Using FAIR to Be Compliant on ISO/IEC 27001

A Practical Guide

March 17, 2025

Authors:

Heather Dart, Ph.D.
Cybersecurity Risk Lead
Danaher Corporation
heather.dart@danaher.com

Jack Jones
Chair, Standards Committee
FAIR Institute
jjones@fairinstitute.org

Pankaj Goyal
Director, Standards & Research
FAIR Institute
pankaj@fairinstitute.org

Michael Smilanich
Risk Advisory Manager
Safe Security
michael.s@safe.security

Todd Tucker
Managing Director
FAIR Institute
TTucker@FAIRInstitute.org

Table of Contents

Introduction

ISO/IEC 27001:2022 ("ISO 27001") is the globally recognized standard for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). It provides organizations with a structured approach to managing information security risks. However, many organizations encounter challenges in adopting ISO 27001, including difficulty in interpreting its requirements, integrating it with existing security frameworks, and maintaining continuous compliance.

The FAIR Cyber Risk Management Framework (FAIR-CRMF) enhances ISO 27001 implementation by offering a structured, quantitative approach to cyber risk assessment and decision-making. By applying FAIR-CRMF, organizations can define their ISMS scope more effectively, adopt a truly risk-based approach to security, and ensure that investments in security controls align with business objectives. This white paper explores these common adoption challenges and demonstrates how FAIR-CRMF provides the necessary tools and methodologies to overcome them.

Why ISO/IEC 27001 Matters

ISO/IEC 27001 has become an essential standard for organizations seeking to establish a strong security posture and meet regulatory or contractual obligations. It provides a comprehensive framework for managing information security risks, ensuring that organizations can:

- Protect sensitive data from unauthorized access and breaches.
- Meet compliance requirements and regulatory expectations.
- Strengthen business resilience against cyber threats.
- Enhance trust with customers, partners, and stakeholders by demonstrating a commitment to security best practices.

For many companies, achieving ISO 27001 certification is not just a matter of improving security—it is a business necessity. Clients, regulators, and industry standards often require compliance with ISO 27001 as part of doing business, particularly in highly regulated sectors such as finance, healthcare, and technology.

Key Challenges in Adopting ISO 27001

Despite its benefits, implementing ISO 27001 is not without challenges. Organizations often face hurdles that can complicate the adoption process, including:

1. **Interpreting ISO 27001 Requirements** – The standard provides high-level guidance rather than prescriptive steps, leaving organizations struggling to determine how best to implement

its requirements. This is particularly true of ISO's risk management requirements, which depend on implementation details that are beyond the scope of ISO 27001 or ISO 27005.

2. **Shifting to a Risk-Based Approach** – Many businesses approach the ISO standards as a compliance exercise rather than using it to drive strategic, risk-based decision-making. Instead, risk management should be the goal, with ISO providing guidance on how to improve risk management. A checklist approach rarely achieves risk management in a cost-effective manner.

3. **Integrating with Existing Security Frameworks** – Organizations that already follow NIST CSF, SOC 2, CIS Controls, or other frameworks must navigate overlapping requirements and avoid duplication of effort.

4. **Defining and Implementing ISMS Scope** – Determining the appropriate scope for an ISMS can be complex, and errors in scoping can lead to security gaps or unnecessary controls.

5. **Sustaining Continuous Compliance** – ISO does not prescribe a one-time certification; it requires ongoing risk assessments, audits, and continuous improvement, which many organizations struggle to maintain without the proper data, metrics, systems, processes and people.

ISO/IEC 27005 and Its Role in Risk Management

ISO/IEC 27005 is a complementary standard that provides detailed guidance on information security risk management within the ISO 27001 framework. It outlines best practices for:

- Identifying, analyzing, and evaluating information security risks.
- Establishing and maintaining a risk treatment process.
- Defining roles and responsibilities for effective risk management.
- Supporting decision-making with structured risk assessment methodologies.

While ISO 27005 offers a comprehensive risk management approach, it does not prescribe a specific method for quantifying risk. This is where FAIR-CRMF enhances ISO 27005 by providing a structured, quantitative model for assessing risk in financial terms. FAIR helps organizations apply a more precise, consistent, and defensible methodology to risk analysis, bridging the gap between high-level risk management principles and practical, data-driven decision-making.

