To be successful and credible as a security professional, you should understand security in business starting from the ground up. You should also know the key security terms and ideas used by other security experts in technical documents and in trade publications. Security implementations are constructed from fundamental building blocks, just like a large building is constructed from individual bricks.

Information Security

Information security (or infosec) refers to the protection of data resources from unauthorized access, attack, theft, or damage. Data may be vulnerable because of the way it is stored, the way it is transferred, or the way it is processed. The systems used to store, transmit, and process data must demonstrate the properties of security. Secure information has three properties, often referred to as the **CIA Triad**:

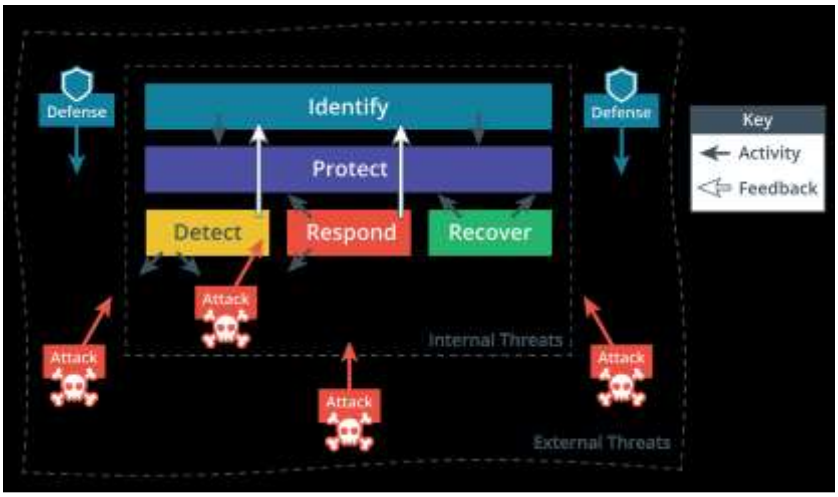
- **Confidentiality** means that certain information should only be known to certain people.
- **Integrity** means that the data is stored and transferred as intended and that any modification is authorized.
- **Availability** means that information is accessible to those authorized to view or modify it.

Non-repudiation
means that a subject cannot deny doing something, such as creating, modifying, or sending a resource. For example, a legal document, such as a will, must usually be witnessed when it is signed. If there is a dispute about whether the document was correctly executed, the witness can provide evidence that it was.

Information security
and cybersecurity tasks can be classified as five functions, following the framework developed by the **National Institute of Standards and Technology (NIST)**

Identify—develop security policies and capabilities. Evaluate risks, threats, and vulnerabilities and recommend security controls to mitigate them.

- Protect—procure/develop, install, operate, and decommission IT hardware and software assets with security as an embedded requirement of every stage of this operations life cycle.
- Detect—perform ongoing, proactive monitoring to ensure that controls are effective and capable of protecting against new types of threats.
- Respond—identify, analyze, contain, and eradicate threats to systems and data security.
- Recover—implement cybersecurity resilience to restore systems and data if other controls are unable to prevent attacks.



Information Security Competencies

IT professionals working in a role with security responsibilities must be competent in a wide range of disciplines, from network and application design to procurement and human resources (HR). The following activities might be typical of such a role:

- Participate in risk assessments and testing of security systems and make recommendations.
- Specify, source, install, and configure secure devices and software.
- Set up and maintain document access control and user privilege profiles.

Monitor audit logs, review user privileges, and document access controls.

- Manage security-related incident response and reporting.
- Create and test business continuity and disaster recovery plans and procedures.
- Participate in security training and education programs.

Information Security Roles and Responsibilities

A security policy is a formalized statement that defines how security will be implemented within an organization. It describes the means the organization will take to protect the confidentiality, availability, and integrity of sensitive data and resources. It often consists of multiple individual policies. The implementation of a security policy to support the goals of the CIA triad might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer. However, each of these organizations, or any other organization (in any sector of the economy, whether profit-making or non-profit-making) should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage.
As part of the process of adopting an effective organizational security posture, employees must be aware of their responsibilities. The structure of security responsibilities will depend on the size and hierarchy of an organization, but these roles are typical.

Overall internal responsibility for security might be allocated to a dedicated department, run by a Director of Security, Chief Security Officer (CSO), or **Chief Information Security Officer (CISO)**. Historically, responsibility for security might have been allocated to an existing business unit, such as Information and Communications Technology (ICT) or accounting.

However, the goals of a network manager are not always well-aligned with the goals of security; network management focuses on availability over confidentiality. Consequently, security is increasingly thought of as a dedicated function or business unit with its own management structure.

- Managers may have responsibility for a domain, such as building control, ICT, or accounting.
- Technical and specialist staff have responsibility for implementing, maintaining, and monitoring the policy. Security might be made a core competency of systems and network administrators, or there may be dedicated security administrators. One such job title is **Information Systems Security Officer (ISSO)**.
- Non-technical staff have the responsibility of complying with policy and with any relevant legislation.
- External responsibility for security (due care or liability) lies mainly with directors or owners, though again it is important to note that all employees share some measure of responsibility.

Information Security Business Units

The following units are ofen used to represent the security function within the organizational hierarchy.

Security Operations Center (SOC)

A **security operations center (SOC)** is a location where security professionals monitor and protect critical information assets across other business functions, such as finance, operations, sales/marketing, and so on. Because SOCs can be difficult to establish, maintain, and finance, they are usually employed by larger corporations, like a government agency or a healthcare company

DevSecOps

Network operations and use of cloud computing make ever-increasing use of automation through software code. Traditionally, software code would be the responsibility of a programming or development team. Separate development and operations departments or teams can lead to silos, where each team does not work effectively with the other.

Development and operations (DevOps) is a cultural shift within an organization to encourage much more collaboration between developers and system administrators. By creating a highly orchestrated environment, IT personnel and developers can build, test, and release software faster and more reliably. Many consider a DevOps approach to administration as the only way organizations can take full advantage of the potential benefits offered by cloud service providers.

DevSecOps extends the boundary to security specialists and personnel, reflecting the principle that security is a primary consideration at every stage of software development and deployment. This is also known as shift left, meaning that security considerations need to be made during requirements and planning phases, not grafted on at the end. The principle of DevSecOps recognizes this and shows that security expertise must be embedded into any development project. Ancillary to this is the recognition that security operations can be conceived of as software development projects. Security tools can be automated through code. Consequently, security operations need to take on developer expertise to improve detection and monitoring.

Incident Response

A dedicated **cyber incident response team (CIRT)**/computer security incident

response team (CSIRT)/computer emergency response team (CERT) as a single point-of contact for the notification of security incidents. This function might be handled by the SOC or it might be established as an independent business unit.

Answer the following questions:

1. **What are the properties of a secure information processing system?**

2. What term is used to describe the property of a secure network where a sender cannot deny having sent a message?

3. A multinational company manages a large amount of valuable intellectual property (IP) data, plus personal data for its customers and account holders. What type of business unit can be used to manage such important and complex security requirements?

4. A business is expanding rapidly and the owner is worried about tensions between its established IT and programming divisions. What type of security business unit or function could help to resolve these issues?