INFORMATION SECURITY MANAGEMENT REPORT

For Aviva plc, Ireland.

Standard Applied: ISO/IEC 27001:2022

SUMMARY

This is an ISM report which shows a comprehensive security framework for Aviva plc, one of the largest financial and insurance companies in Europe, serving countries like the United Kingdom, Ireland, and Canada. (Wiki 2025). As a large-sized company managing sensitive data for over 25 million customers in different countries, Aviva faces many information security challenges, and these would require proper handling and security management methods.

This report applies ISO/SEC 27001:2022, the internationally recognized standard for information security management systems, to develop a tailored ISM structure for Aviva, aligned with its organizational structure and security needs. This ISO 27001 framework addresses certain areas of the organization that should be regulatory-compliant and have quality security management, given their role as a financial service provider within the EU region.

Key Components of this ISM framework include:

- Clearly defined scope stating Aviva's operations, customer data processing systems, and their critical IT infrastructure.
- Aviva's structure with their security hierarchy from the lowest to the highest levels
- Risk plans approach and objectives based on the ISO 27001 requirements
- Detailed roles and responsibilities across all organizational levels, ensuring accountability
- Continuous monitoring and assessment of the security measures to ensure and maintain security
- Structured improvement methods to adapt and get better with security and threat occurrences.

In general, this report shows how ISO 27001 influences and strengthens Aviva's security and compliance with EU standard policies. By implementing this framework, Aviva can achieve high compliance with policy, get a better security structure, protect customer data, and get a competitive advantage in the global market.

I'll be using the PDCA method for structuring this project: PLAN – DO – CHECK – ACT.

PLAN (Define scope, assess risks, set objectives); - DO (Set roles, implement controls, train people) – CHECK (Monitor and assess implemented actions) – ACT (improve based on evaluation)

1. INTRODUCTION

1.1. About Aviva Plc (Wikipedia 2025)

Aviva plc is a British multinational insurance company headquartered in London, England, and is a constituent of the FTSE 100 Index. It has a history dating back to the establishment of the Hand in Hand Fire & Life Insurance Society in 1696, making it over three centuries old. It was created by the merger of two British insurance firms, Norwich Union and CGU plc (itself created by the 1998 merger of Commercial Union and General Accident), as CGNU in February 2000. The name 'Aviva' was adopted in July 2002. Today, Aviva operates as one of the world's leading insurance groups, providing life insurance, pensions, and general insurance products to approximately 25 million customers across its core markets in the United Kingdom, Ireland, and Canada.

As of 2024, Aviva employs approximately 23,000 personnel and reported revenues of £20.747 billion, with total assets under management exceeding £533 billion. The company is led by CEO Amanda Blanc and Chairman George Culmer, and operates through several principal subsidiaries, including Aviva Investors (fund management), Aviva Insurance (general insurance), and specialized divisions for life insurance and retirement products.

The company processes and stores large quantities of highly sensitive personal and financial data, including:

• Customer personal identifiable information (PII) for policy administration

• Financial transaction data, including bank account details and payment card information

• Medical and health information for life insurance

• Investment portfolio data for pension and wealth management clients

• Proprietary business intelligence, including pricing algorithms and risk models.

This amount of sensitive data makes Aviva a target for various threat factors, including cybercriminals, attacks from competitors, and insider threats. A security breach would have major consequences, including large regulatory fines (GDPR penalties of up to €20

million or 4% of global annual revenue), customer lawsuits, reputational damage that could lead to a loss of customer trust, and potential disruption to critical business operations.

1.2. The importance of ISM in Aviva

As explained above, within the large-scale scope of Aviva's business organization, it's an attractive target for all forms of policy non-compliance threats. And a systematic ISM (Information Security Management) structure will provide a more secure system that meets all GDPR (General Data Protection Regulation) requirements and protects the organization from all threats.

1.3. Why I chose ISO/IEC 27001:2022 for Aviva

I used the ISO/IEC 27001:2022 for Aviva because of certain factors, which include:

a) International Recognition and Credibility

ISO 27001 is the globally recognized standard for information security management, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The standard is used by organizations worldwide, providing a common framework that facilitates communication with regulators, business partners, and customers across international borders. (IBM, 2025) This is particularly relevant to Aviva's operations, which are across multiple countries.

b) Regulatory Alignment with CBI

The ISO 27001 is the ISM that helps financial firms meet the CBI (Central Bank of Ireland) regulatory and operational requirements, as the CBI is the topmost financial regulator in Ireland (Centralbank.ie, No year)

c) Risk-Based Approach

ISO 27001 aligns with the ISO 3000 risk management principles, mainly to identify specific assets or processes that require security, assess their possible threats and risks, and then find the most appropriate way to handle them, rather than a broad out-of-bounds control format. This is needed to assess Aviva's risk profile.

