...making excellence a habit.™

The Framework for Cybersecurity – Who Needs It And Why?

A whitepaper

The Framework for Cybersecurity – Who Needs It And Why?

Five years ago, the writing was on the wall.

In early 2013, President Obama issued EO 13636, directing the National Institute of Standards (NIST) to work with stakeholders from around the globe who were interested in voluntarily developing a framework for cybersecurity. The EO also stipulated that the framework should be based on existing standards, guidelines and practices. The work would be done in an effort to reduce cybersecurity risks within organizations that operate critical infrastructure. In the five years that have passed, the NIST Framework and cybersecurity strategies that have been built upon it have grown in importance as threats to critical infrastructure have increased in number and their potential to cause harm.

Globally the definition of critical infrastructure is generally aligned. "Critical Infrastructure" means systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, the economy, national public health or safety, or any combination of those matters.

> "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the nation's infrastructure in the face of such threats."
>
> **-Excerpted from Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, February 2013**

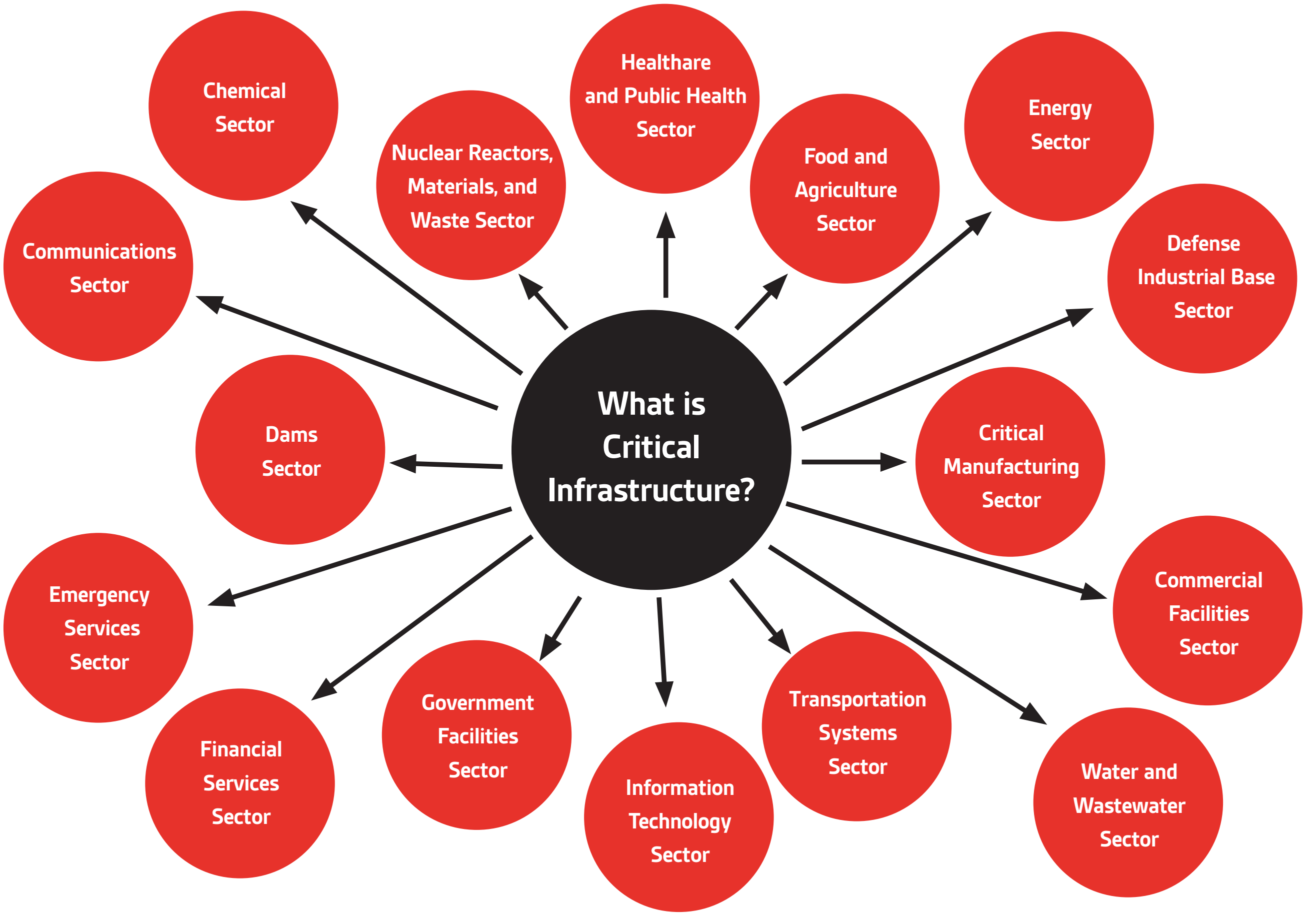

What is Critical Infrastructure?
Chemical Sector
Healthare and Public Health Sector
Nuclear Reactors, Materials, and Waste Sector
Food and Agriculture Sector
Energy Sector
Communications Sector
Defense Industrial Base Sector
Dams Sector
Critical Manufacturing Sector
Commercial Facilities Sector
Emergency Services Sector
Government Facilities Sector
Transportation Systems Sector
Financial Services Sector
Information Technology Sector
Water and Wastewater Sector

Figure 1: The 16 critical infrastructure sectors as defined by the Department of Homeland Security.

The NIST Framework: Structure & Requirements

After the order was signed, the Framework was built through a series of workshops under the guidance of NIST by cross-functional teams representing the needs of global industry. Today, the Framework offers operators of critical infrastructure and other entities a cost-effective, flexible, prioritized and repeatable approach to the creation and application of information security and cybersecurity measures.

