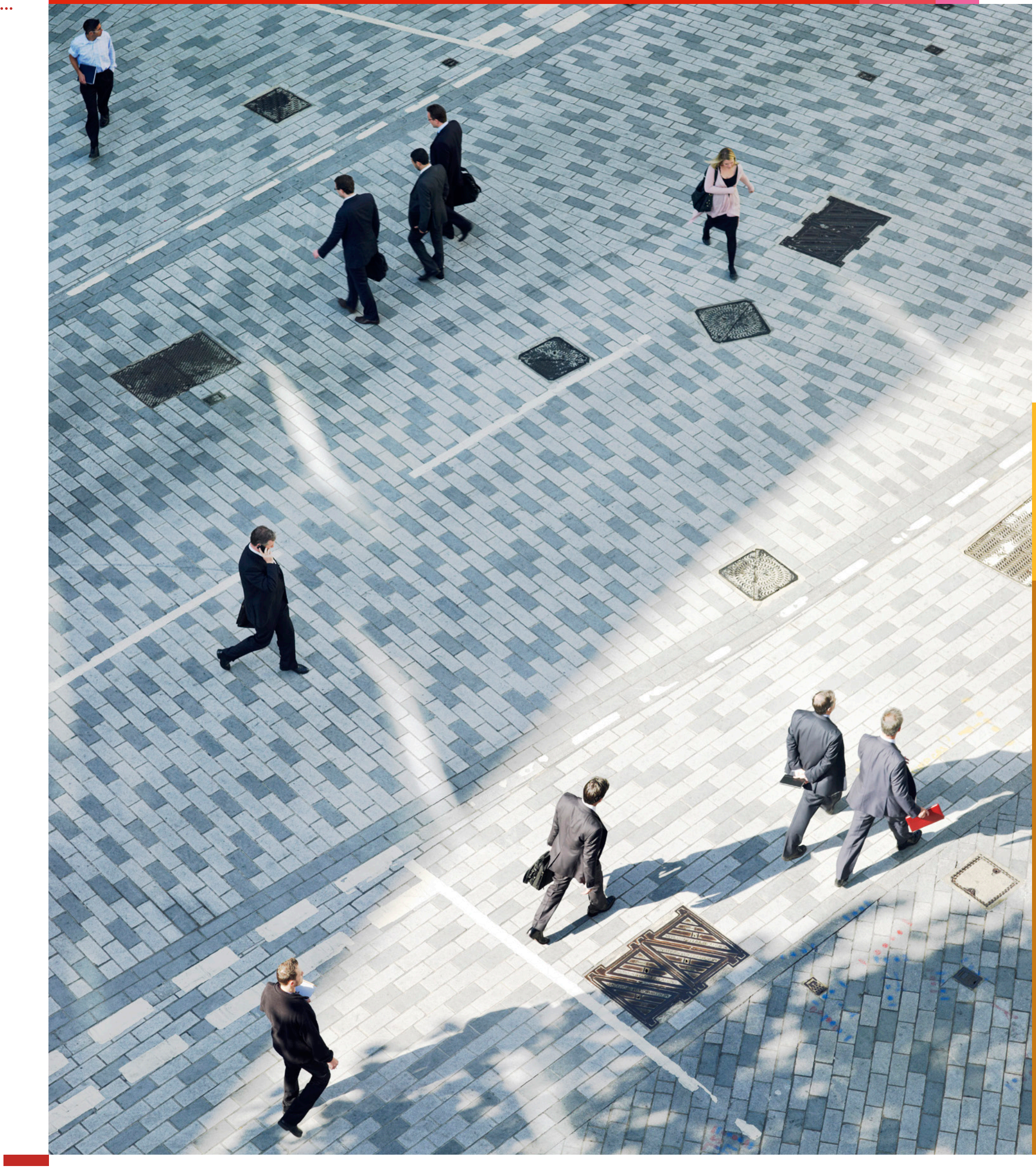
www.pwc.com/cybersecurity

# *Why you should adopt the NIST Cybersecurity Framework*

*May 2014*



pwc

***The National Institute of Standards and Technology Cybersecurity Framework may be voluntary, but it offers potential advances for organizations across industries.***

# NIST Cybersecurity Framework

**What comprises critical infrastructure?**

US Presidential Policy Directive 21 defines critical infrastructure as the following 16 sectors:

- Chemicals
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food & agriculture
- Government facilities
- Healthcare & public health
- Information technology
- Nuclear reactors, materials, & waste
- Transportation systems
- Water & wastewater systems

**Source:** Department of Homeland Security, Critical Infrastructure Sector

While the ***NIST Cybersecurity Framework*** may not constitute a foolproof formula for cybersecurity, its benefits may be missed by those who choose to forgo or postpone implementation of the voluntary guideline, in part or in whole.[1] That's because the Framework comprises leading practices from various standards bodies that have proved to be successful when implemented, and it also may deliver regulatory and legal advantages that extend well beyond improved cybersecurity for organizations that adopt it early.

