Cybersecurity Frameworks

Table of Contents

What is a Cyber Security Framework?

These documents describe guidelines, standards, and best practices for cyber security risk management. These frameworks reduce an organization's exposure to weaknesses and vulnerabilities that cybercriminals can exploit. The word 'Framework' may seem like it is referred to some hardware, but it is not. It is, as mentioned before, a document. This document gives us information that deals with the infrastructure of servers, data storage, etc.

It is more like a structure, whereas we see the building standing tall in real life. It's all due to a solid system. But, when it comes to cyber security, the Cyber Security Framework is there to provide the foundation strength the servers need to be protected from cyberattacks.

Types of Security Frameworks

There are mainly three types of frameworks. Each of the types has its different functions. Those three types are −

- **Control Frameworks** − This framework is known to develop an essential strategy for the cyber security department of an organization. Along with this, it provides an array of security controls, understands the present state of the technology being used, and ensures that these security controls are implemented second to none.
- **Program Frameworks** − This framework analyses the state of the organization's security program. This also helps develop a customized cybersecurity program, measures the program's security, and goes through competitive analysis. Along with this, it also simplifies the communication between the cyber security team and the managers.
- **Risk Frameworks** − These frameworks suggest essential risk assessment and management processes. It helps in structuring a security program, identifying and measuring an organization's security risks, and prioritizing security measures and activities.

What is the best Cyber Security Framework out there?

When we must pick one framework for the organization, it can be very tough. There are many frameworks out there, and it's a tough job to test each one out and figure out the best one. So, we have put together the names of some of the best frameworks. The choice also depends a lot on the needs of the organization. So, there are some frameworks −

- The NIST Cyber Security Framework: The NIST is a set of security standards that many private companies and organizations can use to identify and respond to cyberattacks. This framework has guidelines to help organizations prevent and recover from such cyberattacks. NIST has five functions: Identity, Protect, Detect, Respond and Recover.

- The International Standards Framework (ISO): This is also known as the ISO 270K framework. It is considered the cyber security validation standard for both internal situations and across third parties. ISO 270K assumes that the organization has an Information Security management system. ISO/IEC 27001 requires management to exhaustively manage all the information security risks and to stay alert to threats and vulnerabilities. This can be inferred that the ISO framework is very demanding and requires a lot of hard work to maintain everything perfectly. This framework recommends about 114 different controls broken into 14 categories. If the ISO framework is implemented in an organization, then it will be a selling point for new customers. It is worth it!
- The Health Insurance Portability and Accountability Act: HIPAA provides a framework to manage confidential patient and consumer data, mainly privacy issues. This framework offers electronic healthcare information and is a must for healthcare providers, insurers, and clearinghouses.
- The Centre for Internet Security Critical Security Controls: Better known as CIS, this framework is ideal for start-ups that generally start slow and work their way to the top. Developed this framework back in October 2000. It was made to protect companies from various cyberattacks. It consists of only 20 controls regularly being updated by security professionals from academia, government, and industry. This framework starts from the basics, moves to some critical basic foundations, and finishes with some organization. This framework uses benchmarks based on common standards such as HIPAA or NIST that map security standards and offer different configurations for organizations to improve cyber security.

Why do we need Cyber Security Frameworks?

Cyber Security networks are needed in every organization because setting up one secures many data from cyberattacks. It also removes some guesswork when it comes to securing assets. Frameworks provide a plan to the cyber security managers and give them a systematic plan for acting in different scenarios. Along with the plans, frameworks guide IT and security leaders to manage their organization’s risks more intelligently.

