5 Steps to Navigate the Path to NIST CSF 2.0

A Guide to Cyber Risk Reduction with CSF Framework Alignment

CRITICALSTART®

Table Of Contents

Introduction

In February 2024, the National Institute of Standards and Technology (NIST) released version 2.0 of its Cybersecurity Framework (CSF). This critical update modernized key facets of the framework across each of the five functions of Identify, Protect, Detect, Respond, and Recover.

Additionally, many functions and ideas from those original pillars were extracted and expanded to create the basis for a new function: **Govern**. The Govern function directly addresses the expanded scope and responsibility of cybersecurity across teams and extends roles and stakeholders into executive and board leadership. This revision of the globally recognized CSF framework empowers organizations to engage in strategic decision-making, creates a foundation for both proactive and reactive security practices, and helps focus security through a lens of risk management.

In this eBook, we will discuss what National Institute of Standards and Technology Cybersecurity Framework 2.0 (**CSF 2.0**) is and why it matters, and we'll walk you through five steps you can take to ensure successful alignment so that you can reduce risk across your organization.

What is NIST CSF and Why Does it Matter?

NIST CSF is a framework that helps organizations manage their cybersecurity risks by outlining specific risk-reduction outcomes and the actions that organizations can take to achieve them. The framework has evolved since its original version in 2014 to include updated best practices, address shifts in technological and threat landscapes, and now, emphasize governance.

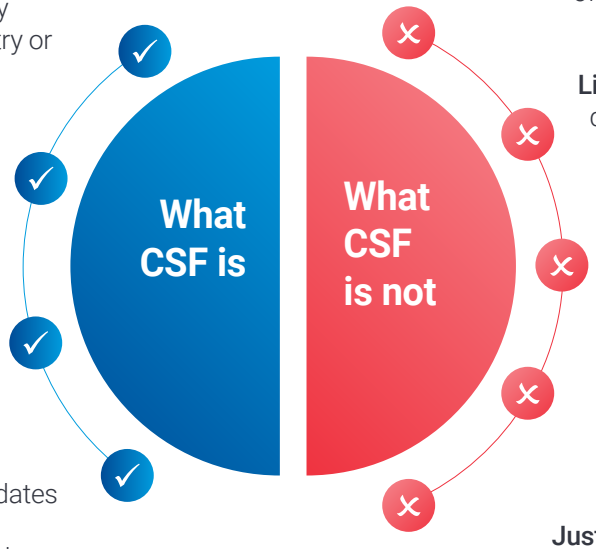
Since its inception, the holistic nature of CSF has provided a foundation for integrated leadership, decision-making, and implementation within cybersecurity. CSF adoption leads to greater assurance that security controls and processes are both technically effective and strategically aligned with business objectives.

A comprehensive framework that includes best practices for tools, processes, and policies that address security challenges across diverse organizations of any industry or size.

Strategically aligned guidance that is contextualized around business objectives for informed leadership and strategic decision-making.

Adaptable to various organization sizes and industries, providing a structured approach to governance, risk assessment, and strategic partnerships.

An evolutionary and living standard, with periodic updates that reflect changes in the cybersecurity domain and the need for organizations to adapt to new threats and technologies.



A specific set of technical requirements, but rather a set of outcomes and actions that organizations can use to manage and reduce risk.

Limited to a particular sector, size, or maturity, as it is designed to be useful regardless of the organization's business objectives and technical sophistication of their cybersecurity programs.

One-size-fits-all, as it allows for customization to fit an organization's unique needs and risk profile.

Static, but rather, it is an evolving framework that changes as new cybersecurity challenges and technologies emerge.

Just for compliance, due to its focus on enhanced cyber resilience across all IT systems, processes, and tools.

10 Reasons to Align Your Organization's Security Strategy to NIST CSF

1. **Enhance Your Cyber Resilience:** CSF continually builds upon previous versions to include new controls and process measurements. Alignment with CSF gives you prescriptive best practices for cyber resilience with structured governance and risk assessment guidance.

2. **Manage Cyber Risk:** CSF offers a comprehensive approach to managing cyber risks by aligning tools, practices, roles, and responsibilities with business objectives.

