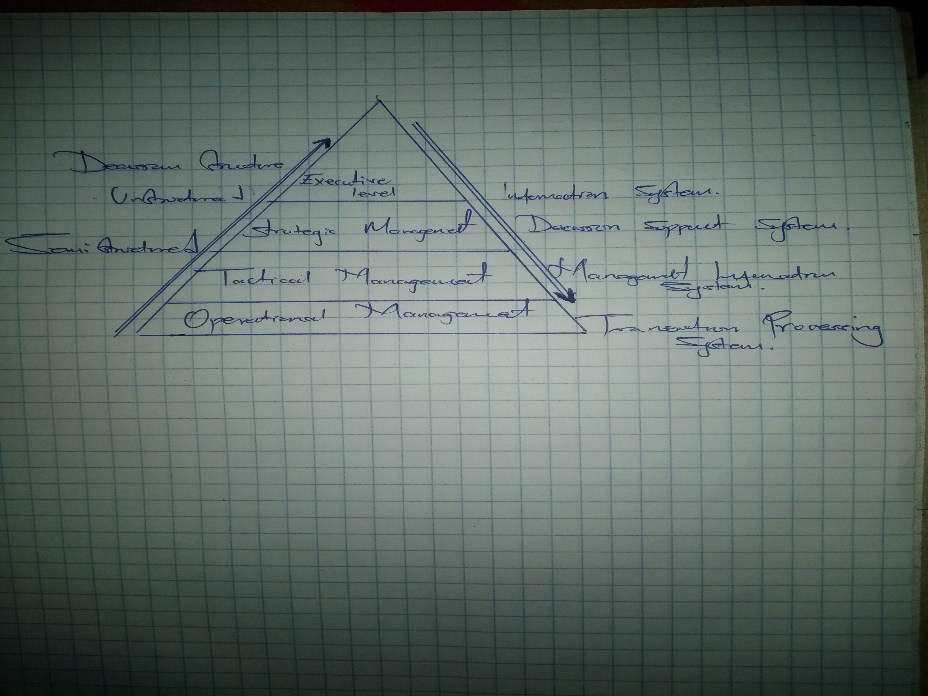
**QUESTION ONE**



(b)

1. Confidentiality:

Confidentiality ensures that information is only accessible to authorized individuals, systems, or processes. The goal is to prevent unauthorized access or disclosure of sensitive data to maintain privacy and protect against data breaches.

2. Integrity:

Integrity ensures the accuracy, consistency, and trustworthiness of data throughout its lifecycle. The goal is to prevent unauthorized or malicious modification, deletion, or alteration of data. Integrity controls such as checksums, digital signatures, version controls, and audit trails help detect and prevent unauthorized changes to data, ensuring its reliability and authenticity.

3. Availability:

Availability ensures that information and resources are accessible and usable when needed by authorized users. The goal is to prevent or minimize disruptions to services, systems, or networks, ensuring continuous operations and timely access to data.

4. Authenticity:

Authenticity verifies the identity of users, systems, or entities and ensures that they are who they claim to be. The goal is to prevent impersonation, identity theft, or unauthorized access by validating the authenticity of individuals or processes.

**QUESTION TWO**

(C) PERT is probabilistic in nature, focuses on uncertainty management, and calculates expected durations, while logical network is deterministic, emphasizes dependency management, and provides a structured view of the project's workflow. Both techniques are valuable tools for effective project planning and scheduling, each with its unique strengths and applications.

**QUESTION THREE**

a. Definitions:

i. Risk Mitigation:

Risk mitigation refers to the process of taking actions to reduce or minimize the impact of potential risks on an organization's objectives. It involves identifying, assessing, and prioritizing risks, and then implementing strategies or measures to reduce their likelihood of occurring or their potential impact if they do occur. Risk mitigation aims to enhance the organization's resilience and ability to cope with adverse events or uncertainties.

ii. System Vulnerability:

System vulnerability refers to a weakness or flaw in a computer system, network, application, or software that could be exploited by attackers or malicious actors to compromise the confidentiality, integrity, or availability of the system or its data. Vulnerabilities may arise due to programming errors, misconfigurations, design flaws, or outdated software. Exploiting vulnerabilities can lead to security breaches, data leaks, unauthorized access, and other security incidents.

iii. Denial of Service (DoS) Attack:

A Denial of Service (DoS) attack is a malicious attempt to disrupt or impair the normal functioning of a computer system, network, website, or service by overwhelming it with a large volume of traffic, requests, or data. The goal of a DoS attack is to exhaust the target's resources, such as bandwidth, memory, or processing power, making it inaccessible to legitimate users or clients. DoS attacks can result in downtime, slow performance, service interruptions, and financial losses for organizations targeted by attackers.

