PART 1: CONSOLIDATED QUESTION & ANSWER BANK

SECTION A: 2-MARK QUESTIONS (ANSWER IN 50–80 WORDS EACH)

1. **What is information security?** (2019, 2020, 2023)

   Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It aims to ensure the confidentiality, integrity, and availability (CIA) of data, whether it is in storage, processing, or transmission.

2. **Define confidentiality in the context of information security.** (2020, 2021, 2022)
   Confidentiality means ensuring that information is accessible only to those authorized to have access. It is a key component of the CIA triad and helps prevent sensitive data from being exposed to unauthorized individuals, thereby protecting privacy and trade secrets.

3. **What is integrity in information security?** (2020, 2022)

   Integrity refers to maintaining the accuracy and completeness of information. It ensures that data has not been altered or tampered with, either maliciously or accidentally, and that it remains trustworthy and reliable over its lifecycle.

4. **Define availability with respect to information security.** (2020, 2022, 2023)

   Availability ensures that authorized users have access to information and associated resources when needed. This is maintained through system redundancy, failover systems, and regular maintenance to prevent downtime and denial-of-service.

5. **What is a threat in information security?** (2019, 2021, 2023)

   A threat is any potential danger to information or systems that could exploit a vulnerability and cause harm. It may be intentional, such as a cyberattack, or unintentional, such as hardware failure or human error.

6. **What is a vulnerability?** (2020, 2022, 2023)

   A vulnerability is a weakness in a system, process, or design that can be exploited by a threat to gain unauthorized access or cause harm. It can be technical (software bugs), physical (unlocked server rooms), or human (lack of training).

7. **Differentiate between virus and worm.** (2021, 2023)

   A virus is a type of malicious code that attaches itself to a host file and spreads when the file is executed. A worm is self-replicating malware that spreads without needing to attach to a host file, often exploiting network vulnerabilities.

8. **Define firewall.** (2020, 2021)

   A firewall is a security system designed to prevent unauthorized access to or from a private network. It monitors and filters incoming and outgoing network traffic based on predetermined security rules, acting as a barrier between trusted and untrusted networks.

9. **What is two-factor authentication?** (2021, 2023)

   Two-factor authentication (2FA) is a security process that requires users to provide two different authentication factors to verify their identity. These usually include something the user knows (password) and something they have (OTP/token) or are (biometrics).

10. **What is cryptography?** (2020, 2022)

    Cryptography is the practice of securing information by transforming it into unreadable formats using encryption algorithms. Only authorized users with the decryption key can convert it back into readable form, ensuring confidentiality and data protection.

11. **Define malicious code.** (2022)
    Malicious code refers to software programs designed to harm, disrupt, or gain unauthorized access to computer systems. Examples include viruses, worms, Trojans, and spyware. These codes often spread through infected files or websites, compromising data and system performance.

12. **What is fire detection in physical security?** (2022)
    Fire detection refers to systems and devices used to identify the presence of fire through heat, smoke, or flame. Common tools include smoke detectors, heat sensors, and fire alarms. These systems are vital in preventing damage and ensuring safety.

13. **Define cost analysis.** (2021, 2022)
    Cost analysis involves evaluating the financial aspects of security decisions by comparing the costs of implementing controls versus the potential losses due to risks. It aids in selecting cost-effective strategies in information security.

14. **What is event logging?** (2020, 2021)
    Event logging is the recording of system activities such as logins, file access, and error events. It is used to monitor system behavior, detect anomalies, and support forensic analysis in case of a security breach.

15. **Define risk mitigation.** (2019, 2021, 2023)
    Risk mitigation refers to the steps taken to reduce the adverse effects of threats on

information systems. Techniques include installing firewalls, encrypting data, and regular updates to minimize vulnerabilities and control impacts.

16. **What is user identity?** (2019, 2022)
    User identity refers to the unique identification of a person using a system, often represented through usernames or biometric traits. Accurate identity management is essential for enforcing access control policies.

17. **What is information classification?** (2020, 2023)
    Information classification is the process of categorizing information based on sensitivity and value. Common levels include public, internal, confidential, and secret. Classification helps define access control and handling policies.

18. **What is access management?** (2022)
    Access management involves granting or denying users the right to use a system or data. It ensures that only authorized individuals can access specific resources based on predefined policies and user roles.

19. **What is DoS attack?** (2019, 2023)
    A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a server, service, or network by overwhelming it with a flood of internet traffic, rendering it inaccessible to legitimate users.