In fact, while the Framework targets organizations that own or operate critical infrastructure, adoption may prove advantageous for businesses across virtually all industries.

The NIST Cybersecurity Framework, which was drafted by the Commerce Department's National Institute of Standards and Technology (NIST), yields no surprises for critical infrastructure executives who have followed its development, particularly for those whose personnel participated in workshops to help craft the guidelines. The Framework does not introduce new standards or concepts; rather, it leverages and integrates industry-leading cybersecurity practices that have been developed by organizations like NIST and the International Standardization Organization (ISO).

The Framework is the result of a February 2013 Executive Order titled ***"Improving Critical Infrastructure Cybersecurity"*** and 10 months of collaborative discussions with more than 3,000 security professionals.[2] It 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 Framework is a reiterative process designed to evolve in sync with changes in cybersecurity threats, processes, and technologies. It will be revised periodically to incorporate lessons learned and industry feedback. In effect, the Framework envisions effective cybersecurity as a dynamic, continuous loop of response to both threats and solutions.

The Framework provides an assessment mechanism that enables organizations to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining cybersecurity programs. It comprises three primary components: ***Profile, Implementation Tiers,*** and ***Core.***

[1] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014

[2] Federal Register, Executive Order 13636—Improving Critical Infrastructure Cybersecurity, February 19, 2013

*The Framework is a risk-based compilation of guidelines designed to help organizations assess current capabilities and draft a prioritized roadmap toward improved cybersecurity practices.*

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 Framework 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.

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

*Figure 1: 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 |

The Framework Core defines standardized cybersecurity activities, desired outcomes, and applicable references, and is organized by five continuous functions: Identify, Protect, Detect, Respond, and Recover. (Figure 2.) The Framework Core, in effect, describes the continuous cycle of business processes that constitute effective cybersecurity.

*Figure 2: Five core functions of effective cybersecurity*

| 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 |

## *Benefits beyond improved cybersecurity*

For most organizations, whether they are owners, operators, or suppliers for critical infrastructure, the NIST Cybersecurity Framework may be well worth adopting solely for its stated goal of improving risk-based security. But it also can deliver ancillary benefits that include effective collaboration and communication of security posture with executives and industry organizations, as well as potential future improvements in legal exposure and even assistance with regulatory compliance.

A guiding principle of the Framework is collaboration to share information and improve cybersecurity practices and threat intelligence. We concur that collaboration has very real benefits.

Our research shows that companies with highly effective security practices make it a point to collaborate with others to advance security and threat awareness. In fact, our annual security survey found that 82% of companies with high-performing security practices collaborate with others to achieve these goals.[3] One of the most effective collaboration methods is participation in Information Sharing and Analysis Centers (ISACs), which have gained traction in security-forward industries like financial services. We recommend that organizations actively participate in ISACs appropriate to their industry.

[3] PwC, The Global State of Information Security® Survey 2014, September 2013

Effective collaboration hinges upon open and meaningful dialogues. To that end, the Framework has created a common language to facilitate conversation about cybersecurity processes, policies, and technologies, both internally and with external entities such as third-party service providers and partners. NIST encourages organizations to share current intelligence on vulnerabilities, threat information, and response strategies. The potential benefits of a common lexicon and increased collaboration are strong. If, for instance, an organization's entire supply chain adopts the Framework lexicon, risks to the supply chain can be better communicated, understood, and potentially mitigated.

*The Framework creates a common language for the discussion of cybersecurity issues that can facilitate internal and external collaboration.*

It's important to note that the Framework casts the discussion of cybersecurity in the vocabulary of risk management. With good reason: Executive leaders and board members typically are well-versed in risk management, and framing cybersecurity in this context will enable security leaders to more effectively articulate the importance and goals of cybersecurity. It can also help organizations prioritize and validate investments based on risk management.

A common lexicon for cybersecurity will also enable security leaders to effectively communicate practices, goals, and compliance requirements with third-party partners, service providers, and regulators. In particular, there should be a more meaningful, structured dialogue of cybersecurity priorities with third parties. Consider, for instance, that our annual security survey found that only 58% of global respondents require third-party partners to comply with their privacy policies.[4] What's more, only half (50%) conduct compliance audits of partners that handle sensitive data to ensure that they can adequately protect the information. A common vocabulary and standard industry practices will help get the conversation started, internally and externally.