The Framework is risk-based and it is comprised of three parts:

1. The Framework Core

2 The Framework Profile

3. The Framework implementation Tiers

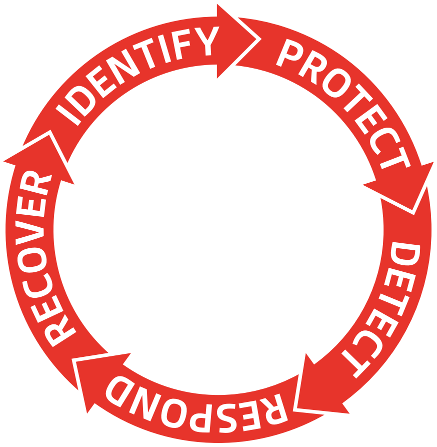
The Framework Core consists of a set of activities that helps organizations achieve specific cybersecurity outcomes. It also references examples of guidance that can be used to achieve those outcomes and have been identified by stakeholders as helpful in their efforts to manage cybersecurity risk. The Framework Core is comprised of four elements:

1. Functions

2. Categories

3. Subcategories

4. Informative References



The Framework Core's five concurrent and continuous Functions include Identify, Protect, Detect, Respond and Recover. When considered together, these functions provide a high-level strategic view of the cybersecurity lifecycle and/or an organization's management of its cybersecurity risk.

The Framework Core also identifies underlying key Categories and Subcategories for each function. These are matched with Informative Reference examples such as existing standards, guidelines and practices for each Subcategory.

The Framework Profile helps to align the Functions, Categories and Subcategories with the specific business requirements, risk tolerance and resources of an organization.

The Framework Implementation Tiers provide context regarding how an organization views cybersecurity risk, and, the processes that it has in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4). They describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They also delineate the extent to which cybersecurity risk management is informed by an organization's needs and how well that is integrated into its overall risk management practices.

To enjoy the most success with the Framework, organizations are urged to select the Tier that: 1) best meets their goals, 2) is feasible to implement, and 3) reduces cybersecurity risk to critical assets and resources to acceptable levels.

With all these pieces working together, the Framework increases an organization's information security transparency. This in turn protects its confidentiality as well as individual privacy and civil liberties.

