Applying the NIST CsF to Establish an Enterprise Cybersecurity Plan

A Cyber Brief

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CsF) provides a risk-based compilation of guidelines that can enable your organization to identify, implement and improve cybersecurity practices. It establishes a common language for internal and external communication of cybersecurity challenges and priorities.

The focus of this article is to examine how the NIST CsF provides the foundation for you to establish an enterprise cybersecurity plan that addresses within its scope compliance priorities such as federal or state regulatory mandates such as HIPAA or HITECH, as well as security standards such as PCI DSS.

Roadmap for Cybersecurity Practices

The CsF is the result of the February 2013 United States Presidential Executive Order titled “Improving Critical Infrastructure Cybersecurity”. The CsF envisions effective cybersecurity as a dynamic practice area that is continually addressing threats with a risk-based approach to prioritize response. The NIST CsF is inclusive of risk-based guidelines that enables you to build a prioritized roadmap towards enhanced cybersecurity practices.

Ali Pabrai
Global Cybersecurity & HITRUST Expert

Organization

The CsF provides your organization with an opportunity to build a credible cybersecurity plan. The CsF enables an organization like yours to determine your current cybersecurity capabilities and set enterprise goals for a target state. It helps you to establish a plan to improve and maintain your cybersecurity program.

The CsF comprises of three primary components:

1. Profile
2. Implementation Tiers
3. Core

Step 1: Define an Enterprise Cybersecurity Profile

The Profile component enables organizations to align and improve cybersecurity practices based on their individual business needs, tolerance for risk, and available resources.

To do so, organizations create a *Current Profile* by measuring their existing programs against the recommended practices in the CsF Core. These practices include processes, procedures, and technologies such as asset management, alignment with business strategy, risk assessment, access control, employee training, data security, event logging and analysis, and incident response plans.

To identify a *Target Profile*, organizations employ the same Core criteria to determine the outcomes necessary to improve their cybersecurity posture. Unique requirements by industry, customers, and business partners can be factored into the Target Profile.

Once completed, a comparison of the Current and Target Profiles will identify the gaps that should be closed to enhance cybersecurity and provide the basis for a prioritized roadmap to help achieve these improvements.

Step 2: Implementation Tiers Establish Cybersecurity Maturity

Implementation Tiers help create a context that enables organizations to understand how their current cybersecurity risk-management capabilities stack up against the characteristics described by the Framework.

Tiers range from Partial (Tier 1) to Adaptive (Tier 4). Figure 1 describes the Tiers of cybersecurity maturity.

Tier 1	Partial	Risk management is ad hoc, with limited awareness of risks and no collaboration with others
Tier 2	Risk Informed	Risk-management processes and program are in place but are not integrated enterprise-wide; collaboration is understood but organization lacks formal capabilities
Tier 3	Repeatable	Formal policies for risk-management processes and programs are in place enterprise-wide, with partial external collaboration
Tier 4	Adaptive	Risk-management processes and programs are based on lessons learned and embedded in culture, with proactive collaboration

Figure 1: Tiers of cybersecurity maturity.

NIST recommends that organizations seeking to achieve an effective, defensible cybersecurity program progress to Tier 3 or Tier 4.

Step 3: CsF Core Defines Desired Cybersecurity Outcomes

The Framework Core defines standardized cybersecurity activities, desired outcomes, and applicable references, and is organized by five continuous functions:

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

Figures 2 and 3 describe the CsF Core.

Figure 2: NIST CSF lifecycle.

Functions	Definition	Categories
Identify	An understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities	Asset management, business environment, governance, risk assessment, risk management strategy
Protect	The controls and safeguards necessary to protect or deter cybersecurity threats	Access control, awareness and training, data security, data protection processes, maintenance, protective technologies
Detect	Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events	Anomalies and events, continuous monitoring, detection processes
Respond	Incident-response activities	Response planning, communications, analysis, mitigation, improvements
Recover	Business continuity plans to maintain resilience and recover capabilities after a cyber breach	Recovery planning, improvements, communications

Figure 3: Five core functions of effective cybersecurity.

The Framework Core describes the continuous cycle of business processes that constitute effective cybersecurity.

Closing Remarks!

Today every organization, every business, and every government agency is required to meet mandates such as HIPAA, HITECH, PCI DSS or others. Further, organizations also must comply with additional regulatory requirements – such as state security mandates.

The NIST CsF is the framework that can enable organizations to shift their reactive security activities to a formal, proactive program.

NIST CsF is a tipping point in cybersecurity.

Organizations must look to not just address compliance requirements in the context of the specific and minimal associated with mandates. Instead, organization should raise the bar for cybersecurity by adopting a formal, proactive framework for addressing not just all compliance requirements, but also the constantly changing world of cyber threats.

When senior executives formally adopt a cybersecurity framework such as the NIST CsF, they are essentially adopting a proactive risk-management standard. They are effectively laying the foundation to reduce the risk to the business.

My final thoughts:

Formally adopt a cybersecurity framework to address all compliance mandates that your organization must meet. The NIST CsF is an excellent choice.

Conduct a comprehensive and thorough risk analysis exercise and document your current profile. Alert senior management to the current profile of the organization (and associated risks to the business).