ISO 27001 Benefits of the FAIR CRM Framework

The FAIR Cyber Risk Management Framework provides a practical and structured approach to overcoming these challenges by:

- **Quantifying Cyber Risk in Financial Terms** – FAIR replaces subjective risk ratings with a structured model that translates cyber risk into measurable business impact.
- **Providing a Cyber Risk Management System (CRMS)** – FAIR-CRMF supports a continuous, data-driven approach to risk management, ensuring compliance efforts remain relevant and effective over time.
- **Enhancing Risk Treatment Decisions** – FAIR-CAM enables organizations to assess control effectiveness and optimize risk mitigation strategies.
- **Improving Communication with Executives** – By framing cybersecurity risks in financial terms, FAIR-CRMF enables CISOs to present clear, business-aligned risk insights to leadership.

By integrating FAIR-CRMF into their ISO 27001 strategy, organizations can move beyond a compliance-driven mindset and establish a sustainable, risk-informed security program.

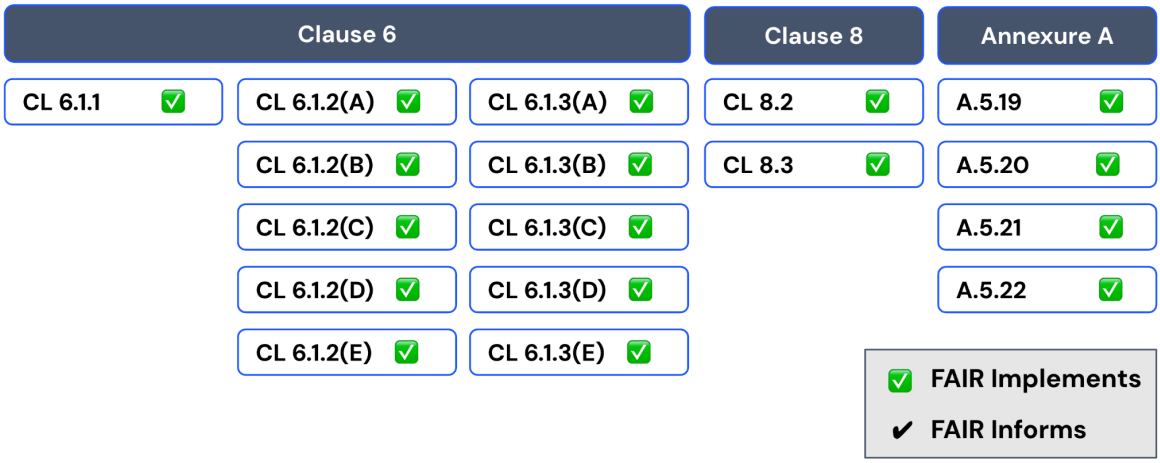
Addressing ISO 27001 Requirements with FAIR

FAIR provides a quantitative approach to cybersecurity risk management, helping organizations:

- Translate cybersecurity risks into financial terms for business decision-making.
- Conduct risk quantification to prioritize security investments based on impact likelihood.
- Establish a structured methodology for assessing, mitigating, and reporting cyber risks.

The following (Figure 1) illustrates where FAIR implements or informs each of the relevant ISO 27001:2022 clauses.

Figure 1: Mapping Support of FAIR for ISO/IEC 27001:2022



Enhancing ISO/IEC Adoption with FAIR

The following table describes in more detail how FAIR helps CRMP leaders address each of the subcategories in the Govern function.

Table 1: How FAIR Supports Compliance with ISO/IEC 27001:2022

ISO/IEC 27001:2022 Clause		How FAIR Helps	Explanation
CL 6.1.1	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, and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities and e) how to 1) integrate.	**Implements**	FAIR provides a structured approach to identifying, assessing, and prioritizing risks and opportunities. By quantifying risk in financial terms, it ensures that the ISMS is aligned with business objectives, reducing undesired effects and supporting continual improvement.
CL 6.1.2	Information security risk assessment: The organization shall define and apply an information security risk assessment process that:	**Implements**	FAIR establishes a repeatable, quantitative risk assessment process that ensures clarity and consistency in evaluating information security risks.
CL 6.1.2(A)	establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria and 2) criteria for performing information security risk assessments.	**Implements**	FAIR helps define objective risk acceptance criteria and standardizes how information security risk assessments are performed, ensuring transparency in decision-making.