[4] PwC, The Global State of Information Security® Survey 2014, September 2013

## *The regulatory and legal advantages of early adoption*

*The Framework may set cybersecurity standards for future legal rulings.*

*As a result, organizations that adopt the Framework at the highest possible risk-tolerance level may be better positioned to comply with future cybersecurity and privacy regulations.*

The executive order that created the Framework stipulated that regulatory agencies will determine which aspects of the Framework should be incorporated into existing regulatory mandates across industry sectors. In effect, the Framework may become the *de facto* standard for cybersecurity and privacy regulation and may impact legal definitions and enforcement guidelines for cybersecurity moving forward.

As a result, organizations that adopt the Framework at the highest possible risk-tolerance level may be better positioned to comply with future cybersecurity and privacy regulations. At the least, businesses that operate in regulated industries should begin monitoring how regulators, examiners, and other sector-specific entities are changing their review processes in response to the Framework.

The Framework may also set cybersecurity standards for future legal rulings. If, for instance, the security practices of a critical infrastructure company are questioned in a legal proceeding, the courts could identify the Framework as a baseline for "reasonable" cybersecurity standards. Organizations that have not adopted the Framework to a sufficient degree—Tier 3 or Tier 4, for instance—may be considered negligent and may be held liable for fines and other damages.

Adoption of the Framework, therefore, should be seen as an exercise of due care, and organizations should understand that their corporate officers and boards may have a fiduciary obligation to comply with the guidelines.

Finally, organizations that adopt the Framework also stand to realize other, as-yet-undefined, incentives. The directive that established the NIST Framework calls for the Department of Homeland Security (DHS) to establish incentives to promote adoption of the framework. These incentives have not yet been established but discussions have revolved around cyber insurance, government grants, technical assistance, and regulatory streamlining, among other possibilities. Government agencies may soon begin to leverage these incentives to encourage adoption of the guidelines.

## *A business requirement for third-party providers?*

Using history as a guide, the Framework may become a business requirement for companies that provide services to critical infrastructure owners, operators, and providers. For example, an organization deemed to be a critical infrastructure provider that adopts the Framework may require that its vendors and suppliers achieve the same Implementation Tier ranking. Doing so will help the organization protect itself from a potential weak link in its supply chain.

Already, we have seen that some service providers in the oil and gas industry are performing self-assessments based on the Framework to better understand their risk-based cybersecurity posture in order to be prepared should future requests for proposals (RFPs) and partnerships require some level of implementation with the Framework.

## *The challenges and limitations of the Framework*

It's important to note that there is no one-size-fits-all solution for cybersecurity, and the government cannot provide comprehensive, prescriptive guidelines for all entities across industries. So while the Framework offers worthwhile standards for improving cybersecurity, it does not fully address several critical areas.

> ***It's important to note that there is no one-size-fits-all solution for cybersecurity, and the government cannot provide comprehensive, prescriptive guidelines across industries.***

Consider, for instance, the lack of data privacy standards. NIST abandoned its proposed methodology to address privacy and civil liberties concerns due to a lack of consensus and support from industry participants.[5] Many were concerned that the approach proposed by NIST was not consistent with private-sector practices and therefore might inhibit adoption of the Framework. The agency is currently drafting privacy principles and requirements to include in future versions of the Framework.

The Framework falls short in other areas. For instance, it does not address the need to implement processes to identify and understand an organization's unique threat adversaries, their motivations, their capabilities, and the data they target. An effective cybersecurity program requires that organizations understand and anticipate threat actors, and then apply commensurate safeguards.

Nor does the Framework discuss an organization's statutory, contractual, and regulatory obligations for cybersecurity. These obligations should be an integral part of a security strategy.

It also does not address the "technology debt" that builds as organizations spend their IT budget on emerging technologies while failing to adequately maintain existing infrastructure. As a result, older IT systems and software may atrophy and critical patches may not be installed, potentially exposing the organization to cybersecurity incidents.

