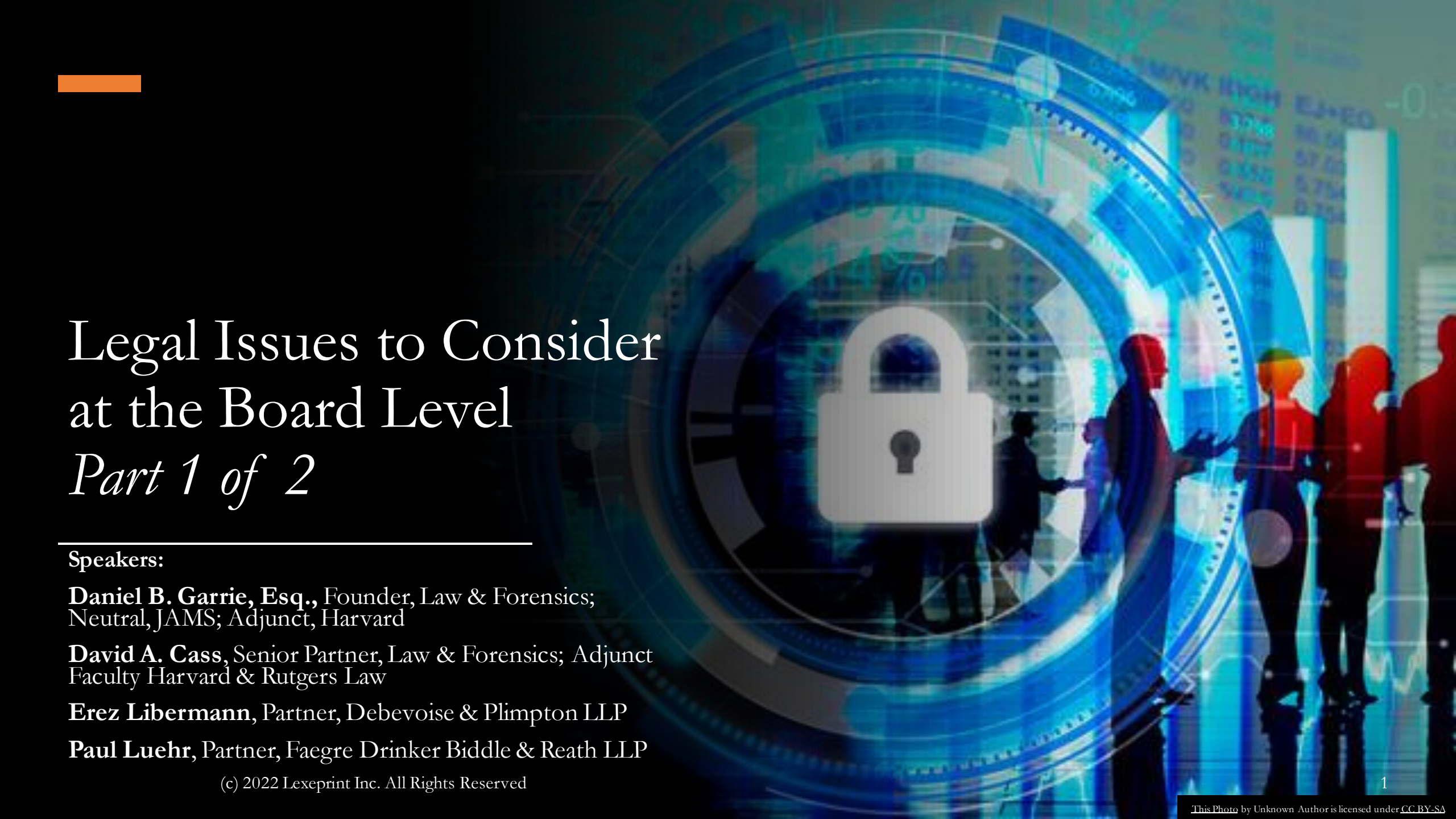


Legal Issues to Consider at the Board Level
Part 1 of 2

Speakers:

Daniel B. Garrie, Esq., Founder, Law & Forensics; Neutral, JAMS; Adjunct, Harvard

David A. Cass, Senior Partner, Law & Forensics; Adjunct Faculty Harvard & Rutgers Law

Erez Libermann, Partner, Debevoise & Plimpton LLP

Paul Luehr, Partner, Faegre Drinker Biddle & Reath LLP

(c) 2022 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA

Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2022 Lexeprint Inc. All Rights Reserved

Speakers



Daniel B. Garrie, Esq.
Founder, Law & Forensics
Neutral, JAMS
Adjunct, Harvard



David A. Cass
Senior Partner, Law & Forensics
Adjunct Faculty Harvard & Rutgers Law



Erez Libermann
Partner
Debevoise & Plimpton LLP



Paul Luehr
Partner
Faegre Drinker Biddle & Reath LLP

(c) 2022 Lexeprint Inc. All Rights Reserved



Agenda

Part 1:

- Cyber Risk Landscape
- Legal, Business, and Technical Issues to Consider at the Board Level
- Essential Questions for the Board

Part 2:

- SEC on Cybersecurity for the Board
- Cyber Risk Assessment

(c) 2022 Lexeprint Inc. All Rights Reserved



Cyber Risk Landscape

(c) 2022 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-ND

What is a data breach and cyber-attack?

- A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve Personally Identifiable Information (PII), trade secrets or intellectual property.

  *National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*

- A cyber-attack is a deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.

  **National Research Council*

(c) 2022 Lexeprint Inc. All Rights Reserved



Questions to consider when assessing threat of a data breach

- Threats – Who is attacking?
- Vulnerabilities – What weaknesses can be attacked?
- Impacts – What the attack does – what is the financial damage of any breach?

(c) 2022 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-NC

The act of protecting information and communications technology (ICT) systems and their contents has come to be known as cybersecurity

- A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It usually refers to one or more of three things:
- A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software and the information they contain and communicate, including software and data, as well as other elements of cyberspace.
- The state or quality of being protected from such threats.
- The broad field of endeavor aimed at implementing and improving those activities and quality.

(c) 2022 Lexeprint Inc. All Rights Reserved



What are some weapons?

- Social Engineering
- Unpatched Vulnerabilities
- Bypassing Security
- Denial of Service Attacks (DoS)
- Group Phishing
- Spear Phishing
- Viruses/Worms
- Trojan Horse
- Zero Day Exploit
- Website Exploit
- Spyware, Malware, Ransomware

(c) 2022 Lexeprint Inc. All Rights Reserved



Legal, Business, and Technical Issues to Consider at the Board Level

(c) 2022 Lexeprint Inc. All Rights Reserved



Board Duties

- Board duties generally fall within seven categories:
  - Governance
  - Strategy
  - Risk
  - Talent
  - Compliance
  - Culture
  - Insurance
- With respect to cybersecurity, the board's duties in each of these categories play a critical role in effective oversight of the cybersecurity program.

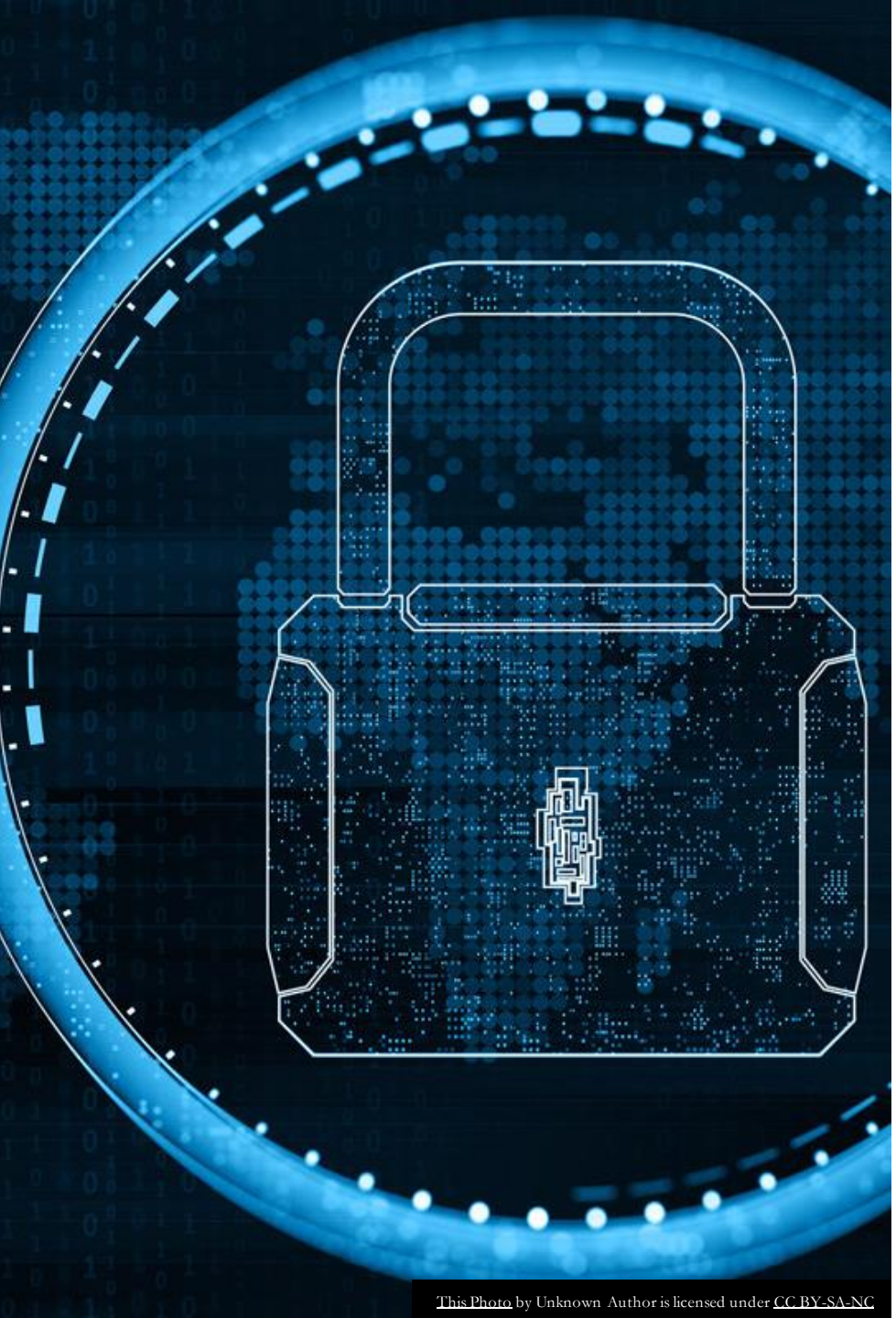
(c) 2022 Lexeprint Inc. All Rights Reserved



Cyber Risk Mitigation Model for the Board of Directors

- HR & Compliance
  - Provide training and education
- Business Units/Operations
  - Implement and drive conformance with the cyber strategy
- Government Affairs & Communications
  - Help shape policy (including crisis management plan) and assure good communications with regulations
- Finance
  - Assure maximum efficiencies with limited dollars
- Internal Audit & Compliance
  - Assure accountability and effective systems and controls

(c) 2022 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA-NC

Cyber Risk Mitigation Model for the Board of Directors

- Acquisitions & Growth
  - Adopt strategies to decrease risks in entering into new markets
- Procurement
  - Protect against third party intrusions
- Legal/Regulatory & Privacy
  - Assure compliance with applicable cyber and privacy laws
- IT & Security
  - Evaluate cyber risks and drive implementation of cyber strategy and ERM

(c) 2022 Lexeprint Inc. All Rights Reserved



Board Compliance

- In general, boards rely on the general counsel, internal audits and ERM, among other functions, to provide independent risk assessments and to confirm risk management processes are in place.
- For the foreseeable future, cyber risks are potentially more consequential than other enterprise-significant risks.

