

Benefits of an ISMS Program

ISO/IEC 27001

January 31, 2025



Introduction

Information Security Management System (ISMS), as defined by ISO/IEC 27000:2012

part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

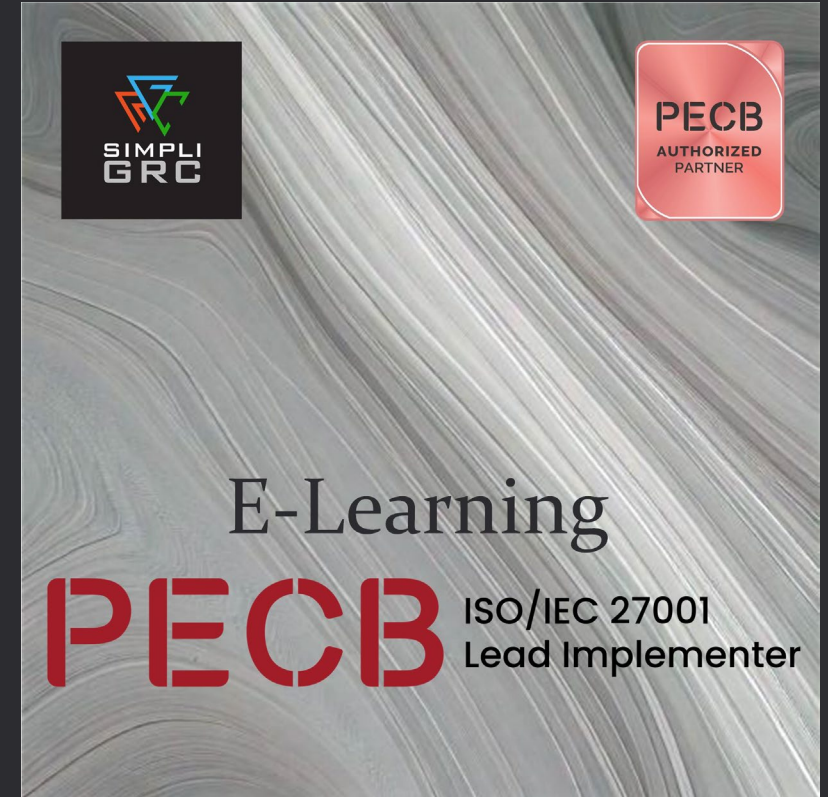
Break down the definition and the following can be interpreted as characteristics of an ISMS:

1. A risk-based approach focused on the business or operations
2. Authorize and scope the ISMS program to increase the security of Confidentiality, Integrity, and Availability (CIA)
3. A plan to implement an ISMS
4. Operational governance, risk, and compliance functions through the implementation of policies, processes, procedures, and guidelines, where necessary
5. Monitoring, reviewing, and maintaining the authorized People, Process, and Technology (PPT) controls
6. Continual improvement where gaps or deviations from the authorized ISMS program are discovered



Benefits of ISO/IEC 27001 ISMS

1. Enhanced Security
 - Developed from industry practitioners and evolved over the years or decades.
 - Intended to protect the CIA of your valued assets
2. Improved Risk Management
 - Assesses risk to your valued assets to prioritize your resources
3. Operational Efficiency and Resiliency
 - Flexible to apply to any scope of your organization
 - Integrates PPT across your ISMS program
 - Incorporate requirements to continually improve the ISMS program as the business or operations evolves
 - Enables the integration of external regulatory compliance programs
 - Leverages other ISO standards to extend your ISMS program
4. Industry Recognized
 - Formal certification instills external confidence in your ISMS
 - A competitive advantage to your competitors that are not certified
 - Global recognition and trust in your ISMS



The graphic features a background of wavy, light-colored lines. In the top left corner is the SIMPLI GRC logo, and in the top right corner is a red rounded rectangle with the text 'PECB AUTHORIZED PARTNER'. The main text in the center reads 'E-Learning' in a large, dark font, followed by 'PECB' in a large, bold, red font, and 'ISO/IEC 27001 Lead Implementer' in a smaller, dark font to the right of 'PECB'.