20. **What is perimeter security?** (2020, 2023)
    Perimeter security refers to the physical and logical barriers used to protect the outer boundary of a network or facility. Examples include fences, firewalls, surveillance systems, and intrusion detection systems.

21. **What is a threat agent?** (Model Paper)
    A threat agent is an entity that initiates a threat by exploiting a vulnerability in a system. It can be a person (e.g., hacker), process (e.g., malware), or even a natural event (e.g., flood). Understanding threat agents helps in implementing effective controls.

22. **What is MITM? (Man-in-the-Middle Attack)** (Model Paper)
    MITM is a type of cyberattack where the attacker secretly intercepts and relays communication between two parties. The attacker can manipulate or steal the data, compromising confidentiality and integrity.

23. **What are RATs?** (Model Paper)
    RATs (Remote Access Trojans) are malware that allow attackers to remotely control a victim’s device. They are often used for spying, data theft, or spreading other malicious code without the user’s knowledge.

24. **What is Information Security Governance?** (Model Paper)
    Information security governance is the system by which an organization directs and controls information security. It involves leadership, organizational structures, and policies to ensure information security strategies support business objectives.

25. **List types of asset owners.** (Model Paper)
    The three main types of asset owners are:

- **Owner** – has authority over the asset
- **Custodian** – responsible for safeguarding the asset
- **User** – utilizes the asset in daily operations

26. **Define Risk.** (Model Paper)
    Risk in information security refers to the potential for loss, damage, or destruction of an asset due to a threat exploiting a vulnerability. It is usually assessed in terms of likelihood and impact.

27. **What is Cost Benefit Analysis?** (Model Paper)
    Cost Benefit Analysis (CBA) evaluates the cost of implementing a security control against the expected benefit (such as reduced losses). It helps in deciding whether a security investment is justified.

28. **What is a policy?** (Model Paper)
    A policy in information security is a set of rules or guidelines that define acceptable use and procedures for protecting information assets. It sets the foundation for organizational security behavior.

SECTION B: 6-MARK QUESTIONS (ANSWER IN ~250 WORDS EACH)

1. **Explain hackers.** (2019) Hackers are individuals who use technical knowledge to gain unauthorized access to systems, networks, or data. They exploit vulnerabilities for various motives including financial gain, political activism, curiosity, or challenge. Hackers are commonly categorized into three main types:

- **White Hat Hackers:** Also known as ethical hackers, they work legally to identify and fix security vulnerabilities. Organizations often hire them to conduct penetration testing and ensure their systems are secure.
- **Black Hat Hackers:** These hackers break into systems with malicious intent. They may steal data, deploy malware, or damage infrastructure.

- **Gray Hat Hackers:** They operate between ethical and malicious boundaries. They might breach systems without permission but not always for personal gain, sometimes notifying the affected parties afterward.

Hackers may use various tools like keyloggers, rootkits, sniffers, and Trojan horses. Common attack methods include phishing, brute force attacks, and denial-of-service attacks.

While the term “hacker” often has a negative connotation, ethical hackers play a crucial role in strengthening cybersecurity. Governments and organizations now offer certifications like CEH (Certified Ethical Hacker) to formalize ethical hacking practices.

Understanding hacker behavior is essential for developing strong security policies, user awareness programs, and effective incident response mechanisms.

2. **Enumerate the types of risk.** (2019) Risk in information security refers to the potential harm or loss resulting from a threat exploiting a vulnerability. Several types of risks are commonly recognized:

- **Operational Risk:** These arise from internal processes, people, or systems failures. Examples include system crashes or human error.
- **Strategic Risk:** Risks related to high-level business decisions. For instance, entering a new market without adequate research.
- **Compliance Risk:** Arising from failure to comply with laws, regulations, or policies. Non-compliance can lead to fines and reputational damage.
- **Reputational Risk:** Events that can damage a company’s brand or public trust. Data breaches and unethical practices often fall here.
- **Financial Risk:** Involves monetary loss due to fraud, market fluctuations, or cyber theft.
- **Environmental Risk:** These include natural disasters like floods or earthquakes that disrupt business continuity.

Risk assessment involves identifying, analyzing, and prioritizing these risks to implement appropriate mitigation strategies. Security controls such as firewalls, antivirus, and backup systems are employed to reduce risk likelihood or impact.

Regular risk evaluation ensures that emerging threats and changes in business operations are effectively managed.

3. **Write a note on Perimeter Security.** (2019, 2020, 2021)

Perimeter security refers to the systems and practices used to protect the outermost boundaries of an organization's physical and digital assets. It forms the first line of defense against external threats and intrusions. In the physical context, perimeter security includes fences, surveillance cameras, security guards, motion detectors, and access control systems. These tools help deter unauthorized access and detect suspicious activity.