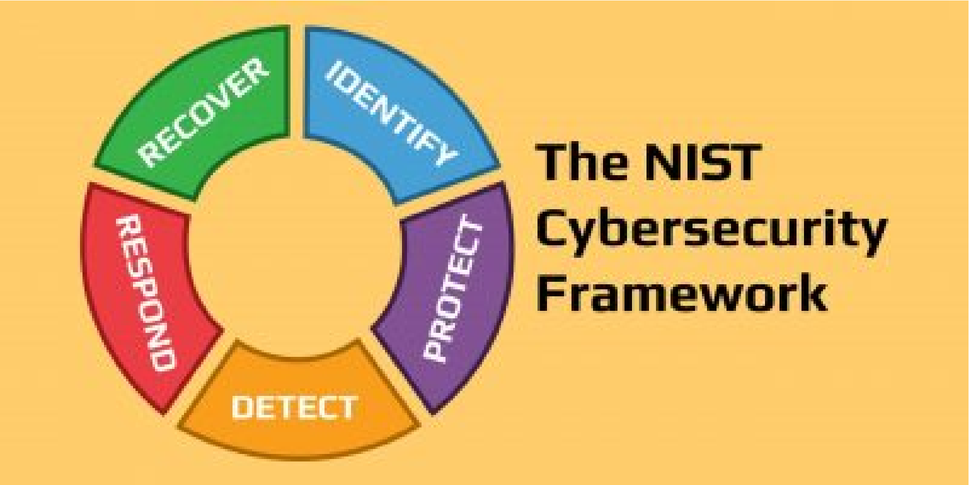
Companies can adjust the existing framework to meet their needs and requirements or even create their custom framework. Custom frameworks can be challenging as some businesses must adopt security frameworks that comply with commercial or government regulations. Custom-made frameworks may be insufficient to meet the standards to secure a network against dangerous cyber threats.

All in all, Cyber Security frameworks are needed by all companies and organizations, no matter if the company is big or small. In the future, there will be even more advanced frameworks.

Cybersecurity Frameworks

1. NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) is a non-regulatory US government agency dedicated to promoting American industrial competitiveness and innovation. NIST provides various resources and standards, including a framework for "Improving Critical Infrastructure cyber security," also known as the NIST cyber security framework.



NIST Cybersecurity Framework

The NIST cybersecurity framework was designed to help protect critical infrastructure, such as dams and power plants, against cyber attacks, but you can apply these principles to any organization. It offers an organized mechanism to help you identify risks and locate the assets that require protection. It also defines methods that can help protect these assets.

The framework is highly extensive. Its most basic document consists of 41 pages. Implementing the framework may require thousands of work hours and hundreds of procedures, controls, and documentation pages. However, the core principles are easy to understand. The framework offers a basic pattern for cyber defense, including:

- Identification
- Protection
- Detection
- Response
- Recovery

2. ISO/IEC 27001 and 27002

The International Standards Organization (ISO) 27001/27002 framework (also known as ISO 27K) is an internationally recognized standard for cyber security. This framework requires organizations adopting the ISO 27001 standard to adopt the following practices:

- Use an information security management system (ISMS).

- Assign management roles to systematically manage the organization's security risks while accounting for cyber threats and vulnerabilities.
- Design and implement coherent and comprehensive information security controls to mitigate identified risks.
- Adopt an ongoing risk management process.

3. Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a nonprofit organization created by Eastern Europe and Asia countries. It focuses on improving cyber security readiness and response across the public and private sectors. The CIS includes the following four program divisions:

- The Integrated Intelligence Center—facilitates relationships between private-sector and government entities to help create comprehensive coordinated security intelligence.
- The Multi-State Information Sharing and Analysis Center—aims to improve overall cyber security for local, territorial, tribal, and state governments. It achieves this objective by promoting collaboration and information sharing between members, the United States Department of Homeland Security, and private-sector partners.
- The Security Benchmarks—creates and promotes consensus-based standards to improve the security and privacy of Internet-connected systems and ensure the integrity of private and public Internet-based transactions and functions.
- The Trusted Purchasing Alliance—helps private and public sectors procure cyber security policies and tools cost-effectively.

The CIS provides its members with various resources, including emails detailing cyber safety tips, online papers and guides, instructional videos, and informative podcasts. Additionally, the CIS offers cyber security policy development advice at all levels, including national and international parties.