(c) 2022 Lexeprint Inc. All Rights Reserved



Board Compliance

- It is important that the general counsel, internal audits and ERM give cybersecurity a high priority. Boards should undertake regular, proactive discussions with these functions to ensure their leaders recognize that cyber risk is dynamic and requires continuous external screening for new forms of threat mitigation.
  - For example, internal audits can no longer focus solely on perimeter defense controls, without consideration of risk-based controls.
  - Likewise, ERM should monitor and screen externally new forms of cyber risks, with the awareness that some cyber risks are more qualitative and difficult to measure.

(c) 2022 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY

SEC on Board Responsibility

The SEC has stated:

- A director is expected to attend the Company's annual meeting of members. A director who is unable to attend any meeting (which it is understood will occur on occasion) is expected to notify the Chairman of the Board or the Chairman of the appropriate committee in advance of such meeting. In addition, directors are expected to act in the best interests of the Company, maintain independence and integrity, develop and maintain a sound understanding of the Company's strategies, industries and businesses, review management development and succession planning, endeavor to be available on reasonable notice, attend and prepare for meetings, and provide active, objective and constructive participation at meetings of the Board and its committees.

(c) 2022 Lexeprint Inc. All Rights Reserved



Potential impacts and possible implications for the board include:

- Loss of IP
- Regulatory Risk
- Reputational Risk
- Legal expenses

(c) 2022 Lexeprint Inc. All Rights Reserved



Essential Questions for the Board

(c) 2022 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA-NC



What to Ask Fellow Board Members?

- General Questions
  - Does your insurance cover the Board if there is a cyber - attack?
  - Does your insurance cover the C-Suite if there is a breach?
  - Is there a Board committee assigned to address cybersecurity?

(c) 2022 Lexeprint Inc. All Rights Reserved



What to Ask Fellow Board Members?

- Technology Specific Risks
  - Who has board ownership of the operational management of IT?
  - Are you confident that the organization has identified the key systems and information assets and assessed their vulnerability to attack?

(c) 2022 Lexeprint Inc. All Rights Reserved



What to Ask Fellow Board Members?

- Operational Cyber Risks
  - Do the outsourced providers and contractors have controls and policies in place and do they align with our company's expectations?
  - Is there a written security policy which is supported by regular testing and training?
  - Are you confident employees understand and follow this?

(c) 2022 Lexeprint Inc. All Rights Reserved



What to Ask the C-Suite?

- CISO and CIO
  - How confident are you that your organization's most important systems and information are being properly managed?
  - How confident are you they can withstand cyberattacks from internal and external actors?
  - Does your IT strategy adequately reflect cyber risk?

(c) 2022 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY-SA

What to Ask the C-Suite?

- CFO and General Counsel
  - Is legal involved in the incident response plan?
  - Do you know who your incident response vendor?
  - Do you know who your contact is with the federal and local law enforcement?
  - Have you identified your publication relations/crises management firm?
  - Do you have a law firm retained?
  - Does your company have cyber insurance?

(c) 2022 Lexeprint Inc. All Rights Reserved



What to Ask the C-Suite?

- Everyone
  - Do you have a full and accurate picture of the impact on your organization following a successful cyber-attack, from a financial perspective?
  - Do you have a full and accurate picture of the impact on your organization following a successful cyber-attack, from a operational perspective?
  - Do you have a full and accurate picture of the impact on your organization following a successful cyber-attack, from a reputational perspective?

(c) 2022 Lexeprint Inc. All Rights Reserved



Questions to Ask After a Breach

- How many breaches were there?
- How far did hackers get into the system?
- How quickly did management address or react to the breach?
- What were the results of penetration testing on third parties?

(c) 2022 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA

What to Consider When the CISO Presents Cyber Concerns

Updates from the chief information officer on information security and cyber threat intelligence that is both meaningful and actionable.

- **Identification**.
  Which are the top three to five threats that are most relevant to the organization?
- **Protection**.
  Which actions have been taken to mitigate these threats?
- **Detection**.
  What mechanisms are being used to detect incidents? What activity has been seen since the last report?
- **Response/Recovery.**
  How did the company respond to each incident?

(c) 2022 Lexeprint Inc. All Rights Reserved



(c) 2022 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC

Contact Us



Daniel B. Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



David Cass
Email: David@lawandforensics.com



Erez Libermann
Email: eliebermann@debevoise.com
URL:
https://www.debevoise.com/erezliebermann/?tab=biography



Paul Luehr
Email: paul.luehr@faegredrinker.com
URL:
https://www.faegredrinker.com/en/professionals/l/luehr-paul-h#tab-Overview

(c) 2022 Lexeprint Inc. All Rights Reserved



Daniel B. Garrie, Esq.
Law & Forensics LLC – Founder
JAMS – Neutral
Harvard – Adjunct
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybersecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, he successfully built and sold several technology start-up companies.

Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been awarded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack.IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2022 Lexeprint Inc. All Rights Reserved.



David Cass
Law & Forensics LLC – Senior Partner
Contact:
E: david@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

David Cass is a senior partner at Law & Forensics LLC where he leads the Cryptocurrency and Digital Banking Practice and is a member of the Cyber Security and Forensics Practice. He has extensive experience in financial services regulation, cryptocurrency, digital assets, blockchain, cloud, and digital banking.

He most recently served as a lead regulator for the Federal Reserve Bank of New York where he was a member of the Large Institution Supervision Committee (LISCC). Prior to this appointment, David was the CISO & Global Partner of IBM's Cloud Security Service Unit where he was responsible for its security practices, processes, and policies.

He has been an active contributor of the FS-ISAC and the European Banking Federation on Cloud Compliance and Security for financial services firms and has worked closely with US and international regulators. He was part of the team that introduced the first financial services blockchain initiative utilizing public cloud supported by 10 major international banks.

Previously, he served as SVP & CISO for Elsevier where he led an organization of experienced legal, risk, and security professionals who provided data protection, privacy, security, and risk management guidance on a global basis. He also served as Elsevier's HIPAA officer.

David has an MSE from the University of Pennsylvania, and an MBA from MIT. He is a frequent speaker at high-profile conferences and served on a public corporation's Board of Directors. He also is an editorial board member for The Journal of Law & Cyber Warfare and serves as a board member for the UCLA Extension Silicon Beach Innovation Lab. He is a faculty member for the non-profit Global Cyber Institute, and an adjunct faculty member for Harvard and at the Rutgers Law School. He is a member of the New York City Cyber Critical Services & Infrastructure team organized by the NYPD and the office of the NY District Attorney.

In his free time, David is a volunteer firefighter & Swiftwater Rescue Technician.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Erez Libermann
Debevoise & Plimpton LLP – Partner
Contact:
E: eliebermann@debevoise.com
URL: https://www.debevoise.com/erezliebermann/?tab=biography

Debevoise & Plimpton

Erez Liebermann is a litigation partner and a member of the firm's Data Strategy & Security Group. His practice focuses on advising major businesses on a wide range of complex, high-impact cyber-incident response matters and on data-related regulatory requirements.

With decades of experience in data issues as a litigator, federal prosecutor and senior in-house counsel at a global insurance company, Mr. Liebermann regularly advises clients at the C-suite and board level on building strategies to reduce their data-related regulatory and reputational risks, and on navigating high-profile government investigations following data incidents. He is also widely acknowledged as a leading cybersecurity and data privacy professional and is ranked among the leading lawyers by *Chambers USA* (2022), where clients note that he is "one of the most intelligent attorneys, [and] very practical and great to work with."

Prior to joining Debevoise, Mr. Liebermann co-chaired the U.S. cybersecurity and privacy practice of another international law firm where he advised companies on a broad range of data privacy and cybersecurity issues. Before that, Mr. Liebermann served as Chief Counsel of Cybersecurity & Privacy at Prudential, where he led the company's legal, regulatory and investigative matters on cyber, privacy, data science and artificial intelligence, including advising the company's senior management and board. In addition to his role as counsel, Mr. Liebermann built and managed Prudential's global technical incident response, threat intelligence and threat hunting team.

Before that, Mr. Liebermann spent 10 years investigating and prosecuting global cyber and white collar crimes as Deputy Chief of the Criminal Division of the U.S. Attorney's Office for the District of New Jersey. He also served as Chief of the Computer Hacking and Intellectual Property Section, and National Security Cyber Specialist where he led groundbreaking cyber prosecutions, including the largest credit card hacking case charged to date, *US v. Vladimir Drinkman et al.* , relating to hacks into 7-Eleven, JC Penney, Heartland Payment Systems, Hannaford Brothers, Visa, Jet Blue, and others. He also prosecuted a group of individuals for leading a stock pump and dump scheme facilitated by a global botnet. He received the Attorney General's Distinguished Service Award for the *Drinkman* prosecution.

Earlier in his career, Mr. Liebermann served as a law clerk to Chief Justice Deborah Portiz of the New Jersey Supreme Court and U.S. District Court Judge Faith Hochberg in Newark.

He is a frequent commentator on cyber and data privacy issues, and serves on the New York State Cybersecurity Advisory Board.

Mr. Liebermann received his J.D. from Columbia Law School in 1999 and his B.S. in aerospace engineering from the University of Virginia in 1996.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Paul Luehr
Faegre Drinker Biddle & Reath LLP – Partner
Contact:
E:paul.luehr@faegredrinker.com
URL: https://www.faegredrinker.com/en/professionals/l/luehr-paul-h#tab-Overview

Paul Luehr, CIPP/US, leads Faegre Drinker's cybersecurity practice and has spent over 25 years on the cutting edge of law and technology. He pioneered early digital investigations and led the first internet team at the Federal Trade Commission and prosecuted hackers, fraudsters, and terrorists as a prosecutor with the US Department of Justice. He then joined a global cybersecurity consulting firm and became the "go-to" professional for companies facing some of the largest data breaches on record.

