CIS vs. NIST: Which Framework is Right For Your Business?

Designing and managing security architecture is a multifaceted task, and doing so without proper guidance can be challenging. Thankfully, numerous security frameworks are available to provide direction for your business.

Two primary models in cyber security that are generally recognized internationally are CIS (Center for Internet Security) and NIST (National Institute of Standards and Technology).

Knowing about these frameworks is necessary to select what is best aligned with your compliance, industry requirements, and risk management needs

In this article, we will shed light on the differences between CIS and NIST so that you can confidently pick one that suits your needs.

Understanding CIS and NIST Frameworks

CIS and NIST are two important frameworks in cybersecurity, each with its own approach and focus, though they share some common aspects. CIS focuses on practical solutions by collaborating with companies and stakeholders to create tools and resources that work in real-world situations.

They aim to provide actionable guidance for improving cybersecurity. In contrast, NIST adopts a more research-based approach, conducting studies and experiments to gain deeper insights into cybersecurity issues. They focus on understanding the underlying principles and developing standards based on their findings.

Let’s take a closer look at what they involve:

CIS

The CIS (center for internet security) is a pioneer in the field. To begin with, it is the third system of this kind in the world. This guarantees that this is sustainable while maximally cost-effective and convenient.

CIS is a non-profit, that makes finance available for the purpose of cyber security in the whole world. The main objective of this standardization approach is to produce the official norms in cyber security that combine the contributions of several experts rooted in different fields.

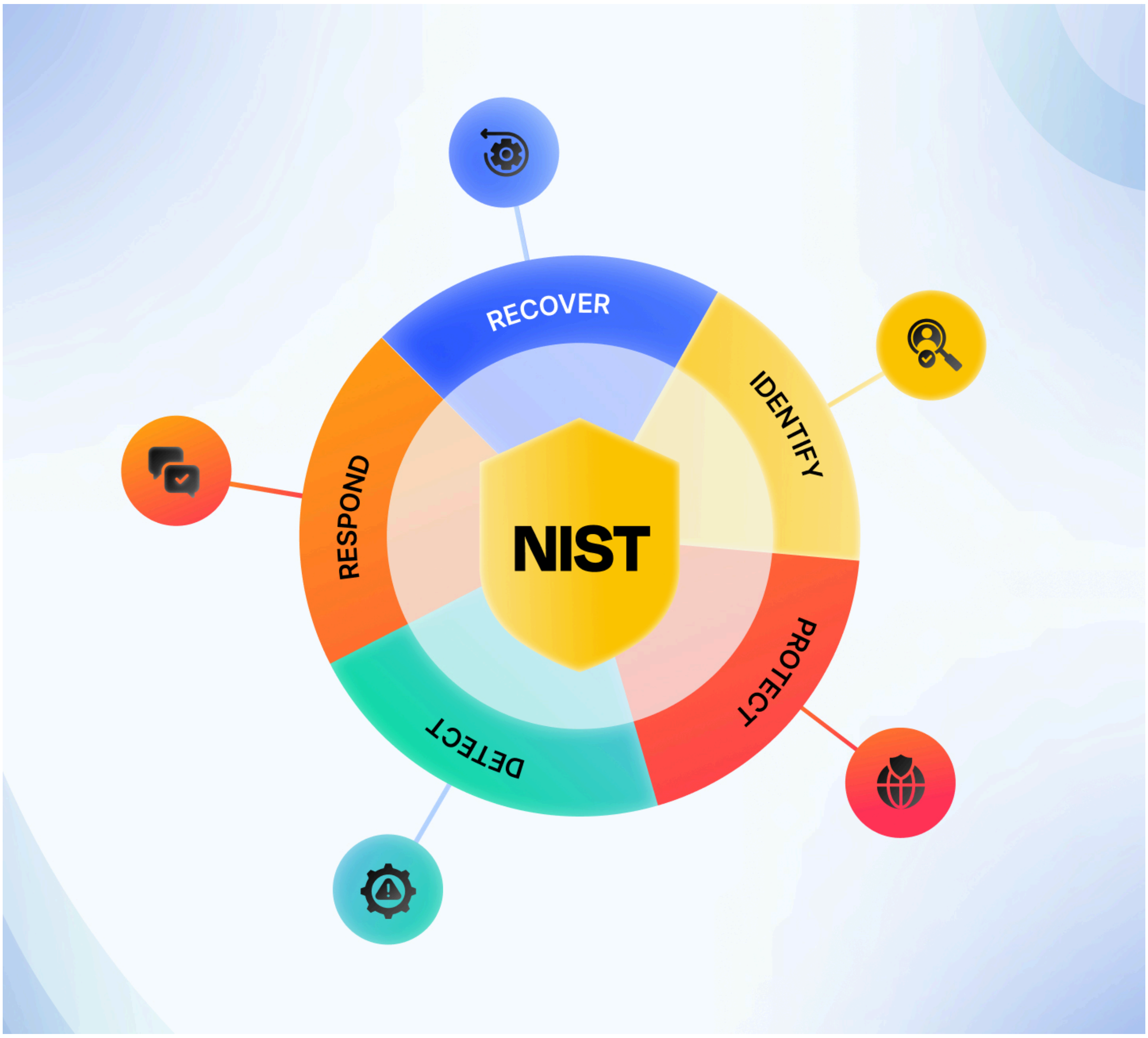
Who needs CIS?