3. **Adopt Best Practices Quickly:** CSF is widely adopted across various industries globally because it provides a universal language and structured approach for cybersecurity risk management.

4. **Determine the ROI of Your Security Tools:** CSF provides a framework for measuring the technical effectiveness of your cybersecurity tools and helps you clearly articulate the return you are getting on your investments.

5. **Create a Culture of Shared Responsibility:** The universal language and structured guidelines provided by CSF improves organizational communication regarding the cross-functional roles and responsibilities around cybersecurity risk management.

6. **Align Actions Around Business Context:** The framework is flexible and adaptable to suit different organizational contexts, providing detailed guidance and examples without being rigid or overly prescriptive regarding implementation and execution.

7. **Gain Confidence in Your Security Strategy:** By leveraging CSF, you gain definitive answers to questions regarding your security gaps, inefficiencies, and other areas that you can improve to make your solutions and practices stronger, more effective, and ultimately, trustworthy.

8. **Emphasize Governance:** CSF provides a foundation for integrating cybersecurity into business strategy, ensuring a strategic alignment with business objectives to manage cyber risks more effectively. This critical component of cybersecurity strategy is propelled to the forefront with CSF 2.0's introduction of the Govern pillar.

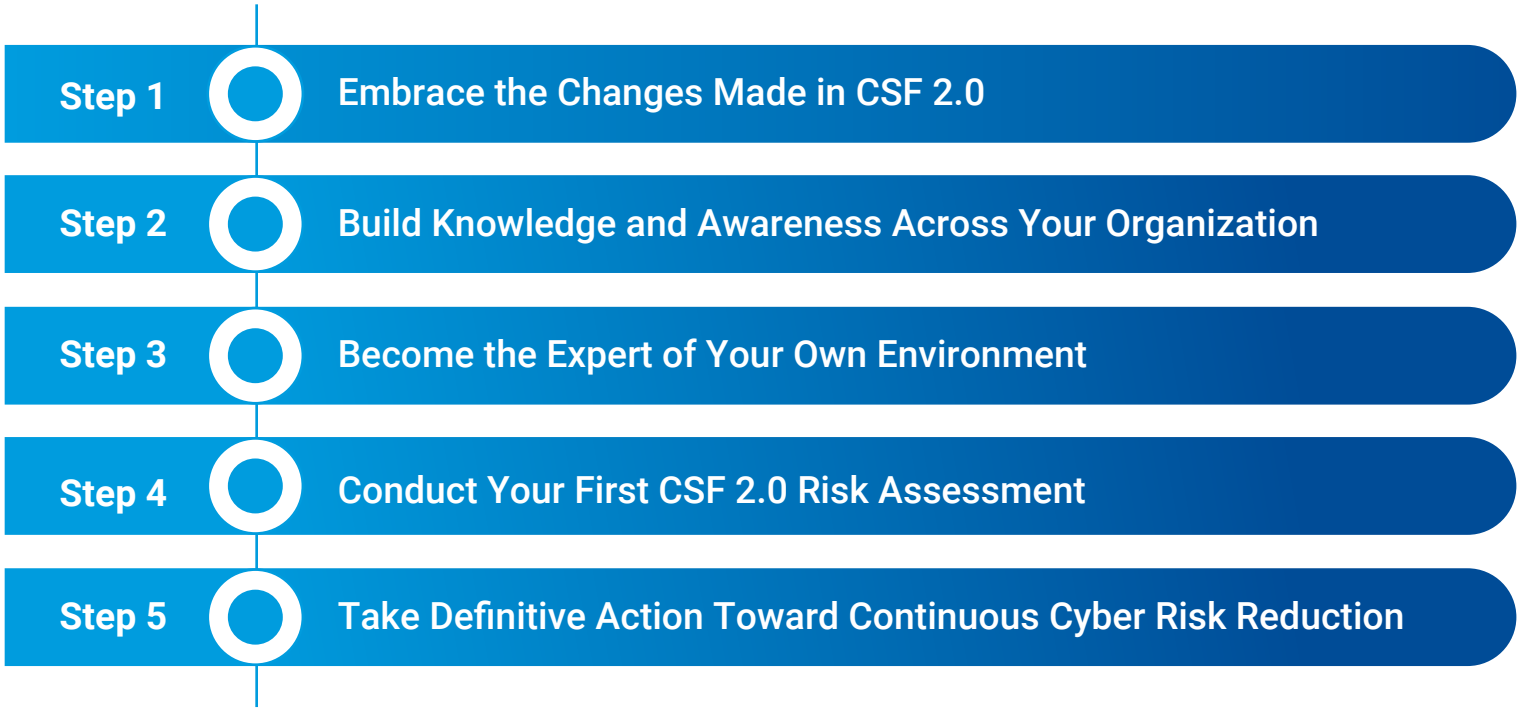
9. **Determine Security Spend Based on Data:** CSF risk assessments help you identify and highlight the areas where your organization can improve practices, which helps you prioritize cybersecurity efforts and spending decisions.

