27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

How to implement NIST Cybersecurity Framework using ISO 27001

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Executive summary

An organization can find many alternatives available in the market, from best practices to internationally recognized standards, to address information security risks. But, although many of these clearly state that their requirements and recommendations are not exhaustive, and should be complemented with other practices, there are not too many materials regarding the integration of practices.

In this document, you will find information about ISO 27001, the leading ISO standard for information security management, and NIST Cybersecurity Framework, a response to the U.S. Presidential Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, issued in 2013. You'll learn about their similarities and differences, and how they can be used together to improve information protection. Furthermore, you'll find links to additional learning materials like articles and other white papers.

Introduction

In order to maintain the trust of customers and organizations in the use of cyber environments, as well as the normal operations of critical infrastructures that support them, a proactive risk management approach is now part of many managers' agendas. That can involve the implementation of multiple standards, frameworks, and best practices, adopted either as mandatory or voluntarily.

In scenarios with multiple approaches, an integrated management system can prove to be very valuable. Such integration can take advantage of the best security measures of each approach, while optimizing resources, making it more likely that the organization will withstand cyber risks against its information and infrastructure, and successfully achieve its objectives in a cost-effective way.

Considering this, the purpose of this white paper is to present a U.S. approach to managing cyber security risks, NIST Cybersecurity Framework. We'll examine its similarities and differences compared to ISO 27001, the leading ISO management standard for information security, and how the two can be integrated and applied together to manage cyber security risks.

Why should an organization care about cyber risk and cyber security?

Cyber risk and cyber security are concepts mainly related to information technology. Even so, the impacts of incidents in cyber environments, and the savings that can be achieved through security controls, are evident in business operations, in terms of:

Customers: Incidents involving the unauthorized access or disclosure of personal information can have a serious impact on the lives of the people to whom it belongs. By avoiding this kind of damage, you can save your organization a series of legal proceedings that can be tedious, stressful, and expensive.

Financial costs: Besides losses stemming from customer-related risks, there are other ways cyber risks can cost an organization money. Ransomware and malware attacks can cost thousands of dollars by making information useless or unavailable. And, by not managing your cyber risks properly, your organization may have to spend more in terms of insurance costs.

Business advantages: Business strategies, production plans, trade secrets, or any other sensitive business information that is compromised by a cyber incident can cost millions of dollars to an organization in terms of business competitiveness.

Organization reputation: After an incident has become public knowledge, an organization will have a hard time retaining its current customers – not to mention finding new ones – regardless of any subsequent efforts to improve security.

Personal careers: Being remembered or associated with a cyber security incident can not only end a career, but also subject the person to legal processes. This is especially true for top management, who has the power and duty to be diligent regarding business security.

So, in short, an organization’s leaders and managers who want to protect their company and personnel should take steps to prevent these outcomes and keep their customers’ information secure.

An overview of NIST Cybersecurity Framework

Cybersecurity Framework (CSF) is the common name of the document “Framework for Improving Critical Infrastructure Cybersecurity,” published by the National Institute of Standards and Technology (NIST) on February 12, 2014.

CSF follows the U.S. president’s executive order “Improving Critical Infrastructure Cybersecurity” issued in 2013, and was initially intended for U.S. companies that are considered to be part of critical infrastructure (e.g., communication, information technology, defense industrial base, etc.). However, it is suitable for use by any organization that faces cyber security risks, though it is voluntary.

The framework is divided into three parts:

Core: contains an array of activities, outcomes, and references, organized into five functions (Identify, Protect, Detect, Respond, Recover), 22 categories, and 98 subcategories, with detailed approaches to aspects of cyber security.

Implementation Tiers: these four tiers (Partial, Informed, Repeatable, Adaptive) can be used by an organization as references to clarify for itself and its partners the organization’s visions on cyber security risk and the degree of sophistication of the management approach.

Profile: a list of outcomes that an organization can choose from the categories and subcategories, based on its business needs and individual risk assessments (Current Profile), as means to support prioritization and measurement of progress toward a desirable risk level (Target Profile).

