Protect ○ Comply ○ Thrive

IT Governance USA Blog

Blog Home Business Continuity Cyber Security Data Protection IT Best Practice

IT Governance PCI DSS Other Blogs

What is an Information Security Management System (ISMS)?

Julia Dutton August 23, 2021

What is an ISMS?

An information security management system (ISMS) is a framework of policies and procedures for systematically managing an organization's sensitive data.

It includes the processes, people, technology, and procedures that are designed to protect against unauthorized access, use, disclosure, disruption, modification, or destruction of information.

How does an ISMS work?

An ISMS works by providing an organization with a structured framework for managing and

SOCIAL MEDIA

Search the site

Search

RECENT POSTS

safeguarding its information assets.

It consists of policies and procedures that define how processes and activities related to information security are to be managed.

The ISMS also outlines the roles and responsibilities of personnel involved in managing information security and provides guidance on how to identify, assess, and mitigate risks.

It can also be used to monitor the effectiveness of security measures and to provide evidence of compliance with applicable laws and regulations.

What are the benefits of an ISMS?

Cost savings: An ISMS can help organizations save money in the long run by reducing the cost of responding to data breaches, ensuring compliance with applicable laws and regulations, and reducing the cost of insurance premiums.

Risk reduction: An ISMS helps organizations identify and address potential security risks before they have a chance to become a problem. This can help reduce the risk of data breaches, financial losses, and reputational damage.

Enhanced competitiveness: An ISMS can help organizations gain a competitive edge by demonstrating their commitment to data security and compliance. This can help them stand out in a crowded market and attract more business.

Implementing an ISMS

Google Sparks Controversy with the Release of ZIP Domains

FBI Dismantles Russian Malware That Stole Government Secrets

May 2023 CMMC Rulemaking: It’s Time to Get CMMC Certified

Google Joins AI Cybersecurity Party with Cloud Security Workbench

What Are Your Data Breach Notification Requirements?

There are numerous ways of approaching the implementation of an ISMS. The most common method to follow is a 'Plan Do Check Act' process.

ISO 27001 is the international security standard that details the requirements of an ISMS.

ISO 27001, along with the best-practice guidelines contained in ISO 27002, serve as two excellent guides to get you started with implementing an ISMS.

An ISMS that is certified and audited can provide customers with the assurance that the organization has taken steps to protect its information assets from risks that have been identified.

The strength of an ISMS is based on the robustness of the information security risk assessment, which is key to any implementation.

Recognizing the risks that the organization and its data may face in the future is necessary to implement the mitigating measures (controls).

ISO 27001 provides a recommended list of controls that can help assess whether the necessary controls have been considered for legislative, business, contractual, or regulatory purposes.

Getting started with your ISMS

The key to an effective ISMS is a risk assessment. After all, it's only when you know what threats you face that you can implement appropriate defenses.

This can be a labor-intensive task, but you can simplify the process with our risk assessment tool

Reduce the risk of staff-related information security incidents with staff awareness training
Find out more

CATEGORIES

- Business Continuity
- CCPA
- Cyber Security
  - CMMC
  - ISO 27001
  - NYSE Guides
  - Risk Management
- Data privacy
- Data Protection
  - #BreachReady
- EU GDPR
- HIPAA
- IT Best Practice
  - ITIL/ITSM/ISO 20000
  - Project Management
- IT Governance
  - COBIT
- News
- NIS Directive

vsRisk.

With this software package, you'll receive a fast and straightforward way to create your risk assessment methodology and deliver repeatable, consistent assessments year after year.

Its asset library assigns organizational roles to each asset group, applying relevant threats and risks by default.

Meanwhile, its integrated risk, vulnerability, and threat databases eliminate the need to compile a list of risks, and the built-in control sets help you comply with multiple frameworks.

Get started

A version of this blog was originally published on 27 July 2018.

Related Posts

Cyber November – get more for

Protect your home office from cyber crime

A quick guide to Cybersecurity Trends – part 2

- NIST
- NY Cybersecurity Requirements
- NYDFS
- Other Blogs
  - Book Reviews
  - Breaches and Hacks
  - Guest Posts
  - Podcasts
  - Product Blog
  - Quiz
  - Technical Experts
  - Training
- PCI DSS
- Penetration Testing
- Phishing
- SOC 2
- Uncategorized
  - State data privacy laws

your money in November

About The Author

Julia Dutton