NIST Cybersecurity Framework and ISO 27001

May 2018

Protect • Comply • Thrive

NIST Cybersecurity Framework and ISO 27001

Introduction

It is important for your organization to take adequate measures to protect the confidentiality, integrity and availability of its information, as well as the IT systems that maintain it. This is particularly true of organizations that support critical infrastructure – they are, after all, essential to business and society.

An information security management system (ISMS) is a centrally managed framework designed to keep the information and organization maintains safe. It is made up of the policies, procedures, and technical and physical controls that ensure private data is adequately protected, data breaches are properly managed and business continuity is promoted.

An ISMS can be applied to the entire organization or only to a specific area containing information that needs protection. The controls that safeguard against risks related to people, resources, assets, and processes can be technical or nontechnical.

Organizations of all shapes and sizes can benefit from implementing an ISMS. Adopting existing frameworks and modifying them to better fit your cybersecurity needs is almost certainly a better alternative to building and maintaining a custom ISMS from scratch.

There are a number of existing frameworks, which vary in popularity, approach, sector, and scope. Among the more popular and widely applicable are the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and ISO/IEC 27001:2013 (ISO 27001), the international standard for information security management.

This green paper compares the NIST CSF and ISO 27001.

A critical infrastructure overview

Critical infrastructure drives the US economy, security, and overall health, and comprises 16 critical sectors.[1] Each sector delivers the assets, systems, and networks – physical and virtual – that are so vital to sustaining the American way of life that it is a top government priority to protect them. If any harm were to come to any critical infrastructure sector, it could cause major disruption, with potentially catastrophic outcomes.

Industrial processes that cannot be run by human hands alone are managed by industrial control systems. They are used to manage large-scale industrial processes and are increasingly integrated with IT networks.[2]

Cyber threats are on the rise

Critical infrastructure threats can be digital, physical, or both. Criminal hackers target the software and networks that drive critical sector business functions, and control

systems that operate physical processes. Examples range from financial databases to railroad switches. While operational controls increasingly take advantage of the automation and efficiency that the Internet affords, the heightened connectivity also introduces new vulnerabilities.

Criminal hackers and cyber crime syndicates are becoming more aggressive, organized, and sophisticated. They are also learning a great deal about US critical infrastructure systems. According to cybersecurity expert Robert M. Lee, CEO of industrial cybersecurity firm Dragos, Inc., criminals are learning "not just from a computer technology standpoint but from an industrial engineering standpoint".[3]

Data breaches can be costly

Cyber crime impacts organizations of all types and sizes. When breached, an organization can suffer levies, lost revenue, damaged intellectual property, lawsuits, and reputational damage.

US data breaches in 2017[4]		
Industry	Breaches	Records affected
Banking/credit/ financial	99	2,910,117
Business	680	159,365,480
Educational	116	1,146,861
Government/ military	70	5,838,098
Medical/health care	374	5,141,972
Total	1339	174,402,528

Research and publishing firm Cybersecurity Ventures has predicted that, globally, cyber crime will cost $6 trillion by 2021.[5] According to the IBM-sponsored "2017 Ponemon Cost of Data Breach Study", the average cost of a data breach in the US is $7.3 million.[6]

NIST Cybersecurity Framework

In 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity", to establish a voluntary, risk-based cybersecurity framework outlining best practice for critical infrastructure sectors.[7]

In response to the executive order, the government and private sector collaborated to develop the CSF. This is an accessible outline of cost-effective risk reduction that addresses business needs. The Framework was developed for critical infrastructure sectors but has proven flexible enough to be adopted by large and small organizations across all industry sectors.

The CSF comprises three primary elements: the core, profiles and tiers.

ISO 27001: Background

The ISO 27000 series is developed and maintained by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to provide a globally-recognized framework for best-practice information security management.

ISO 27001 sets out the requirements against which an organization's ISMS can be audited and certified. Achieving accredited certification to ISO 27001 provides independent, expert verification that information security is managed in line with international best practice and business objectives.

Framework key features by category

The sections below describe the similarities and differences between the NIST CSF and ISO 27001 by key categories.

Structure and approach – NIST CSF

The CSF is a set of practices that apply across an organization. The CSF **core** gives structure to cybersecurity risk management

by identifying five critical functions that comprise cybersecurity. They are:

- Identify (ID)
- Protect (PR)
- Detect (DE)
- Respond (RS)
- Recover (RC)

The practices described in each function include critical business activities such as governance and risk management, as well as other management processes to oversee the program. This is distinct from the approach taken by ISO 27001, as you will see.

The structure is open-ended, in that you can apply CSF information security as a set of practices regardless of how your organization is run.

These are fundamental, concurrent, and continuous functions to help you better understand the organization's cybersecurity processes. Each function contributes to the overall cybersecurity risk management program, and determines how each person fits into the program. The core helps risk managers identify and locate gaps that undermine cybersecurity efforts.

Categories

Categories subdivide the five core functions to help organize specific cybersecurity activities. Some of the categories provided by the Framework include:

- Business environment (ID)
- Awareness and training (PR)
- Security continuous monitoring (DE)
- Mitigation (RS)
- Improvements (RC)

Subcategories

Subcategories describe specific outcomes within their categories. For instance, one of the subcategories in the 'business environment' category is "The organization's role in the supply chain is identified and communicated".