Today, Paul works with clients on incident response, data governance, global privacy and security compliance, and M&A cyber due diligence. For each of the last five years (2018-22), the *Cybersecurity Docket* has named Paul to its annual list honoring the "nation's best and brightest data-breach-response attorneys." His insights have been featured on national and British television, National Public Radio, and in publications such as *Bloomberg*, *The Wall Street Journal* and *The New York Times*.

Paul is graduate of Harvard University and the UCLA School of Law.

(c) 2022 Lexeprint Inc. All Rights Reserved.

dentons.com

DENTONS

A cybersecurity guide for directors



By R. William "Bill" Ide III and Amanda Leech, Dentons Governance Center





A cybersecurity guide for directors

By R. William "Bill" Ide III and Amanda Leech, Dentons Governance Center[1]

With the ever-present reality of cybersecurity breaches, there has been a tendency in board governance literature to treat cybersecurity risks differently than other risks facing the organization. In practice, however, boards have long been tasked with protecting their companies from significant risks. While cybersecurity may appear to many board members to be a daunting new risk, the long-established "tried and true" board governance approach to risk oversight described herein works well and should be applied to cybersecurity risk.

Board duties generally fall within six categories: (i) governance, (ii) strategy, (iii) risk, (iv) talent, (v) compliance and (vi) culture. With respect to cybersecurity, the board's duties in each of these categories play a critical role in effective oversight of a company's cybersecurity program.

Every director should have a general understanding of cybersecurity risk and what it means for directors' oversight responsibilities. While the basic business-judgment obligations of directors are the same for this emerging area of risk, cybersecurity itself is a dynamic and complex subject. The purpose of this guide is to provide a "plain English" review that helps directors and senior managers carry out their cybersecurity oversight duties, including cyber strategy development and governance. Effective oversight in this area can mean the difference between "learning the hard way" and incurring significant damages, or successfully mitigating the damages that frequently accompany a significant breach.

While this guide is specific to boards of directors, the fiduciary principles of oversight apply to senior management as well. Senior management also delegates and oversees, but at a more granular level than boards. In the end, senior managers should also follow the principles of this guide to establish proper oversight, ensure that sufficient processes and controls are in place and assure their boards that cyber risks are identified and managed well.

Cybersecurity oversight: The role of the board

For company management and boards of directors, a record number of recent incursions—such as those at Target and Sony—demonstrate that cybersecurity risk is as significant as other critical strategic, operational, financial and compliance risks under boards' purviews.

Since the passage of the Sarbanes–Oxley Act of 2002, the Delaware courts have repeatedly broadened proactive duties of oversight for independent directors in areas of material impact on shareholder value such as risk, compliance and executive compensation. Just as boards are charged with overseeing a company's financial systems and controls, they also have a duty to oversee a company's management of cybersecurity, including oversight of appropriate risk mitigation strategies, systems, processes and controls.

Without effective oversight and accountability, an organization's cybersecurity governance systems, policies and procedures can be rendered meaningless, leaving the enterprise vulnerable to attack. In today's world of continually reported material data breaches, boards cannot claim lack of awareness as a defense against allegations of oversight failures. Regulators and shareholders are increasingly demanding more evidence of director attentiveness to cyber risk. As the Target breach demonstrated, breaches can result in calls for director removal. Even if directors are re-elected, the board and the company will likely face numerous shareholder derivative and class action lawsuits.

Cybersecurity governance

The first question for the board is: Who owns management of the cybersecurity risk at the board level and management level? Typically, boards delegate cybersecurity oversight to the audit committee—or to the risk committee if one is part of the board's governance structure—for a more concentrated review, with periodic reports to the full board. Others approach cybersecurity as a matter to be overseen by the full board. Company size, industry and existing board risk management structures will dictate the best approach. For the foreseeable future, cybersecurity will require considerable attention by boards working with management, internal audit, enterprise risk management (ERM) and cybersecurity experts as the threats continue to evolve and the total enterprise seeks to adjust. Processes, systems and controls must remain fluid for the foreseeable future.

At the management level, the CEO is ultimately accountable to the board for management of cybersecurity risk. Often, a CEO looks to business information technology (IT) or, in larger organizations, a chief information security officer (CISO) to interface with the board and hold accountability for cybersecurity risk management. This approach builds from a technology knowledge platform, but the major challenge is governance of the total enterprise requiring established management skills of communications, project management, behavioral science and command presence.

Technical solutions are one piece of managing the risk, but as the following chart shows, every function in the enterprise has a role to play. For success, each business unit must own and embrace cybersecurity as a priority. Tension between a decentralized business model and cybersecurity's desire for centralization requires high-level management attention to resolve conflicts. Decentralization favors local decision-making by each unit; on the other hand, cybersecurity must by its nature be centralized, and at times must seek to override those local decisions. Accordingly, IT or the CISO should report to a senior management member who can oversee the enterprise's cybersecurity program decision-making, and to whom the board can look as accountable for cybersecurity.

Cybersecurity strategy and risk oversight

Too often, IT presents boards with cybersecurity reports that are technical but lack an enterprise-wide strategic overlay. For effective oversight, boards should hold senior management accountable to ensure that a clear and concise cybersecurity strategy, understandable in nontechnical terms, is in place, along with systems and controls to monitor its implementation. This requires regular dialogue between the board and management, and the sharing of accurate and useful information, including metrics to track performance and provide accountability. Most importantly, a concise, high-level, "plain English" cybersecurity strategic plan must be agreed to by the board and senior management.

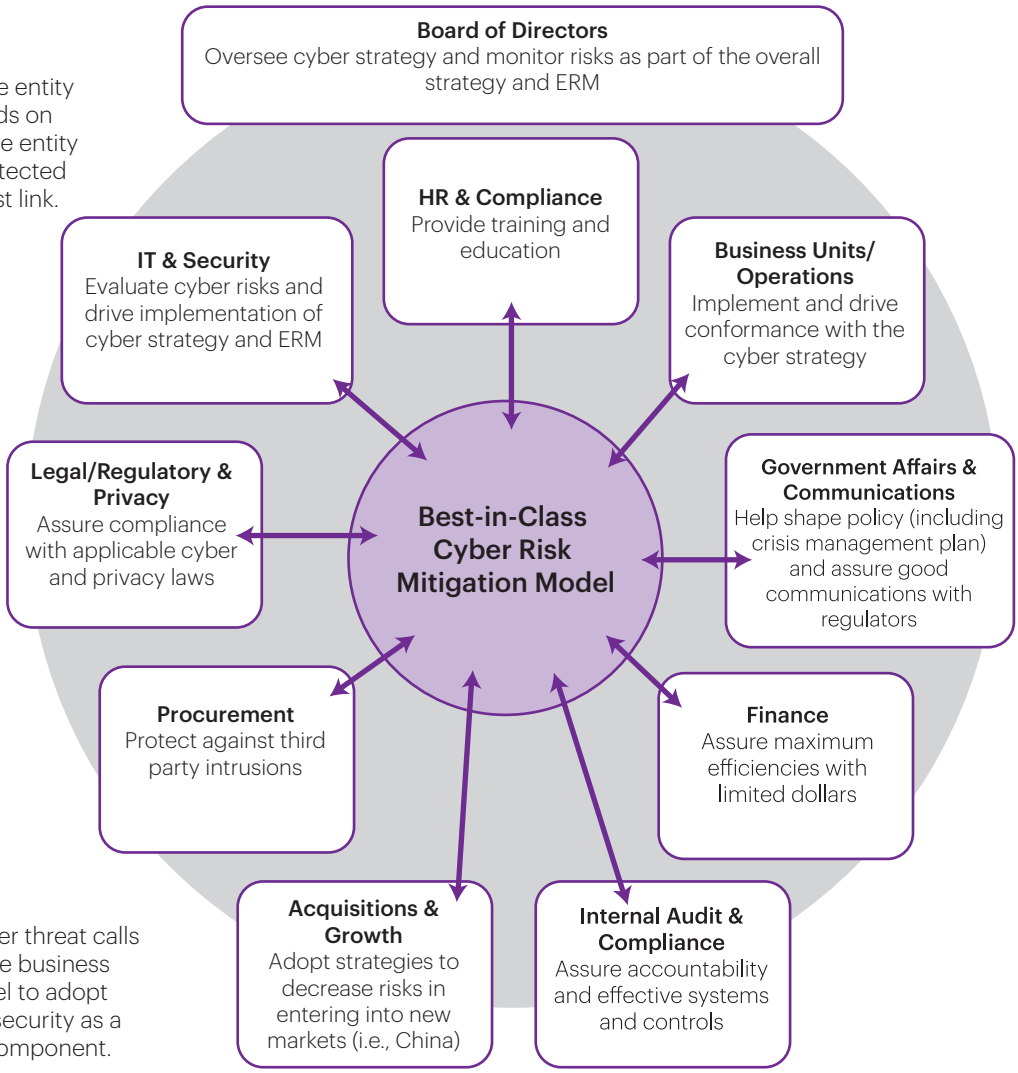
Risk-based strategy

Instead of a castle-and-moat, "keep the bad guys out" prevention-based approach, cybersecurity strategy has evolved to a risk-based approach. Because a perimeter defense cannot provide complete protection, the risk-based approach focuses instead on prioritizing and protecting identified "crown jewels" (for example, third-party information, intellectual property and critical process control networks). Risk-based defense includes detecting and responding before the additional protections around the "crown jewels" can be compromised, while also stopping intruders before they inflict other forms of disruptive and reputational damages, as in the Sony breach.

While perimeter defenses remain essential for deterring less sophisticated attacks, effective cyber strategies now allocate security resources around a company's information and processes, with additional layers of protection around the most valuable assets. Tomorrow, new technologies and techniques may require further shifts in strategies. Boards should regularly seek independent third-party reviews on strategic best practices for companies with a similar industry, size and risk profile.

Cybersecurity Governance Components

Success of the entity now depends on cyber – and the entity is only as protected as its weakest link.



The cyber threat calls for the business model to adopt cybersecurity as a key component.

These critical components all need to collaborate and be a part of the cybersecurity strategy.

Risk prioritization

This key part of strategy begins with the identification and prioritization of cyber risks. Cybersecurity resources are finite, so the strategy should focus on the most material cyber risks, considering the likelihood of harm if risks were realized. To facilitate this prioritization, many companies maintain a risk register of material cyber risks—a central repository for all risks identified by the company, including data, locations, access points, security devices and other related information. The risk prioritization process should precede the budget and resource allocation process to ensure alignment between resources and risks.

