Cybersecurity Frameworks Comparison

NIST CSF vs ISO 27001/2 vs NIST 800-171 vs NIST 800-53 vs SCF

Cybersecurity "Goldilocks" Framework – Not Too Hard. Not Too Soft. Just Right!

When you graphically depict the various, leading cybersecurity frameworks from "easier to harder" it primarily focuses on the sheer number of unique cybersecurity and privacy controls. We refer to it as the "cybersecurity Goldilocks dilemma" since organizations struggle with finding a cybersecurity framework that is "not too hard, not too soft, but just right!" for their specific needs. To solve this, it comes down to first defining your "must have" and then "nice to have" requirements, since that helps point you to the most appropriate framework for your specific needs. This guide will help explain those concepts in greater detail.

What Is The Best Cybersecurity Framework?

The concept of a "best" cybersecurity framework is misguided, since the most appropriate framework to align with is entirely dependent upon your business model. The applicable laws, regulations and contractual obligations that your organization must comply with will most often point you to one of five (5) starting points to kick off the discussion about *"Which framework is most appropriate for our needs?"*

- NIST Cybersecurity Framework (NIST CSF)
- ISO 27001/27002
- NIST SP 800-171
- NIST SP 800-53 (moderate or high baselines)
- Secure Controls Framework (SCF) (or a different metaframework)

The number of included controls (e.g., requirements) directly impacts the number of domains covered by a specific cybersecurity framework. The lesser number of controls in a cybersecurity framework might make it appear easier to implement, but it also might not provide the necessary coverage that your organization needs from the perspective of administrative, technical and physical cybersecurity and privacy practices.

Defining "just right" for your cybersecurity and privacy controls is primarily a business decision, based on your organization's risk profile, which needs to consider applicable laws, regulations and contractual obligations that are required to support existing or planned business processes.

+1-855-205-8437
https://www.complianceforge.com
support@complianceforge.com

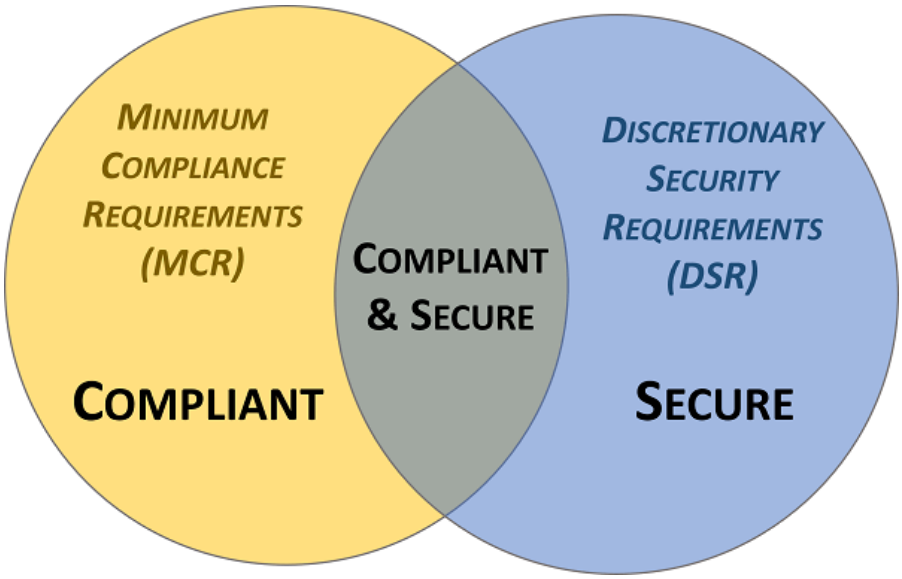
Defining Minimum Security Requirements (MSR) For Your Organization

Minimum Security Requirements (MSR) are made up on a combination of both mandatory and discretionary requirements. This can be considered a combination of you "must have" and "nice to have" requirements:

- **Minimum Compliance Requirements (MCR)** are "must have requirements" that are defined by applicable laws, regulations and contractual obligations that your organization must comply with.
- **Discretionary Security Requirements (DSR)** are "nice to have requirements" that are not legally-required but you feel you require to be secure, such as FIM, DLP, MFA, etc.