In the digital realm, perimeter security involves firewalls, intrusion detection and prevention systems (IDPS), and demilitarized zones (DMZs). Firewalls filter incoming and outgoing traffic based on predefined rules, while IDPS monitor network activity to detect potential intrusions. DMZs host external-facing services such as web and email servers, creating a buffer between the internet and the internal network.

Effective perimeter security relies on a layered approach called defense-in-depth, which combines multiple safeguards to mitigate the risk of breach. As threats evolve, traditional perimeter security models are shifting towards zero-trust architectures, where no device or user is trusted by default—even inside the network.

Maintaining perimeter security requires regular assessments, patch management, and awareness training. In summary, both physical and cyber perimeter protections are essential to defend against unauthorized access and ensure organizational security.

4. **Explain social engineering.** (2019, 2020, 2021)

Social engineering is a manipulation technique that exploits human error to gain access to private information, systems, or physical locations. Unlike technical hacking, social engineering targets the human element—convincing individuals to divulge confidential information or perform actions that compromise security.

Common types of social engineering attacks include:

- Phishing: Attackers impersonate legitimate entities in emails or messages to trick users into revealing sensitive information or downloading malware.
- Pretexting: The attacker fabricates a scenario (pretext) to obtain information or access.
- Baiting: Enticing users with offers (e.g., free USB drives or music downloads) that contain malicious code.

- Tailgating: Gaining physical access by following an authorized person into a secured area.

Attackers often rely on urgency, authority, or curiosity to manipulate victims. For instance, an attacker posing as IT support may ask a user to “verify credentials urgently.”

To mitigate social engineering risks, organizations must train employees in security awareness, implement verification protocols, and limit the information shared publicly. Multi-factor authentication and strong access controls also help reduce the success rate of such attacks.

In conclusion, social engineering is a low-tech yet highly effective form of attack. Combating it requires not only technical solutions but also educating individuals to recognize and resist manipulation tactics.

5. **Explain Access and Privilege Management.** (2022)

Access and privilege management refers to the processes and tools used to ensure that individuals have the right level of access to information systems and data based on their roles. This ensures that sensitive information is protected and that users only access resources necessary for their job functions.

Access control begins with authentication, where users verify their identity using credentials like passwords, tokens, or biometrics. After authentication, authorization determines what actions a user is allowed to perform. For example, a finance team member may have access to budgeting software but not HR records.

Privileges refer to the specific rights assigned to a user or role. These can include read, write, execute, and delete permissions. Effective privilege management uses the principle of least privilege, where users receive only the access necessary to complete their tasks.

Tools such as role-based access control (RBAC), attribute-based access control (ABAC), and identity and access management (IAM) systems automate and enforce these rules. Regular reviews and audits are essential to identify and revoke unnecessary access rights, particularly when roles change or employees leave.

Proper access and privilege management helps reduce insider threats, supports regulatory compliance, and ensures data confidentiality and integrity within the organization.

6. **Write a note on Safe Disposal of Physical Assets.** (2020, 2023)

Safe disposal of physical assets is an essential part of an organization’s information security policy. It involves securely discarding hardware and devices to ensure that sensitive data is not recoverable by unauthorized individuals. Improper disposal can lead to serious data breaches and legal consequences.

Assets that often require secure disposal include hard drives, computers, mobile devices, CDs/DVDs, USBs, and printed documents. Even when deleted, data may remain retrievable on storage media using forensic tools, hence requiring special methods.

Common techniques for safe disposal include:

- Degaussing: Using strong magnetic fields to erase data from magnetic storage devices.
- Shredding: Physically destroying media like CDs, hard drives, or documents.
- Overwriting: Writing over existing data with random or specific patterns to make original data unrecoverable.
- Secure Erase Software: Specialized tools that permanently delete files and formatting.

Organizations must maintain a disposal policy that outlines procedures for media sanitization, logging disposed items, and ensuring compliance with privacy regulations like GDPR or HIPAA.

Additionally, disposal should be documented, and certificates of destruction should be obtained from third-party vendors if disposal services are outsourced. Employees should be trained in identifying and handling sensitive assets slated for disposal.

Safe disposal protects intellectual property, personal information, and helps prevent data leaks that could harm an organization's reputation and financial stability.