d) Comprehensive Coverage

The standard addresses all the needed ISM aspects, and I'll be drafting them as follows:

- Scope Definition (ISO 27001 Clause 4.3)

- Leadership and Organizational Structure (ISO 27001 Clause 5)
- ISM Planning (ISO 27001 Clause 6)
- Support (Clause 7)
- Operational Implementation (ISO 27001 Clause 8)
- Performance Evaluation and Monitoring (ISO 27001 Clause 9)
- Continual Improvement (ISO 27001 Clause 10)

1. SCOPE DEFINITION (ISO 2701 CLAUSE 4)

1.1. Define Scope

ISO/IEC 27001:2022 Clause 4.3 – "**Determining the scope of the information security management system**"

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining scope, the organization shall consider:

a) External and internal issues referred to in 4.1
b) the requirements referred to in 4.2 (interested parties)
c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations

The scope shall be available as documented information.

This clause requires the organization to determine the boundaries and applicability of the information security management to establish its scope.

This means that a company cannot effectively protect everything at once. There has to be a defined area on which the company should focus its security implementation to protect its critical assets and processes efficiently. On the other hand, if the company decides to overhaul everything and go beyond its boundaries, it might be expensive and, in the end, may not reach the critical aspects that are unachievable. (Intertek 2022)

For Aviva, with its large organization size, operations across different countries, and extensive daily data operations, a scope that is too broad without specification would be impossible to implement and maintain, while one that is too narrow would miss critical regulatory policies. So there has to be a balance.

1.2. Proposed Scope for Aviva Ireland. (HighTable, 2025)

The organization shall determine the boundaries and applicability of the information security management system to establish its scope

The ISMS shall apply to the following areas within Aviva.

- Geographic Scope – Irish office operations
- Business/Service Processing Scope – Only direct business processes involving the customers and product/service delivery
- Information Assets – All relevant data handled by Aviva (Customers' data, authentication credentials, intellectual property, etc.)
- Technology systems – Technologies and methodologies used in Aviva for productivity (Customer relationship management (CRM) systems, Cloud services, Network infrastructure, etc.)

1.3. Application of ISO 27001 Clause 4.3 Requirements (Scope) to Aviva.

1.3.1. *The external and internal issues referred to in 4.1 (4.3 a)*

Consideration / Identification of External Issues (Canwaygo, 2025)

- Regulatory Changes: Changes in GDPR, DORA laws for handling data; Brexit effects on cross-border data handling.
- Technological Advancements: New emerging technologies and their adoptions (AI, cloud services, etc.); New threats created because of these technological advancements
- Economic Conditions: How the current economy affects the business and its security impact. A poor economy may lead to low security strategies, causing vulnerability, and vice versa.
- Supply Chain Issues: Reliance on external 3rd party service providers has a significant effect on the organization

Consideration / Identification of Internal Issues (Canwaygo, 2025)

- People: The Level of security knowledge and skills among employees is necessary; a lack of it may lead to a data breach.
- Lack of Regular Review/Updates: This can lead to outdated security management, causing vulnerability to threats/attacks.
- Poor organizational structure/communication: Without a proper hierarchy, the workflow would be scattered, leading to security issues within the organization

- Inadequate Resource allocation: Limited budget on security measures can lead to security gaps; providing adequate funding for security systems within the organization is very important.

1.3.2. *The requirements referred to in 4.2 (4.3 b)*

Understanding the Expectations of Interested Parties (Stakeholders)
Aviva is expected to understand and meet the expectations of its interested parties, which include: (Pretesh Biwas, 2025)

- Regulators (CBI) – Expect compliance with local and global laws and policies.
- Customers/Clients – Expect confidentiality, integrity, and availability of personal and financial data.
- Shareholders – Expect protection on investment
- Employees – Expect a safe and healthy work environment
- Competitors – Expect fair competition based on environmental regulations

1.3.3. *Interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations (4.3 c)*

Dependencies: processes that are provided from outside the company's scope, third parties
Interfaces: helps the company process which input and output would be going in or out of the ISM boundaries to the dependencies (Intertec International, 2021)
Aviva should have security information regarding the data exchanges between these interfaces.

- Technology Interface – Cloud services processing on behalf of Aviva, APIs for data exchange; Email and communication systems; 3rd party connection (VPNs).
- Process Interfaces – Legal / Regulatory reporting to the govt/agencies; HR Processes for employee data handling; Customer Interaction process
- People Interface – Physical AP like authorized offices, Employee Access to the organizational data; Third Party Access used by third-party staff to access the organization's facilities.