Those two considerations come together to address the "Compliant vs Secure" balancing act that determines if an organization's cybersecurity and/or privacy program will be both secure and compliant, or just compliant (e.g., focus on the bare minimums):

- Lesser mature organizations tend to focus on compliance over security.
- More mature organizations tend to focus on making compliance a natural byproduct of being secure.



This concept is further explained in the Integrated Controls Management (ICM) framework:

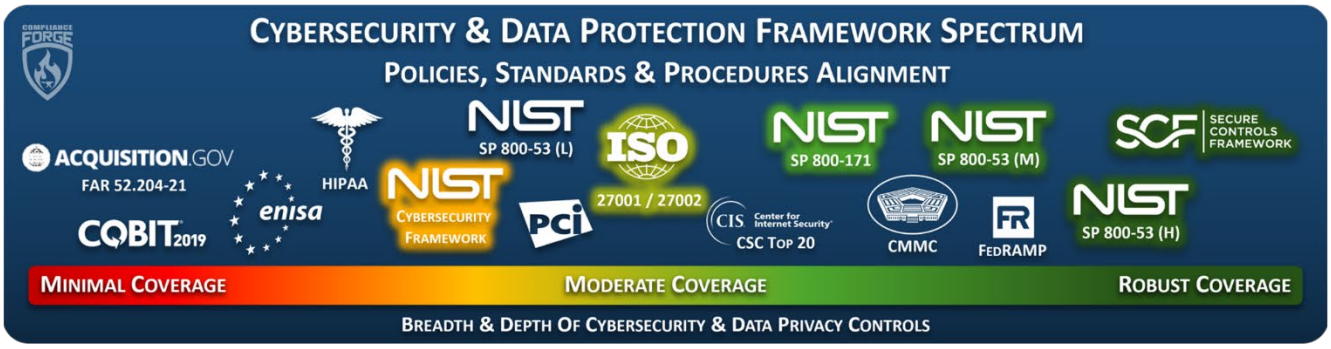
- MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