CIS benchmarks come in 3 levels, each depending on the complexity of your IT system:

Level 1	**Level 2**	**Level 3**
This level begins from the ground up. It takes network security at the most basic level, covering password rules plus system resilience. This level targets small companies that may only use fundamental IT equipment and services.	This is quite complex and helps users make deep-dive decisions on the security procedures with proper advice/guidance. The plan best suits middle and large-scale businesses that have complex IT systems.	The most advanced level, Level 3 benchmarks provide the highest security recommendations. It includes Security Technical Implementation Guide (STIG) profiles and covers topics like disaster recovery plans and encryption.

NIST

NIST, the National Institute of Standards and Technology, operates under the U.S. Department of Commerce. Their Cybersecurity Framework helps businesses comprehend, manage, and mitigate cybersecurity risks. It offers voluntary guidelines to assist businesses in prioritizing cybersecurity efforts.



Who needs to be NIST compliant?

Anyone looking to collaborate with the United States federal government, including contractors, vendors, and subcontractors, must adhere to NIST standards and regulations.

This is an imperative issue as these agencies have access to classified information for the government, and any act of carelessness could trigger a cyber-attack and imperil national security. Some organizations and authorities may also stipulate compliance with NIST regulations as a mandate for cooperation and partnership.

Key Differences between NIST and CIS

The key difference between NIST and CIS is that CIS provides the CIS controls, which offer a prioritized set of actions to safeguard against common cyberattacks. On the other hand, NIST offers a big-picture strategy, focusing on overarching principles and frameworks.

Let’s dive deep into the differences below:

Functions	NIST	CIS
Approach to security	NIST frameworks, such as the NIST Cybersecurity Framework	CIS is quite known for its prescriptive approach. Prescriptive

	(CSF) and Special Publication (SP) series, focus on taking a broader, more flexible approach to cybersecurity.	means it offers specific configuration guidelines and benchmarks for securing complex systems, applications, and platforms.
Compliance and Standards	NIST frameworks are often referenced in regulatory compliance and industry standards, such as HIPAA, PCI DSS, and GDPR.	While CIS provides valuable benchmarks for secure configuration, it may not cover all compliance requirements or industry-specific regulations
Applicability	This is commonly used across various industries and sectors due to its adaptable nature and emphasis on risk management.	It is widely adopted by companies who want concrete guidance on system configuration and hardening to improve security posture.
Prescriptiveness	It provides a more flexible approach. It allows companies to tailor security measures based on risk tolerance and specific operational requirements.	Offers specific configuration guidelines. This way, it is easier for companies to implement security controls
Community Support and Resources	Offers extensive documentation, resources, and tools to support organizations in implementing its frameworks.	Benefits from a wide community of cybersecurity professionals contributing to benchmark development and sharing best practices.
Flexibility	NIST CSF has greater flexibility and customization options than CIS.	CIS is also customizable. However, it is not as flexible as NIST.
Use Cases	NIST can be used to build a strategic, risk-based cybersecurity program.	CIS Controls are used primarily for tactical improvements to a company’s cybersecurity defenses.
Complexity	NIST CSF requires more interpretation and understanding of a company’s risk profile	CIS is easier to understand and implement as it is more prescriptive in nature.
Continuous Improvement	It updates its publications and frameworks based on industry feedback, technological advancements, and emerging trends.	Regularly updates its benchmarks and guidelines in response to emerging cyber threats and evolving technology updates.