Ranking risks and determining which to accept, mitigate or transfer is a substantial undertaking. Its effectiveness depends on the quality of information and knowledge of individuals who make the recommendations. Board members must be assured that every function in the company has been solicited to contribute to the strategy's development. In particular, those with responsibility for law, privacy, physical security and crisis management response will need to offer integral input. Many industries will have specific regulatory concerns that must be woven into the strategy. As part of the risk prioritization process, senior management should provide detailed recommendations about the plan to the board, including identification of risks to be accepted, mitigated or transferred (through cyber insurance).

Strategy best practices and standards

Cyber risk has escalated so rapidly, and so publicly, that entities everywhere are scrambling to regain ground and keep up with the evolving cyber threat. Governments, regulators, industries, companies and thought leaders alike are looking for the right approach—or approaches—to address this complex and dynamic issue. So it's no surprise that cybersecurity strategy best practices, standards and public policies are still very fluid and multiplying rapidly.[1]

Today, it is unclear today what standards will become widely viewed as best practices, and whether those standards will vary by industry and/or company size. Boards and management should agree on the best approach for their company. For purposes of demonstration, let's assume that the standards defined below are the right approach in the present discussion.

In February 2014, in response to Executive Order 13636, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity, a set of industry standards and best practices for cybersecurity risk management.[2] The NIST Cybersecurity Framework was developed as a voluntary framework to reduce cyber risks to critical infrastructure, and incorporates globally accepted technical standards, guidelines and practices, including ISO 27001, ISA 62443 and COBIT 5, among others. The framework includes five functions that together can comprise the foundation of a cybersecurity risk strategy for any enterprise:

- Identify: Develop organizational understanding of the overall cyber risk context, including asset management (systems, data, hardware, devices, communication flows), business environment (prioritization of risks, objectives and activities) and governance (every part of the enterprise must know its role and be accountable). In other words, what are the cyber activities that could be harmed and in what ways?

- Protect: Deploy safeguards to prevent intrusions, including access control, awareness and training, data security, information protection processes, maintenance and protective technology.

- Detect: Enable timely discovery of a cybersecurity breach to limit the harm from intrusions through surveillance, detection of anomalies and events; continuous security monitoring; and detection processes.

- Respond: Implement plans and activities to contain any damage resulting from a cybersecurity breach through comprehensive crisis management incident response planning and implementation of tabletop exercises.

- Recover: Develop plans and activities to resume normal operations following a cybersecurity event, including post-event mitigation and lessons learned.

As an initial matter, the company should develop a detailed plan highlighting the gaps between current practices and best practices in each of the above functions, along with concrete steps for remediation. High priority should be given to implementing a robust incident response plan to minimize damages from breaches. In addition to any required remediation, the board should monitor the development of the complete cybersecurity strategy, beginning with risk prioritization, as well as the program's effectiveness. There are two major activities to monitor: (i) the build-out and installation of the strategic plan and (ii) the effectiveness of the plan. The utilization of dashboards to monitor the installation and effectiveness of the strategic plans is essential for meaningful board oversight of cybersecurity strategy.

Dashboards

With respect to cybersecurity, effective dashboards should be carefully tailored to meet the needs of the company and its board. As a result, creating a dashboard requires input from both management and the board. The general trend is a bifurcated approach, in which maturity and overall effectiveness are monitored by separate dashboards. Below are descriptions of both, as well as sample dashboards that can be modified to the particular dynamics of industries and size.

Maturity dashboards

The maturity dashboard presents metrics that depict the maturity of the company's cybersecurity program. At its most basic, this dashboard can simply be an assessment of the company's cybersecurity strategy with respect to the five NIST designed functions, detailed above. NIST recommends that, with respect to each function, a company determine the maturity of its program using the following terms: (i) partial, (ii) risk-informed, (iii) risk informed and repeatable or (iv) adaptive. For companies that have previously identified weaknesses and remediation efforts in its cybersecurity program, the maturity dashboard should also include metrics that allow the board to monitor the progress of the identified improvement efforts.

Sample maturity dashboard

- NIST assessment

Function	Target	Actual	Change
Identity			
Protect			
Detect			
Respond			
Recover			

**Actual state can be color coded. for example, red can be used if the target state has not been achieved; green can be used if the target state has been acheived.*

- Implementation of projects

Project	Projected Timeframe	On Track	Notes
1.			
2.			
3.			
4.			

**Additional rows should be added to table as needed.*
† The "on-track" column shuold include "yes" or "no." Again, the boxes can be color-coded for ease of review

- Summary of implementation challenges

Project	Item Number:
Summary of Challenges	
Proposed New Timeline:	# of Previous Extensions:

Effectiveness dashboards

In contrast to the maturity dashboard, the effectiveness dashboard provides metrics that allow the board to ascertain how effective the program is. It generally focus on threat assessment, threat detection, remediation metrics and recovery metrics. Some boards also request certain protection-related metrics when the program is maturing; however, as protection efforts become consistent, these metrics have limited usefulness. The effectiveness dashboard is most useful when it provides numerical metrics rather than high-level conclusory determinations based on underlying numbers not provided to the board.

Sample end-of-quarter effectiveness dashboard

- 1. Number of severe incidents: _____
- 2. Description of severe incident

Type of Incident		**Status: Resolved or Ongoing**
Description		
How Discovered:		
Time to Discovery:	**Time to Resolve:**	**Estimated Cost:**

** Table should be reproduced for each severe incident in the applicable time period. External incidents that suggest new forms of risk should also be reported with description of mitigation activities.*

- 3. Detection metrics

  Physical access controls – number of incidents: _____
  Environmental controls – number of incidents: _____

Item	Detected/Received	Resolved	Notes
Unauthorized User Accounts			
Unauthorized Devices			
Credential Theft			
Incidents Involving PPI			
Alerts from Security Service Provider			

4. Training metrics

Metric	End of Q1	End of Q2	End of Q3	End of Q4
Percent of New Hires Competing training w/in 30 days				
Percentage of Employees Current on Annual Awareness Training				

**Metrics should be included for cuirrent and at least two previous quarters to show trends.*

While it is management's responsibility to develop and implement the cybersecurity strategy, and boards should not micromanage, boards have an obligation to retain the prerogative to fully understand a company's risk exposures. In the event that a board finds itself in need of additional information about a particular issue, it can engage in a deep dive. Similarly, if a board observes a large number of stakeholders providing input on the same cybersecurity concern—or if management faces delays in implementing a particular aspect of the strategy—the board can use a deep dive to assure proper management of the identified risk area. While boards should generally stay focused on the macro and defer to management on the micro, as noted above, there are times when they should be more deeply involved in the tactics and implementation of strategy (for instance, in the event of a material cyber incident). On these occasions, especially, good communication and leadership are critical for maintaining trust between management and the board.

Talent

A major responsibility of a board is to ensure the company has the right talent to accomplish its goals. Selection, evaluation and compensation of the CEO is the major task. However, it is also important that the board ensures the right skills and experiences are brought to bear in managing something as vital to the organization as cybersecurity.

Following the departure of Target's CEO, much was made of the fact that the company did not have a CISO or a chief security officer (CSO).[4] A key area of board oversight is ensuring that the company's organizational structure is aligned behind its strategy, and that management has the skills and experience to execute the strategy.

Historically, the business IT function has primarily been a technology provider, charged with delivering top quality data, Internet connectivity, hardware, software and other technologies to business units. Many companies also allowed business units to use third-party technologies. Following decades in which entities have become totally dependent on IT for their flow of information, the cyber threat has now developed into something far more dangerous than previously anticipated. Nevertheless, many companies that relied on the IT function for cyber risk management continued to do so without considering that the threat has grown exponentially beyond just a question of technology.

As cyber threats have continued to escalate, it is increasingly unrealistic to expect that IT alone is able to provide adequate protection against cyber risks. These should be managed through the lens of the entire enterprise. History demonstrates that "viewing data breaches as a 'technical issue' is a recipe for failure."[5] While IT will likely always have a major role in cyber risk mitigation, there are significant differences in the skills and goals of the IT function and the information security function.

More and more enterprises are appointing a CISO to lead cybersecurity. While the CISO must honor and reinforce the business support mission of IT, his/her highest responsibility is prioritizing security measures to mitigate cyber risk. Further, the CISO must have a national security outlook, including awareness of "tail risks" and "black swans." It will be rare that a CISO will have the business operations, project management, communications and C-suite skills to eliminate the need of a senior management member overseeing the CISO for the CEO and the board.

Distinguishing responsibility between the delivery of IT and information security is an important governance step. Assuring cyber risk management throughout the full enterprise, beyond IT, raises other governance dynamics. The cyber threat involves information in the hands of suppliers and other third parties beyond the purview of IT, in which procurement and legal experts must be involved. Dealing with significant insider risks and pressures to compromise are also beyond the scope of IT. Further, limiting oversight to IT can restrict the budget, influence and authority required to manage cyber risk effectively, which places the whole company at greater risk.

The risk-reward considerations for cybersecurity management are so significant that senior management must be in charge of the process. In addition, "deferring responsibility to IT inhibits critical analysis and communication about security issues, and hampers the implementation of effective security strategies."[6] In the end, senior management must lead cyber risk decisions so the appropriate cybersecurity strategy can be effectively implemented and monitored throughout the enterprise, with effective oversight by the board.

In addition to the management skills and experiences needed to address cyber risk, an advocate is needed

to assure such skills and experience at the board level. As noted previously, cybersecurity is primarily a governance challenge beyond IT. A CEO whose company manages cybersecurity well would bring to valuable insights and experiences. The right IT technologist could be a positive contribution to a board, but for most companies that would not be necessary.

Compliance

In general, boards rely on the general counsel, internal audits and ERM, among other functions, to provide independent risk assessments and to confirm risk management processes are in place. For the foreseeable future, cyber risks are potentially more consequential than other enterprise-significant risks. It is important that the general counsel, internal audits and ERM give cybersecurity a high priority. Boards should undertake regular, proactive discussions with these functions to ensure their leaders recognize that cyber risk is dynamic and requires continuous external screening for new forms of threat mitigation. For example, internal audits can no longer focus solely on perimeter defense controls, without consideration of risk-based controls. Likewise, ERM should monitor and screen externally new forms of cyber risks, with the awareness that some cyber risks are more qualitative and difficult to measure.

Increasingly, cybersecurity is becoming more of a legal and regulatory area where the general counsel's lead on assuring disclosures, full understanding of legal risks and adequate crisis management plans will be critical.

For independent verification as to the status of the company's cybersecurity program, the board should strongly consider authorization of an ethical hacking program. Ethical hacking is designed to uncover vulnerabilities, and is conducted internally or by an external contractor. Few companies receive pristine reports from ethical hacking. While the greatest value from ethical hacking can be achieved by leveraging findings across the enterprise to remediate immediate security vulnerabilities, the activity also has important awareness-raising implications for internal audits, ERM and the board. Finally, internal auditors and the general counsel should periodically commission a third-party cybersecurity strategy and governance review to assure that the company is keeping pace with best practices and that the picture presented to the board is verified as accurate.