For more detailed information, you can review the NIST document at the following link. (The document is publicly available and is free of charge).

Understanding ISO 27001

Published by the International Organization for Standardization (ISO) in 2005, and revised in 2013, ISO/IEC 27001 is an information security standard. Although not mandatory, it is accepted all over the world as a de facto main framework for information security / cyber security implementation.

ISO 27001 comprises two distinct sections:

Main content: composed of 11 sections, from which sections 4 to 10 define requirements for the establishment, implementation, maintenance, and continual improvement of an Information Security Management System (ISMS).

Annex A: a set of 35 control objectives and 114 generic security controls, grouped into 14 sections, which provide orientation on how to treat risks identified as unacceptable through the risk assessment process.

For more detailed information, you can read the following white paper: Clause-by-clause explanation of ISO 27001.

NIST CSF and ISO 27001 similarities

The secret to successfully integrating two separate programs is understanding how they are similar and how they are different, so you can know what to put together and what to break apart.

So, let's first take a look at the common points between NIST CSF and ISO 27001:

Implementation based on methodology: Both CSF and ISO 27001 provide methodologies for how to implement cyber security and information security in an organization. Although their steps are not 100% aligned, minor adaptations can easily narrow the gaps.

Clauses for ISO 27001 implementation	NIST CSF steps for implementation of a cyber security program
Clause 4 – Context of the organization	Step 1 - Prioritize and Scope
Clause 5 – Leadership	CSF considers most of the requirements related to leadership as controls to be implemented as the result of risk assessment.
Clause 6 – Planning	Step 2 – Orient Step 1 - Prioritize and Scope
Clause 7 – Support	Step 6 - Determine, Analyze, and Prioritize Gaps
Clause 8 – Operation	Step 2 – Orient Step 3 - Create a Current Profile Step 4 - Conduct a Risk Assessment Step 5 - Create a Target Profile Step 6 - Determine, Analyze, and Prioritize Gaps Step 7 - Implement Action Plan
Clause 9 – Performance evaluation	Step 7 - Implement Action Plan
Clause 8 – Continual improvement	Although there is no specific step for continual improvement, CSF recommends all steps should be repeated as necessary to continuously improve cyber security.

From the table above, we can see that NIST CSF is more focused and detailed on the operation phase than in planning. This occurs because CSF assumes that an organization already has management practices implemented, and the framework for cyber security is to be integrated with them.

For a better understanding of how to develop a risk assessment and risk treatment process approach that can be used to support CSF, see these articles: ISO 27001 risk assessment & treatment – 6 basic steps and Risk Treatment Plan and risk treatment process – What's the difference?

Security implementation based on risk management and recommendations: In both approaches, security controls and safeguards are implemented only if risks are considered unacceptable, and also provide references for control development.

ISO 27001 Annex A control sections	NIST CSF control categories
A.5 – Information security policies	Governance
A.6 – Organization of information security	Asset Management; Governance; Risk Assessment; Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Detection Processes; Communications
A.7 – Human resource security	Governance; Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures
A.8 – Asset management	Asset Management; Data Security; Information Protection Processes and Procedures; Protective Technology
A.9 – Access control	Identity Management and Access Control; Data Security; Protective Technology
A.10 – Cryptography	There is no specific category covering cryptographic controls.
A.11 – Physical and environmental security	Asset Management; Business Environment; Identity Management and Access Control; Data Security; Information Protection Processes and Procedures; Maintenance; Protective Technology
A.12 – Operations security	Business Environment; Risk Assessment; Data Security; Information Protection Processes and Procedures; Protective Technology; Security Continuous Monitoring; Analysis; Mitigation

A.13 – Communications security	Asset Management; Identity Management and Access Control; Data Security; Protective Technology
A.14 – System acquisition, development and maintenance	Data Security; Information Protection Processes and Procedures; Security Continuous Monitoring; Detection Processes
A.15 – Supplier relationships	Business Environment; Supply Chain Risk Management; Maintenance; Security Continuous Monitoring
A.16 – Information security incident management	Information Protection Processes and Procedures; Anomalies and Events; Detection Processes; Response Planning; Communications; Analysis; Mitigation; Improvement; Recovery Planning
A.17 – Information security aspects of business continuity management	Business Environment; Risk Assessment; Information Protection Processes and Procedures; Protective Technology
A.18 – Compliance	Governance; Risk Assessment; Information Protection Processes and Procedures; Detection Processes

Technology neutrality: Both CSF and ISO 27001 rely on general concepts of security, which gives organizations the freedom to adopt the technologies most suitable for their environments.

