1. *What is Information Assurance (IA)?*

**B. Managing risks related to information**

2. *What does Enterprise Information System (EIS) aim to improve?*

**B. Integration of business processes**

3. *How does IA support the goals of EIS?*

**B. By reducing potential risks**

4. *Which of the following is a common cyber threat to EIS?*

**C. Malware**

5. *What is the purpose of an Insider Threat?*

**C. To use authorized access to harm the organization**

6. *What is a data breach?*

**A. Unauthorized access to data**

7. *Which strategy helps ensure Information Assurance in EIS by identifying, assessing, and mitigating risks?*

**C. Implementing a risk management framework**

8. *What is the role of security controls in Information Assurance?*

**C. To implement technical, administrative, and physical protections**

9. *How can organizations detect and respond to cyber attacks effectively?*

**B. By having a process in place for monitoring and responding**

10. *What is the primary focus of Information Assurance?*

**B. Ensuring data integrity, confidentiality, and availability**

## "Information Assurance and Security in Business Processes"

1. *What is the primary goal of Information Assurance (IA)?*

**B. Protecting the confidentiality, integrity, availability, and authenticity of information.**

2. *How does Information Assurance differ from Cybersecurity?*

**A. Information Assurance focuses on risk management, while Cybersecurity focuses on network architecture.**

3. *What is the main focus of Information Security within the context of IA?*

**B. Deploying security solutions, encryption, and policies.**

4. *What is the scope of Information Assurance in comparison to Information Security?*

**A) Information Assurance has a broader scope, while Information Security has a narrower scope.**

5. *What is one operational benefit of Information Assurance mentioned in the presentation?*

B**. Improved customer service**.

6. *What is the significance of end-to-end encryption in Information Assurance?*

**B. It ensures data remains unreadable to unauthorized parties during storage and transmission.**

7. *What does the acronym GRC stand for in the context of Information Assurance?*

**B. Governance, Risk, and Compliance**.

8. *What is the primary goal of the "Confidentiality" pillar in Information Assurance?*

**C. Protecting data from unauthorized access, safeguarding privacy.**

9. *What does "Non-repudiation" mean in the context of the Five Pillars of Information Assurance*?

**C) Ensuring actions within the system are traceable.**

10. *Why is it important to create a security-centric culture throughout an organization, as mentioned in the Responsibility for Information Assurance?*

**C. It ensures information security is an organization-wide responsibility.**

## "Implications for Information Assurance in Inter-Organizational business processes"

1. *Why is Information Assurance (IA) important in inter-organizational business processes*?

**C. To ensure information security**

2. *What is the main role of Information Assurance (IA) in secure data sharing among organizations?*

**C. Implement access controls and encryption**

3. *What does MFA means in Access Control?*

**B. Multi-Factor Authentication**

4. *In Security Protocols and Standards, what is the processes that may require adherance to various security standards and regulations?*

**D. Inter-organizational**

5. *What is an essential measure to protect data during transmission?*

**B. Secure Channels like VPNs**

6. *What should organizations do to ensure the security of third-party organizations involved in inter-organizational processes?*

**C. Assess and manage their security practices**

7. *What is the definition of a third party in the context of Third-Party Risk Management (TPRM)?*

**A. Any external entity, including suppliers, manufacturers, and service providers.**

8. *Data Governance aims to ensure data is:*

**B. Secure, private, accurate, and available.**

9. *What does "IAM" stand for in the context of cybersecurity and IT management?*

**B. Identity and Access Management**

10. *How can an organization promote a security culture?*

**C. By providing cybersecurity training and awareness programs**

11. *According to the statement, what is the scope of data governance?*

**C. Everything related to data security and usability.**

12. *What is the purpose of "Security Awareness" in the statement?*

**C. Educating on security best practices and IA importance.**

13. *It is the promote a culture of security across organizations involved in the process, emphasizing the importance of IA in all activities.*

**B. Cultural Security**

14. *Feedback Loops is an example of feedback mechanisms to continuously improve IA practices based on evolving threats and vulnerabilities.*

**A. True**