Framework Foundations: ISO/IEC 27001

Introduction to ISO/IEC 27001

ISO/IEC 27001 is the globally recognized standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides a systematic framework for managing sensitive data and ensuring confidentiality, integrity, and availability.

This voluntary standard helps organizations build a resilient security posture and reduce risk. Its broad applicability and global recognition make it especially relevant for entities handling sensitive or regulated data. To support implementation, Annex A offers a structured set of reference controls that guide risk treatment and ensure alignment with industry best practices.

What's New in ISO/IEC 27001:2022

The 2022 update introduced several key changes to keep pace with evolving threats:

- Cloud Security: Addresses modern infrastructure risks.
- Threat Intelligence: Enhances proactive defense.
- Data Masking: Protects sensitive data in transit and at rest.

These updates ensure the standard remains effective in addressing today's cybersecurity challenges.

Objectives of ISO/IEC 27001

This standard aims to achieve the following key objectives:

- Protect confidentiality, integrity, and availability of information assets
- Establish governance and accountability for security practices
- Enable continuous improvement of security controls

Key Requirements

ISO/IEC 27001 outlines a comprehensive set of requirements for establishing, implementing, maintaining, and continually improving an ISMS. These requirements are designed to help organizations manage information security risks systematically and effectively, and include:

1. Leadership & Governance

- Define an information security policy aligned with business objectives
- Assign roles and responsibilities for security management
- Ensure top management commitment and oversight

2. Risk Management

- Conduct risk assessments to identify threats and vulnerabilities
- Establish a risk treatment plan to mitigate identified risks
- Maintain a risk register and review it regularly

3. Security Controls (Annex A)

- Implement controls across 4 themes (as per ISO/IEC 27002:2022):
  - Organizational controls
  - People controls
  - Physical controls
  - Technological controls
- Tailor controls to the organization's context and risk profile

4. Documentation & Evidence

- Maintain documentation of policies, procedures, and control implementation
- Keep records of incident response, audit results, and corrective actions

5. Continuous Improvement

- Monitor and measure ISMS performance
- Conduct internal audits and management reviews
- Implement corrective and preventive actions

Certification Process:

Achieving ISO/IEC 27001 certification involves a two-stage audit by an accredited third-party. This process includes a Stage 1 (documentation review) and Stage 2 (on-site assessment) audit. Successful certification demonstrates a verifiable commitment to information security best practices.

Regulatory Alignment

ISO/IEC 27001, though voluntary, is widely adopted as a foundation for regulatory compliance with frameworks like EU GDPR, UK GDPR, and the NIS2 Directive. For CISOs, aligning with ISO/IEC 27001 streamlines compliance efforts, demonstrates due diligence in managing information security risks, and supports both internal governance and external audits. This not only simplifies regulatory obligations but also enhances stakeholder trust and reinforces the organization's commitment to cybersecurity and data protection.

How Cisco + Splunk Support Compliance

To support ISO/IEC 27001 compliance, Cisco and Splunk offer a range of integrated solutions aligned with the standard's core clauses and Annex A controls. The following tables illustrate how specific products and capabilities from both vendors help organizations meet requirements –helping to enable effective governance, risk management, operational security, and continuous improvement.

ISO/IEC 27001 Clause	How Cisco + Splunk Support Compliance	Relevant Products
5. Leadership	Governance frameworks and dashboards provide executive visibility and oversight	Cisco XDR, Splunk Enterprise Security
6. Planning	Risk-based planning supported through vulnerability management and alerting tools	Cisco XDR, Splunk Enterprise Security, Cisco Secure Firewall, Cisco Secure Malware Analytics, Cisco Secure Endpoint, Splunk SOAR, Splunk ARI, Splunk UBA
7. Support	Training, documentation, and role-based access controls enhance user awareness and security	Cisco Duo, Cisco Security Awareness Training, Splunk Knowledge Manager
8. Operation	Secure operations enabled via firewall reviews, log monitoring, and automated response	Cisco Secure Firewall, Cisco Secure Firewall Management Center, Splunk ES, Splunk SOAR
9. Performance Evaluation	KPIs and monitoring tools track security performance and compliance posture	Cisco SNA, Cisco Secure Client with ISE Posture Check, Cisco Catalyst Center Assurance and Analytics, Splunk ES, Splunk ARI, Splunk SOAR
10. Improvement	Analytics and audit tools support continuous improvement and remediation	Cisco XDR, Cisco SNA, Splunk SOAR, Splunk ES

Annex A Requirement	How Cisco + Splunk Support Compliance	Relevant Products
A.5 Information security policies	Enforce and monitor security policies	Cisco XDR, Cisco SNA, Meraki Systems Manager, Splunk Enterprise Security, Splunk SOAR
A.6 Organization of information security	Centralized security management & role-based access	Cisco ISE, Cisco Duo, Splunk SOAR, Splunk ES
A.8 Asset management	Asset discovery and classification	Cisco Cyber Vision, Cisco ISE, Cisco SNA, Cisco FirePOWER, Cisco Multicloud Defense, Cisco Attack Surface Management, Splunk Asset and Risk Intelligence (ARI), Splunk SOAR
A.9 Access control	Identity and access management	Cisco Duo, Cisco ISE, Cisco Secure Access, Cisco Secure Firewalls, Splunk ES, Splunk SOAR, Splunk User Behavior Analytics (UBA)
A.12 Operations security	Visibility and control over IT operations	Cisco Secure Firewall, Cisco XDR, Cisco SNA, Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco ISE, Cisco SD-WAN, Splunk ES, Splunk SOAR, Splunk UBA, Splunk ITSI
A.13 Communications security	Secure data in transit	Cisco Umbrella, Cisco Secure Network Analytics (SNA), Cisco Secure Firewall, Cisco XDR, Splunk Enterprise Security, Splunk SOAR
A.14 System acquisition, development and maintenance	Secure system development and integration	Cisco Secure Workload, Splunk Security Essentials
A.16 Information security incident management	Real-time incident detection and response	Cisco XDR, Splunk SOAR
A.17 Business continuity management	Monitoring and failover capabilities	Cisco Secure Network Analytics, Cisco ThousandEyes, Splunk Observability Cloud
A.18 Compliance	Audit trails and regulatory reporting	Cisco Secure Audit, Splunk Compliance Analytics

ISO/IEC 27001 Compliance with Cisco Security + Splunk

Cisco and Splunk together provide a robust foundation for ISO/IEC 27001:2022 compliance. Cisco's integrated security architecture delivers unified visibility, control, and threat response across hybrid environments, while Splunk's advanced analytics and automation capabilities enhance detection, investigation, and response at scale. This synergy enables organizations to effectively establish, implement, and continuously improve their ISMS.

Unlike fragmented point solutions, Cisco offers a cohesive platform that integrates networking, security, observability, and collaboration. Splunk complements this with powerful data correlation and analysis across diverse sources, enabling faster insights and automated workflows. Together, they empower security teams to build a future-ready Security Operations Center (SOC), reduce dwell time, and respond to threats with precision. By choosing Cisco and Splunk, organizations can break free from vendor silos and fragmented tooling. This joint approach supports a more efficient and scalable path to ISO/IEC 27001 compliance – ensuring robust information security, operational resilience, and continuous improvement in today's complex digital landscape.

Resources

For more information and guidance on ISO/IEC 27001 compliance, please refer to the following resources:

- Cisco Security Portfolio Mapping to NIST CSF 2.0 and Other Global Frameworks
- ISO/IEC 27001:2022
- ISO/IEC 27002:2022

P0708081101 10/25