4. SOC2 Framework

The Service Organization Control (SOC) Type 2 was developed by the American Institute of Certified Public Accountants (AICPA) to provide a trust-based cyber security framework and auditing standard. It helps verify that partners and vendors manage client data securely.

The SOC2 framework defines over 60 compliance requirements and extensive auditing processes for third-party controls and systems. A SOC2 audit may take a year to complete, and at the end of the process, auditors issue a report that attests to the vendors' cyber security posture.

Since SOC2 is highly comprehensive, it is also one of the most difficult frameworks to implement. Organizations in the banking or finance sector may especially struggle to implement SOC2 because they are required to meet a higher standard for compliance. Still, this framework is highly important and should serve as a central tool in third-party risk management programs.

5. NERC-CIP

The North American Electric Reliability Corporation—Critical Infrastructure Protection (NERC CIP) provides a set of cyber security standards for the utility and power sectors. NERC CIP was created in response to the rise in attacks on critical US infrastructure and increasing third-party risks. It aims to help reduce cyber risk and maintain the reliability of bulk electric systems.

The NERC CIP framework requires organizations to identify and mitigate risks in their supply chain. It specifies various controls to help identify and mitigate supply chain risks, including:

- Categorize systems and critical assets
- Train personnel
- Create and plan incident response programs
- Design effective recovery plans for critical cyber assets
- Perform ongoing vulnerability assessments

6. Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) is a nonprofit organization that promotes research into security best practices for cloud computing and using cloud technologies to secure other forms of computing. CSA offers membership to any interested parties with the relevant expertise to contribute to cloud computing security.

CSA employs the expertise of its global members, which include industry practitioners, governments, associations, and corporations, to provide cloud security resources, such as research, certification, education, products, and events.

The organization facilitates activities and knowledge to benefit the entire cloud community. For example, it provides a forum that enables various parties to collaboratively create and maintain a trusted cloud ecosystem.

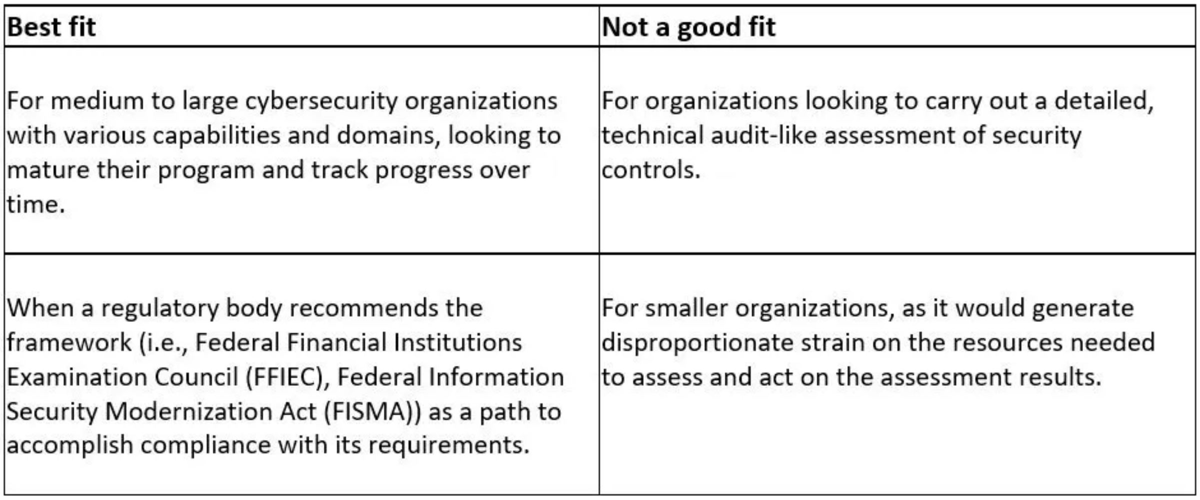
7. Cybersecurity and Infrastructure Security Agency (CISA)

The Cyber Security and Infrastructure Security Agency (CISA) is a division of the Department of Homeland Security (DHS) responsible for defending the Internet’s infrastructure and improving its security and resilience. It helps protect against infrastructure threats originating from natural disasters, terrorist attacks, cyberwarfare, etc.