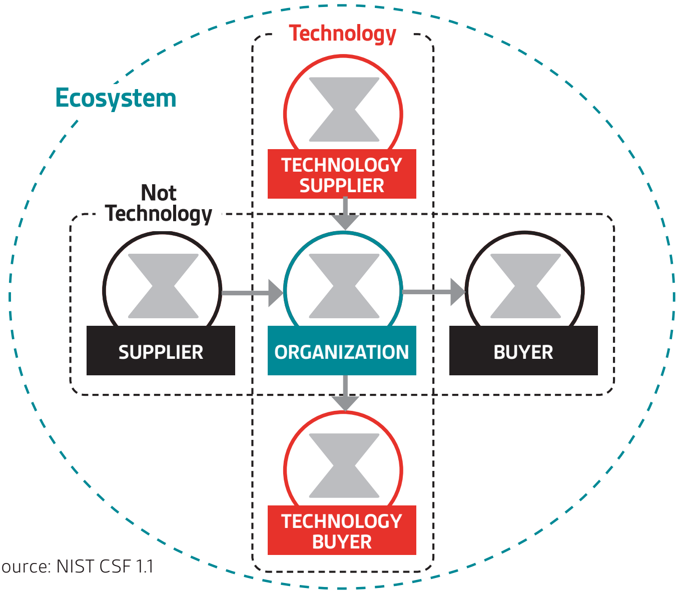
Securing the Supply Chain

Version 1.1 of the NIST Framework added guidance to help organizations secure their supply chain relationships. Because an organization is only as strong as its weakest supplier, it is imperative to work closely with suppliers to understand the cybersecurity risks that they can introduce.

In essence, the NIST Framework's profile is a prioritized list of cybersecurity requirements. Organizations can create and use target profiles to make informed decisions about their suppliers, including what type of cybersecurity processes the supplier has in place and if they continuously increase transparency of those processes. Organizations also can use target profiles and onsite or virtual audits to track and address residual cybersecurity risk. For example, an organization might implement these tools if it wants to use a product or service that does not meet the terms of their cybersecurity requirements right out of the box

While supply chain cybersecurity risk is very important, to date, many companies do not have a great deal of experience with it. Typically, this is due to a lack of resources and tight budgets. It takes a reasonable number of resources and money to create and enact a strong supply chain cybersecurity management process. When it is done correctly, however, it does result in significant improvements.

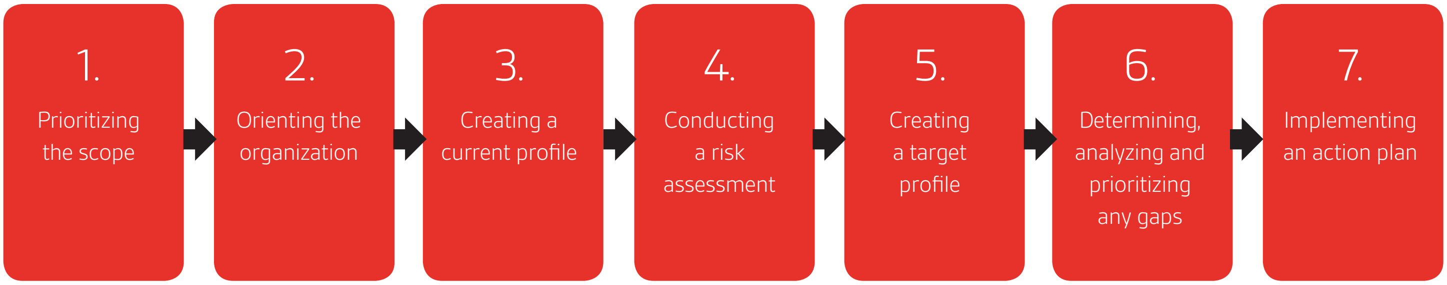
Cybersecurity Supply-Chain Relationships



Source: NIST CSF 1.1

Seven-Step Framework & Governance

Coordination of the Framework is broken down into seven steps:



1. Prioritizing the scope
2. Orienting the organization
3. Creating a current profile
4. Conducting a risk assessment
5. Creating a target profile
6. Determining, analyzing and prioritizing any gaps
7. Implementing an action plan

These steps enable organizations to measure where they are today, determine where they want to be tomorrow and act on the differences.