7. **Write a note on Business Requirements.** (2022, 2023) Business requirements in the context of information security refer to the foundational needs and expectations that an organization must fulfill to operate securely and achieve its strategic goals. These requirements guide the development of policies, procedures, and technologies used to protect data, systems, and operations.

Key business requirements include:

- **Confidentiality:** Ensuring that sensitive data is accessible only to authorized personnel.
- **Integrity:** Maintaining the accuracy and consistency of data over its lifecycle.
- **Availability:** Guaranteeing reliable access to systems and data whenever needed.
- **Compliance:** Adhering to legal, regulatory, and contractual obligations (e.g., GDPR, HIPAA).
- **Accountability:** Enforcing actions through user identification and audit trails to ensure responsibility and traceability.

Meeting business requirements involves aligning IT and security strategies with business objectives. For example, an e-commerce platform must maintain high system availability, protect customer data, and comply with financial regulations.

Risk assessment plays a central role in identifying security gaps that could hinder business objectives. Based on these findings, organizations implement security controls like access management, encryption, and incident response planning.

Business requirements are also influenced by stakeholder interests including customers, regulators, shareholders, and employees. Understanding these perspectives ensures that security measures support operational resilience and stakeholder confidence.

In summary, business requirements define the expectations for secure and efficient operations, making them a critical input in the design and maintenance of any information security framework.

8. **Explain Threat Identification.** (2020, 2023) Threat identification is a crucial step in risk management where potential sources of harm to an organization's assets are recognized and documented. The purpose is to understand what might go wrong, so that appropriate defenses can be designed to mitigate those risks.

Threats can come from various sources, both internal and external. Common examples include:

- **Natural Threats:** Floods, earthquakes, fires, or other environmental hazards.
- **Technical Threats:** Hardware failure, software bugs, or network downtime.
- **Human Threats:** Includes both malicious (e.g., hacking, social engineering) and unintentional (e.g., employee error).
- **Physical Threats:** Theft, vandalism, unauthorized access to facilities.

The process involves:

- Identifying and listing possible threats to assets.
- Determining how these threats could exploit vulnerabilities.
- Understanding past incidents or known attack patterns.

Threat identification tools include vulnerability scanners, threat modeling diagrams, and security audits. Threat intelligence feeds may also help anticipate emerging risks.

Once threats are identified, they are analyzed for likelihood and impact. This information supports risk assessment and influences the selection of appropriate security controls. Regular threat reviews are essential to adapt to changing environments.

By identifying threats early, organizations can take proactive measures to safeguard their data, systems, and reputation from potential harm.

9. **Explain Event Logging.** (2023) Event logging is the systematic recording of events that occur within a computer system, application, or network. It plays a vital role in information security by enabling monitoring, auditing, and forensic analysis.

Each log entry typically includes a timestamp, user ID, event type, source of the event, and the result or status. Examples of logged events include login attempts, file access, configuration changes, and system errors.

Benefits of event logging include:

- **Security Monitoring:** Detect unauthorized access or unusual activity.
- **Accountability:** Trace actions back to individual users or processes.
- **Compliance:** Fulfill legal or regulatory requirements (e.g., HIPAA, PCI-DSS).
- **Troubleshooting:** Identify the root cause of system errors or failures.
- **Forensics:** Aid in post-incident investigations by reconstructing events.

Best practices in event logging include:

- Defining which events should be logged.
- Ensuring logs are securely stored and protected from tampering.
- Regularly reviewing and analyzing logs.
- Using centralized log management tools (e.g., SIEM systems).

Logs must also be retained for a specified period depending on compliance standards. Event logging, when properly implemented, not only supports operational integrity but also enhances the security posture of the organization.

SECTION C: 10-MARK QUESTIONS (ANSWER IN ~500 WORDS EACH)

1. **Explain the CIA triad with examples.** (2019, 2021) The CIA triad—Confidentiality, Integrity, and Availability—is a foundational model in information security. It helps guide policies for information assurance and forms the basis for developing effective security strategies.

1. Confidentiality: Confidentiality ensures that sensitive data is accessible only to authorized users. It is achieved using encryption, authentication, and access control mechanisms. For example, a company's payroll file should be viewable only by HR personnel. Breaches of confidentiality may occur through hacking, insider threats, or accidental exposure.

2. Integrity: Integrity involves maintaining the accuracy and consistency of data throughout its lifecycle. Techniques such as hashing, checksums, and digital signatures help preserve integrity. For instance, if a financial record is altered without authorization, the system must detect and flag the change. Data corruption or unauthorized modification compromises integrity.