1.3.4. The scope shall be available as documented information. (4.3)

The Information Security Committee within Aviva should Document and Communicate the Scope thus: (Pretesh Biswas, 2023)

- Document all required scope areas, outlining organizational boundaries, information assets, etc.
- Publish a formal ISMS Scope Statement document approved by the Board Information Security Committee
- Make the scope statement accessible to all personnel involved in ISMS implementation and operation
- Clearly communicate the established scope to all relevant stakeholders
- Regularly review and update ISMS scope annually or when needed

2. LEADERSHIP AND ORGANIZATIONAL STRUCTURE (ISO 27001 CLAUSE 5)

2.1. The Critical Role of Leadership and Organizational Structure in an Organization's ISM

This clause explicitly defines top management responsibilities, establishes the general roles and responsibilities for the ISMS, and specifies the contents of the top-level Information Security Policy. Without leadership and an organizational hierarchy, information security risk management is relegated to technical personnel who are unaware of business objectives, inadequately informed, and unable to lead necessary change. (Advisera, 2025)

This clause is important because it requires companies to define clear primary security responsibilities and for a major company like Aviva, lack of proper leadership compliance could result in a security breach which could lead to fatal consequences.

2.2. ISO 27001 Clause 5.1: Leadership and Commitment Requirements

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

1) *ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;*
2) *ensuring the integration of the information security management system requirements into the organization's processes;*
3) *ensuring that the resources needed for the information security management system are available;*

4) *communicating the importance of effective information security management and of conforming to the information security management system requirements;*
5) *ensuring that the information security management system achieves its intended outcome(s)*
6) *directing and supporting persons to contribute to the effectiveness of the information security management system;*
7) *promoting continual improvement; and*
8) *supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.*

Application of ISO 27001 Clause 5.1 Requirements to Aviva's Leadership and Organization's Management

Aviva's Board Information Security Committee and relevant top management should ensure that all information security objectives align with business goals such as digital transformation, customer experience enhancement, and operational efficiency. It also requires that leadership demonstrate a genuine effort to engage people and other relevant management leaders in supporting the ISMS.

2.3. ISO 27001 Clause 5.2: Policy Requirements

Top management is to establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system.

The information policy shall:

e) be available as documented information;

f) be communicated within the organization;

g) be available to interested parties, as appropriate.

Application of ISO 27001 Clause 5.2 Requirements to Aviva's Leadership and Organization's Management

This clause requires that Aviva's top management must establish information security policies and frameworks, which align with the organization's purposes and provide a framework for setting information security objectives, including a commitment to fulfill applicable requirements and the continual improvement of the ISMS. (Advisera, 2025)

There are 3 major types of security policies that Aviva can set up to achieve this: (Varonis, 2024)

- Program policies (highest level); Aviva can set this up to state general security commitments and to demonstrate transparency. They can be available in Aviva's internal communications, annual reports
- Issue/Topic-specific policies: These are detailed polices used to address specific security areas. Like the data privacy (email-specific) topic within Aviva's organization.
- System-specific policies - cover specific technical procedures or individual computer systems like firewalls and web servers. E.g., Server hardening standards

2.4. ISO 27001 Clause 5.3: Organizational Roles, Responsibilities, and Authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this document;

b) reporting on the performance of the information security management system to top management

Application of ISO 27001 Clause 5.2 Requirements to Aviva's Leadership and Organization's Management

For Aviva, this clause means explicit documentation and implementation of security responsibilities in role descriptions:

Every job includes a security Responsibilities and is only implemented by the responsible personnel, for example:

- Coordination of the ISMS so that it is compliant with ISO 27001 is usually performed by a security manager (e.g., CISO)
- Performing regular security activities (e.g., backup) – this is usually done by everyone in the company

Finally, these tasks are to be submitted and audited by an auditor. (Advisera 2025)

3. PLANNING (ISO 27001 CLAUSE 6)

Planning is the Foundation of ISM

Instead of implementing every possible security control regardless of actual risk, this ISM clause requires that organizations understand their specific risk context, assess which risks require treatment, and, more importantly, "plan" appropriate responses. This risk-based approach is particularly suitable for a financial organization like Aviva, where risk management is very important.

There are 3 sub-clauses:

3.1. ISO 27001 Clause 6.1 Actions to address risks and opportunities

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects;

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

1) integrate and implement the actions into its information security management system

processes; and

2) evaluate the effectiveness of these actions

Application of ISO 27001 Clause 6.1 Requirements to Aviva's ISM Planning

This clause requires Aviva to analyze and manage risks and opportunities relevant to the specified context of the organization (4.1 - internal and external issues) and (4.2 - the needs and expectations of interested parties), as a way to ensure that the ISMS plan can achieve its objectives, prevent or mitigate undesired consequences, and continually improve.