10. **Improve Continuously:** CSF alignment gives you a path that lets you anticipate and manage risk by integrating new technologies and keeping pace with the rise of emerging threats, so you can continuously improve your security posture, no matter what comes next.

The Five Steps to NIST CSF Alignment

Whether you're already using a framework or you're starting from scratch, read on to learn five steps your organization can take to move toward risk reduction with CSF adoption. We'll walk you through the improvements made to the latest CSF framework and provide a guide to NIST's documentation, and then we'll walk through actions you can take to achieve the greatest results in the least amount of time.

In the following sections, you will:



Step 1: Embrace the Changes Made in CSF 2.0

If your organization has assessed based upon CSF 1.1, you might wonder if it's worth the effort to migrate to 2.0—especially if you feel like what you have is working. In short, you're going to want to make that effort.

A lot has changed since the original 2014 adoption date of CSF 1.0 and even more since the 2018 update to version 1.1. The rise of automation, acceleration of development and deployment pipelines, expanded software supply chains, and deeply diversified cloud and hybrid networks have all increased speed and complexity in computing environments. Those changes all add up to increased risk that has challenged cybersecurity teams and tools.

CSF 2.0 modernizes and future-proofs the framework by incorporating updated best practices, addressing new technological and threat landscapes, and emphasizing governance—a key aspect that integrates leadership and strategic decision-making—in cybersecurity. This holistic approach ensures that cybersecurity measures are technically effective and strategically aligned with business objectives, facilitating a comprehensive risk management strategy now and into the next several years.

> CSF 2.0 reflects the need for greater risk management in the face of significant evolution, both on the side of the organization, and in terms of cyberattacks.
>
> - Randy Watkins, Chief Technology Officer, Critical Start

Step 1: Embrace the Changes Made in CSF 2.0 (continued)

The Advantages of CSF 2.0

Prioritize Controls Based on Risk

Implement controls that address the most critical risks first, ensuring effective use of resources.

Detect and Respond Strategically

Develop protocols to prioritize alerts, focusing on those with the highest impact to manage workloads effectively.

Adopt a Layered Security Approach

Ensure all assets are identified and protected with appropriate security measures.

Set Measurable Alignment Goals

Regularly assess alignment with the framework to ensure continuous improvement and adaptability.

