CYBER SECURITY HUB

# IMPLEMENTING A RISK-BASE CYBER SECURITY FRAMEWORK

The NIST CSF quick guide to clarity, readiness, buy-in and risk management for business security leaders

Sponsored by: tracesecurity

# Cyber Security Begins With Understanding An Organization's Risk

Cyber security risk exists throughout an organization through its people, process, and technology. Where is information stored? What are the external threats to that information? How can that information be accessed internally? What are your internal threats? Have you considered the environmental threats to your information? To protect its information, it is imperative for the organization to be able to answer these questions. Then, the organization can begin the process of mitigating its cyber security risk.

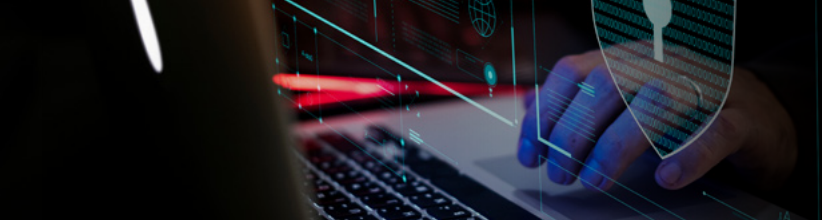
Because risk is ever-evolving, this process must be ongoing. This is why all regulations and standards require risk assessment and risk management to be both the starting point and foundation of a cyber security program.

Simply put, risk assessment and risk management are the foundation of an enterprise cyber security program. "You need to be able to measure risk in order to manage it effectively," says Bob Turner, CISO for the University of Wisconsin-Madison. Cyber security is an enabler to IT and creates focus for measuring an organization's risk. "Robust risk management is important to leaders, decision makers, managers, and technicians."

"A risk assessment prioritizes the benefit and impact to the organization," notes Glenda Lopez, Director of Global Risk and Compliance with The Henry M. Jackson Foundation for the Advancement of Military Medicine. "You can then weigh this against the cost of a data breach. And you can compare the value to cost of a breach."

> "You need to be able to measure risk in order to manage it effectively."

**Bob Turner, CISO,**
**University of Wisconsin-Madison**





# Standardizing The Control Framework For Enterprise Value

Now that you have established risk assessment and risk management as the foundation for the cyber security program, how do you identify the appropriate control framework for your program? To start, the control framework selected should be based on a common standard. The value of a standard is multi-faceted. Operationally, standards can help streamline processes and reduce costs.

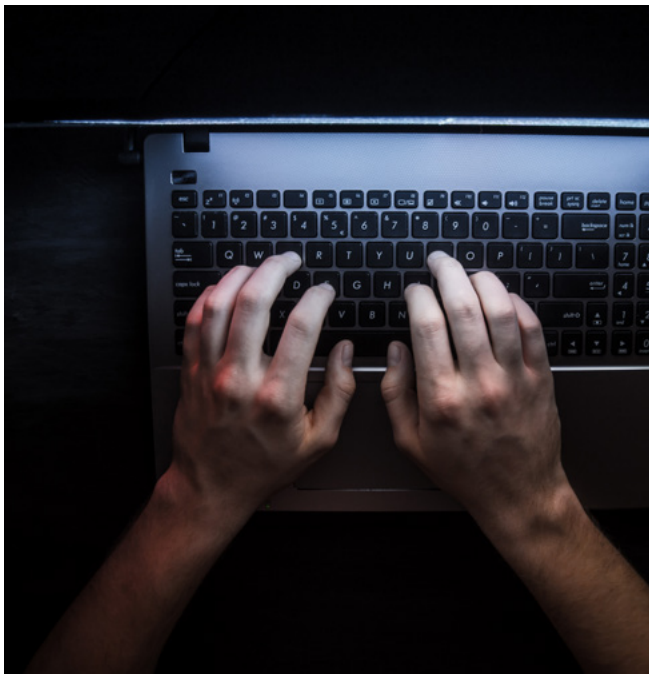
Organizationally, standards define terminology and manage systems, processes, and controls in a uniform manner. Legally, the FTC, SEC, state legislators, and others are increasingly using language requiring "reasonable" safeguards. According to Tara Swaminatha, a data privacy and cyber security partner at Squire Patton Boggs in Washington, D.C., and former federal prosecutor in the Computer Crime & Intellectual Property Section at the U.S. Department of Justice, organizations having developed a cyber security program following NIST CSF will mitigate cyber security-related liability exposure in the face of regulatory enforcement actions.