CISA constantly identifies and assesses threats to Internet infrastructure, consulting with the government as well as the private sector. It provides many resources, including threat analysis, cyber security tools, and incident response across .gov websites. CISA delivers tools for technical coordination country-wide to facilitate emergency communications between partners.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST CSF) may be one of the most referred-to frameworks in the industry. Twenty-three categories are aligned to the five functions of this security framework: **Identify, Protect, Detect, Respond and Recover**. Each category includes subcategories, representing control objectives that together provide a foundation for a comprehensive cybersecurity program.

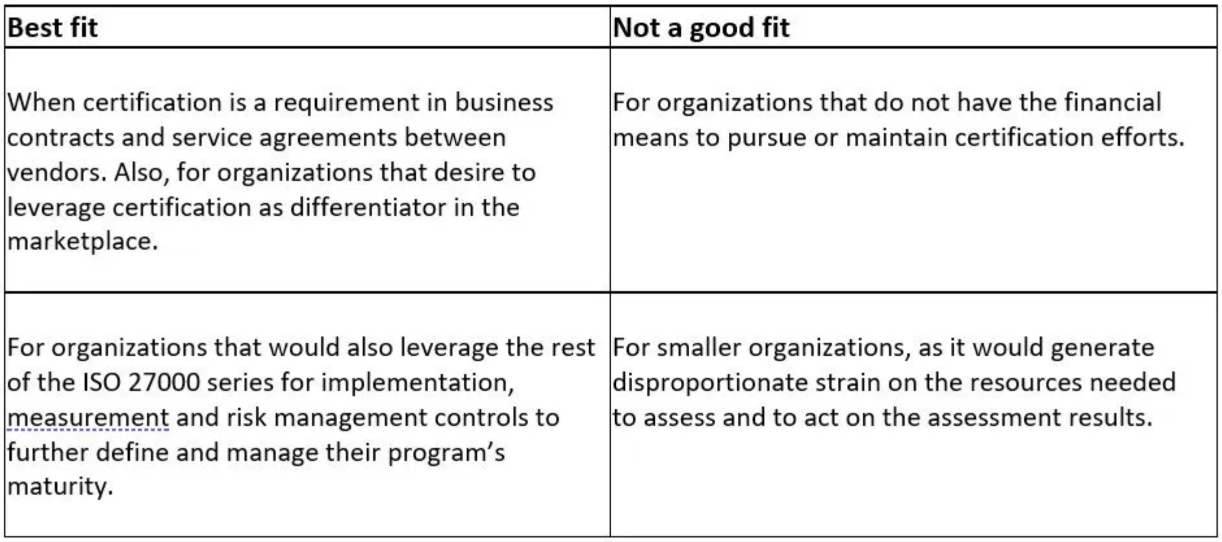


Best fit	Not a good fit
For medium to large cybersecurity organizations with various capabilities and domains, looking to mature their program and track progress over time.	For organizations looking to carry out a detailed, technical audit-like assessment of security controls.
When a regulatory body recommends the framework (i.e., Federal Financial Institutions Examination Council (FFIEC), Federal Information Security Modernization Act (FISMA)) as a path to accomplish compliance with its requirements.	For smaller organizations, as it would generate disproportionate strain on the resources needed to assess and act on the assessment results.

ISO 27001 by the International Organization for Standardization

This security framework is most recognized due to the opportunity to certify compliance through an independent technical audit and prove that data protection standards have been achieved by the company. ISO 27001 divides its controls as: **Organizational, People, Physical and Technological**.