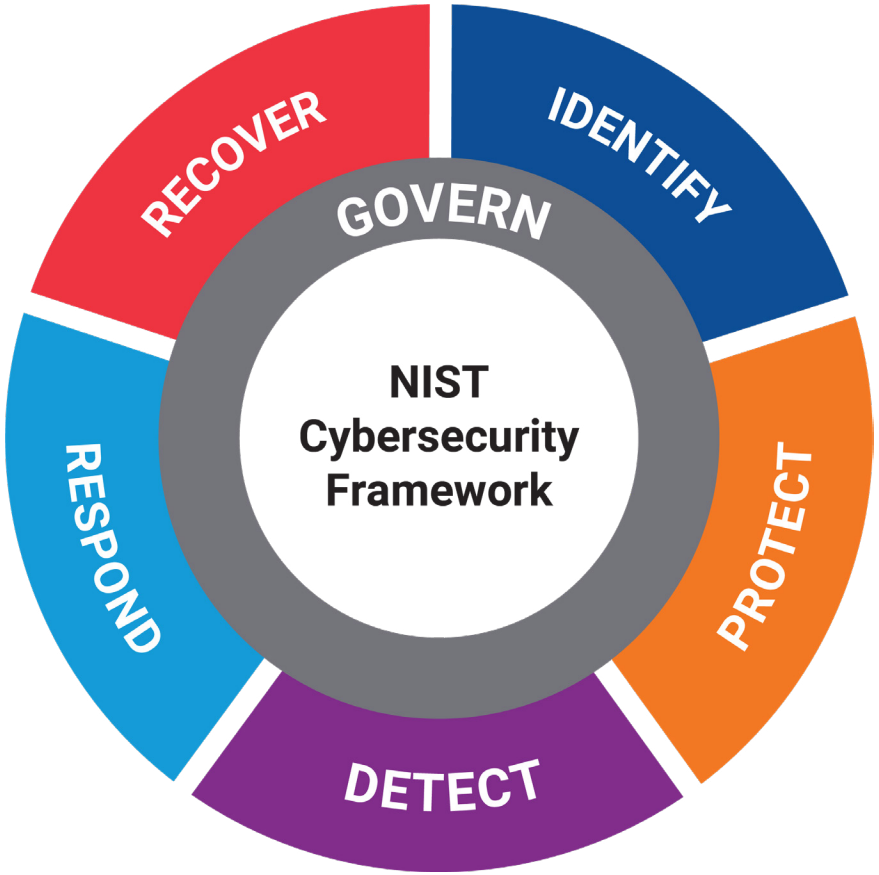
Step 1: Embrace the Changes Made in CSF 2.0 (continued)

Govern: Why the Sixth Pillar Emerged

The new, sixth pillar of the NIST CSF, Govern, extends cybersecurity risk management responsibilities throughout the organization, up to and including the C-suite and boards. The goal of Govern, which serves as a foundation for the original five pillars, is to encourage a proactive and adaptive approach to cybersecurity by focusing on policies, procedures, and security team roles and responsibilities, elevating the critical role cyber risk management plays in business and compliance outcomes. The Govern pillar also stresses the importance of software supply chain security and the creation of clear strategies, plans, and actions regarding cyber incidents originating from supply chain ecosystem software, systems, and connections.

The Govern pillar of CSF 2.0 extends cybersecurity risk management responsibilities throughout the organization and encourages cross-functional coordination to improve compliance outcomes. It does this by providing guidelines around:

- ✓ Addressing organizational context when considering security strategies and implementations
- ✓ Establishing cybersecurity supply chain risk management, roles, responsibilities
- ✓ Emphasizing secure software development and deployment
- ✓ Creating a Cybersecurity Supply Chain Risk Management (C-SCRM) strategy, objectives, policies, and processes plan
- ✓ Separating proactive from reactive security measures for greater risk reduction



Source: *National Institute of Standards and Technology*

Step 2: Build Knowledge and Awareness Across Your Organization

Every endpoint, server, application, user account, device, and network connection represent an entry point for an attacker—and that means organizational risk. Now, more than ever, cybersecurity is everybody's responsibility.

As you move toward alignment with CSF 2.0, it is imperative that you establish security roles and responsibilities across your teams, from individual contributors to leadership to the board. Then, you need to take the next logical step and build awareness in each stakeholder. NIST has created several tools that are readily available to help you train your teams. The following quick guide can help you find what you need to build awareness across your organization.

What are you looking for?	NIST official link
The official NIST CSF website	Cybersecurity Framework | NIST
The official NIST CSF 2.0 full guide	The NIST Cybersecurity Framework (CSF) 2.0
Quick-start Guides by organizational profile, business size, and specific topics (includes a C-SCRM quick start guide)	Navigating NIST's CSF 2.0 Quick Start Guides
References and implementation examples for NIST CSF 2.0	CSF 2.0 Informative References
Details of the Govern pillar	NIST CSF 2.0 Reference Tool

Step 2: Build Knowledge and Awareness Across Your Organization (continued)

Understand the Importance of Supply Chain Risk Management

Even if you have full visibility of every asset in your organization, are you certain that there aren't potential risks, malicious code, compromised systems, or vulnerabilities originating from within your supply chain ecosystem? Do you have clear communication paths defined to effectively communicate and take action to mitigate supply chain risks?