How To Identify The Most Appropriate Cybersecurity Framework

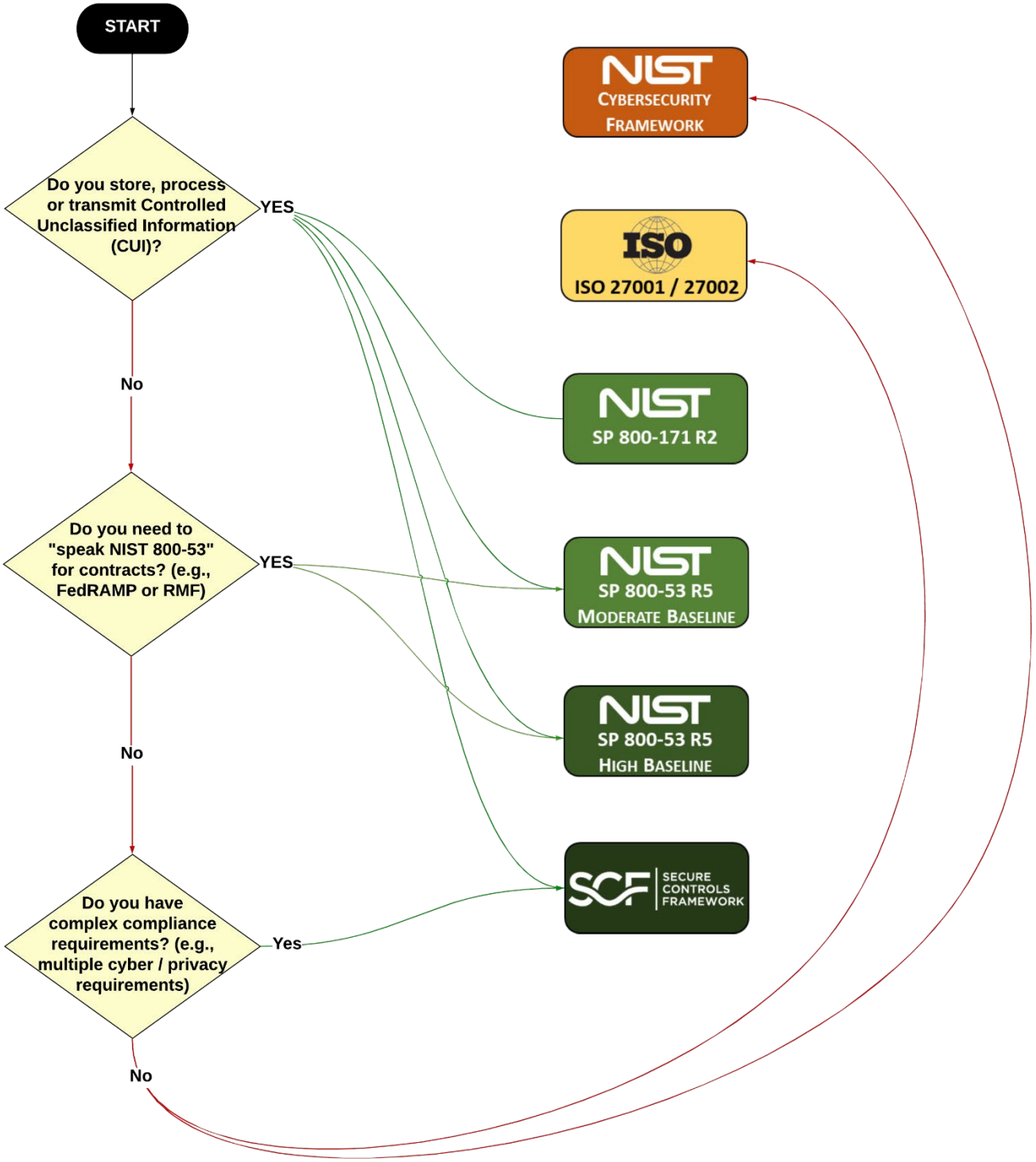
There are a few questions that can help quickly narrow down appropriate and inappropriate frameworks for your needs:

1. Do you store, process or transmit Controlled Unclassified Information (CUI)?
    a. If yes, look at NIST SP 800-171, NIST SP 800-53 or Secure Controls Framework (SCF).
    b. If no, proceed to question 2.
2. Do you need to "speak NIST 800-53" for a contract? (e.g., FedRAMP or RMF)
    a. If yes, look at NIST SP 800-53 (moderate or high baseline)
    b. If no, proceed to question 3.
3. Do you have complex compliance requirements? (e.g., multiple cybersecurity / privacy requirements)
    a. If yes, look at Secure Controls Framework (SCF).
    b. If no, look at NIST Cybersecurity Framework (CSF) or ISO 27001 / 27002.

See the graphic on the next page to visualize this decision process.



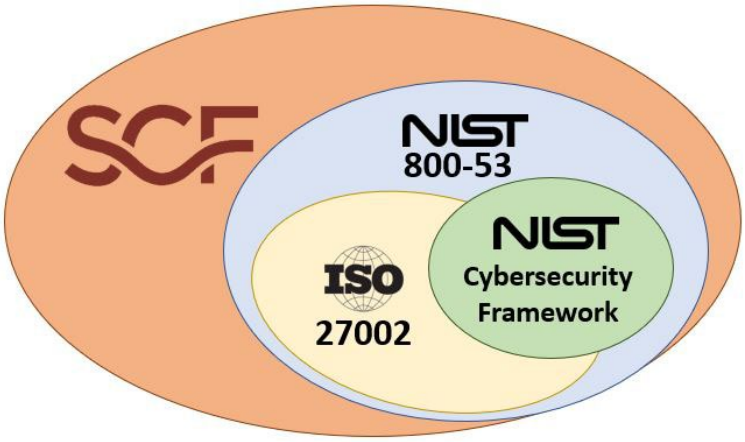
Not All Frameworks Are Created Equally!



