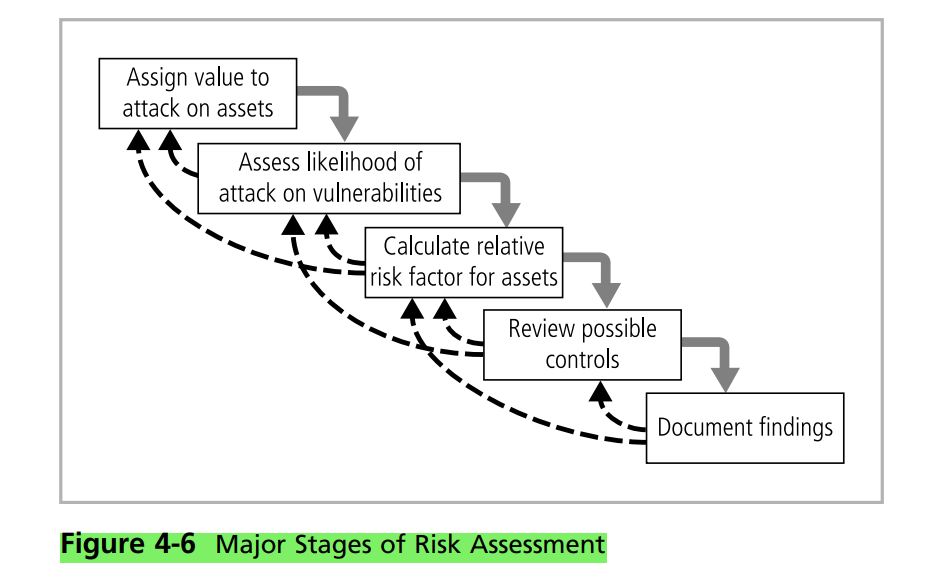
Risk identification in information security means recognizing and making a list of potential problems or dangers that could harm a company's data or computer systems. It's like making a checklist of all the things that might go wrong in terms of security.

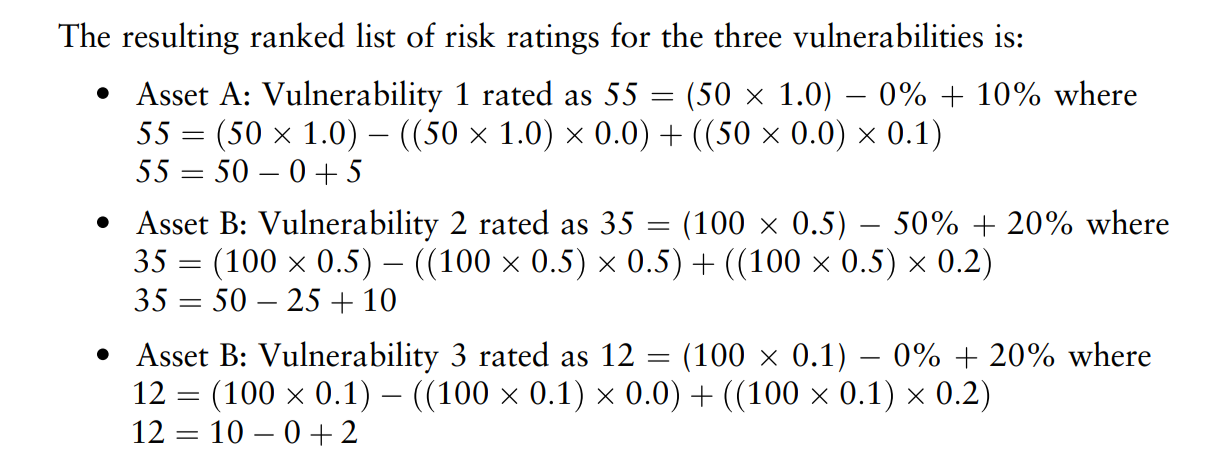


1. **What is risk assessment?**

Risk assessment in information security means evaluating and figuring out how likely and how bad those potential security problems are. It's like deciding which problems on your checklist are most concerning and need the most attention.

Risk assessment is the process of identifying, analyzing, and evaluating potential risks or threats that could impact an organization, project, or activity. It helps in understanding the likelihood and consequences of these risks and determining how to mitigate or manage them.





1. **What is risk Control?**

Risk control in information security involves taking actions to reduce or manage the problems you've identified and assessed. It's like doing things to lower the chances of security issues happening or lessen their impact if they do occur.

Strategies:

1. Defend control strategies (Research and acknowledgment).
2. Transfer Control (Risk Transference).
3. Mitigate Control (risk Limitation & and risk planning).
4. Accept (risk Assumption)
5. Terminal (Risk Avoidance)

**Chapter 07**

**Intrusion Detection:**

**IDS (Intrusion Detection System) and IPS (Intrusion Prevention System)** are two cybersecurity technologies used to protect computer networks and systems from various forms of malicious activities, such as unauthorized access, attacks, and breaches. They play crucial roles in identifying and mitigating security threats.

1. **Intrusion Detection System (IDS):**

An IDS is a monitoring and alerting system that observes network traffic and system activities for signs of suspicious or potentially harmful activities. When it detects such activities, it generates alerts or notifications to network administrators, allowing them to investigate and respond to potential threats. IDS does not actively block or prevent detected intrusions; instead, it acts as a monitoring tool to raise awareness of security incidents.

* Example: Consider an organization that has deployed an IDS to protect its network. The IDS continually analyzes network traffic for known attack patterns or anomalies. If an employee's computer becomes infected with malware and starts communicating with a command-and-control server outside the network, the IDS can detect this unusual behavior and generate an alert for the IT security team to investigate the issue.

1. **Intrusion Prevention System (IPS):**

An IPS, on the other hand, goes a step further than an IDS by actively blocking or preventing malicious activities in real time. It not only detects suspicious activities but can also take automatic action to stop or mitigate threats, thus providing a more proactive approach to cybersecurity.

* **Example:** Suppose an organization has an IPS in place. If the IPS detects a known malicious attack pattern, such as a Distributed Denial of Service (DDoS) attack, it can immediately take action to block the incoming traffic from the attacking source, preventing the attack from disrupting the network or services. Additionally, if the IPS identifies an attempt to exploit a known software vulnerability on a web server, it can apply rules to block the malicious traffic, preventing the exploitation of the vulnerability and potential data breaches.

**Honey Pots:**

**Purpose:** To attract and deceive attackers, collecting information about their tactics and motives.

**Advantages of Honeypots:**

1. Enhanced Threat Detection
2. Reliable Alerts (few false positives)
3. Valuable Threat Intelligence
4. Reduced Attack Surface
5. Deception and Diversion
6. Research and Education

**Disadvantages of Honeypots:**

1. Resource Intensive
2. False Negatives (missed advanced attacks)
3. False Positives (though less common)
4. Security Risks (if not properly configured)
5. Complexity
6. Legal and Ethical Considerations.

**Fire Wall:**

Firewalls are a fundamental component of network security, but they have certain limitations that organizations should be aware of to develop a comprehensive security strategy.