Most computing environments rely on complex, distributed, and extensive interconnected systems and software. If not properly vetted and secured, each connection point, user account, and data access point represents a potential weak spot where attackers could strike. CSF 2.0 introduced the Cybersecurity Supply Chain Risk Management (C-SCRM) process for identifying, assessing, and mitigating risks throughout the cybersecurity supply chain.

Using the C-SCRM Quick Start Guide from NIST, you can quickly establish and operate supply chain risk management capabilities, including:

- Establishing security requirements for ecosystem suppliers, products, and services.
- Defining rules and protocols for information sharing.
- Creating contractual SLAs regarding communication of compromises.
- Specifying rights and responsibilities of your organization, your suppliers, and their supply chain partners with respect to cyber risk.

Step 3: Become the Expert of Your Own Environment

In a 2023 survey of over 1,000 organizations, Critical Start learned that 91% of respondents had a risk management strategy in place for most or all security functions. Yet... Out of the same group:

- **Only 31% have a continuous and comprehensive asset inventory.**
- **Just 28% say they scan for vulnerabilities monthly or better.**
- **A full 73% lack comprehensive and continuous monitoring and detection of security events across all assets.**

Those statistics provide a startling look at the reality of modern security programs, indicating that while there is a lot of planning going on, there is much work left to do on the implementation side. Fortunately, CSF 2.0 can help you bridge the gap between strategy and execution. But first, you need to understand what is in your environment.

Step 3: Become the Expert of Your Own Environment (continued)

Your Environment Viewed Through a CSF Lens

Here are some framework-aligned steps you can take to become the definitive expert of your own environment:

Govern

- Clearly define security policies, practices, roles, and responsibilities within the context of your business objectives.
- Create your C-SCRM so that you have contextualized awareness of your software supply chain.

Identify

- Ensure you have complete and automated asset awareness—not just an inventory, but a risk-aware measurement of the potential impact of each asset if it were breached.
- Conduct regular vulnerability scans and prioritize remediation based on asset context.

Protect

- Ensure that your Security Operations Center (SOC) or Managed Detection and Response (MDR) provider is receiving all expected signals from your security tools so that you're not leaving coverage gaps.

Detect

- Know what signals you should expect so that you catch the unexpected faster.

Respond

- Have plans, strategies, and playbooks in place so your response to incidents becomes second nature.

Recover

- Clearly define what it means to restore business operations so that you can validate response actions.

Step 3: Become the Expert of Your Own Environment (continued)

Contextualization is the Key to Effective Implementation

One of the most compelling benefits of CSF is its flexibility. Once you have a strong understanding of what you have across the entire risk management lifecycle, you can start wrapping policies, processes, controls, roles, and responsibilities around your unique computing environment. This contextualization of controls is imperative to an effective implementation, but first, you need to have a deep understanding of what you have so you can clearly define your scope and goals.

You must know

What assets you have, and what risk they pose to the organization if breached.

What constitutes a true positive in the context of your environment and known good behaviors.

Your gaps and inconsistencies that result from a heterogenous security stack, missing security agents, and misconfigured tools and assets.

Your target maturity levels and the accepted levels of risk across your industry.

So that you can

Prioritize controls based on risk: Assess and prioritize cybersecurity controls based on specific risks to the organization, ensuring resources are allocated effectively.

Strategically manage alert volumes: Implement strategies to manage and prioritize security alerts, reducing alert fatigue and focusing on significant threats.

Adopt a layered security approach: Layer defensive mechanisms to provide redundancy and mitigate the impact of a single security control failure.

Set measurable alignment goals: Establish clear, measurable goals for cybersecurity alignment with business objectives, facilitating progress tracking and adjustment.

