ITIL® INFORMATION SECURITY MANAGEMENT

ITIL 4 Guide ›

(This article is part of our ITIL v3 Guide. Use the right-hand menu to navigate.)

ITIL information security management

Today, nearly every major company is in the technology business. Even the largest industrial and mining operations in the world depend heavily on complex IT services (and the hardware, software, networks, people, and processes that comprise them) to turn a profit.

More than ever, that means that IT has to be able to help the business manage risk, ensuring that resources are used responsibly and protected against potential threats or losses.

That's exactly the goal of ITIL Information Security Management, or ISM: to "align IT and business security and ensure that information security is effectively managed in all service and Service Management activities."

Unlike some ITIL processes that are invoked on an as-needed basis, security is not a single step in a service lifecycle. It's a continuous, integral need that requires stringent controls.

Free Download ›

According to ITIL, the objectives of Information Security Management are to ensure that:

- *Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability)*
- *Information is observed by or disclosed to only those who have a right to know (confidentiality)*
- *Information is complete, accurate, and protected against unauthorized modification (integrity)*
- *Business transactions, as well as information exchanges between enterprises or with partners, can be trusted (authenticity and non-repudiation*

A few other helpful definitions as we dive further into ISM are:

- **Information Security Policy** — An overarching security policy for your company that has the full support of top executive IT and business management. It should include separate policies for use and misuse of assets, access control, password control, email and internet, anti-virus, information classification, document classification, remote access, supplier access to your IT services and information, and asset disposal.

  ITIL recommends that you make these policies widely available to all of your users and customers, and that you review and revise them at least every twelve months.

- **Information Security Management System (ISMS)** – This is just a wordy way of referring to the set of policies you put in place to manage security and risk across your company. The most important thing is that you take a calculated and comprehensive approach to designing, implementing, managing, maintaining and enforcing information security processes and controls. ITIL suggests that your ISMS should address what it calls “The Four P’s”: people, process, products and technology, and partners and suppliers.

  Many global IT organizations seek global certification for their ISMS frameworks, which is done through ISO 27001. Typically, an ISMS framework addresses five key elements:

1. Control
   You should establish management framework for managing information security, preparing and implementing an Information Security Policy, allocating responsibilities, and establishing

Figure 3. Framework for Managing IT Security

and controlling documentation.

2. Plan
   In the planning phase of the framework, you will be responsible for gathering and fully understanding the security requirements of the organization — then recommending the appropriate measures to take based on budget, corporate culture around security, and other factors.
3. Implement
   Next, you'll put the plan into action, making sure that you have the proper safeguards in place to properly enact and enforce your Information Security Policy in the process.
4. Evaluate
   Once your policies and plans are in place, you need to properly oversee them to ensure that your systems are truly secure and your processes are running in compliance with your policies, SLAs, and other security requirements.
5. Maintain
   Finally, an effective ISMS means you are continuously improving the entire process — looking for opportunities to revise SLAs, security agreements, the way you monitor and control them, and more.

- A **security management information system** (or SMIS) is simply a tool or repository that stores data that supports your security management practices. It's part of your overall service knowledge management system (or SKMS). Ultimately, it should serve as the primary place for storing things like your security policies and plans, as well as all associated documents, measurements, and plans of action.

Who is responsible for Information Security Management?

Large organizations typically appoint a Security Manager who is accountable for the ISM process, end-to-end. Their job is to make sure that effective security policies are created, shared, and approved, and they are also responsible for overall security operations (from architecture and administration to recovery).

Key activities of Information Security Management (and thus responsibilities of the Security Manager), according to ITIL, include:

1. Creating (and revising as needed) an overall Information Security Policy for your company, and

all necessary supporting policies.
2. Communicating, implementing, and enforcing these policies
3. ssessing and classifying all information assets and documentation
4. Implementing (and revising as needed) a set of security controls
5. Monitoring and managing all security breaches and major security incidents
6. Analyzing, reporting, and reducing the volume and impact of severity breaches and incidents
7. Scheduling and completing security reviews, audits, and penetration tests.

Recommended security controls

Because security is a continuous process, you should put in place a set of measures and controls that help minimize both threats and the impact of human errors. ITIL suggests five different types of measures:

First, *preventative* measures are designed to keep a security incident from happening altogether. Much of this practice is focused on access management tasks like assigning appropriate rights and permissions, verifying identification, and ensuring that unauthorized people cannot access your information and systems.

Reductive measures seek to reduce the impact of incidents that do occur, like putting contingency plans into place and testing them, for example, or performing automated backups of your critical data and systems.

Detective measures are exactly as they are named: controls put in place to identify a risk or threat as quickly as possible. This means putting the best possible monitoring systems in place — including network and systems monitoring tools, alerts, etc.

Repressive measures are like counterattacks. When a potential threat is detected, like a possibly malicious bot continuously trying to log in with an assortment of username and password combinations, automatically blocking further attempts from that IP address (or temporarily locking the usernames associated with the login attempts) is a great example of a repressive measure.

Finally, *corrective measures* seek to repair any damage caused by an error or incident. Restoring a backup is a top example.

Measuring your effectiveness

ITIL recommends a wide variety of metrics and KPIs you can use to keep track of how efficient and effective your ISM process and activities are. Key examples include:

- Percentage decrease in security breaches reported to your Service Desk, or in the impact of breaches and incidents
- Increase in support of your security procedures by senior management, and in conformance to your policies across the company
- The number of improvements suggested or made to your security procedures
- Increased awareness of your security policies across the organization

Key recommendations

First, ensure that you secure adequate support from senior leadership in the executive suite. Without

buy-in, your efforts to create (and enforce) strong security policies could prove futile. To improve executive commitment, it's helpful to make sure your security strategy focused on business priorities and the IT services they count on, not just technology.

Second, don't forget to gather information from across your business as you create your security strategy and ISMS. Talking with and gathering data from every aspect of the organization is essential, to make sure you properly understand and address all risks, requirements, and priorities.

Don't forget the education, either. As you define your security requirements and create policies, making sure employees (and suppliers, etc.) are aware of them is critical. Setting proper expectations upfront will go a long way to widespread adoption and compliance.

Finally, remember that as your business evolves, so will the potential risks and security needs. Remember to regularly re-evaluate your policies and systems to ensure you are keeping up with new requirements (and even new threats from hackers as they become more sophisticated).