Integration with External Programs

1. CSA z246.1 in Canada
 - Assesses risk to your valued assets to prioritize your resources
2. Privacy Regulations
 - ISO/IEC 27701 Privacy Information Management System (PIMS)
 - GDPR in EU
 - California Consumer Privacy Act (CCPA)
3. ISA/IEC 62443-2.1:2024
 - Replaces Cyber Security Management System (CSMS) with Information Security Management System (ISMS)
4. ISO Standards
 - All ISO standards are developed with the similar objectives and structure, especially with the management systems. Examples include:
 - ISO 22301: Business Continuity Management System
 - ISO/IEC 27035: Information Security Incident Management
 - ISO 28000: Supply Chain Security Management System
 - ISO 31000: Enterprise Risk Management
 - ISO/IEC 42001: Artificial Intelligence Management System



More compliance and security programs are gravitating towards ISO/IEC 27001 due to its credibility and maturity over the decades. The number of proven best practices included in a comprehensive ISMS are a significant advantage for any organization targeting improved information security.

Pros and Cons

ISO 27001 Characteristics	Pros	Cons
Risk Management	<ul style="list-style-type: none">• Integrates with ISO 31000 and 27005• Focus on risk makes it applicable to any environment	<ul style="list-style-type: none">• Deep learning curve and experience required to implement or assess
Enhanced Security of CIA	<ul style="list-style-type: none">• Reduces information security risks by safeguarding valued assets• Integrates with standards and frameworks• Internationally recognized	<ul style="list-style-type: none">• Less specialized than specific standards or frameworks (e.g. PCI, ISA/IEC 62443, NERC CIP, etc.)
An ISMS Plan	<ul style="list-style-type: none">• An integrated plan across 7 clauses of the standard• Integrates with other management systems like ISO 22301, ISO/IEC 27035, ISO 28000, ISO/IEC 42001, etc	<ul style="list-style-type: none">• Deep learning curve and experience required to implement or assess
Operational GRC Functions	<ul style="list-style-type: none">• Plan-Do-Check-Act cycle is applicable to all GRC functions with integration	<ul style="list-style-type: none">• Complications may occur with integration across all GRC functions
Monitoring and Controlling PPT	<ul style="list-style-type: none">• PPT approach strengthens sustainability and comprehensive information security• Reduces compliance risks with non-technical controls• Structured auditing practices from authorized auditors	<ul style="list-style-type: none">• Larger investment and more time required
Continual Improvement	<ul style="list-style-type: none">• Controls and checks to measure operational performance and correct deficiencies	<ul style="list-style-type: none">• Increased resources to monitor and correct gaps in the ISMS

Value of Certifying Your ISMS

1. The certification process increases awareness
 - The process to implement an ISMS facilitates the identification of information security gaps and framework to correct them
 - The interested parties impacted by the ISMS will obtain a higher understanding of information security and how it applies to your valued assets
2. Promotes comprehensive and applicable planning
 - Size your ISMS from one team to one department to the entire organization that fits your business and information security goals
 - Prioritizes resources for your critical processes through risk management
3. Competitive advantage
 - Publicly recognized for a strong ISMS without disclosing details
 - Customers will acknowledge a level of safety and trust with certification versus competitors that are not certified
4. Stronger information security
 - All ISO standards are developed with the similar objectives and structure, especially with the management systems
 - Your ISMS program is sustained and improved through internal controls, certification audits, and monitoring



How SimpliGRC Can Support

Certified staff in
ISO/IEC 27001 Lead
Implementation /
Lead Auditor /
Instructor

Successfully
completed several
NIST CSF, CIP, CIS,
and ISO assessments
and audits

Softening silos and
sub-cultures to
achieve enterprise or
project goals

Experienced in
Business Impact
Analysis and Risk
Assessments

Senior analysis and
project management
services

IT / OT convergence
services in complex
environments

Strategy development
and implementation

Process development
and re-engineering

The managing
directors deliver the
services to offer the
direct experience and
competencies

Local to Calgary and
Edmonton in Alberta,
Canada

THANK YOU

info@simpligrc.com

<https://simpligrc.com/about/contact/>