Culture

Cyber risks should be managed through the lens of the entire enterprise. Every employee has a role to play, and a top-down culture of cybersecurity is essential for containing and managing this evolving risk. Studies show that employee lapses are the major enablers of cyber intrusions. A strong culture of inspiration and accountability is the best preventive measure for threats from misinformed, inattentive or malicious employees. Peter Drucker said, "Culture eats strategy for breakfast."[7] He might have added that it feeds on policies, systems and controls which are only as effective as the culture of the organization in which they exist. With regard to cybersecurity, the culture either supports and reinforces policies, systems and controls, or it overrides and undermines them. It is essential that all employees—without exception—understand that everyone has an equally important role and obligation to protect the enterprise from cyber intrusions. They must feel empowered to so act.

Cybersecurity, like all major risks, requires a culture of accountability, collaboration and continuous education and training, with all efforts geared toward supporting the strategy and mitigating cyber risks. Creating that culture drives individual awareness and acceptance of the strategy, shared commitment to its implementation and, ultimately, cyber risk mitigation. All of this starts with a "tone at the top" from the board and senior management. For values and behavior to permeate through the organization, the highest levels of the enterprise must lead by example. If a board member or C-suite member is cavalier about passwords or phishing, that will soon be known throughout an organization. Cybersecurity requires all at the top to live in glass houses.

About the authors:



R. William (Bill) Ide, III, a partner at Dentons, chairs the advisory board to the Conference Board's Governance Center and serves as the general counsel and secretary of the EastWest Institute. Bill formerly served as senior vice president and general counsel of Monsanto Company. He was counsel to the United States Olympic Committee and president of the American Bar Association, and he previously served as a member of the board of directors of Albemarle Corporation and Popeyes Louisiana Kitchen, Inc.



Amanda K. Leech is a senior managing associate at Dentons. She focuses her practice on general corporate counseling of both privately held and public companies, focusing on mergers, acquisitions, joint ventures and strategic alliances. Amanda also counsels boards of directors on implementing corporate governance and compliance programs, and assists boards of directors with special independent review and investigations.

Endnotes:

[1] Bill Ide and Amanda Leech are Members of the Dentons Governance Center and the Guide is based upon their working with and service on public company boards. Dentons Governance Center colleagues Joseph Blanco and Crystal Clark made substantial contributions to this Guide.

[2] The International Organization for Standardization's ISO 27001 has been an international information security management standard since 2005. In 2011, the SEC issued interpretive guidance on companies' disclosure obligations regarding cybersecurity risks and material breaches, and has prioritized information sharing about cybersecurity practices and incidents. In 2014, the FTC asserted itself as the Federal government's principal cybersecurity regulator with a series of rules requiring employers to take "reasonable" cybersecurity measures. And in January 2015, the Obama Administration proposed new cybersecurity legislation to address online fraud and data breaches. Similar activities are taking place at the state level and in the Congress. While this is far from an exhaustive summary, as long as the cyber threat continues, it is reasonable to assume that legislators and regulators will continue to respond with new policy proposals.

[3] http://www.nist.gov/cyberframework/

[4] Brian Krebs, The Target Breach, By the Numbers, Krebs on Security, May 6, 2014, http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[5] Online Trust Alliance, 2014 Data Protection & Breach Readiness Guide 4 (2014).

[6] National Association of Corporate Directors, Cyber-Risk Oversight Handbook 7 (2014).

[7] Bill Aulet, Culture Eats Strategy For Breakfast, Techcrunch.com, April 12, 2014, http://techcrunch.com/2014/04/12/culture-eats-strategy-for-breakfast/

About Dentons

Dentons is a global law firm driven to provide a competitive edge in an increasingly complex and interconnected world. A top 20 firm on the Acritas 2014 Global Elite Brand Index, Dentons is committed to challenging the status quo in delivering consistent and uncompromising quality in new and inventive ways. Dentons' clients now benefit from 3,000 lawyers and professionals in more than 80 locations spanning 50-plus countries. With a legacy of legal experience that dates back to 1742 and builds on the strengths of our foundational firms—Salans, Fraser Milner Casgrain (FMC), SNR Denton and McKenna Long & Aldridge—the Firm serves the local, regional and global needs of private and public clients.

www.dentons.com.

DENTONS Know the way

dentons.com

© 2015 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates.
This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content.
Please see dentons.com for Legal Notices.

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

Note to Readers on the Update

Version 1.1 of this Cybersecurity Framework refines, clarifies, and enhances Version 1.0, which was issued in February 2014. It incorporates comments received on the two drafts of Version 1.1.

Version 1.1 is intended to be implemented by first-time and current Framework users. Current users should be able to implement Version 1.1 with minimal or no disruption; compatibility with Version 1.0 has been an explicit objective.

The following table summarizes the changes made between Version 1.0 and Version 1.1.

Table NTR-1 - Summary of changes between Framework Version 1.0 and Version 1.1.

Update	Description of Update
Clarified that terms like "compliance" can be confusing and mean something very different to various Framework stakeholders	Added clarity that the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. However, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing.
A new section on self-assessment	Added Section 4.0 *Self-Assessing Cybersecurity Risk with the Framework* to explain how the Framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.
Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes	An expanded Section 3.3 *Communicating Cybersecurity Requirements with Stakeholders* helps users better understand Cyber Supply Chain Risk Management (SCRM), while a new Section 3.4 Buying Decisions highlights use of the Framework in understanding risk associated with commercial off-the-shelf products and services. Additional Cyber SCRM criteria were added to the Implementation Tiers. Finally, a Supply Chain Risk Management Category, including multiple Subcategories, has been added to the Framework Core.
Refinements to better account for authentication, authorization, and identity proofing	The language of the Access Control Category has been refined to better account for authentication, authorization, and identity proofing. This included adding one Subcategory each for Authentication and Identity Proofing. Also, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.
Better explanation of the relationship between Implementation Tiers and Profiles	Added language to Section 3.2 *Establishing or Improving a Cybersecurity Program* on using Framework Tiers in Framework implementation. Added language to Framework Tiers to reflect integration of Framework considerations within organizational risk management programs. The Framework Tier concepts were also refined. Updated Figure 2.0 to include actions from the Framework Tiers.

Consideration of Coordinated Vulnerability Disclosure	A Subcategory related to the vulnerability disclosure lifecycle was added.

As with Version 1.0, Version 1.1 users are encouraged to customize the Framework to maximize individual organizational value.

Acknowledgements

This publication is the result of an ongoing collaborative effort involving industry, academia, and government. The National Institute of Standards and Technology (NIST) launched the project by convening private- and public-sector organizations and individuals in 2013. Published in 2014 and revised during 2017 and 2018, this *Framework for Improving Critical Infrastructure Cybersecurity* has relied upon eight public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with stakeholders from across all sectors of the United States along with many sectors from around the world.

The impetus to change Version 1.0 and the changes that appear in this Version 1.1 were based on:

- Feedback and frequently asked questions to NIST since release of Framework Version 1.0;
- 105 responses to the December 2015 request for information (RFI), *Views on the Framework for Improving Critical Infrastructure Cybersecurity*;
- Over 85 comments on a December 5, 2017 proposed second draft of Version 1.1;
- Over 120 comments on a January 10, 2017, proposed first draft Version 1.1; and
- Input from over 1,200 attendees at the 2016 and 2017 Framework workshops.

In addition, NIST previously released Version 1.0 of the Cybersecurity Framework with a companion document, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*. This Roadmap highlighted key "areas of improvement" for further development, alignment, and collaboration. Through private and public-sector efforts, some areas of improvement have advanced enough to be included in this Framework Version 1.1.

NIST acknowledges and thanks all of those who have contributed to this Framework.

Executive Summary

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To better address these risks, the Cybersecurity Enhancement Act of 2014[1] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" (February 2013), and provided guidance for future Framework evolution. The Framework that was developed under EO 13636, and continues to evolve according to CEA, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the

[1] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with the private sector and government agencies at all levels. As the Framework is put into greater practice, additional lessons learned will be integrated into future versions. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Expanded and more effective use and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing evolving guidance for individual organizations while increasing the cybersecurity posture of the Nation's critical infrastructure and the broader economy and society.

Table of Contents

Note to Readers on the Update ii
Acknowledgements iv
Executive Summary v
1.0 Framework Introduction 1
2.0 Framework Basics 6
3.0 How to Use the Framework 13
4.0 Self-Assessing Cybersecurity Risk with the Framework 20
Appendix A: Framework Core 22
Appendix B: Glossary 45
Appendix C: Acronyms 48

List of Figures

Figure 1: Framework Core Structure 6
Figure 2: Notional Information and Decision Flows within an Organization 12
Figure 3: Cyber Supply Chain Relationships 17

List of Tables

Table 1: Function and Category Unique Identifiers 23
Table 2: Framework Core 24
Table 3: Framework Glossary 45

1.0 Framework Introduction

The United States depends on the reliable functioning of its critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To strengthen the resilience of this infrastructure, the Cybersecurity Enhancement Act of 2014[2] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to "facilitate and support the development of" cybersecurity risk frameworks. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued in February 2013[3], and provided guidance for future Framework evolution.

Critical infrastructure[4] is defined in the U.S. Patriot Act of 2001[5] as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). This reliance on technology, communication, and interconnectivity has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as technology and the data it produces and processes are increasingly used to deliver critical services and support business/mission decisions, the potential impacts of a cybersecurity incident on an

[2] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] The Department of Homeland Security (DHS) Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors

[5] See 42 U.S.C. § 5195c(e)). The U.S. Patriot Act of 2001 (H.R.3162) became public law 107-56 on October 26, 2001 and may be found at: https://www.congress.gov/bill/107th-congress/house-bill/3162

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

organization, the health and safety of individuals, the environment, communities, and the broader economy and society should be considered.

To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required. Because each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization's approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

The Framework remains effective and supports technical innovation because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

While the Framework has been developed to improve cybersecurity risk management as it relates to critical infrastructure, it can be used by organizations in any sector of the economy or society. It is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. The common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.
- *Framework Implementation Tiers* ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the

characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

- A ***Framework Profile*** ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO)

31000:2009[6], ISO/International Electrotechnical Commission (IEC) 27005:2011[7], NIST Special Publication (SP) 800-39[8], and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline[9].

