iGUIDE

ISMS

Information Security Competency Skills

iNFOSECBASE

Contents

A Guide to Information Security Competency Skills

Introduction

An ISO 27001 Competencies Register is a structured document that outlines the essential skills, knowledge and expertise required for personnel involved in managing and maintaining an Information Security Management System (ISMS). Ensuring that employees have the necessary competencies is a key requirement of ISO 27001:2022, particularly under Clause 7.2: Competence.

This register helps organisations identify skill gaps, plan targeted training and demonstrate compliance with regulatory and certification requirements. By mapping roles to specific competencies, organisations can strengthen their information security posture and ensure that all personnel, from general employees to specialised IT security teams, are equipped to handle security-related responsibilities effectively.

Competency Skills

General Information Security Awareness

For All Staff

- Understanding of information security principles
- Awareness of ISO 27001 policies and procedures
- Identifying and reporting security incidents
- Phishing and social engineering awareness
- Data classification and handling

ISMS Leadership & Governance

For ISMS Owners, Top Management and Security Officers

- Knowledge of ISO 27001 requirements and Annex A controls
- Understanding of risk management frameworks
- Security policy development and enforcement
- Business continuity and disaster recovery (BCP/DRP)
- Compliance with legal, regulatory and contractual requirements (e.g. GDPR, HIPAA, PCI-DSS)
- Security governance and oversight

Risk Management & Compliance

For Risk Managers & Compliance Officers

- Risk identification, assessment and treatment (ISO 27005 methodology)
- Understanding of information asset management and risk register maintenance
- Conducting internal security audits (ISO 19011 guidelines)
- Handling non-conformities and corrective actions
- Security incident and breach management processes

IT & Cybersecurity

For IT, Network and Security Teams

- Implementation of ISO 27001 Annex A security controls
- Access control and identity management (IAM, MFA, Role-Based Access Control [RBAC])
- Network security (firewalls, IDS/IPS, secure configurations)
- Cryptographic controls (encryption, hashing, PKI)
- Vulnerability management and penetration testing
- Secure software development (SDLC, DevSecOps, OWASP)
- Cloud security (AWS, Azure, Google Cloud security principles)

Incident Response & Business Continuity

For Incident Response Teams & BCP Managers

- Security incident detection, reporting and response handling
- Digital forensics and root cause analysis
- Disaster recovery planning and execution
- Crisis communication and stakeholder management
- Conducting security incident training/BCP testing and simulations

Vendor & Third-Party Security Management

For Procurement & Vendor Managers

- Third-party risk assessment and supplier due diligence
- Security requirements in contracts and SLAs
- Vendor compliance monitoring and audits

Security Awareness & Training

For HR & Training Coordinators

- Developing and delivering security awareness training
- Tracking and logging employee security competencies and training records
- Conducting phishing simulations and awareness campaigns

Summary

The ISO 27001 Competencies Register categorises required skills across various domains, including information security governance, risk management, IT security, incident response, business continuity and vendor management. It ensures that employees possess the necessary expertise to implement and maintain security controls, manage risks, respond to incidents and comply with legal and regulatory requirements.

By maintaining a well-documented competencies register, organisations can:

- Ensure compliance with ISO 27001 requirements
- Identify and address training needs
- Improve security awareness across all staff levels
- Strengthen incident response and risk management capabilities
- Support continuous improvement in information security practices

A structured approach to tracking competencies helps organisations maintain a robust ISMS, reducing security risks and fostering a culture of information security awareness.