Step 4: Conduct Your First CSF 2.0 Risk Assessment

Now that you understand what CSF 2.0 is, why it exists, and how it brings clarity and direction to your security strategy, it's time to act by conducting a risk assessment.

There are several ways to go about conducting a risk assessment using a framework. You can create your own questionnaires based on framework definitions, download a third-party questionnaire, or outsource to a risk assessment contract vendor or Managed Security Service Provider (**MSSP**). While each option provides certain benefits to the organization, there are drawbacks that may limit its effectiveness or accessibility. of controls is imperative to an effective implementation, but first, you need to have a deep understanding of what you have so you can clearly define your scope and goals.

	Create a risk assessment questionnaire based off the framework definitions	Downloading a third-party questionnaire	Outsourcing to a Risk Assessment Contract Vendor or MSSP
Pros	Cost-effective and can be tailored to specific organizational needs. Ensures confidentiality and control over the assessment process. Flexibility to include questions relevant to the company's unique risks and culture.	Access to expertly crafted questions that have been tested for reliability and validity. Saves time compared to creating a questionnaire from scratch. Can provide industry benchmarks and standards for comparison.	Leverages the expertise and resources of specialized risk management professionals. Comprehensive approach that often includes both assessment and mitigation strategies. Can provide an objective and unbiased assessment of risks.
Cons	May lack the rigor and comprehensiveness of professionally developed tools. Potential for bias in question formulation and interpretation of responses. Requires significant time and expertise to develop effectively.	May not fully align with the specific context or risks of the organization. Cost associated with purchasing proprietary questionnaires. Potential for over-reliance on the tool's results without proper internal analysis.	Can be the costliest option among the three. Requires sharing sensitive company information with an external party. Potential for misalignment between the vendor's methods and the company's needs.

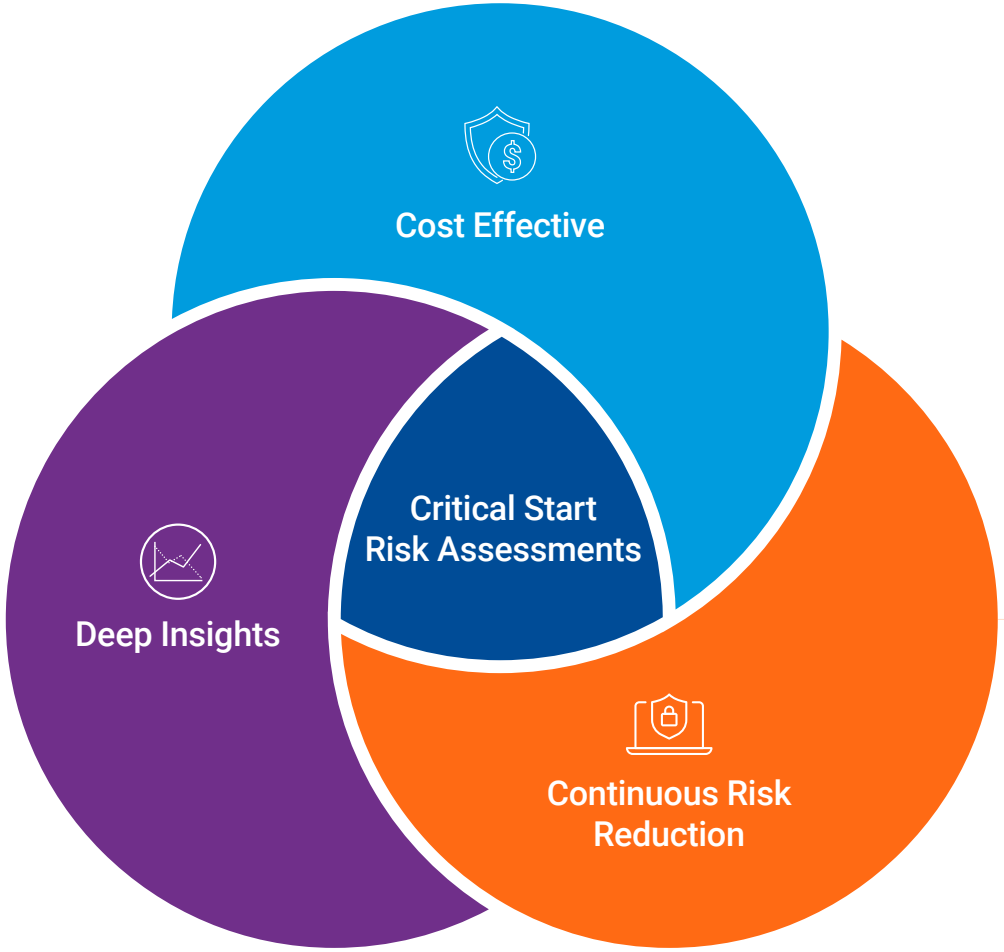
Step 4: Conduct Your First CSF 2.0 Risk Assessment (continued)