If You Are Unsure Where or How To Start, Follow These Steps:

- **Have a discussion with your legal and procurement departments to find out what laws, regulations and contractual obligations your organization needs to comply with**. If they don't know, then you need to perform that discovery with their involvement to ensure you have the facts. Do not try to work off assumptions!
- **Talk with peers in your industry to identify what framework(s) their organization chose to align with and what those decisions were that led them to adopting one framework over another**. You still have to do your own analysis to determine what is right, but talking with peers can help avoid "re-inventing the wheel" on certain aspects of the analysis process.
- **Determine what resources you have available to adopt and implement a framework**. If it is a flip of the coin decision between two frameworks where you feel both meet your needs, you need to be sure to take into account which framework will be the most efficient to implement and maintain.
- **Evaluate your organization's business and IT strategies to identify components that may require the adoption of a specific framework**. For example:.
    - Your CEO puts out a roadmap to grow business and next year the company will start going after US Government and Department of Defense (DoD) contracts. This means your organization will have to address DFARS, FAR and CMMC compliance, which is based on NIST SP 800-171. This means alignment with NIST SP 800-53 or SCF might be the best path forward.
    - A business unit is expanding into the European market and will focus on B2C sales. This means your organization will have to address EU GDPR for robust privacy practices, on top of cybersecurity. This means you could select any framework to address underlying cybersecurity practices, but you need a privacy program. The SCF might be the best path forward.
- **Speak with a reputable consultant**. Not all "cybersecurity professionals" have the same backgrounds, experiences and competencies. Speak with a Governance, Risk and Compliance (GRC) professional about compliance-related frameworks and scoping decisions.

NIST CSF < ISO 27001/2 < NIST SP 800-53 < Secure Controls Framework (SCF)