(b)

Financial Risk:

Financial risk encompasses the possibility of financial loss or instability due to fluctuations in market conditions, economic factors, or financial management decisions. This includes risks related to currency exchange rates, interest rates, creditworthiness, liquidity, investment decisions, and market volatility. Companies may face financial risks when making investments, borrowing funds, managing cash flow, or engaging in international trade.

Operational Risk:

Operational risk arises from internal processes, systems, people, or external events that can disrupt or negatively impact the company's operations. This includes risks associated with human error, technology failures, supply chain disruptions, regulatory compliance issues, fraud, theft, natural disasters, and other unexpected events. Operational risk management involves identifying, assessing, and mitigating potential threats to ensure business continuity and resilience.

Reputational Risk:

Reputational risk pertains to the potential damage to a company's reputation, brand image, credibility, and public perception resulting from negative publicity, scandals, ethical lapses, product recalls, customer complaints, or social media backlash. A tarnished reputation can lead to loss of customer trust, decreased sales, stakeholder distrust, legal liabilities, and difficulty in attracting and retaining talent. Managing reputational risk requires proactive communication, transparency, ethical behavior, and effective crisis management strategies.

Compliance and Regulatory Risk:

Compliance and regulatory risk refers to the potential legal, regulatory, or compliance violations that may expose the company to fines, penalties, lawsuits, regulatory sanctions, or reputational damage. Companies operating in highly regulated industries or global markets must adhere to various laws, regulations, industry standards, and corporate governance requirements. Failure to comply with regulatory obligations related to data privacy, consumer protection, environmental regulations, financial reporting, and occupational health and safety can result in significant financial and legal consequences.

Cybersecurity Risk:

Cybersecurity risk involves the threat of unauthorized access, data breaches, cyberattacks, malware infections, ransomware, phishing scams, and other cyber threats targeting the company's digital assets, networks, systems, and sensitive information. With the increasing reliance on digital technologies, cloud services, mobile devices, and interconnected networks, companies face heightened cybersecurity risks that can lead to data loss, financial theft, business disruption, regulatory fines, and damage to customer trust. Effective cybersecurity measures, such as robust security policies, access controls, encryption, threat detection, incident response plans, and employee training, are essential for protecting against cyber threats and safeguarding critical assets.

(c)

Risk Identification:

The first step in risk management is to identify potential risks that could affect the organization's objectives, projects, processes, or activities. This involves systematically identifying internal and external factors, events, threats, vulnerabilities, and uncertainties that could lead to adverse outcomes or disruptions. Various techniques such as brainstorming, risk workshops, interviews, checklists, historical data analysis, and risk registers can be used to identify risks comprehensively. The goal is to create a comprehensive inventory of risks that the organization may face.

Risk Assessment:

Once risks have been identified, the next step is to assess and analyze them to understand their potential impact and likelihood of occurrence. Risk assessment involves evaluating the severity of the risk (consequences), the likelihood of the risk occurring, and the effectiveness of existing controls or mitigation measures. Quantitative techniques, such as probability analysis, impact assessment, risk matrices, and scenario analysis, can be used to quantify and prioritize risks based on their potential impact and likelihood. Qualitative assessments, including expert judgment, risk rating scales, and risk ranking methods, may also be employed to evaluate risks that cannot be easily quantified.

Risk Mitigation:

After assessing risks, the organization develops and implements risk mitigation strategies and action plans to reduce, transfer, or manage the identified risks effectively. Risk mitigation measures aim to minimize the likelihood of risk occurrence, mitigate its impact, or enhance the organization's ability to respond to and recover from adverse events. Depending on the nature of the risks, mitigation strategies may include implementing controls, improving processes, enhancing security measures, diversifying investments, purchasing insurance, establishing contingency plans, and allocating resources to address high-priority risks. The effectiveness of risk mitigation measures should be regularly monitored, reviewed, and adjusted as needed to ensure their adequacy and relevance.

Risk Monitoring and Review:

The final step in the risk management process involves monitoring and reviewing the effectiveness of risk mitigation measures and reassessing the organization's risk profile over time. Continuous monitoring helps track changes in the internal and external risk environment, identify emerging risks, evaluate the performance of existing controls, and ensure that risk management practices remain aligned with the organization's objectives and risk tolerance. Regular risk reviews, audits, performance metrics, key risk indicators (KRIs), and incident reporting mechanisms enable stakeholders to stay informed about potential risks and take proactive measures to address them. Feedback loops and lessons learned from past experiences are used to improve risk management processes and enhance organizational resilience.