A Better Way to Achieve CSF 2.0 Alignment

When you conduct a self-assessment, either internally or through a third party, you'll often find that your results lack:

- Data-driven conclusions that clearly show the best actions you can take to reduce risk.
- An easy way to conduct comparative analysis that measures and articulates improvements over time.
- Comparative analysis against target maturity levels or industry peer benchmarks.
- The ability to quickly crosswalk between frameworks so that you can accelerate evidence gathering for compliance.

Fortunately, there is a better way to evaluate your organization against CSF 2.0 and other leading cybersecurity frameworks. CRITICAL**START**® Risk Assessments give you a clear picture of your risk profile and benchmark your data against industry peers. With customizable dashboards and reports along with peer benchmarking, you'll gain the insight you need to prioritize your next steps toward security improvement and drive toward continuous risk reduction.



Step 5: Take Definitive Action Toward Continuous Cyber Risk Reduction

Critical Start Risk Assessments simplifies the continuous cyber risk reduction process by providing an easy-to-use tool that records, tracks, and analyzes risk assessment data. Along with CSF 2.0 and 1.1, Critical Start Risk Assessments offers assessments for NIST 800-171, CIS Critical Security Controls v8 and more. Future assessments are made available to customers at no cost as they are released.

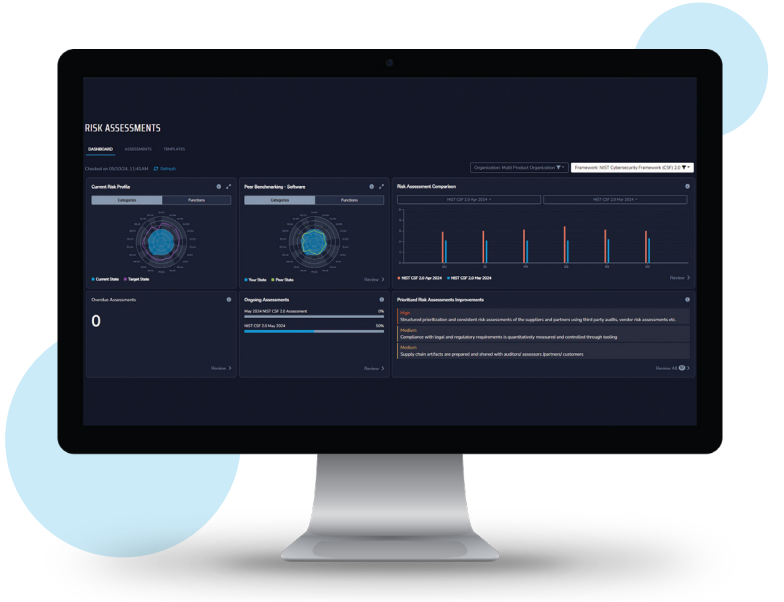
Each questionnaire captures essential data and provides the ability to attach evidence and add cross-functional reviewers to improve accuracy. Assessment analysis includes peer benchmarking for greater visibility into your organization's risk posture versus competitors. Risk-Ranked Recommendations help you prioritize your security improvement efforts and manage budgets effectively. And comparisons across recurring internal assessments deliver critical tracking metrics and prove the value of your security improvements over time.