3.2. ISO 27001 Clause 6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1) the risk acceptance criteria; and

2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

2) identify the risk owners;

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

Aviva's Risk Assessment Methodology

Aviva should assess risk information security objectives and define a plan on how to achieve them. (Advisera 2025)

For example, it should follow the steps:

- Asset Identification: Identify assets within the planned scope
- Threat and Vulnerability Analysis: For each asset, analyze potential threats
- Identify the Vulnerability impact level
- Treat in order of importance

3.3. ISO 27001 Clause 6.1.3: Information Security Risk Treatment

the organization shall define and apply an information security risk treatment process. The organization must:

a) Select appropriate information security risk treatment options considering risk assessment results

b) Determine all controls necessary to implement risk treatment options

c) Compare controls determined in 6.1.3 b) above with those in Annex A and verify no necessary controls have been omitted

d) Produce a Statement of Applicability containing necessary controls and justification for inclusions, whether implemented, and justification for exclusions of Annex A controls

e) Formulate an information security risk treatment plan

f) Obtain risk owners' approval of the risk treatment plan and acceptance of residual risks.

Aviva's Risk Treatment

This means that Aviva will have to choose the necessary risk treatment options based on the risk assessment results, which include: (HighTable, 2025)

- Accepting the Risk
- Treating the Risk
- Mitigating the Risk
- Transferring the Risk
- Avoiding the risk

3.4. ISO 27001 Clause 6.2: Information Security Objectives and Planning to Achieve Them

It requires the organization to establish measurable information security objectives at relevant functions and levels. These objectives must:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

h) what will be done;

i) what resources will be required;

j) who will be responsible;

k) when it will be completed; and

l) how the results will be evaluated.

Aviva's Information Security Objectives

For this clause, Avira should establish information security objectives, define the plan on how to achieve them, manage and monitor these objectives.

3.5. ISO 27001 Clause 6.3: Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner

Aviva’s Plan for Changes

Aviva has to plan before any change in policy or procedure, especially on the consequences of such a change, so the proper steps to follow to achieve this clause include: (Advisera, 2025)

- Define what level of changes needs to be controlled
- Define who is authorized to make significant changes
- Define the decision to be made by the authorized person

4. OPERATIONS (ISO 27001 CLAUSE 8)

ISO 27001 Clause 8 requires organizations to plan, implement, and control processes needed to meet information security requirements. And, for Aviva, this clause is very important because they will show how the organization executes the ISMS plan through daily security activities.

4.1. Clause 8.1 — Operational planning and control

The organization shall plan, implement, and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

- *establishing criteria for the processes;*
- *implementing control of the processes in accordance with the criteria.*

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products, or services that are relevant to the information security management system are controlled.

4.2. Clause 8.2 — Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2a).
The organization shall retain documented information of the results of the information security risk
assessments.

4.3. Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

Key Operational Controls for Aviva

Avira should be able to define its operational control according to the required criteria, based on ISMS requirements, perform risk assessments at a planned interval, and implement the generated Risk Treatment plan.

5. PERFORMANCE EVALUATION AND MONITORING (ISO 27001 CLAUSE 9)

This part deals with systemic monitoring, measurement, analysis, evaluation, and internal audit of the ISMS to ensure it's achieving its intended outcome. (Advisera, 2025)

5.1. Clause 9.1 — Monitoring, measurement, analysis, and evaluation

The organization shall determine:
a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid.
c) when the monitoring and measuring shall be performed;
d) who shall monitor and measure;
e) when the results from monitoring and measurement shall be analyzed and evaluated;
f) who shall analyze and evaluate these results.
Documented information shall be available as evidence of the results.
The organization shall evaluate the information security performance and the effectiveness of the information security management system.

Aviva's Expectation

The organization should establish KPI (Key Performance Indicators) to track the security effectiveness as stated in this clause. (Advisera, 2025)

5.2. Internal Audit (Clause 9.2)

1) 9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to
1) the organization's own requirements for its information security management system;

2) 9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit program (s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit program(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit program (s) and the audit results.

Aviva's Audit Method

The organization is expected to conduct annual internal audit, at planned intervals, assess the implementation and maintenance of the ISMS in use, and comply with ISO 27001. (Advisera, 2025)

5.3. Management Review (Clause 9.3)

1) 9.3.1 General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

2) 9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

3) Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Aviva's Expectations Based on Clause 9.3
Aviva is expected to ensure that top management is regularly engaged with the ISMS performance, so that it is always effective in achieving the information security objectives.

