A board's guide to the NIST Cybersecurity Framework for better risk oversight

August 2022

pwc

pwc.com/cybersecurity

Many directors are concerned about their effectiveness in overseeing cybersecurity. We believe the NIST Cybersecurity Framework (commonly called “CSF”)[1] can be a particularly useful tool for boards. The CSF provides guidance on how directors can engage with company leadership around this critical issue. And, directors don’t need to read the CSF cover to cover. Instead, you can start with our primer.

Too often, business leaders assume that cybersecurity is only a technology issue. While it’s true that technology is an important component, many other disciplines need to be included. To manage cyber risk effectively, companies need a concerted effort that aligns risk management activities across functional areas: IT, security, risk, operations, legal, compliance, human resources, internal audit, marketing/PR and the executive team. Without this coordination, adverse events may quickly cascade into large-scale disruptions.

To enable these various functions to communicate effectively, companies need a common language that allows cyber risk discussions in non-technical, intuitive terms. Enter the NIST CSF. It provides a high-level framework for managing and improving a cybersecurity program. It also supports conversations between cyber risk stakeholders across the enterprise—up to and including the board of directors.

The CSF is rooted in security principles (not tactical security capabilities). It enables boards to focus on security while staying at the appropriate oversight level.

---

[1] US National Institute of Standards and Technology (NIST) Cybersecurity Framework, https://www.nist.gov/cyberframework

What is the NIST CSF, exactly?

Created by the US National Institute of Standards and Technology (NIST), the CSF is a structured collection of cyber risk fundamentals that can be used when discussing, prioritizing, and addressing key components of a cyber risk management program. It is by design a high-level, non-prescriptive tool for framing the important issues so stakeholders can speak a common language.

At the highest level, the CSF is organized into five "functions"—or key activities. Together these define a holistic approach to a company's cyber risk management:

- Identify – What matters most to our business and what are our biggest threats?
- Protect – What measures have we taken to ensure that key elements of our business are safe?
- Detect – How alert are we to threatening events or potential disruptions?
- Respond – How quickly and effectively can we react when bad things happen?
- Recover – Once we've experienced an attack or disruption, how quickly will we be able to resume normal operations?

Each of the five functions comprises a number of lower level activities that represent the tactics for mitigating cyber risk. Those activities are broken down as "categories" and "sub-categories," each providing a more granular and detailed description of leading practices. These activities can serve as a guide for a company's information security function.

The CSF is organized into five "functions"

Identify

Protect

Detect

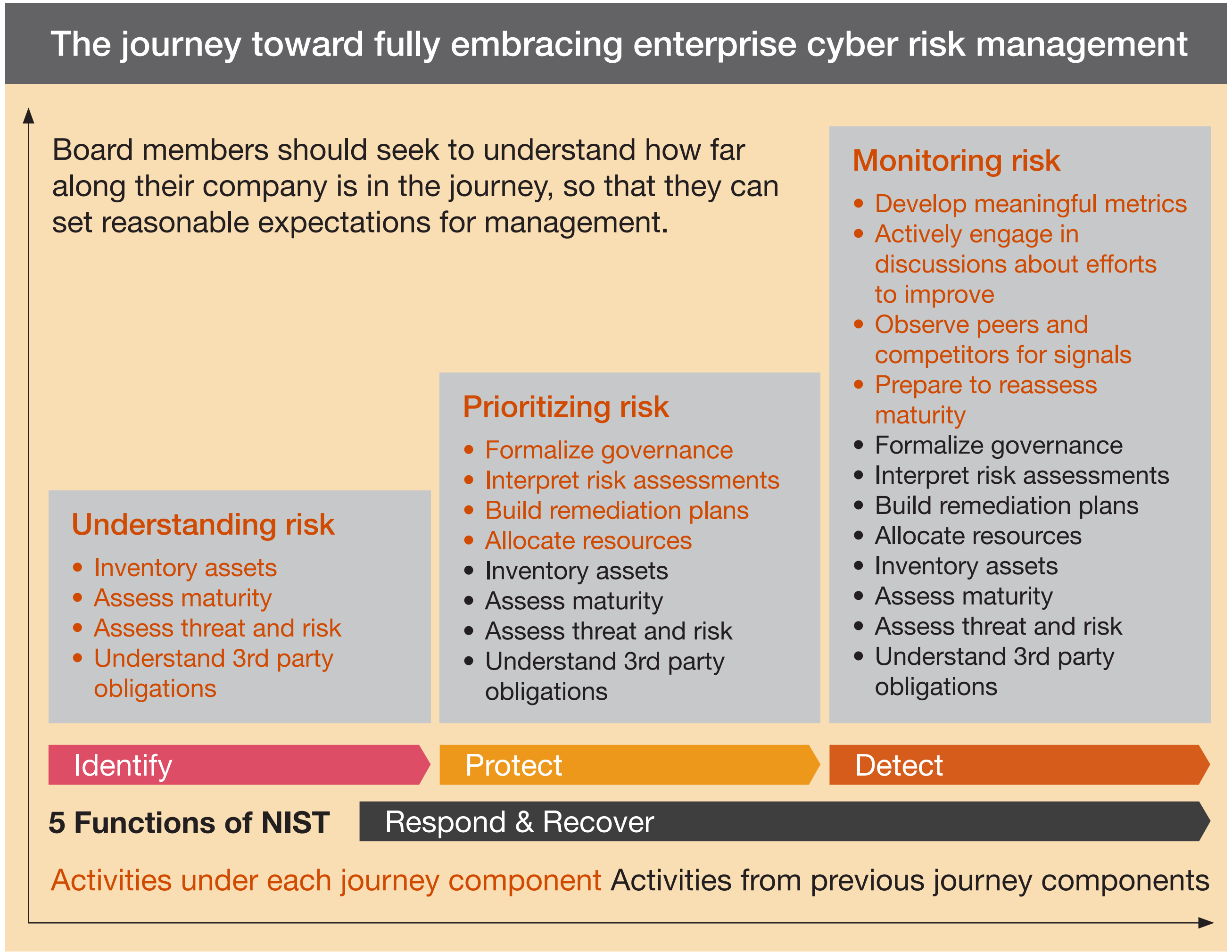
Respond

Recover

What does using the CSF mean for our company?