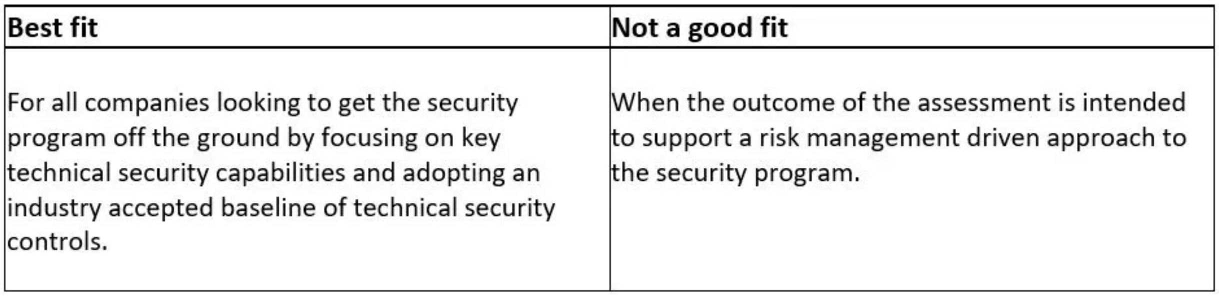
As an alternative to ISO 27001, organizations may pursue SOC 2 certifications as proof of independent security audits. The decision to pursue either is most often influenced by geography (i.e., ISO 27001 is more globally recognized than SOC 2) and contractual agreements.



Best fit	Not a good fit
When certification is a requirement in business contracts and service agreements between vendors. Also, for organizations that desire to leverage certification as differentiator in the marketplace.	For organizations that do not have the financial means to pursue or maintain certification efforts.
For organizations that would also leverage the rest of the ISO 27000 series for implementation, measurement and risk management controls to further define and manage their program's maturity.	For smaller organizations, as it would generate disproportionate strain on the resources needed to assess and to act on the assessment results.

The Center for Internet Security Critical Security Controls

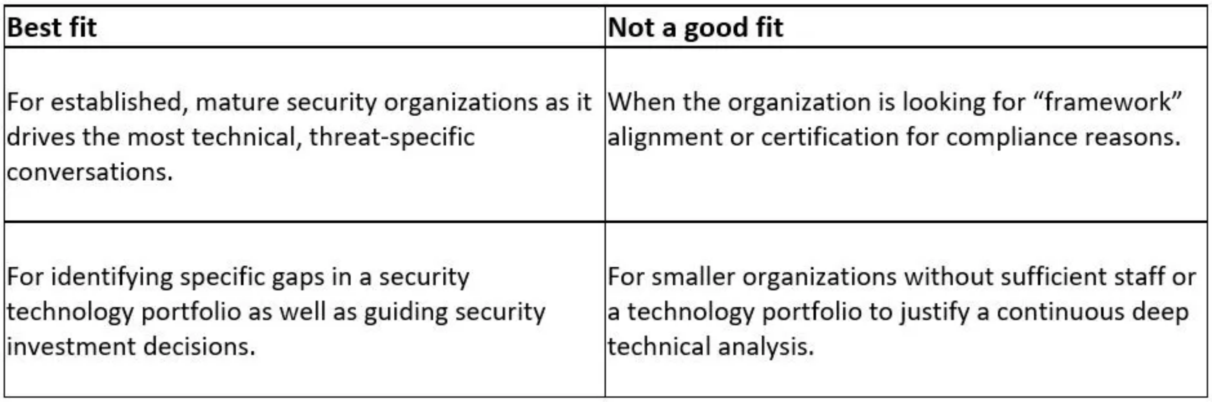
CIS Controls is a prioritized set of safeguards. The safeguards refer to controls that are technical in nature and are prioritized by three implementation groups that enable companies of all sizes to benefit. Large organizations can leverage the full extent of CIS Controls, while smaller security organizations with limited resources can begin by identifying a starting set of safeguards.