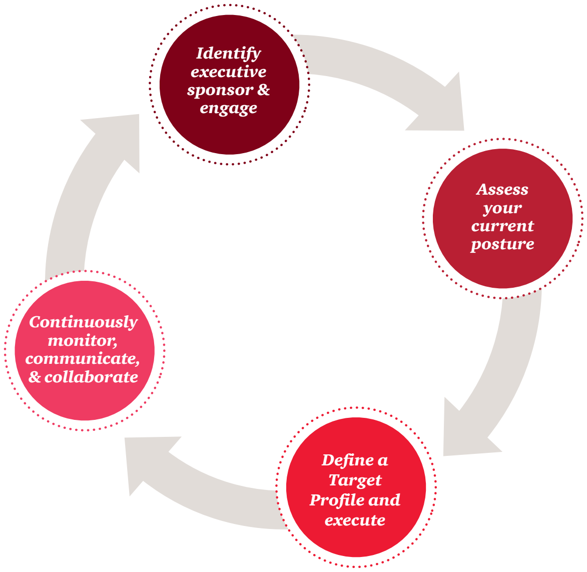
Finally, it's worth noting that a key challenge for many will be the extended timeframe necessary to fully adopt the Framework. For larger organizations in particular, the initial identification of assets may be a multi-year journey that may delay implementation of detection activities for several years. The hard truth is that most organizations cannot afford to defer improvement of cybersecurity programs over a period of years.

[5] http://www.nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-Update-011514-2.pdf

## *Taking action to implement the Framework*

It is our opinion that the NIST Cybersecurity Framework represents a tipping point in the evolution of cybersecurity, one in which the balance is shifting from reactive compliance to proactive risk-management standards. While the Framework is voluntary, organizations across industries may gain significant benefits by adopting the guidelines at the highest possible risk-tolerance level given investment capital.

Doing so will not only help improve cybersecurity programs, but also potentially advance regulatory and legal standing for the future. The following is our four-step process to get started:


Identify executive sponsor & engage
Assess your current posture
Define a Target Profile and execute
Continuously monitor, communicate, & collaborate

1. ***Identify your executive business sponsor and engage:*** Although not specifically included in the Framework, executive alignment and business context for your organization's desired cybersecurity posture is critical for appropriate implementation of the Framework.

2. ***Assess your current posture:*** Use a risk-based approach to assess your cybersecurity practices against the Framework Core industry standards and guidelines. This will help you determine the elements to include as desired control objectives.

3. ***Define a Target Profile and Execute:*** Based on your assessment, establish a Current Profile of cybersecurity activities and risk-management practices. Using a combination of the Framework Core and business-specific requirements that have been endorsed by your executive sponsor, create a baseline to guide cybersecurity risk-management activities. Next, determine a Target Profile to identify gaps and draft a prioritized action roadmap and execution program to achieve the Target Profile.

4. ***Continuously monitor, communicate, and collaborate:*** In a reiterative process, continuously monitor and routinely assess your critical infrastructure asset's Current Profile against the business-defined Target Profile. Share information about the Target Profile with your executive sponsor, who can help transform progress toward the Target Profile into a business context. Use this business context to inform internal stakeholders, general counsel, internal audit functions, lines of business, and the board of directors, if necessary.

The potential benefits of adopting the NIST Cybersecurity Framework are many, but implementation may involve certain challenges.

Critical infrastructure owners and providers, for instance, may find it difficult to objectively assess their Implementation Tier. Doing so demands a holistic view of the entire risk ecosystem, as well as the ability to be truly objective. This may be difficult for critical infrastructure companies that segregate the management of their corporate back-office IT systems and networks from their operational technology (OT) assets and process control networks (PCN). These organizational silos can make it difficult for a single person to assess the entire connected enterprise, since doing so will demand an in-depth understanding of all IT and OT assets.

It may be more effective to seek assistance from a third party with deep experience across the risk ecosystem specific to your industry. An experienced third party can assess your enterprise from an independent viewpoint and provide an objective perspective of your organization and how it compares with others in your industry. Engaging a skilled third-party partner may help you more effectively and quickly design and implement an integrated cybersecurity program that realizes the goals of your target state.

## Cybersecurity leadership team

***David Burg***
Principal, US & Global Cybersecurity Leader
david.b.burg@us.pwc.com

***Michael Compton***
Principal, Cybersecurity Strategy & Operations
michael.d.compton@us.pwc.com

***Peter Harries***
Principal, Health Industries
peter.harries@us.pwc.com

***John Hunt***
Principal, Public Sector
john.d.hunt@us.pwc.com

***Mark Lobel***
Principal Technology, Entertainment,
Media & Communications
mark.a.lobel@us.pwc.com

***Gary Loveland***
Principal, Consumer and Industrial Products & Services
gary.loveland@us.pwc.com

***Joe Nocera***
Principal, Financial Services Industry
joseph.nocera@us.pwc.com

***Dave Roath***
Partner, Risk Assurance
david.roath@us.pwc.com

### Lead Author

**Jim Guinn, II**
Managing Director
jim.guinn@us.pwc.com