Informative references

Informative references refer to existing best-practice standards, guidelines, and practices that are common across critical infrastructure sectors (including ISO 27001). They suggest methods to implement controls that meet the objectives established in the subcategories.

The references suggested by the Framework are merely advisory – an organization is free to use any reference (or part thereof) suitable for its industry or business.

Structure and approach – ISO 27001

ISO 27001 sets requirements for "establishing, implementing, maintaining and continually improving an [ISMS]". It features a high-level structure, with common terms, text, and core definitions. ISO 27001 is primarily supported by ISO 27000 – the series' glossary and overview from which organizations can reuse terms and definitions – and ISO 27002, which provides guidance on implementing information security.

ISO 27001 lays out an organizational cybersecurity program based on information security leadership and high-level support for policy. ISO 27001, by default, requires management oversight. Unlike the CSF, which is a structured set of practices, ISO 27001 defines a way of running an organization to achieve information security objectives. This naturally bleeds through into common practices, such as communication, training and awareness, management review, and so on.

Two critical steps of an ISO 27001 ISMS implementation are the risk assessment and risk treatment. These ensure that measures to secure the organization's information assets are based on actual threats, and balanced against the costs and other barriers to implementation.

The Standard also specifies a range of processes for managing information security across the business more generally. This includes processes for managing competence and awareness, documentation, reviewing information security performance, and taking corrective action as needed to ensure the ISMS is capable of meeting the challenges of a changing threat environment.

Continual improvement – NIST CSF

The CSF uses 'profiles' as a built-in mechanism for improving cybersecurity. By describing the organization's current state and the state it wishes to reach, it allows the organization to develop a clear improvement plan. The CSF uses 'tiers' to tie profiles to the organization's risk management processes. The more sophisticated the process, the higher the tier, which is intrinsically linked to the effectiveness of cybersecurity measures.

The CSF explains that profiles should be regularly reviewed. As the organization's objectives and requirements change – whether related to business opportunities, legislation, or contracts – target profiles may change. Target profiles may also need to adapt to new technologies or threats.

The CSF provides examples of how you might manage improvement. Because the organization defines its target profiles and tiers, it is an effective model for reaching a defined state of cybersecurity (such as when mandated through contracts), but it pays less attention to managing the effectiveness of cybersecurity already in place.

'Tiers' are part of the continual assessment and improvement process. By integrating them into audit, monitoring, and reviewing practices, you can set goals for improvement.

Continual improvement – ISO 27001

ISO 27001 places a significant emphasis on continual improvement, and demands a very structured, cyclical approach. The Standard takes into account that influencing factors are expected to change over time.

ISO 27001 requires organizations to review their ISMS on a regular and scheduled basis, to ensure it is running at optimal levels and that it keeps up with evolving threats.

Clauses 5.1 and 5.2 specify that the organization's leadership shall support continual improvement, and that this commitment to continual improvement be included in the information security policy. As such, there should be pressure from the organization's top management to ensure that the ISMS is not only effective but in a constant state of improvement – both in terms of protecting information assets and in the return on investment. This is supported by Clause 9.3, which states that top management must review the organization's ISMS at regular intervals, taking into account the results of continual testing and measurement.

Guidance materials – NIST CSF

NIST Special Publication 800-53 (SP 800-53) provides a catalog of security and privacy controls designed to protect organizations' vital operations and assets, while also protecting the privacy of individuals.

A primary objective of SP 800-53 is to make computer systems resistant to attacks and limit the damage from attacks when they occur. SP 800-53 provides control guidance for all computing platforms, including:

- General purpose computing systems
- Cyber-physical systems
- Cloud and mobile systems
- Industrial/process control systems
- Internet of Things (IoT) devices

NIST SP 800-37 provides guidance on NIST's Risk Management Framework – a standard that provides a process for integrating security and risk management activities into the system development life cycle – through the following steps for security:

1. Categorize system
2. Select controls
3. Implement controls
4. Assess controls
5. Authorize system
6. Monitor controls

The publication helps align risk management systems with the organization's mission and business objectives. It also makes sure that the

system is properly integrated into the enterprise architecture and system development life cycle processes.

NIST SP 800-171 documents 110 recommended requirements to protect controlled unclassified information (CUI) under certain conditions, such as when it exists within non-federal information systems. The guidance directs organizations to ensure security compliance rules are built into contracts.

The publication maps security controls from NIST SP 800-53 and ISO 27001 to the 110 requirements in order to provide guidance on compliance.

Guidance materials – ISO 27001

ISO 27002 is the code of conduct – recommended and preferred practices – that can be used to implement ISO 27001. The practices described in ISO 27002 are considered internationally applicable and include guidance on the 14 control categories listed in Annex A of ISO 27001.

ISO 27005 further elaborates on the concepts specified in ISO 27001, and was created to help implement information security risk management. Like other ISO 27000-series standards, it is designed to be compatible with ISO 27001.