We view all companies as being on a journey to understand their cyber risk and address it appropriately. Directors should understand where their companies are in that journey, and expect to receive higher quality information as the journey progresses. The journey has three phases:

- Understanding risk – Companies assess what cyber risk really means for them, identifying the key assets that drive the business, and the nature of the threats they face.
- Prioritizing risk – Companies focus more precisely on the areas that matter most and make decisions based on those priorities.
- Monitoring risk – Companies develop the ability to know with increasing agility when changes in the technology or business environment or evolving threats change their risk exposure. For example, they may have implemented advanced capabilities for monitoring technology assets and deploying automated threat response. In other words, the five CSF functions—Identify, Protect, Detect, Respond and Recover—operating in harmony.



The journey toward fully embracing enterprise cyber risk management

Board members should seek to understand how far along their company is in the journey, so that they can set reasonable expectations for management.

Understanding risk

- Inventory assets
- Assess maturity
- Assess threat and risk
- Understand 3rd party obligations

Prioritizing risk

- Formalize governance
- Interpret risk assessments
- Build remediation plans
- Allocate resources
- Inventory assets
- Assess maturity
- Assess threat and risk
- Understand 3rd party obligations

Monitoring risk

- Develop meaningful metrics
- Actively engage in discussions about efforts to improve
- Observe peers and competitors for signals
- Prepare to reassess maturity
- Formalize governance
- Interpret risk assessments
- Build remediation plans
- Allocate resources
- Inventory assets
- Assess maturity
- Assess threat and risk
- Understand 3rd party obligations

5 Functions of NIST

Activities under each journey component Activities from previous journey components

The people, processes and technology that underpin these phases don't materialize overnight, but they can evolve when company and board leadership makes them a priority. Some companies are further along in their journey. For example, financial services firms have had to comply with stringent industry regulations, driving them to have more mature capabilities. Other companies are at earlier stages.

A company can also assess how well it is addressing cyber risk by using a maturity model, such as the widely accepted Capability Maturity Model Integration (CMMI)[2]. Such models allow companies to define current and target states for their security capability maturity, and measure their progress against their goals. A maturity model such as CMMI is a tool that can be used with NIST CSF to enable the development of maturity ratings. The ratings can enable companies to benchmark progress, internally and against their peers.

Once directors understand where their company is on the journey, they can discuss whether management's plans for the next six, twelve and twenty-four months are reasonable.

---

[2] Capability Maturity Model Integration (CMMI), https://cmmiinstitute.com/cmmi

How can our board take the first step?

The five functions of the NIST CSF each focus on key strategic questions. Directors can engage with executives and their risk and security leadership by framing questions to target these key strategic areas.

In the event the board needs an additional level of detail from management, directors can focus questions in categories or subcategories as needed.

A chief information security officer is likely to appreciate the structured nature of the conversation and could develop more impactful communication with the board as a result.

Here are some examples of questions to get the conversation started

Identify	Do we have adequate visibility into our business processes to identify where cyber controls are needed? Are we capable of managing cyber risks throughout their lifecycle?
Protect	Are we deploying adequate controls for protecting our environment from cyber threats and risks? Are we keeping our organization educated about cyber risks?
Detect	Are we capable of detecting rapidly evolving threats targeting our organization in a timely fashion?
Respond	Are we prepared to respond and limit the disruptive effects of cyber incidents through an organization-wide orchestrated approach?
Recover	Once we’ve experienced an attack how quickly will we be able to resume normal operations?

Conclusion and useful resources

While not a silver bullet, the principles outlined in the NIST CSF can help companies make basic cyber hygiene part of their muscle memory. Using it, they can develop robust cyber risk management that is more proactive than reactive.

Most importantly, the CSF provides a common language for all stakeholders. By understanding and leveraging the CSF, boards can play an active role engaging with security leadership and company leadership about the company's cybersecurity strategy and its effort to build cyber resiliency.

Resource links

NIST Cybersecurity Framework

From PwC:

Overseeing cyber risk: the board's role

Cybersecurity, Risk & Regulatory

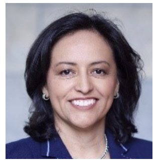
pwc.com/cybersecurity

How PwC can help

For more information about the topics in this publication, please contact any of the following individuals:

Sean Joyce
Global Cybersecurity and Privacy Leader
US Cyber, Risk and Regulatory Leader
sean.joyce@pwc.com

Matt Gorham
Leader, Cyber & Privacy Innovation Institute, PwC
matt.gorham@pwc.com



Maria Castañón Moats
Leader, Governance Insights Center
maria.castanon.moats@pwc.com

Barbara Berlin
Managing Director, Governance Insights Center
barbara.berlin@pwc.com

www.pwc.com/us/GovernanceInsightsCenter