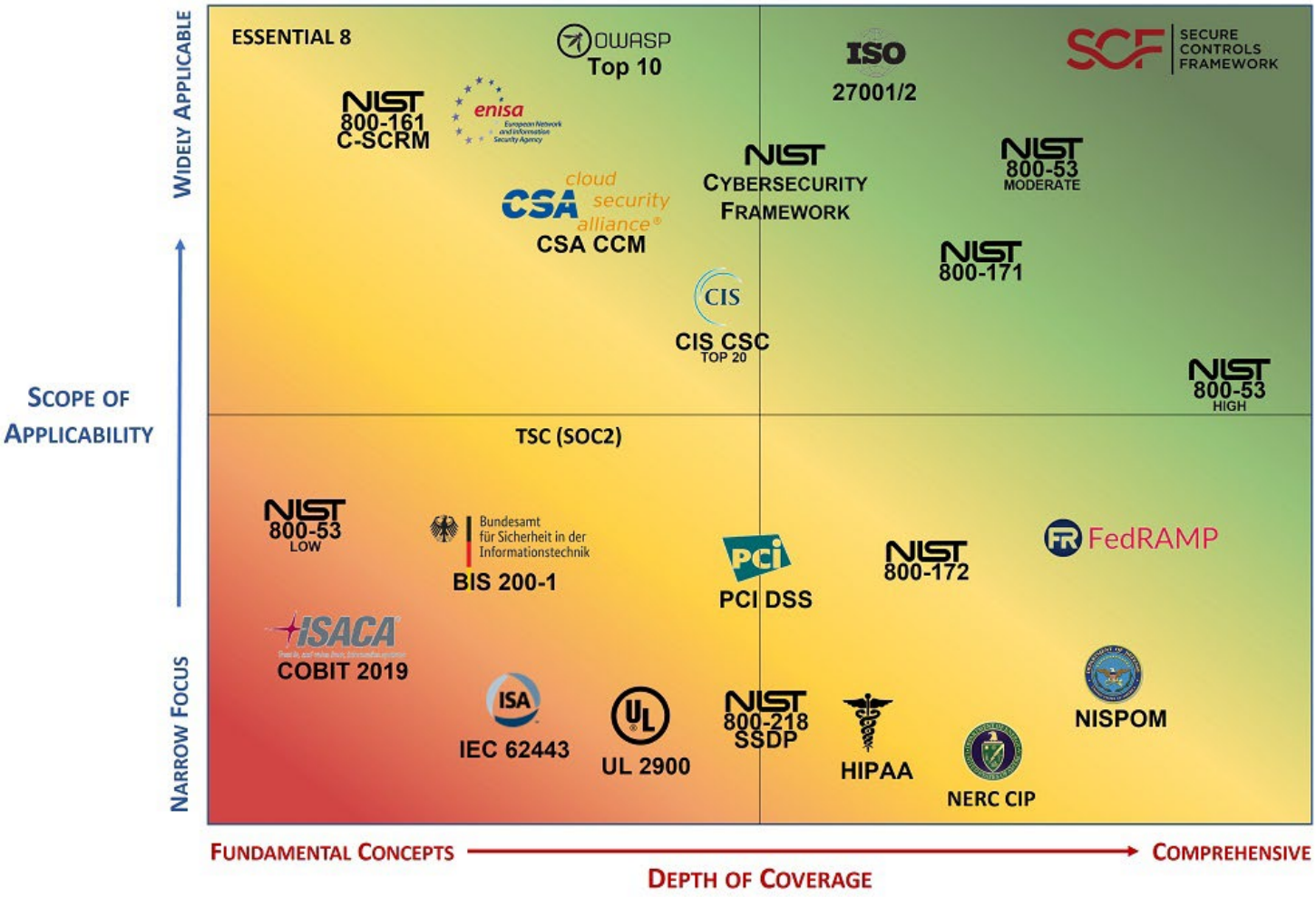


To help provide further context to the image:

- ISO 27001/2 is essentially a subset of the content found in NIST 800-53 (ISO 27002 went from fourteen (14) sections in 2013 to three (3) sections in 2022) where ISO 27002's cybersecurity controls fit within the twenty (20) families of NIST 800-53 rev5 security controls.
- NIST CSF is a subset of NIST 800-53 and also shares controls found in ISO 27001/2.
- NIST CSF incorporates parts of ISO 27001/2 and parts of NIST 800-53, but is not inclusive of both - this is what makes NIST CSF is a common choice for smaller companies that need a set of "industry-recognized secure practices" to align with, where ISO 27001/2 and NIST 800-53 are better for larger companies or those that have unique compliance requirements.

If you look at this from the perspective of a debate over which soft drink tastes best (e.g., Coke vs Pepsi), it generally comes down to personal preferences, since both products are essentially sugary, carbonated drinks and only differ slightly in flavor and packaging. The same arguments can be made for cybersecurity's two heavy hitters – NIST 800-53 and ISO 27002. Gaining popularity is the NIST Cybersecurity Framework (NIST CSF), but it lacks appropriate coverage out of the box to be considered a comprehensive cybersecurity framework. For more complex compliance requirements, the SCF is a "metaframework" that encompasses over 100 laws, regulations and frameworks in a hybrid framework that can span multiple compliance requirements.

It is not uncommon for experienced cybersecurity practitioners to have fundamental misunderstandings of the differences between laws, regulations and frameworks. However, in this context, what is depicted on the heatmap is referred to as a "framework" since by the NIST Glossary definition, a framework is *"a layered structure indicating what kind of programs can or should be built and how they would interrelate."* Even a law or regulation can serve as a framework for building a cybersecurity program.



We understand that it can be a little confusing when you look at it from a "heat map" perspective, since each cybersecurity framework has its own unique scope of applicability (e.g., specialization) and depth of coverage. However, understanding this can help you make an informed decision on where to start for the most appropriate framework(s) for your needs (often, organizations utilize more than one framework). You may even find you need to leverage a metaframework (e.g., framework of frameworks) to address more complex compliance requirements.