Other publications in the ISO series go into considerably more detail about specific aspects of information security, such as **ISO 27035-1**, which offers more detailed information on information security incident management.

NIST CSF and ISO 27001 resources

Sometimes, help from an external source may be necessary. For ISO 27001, there is an immense amount of outside resources such as consultants, and information sharing and analysis centers (ISACs). Similarly, there is a lot of support for the NIST CSF, including information experts from the government and federal agencies.

Certification/third-party assurance

Organizations may seek certification to a scheme in order to demonstrate compliance to their partners and customers. In some cases, they may do so in pursuit of business opportunities.

There is currently no certification scheme for the NIST CSF. ISO 27001 certification, however, is a rigorous process, which means that an organization can prove its security credentials by presenting the certificate to new and existing clients as proof that their ISMS has been audited by an independent third party.

ISO 27001-accredited certification demonstrates to others that your organization is taking effective measures to protect private data. Without certification, you might have to submit to external audits from every one of your partners or clients, which is disruptive and a drain on budgets and productivity.

Recognition

Both the NIST CSF and ISO 27001 can benefit your organization and are compatible with one another, as well as other frameworks. Both frameworks are internationally recognized.

NIST publications in general are highly regarded overseas due to their thoroughness and because they are often mandated for working with the US government. Due to the certifying power of ISO 27001, it is recognized by organizations and governments around the world, and is often noted as providing evidence of compliance with data protection laws and regulations.

Useful NIST CSF and ISO 27001 resources

Implementing the NIST Cybersecurity Framework or ISO 27001 can be a large and complex project, with many moving parts. However, it can help your organization to better protect its critical information assets as well as the systems on which they reside. With the right support, an organization will be able to accomplish an implementation within the allotted time and budget. IT Governance, a global market leader in information security consulting, tools, and training, can offer guidance to steer you in the right direction while simplifying the process.

A leading global authority on information security, IT Governance helps organizations address the challenges of NIST compliance with a comprehensive suite of information resources, toolkits, training, and advisory services.

IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses and professional consultancy services.

<table>
<tr><th colspan="3">NIST and ISO 27001 solutions and services</th></tr>
<tr><td rowspan="2">Information resources</td><td colspan="2">Standards</td></tr>
<tr><td colspan="2">ISO/IEC 27001:2013 (ISO 27001 Standard) ISMS Requirements

ISO 27001 is the standard detailing the specifications of an information security management system (ISMS) that your organization can implement to improve the state of its information security.</td></tr>
<tr><td rowspan="3">Education</td><td colspan="2">Training courses</td></tr>
<tr><td colspan="2">ISO27001 Certified ISMS Foundation Training Course

Take the first steps towards building a career in ISO 27001. Learn from the experts about ISO 27001 best practice and find out how to achieve compliance with the Standard.

ISO27001 Certified ISMS Lead Implementer Training Course

This certificated, practitioner-led course equips you with the skills to lead an ISO 27001-compliant information security management system (ISMS) implementation project.</td></tr>
<tr><td>Live Online

Our unique real-time online training courses let delegates study from any location in the world and acquire the knowledge to implement and audit compliance to international IT standards and best practice frameworks.</td><td>E-learning

Increase your employees' awareness of information security and ISO 27001 with the expertise at IT Governance.</td></tr>
<tr><td rowspan="2">Software</td><td colspan="2">Risk assessment software</td></tr>
<tr><td colspan="2">vsRisk Standalone - Basic</td></tr>
</table>

	vsRisk™ is a leading information security risk assessment tool that delivers fast, accurate, auditable and hassle-free risk assessments year after year.
Productivity tools	**Toolkits** ISO 27001 Cybersecurity Documentation Toolkit This ISO 27001 toolkit provides all of the information security management system (ISMS) documents you need in order to comply with the Standard.
Advice and consultancy	**Consultancy** ISO 27001 Consultancy We have helped more than 600 companies successfully implement an ISO 27001 ISMS. We provide a 100% certification guarantee.
Comprehensive solutions	**Packages** Comprehensive Solutions Packages The most comprehensive mix of ISO 27001 tools and resources available on the market. Choose from four expertly curated packages to meet the unique needs of your organization.

Contact us: **+1** 877 317 3454
www.itgovernanceusa.com servicecenter@itgovernanceusa.com

[1] Department of Homeland Security, "Critical Infrastructure Sectors", July 2017, https://www.dhs.gov/critical-infrastructure-sectors.
[2] NIST, "Guide to Industrial Control Systems (ICS) Security", June 2011, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf.
[3] Jesse Dunietz, "Is the Power Grid Getting More Vulnerable to Cyber Attacks?", *Scientific American*, August 2017, https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/.
[4] Identity Theft Resource Center, "2017 – Data Breach Category Summary", December 2017, http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReportSummary2017.pdf.
[5] Steve Morgan, "2017 Cybercrime Report", *Cybersecurity Ventures*, 2017, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.
[6] Ponemon Institute, "2017 Ponemon Cost of Data Breach Study", 2017, https://www.ibm.com/security/data-breach.
[7] NIAC, "Securing Cyber Assets – Addressing Urgent Cyber Threats to Critical Infrastructure", August 2017, https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.