1.3 Document Overview

The remainder of this document contains the following sections and appendices:

- Section 2 describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- Section 3 presents examples of how the Framework can be used.
- Section 4 describes how to use the Framework for self-assessing and demonstrating cybersecurity through measurements.
- Appendix A presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- Appendix B contains a glossary of selected terms.
- Appendix C lists acronyms used in this document.

[6] International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[9] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

2.1 Framework Core

The *Framework Core* provides a set of activities to achieve specific cybersecurity *outcomes*, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in **Figure 1**:

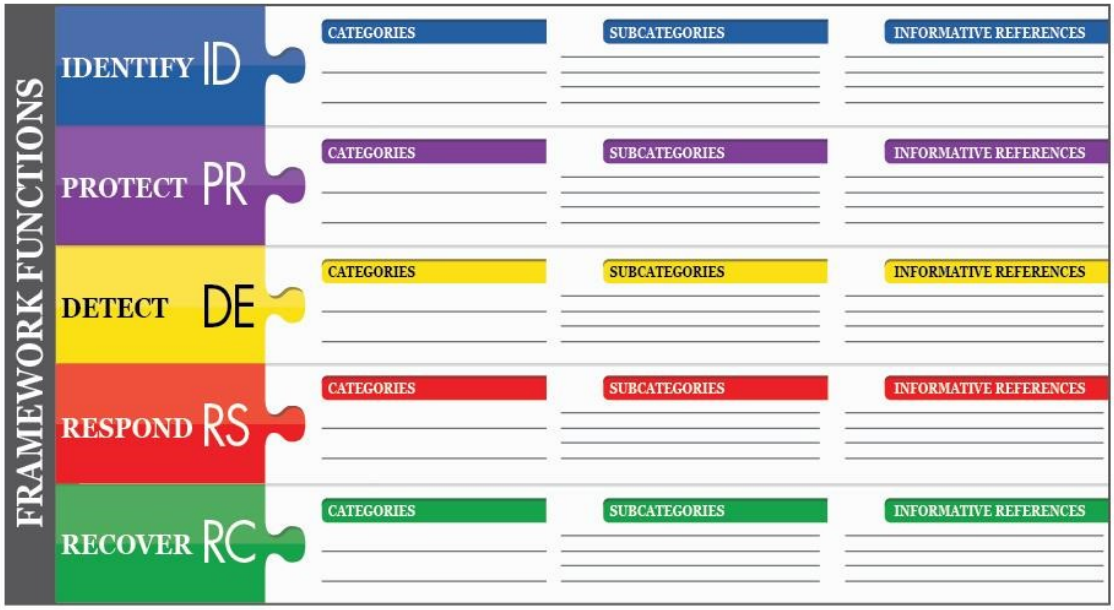


Figure 1: Framework Core Structure

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes."
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See Appendix A for the complete Framework Core listing.

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

  The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

2.2 Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

Successful implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination. Still, Tier selection and designation naturally affect Framework Profiles. The Tier recommendation by Business/Process Level managers, as approved by the Senior Executive Level, will help set the overall tone for how cybersecurity risk will be managed within the organization, and should influence prioritization within a Target Profile and assessments of progress in addressing gaps.

The Tier definitions are as follows:

Tier 1: Partial

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

Tier 2: Risk Informed

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

Tier 3: Repeatable

- *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

2.3 Framework Profile

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations. This Framework does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory can contribute to the roadmap described above. Prioritizing the mitigation of gaps is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. Furthermore, the Framework is a risk-based approach where the applicability and fulfillment of a given Subcategory is subject to the Profile's scope.

2.4 Coordination of Framework Implementation

Figure 2 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

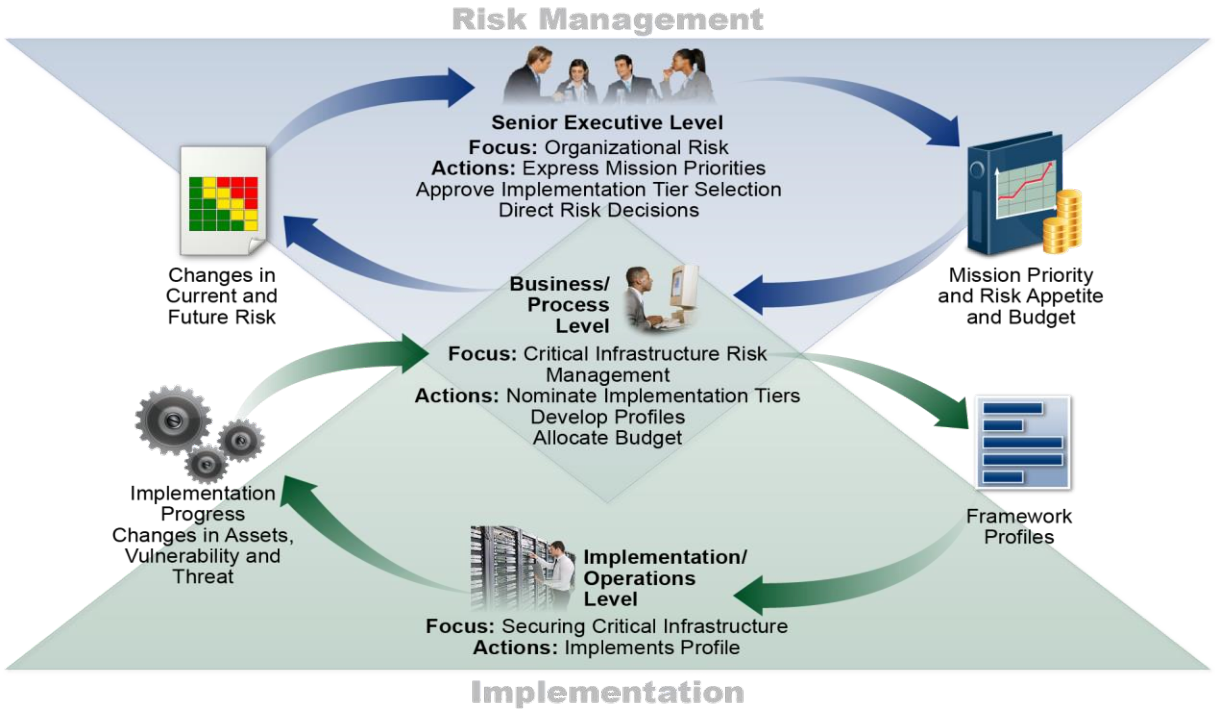


Figure 2: Notional Information and Decision Flows within an Organization

3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The Framework can be applied throughout the life cycle phases of plan, design, build/buy, deploy, operate, and decommission. The plan phase begins the cycle of any system and lays the groundwork for everything that follows. Overarching cybersecurity considerations should be declared and described as clearly as possible. The plan should recognize that those considerations and requirements are likely to evolve during the remainder of the life cycle. The design phase should account for cybersecurity requirements as a part of a larger multi-disciplinary systems engineering process.[10] A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as captured in a Framework Profile. The desired cybersecurity outcomes prioritized in a Target Profile should be incorporated when a) developing the system during the build phase and b) purchasing or outsourcing the system during the buy phase. That same Target Profile serves as a list of system cybersecurity features that should be assessed when deploying the system to verify all features are implemented. The cybersecurity outcomes determined by using the Framework then should serve as a basis for ongoing operation of the system. This includes occasional reassessment, capturing results in a Current Profile, to verify that cybersecurity requirements are still fulfilled. Typically, a complex web of dependencies (e.g., compensating and common controls) among systems means the outcomes documented in Target Profiles of related systems should be carefully considered as systems are decommissioned.

The following sections present different ways in which organizations can use the Framework.

3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization's current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired

[10] NIST Special Publication 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016 (updated March 21, 2018), https://doi.org/10.6028/NIST.SP.800-160v1

outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and

Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

3.3 Communicating Cybersecurity Requirements with Stakeholders

The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services. Examples include:

- An organization may use a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.
- An organization can better manage cybersecurity risk among stakeholders by assessing their position in the critical infrastructure and the broader digital economy using Implementation Tiers.

Communication is especially important among stakeholders up and down supply chains. Supply chains are complex, globally distributed, and interconnected sets of resources and processes

between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.[11]

Cyber SCRM is the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber SCRM addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization.

A primary objective of cyber SCRM is to identify, assess, and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain[12]." Cyber SCRM activities may include:

- Determining cybersecurity requirements for suppliers,
- Enacting cybersecurity requirements through formal agreement (e.g., contracts),
- Communicating to suppliers how those cybersecurity requirements will be verified and validated,
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies, and
- Governing and managing the above activities.

As depicted in Figure 3, cyber SCRM encompasses technology suppliers and buyers, as well as non-technology suppliers and buyers, where technology is minimally composed of information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). Figure 3 depicts an organization at a single point in time. However, through the normal course of business operations, most organizations will be both an upstream supplier and downstream buyer in relation to other organizations or end users.

[11] Communicating Cybersecurity Requirements (Section 3.3) and Buying Decisions (Section 3.4) address only two uses of the Framework for cyber SCRM and are not intended to address cyber SCRM comprehensively.

[12] NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161

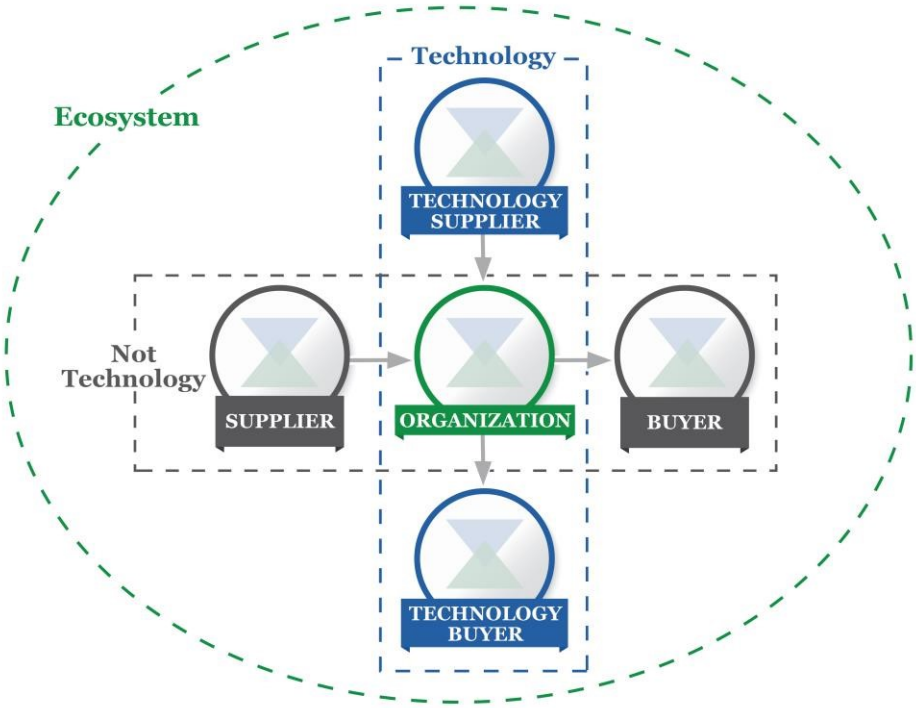


Figure 3: Cyber Supply Chain Relationships

The parties described in Figure 3 comprise an organization's cybersecurity ecosystem. These relationships highlight the crucial role of cyber SCRM in addressing cybersecurity risk in critical infrastructure and the broader digital economy. These relationships, the products and services they provide, and the risks they present should be identified and factored into the protective and detective capabilities of organizations, as well as their response and recovery protocols.