Secure Controls Framework (SCF) Overview

If you are not familiar with the Secure Controls Framework (SCF), it was developed with the ambitious goal of providing a comprehensive catalog of cybersecurity and privacy control guidance to cover the strategic, operational and tactical needs of organizations, regardless of its size, industry or country of origin. By using the SCF, your IT, cybersecurity, legal and project teams can speak the same language about controls and requirement expectations! The SCF is a "metaframework" which is a framework of frameworks. The SCF is a superset that covers the controls found in NIST CSF, ISO 27002, NIST 800-53 and over 100 other laws, regulations and frameworks. These leading cybersecurity frameworks tend to cover the same fundamental building blocks of a cybersecurity program, but differ in some content and layout. Before picking a framework, it is important to understand that each one has its benefits and drawbacks. Therefore, your choice should be driven by the type of industry your business is in and what laws, regulations and contractual obligations your organization needs to comply with.

The SCF is an open source project that provides free cybersecurity and privacy controls for businesses. The SCF focuses on internal controls, which are the cybersecurity and privacy-related policies, standards, procedures and other processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected.

The SCF is a "best in class" approach that covers over 100 cybersecurity and privacy laws, regulations and frameworks, including NIST 800-53, ISO 27001/2 and NIST CSF. Being a hybrid, it allows you to address multiple cybersecurity and privacy frameworks simultaneously. The SCF is a free resource for businesses to use. ComplianceForge's Digital Security Program (DSP) has 1-1 mapping with the SCF, so the DSP provides the most comprehensive coverage of any ComplianceForge product.

The SCF is commonly use by medium to large businesses, but can be used by any business with complex cybersecurity and privacy requirements.

The SCF can be used for:

- Any sized business
- Any industry

The SCF should not be used for:

- Simple compliance needs

NIST SP 800-53 Overview

The National Institute of Standards and Technology (NIST) is on the fifth revision (rev5) of Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations. From rev4 to rev5, NIST dropped the "US Government" focus for NIST SP 800-53 and now has it generalized enough for private industry to use. There are still "NISTisms" for wording that are entirely US Government-focused, but it is a significant improvement for private industry adoption. NIST 800-53 "best practices" are the de facto standard for private businesses that do business with the US federal government.

One thing to keep in mind is that NIST 800-53 is a super-set of ISO 27002 - that means you will find all the components of ISO 27002 covered by NIST 800-53. However, ISO 27002 does not cover all of the areas of NIST 800-53.

The Federal Information Security Management Act (FISMA) and the Department of Defense Information Assurance Risk Management Framework (RMF) rely on the NIST 800-53 framework, so vendors to the US federal government must meet those same requirements in order to pass these rigorous certification programs. Additionally, for NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, NIST 800-53 is called out as the best practices for government contractors to secure their systems. That further helps strengthen NIST 800-53 as a best practice within the US, especially for any government contractors. We have a section that describes NIST 800-171 and Cybersecurity Maturity Model Certification (CMMC) if you are interested in that subject.

NIST 800-53 includes what both ISO 27002 and NIST CSF addresses, as well as a whole host of other requirements. NIST 800-53 is the basis for the controls found in NIST 800-171 / CMMC. NIST 800-53 is commonly found in the financial, medical and government contracting industries. One great thing about NIST 800-53, and it applies almost universally to all NIST 800-series publications. As with other NIST publications, it is freely available, at no cost to the public: http://csrc.nist.gov/publications/PubsSPs.html.

NIST 800-53 Moderate is commonly use by medium to large businesses and is primarily US-focused.

NIST 800-53 Moderate can be used for:

- Defense Contractors (CMMC, RMF, etc.)
- Government Contractors (FedRAMP, RMF, etc.)
- Technology Businesses (e.g., MSPs, CSPs, etc.)
- General Business (large)
- Retail (large)
- Healthcare (large)
- Insurance (large)

NIST 800-53 Moderate should not be used for:

- Smaller Businesses

NIST 800-53 High is commonly use by medium to large businesses with an explicit requirement for the high baseline and is primarily US-focused.