Prioritizing the Scope requires planners to consider the scope and context of their organizations. They also must determine where the Framework fits into subsets of their critical operations and in which areas it is needed.

Scope should be based on management considerations, organizational objectives and priorities as well as other internal or external factors including other interested parties that have a stake in the organization. Organizations using the Framework for the first time may want to limit their scope initially to get familiar with it first.

Scope also includes assets and services that are: 1) Out-of-Scope – Internal but Interrelated/Outside the scope but Within the Organization and 2) Out of Scope – External but Interrelated.

Orienting the organization

When orienting themselves, organizations identify their in-scope system assets, people, processes, information technology, facilities, regulations and informative references. This includes any cybersecurity and risk management standards, methods and guidelines. It is important to evaluate all of the above in a manner that helps to better understand the overall effectiveness of the organization.

Creating a Current Profile

By using the same evaluation approach as orienting, organizations take a look at the same in-scope systems and assets listed above along with the activities that enable them to identify their current cybersecurity risk management stake. Outputs from that evaluation comprise a current profile and indicate the proper Tier level for the organization to utilize.

Conducting Risk Assessment

The risk assessment involves using the Framework to perform a risk management process by evaluating an organization's risk management strategy and methodology. The assessment considers all in-scope portions of an organization and evaluates regulatory requirements, as well as all applicable cybersecurity risk management standards, tools and guidelines.

Creating a Target Profile

Looking ahead to where the organization wants to be next against where it is today develops the target profile.

Determining, analyzing and prioritizing

The next step is to take that target profile, determine the gaps, identify the issues that must be addressed as well as the actions required to get there. Equally important, organizations must understand who the owners and stakeholders are in order to develop a plan that will succeed.

Implementing the plan

After determining where you are, where you want to be, and the plan to overcome the gaps and obstacles, it is time to implement the plans and start the cycle again.

Good Governance

What determines a reasonable approach? A good cybersecurity plan requires good governance of risk. The plan must take into consideration any privacy implications, especially in light of regulations such as GDPR. Thorough training ensures that individuals within an organization understand their responsibilities and their ownership of security processes, procedures and outcomes. People also need to know who they report to at the management level.

Management must exemplify good cybersecurity leadership and understand the strategic direction of the company. Top management also must support 1) compliance of an organization's cybersecurity processes, 2) all applicable privacy laws and regulations, and 3) any local, national and global requirements.

Once a cybersecurity system and good governance are implemented, organizations must employ appropriate metrics. The metrics enable organizations to continuously determine how effective their new processes are and how much value they are producing in terms of adequate or improved cybersecurity. Metrics fuel necessary vigilance as new cybersecurity threats emerge every day.

Maturity

None of the above takes place overnight. Implementing a cybersecurity framework takes time and time yields the benefit of maturity. Partial compliance or implementation indicate that an organization is at a lower level of maturity than an organization that has fully implemented the Framework and is operating in compliance with it. Having a robust cybersecurity framework and posture in place is expected at an organization that operates critical infrastructure; however, even the smallest organizations need a compliant and robust cybersecurity strategy that addresses their level of complexity and risk.

