Deepak S
221801008
AIDS III rd year

Data Information And Security - AD19652

ASSIGNMENT - 2

1. Discuss in detail about what is risk management and how to identify and accss risk in an Organization.

Risk management:

Risk management is praess of identifying, assessing and controlling risks that could impact an Organization operations, assessts and objectives. It involves systematic efforts to mitigate potential threats while maximizing opportunities.

Effective risk management ensures business continuity enhances decision making, safeguards an organization from financial losses, security branches, regulatory non-compliance and reputational damage.

Steps to identify & assess risks in an organization:

1) Risk identification: Identify potential risks that could affect because of business operations, data & resources. Categories of risk includes: strategic risks, operational risks, financial risks, cybersecurity risks.
2) Risk assessment: After identifying risks, organization asses them based on two keey factors.
   Likelihood (Probability)
   Impact (Severity)

2. Discuss in detail about assessing and controlling of risks:

Risk assessment process:

- Risk Identification: Recognizing all potential threats
- Risk analysis: Evaluating the nature and impact of risks.

* Risk Evaluation : Prioritizing risks based on severity.

Risk control strategies:

Once risks are assessed, organizations implement control measures

Risk avoidance: Eliminating the activity that generates risks.

Risk mitigation: Reducing the impact or likelihood of risks.

Risk transfer: shifting responsibility to third portion

Risk acceptance: Acknowledging & preparing for risks that cannot be avoided.

Implementing risk control:

Preventive controls: firewalls, security policies, staff training.

Detective controls: Security audits, intrusion detection systems.

Corrective controls: Disaster recovery plans, backup solutions

Compensatory controls: Alternative security measures when primary control fails.

3) Discuss in detail about blueprint for information security?

A blueprint for information security is a structured framework that defines how an organization protects the digital and physical information assets. It consists of security policies, procedures and technologies that ensure confidentiality, integrity & availability of information.

Components of an information Security blueprint

Risk management framework: Defines security policies and risk assessment method.

Access control measures: Role based access control Multifactor authentication

Network security strategy: Firewalls, VPNs, Intrusion detection and prevention system (IDS/IPS)

Data protection strategy: Encryption, Secure backups, Data loss prevention

Incident Response plan: Steps for handling cyber threats and security breaches.

Importance of an Information Security blueprint:

Ensures proactive security measures are in place.

Protects sensitive information from cyber threats

Supports business continuity and disaster recovery

Helps in regulatory compliance and legal protection.

4. Discuss in detail about information security policy?

An information security policy (ISP) is a set of rules and guidelines that define how an organization protects its information assests. It establishes the principles for data protection, system security & compliance with legal and regulatory requirements.

Key elements of an Information security policy:

1) Purpose & Scope: Define the objective and areas covered by the policy

2) Roles and responsibilities: Assigns, security duties to employee IT teams and executives

3) Access control policies: Specifies who can access what data and how

4) Data protection guidelines: Encryption, handling, data retention

Benefits:

Prevents data breaches & cyber threats

Defines clear security responsibilities across the organization.

Ensures regulatory compliance & avoids legal penalties

Reduces risks associated with them human errors and insider threats.