Cross-industry applicability: Although CSF was created for use by U.S. organizations part of the so-called "critical infrastructure," it can be applicable to any type of organization, as can ISO 27001.

Focus on adding value to the business: Both CSF and ISO 27001 have, as their ultimate goal, to deliver business benefits through risk management, while observing legal and regulatory requirements, as well as requirements of all interested parties.

NIST CSF and ISO 27001 differences

Now that we have seen which points these two approaches have in common, let's take a look at their differences (and, by differences, I do not mean things that will work against each other and exclude each other – on the contrary, they are synergistic):

Cybersecurity Framework provides better support for implementation of controls and safeguards. Besides ISO 27001, CSF works side by side with other well-known frameworks and best practices, like COBIT (Control Objectives for Information and Related Technologies), NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), ISA 62443 (Security for Industrial Automation and Control Systems), and CCS CSC (Council on Cyber Security Top 20 Critical Security Controls), which makes CSF better suited for integration than ISO 27001.

Cybersecurity Framework provides a basis for self-assessment and definition of objectives. Via Profiles (Current and Target), and Implementation Tiers (Partial, Risk Informed, Repeatable, and Adaptive), organizations have a solid basis to identify where they are at the moment and what they want to achieve, making it easier to define the task, how far they want to go with their implementation, and which action plans should be developed for closing the gaps.

ISO 27001 is certifiable. There are many benefits to be had with a system in which a third-party who is trusted by your clients, partners, and regulators can vouch for your efforts to keep information safe. Money saved by consolidating specific audits for each interested party into a single one accepted by all of them, better public image, and increased competitiveness are just some of the ways this can pay off.

ISO 27001 is internationally recognized. No matter how good NIST CSF is, if any organization outside the U.S. wants to prove its ability to protect its clients, partners, and other interested parties against cyber risks, ISO 27001 will be a much better option than NIST CSF.

ISO 27001 goes beyond IT. IT environments are only one aspect that needs to be considered when we want to protect information. Paper-based information, as well as information flowing through conversations and meetings, also needs to be protected, and ISO 27001 is better prepared to manage these situations.

Integration of ISO 27001 and NIST Cybersecurity Framework

By reviewing the similarities and differences between ISO 27001 and NIST CSF, we can note that combining them can bring more advantages than complications. But, how can this be done?

We have three scenarios to consider:

1. An organization has already implemented ISO 27001, and wants to adopt NIST CSF.
2. An organization has already implemented NIST CSF, and wants to adopt ISO 27001.
3. An organization has no structured approach to information security, and is searching for alternatives.

NIST Cybersecurity Framework is a better fit for defining the security profiles that are to be achieved, and for structuring the security controls and safeguards that are to be implemented, especially those related to cyber environments. ISO 27001 is a better fit for integrating all elements in a cohesive system aligned with the overall context of an organization's management and productive processes. That said, in each scenario, the best results can be achieved as follows:

An organization has already implemented ISO 27001, and wants to adopt NIST CSF.

For this scenario, because all elements of the management system are already in place, the organization should consider:

- Reviewing the risk management process, to include the concepts of Current Profile and Target Profile.
- Using the Statement of Applicability and the Framework Core to create a Current Profile.
- Performing an internal audit of its risk management process and implemented controls, considering as a reference the NIST CSF Framework Core and Framework Implementation Tiers. This way, the organization will have an overview of how compliant its current controls are.
- Defining a Target Profile, considering the created Current Profile, business and security objectives, and the results of the internal audit.
- Preparing action plans to achieve the proposed Target Profile.