Harmonizing the NIST Framework Around the Globe

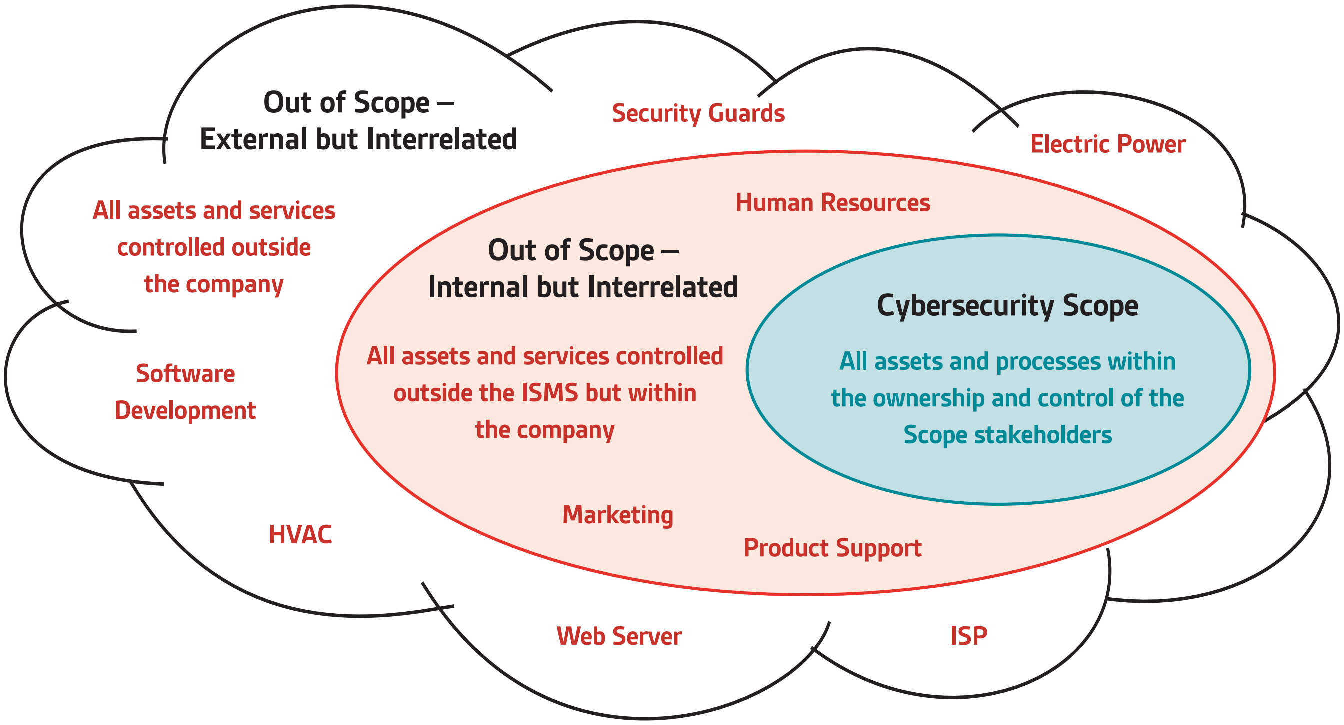
When it was launched, the ISO/IEC 27001 Information Security standard; which is an informative reference in the NIST Framework, attracted the interest of organizations worldwide. Today, the NIST Framework is being adopted globally. In the US, the National Highway Transportation Safety Administration has urged auto manufacturers to use it to mitigate threats related to vulnerabilities and protect assets such as those found in connected cars. In addition, multi-national IT and cloud computing companies are increasingly interested in certification.

In terms of international harmonization, the newly released ISO/IEC 27103, (Information technology — Security techniques — Cybersecurity and ISO and IEC Standards) uses the NIST CSF terminology and structure as a foundation.

> A statement of cooperation between the U.S. and the U.K. was issued following a meeting between President Obama and Prime Minister David Cameron. It includes a reference to the NIST Framework of standards as a basis for international harmonization on industry "best practices." The two leaders agreed that cyber threats are among the most "serious economic and national security challenges that both nations face," according to a fact sheet issued by the White House.

While it does not name the NIST Framework formally, it provides references to the NIST Framework structure and how it's used with other standards.

Pictorial Scope (Example)


Out of Scope – External but Interrelated
All assets and services controlled outside the company
Security Guards
Electric Power
Software Development
HVAC
Web Server
ISP
Human Resources
Out of Scope – Internal but Interrelated
All assets and services controlled outside the ISMS but within the company
Marketing
Product Support
Cybersecurity Scope
All assets and processes within the ownership and control of the Scope stakeholders