NIST 800-53 High can be used for:

- Defense Contractors (large)
- Government Contractors (large)
- Technology Businesses (large)

NIST 800-53 High should not be used for:

- Smaller Businesses

NIST SP 800-171 Overview

The National Institute of Standards and Technology (NIST) is on the second revision (rev2) of Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The US National Archives (NARA) runs the Controlled Unclassified Information (CUI) Program for the US Government and NARA specifies NIST SP 800-171 and 800-171A as the minimum requirements to protect CUI. NIST SP 800-171 is the basis for the controls used by the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC). As with other NIST publications, it is freely available, at no cost to the public - http://csrc.nist.gov/publications/PubsSPs.html.

NIST 800-171 can be used by any sized organization, since it is the required set of controls necessary to protect CUI where it is stored, processed and/or transmitted.

NIST 800-171 can be used for:

- Defense Contractors
- Government Contractors
- Technology Businesses (MSPs, MSSPs, etc.)

NIST 800-171 should not be used for:

- FedRAMP or RMF compliance

ISO 27001 / 27002 Overview

The International Organization for Standardization (ISO) is a non-governmental organization that is headquartered in Switzerland. ISO can be a little more confusing for newcomers to IT security or compliance, since a rebranding occurred in 2007 to keep ISO's IT security documents in the 27000 series of their documentation catalog - ISO 17799 was renamed and became ISO 27002. To add to any possible confusion, ISO 27002 is a supporting document that aides in the implementation of ISO 27001. Adding a little more confusion to the mix, it is important to note that companies cannot certify against ISO 27002, just ISO 27001.

ISO 27001 Appendix A contains the basic overview of the security controls needed to build an Information Security Management System (ISMS), but ISO 27002 provides those specific controls that are necessary to actually implement ISO 27001. Essentially, you can't meet ISO 27001 without implementing ISO 27002:

- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls

To keep things simple, just remember that ISO 27001 lays out the framework to create an "Information Security Management System (ISMS)" (e.g., a comprehensive IT security program), whereas ISO 27002 contains the actual "best practices" details of what goes into building a comprehensive IT security program. Since ISO's information security framework has been around since the mid-1990s, it was in "right time at the right place" to evolve into the de facto IT security framework outside of the United States. You will find ISO 27002 extensively used by multinational corporations and for companies that do not have to specifically comply with US federal regulations. ISO 27002 is also "less paranoid" than NIST 800-53, which has an advantage of being less complex and therefore easier to implement.

One unfortunate thing about ISO 27001/2, and it applies to all ISO publications, is that ISO charges for its publications - https://www.iso.org/isoiec-27001-information-security.html

ISO 27001 / 27002 is commonly use by medium to large businesses and is internationally-recognized (e.g., ISO 27001 certification).

ISO 27001 / 27002 can be used for:

- General Business
- Retail
- Healthcare
- Insurance

ISO 27001 / 27002 should not be used for:

- Defense Contractors
- Government Contractors

NIST Cybersecurity Framework (NIST CSF) Overview

NIST Cybersecurity Framework (NIST CSF) has the least coverage of the major cybersecurity frameworks. NIST CSF works great for smaller and unregulated businesses that just want to align with a recognized cybersecurity framework. The downside to the NIST CSF is that its brevity makes it incompatible with common compliance requirements, such as NIST 800-171, GDPR, CPRA/CCPA and PCI DSS (depending on SAQ level). For those, more comprehensive frameworks, such as NIST 800-53 or ISO 27002 are recommended.

In reality, NIST CSF is a "dumbed down" and civilianized version of NIST 800-53. It came out nearly a decade ago when NIST 800-53 was entirely focused on the US Government, so there was a need for a subset of the controls that NIST 800-53 provided but for the non-enterprise space in private industry (e.g., tailored for small to medium businesses). Over the past

decade, different US Federal agencies have published documents describing how NIST CSF v1.1 controls can be leveraged to comply with HIPAA, FINRA, etc.

