CU | Coventry
Coventry University Group

CU | London
Coventry University Group

CU | Scarborough
Coventry University Group

Information Security Standards

Introduction to Information Security Standards

- Information Security Standards are guidelines and rules that organizations follow to protect their data and systems from unauthorized access, breaches, and other threats.
- It helps ensure that sensitive information is kept safe and that systems are secure from cyber-attacks.
- Following these standards helps businesses avoid security breaches and maintain trust.

Why Information Security Standards Matter?

- Security breaches can cause financial loss and damage a company's reputation.
- These standards help organizations comply with laws and regulations.
- Customers and partners trust companies that follow security standards.
- Protects personal and business data from unauthorized access.

Overview of ISO/IEC 27001

- ISO/IEC 27001 was created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

- ISO/IEC 27001 is a global standard for managing information security.

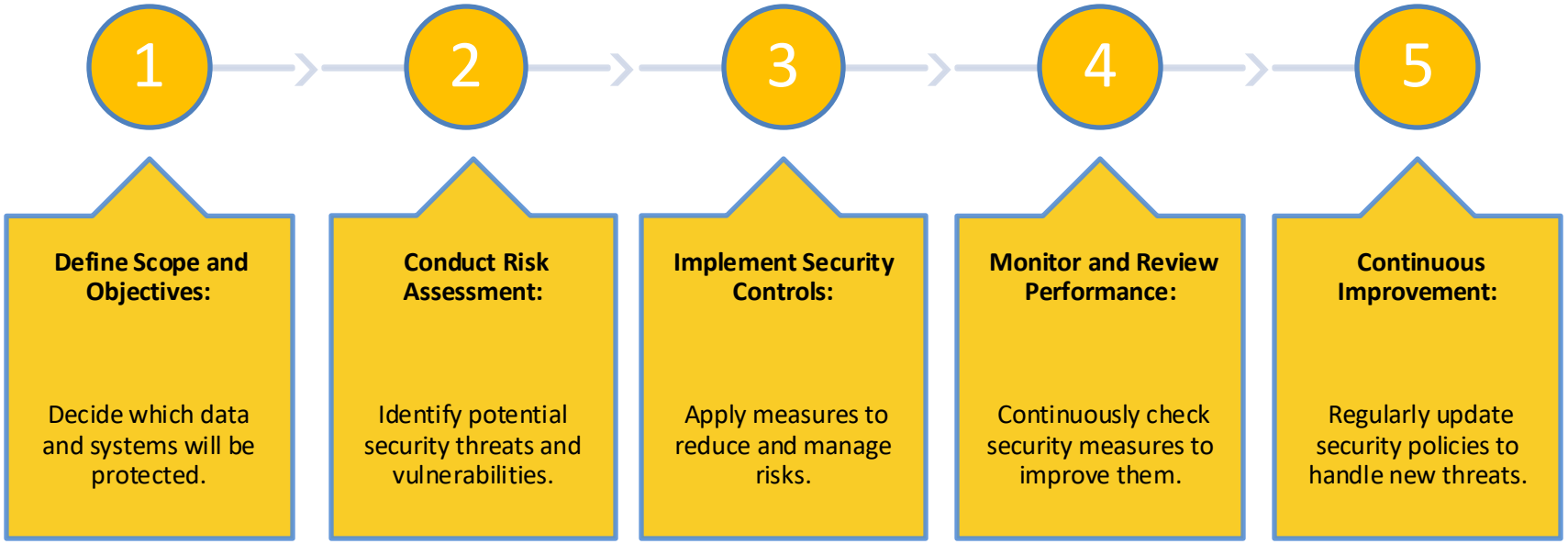
- It provides a framework for organizations to protect their sensitive information, ensuring it's kept safe and secure.

- - The standard includes guidelines on policies, procedures, and controls.
- - Helps organizations prevent security threats and data breaches.

Three Key Principles of ISO/IEC 27001

- **Confidentiality**: Ensuring only authorised people can access sensitive information.
- **Integrity**: Keeping data accurate and trustworthy, preventing unauthorised changes.
- **Availability**: Ensuring data is accessible when needed, without disruptions.
- These principles work together to create a strong security system.

Steps to Implement ISO/IEC 27001



ISO 27001: Risk Management Approach

- Identify Security Risks Before They Cause Damage.

- Assess How Likely Risks Are To Occur And Their Potential Impact.

- Apply Security Measures To Reduce Risks And Prevent Incidents.

- Regularly Monitor Security Risks And Update Controls As Needed.

What is ISO 27005?

- ISO 27005 is a standard that provides guidelines for managing information security risks.

- It helps organizations identify, assess, and treat risks related to the protection of information.

- In simpler terms, it offers a structured approach to understanding potential security threats and vulnerabilities, and how to deal with them to keep information safe.

- It's part of the larger ISO 27000 family of standards, which focus on information security management systems (ISMS).