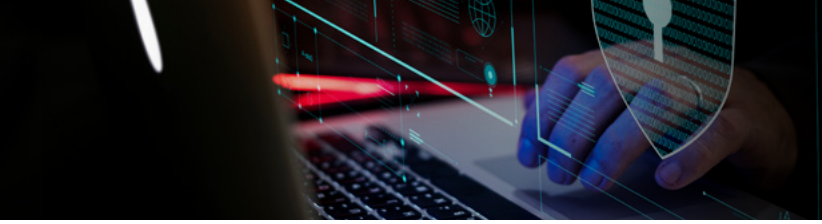
"Under current law in the United States, businesses have no clear guidance about how to build a security program that would comply with the law," writes Swaminatha. "No matter what security protections a business employs, it cannot be certain that the protections would be judged as being sufficient in a lawsuit or regulatory investigation." In many areas of the law, negligence standards tend to be much clearer and businesses generally know they can be considered legally sufficient if certain standards or conditions are met. In other words, those standards instruct businesses adequately on the steps to take to be reasonable and not negligent.

By identifying and quantifying levels of risk, a framework can recommend specific methods of mitigation for the enterprise.

> "With all the data breaches in the news, individuals buying products or services and companies doing business with providers or payers want assurances that security, privacy, compliance, and risk management are taken seriously. NIST CSF is one way to do that."

**Rebecca Wynn, Head of Information Security & Data Protection Officer, Matrix Medical Network**







# Why The NIST Cyber Security Framework Is The Go-To Standard

In the United States, the NIST Cyber Security Framework (CSF) is widely pointed to as the go-to standard for security practices and development.

The NIST CSF was developed through an international partnership of small and large organizations, including owners and operators of the nation's critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST). President Trump went one step further and issued EO 13800 in 2017, Strengthening the Cyber Security of Federal Networks and Critical Infrastructure, and made the framework created by Obama's order part of federal government policy. Furthermore, the federal government gave small to mid-size companies assistance when President Trump signed the NIST Small Business Cyber Security Act in January 2018. It directed NIST to develop a streamlined version of its famed Cyber Security Framework.

"The updated NIST cyber security framework is a pragmatic tool to enable an organization to gain clarity on its current level of capability for cyber risk management," says James Turner, cyber security industry analyst for IBRS.

> "The updated NIST cyber security framework is a pragmatic tool to enable an organization to gain clarity on its current level of capability for cyber risk management."
>
> **James Turner, Cyber Security Industry Analyst, IBRS**

**In terms of enterprise value, the CSF:**

**1. Provides a common language and systematic methodology for managing cyber security risk.**

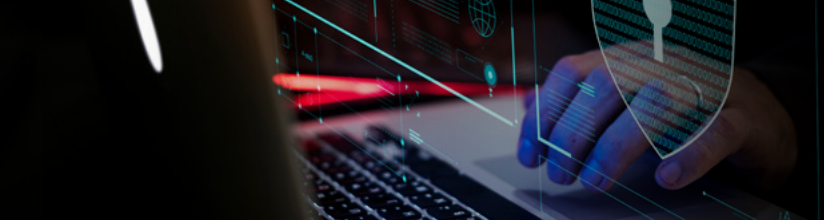
Enterprise security leaders must self-assess their situation and gain the validation of an external risk assessment to gain the support of the entire organization. The Framework can be used as an effective communication tool for senior stakeholders (CIO, CEO, Executive Board, etc.), especially as the importance of cyber security risk management receives elevated attention in C-suites and Board rooms. The Functions inside the Framework Core offer a high-level view of cyber security activities and outcomes that could be used to provide context to senior stakeholders beyond current headlines in the cyber security community.

**2. Can be used by organizations in any industry.**

The NIST CSF maps to leading industry regulations and standards, including COBIT, FFIEC, HIPAA, HITRUST, and ISO, enabling compliance reporting to align with many regulatory agencies.