Best fit	**Not a good fit**
For all companies looking to get the security program off the ground by focusing on key technical security capabilities and adopting an industry accepted baseline of technical security controls.	When the outcome of the assessment is intended to support a risk management driven approach to the security program.

MITRE ATT&CK® knowledge base

MITRE ATT&CK® is not a framework. Instead, it’s a knowledge base that security organizations should consider leveraging to mature their capabilities to address very specific, real-life threats from adversaries. MITRE ATT&CK® provides continuously updated technical knowledge from the attacker’s perspective.



Best fit	**Not a good fit**
For established, mature security organizations as it drives the most technical, threat-specific conversations.	When the organization is looking for “framework” alignment or certification for compliance reasons.
For identifying specific gaps in a security technology portfolio as well as guiding security investment decisions.	For smaller organizations without sufficient staff or a technology portfolio to justify a continuous deep technical analysis.

Comparison NIST & ISO27001

When it comes to the protection of sensitive information, organisations have access to hundreds of different cyber security frameworks from which to choose. The Cyber Security Framework developed by the National Institute of Standards and Technology (NIST) and the one developed by the International Organization for Standardization (ISO) are two of the most common examples. Each of these architectures places an emphasis on achieving a high level of security as one of its key aims. Both share certain qualities while also revealing some obvious differences between the two.

National Institute of Standards and Technology Cyber security Framework (NIST) Framework

It comprises three main components that may assist a business owner evaluate and rank the state of his company's risk maturity, as well as the steps he has to take to enhance it.

- Core: Identification, protection, reaction, and recovery are the five essential functions that make up the core processes. In order to address concerns around cyber security, the framework used these elements. These actions, which were split down into a total of 23 activities, covered everything from the fundamentals of developing a cyber security programme to the fundamental aspects of risk management systems.
- Implementation tiers: The NIST CSF employed a scoring system with points ranging from 0 to 4 on a scale from 0 to establish an overall score that the firm could use as a benchmark for its level of risk maturity.
- Profiles: It is beneficial to organisations in evaluating their current risk tolerance level. Aside from that, it educates the organisation on how to reduce risks and gives security measures a higher priority, both of which are positive outcomes. If the company compares its present profiles to its ideal profiles, it may be able to more effectively deploy its resources to improve its security management over time, which will help the company expand.

Strengths of the NIST framework

- Make it possible for management of cyber risks and safety to continue for the long term.
- The internet really needs to have greater safeguards in place.
- Connect the links between the world of business and the community of technical innovators.
- Make sure you are well-prepared for the time when you will be required to comply with the requirements.

Weakness of the NIST framework

When it comes to the protection of cloud environments or cloud computing systems, there are very few hazards. It is not possible to get international accreditation using this method.

ISO Framework

The International Organization for Standardization (ISO) is a non-governmental organisation with its headquarters in Geneva that has published more than 22600 standards for use in a diverse array of industries. It encompasses a wide range of processes involved with the management of IT risk and with the protection of data. The framework for the development of an information systems management system is described. It is generally agreed upon that the set ofstandards k nown as ISO 27001 provides a trustworthy basis for security management. Determination is made on the prerequisites for creating, implementing, and improving information security management systems. Increasing the security of a company's sensitive data may be accomplished in a number of ways, one of which is through adopting ISO. The implementation of ISO guarantees that data can be relied on, that it is always available, and that it is always maintained safe. An audit against an ISO framework is conducted in two stages. The first step of the audit is referred to as the "documents review," and it is during this phase that the auditor looks into the written records of the system's operations, policies, and procedures to determine whether or not they comply with ISO 27001. An on-site review is part of the second step, which is known as the "certification audit." The goal of this phase is to verify whether or not the organisation in question has implemented an ISMS in line with ISO 27002. However, ISO certification has a time limit of three years before it must be renewed(Middleton, 2022).