In the figure above, "Buyer" refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations. "Supplier" encompasses upstream product and service providers that are used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

Whether considering individual Subcategories of the Core or the comprehensive considerations of a Profile, the Framework offers organizations and their partners a method to help ensure the new product or service meets critical security outcomes. By first selecting outcomes that are relevant to the context (e.g., transmission of Personally Identifiable Information (PII), mission critical service delivery, data verification services, product or service integrity) the organization then can evaluate partners against those criteria. For example, if a system is being purchased that will monitor Operational Technology (OT) for anomalous network communication, availability may be a particularly important cybersecurity objective to achieve and should drive a Technology Supplier evaluation against applicable Subcategories (e.g., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

3.4 Buying Decisions

Since a Framework Target Profile is a prioritized list of organizational cybersecurity requirements, Target Profiles can be used to inform decisions about buying products and services. This transaction varies from Communicating Cybersecurity Requirements with Stakeholders (addressed in Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier. The objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements. Often, this means some degree of trade-off, comparing multiple products or services with known gaps to the Target Profile.

Once a product or service is purchased, the Profile also can be used to track and address residual cybersecurity risk. For example, if the service or product purchased did not meet all the objectives described in the Target Profile, the organization can address the residual risk through other management actions. The Profile also provides the organization a method for assessing if the product meets cybersecurity outcomes through periodic review and testing mechanisms.

3.5 Identifying Opportunities for New or Revised Informative References

The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

3.6 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology to address individual privacy and civil liberties implications that may result from cybersecurity. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program engender privacy and civil liberties considerations. Technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and cybersecurity have a strong connection. An organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed. Some examples include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; and cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including some types of incident detection or monitoring that may inhibit freedom of expression or association.

The government and its agents have a responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or its agents that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.

To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in Appendix A, the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

Governance of cybersecurity risk

- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program.
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained.
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.
- Process is in place to assess implementation of the above organizational measures and controls.

Approaches to identifying, authenticating, and authorizing individuals to access organizational assets and systems

- Steps are taken to identify and address the privacy implications of identity management and access control measures to the extent that they involve collection, disclosure, or use of personal information.

Awareness and training measures

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities.
- Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies.

Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization's anomalous activity detection and cybersecurity monitoring.

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities.
- Process is in place to conduct a privacy review of an organization's cybersecurity mitigation efforts.

4.0 Self-Assessing Cybersecurity Risk with the Framework

The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives. Ideally, organizations using the Framework will be able to measure and assign values to their risk *along with* the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be.

Over time, self-assessment and measurement should improve decision making about investment priorities. For example, measuring – or at least robustly characterizing – aspects of an organization's cybersecurity state and trends over time can enable that organization to understand and convey meaningful risk information to dependents, suppliers, buyers, and other parties. An organization can accomplish this internally or by seeking a third-party assessment. If done properly and with an appreciation of limitations, these measurements can provide a basis for strong trusted relationships, both inside and outside of an organization.

To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are implemented and managed. While measurements of all those items is beyond the scope of the Framework, the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities in the following ways:

- Making choices about how different portions of the cybersecurity operation should influence the selection of Target Implementation Tiers,
- Evaluating the organization's approach to cybersecurity risk management by determining Current Implementation Tiers,
- Prioritizing cybersecurity outcomes by developing Target Profiles,
- Determining the degree to which specific cybersecurity steps achieve desired cybersecurity outcomes by assessing Current Profiles, and
- Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References.

The development of cybersecurity performance metrics is evolving. Organizations should be thoughtful, creative, and careful about the ways in which they employ measurements to optimize use, while avoiding reliance on artificial indicators of current state and progress in improving cybersecurity risk management. Judging cyber risk requires discipline and should be revisited periodically. Any time measurements are employed as part of the Framework process, organizations are encouraged to clearly identify and know why these measurements are important and how they will contribute to the overall management of cybersecurity risk. They also should be clear about the limitations of measurements that are used.

For example, tracking security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. Verifying achievement of some organizational objectives requires analyzing the data only *after* that objective was to have been achieved. This type of lagging measure is more

absolute. However, it is often more valuable to predict whether a cybersecurity risk *may* occur, and the impact it *might* have, using a leading measure.

Organizations are encouraged to innovate and customize how they incorporate measurements into their application of the Framework with a full appreciation of their usefulness and limitations.

Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material, including Informative References, relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: Framework Core

Function	Category	Subcategory	Informative
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI **ISA 62443-2-1:2009** 4.2.3 **ISA 62443-3-3:2013** SR 7 **ISO/IEC 27001:2013** A.8 **NIST SP 800-53 Rev. 4** C
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI **ISA 62443-2-1:2009** 4.2.3 **ISA 62443-3-3:2013** SR 7 **ISO/IEC 27001:2013** A.8 **NIST SP 800-53 Rev. 4** C
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, AP **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, AP BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3 **ISO/IEC 27001:2013** A.8 **NIST SP 800-53 Rev. 4** C
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, AP DSS06.03

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
		third-party stakeholders (e.g., suppliers, customers, partners) are established	**ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** C
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, AP APO10.03, APO10.04, AI **ISO/IEC 27001:2013** A.1 A.15.1.3, A.15.2.1, A.15.2 **NIST SP 800-53 Rev. 4** C
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, AP **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** P
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, AP **ISA 62443-2-1:2009** 4.2.2 **NIST SP 800-53 Rev. 4** P
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BA **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** BAI03.02, DSS **ISO/IEC 27001:2013** A.1 A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** C 14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**CIS CSC** 19 **COBIT 5** APO01.03, AP EDM01.02 **ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.5 **NIST SP 800-53 Rev. 4** - security control families

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
	management of cybersecurity risk.	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**CIS CSC** 19 **COBIT 5** APO01.02, AP DSS05.04 **ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4**
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**CIS CSC** 19 **COBIT 5** BAI02.01, ME **ISA 62443-2-1:2009** 4.4.3 **ISO/IEC 27001:2013** A. A.18.1.3, A.18.1.4, A.18. **NIST SP 800-53 Rev. 4** - security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**COBIT 5** EDM03.02, AP DSS04.02 **ISA 62443-2-1:2009** 4.2.3 4.2.3.9, 4.2.3.11, 4.3.2.4.3 **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** S 9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, AP APO12.04, DSS05.01, DS **ISA 62443-2-1:2009** 4.2.3 4.2.3.12 **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** C 3, RA-5, SA-5, SA-11, SI
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** S

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
		ID.RA-3: Threats, both internal and external, are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, AP APO12.04 **ISA 62443-2-1:2009** 4.2. **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** F 16
		ID.RA-4: Potential business impacts and likelihoods are identified	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2. **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** F 9, PM-11
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** F
		ID.RA-6: Risk responses are identified and prioritized	**CIS CSC** 4 **COBIT 5** APO12.05, AP **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** F
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO12.04, AP BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3. **ISO/IEC 27001:2013** Cla Clause 9.3 **NIST SP 800-53 Rev. 4** F
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3. **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** F

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** S 11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, AP APO12.05, APO13.02, B BAI04.02 **ISA 62443-2-1:2009** 4.3. **ISO/IEC 27001:2013** A. A.15.1.3, A.15.2.1, A.15. **NIST SP 800-53 Rev. 4** S
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, AP APO10.05, APO12.01, A APO12.04, APO12.05, A BAI02.03 **ISA 62443-2-1:2009** 4.2. 4.2.3.4, 4.2.3.6, 4.2.3.8, 4. 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** 14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	**COBIT 5** APO10.01, AP APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3. **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** S 9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**COBIT 5** APO10.01, AP APO10.05, MEA01.01, M MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3. **ISA 62443-3-3:2013** SR **ISO/IEC 27001:2013** A.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			NIST SP 800-53 Rev. 4 A 16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2 **ISA 62443-3-3:2013** SR 2 7.3, SR 7.4 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C IR-6, IR-8, IR-9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS **ISA 62443-2-1:2009** 4.3.3 **ISA 62443-3-3:2013** SR 1 1.4, SR 1.5, SR 1.7, SR 1. **ISO/IEC 27001:2013** A.9 A.9.2.4, A.9.2.6, A.9.3.1, **NIST SP 800-53 Rev. 4** A IA-3, IA-4, IA-5, IA-6, IA IA-11
		PR.AC-2: Physical access to assets is managed and protected	**COBIT 5** DSS01.04, DSS **ISA 62443-2-1:2009** 4.3.3 **ISO/IEC 27001:2013** A.1 A.11.1.3, A.11.1.4, A.11.1 A.11.2.3, A.11.2.5, A.11.2 **NIST SP 800-53 Rev. 4** P PE-6, PE-8
		PR.AC-3: Remote access is managed	**CIS CSC** 12 **COBIT 5** APO13.01, DS **ISA 62443-2-1:2009** 4.3.3 **ISA 62443-3-3:2013** SR 1 **ISO/IEC 27001:2013** A.6 A.13.1.1, A.13.2.1

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			NIST SP 800-53 Rev. 4 A AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**CIS CSC** 3, 5, 12, 14, 15, **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3. **ISA 62443-3-3:2013** SR 2 **ISO/IEC 27001:2013** A.6 A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** A 5, AC-6, AC-14, AC-16, A
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS **ISA 62443-2-1:2009** 4.3. **ISA 62443-3-3:2013** SR 3 **ISO/IEC 27001:2013** A.1 A.13.2.1, A.14.1.2, A.14.1 **NIST SP 800-53 Rev. 4** A
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS DSS06.03 **ISA 62443-2-1:2009** 4.3. 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A. **NIST SP 800-53 Rev. 4** A 16, AC-19, AC-24, IA-1, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS **ISA 62443-2-1:2009** 4.3. 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6 4.3.3.6.9

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			ISA 62443-3-3:2013 SR 1.7, SR 1.8, SR 1.9, SR 1. **ISO/IEC 27001:2013** A.9 A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** A 11, AC-12, AC-14, IA-1, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BA **ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.7 **NIST SP 800-53 Rev. 4** A
		PR.AT-2: Privileged users understand their roles and responsibilities	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DS **ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** A
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03, AP APO10.05 **ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** F
		PR.AT-4: Senior executives understand their roles and responsibilities	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, AP **ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** A
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2 **ISO/IEC 27001:2013** A.6

