iGUIDE

ISMS

Information Security Business Continuity Planning

iNFOSECBASE

Contents

A Guide to Business Continuity Planning

Introduction

Business continuity planning is a critical aspect of ISO 27001, ensuring that organisations can sustain essential operations and protect information assets during and after disruptions.

Annex A control A.5.30 (ICT readiness for business continuity) of the standard emphasises the importance of having robust strategies to maintain the availability, integrity and confidentiality of information, even in the face of unforeseen events such as cyberattacks, natural disasters or system failures.

A well-developed business continuity plan supports the overall goals of the Information Security Management System (ISMS) whereby organisations can minimise downtime, reduce the impact of disruptions and demonstrate resilience. This guide explores the key principles and steps involved in developing an effective ISO 27001-compliant business continuity plan.

Importance of Business Continuity Planning in ISO 27001

Business continuity planning ensures:

- Critical business functions are maintained during incidents such as cyberattacks, natural disasters or system failures.
- Information security objectives, such as confidentiality, integrity and availability, are not compromised.
- Compliance with ISO 27001 requirements and stakeholder expectations.
- A structured approach to managing disruptions with minimal impact on operations.

Key Elements of ISO 27001 Business Continuity Planning

Understanding the Organisation

- Identify critical business processes and supporting resources, including people, technology and data.
- Conduct a Business Impact Analysis (BIA) to evaluate the potential impact of disruptions on operations and identify recovery priorities.

Risk Assessment and Treatment

- Assess risks that could disrupt business operations, such as cyber threats, natural disasters or supply chain failures.
- Implement risk treatment measures to mitigate these risks, such as redundancies, backups or alternate suppliers.

Developing the Business Continuity Plan

- Define strategies for maintaining or restoring critical operations during a disruption.
- Include procedures for communication, resource allocation and decision-making.

- Ensure the plan aligns with organisational objectives and information security requirements.

Disaster Recovery Plan (DRP)

- Integrate disaster recovery planning into the overall business continuity strategy.
- Focus on restoring IT systems, applications and data necessary to support critical operations.
- Specify recovery time objectives (RTOs) and recovery point objectives (RPOs).

Testing and Validation

- Regularly test the business continuity and disaster recovery plans to ensure they are effective.
- Conduct drills, simulations and tabletop exercises to validate the plans and identify areas for improvement.

Training and Awareness

- Provide training to employees and stakeholders on their roles and responsibilities during a disruption.
- Foster awareness of business continuity procedures across the organisation.

Continual Improvement

- Review and update the business continuity plan regularly to reflect changes in the organisation, technology or external threats.
- Learn from past incidents and incorporate lessons learned into the plan.

Steps to Implement ISO 27001-Compliant Business Continuity Plans

Establish a Business Continuity Policy

- Define the organisation's commitment to business continuity and its objectives.

Integrate with the ISMS

- Align business continuity plans with the broader ISMS to ensure a cohesive approach to risk management and resilience.

Engage Stakeholders

- Involve relevant stakeholders, including management, IT teams and external partners, in the planning and implementation process.

Monitor and Evaluate

- Use key performance indicators (KPIs) to monitor the effectiveness of the business continuity plan.
- Conduct regular audits to assess compliance with ISO 27001 requirements.

Benefits of Business Continuity Planning

- **Minimised Downtime**: Ensures critical operations can continue or resume quickly during disruptions.

- **Enhanced Resilience**: Strengthens the organisation's ability to respond to and recover from incidents.
- **Improved Stakeholder Confidence**: Demonstrates a commitment to protecting services, information and assets.
- **Regulatory Compliance**: Meets ISO 27001 requirements and other legal or contractual obligations.
- **Cost Savings**: Reduces financial and reputational losses associated with extended downtime or data breaches.

Summary

By integrating business continuity planning into an ISO 27001-compliant ISMS, organisations can build resilience, ensure operational continuity and maintain stakeholder trust. A proactive approach to planning, testing and improving business continuity measures helps organisations stay prepared for disruptions while safeguarding critical assets and services.

Business continuity planning is a vital part of ISO 27001, focusing on maintaining critical operations and protecting information assets during disruptions. Control A.5.30 emphasises the need for strategies that ensure the availability, integrity and confidentiality of information in scenarios like cyberattacks, natural disasters or system failures.

Effective planning involves identifying critical processes, assessing risks and creating actionable plans, including disaster recovery measures. Regular testing, stakeholder involvement and continuous improvement are essential to ensure readiness.