Strengths of ISO

An important competitive advantage in the market Recovering from financial failures brought on by security breaches requires specific expertise. The reduction of the costs associated with breaching the law led to cost savings. It brings about a huge improvement in the overall order inside.

Weakness of ISO

The additional cost incurred as a result of needing to do more work.

• It is required to be updated once every three years.

• It is imperative that cash be set aside for IT. However, ISO 27001 does not provide a clear definition of scope. • Because of this, it is simple for clients to be deceived into thinking that the certification applies to the whole organisation rather than simply a particular sector of the business.

The similarities between ISO and NIST

Both of these all-encompassing frameworks address the management of the risks associated with cybersecurity. Because there is considerable interest among companies in adopting the NIST framework and in satisfying the standards of ISO, the 27001 recommendations ought to be easy to put into practise. Many of the framework-specific controls, as well as the definitions and codes that are used in one framework, may be used in another framework. Thisis also true for the majority of the controls. Both of these frameworks make use of vocabulary that is globally known, which makes it easier for professionals working in a broad variety of fields to communicate clearly and effectively about challenges related to cyber security.

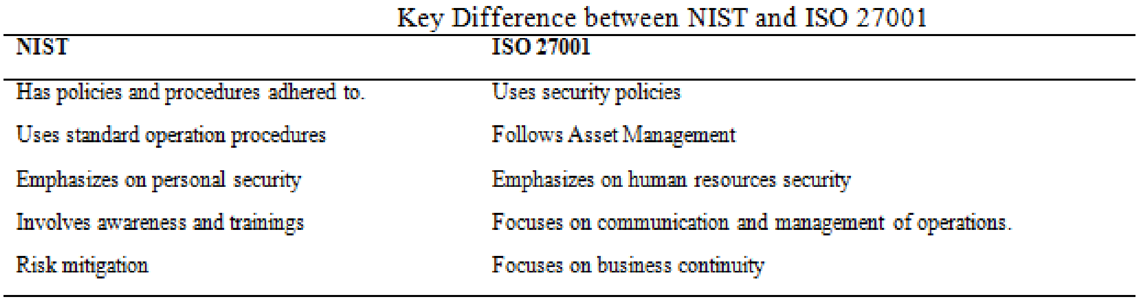
The differences between NIST and ISO

There are some differences between NIST CST and ISO such as cost, certification, and risk maturity.

- Cost: While the resources of the NIST may be accessed without charge at any time, those of the ISO cannot. Most new and developing organisations want to start their cyber security risk management programme with NIST, and as they grow, they will want to raise their investment in ISO 20071, which is where they will want to manage their cyber security risk.
- Certification: You have the opportunity to get third-party certification with ISO 20071, which will be acknowledged in any region of the globe. Although this may come at a high cost, there is a possibility that it may assist the organisation in gaining the trust of its stakeholders and consumers. Despite this, NIST does not provide any type of certification of any kind.
- Risk maturity: If your firm is just getting started on formulating a plan for mitigating the dangers posed by cyberspace and you want to make sure you don't make the same errors again, NIST could be the way to go. If your organisation is already well-established and ready to seek certification, ISO 20071 is a good standard to adopt.

The Complexity of ISO 27001 and NIST

You should anticipate that ISO 27001 will be as complicated as it must be for a firm of Your Size and Type in order to be successful. To maintain adequate control over its vulnerabilities, a bigger company will need to take into consideration and put into practise an increased number of precautions, regulations, and processes. In addition to bigger activities, actions involving a large number of employees should be carried out. One example of this would be making certain that every employee had exceptional cyber security expertise. The framework developed by NIST is more complicated than the one developed by ISO. The NIST framework is difficult to implement in many companies' operations because such companies lack the in-house NIST knowledge necessary to do so. CyberStorngTM and cyber saint® are two products that were created with the goal of making this procedure easier. Cyber strong simplifies the process of adopting NIST by dividing it up into five distinct steps: identifying, protecting, detecting, reacting, and recovering. As a consequence of this, consolidate all of the operations into a single system. Table 1 provides a summary of the key differences between the cyber security frameworks developed by NIST and ISO.