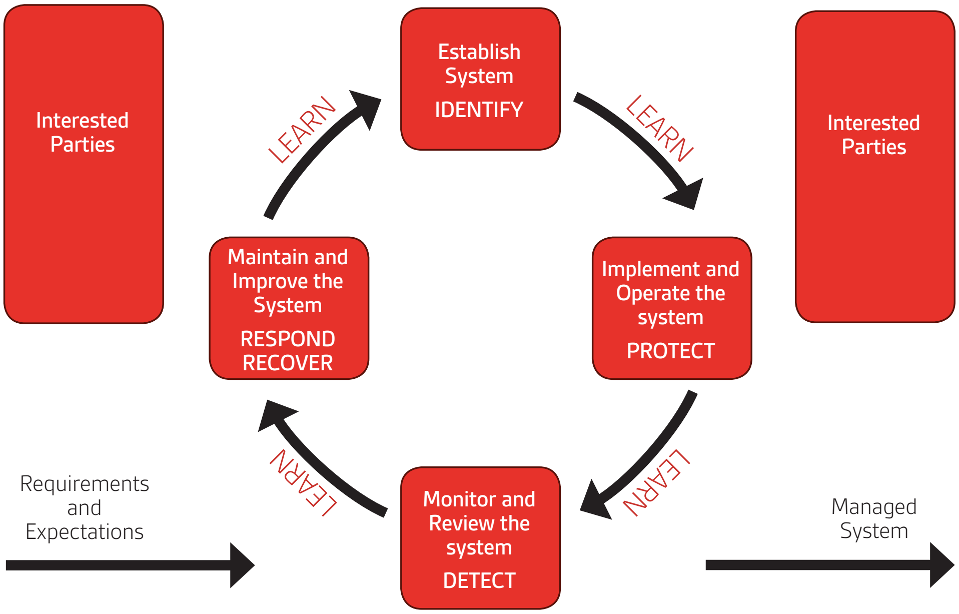
The Cybersecurity Lifecycle

Adding to the initial seven steps previously described, are four system-level steps that integrate with the Plan Do Check Act. (Figure ....) along with the work-learn process of the Cybersecurity Lifecycle:

1. Identify – establish system
2. Protect – implement and operate system
3. Detect – monitor and review system
4. Respond/Recover – maintain & improve system

When put in the context of the Framework, these four steps exemplify the fact that cybersecurity must be an ongoing lifecycle. They provide a means for the elements of each organization's cybersecurity system to study and learn from real threats and calculate the risk of potential threats. Robust cybersecurity systems are constantly monitoring and adapting in real-time. When used with current standards, such as ISO/IEC 27001, the Framework's steps provide a holistic approach to cyber and information security.

How to Use the Framework



Mapping ISO/IEC 27001 to the Framework

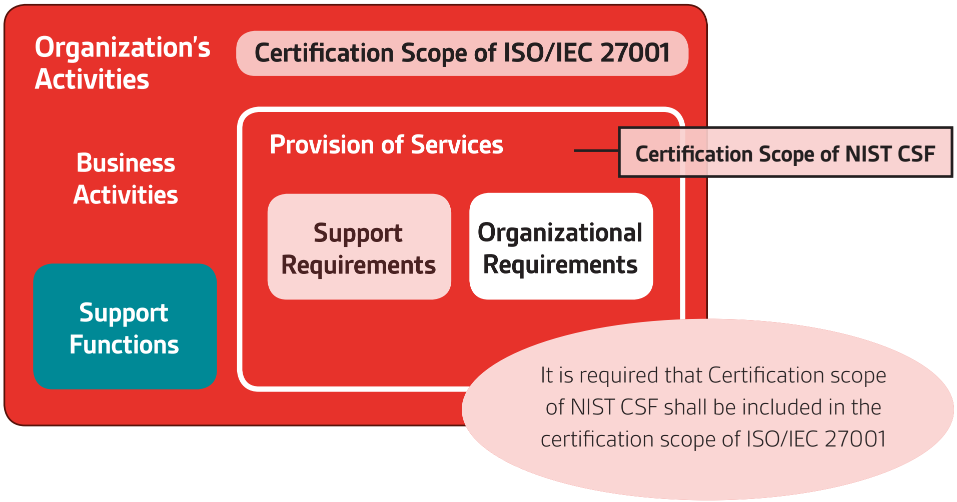
Risk management in ISO/IEC 27001 already exists and compliments many of the requirements of the Framework. Version 1.1, released in April 2018, closed a lot of the original gaps allowing for seamless integration into a formal ISO/IEC 27001 management system.