Overall, NIST CSF does not introduce new standards or concepts, but leverages and integrates industry-leading cybersecurity practices that have been developed by organizations like NIST and ISO. NIST CSF if organized into five categories of controls:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

The NIST CSF comprises a risk-based compilation of guidelines that can help organizations identify, implement, and improve cybersecurity practices, and creates a common language for internal and external communication of cybersecurity issues. The NIST CSF is designed to evolve with changes in cybersecurity threats, processes, and technologies. Essentially, the NIST CSF envisions effective cybersecurity as a dynamic, continuous loop of response to both threats and solutions. However, the "framework implementation tiers" should be avoided, since it is bad guidance. For example, you have to get to Tier 3 before you document policies, standards or procedures. That means a business at Tier 1 and Tier 2 would be considered negligent for failing to meet "reasonable expectations" for a security program. This is an example of "the path to hell is paved with good intentions" so that component of NIST CSF should be avoided.

NIST CSF is commonly use by smaller businesses and unregulated industries.

NIST CSF can be used for:

- General Business
- Retail
- Healthcare (small)
- Insurance
- Education

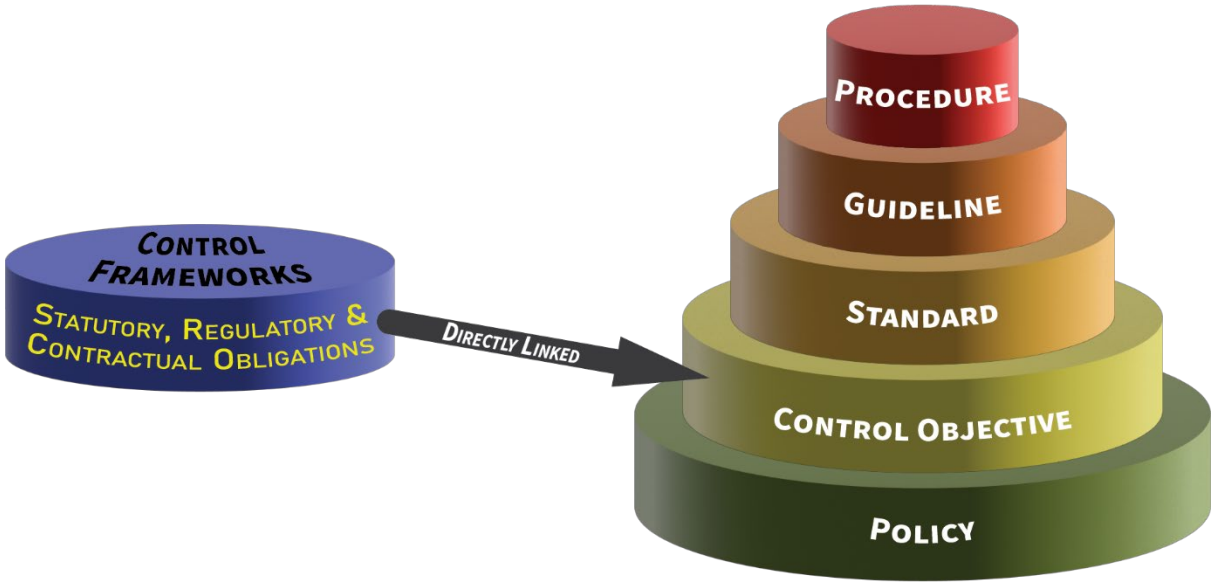
NIST CSF should not be used for:

- Defense Contractors

Policies, Controls, Standards, Procedures & Guidelines Structure

Cybersecurity documentation is comprised of six (6) main parts:

(1) Policy that establishes management's intent;
(2) Control Objective that identifies leading practices (linked to controls);
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.



Let ComplianceForge Help You With Your Documentation Needs!

If you have questions or need documentation, please contact us at support@complianceforge.com or +1-855-205-8437