Why Critical Start Risk Assessments?

All too often, risk assessment results get shoved into a drawer or forgotten in a spreadsheet on a shared drive. You put in all that work only to limit the actionability of your data.

The powerful Risk Assessments offering from Critical Start makes your data actionable by:

- ✓ Gathering and consolidating all risk assessment data into a single platform for historical comparison and trend analysis.
- ✓ Assessing your security risk profile against industry peer benchmarks and target maturity levels.



- ✓ Automatically migrating existing CSF 1.1 assessment data (or cross walking other assessment framework data) to CSF 2.0 for rapid gap analysis.
- ✓ Tracking, measuring, and visualizing security risk improvements and providing detailed reports to each organizational stakeholder.
- ✓ Identifying and prioritizing your best next steps with Risk-Ranked Recommendations.
- ✓ Giving you the data you need to make strategic and impactful security investment decisions.

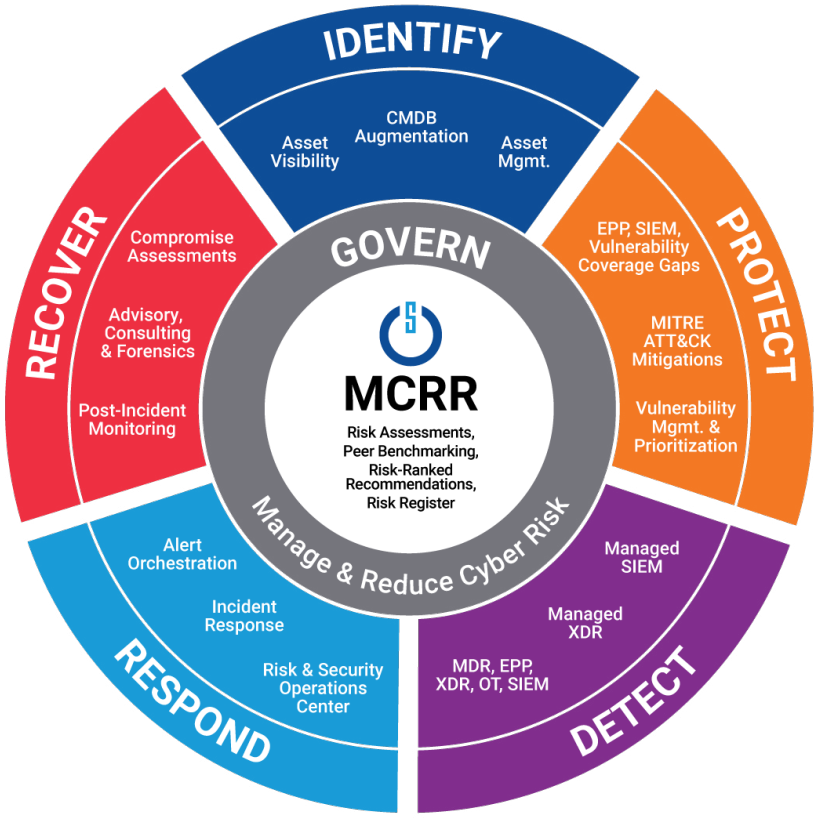
Step 5: Take Definitive Action Toward Continuous Cyber Risk Reduction (continued)

Beyond Risk Assessments – Managed Cyber Risk Reduction

Critical Start is the world's first Managed Cyber Risk Reduction (**MCRR**) vendor. With Critical Start, you can begin your journey toward better security with Risk Assessments and then move meaningfully toward full risk management with a complement of tools and services that align with CSF 2.0, plus support a wide array of additional cybersecurity frameworks.

Learn More

> Organizations increase the odds substantially of outwitting cyber-attackers by taking a more proactive and holistic approach to reducing cyber risk, like the one presented by Critical Start's new Managed Cyber Risk Reduction.
>
> CRAIG ROBINSON, RESEARCH VICE PRESIDENT AT IDC



Learn More and Get Started

CRITICALSTART®
Don’t Fear Risk. Manage It.

For more information, contact us at:
https://www.criticalstart.com/contact/