When to Choose NIST Over CIS?

NIST is better suited for mature companies prioritizing strategic planning and risk management, while CIS is a top choice for executing security controls. This is because NIST frameworks offer a broader perspective and help organizations diagnose weaknesses, organize priorities, and develop long-term cybersecurity strategies tailored to their security environment.

When to Choose CIS Over NIST?

You must choose CIS if your company seeks to implement specific security controls in the short term, while NIST is better suited for mature organizations. This is because it provides clear guidance on actionable steps to improve cybersecurity readiness, making it suitable for companies prioritizing immediate action.

Use Cases of CIS vs. NIST

Here are some use cases for NIST:

- NIST standards are mandatory for all federal agencies as NIST is a federal agency under the Department of Commerce.
- Government contractors must comply with NIST standards, especially those involved in the federal supply chain. Compliance may involve adhering to specific NIST special publications such as 800-53 and 800-171.
- Private businesses aiming for government contracts in the future may prioritize NIST compliance. Complying with NIST standards can provide a competitive edge during contract bidding processes and demonstrate readiness to handle government data securely
- NIST frameworks, including the NIST CSF, are suitable for organizations with a mature security posture. They offer customization options to align with an organization’s resources, goals, needs, and risk tolerance levels

Here are some use cases for CIS critical security controls:

- The CIS Controls are widely adopted by global enterprises of all sizes and by various security solution vendors, integrators, and consultants.
- Several notable users of the CIS Controls include organizations such as the Federal Reserve Bank of Richmond, the University of Massachusetts, and more.
- One specific use case of CIS Controls involves keeping track of all devices and software within an organization’s environment. This control enables cybersecurity experts to maintain an updated inventory of authorized devices (such as computers, servers, and mobile devices) and software (including applications and operating systems)

How to implement NIST or CIS frameworks?

We must clarify that the comparison between CIS and NIST frameworks isn’t aimed at declaring a definitive winner. Rather than being adversaries, these cybersecurity control frameworks are better viewed as complementary tools.

Many organizations recognize the unique strengths of each framework and choose to implement both to achieve well-rounded cybersecurity coverage.

However, implementing these frameworks may take some time if you choose the manual approach or go to a consultant who will charge you a hefty price tag.

This is where you need the help of a compliance automation platform like Sprinto, which is facilitated to help you implement cybersecurity frameworks like CIS or NIST.

Here’s how Sprinto helps in the implementation process:

1. Assessment and Mapping

Sprinto provides extensive features like control mapping and risk assessment to assess your current cybersecurity posture and map it against the requirements of the chosen framework, be it CIS or NIST. This initial assessment helps identify gaps and prioritize areas for improvement.

2. Automated Controls

Sprinto offers automated controls that align with the specific requirements of CIS or NIST frameworks. These controls automate manual tasks, making implementation faster and more efficient.

For example, CIS specifies 18 controls, and NIST specifies more than 1000 controls. All these can be mapped and monitored.

3. Continuous Monitoring and Improvement

Sprinto provides continuous monitoring capabilities, allowing you to track implemented controls’ effectiveness and identify improvement areas in real-time.

Interested to know more about how Sprinto works? Get in touch with our experts.

FAQs

Does CIS map to NIST?

Yes, the CIS can be mapped to the NIST Cybersecurity Framework (CSF). The CIS controls are designed to align with other cybersecurity frameworks and have been globally adopted.

Is CIS better than NIST?

Comparing CIS and NIST is not a matter of one being definitively better than the other. Both frameworks offer valuable cybersecurity resources but have different focuses and strengths.

Who are NIST’s competitors?

The main competitors of NIST include CIS and ISO groups. However, recent research suggests that NIST significantly influences cybersecurity standards for infrastructure firms and the private sector, particularly considering the absence of universally defined cybersecurity standards.