Key Difference between NIST and ISO 27001

NIST	ISO 27001
Has policies and procedures adhered to.	Uses security policies
Uses standard operation procedures	Follows Asset Management
Emphasizes on personal security	Emphasizes on human resources security
Involves awareness and trainings	Focuses on communication and management of operations.
Risk mitigation	Focuses on business continuity

Choosing a security framework, conducting a thorough assessment, prioritizing findings and driving initiatives is undoubtedly a resource-intensive challenge for any organization. Therefore, companies should consider the need from a variety of angles to select a framework that will provide the best value:

1. **Security program maturity** – Is the program newly established with a relatively small team and broad functions or has it grown to have an appropriate level of staffing and technology? This may impact the appetite for in-depth assessments. Are the resources available to staff the effort and most importantly, drive action from the outcome of the assessment?

2. **Regulatory landscape** – The industry, types of business processes and data types being processed can drive a list of compliance activities and required assessments. Understanding the external drivers will help select a framework that maximizes alignment with the requirements and derive efficiencies. For example, the Federal Financial Institutions Examination Council (FFIEC) provides a mapping of its requirements to the NIST Cybersecurity Framework.

3. **Expected outcome** – this may be the most important element that an organization should answer. “What is the outcome we need to accomplish?” will be a key driver for this exercise. Is there a compliance issue? Is it a general need to understand the capabilities of the security program and the level of protection and risk mitigation it provides? Is it a regulatory activity? Is it to facilitate prioritization of the security program investments and/or build a security strategy?

Finally, common security frameworks bring the expertise of many industry professionals to a maturing security organization by defining a set of best practices for alignment and benchmarking. While there are many other security frameworks available (e.g. NIST 800-53, Secure Controls Frameworks (SCF), HITRUST), the ones covered in this blog have been adopted widely and leveraged often for establishing trust in a company's data security practices.

Once a framework is selected, it is important to consider some important next steps as part of the process of adopting a framework:

- A framework assessment is not a complete and final solution to all security issues. Control framework assessments by themselves do not measure risk if all that is assessed is compliance or alignment with security controls. Controls are an important component in understanding how risks the organization is subject to are mitigated, but they do not paint a complete risk picture. To understand the risk exposure, a risk assessment needs to be performed that includes the identification of critical assets, threats, and vulnerabilities applicable to these assets and then applying the controls present in the environment to mitigate identified risks. The risk assessment should be performed in accordance with industry-accepted methodologies, like NIST 800-30, FAILR, Octave, etc., and will result in a prioritized list of residual risks for the environment. Once an assessment has been completed, it is time to prioritize findings, reflect the results in the organization's investment decisions and continuously measure risk reduction as solutions are implemented.
- Educate the Board of Directors and/or executive leadership on the ratings and tiers of the framework selected before presenting the outcome of an assessment. There is a risk that the focus becomes earning a high score across the spectrum. In many cases, this is not reasonable to achieve or necessary based on the risk appetite of the organization. Leadership should understand how the framework is used as a tool to determine capability and enable maturity as opposed to simply being a scorecard. It is also important to demonstrate how the control maturity fits into the overall risk picture and the risk mitigation value provided by the controls in the environment.
- Think outside the box. Frameworks, while comprehensive in concept, may not have an emphasis on the company's unique risk exposures. Encourage and allow flexibility. Deviations from the frameworks may be necessary to meet business, cultural and other constraints, or requirements of the environment.
- Don't get complacent. Regularly re-evaluate the selected framework against business needs and external factors. Recognize that, over time, doing the same thing does not mean that ratings or tiers stay the same as well (in fact, they may deteriorate as the risk profile of the business or environment changes). Similarly, incremental improvements and ongoing investment may only result in sustaining previously assessed levels of framework capability and maturity. It takes meaningful effort to move the needle!