ISO/IEC 27001:2022 Clause		How FAIR Helps	Explanation
CL 6.1.2(B)	ensures that repeated information security risk assessments produce consistent, valid, and comparable results.	**Implements**	FAIR ensures that repeated risk assessments produce consistent, valid, and comparable results by using a structured methodology based on loss event frequency and loss magnitude.
CL 6.1.2(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.	**Implements**	FAIR provides a systematic approach to identifying and analyzing risks associated with confidentiality, integrity, and availability, as well as assigning risk ownership based on financial impact.
CL 6.1.2(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), and (3) determine the levels of risk.	**Implements**	FAIR facilitates a structured analysis of security risks by assessing their potential financial and operational consequences, calculating likelihood based on data-driven estimations, and determining overall risk levels.
CL 6.1.2(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. The organization shall retain documented information about the information security risk assessment process.	**Implements**	FAIR enables organizations to evaluate risks by comparing analysis results with predefined criteria, prioritizing risks based on potential financial impact to guide treatment decisions.
CL 6.1.3	Information security risk treatment: The organization shall define and apply an information security risk treatment process to:	**Implements**	FAIR supports an objective, data-driven approach to risk treatment, ensuring that mitigation decisions are based on measurable impact and cost-effectiveness.

ISO/IEC 27001:2022 Clause		How FAIR Helps	Explanation
CL 6.1.3 (A)	select appropriate information security risk treatment options, taking account of the risk assessment results. The organization shall retain documented information about the information security risk treatment process.	**Implements**	FAIR helps organizations select the most effective risk treatment options by performing cost-benefit analyses, ensuring that mitigation strategies provide the best return on investment.
CL 6.1.3 (B)	determine all controls that are necessary to implement the information security risk treatment option(s) chosen.	**Implements**	FAIR-CAM (Controls Analytics Model) enables organizations to determine which controls are necessary by assessing their effectiveness in reducing risk.
CL 6.1.3 (D)	produce a Statement of Applicability that contains the necessary controls (see 6.1.3(B) and (C) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A.	**Implements**	FAIR assists in producing a defensible Statement of Applicability by quantifying the necessity and effectiveness of security controls, helping justify control selection or exclusion.
CL 6.1.3 (E)	formulate an information security risk treatment plan. The organization shall retain documented information about the information security risk treatment process.	**Implements**	FAIR supports the development of risk treatment plans by ensuring risks are quantified, prioritized, and managed based on financial exposure and business impact.
CL 6.1.3 (F)	obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.	**Implements**	FAIR facilitates risk owner approval by providing clear, quantified risk assessments, making it easier to justify treatment plans and residual risk acceptance.
CL 8.2	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 6.1.2(A). The organization shall retain documented information of	**Implements**	FAIR supports continuous risk assessment by providing a structured methodology for evaluating security risks at planned intervals and after significant changes.

ISO/IEC 27001:2022 Clause		How FAIR Helps	Explanation
	the results of the information security risk assessments.		
CL 8.3	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.	**Implements**	FAIR ensures the effectiveness of risk treatment plans by tracking risk reduction over time and measuring whether security investments are achieving the intended results.
A.5.19	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of suppliers' products or services.	**Implements**	FAIR helps manage supplier-related risks by quantifying their potential impact, enabling organizations to prioritize security measures for third-party relationships.
A.5.20	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	**Implements**	FAIR facilitates the establishment of security requirements for suppliers by evaluating risks based on financial exposure and business-critical functions.
A.5.21	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	**Implements**	FAIR provides a structured approach to assessing and managing security risks in the ICT supply chain, ensuring transparency and accountability.
A.5.22	The organization shall regularly monitor, review, evaluate, and manage change in supplier information security practices and service delivery.	**Implements**	FAIR supports ongoing monitoring, evaluation, and management of supplier security practices by quantifying risks and ensuring security controls remain effective.

Conclusion

ISO 27001 adoption presents organizations with both opportunities and challenges. By integrating the FAIR Cyber Risk Management Framework and a Cyber Risk Management System into their ISMS, organizations can move beyond checkbox compliance and establish a security program that is risk-driven, sustainable, and aligned with business objectives. Additionally, leveraging FAIR-CRMF alongside ISO 27005 ensures a comprehensive, quantitative approach to risk assessment, making cybersecurity risk management more precise, actionable, and aligned with business priorities.