**Elements (Components) Required to Establish and Maintain an ISMS**

1. **Governance Framework**
   * Define the scope and boundaries of the ISMS.
   * Establish governance structures (boards/committees) for information security.
   * Develop and enforce information security policies aligned with business objectives.
2. **Risk Management**
   * Regularly identify and assess information security risks.
   * Develop strategies to handle identified risks (avoidance, transfer, acceptance, mitigation).
   * Implement continuous risk assessment and monitoring.
3. **Information Security Policy**
   * Draft comprehensive information security policies.
   * Ensure all employees are aware of and adhere to these policies.
   * Regularly review and update policies based on organizational needs and threat landscape changes.
4. **Roles and Responsibilities**
   * Define and assign information security roles and responsibilities.
   * Provide regular training and awareness programs for all employees regarding their security duties.
5. **Information Asset Management**
   * Maintain an accurate inventory of information assets.
   * Classify and manage these assets appropriately.
6. **Access Control**
   * Establish and enforce policies for access control.
   * Implement procedures for granting, reviewing, and revoking access.
7. **Incident Management**
   * Develop and maintain an incident response plan.
   * Implement procedures for incident detection, reporting, and resolution.
8. **Business Continuity Management**
   * Conduct business impact analyses to identify critical processes and dependencies.
   * Develop and maintain disaster recovery and business continuity plans.
9. **Compliance and Audit**
   * Ensure compliance with legal, regulatory, and contractual requirements.
   * Perform regular internal audits and management reviews to assess ISMS effectiveness.
10. **Continuous Improvement**

* Monitor and evaluate the ISMS regularly to identify improvement areas.
* Implement corrective and preventive actions to address nonconformities.

1. **Performance Evaluation**

* Identify and monitor Key Performance Indicators (KPIs) for the ISMS.
* Regularly report on information security performance to relevant stakeholders.

1. **Technology-Based Measures**

* Implement technical controls like intrusion detection systems, firewalls, encryption, and anti-malware.
* Regularly maintain and review the effectiveness of these controls

**Processes Required to Establish and Maintain an ISMS (COBIT Framework)**

**1. Evaluate, Direct, and Monitor (EDM)**

The EDM domain focuses on the governance and oversight of IT. It ensures that the IT function aligns with the overall business strategy, delivers value, manages risks effectively, optimizes resources, and provides transparent communication with stakeholders.

**2. Align, Plan, and Organize (APO)**

The APO domain involves strategic planning and organization of IT resources. It ensures that IT strategies are aligned with business goals, establishes a robust IT management framework, manages innovation, controls costs, maintains quality, and ensures security and risk management.

**3. Build, Acquire, and Implement (BAI)**

The BAI domain covers the development and implementation of IT solutions. It ensures that IT projects and programs are managed efficiently, IT solutions are built to meet business needs, changes are managed effectively, and IT assets and configurations are properly controlled.

**4. Deliver, Service, and Support (DSS)**

The DSS domain focuses on the operational aspects of IT. It ensures that IT services are delivered effectively and efficiently, service requests and incidents are managed promptly, problems are resolved, continuity of services is maintained, security services are managed, and business process controls are in place.

**5. Monitor, Evaluate, and Assess (MEA)**

The MEA domain involves monitoring, evaluating, and assessing IT performance and compliance. It ensures that IT performance and conformance to standards are monitored, internal controls are effective, compliance with external requirements is maintained, and business controls provide the necessary assurance.