6. Improvement (ISO 27001 CLAUSE 10)

6.1. Continual Improvement (Clause 10.1)

The organization shall continually improve the suitability, adequacy, and effectiveness of the information security management system.

6.2. Nonconformity and corrective action (Clause 10.2)

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it;

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.

Aviva's Clause 10, Continual ISMS Improvement

Aviva can stand out as a policy-compliant organization by implementing the necessary controls, taking corrective actions to mitigate risks, and continually improving its ISMS to achieve appropriate security and boost performance. (Advisera, 2025)

CONCLUSION

This report shows a comprehensive Information Security Management framework for Aviva plc, based on ISO/IEC 27001:2022 requirements. The framework addresses the specific security challenges facing the major financial services organization based in Ireland, handling sensitive data for over 25 million customers globally.

Key accomplishments of this structure as based on the ISO 27001 approach, include:

Structured Governance: Appropriately implementing the Organization hierarchy would help define the key responsibilities and roles.

Comprehensive Scope: Clearly defining the scope or specific area for compliance would save time, costs, and resources, and ensure that the appropriate data, procedures, and applications are secured

Control Implementation: Practical implementation of security measures, as seen in clause 8, like training staff, setting up firewalls, etc., as required to ensure policy adherence, helps make the entire process achievable and faster.

Continuous Monitoring: Constant monitoring and checking of the KPI, internal audits, and management review as per clause 9, ensures that the ISMS is working and achieving the intended outcomes

Adaptive Improvement: Continuous correction and improvement process as per Clause10 ensure that Aviva is evolving with new policy requirements and threat changes rather than staying stagnant and outdated.

References

IBM, What is ISO 27001?, https://www.ibm.com/products/cloud/compliance/iso-27001, 2025; Accessed at:

Centralbank.ie, Banking & Payments Federation Ireland, https://www.centralbank.ie/docs/default-source/publications/discussion-papers/discussion-paper-8/bpfi-response-to-dp8.pdf, Pg 8. Accessed at: 08/11/2025.

HighTable, How to Define ISO 27001 Scope with Examples and Template, https://hightable.io/how-to-define-iso-27001-scope/, May 10, 2025, Accessed at: 08/11/2025.

Canwaygo, ISO 27001 Clause 4.1 Understanding The Organization And Its Context, https://www.canwaygo.com/iso-27001-clause-4-1-understanding-the-organisation-and-its-context/, 2025, Accessed at: 08/11/2025.

PRETESH BISWAS, ISO 14001:2015 Clause 4.2 Understanding the needs and expectations of interested parties, https://preteshbiswas.com/2023/09/07/iso-140012015-clause-4-2-understanding-the-needs-and-expectations-of-interested-parties/, 2023, Accessed at: 08/11/2025.

Intertec International, Defining The Scope of Your ISMS For ISO 27001 Certification, https://blog.intertecintl.com/defining-the-scope-of-your-isms-for-iso-27001, 2021. Accessed at: 08/11/2025

Advisera, ISO 27001 clause 5 Leadership, https://advisera.com/iso27001/clause-5-leadership/, 2025. Accessed at: 08/11/2025.

Varonis, What is a Security Policy? Definition, Elements, and Examples, https://www.varonis.com/blog/what-is-a-security-policy, 2024. Accessed at: 08/11/2025

Advisera, ISO 27001 clause 5.3 Organizational roles, responsibilities and authorities, https://advisera.com/iso27001/clause-5-3-organizational-roles-responsibilities-and-authorities/, 2025. Accessed at: 08/11/2025

HighTable, ISO 27001:2022 Clause 6.1.3 Information Security Risk Treatment Explained, https://hightable.io/iso-27001-clause-6-1-3-information-security-risk-treatment/, 2025. Accessed at: 08/11/2025

Advisera, ISO 27001 clause 6.3 Planning of changes, https://advisera.com/iso27001/clause-6-3-planning-of-changes/, 2025. Accessed at: 08/11/2025

Advisera, ISO 27001 clause 9 Performance evaluation, https://advisera.com/iso27001/clause-9-performance-evaluation/, 2025. Accessed at: 08/11/2025

Advisera, ISO 27001 clause 9.2 Internal audit, https://advisera.com/iso27001/clause-9-2-internal-audit/, 2025. Accessed at: 08/11/2025

Advisera, ISO 27001 clause 10 Internal audit, https://advisera.com/iso27001/clause-10-2-nonconformity-and-corrective-action/, 2025. Accessed at: 08/11/2025