Develop your target profile and ensure senior leadership is 100% on-board with establishing a time-frame for achieving defined requirements.

Implement an active and vibrant risk management program to address identified compliance and security gaps, and achieve the defined target profile.

Tomorrow starts now! Get started and establish a credible cybersecurity plan organized and aligned with the NIST CsF to prioritize security initiatives and continually address regulatory compliance mandates.

FEATURED SPEAKER WORLDWIDE

Uday Ali Pabrai

Global Cybersecurity & HITRUST Expert

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP), HITRUST (CCSFP), Security+, a global cybersecurity & HITRUST expert, is the chairman & chief executive of ecfirst.

A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, GDPR, FERPA, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations in USA. ecfirst is an approved HITRUST CSF Assessor.

Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Canada, Saudi Arabia, Bahrain, Jordan, Egypt, Ghana and other countries. Conferences Mr. Pabrai has been featured at include AHIMA, HCAA, ISACA CSX, HIMSS, InfraGard (FBI), ISSA, HIPAA Summit, Google Privacy & Security Summit, Microsoft Tech Summit, Internet World, DCI Expo and hundreds of others.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the Defense Intelligence Agency (DIA), and the Naval Surface Warfare Center. His career was launched with Fermilab, a U.S. Department of Energy nuclear research entity.

Mr. Ali Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

Mr. Pabrai can be reached at Pabrai@ecfirst.com or +1.949.528.5224.
Control your excitement!

"We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years – with one unanimous word that keeps resounding among audiences and staff alike – *AWESOME!*"

"He is a *tremendously engaging and knowledgeable presenter* who is able to *distill the essence of complex cybersecurity topics into comprehensible and actionable components* for both highly skilled, technical audiences as well as those who are just entering or transitioning into the security part of the IT industry."

"His "behind the curtain" professionalism and *enthusiastic willingness to help develop, customize and deliver great content paired with his absolute commitment to professionalism as a presenter and "doing what it takes" is a rare combination.*"

"We greatly look forward to working with Mr. Pabrai each and every time and know he will deliver excellence."

Michael Mach *CMP, CMM, CED*
Conference Program Manager
ISACA

"I have 20+ years of experience in the Healthcare IT industry in a variety of roles including Cybersecurity software and services. During this time I have seen numerous speakers on the topic of Cybersecurity and *Ali Pabrai is among the best.* He covers the state of the industry, healthcare-specific regulations, process, product, best practices and call-to-action takeaways in a manner that can be understood at multiple levels including technical, clinical, supply chain and executive."

"Ali also weaves in stories and humor to keep the audience engaged on what can be a dry yet frightening topic. *I highly recommend Ali Pabrai as a speaker, trainer and consultant in this area.*"

Chris Liburdi
Director – Business Development/Business Technology
Vizient

"The professionalism and complete subject matter knowledge make ecfirst the consultants of choice for HIPAA and HITECH information and issues. Our experience with ecfirst was unwavering in addressing all issues and enabling a foundation for an active and vibrant compliance program. Pabrai's leadership was exceptional, very devoted to ensuring all areas were appropriately addressed."

Blake Anderson
Department of Health
State of Utah

Pabrai @ Global Events

Published Author

Getting Started with HIPAA
First published book on HIPAA!

UNIX Internetworking
First book on UNIX & Networks!

Internet & TCP/IP Network Security
First book on TCP/IP security!

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

ecfirst | HITRUST Authorized CSF Assessor

Perfecting the Art of Active Cyber Defense

Client Reference

"I just wanted to take a moment and say thank you. Thank you and the ***excellent team*** at ecfirst for ***hard work***, late hours and ***diligence*** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an ***exceptional partner*** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfirst in the cybersecurity space in the future. I continue to recommend ecfirst highly and often!"

BRG Berkeley Research Group — **Chip Goodman | Vice President of Information Technology**

"The ecfirst team literally helped us build our HIPAA practices from ground up since 2012, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an ***integral part*** of our business strategy and have been ***extremely satisfied*** with the ***quality and value*** of the services that ecfirst has rendered."

BrightOutcome COLLABORATIVE SYMPTOM MANAGEMENT — **DerShung Yang | Founder & President**

"Provant Health partnered with ecfirst to build a plan and assist in executing it with the goal of achieving HITRUST certification. Ali Pabrai and his team were ***flexible, collaborative*** and most importantly patient as we worked to educate our management team and key employees on the meaning and value of HITRUST. I'd recommend ecfirst to any company who wants to understand HITRUST or work on assessing and remediating their processes and systems in preparation for certification."

provant health life. changing. — **Tom Basiliere | Chief Information Officer**

Kris Laidley | Kris.Laidley@ecfirst.com | +1.515.987.4044 ext 25

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

Kris Laidley

Team Lead, Business Development & Certification Program

ecfirst/HIPAA Academy

Phone: +1.515.987.4044 ext 25

Email: Kris.Laidley@ecfirst.com

Robert Acosta

National Sales Director

ecfirst/HIPAA Academy

Phone: +1.949.793.5700

Email: Bob.Acosta@ecfirst.com

www.ecfirst.com