"HIPAA is the main compliance driver for healthcare," says Randall Frietzsche, enterprise CISO for Denver Health. HIPAA points to NIST for details on how to determine conformance. "Talking to committees and the board about encryption and firewalls doesn't mean much to them, but when I can explain this is what

> "HIPAA is the main compliance driver for healthcare."
>
> **Randall Frietzsche, Enterprise CISO, Denver Health**





HIPAA says or the government requires, it provides a level-set about protecting the organization and detecting threats. All areas of our strategy are aligned with the frameworks and programs of the team." As a technical leader, Frietzsche uses the Framework to provide specifics to the security team about guidance for pursuing it with mappings to multiple technical sources. Even if HIPAA were not the driver, Frietzsche says a compliance framework would have been used to build an appropriate structure for the security program.

The Health Information Trust Alliance, or HITRUST, is a privately held company located in the United States that, in collaboration with healthcare, technology and information security leaders, has established a Common Security Framework that can be used by organizations that create, access, store or exchange data. "The HITRUST controls framework is widely adopted in the healthcare industry," says Matrix Medical Network's Rebecca Wynn. The organization has released a single framework assessment that includes the controls necessary to address the NIST CSF requirements and an addendum to the HITRUST CSF Assessment report has been added to display the HITRUST CSF controls through the lens of the NIST CSF Core Subcategories.

Universities, by their nature, are open networks. "We cannot assume the network is safe," says Randy Marchany, CISO for university Virginia Tech (VT). "Organizationally, we need to have a policy stating what frameworks the organization will follow. I need a data classification set of policies and standards that declares what is high-risk data, etc. And then you need a standard that describes the minimum security standards declared." In some organizations, policy and standards information has always been there, but having separate end-point and server teams, for example, it may not all reside together in one place. Also, different departments have specific requirements, such as laws requiring HR to report breaches.

**3. Can be used by an organization, regardless of its size, industry, or cyber security maturity.**

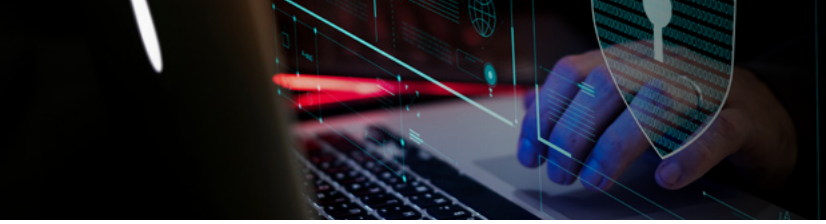
The five primary pillars for a successful and holistic cyber security program are: **Identify, Protect, Detect, Respond and Recover**. Known as the Framework Core, they aid organizations in easily expressing their management of cyber security risk at a high level and enabling risk management decisions.

The five functions are further split into 23 categories designed to cover the breadth of cyber security objectives for an organization, while not being overly detailed. Categories cover topics across cyber, physical, and personnel, with a focus on business outcomes.

Categories are further split into 108 subcategories, which are outcome-driven statements that provide considerations for creating or improving a cyber security program. Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it enables risk-based implementations that are customized to the organization's needs.

**The Framework Core consists of five primary pillars for a successful and holistic cyber security program:**

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





**NIST offers four tiers of expressing security capability:**

- **Tier 1 – Partial:** Organizational cyber security risk is not formalized and managed in an ad-hoc and sometimes reactive manner. There is also limited awareness of cyber security risk management.
- **Tier 2 – Risk-Informed:** There may not be an organizational-wide policy for security risk management. Management handles cyber security risk management based on risks as they happen.
- **Tier 3 – Repeatable:** A formal organizational risk management process is followed by a defined security policy.
- **Tier 4 – Adaptable:** An organization at this stage will adapt its cyber security policies based on lessons learned and analytics-driven to provide insights and best practices. The organization is constantly learning from the security events that do occur in the organization and will share that information with a larger network.

An organization may use this tiered approach to describe its strategy and cyber security goals. According to NIST, "Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it enables scalability. A small organization with a low cybersecurity budget, or a large corporation with a big budget, are each able to approach the outcome in a way that is feasible for them. It is this flexibility that allows the Framework to be used by organizations which are just getting started in establishing a cybersecurity program, while also providing value to organizations with mature programs."