With regard to the Implementation Tiers, the ISO/IEC 27001 certification standard assesses the process by which an organization can evaluate the level of security maturity and validates that process. The Current Profile can be evaluated by a gap assessment using the Framework in conjunction with Annex A of ISO/IEC 27001, which also serves as a facilitator for assessing the Tier level. The Current Profile will be expanded by a number of additional clauses to create a Target Profile. All profiles must be documented.

The Framework does not specifically require descriptions of decision-making and information flows; however, that is reasonably well covered in the core clauses of ISO/IEC 27001's high level structure along with the governance and management systems portion of the standard.

It is required that the certification scope for NIST be included in the certification scope of the ISO/IEC 27001 process. This shows that it is being covered, as well as a provision for an organization's supply chain, organizational requirements and business activities. There are additional audit durations on top of what is required for ISO/IEC 27001 that are based on the size and complexity of an organization and its risk level. Therefore, each organization is evaluated on its own merit from that perspective.

Certification Scope of NIST CSF


Organization's Activities
Certification Scope of ISO/IEC 27001
Business Activities
Provision of Services
Certification Scope of NIST CSF
Support Requirements
Organizational Requirements
Support Functions
It is required that Certification scope of NIST CSF shall be included in the certification scope of ISO/IEC 27001

Certifying the Cybersecurity Framework:

There are an increasing number of organizations claiming that they are compliant to the Cybersecurity Framework; however, it is unclear just how much confidence can be placed in that statement. The Framework was intended to manage cybersecurity risk cost-effectively and based on an organization's needs without placing additional regulatory requirements on them. Instead, the Framework relies on a variety of existing standards, guidelines and practices, which enable critical infrastructure providers to achieve resilience. All of these elements should be recognized in any certification requirements.

In 2014, the NIST working group asked BSI if the Framework could be certified. BSI's experts agreed to research the viability of a certification model. Subsequently, BSI presented a model for certification at a NIST workshop in 2015 where feedback, questions and comments were taken and used as a feeder system to improve the model. In 2016, BSI issued a formal public Request for Information (RFI). Based on that input, the model was improved further and presented at the NIST Workshop in 2017. Final changes and improvements were made and BSI launched a pilot program with a large global client in late 2017, followed by the formal launch of the first NIST CSF certification in March 2018. The global ground swell and number of inquiries has grown exponentially since then with the first organization being certified in July 2018

Auditing

The audit process is very similar to ISO/IEC 27001 and the certification cycle for the Framework is synchronized with the ISO/IEC 27001 certification cycle. They are melded together as one holistic information security and cybersecurity process. In addition, everything is managed, monitored and audited as a single system for consistency.

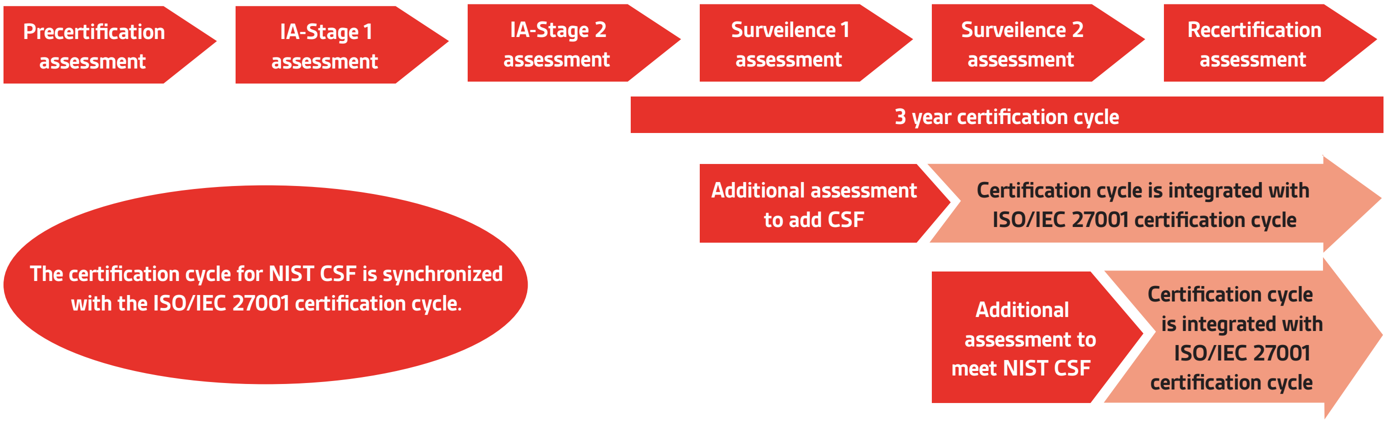
The ISO/IEC 27001 Statement of Applicability (SOA) reporting format documents the organization's understanding of both the aim and justification for each control. It also determines whether or not there is sufficient level of conformity in those areas of the Framework. After looking at the controls, an organization can use the standard to evaluate its Tier Level based on what the assessor sees. The assessor tries to match what he/she observes with objective evidence supplied by the organization and compares any differences. The assessor then provides feedback related to the maturity (or Tier) level using a proprietary model developed by BSI, which is subsequently measured based on a hybrid of internationally accepted standards. Those standards were used to build a fit-for-purpose process that allows for the measurement that provides context on how an organization views cybersecurity risk and how mature the processes are that manage that risk. (The Tiers or maturing levels range from Tier 1 partial to Tier 4 adaptive.)