3. Availability: Availability guarantees that authorized users can access data and systems when needed. This is maintained through redundancy, failover systems, regular maintenance, and security measures against DoS attacks. An example is a bank's online system being accessible 24/7. If downtime occurs due to a cyberattack, it negatively impacts availability.

Together, the CIA triad supports robust data protection. An organization must balance all three aspects. Over-focusing on one can risk the others—for instance, strong encryption might reduce system availability. The CIA model remains a core framework used by security professionals to evaluate risk, design policies, and implement technology controls.

2. **Discuss the process and importance of Information Classification.** (2022, 2023) Information classification is the process of categorizing data based on its sensitivity and the impact it would have if disclosed, altered, or destroyed without authorization. It is a critical element of information security management, helping ensure appropriate protection and access control.

Purpose of Classification: The primary goal is to determine the required level of security controls. It also supports compliance, minimizes risk, and improves resource allocation by identifying what data needs stringent protection.

Common Classification Levels:

- **Public:** Information that can be shared freely.
- **Internal Use Only:** Data not meant for external sharing but not highly sensitive.
- **Confidential:** Business-sensitive information requiring restricted access.
- **Highly Confidential or Secret:** Data whose exposure would cause significant harm (e.g., trade secrets, legal documents).

Steps in the Classification Process:

1. **Identify assets** that require classification.

2. **Assess sensitivity** and business impact.
3. **Label data** based on category.
4. **Apply controls** like encryption, access restriction, and logging.
5. **Review regularly** to update classifications as needed.

Importance of Classification: Classification ensures that resources are not wasted protecting low-risk data and that high-risk data is adequately secured. It also assists in incident response by clarifying which data, if compromised, requires priority action. Proper classification supports legal and regulatory compliance (e.g., GDPR, HIPAA).

In summary, information classification underpins data governance, ensures compliance, and contributes to a strong cybersecurity posture by enforcing security proportional to data value.

3. **Explain Risk Mitigation Techniques.** (2019)

   Risk mitigation refers to strategies and processes implemented to reduce the impact or likelihood of information security threats. It is a core part of risk management and focuses on proactively addressing identified risks before they materialize.

Types of Risk Mitigation Techniques:

1. **Risk Avoidance:** This involves eliminating the risk entirely by choosing not to engage in certain activities. For example, a company may avoid storing sensitive customer data online to prevent exposure to data breaches.
2. **Risk Reduction:** This is the most common approach and involves implementing controls to lower either the likelihood or impact of the risk. Firewalls, antivirus software, employee training, patch management, and encryption are examples of reducing exposure to threats.
3. **Risk Transfer:** Organizations shift the risk to a third party, typically through insurance or outsourcing. For instance, purchasing cybersecurity insurance can help cover financial losses resulting from data breaches.
4. **Risk Acceptance:** Sometimes, a risk may be considered acceptable if the cost of mitigation exceeds the potential loss. In such cases, organizations acknowledge the risk and monitor it regularly.

Implementation Steps:

- Identify risks and analyze their potential impact.
- Determine appropriate mitigation options.

- Implement controls and countermeasures.
- Monitor effectiveness and update the strategy.

Risk mitigation helps minimize business disruption, protects data integrity, and ensures legal compliance. It also builds customer trust and organizational resilience. Effective mitigation requires a blend of technological tools, strategic policies, and employee involvement.

4. **Describe Information Access Authorization and its controls.** (2020, 2021)

   Information access authorization is a key aspect of access control in cybersecurity. It defines who is allowed to access specific data or systems and what actions they are permitted to perform. This ensures that only authorized individuals can view or modify sensitive information.

Types of Authorization Controls:

1. **Discretionary Access Control (DAC):** The data owner decides who gets access. It's flexible but less secure.
2. **Mandatory Access Control (MAC):** Access is granted based on classification levels. Often used in government.
3. **Role-Based Access Control (RBAC):** Access is based on the user’s role in the organization. Common in enterprise settings.
4. **Attribute-Based Access Control (ABAC):** Grants access based on attributes such as location, device, and time.

Process:

- **Authentication:** The user must prove identity (e.g., password, biometrics).
- **Authorization:** The system then checks what resources the user can access.

Enforcement Tools:

- Access control lists (ACLs)
- Policy enforcement points (PEPs)
- Identity and Access Management (IAM) solutions

Best Practices:

- Apply the principle of least privilege.
- Conduct periodic access reviews.

- Use multi-factor authentication (MFA).

Proper implementation of access authorization helps prevent data leaks, limits insider threats, and ensures that users only interact with data relevant to their role. It also supports compliance with regulations like GDPR and HIPAA.