"Choosing to move to the CSF was a result of an external assessment where we were able to see the benefits of having tiered implementation of common cybersecurity operational tasks," remarked CISO Turner. At the time of the assessment, the university had been focused on gaining a common understanding on security control requirements and effectiveness. "We did manage incident response to an earlier version of NIST but did not have the best view of the cause and effect that the CSF represents."

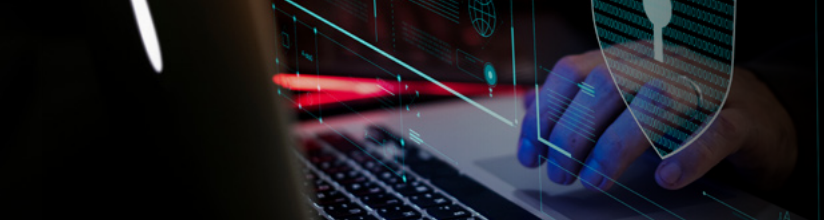
According to NIST, "Because the Framework is **outcome driven** and does not mandate how an organization must achieve those outcomes, it **enables scalability**."

**4. Could be a requirement for working with government agencies.**

Beyond the enterprise uptake of the NIST Framework, the U.S. government mandated its adoption in the public sector via Executive Order in 2018. This could lead to a requirement where suppliers for an agency or government-funded entity (such as a University or Healthcare system) will need to document and demonstrate capability to conform with the NIST Framework.

"As a university receiving federal grants, we must make sure that university standards meet the needs of the federal requirements," says Randy Marchany, CISO for university Virginia Tech (VT). "Pressure will come when the US Department of Education suggests that tools use the NIST SP 800-171 standard."

"We know that grant awards are based on what the research team can deliver, which includes protection of government data associated with the research," says University of Wisconsin-Madison's Turner. "That is one reason we are focused on being at the top tiers of the CSF and being able to prove it through external assessment and continuous monitoring."





# Value Of An External Assessment

Whether you are in the early stages of implementing the NIST CSF or updating your current program, external consultants can play a vital role. Having an external consultant perform an initial risk assessment using the NIST and the CSF can jump start your program. For existing programs, using a consultant to perform a third-party analysis can provide independent validation.

"One of the big values of an external consultant, is they are not internal and not politically motivated, so they are given a bit more trust," says VT CISO Marchany. "It does cost, and security is a loss-leader; we're insurance. A consultant can come in and bless the strategy or help gain approval of a strategy. There's value in a peer review to overcome internal inertial, or you respond when an incident occurs."

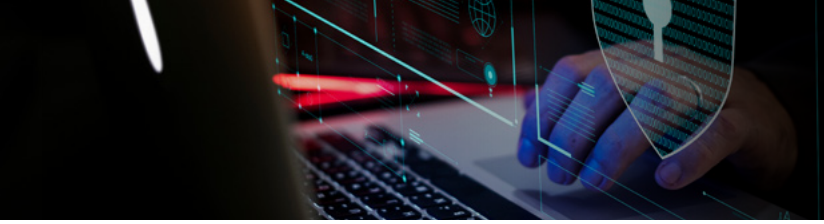
"An external assessment is important to utilize their knowledge as well as verify that current releases of tools are in place," says Lopez. "A third party will offer an unbiased control review and assemble evidence necessary for assessment. They'll suggest possible paths forward."

You must be willing to accept the results of an external assessment and take action. "Knowing where you stand against the frameworks and checklists is paramount – there is always opportunity to learn how to be better," observes CISO Bob Turner.

An additional benefit of working with a company that provides an external assessment and audit of processes is that you gain access to their documentation and can speak with a subject-matter expert on emerging topics like GDPR. "Industrial control and healthcare are serious markets dealing with health and safety," notes Denver Health's Freitzsche. "Priority always has to be for building the validation and program roadmap."

# Conclusion

Building an effective security program starts with understanding the true risk for the organization. Assessing the risk leads to mitigation and management of risk. No matter the previous experience working with security standards and frameworks, the size of the organization, or the budget available, both private and public sector enterprises are turning to the NIST Cyber Security Framework as the basis to identify security priorities. The priority, size of gap, and estimated cost of the corrective actions help organizations plan and budget for cyber security improvement activities.