Executive Level

When it comes to guidance and support for executive management, the BS 31111 Cyber Risk/Resilient Guidance Standard is targeted at an organization's senior level executives and professionals working in all sizes of organizations who have a responsibility and accountability for Risk Management and Information Security.

Non-technical in nature, and clearly written, BS 31111 is something that organizations like to put in the hands of their CEOs and CIOs. It provides them with a framework to assess and prioritize cyber risks in the context of their organizations and in the language they understand. By delivering best practice framework that can be used and understood effectively by a wide range of professionals, the guidance provided by BS 31111 delivers improved planning and value for organizations. It also helps people who use it to understand the importance of cybersecurity, how it should be working, and how it adds value to their organizations. BS 31111 also references the NIST Framework in many areas.

Audit Process for NIST CSF Certification


Precertification assessment
IA-Stage 1 assessment
IA-Stage 2 assessment
Surveilence 1 assessment
Surveilence 2 assessment
Recertification assessment
3 year certification cycle
Additional assessment to add CSF
Certification cycle is integrated with ISO/IEC 27001 certification cycle
The certification cycle for NIST CSF is synchronized with the ISO/IEC 27001 certification cycle.
Additional assessment to meet NIST CSF
Certification cycle is integrated with ISO/IEC 27001 certification cycle

BSI's experience gathered from thousands of audits indicate that the average ISO/IEC 27001 certified organization is at the Tier 3 level, i.e. that the system is effective and repeatable. The audits also provide evidence that people, processes and technology are being addressed on a continuous basis and more deeply into the organization. It is important to note that each area within the Framework – from recovery planning to improvements, to communications, to response planning – is evaluated on its own merit. Therefore, an organization could be Tier 3 on average, but a lower or higher Tier in other areas. That is why it is very important to get feedback from a competent and independent third party, another incredibly important management tool.

Organizations that pass their audits receive an additional certificate that shows their cybersecurity systems were evaluated and are in compliance with the NIST Cybersecurity Framework. Whether an organization is in cloud security, privacy, network system applications or specialist information security requirements, each maps directly to ISO/IEC 27001 and can be integrated with the Framework. This makes it a great foundation to build upon because it was created to manage all of an organization's security requirements.

Conclusion

Transparency, assurance and accountability are the key elements to increase trust, thus showing our governments, clients and all interested parties that industry takes cybersecurity seriously, which may in turn avoid unwanted regulatory legislation.

Security certifications are a good tool to increase trust, ONLY if:

- Auditors are qualified and properly certified,
- The control framework is relevant and its capability to address requirements can be verified, and
- The certifying body is totally independent and holds internationally accepted accreditations and the CB's own process is monitored and verified by the national/international accreditation bodies.

Find out more
Call US: +1 800 492 8977
Email: Inquiry.msamericas@bsigroup.com
Visit: bsigroup.com/en-us