INTRODUCTION TO INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

Every technology-driven business process is exposed to security and privacy threats. Sophisticated technologies are capable of combating cybersecurity attacks, but these aren't enough: organizations must ensure that business processes, policies, and workforce behavior minimize or mitigate these risks.

Because this path is neither easy nor clear, companies adopt frameworks that help guide towards information security (InfoSec) best practices. This is where information security management systems come into play—let's take a look.

What is an ISMS?

An information security management system (ISMS) is a framework of policies and controls that manage security and risks systematically and across your entire enterprise—information security. These security controls can follow common security standards or be more focused on your industry.

For example, ISO 27001 is a set of specifications detailing how to create, manage, and implement ISMS policies and controls. The ISO doesn't mandate specific actions; instead, it provides guideline on developing appropriate ISMS strategies.

The framework for ISMS is usually focused on risk assessment and risk management. Think of it as a structured approach to the balanced tradeoff between risk mitigation and the cost (risk) incurred.

Organizations operating in tightly regulated industry verticals, such as healthcare or finance, may require a broad scope of security activities and risk mitigation strategies.

(Consider InfoSec management within your overall IT security policy.)

Continuous improvement in information security

While ISMS is designed to establish holistic information security management capabilities, digital transformation requires organizations to adopt ongoing improvements and evolution of their security policies and controls.

The structure and boundaries defined by an ISMS may apply only for a limited time frame and the workforce may struggle to adopt them in the initial stages. The challenge for organizations is to evolve these security control mechanisms as their risks, culture, and resources change.

According to ISO 27001, ISMS implementation follows a Plan-Do-Check-Act (PCDA) model for continuous improvement in ISM processes:

- **Plan.** Identify the problems and collect useful information to evaluate security risk. Define the policies and processes that can be used to address problem root causes. Develop methods to establish continuous improvement in information security management capabilities.
- **Do.** Implement the devised security policies and procedures. The implementation follows the ISO standards, but actual implementation is based on the resources available to your company.
- **Check.** Monitor the effectiveness of ISMS policies and controls. Evaluate tangible outcomes as well as behavioral aspects associated with the ISM processes.
- **Act.** Focus on continuous improvement. Document the results, share knowledge, and use a feedback loop to address future iterations of the PCDA model implementation of ISMS policies and controls.

Popular ISMS frameworks

ISO 27001 is a leader in information security, but other frameworks offer valuable guidance as well. These other frameworks often borrow from ISO 27001 or other industry-specific guidelines.

- ITIL, the widely adopted service management framework, has a dedicated component called Information Security Management (ISM). The goal of ISM is to align IT and business security to ensure InfoSec is effectively managed in all activities.
- COBIT, another IT-focused framework, spends significant time on how asset management and configuration management are foundational to information security as well as nearly every other ITSM function—even those unrelated to InfoSec.

ISMS security controls

ISMS security controls span multiple domains of information security as specified in the ISO 27001 standard. The catalog contains practical guidelines with the following objectives:

- **Information security policies.** An overall direction and support help establish appropriate security policies. The security policy is unique to your company, devised in context of your changing business and security needs.
- **Organization of information security.** This addresses threats and risks within the corporate network, including cyberattacks from external entities, inside threats, system malfunctions, and data loss.
- **Asset management.** This component covers organizational assets within and beyond the corporate IT network., which may involve the exchange of sensitive business information.
- **Human resource security.** Policies and controls pertaining to your personnel, activities, and human errors, including measures to reduce risk from insider threats and workforce training to reduce unintentional security lapses.
- **Physical and environmental security.** These guidelines cover security measures to protect physical IT hardware from damage, loss, or unauthorized access. While many organizations are taking advantage of digital transformation and maintaining sensitive information in secure cloud networks off-premise, security of physical devices used to access that information must be considered.
- **Communications and operations management.** Systems must be operated with respect and maintenance to security policies and controls. Daily IT operations, such as service provisioning and problem management, should follow IT security policies and ISMS controls.
- **Access control.** This policy domain deals with limiting access to authorized personnel and monitoring network traffic for anomalous behavior. Access permissions relate to both digital and physical mediums of technology. The roles and responsibilities of individuals should be well defined, with access to business information available only when necessary.
- **Information system acquisition, development, and maintenance.** Security best practices should be maintained across the entire lifecycle of the IT system, including the phases of acquisition, development, and maintenance.
- **Information security and incident management.** Identify and resolve IT issues in ways that minimize the impact to end users. In complex network infrastructure environments, advanced technology solutions may be required to identify insightful incident metrics and proactively mitigate potential issues.
- **Business continuity management.** Avoid interruptions to business processes whenever

possible. Ideally, any disaster situation is followed immediately by recovery and procedures to minimize damage.
- **Compliance.** Security requirements must be enforced per regulatory bodies.
- **Cryptography.** Among the most important and effective controls to protect sensitive information, it is not a silver bullet on its own. Therefore, ISMS govern how cryptographic controls are enforced and managed.
- **Supplier relationships.** Third-party vendors and business partners may require access to the network and sensitive customer data. It may not be possible to enforce security controls on some suppliers. However, adequate controls should be adopted to mitigate potential risks through IT security policies and contractual obligations.

These components and domains offer general best practices towards InfoSec success. Though these may vary subtly from one framework to another, considering and aligning with these domains will provide much in the way of information security.

Related reading

- BMC Security & Compliance Blog
- The MITRE ATT&CK Framework Explained
- Top IT Security, InfoSec & CyberSecurity Conferences
- 7 Business-Critical IT Policies & How To Implement Them