An organization has already implemented NIST CSF, and wants to adopt ISO 27001.

For this scenario, because most of the elements of the management system probably will not be in place formally, the organization should first consider reviewing NIST CSF implemented controls, with consideration of ISO 27001 clauses. The following table can help you focus on the most relevant NIST CSF categories:

ISO 27001 clauses	**NIST CSF control categories**
Clauses 4.1 to 4.3	Business environment
Clause 4.4	Governance
Clauses 5.1 to 5.3	Governance
Clause 6.1	Risk Management Risk Assessment Information Protection Processes and Procedures
Clause 7.3	Awareness and Training
Clause 7.4	Communication
Clause 7.5.3	Data Security
Clauses 8.2 and 8.3	Risk Assessment
Clause 9.1	Detection Process and Protective Technology
Clause 10.1	Improvements

After this review, you should be able to identify what kind of documentation and records you already have, and develop action plans to implement what is left.

ISO 27001 clauses 6.2 (Information security objectives and planning to achieve them), 7.1 (Resources), 7.2 (Competences), 7.5.1 (General), 7.5.2 (Creating and updating), 8.1 (Operational planning and control), 9.2 (Internal audit), 9.3 (Management review), and 10.2 (Continual improvement) do not have a direct correlation with NIST CSF and should be developed from scratch.

An organization has no structured approach to information security, and is searching for alternatives.

It may not seem like it, but this situation is the easiest to deal with because you are facing a clean start. The recommendation for this approach is to design all of the information security and cyber security according to ISO 27001 (clauses 4, 5, 7, 9, and 10), and use Cybersecurity Framework when it comes to risk management and implementation of the particular cyber security controls and safeguards.

In general, you should consider these steps in the implementation process:

1. Obtain management support.
2. Treat the implementation as a project.
3. Define the scope.
4. Write an ISMS policy.
5. Define the risk assessment methodology (here you should also consider including the concepts of Current Profile and Target Profile from NIST CSF).
6. Perform the risk assessment & risk treatment.
7. Write the Statement of Applicability.
8. Write the Risk Treatment Plan.
9. Define how to measure the effectiveness of controls.
10. Implement the controls & mandatory procedures.
11. Implement training and awareness programs.
12. Operate the ISMS.
13. Monitor the ISMS.
14. Perform the internal audit.
15. Conduct the management review.
16. Take corrective and preventive actions.

For more detailed information, please see this Diagram of ISO 27001:2013 Implementation Process.

For more information, review the following white paper: Diagram of ISO 27001:2013 Risk Assessment and Treatment process, so you can better understand the risk management process in practice.

Conclusion

Although ISO 27001 provides globally recognized practices, this doesn’t mean that it is the definitive answer for information security. The security implementation must have a holistic view to be effective, and for that, the more inputs you have to set your controls, the better your chances to develop strong defenses and improve your results.

NIST Cybersecurity Framework is a great resource to help design ISO 27001 IT-related controls, and by combining these two approaches, an organization can achieve more reliable and cost-effective results in the implementation, management, and operation of its security controls, improving security levels and users’ confidence.

And, viewing from a CSF implementation perspective, by integrating it with a full management structure, like that provided by ISO 27001, you can take advantage of dealing effectively with challenges like limited resources, organizational alignment, and higher expectations from customers and other interested parties (e.g., government and regulatory bodies) – regardless of your market.

Therefore, if you have a critical dependency on information and cyber environments in your organization, you should consider integrating ISO 27001 and NIST Cybersecurity Framework, to develop aligned security practices and stronger cyber security, allowing your organization to optimize resources and improve business results.

Sample ISO 27001 documentation

Here you can download a free preview of our ISO 27001 Documentation Toolkit. This will allow you to view sample policies and procedures required to implement ISO 27001:2013.

References

27001 Academy
NIST Framework
Free eBook- 9 Steps to Cybersecurity

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

9001 Academy 9100 Academy 13485 Academy 14001 Academy 16949 Academy 18001 Academy

20000 Academy 27001 Academy Conformio eTraining AdviseraBooks

Advisera
Making certification simple.