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			NIST SP 800-53 Rev. 4 A
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BA DSS04.07, DSS05.03, DS **ISA 62443-3-3:2013** SR 3 **ISO/IEC 27001:2013** A.8 **NIST SP 800-53 Rev. 4** M
		PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DS **ISA 62443-3-3:2013** SR 3 4.2 **ISO/IEC 27001:2013** A.8 A.13.2.3, A.14.1.2, A.14.1 **NIST SP 800-53 Rev. 4** S
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3 **ISA 62443-3-3:2013** SR 4 **ISO/IEC 27001:2013** A.8 A.8.3.3, A.11.2.5, A.11.2. **NIST SP 800-53 Rev. 4** C
		PR.DS-4: Adequate capacity to ensure availability is maintained	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BA **ISA 62443-3-3:2013** SR 7 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A
		PR.DS-5: Protections against data leaks are implemented	**CIS CSC** 13 **COBIT 5** APO01.06, DS DSS06.02 **ISA 62443-3-3:2013** SR 5 **ISO/IEC 27001:2013** A.6 A.7.3.1, A.8.2.2, A.8.2.3, A.9.4.1, A.9.4.4, A.9.4.5,

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			A.11.1.5, A.11.2.1, A.13.1 A.13.2.3, A.13.2.4, A.14.1 **NIST SP 800-53 Rev. 4** A 19, PS-3, PS-6, SC-7, SC-
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BA **ISA 62443-3-3:2013** SR 3 3.8 **ISO/IEC 27001:2013** A.1 A.14.1.2, A.14.1.3, A.14.2 **NIST SP 800-53 Rev. 4** S
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** S
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI BAI10.05 **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 7 **ISO/IEC 27001:2013** A.1 A.12.6.2, A.14.2.2, A.14.2 **NIST SP 800-53 Rev. 4** C 5, CM-6, CM-7, CM-9, SA
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**CIS CSC** 18 **COBIT 5** APO13.01, BA BAI03.03 **ISA 62443-2-1:2009** 4.3.4

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			ISO/IEC 27001:2013 A.6 A.14.2.5 **NIST SP 800-53 Rev. 4** SA-10, SA-11, SA-12, SA 13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 7 **ISO/IEC 27001:2013** A.1 A.12.6.2, A.14.2.2, A.14.2 **NIST SP 800-53 Rev. 4** C
		PR.IP-4: Backups of information are conducted, maintained, and tested	**CIS CSC** 10 **COBIT 5** APO13.01, DS **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 7 **ISO/IEC 27001:2013** A.1 A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** C
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**COBIT 5** DSS01.04, DSS **ISA 62443-2-1:2009** 4.3.3 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.1 A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** P 14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	**COBIT 5** BAI09.03, DSS **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 4 **ISO/IEC 27001:2013** A.8 A.11.2.7 **NIST SP 800-53 Rev. 4** M

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
		PR.IP-7: Protection processes are improved	**COBIT 5** APO11.06, AP **ISA 62443-2-1:2009** 4.4. 4.4.3.4, 4.4.3.5, 4.4.3.6, 4. **ISO/IEC 27001:2013** A. 10 **NIST SP 800-53 Rev. 4** C PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	**COBIT 5** BAI08.04, DSS **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** A
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**CIS CSC** 19 **COBIT 5** APO12.06, DS **ISA 62443-2-1:2009** 4.3. **ISO/IEC 27001:2013** A. A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** C 13, IR-7, IR-8, IR-9, PE-1
		PR.IP-10: Response and recovery plans are tested	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3. **ISA 62443-3-3:2013** SR 3 **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** C
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, AP APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3. **ISO/IEC 27001:2013** A. A.7.2.2, A.7.2.3, A.7.3.1, **NIST SP 800-53 Rev. 4** P PS-5, PS-6, PS-7, PS-8, S

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
		PR.IP-12: A vulnerability management plan is developed and implemented	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS **ISO/IEC 27001:2013** A. A.16.1.3, A.18.2.2, A.18. **NIST SP 800-53 Rev. 4**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	**COBIT 5** BAI03.10, BAI DSS01.05 **ISA 62443-2-1:2009** 4.3. **ISO/IEC 27001:2013** A. A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** M MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3. 4.3.3.6.8 **ISO/IEC 27001:2013** A. **NIST SP 800-53 Rev. 4** M
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**CIS CSC** 1, 3, 5, 6, 14, 1 **COBIT 5** APO11.04, BA DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3. 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A. A.12.4.3, A.12.4.4, A.12. **NIST SP 800-53 Rev. 4** A
		PR.PT-2: Removable media is protected and its use restricted according to policy	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DS **ISA 62443-3-3:2013** SR **ISO/IEC 27001:2013** A. A.8.3.1, A.8.3.3, A.11.2.9

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			NIST SP 800-53 Rev. 4 M 5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DS **ISA 62443-2-1:2009** 4.3. 4.3.3.5.4, 4.3.3.5.5, 4.3.3. 4.3.3.6.1, 4.3.3.6.2, 4.3.3. 4.3.3.6.6, 4.3.3.6.7, 4.3.3. 4.3.3.7.2, 4.3.3.7.3, 4.3.3. **ISA 62443-3-3:2013** SR 1.4, SR 1.5, SR 1.6, SR 1. 1.10, SR 1.11, SR 1.12, S SR 2.3, SR 2.4, SR 2.5, S **ISO/IEC 27001:2013** A.9 **NIST SP 800-53 Rev. 4** A
		PR.PT-4: Communications and control networks are protected	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, AP **ISA 62443-3-3:2013** SR 4.1, SR 4.3, SR 5.1, SR 5. **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A CP-8, SC-7, SC-19, SC-2 SC-24, SC-25, SC-29, SC 38, SC-39, SC-40, SC-41,
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	**COBIT 5** BAI04.01, BAI BAI04.04, BAI04.05, DS **ISA 62443-2-1:2009** 4.3. **ISA 62443-3-3:2013** SR **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C 13, PL-8, SA-14, SC-6
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected	**DE.AE-1:** A baseline of network operations and expected data flows for	**CIS CSC** 1, 4, 6, 12, 13, **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
	and the potential impact of events is understood.	users and systems is established and managed	**ISO/IEC 27001:2013** A.1 A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** A
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 2 2.11, SR 2.12, SR 3.9, SR **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	**CIS CSC** 1, 3, 4, 5, 6, 7, 8 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A IR-8, SI-4
		DE.AE-4: Impact of events is determined	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DS **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
		DE.AE-5: Incident alert thresholds are established	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DS **ISA 62443-2-1:2009** 4.2.3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** I
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**CIS CSC** 1, 7, 8, 12, 13, **COBIT 5** DSS01.03, DSS **ISA 62443-3-3:2013** SR 6 **NIST SP 800-53 Rev. 4** A 3, SC-5, SC-7, SI-4

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
	the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events	**COBIT 5** DSS01.04, DSS **ISA 62443-2-1:2009** 4.3.3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** S
		DE.CM-5: Unauthorized mobile code is detected	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** S
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**COBIT 5** APO07.06, APO **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**CIS CSC** 1, 2, 3, 5, 9, 12, **COBIT 5** DSS05.02, DSS **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A CM-8, PE-3, PE-6, PE-20
		DE.CM-8: Vulnerability scans are performed	**CIS CSC** 4, 20

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			COBIT 5 BAI03.10, DSS **ISA 62443-2-1:2009** 4.2.3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** F
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**CIS CSC** 19 **COBIT 5** APO01.02, DS **ISA 62443-2-1:2009** 4.4.3 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** C
		DE.DP-2: Detection activities comply with all applicable requirements	**COBIT 5** DSS06.01, ME **ISA 62443-2-1:2009** 4.4.3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A 18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	**COBIT 5** APO13.02, DS **ISA 62443-2-1:2009** 4.4.3 **ISA 62443-3-3:2013** SR 3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C SI-4, PM-14
		DE.DP-4: Event detection information is communicated	**CIS CSC** 19 **COBIT 5** APO08.04, AP **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 6 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A 5, SI-4
		DE.DP-5: Detection processes are continuously improved	**COBIT 5** APO11.06, AP **ISA 62443-2-1:2009** 4.4.3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4**, C 5, SI-4, PM-14

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BA **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**CIS CSC** 19 **COBIT 5** EDM03.02, AP **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** C
		RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** A
		RS.CO-3: Information is shared consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.1 16.1.2 **NIST SP 800-53 Rev. 4** C IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** C
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6 **NIST SP 800-53 Rev. 4** S

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 6 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS **ISA 62443-3-3:2013** SR 2 2.11, SR 2.12, SR 3.9, SR **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** A
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DS **NIST SP 800-53 Rev. 4** S
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4 **ISA 62443-3-3:2013** SR 5 **ISO/IEC 27001:2013** A.1

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
			NIST SP 800-53 Rev. 4 I
		RS.MI-2: Incidents are mitigated	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** I
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
		RS.IM-2: Response strategies are updated	**COBIT 5** BAI01.13, DSS **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**CIS CSC** 10 **COBIT 5** APO12.06, DS **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**COBIT 5** APO12.06, BA **ISA 62443-2-1:2009** 4.4.3 **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C
		RC.IM-2: Recovery strategies are updated	**COBIT 5** APO12.06, BA **ISO/IEC 27001:2013** A.1 **NIST SP 800-53 Rev. 4** C

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Function	Category	Subcategory	Informative
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6
		RC.CO-2: Reputation is repaired after an incident	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Cla
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Cla **NIST SP 800-53 Rev. 4** C

Information regarding Informative References described in Appendix A may be found at the following locations

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pag
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.0 *for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Syste* https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=11678
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management syste* https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls fo Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.602 Informative References are only mapped to the control level, though any control enhancement might be f achieving a subcategory outcome.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References a definitively determine whether the specified sections in the Informative References provide the desired Subcateg

Informative References are not exhaustive, in that not every element (e.g., control, requirement) of a given Infor mapped to Framework Core Subcategories.

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Appendix B: Glossary

This appendix defines selected terms used in the publication.

Table 3: Framework Glossary

Buyer	The people or organizations that consume a given product or service.
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.

Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the "Data-in-transit is protected" Subcategory of the "Data Security" Category in the "Protect" function.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."

Supplier	Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.
Taxonomy	A scheme of classification.

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

ANSI	American National Standards Institute
CEA	Cybersecurity Enhancement Act of 2014
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical Systems
CSC	Critical Security Control
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCRM	Supply Chain Risk Management
SP	Special Publication