Risk Assessment in ISO 27005

Risk assessment in ISO 27005 consists of **three key steps**:

1.Risk Identification

1. Identify assets, threats, vulnerabilities, and potential impacts.
2. Understand the scope of the risk assessment.
3. Document security incidents and potential risks.

2.Risk Analysis

1. Determine the likelihood of a risk occurring.
2. Assess the potential impact on confidentiality, integrity, and availability (CIA triad).
3. Use qualitative, semi-quantitative, or quantitative risk analysis methods.

3.Risk Evaluation

1. Compare assessed risks against risk acceptance criteria.
2. Prioritize risks for treatment based on their potential damage.
3. Support decision-making on risk mitigation strategies.

ISO 27005: Risk Treatment Process

Once risks are assessed, ISO 27005 defines the **Risk Treatment Process**, which involves selecting and implementing appropriate security measures. The four main treatment options are:

1.Risk Mitigation (Reduction)

1. Implement security controls to reduce risk to an acceptable level.
2. Example: Deploying firewalls to prevent unauthorized access.

2.Risk Avoidance

1. Modify processes or systems to eliminate the risk.
2. Example: Disabling a vulnerable service rather than trying to secure it.

3.Risk Transfer

1. Shift the risk to a third party through contracts, outsourcing, or insurance.
2. Example: Cyber insurance to cover financial losses from security breaches.

4.Risk Acceptance

1. Decide to tolerate the risk because it falls within acceptable limits.
2. Example: Keeping a minor risk due to cost-benefit considerations.

ISO 27005 vs. ISO 27001: How They Work Together

- ISO 27005 is **not a standalone standard**; it complements **ISO 27001**, which is the main standard for establishing an **Information Security Management System (ISMS)**.

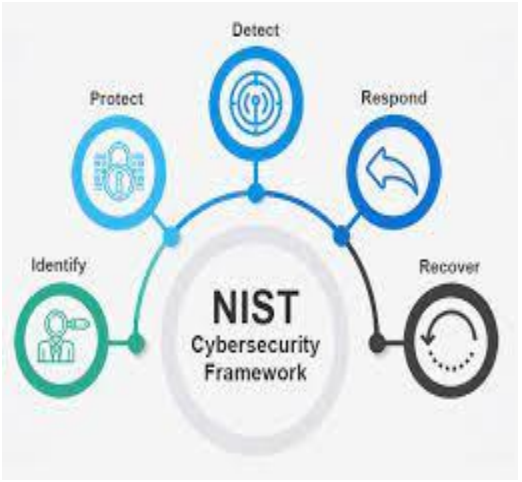
Aspect	ISO 27005	ISO 27001
Focus	Information security risk management	Information Security Management System (ISMS) implementation
Scope	Provides detailed guidance on risk assessment and treatment	Covers a broad ISMS framework, including policies, controls, and continuous improvement
Risk Approach	Defines risk assessment methodologies and treatment strategies	Requires risk management as part of ISMS but does not specify a method
Relationship	Supports ISO 27001 by providing in-depth risk management techniques	Requires risk management but refers to ISO 27005 for detailed implementation

Introduction to NIST SP 800-30

- A risk assessment guideline developed by the U.S. National Institute of Standards and Technology (NIST).
- Helps organizations systematically identify and manage security risks.
- Focuses on evaluating threats, vulnerabilities, and potential impacts.
- Used widely in government agencies and private businesses.

Risk Management Process in NIST SP 800-30

1. **Identify Threats and Vulnerabilities:** Determine what could harm the organization.
2. **Analyses Risks and Their Impact:** Evaluate how serious each risk is.
3. **Determine Risk Mitigation Strategies:** Decide on actions to reduce or eliminate risks.
4. **Monitor and Update Risk Management Plans:** Keep security strategies up to date.



Key Steps in NIST Risk Assessment

- Define scope: Identify what needs to be assessed.
- Gather information on threats and vulnerabilities.
- Analyze risks based on likelihood and impact.
- Create a plan to manage and reduce risks.
- Continuously review and improve security measures.

Comparing ISO 27005 and NIST SP 800-30

- ISO 27005: Provides a structured approach for risk management under ISO 27001.
- NIST SP 800-30: A detailed risk assessment guide commonly used in the U.S.
- Both help organisations identify and manage security risks.
- NIST is often preferred for U.S. government agencies, while ISO 27005 is widely used globally.

Task: NIST 800-30 Risk Assessment for SecureTech Ltd.

Look on AULA for the task

Ref: https://www.nist.gov/privacy-framework/nist-sp-800-30

Best Practices for Risk Management

- Regularly update risk assessments to adapt to new threats.
- Implement strong security controls like firewalls and encryption.
- Educate employees about security risks and safe practices.
- Continuously monitor security systems to detect vulnerabilities.

Common Challenges in Implementing Standards

- High implementation costs can be a barrier for small businesses.
- Employees may resist changes to security policies.
- Cyber threats constantly evolve, requiring ongoing updates.
- Ensuring compliance with multiple regulations can be complex.