# Sponsor Spotlight

tracesecurity

TraceSecurity knows that protecting information is both a business and compliance risk for organizations, regardless of size or industry. We also know that organizations struggle with how to be compliant, how to reduce the risk of a breach, and where they should begin. All regulations and best practices require risk assessment and risk management to be the foundation of their program. At TraceSecurity, we have more than a decade of experience helping organizations build information security programs that reduce the risk of a breach and meet their industry compliance requirements.

The TraceSecurity Risk Assessment draws on years of experience across thousands of engagements to identify risks, describe these threats to your business, and prioritize the order in which they should be addressed. We then share recommendations to ensure that the risk is acceptable to you, serving as a cyber security orientation that helps you know where your organization stands so you can create a plan to get better.

But TraceSecurity doesn't stop there. Once you've completed your Risk Assessment, we want to equip you with the tools to take action on your remediation plan. That's why we offer software that lets you see your results from our assessment, as well as assign, track and monitor remediation activity. Our software also allows you to generate reports that show your plan in action and will be updated once remediation activity is complete, so that you can take control of your information security program — no matter the size of your organization.

TraceSecurity's Risk Assessment is built on the NIST Cyber Security Framework so you can be assured that it meets regulatory requirements. In addition, through our Risk Management software, we provide mappings to all industry specifics standards to ensure your compliance reporting requirements are met. Partner with TraceSecurity to build your information security program and reduce your organization's risk.

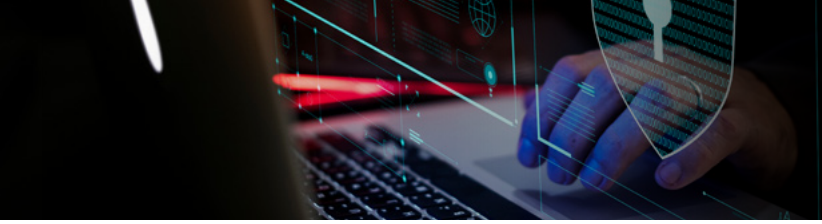
## ABOUT TRACESECURITY

TraceSecurity has been assisting customers with IT security and compliance for more than 15 years. Founded in 2004 to serve the data-intensive financial services industry, our team was built during a time of heavy regulations and rapidly growing cyber security threats.

As time passed, the threats and regulations continued to grow across all industries. Businesses needed to be more secure, but they often lacked the knowledge to identify how to begin their security and compliance programs — so we set out to change that.

We listened to our customers and identified their biggest problems and concerns around IT security and compliance. With their feedback, we created practical, worry-free cyber security solutions that deliver the greatest impact for our customers' investment. Our services and software help organizations of all sizes reduce the risk of security threats and ensure full compliance without unreasonable costs, staffing or time.

TraceSecurity is proud to offer a variety of core solutions to meet your needs. From risk assessments to penetration testing to anti-phishing solutions, we provide services that proactively prepare you and your employees for real-world cyber threats.





CYBER SECURITY HUB

### ABOUT CYBER SECURITY HUB

The Cyber Security Hub is an online news source for global cyber security professionals and business leaders who leverage technology and services to secure the entire perimeter in their enterprise.

We're dedicated to providing the latest industry news, thought leadership and analysis in the cyber security space. Cyber Security Hub's expert commentary, tools and resources are developed through obtaining data and interviewing end users and analysts throughout the industry to deliver practical and strategic advice.

Our editorial team surveys and monitors the latest trends in cyber security and creates news articles, market reports, case studies and in-depth analysis for a captive audience consisting of C-Level executives, VPs and directors of cyber security and information technology.

## CYBER SECURITY HUB

**Dorene Rettas**
Managing Director,
Cyber Security Hub
Dorene.Rettas@CSHub.com

**Alarice Rajagopal**
Editor,
Cyber Security Hub
AlariceR@CSHub.com

**Jodi Lozauskas**
Marketing Manager,
Cyber Security Hub
JodiL@CSHub.com

**Rosecley Morishita**
Editorial Director,
Cyber Security Hub
Rosecley.Morishita@iqpc.com

**Michael Roberts**
Sales Director,
Cyber Security Hub
Mike.Roberts@CSHub.com

### SOCIAL MEDIA INFORMATION:

TWITTER: CSHubUSA

FACEBOOK: CSHubIQPC

LINKEDIN: Cyber Security Hub - Enterprise Security Professionals