

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.01 [Draft 2](#)

National Institute of Standards and Technology

~~February 12, 2014~~
[Revised December 5, 2017](#)

Note to Reviewers on the Update and Next Steps

Version 1.1 Draft 2 of Cybersecurity Framework refines, clarifies, and enhances Version 1.0 issued in February 2014. It incorporates comments received on Version 1.1 Draft 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.

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

The impetus to change Version 1.0 and the proposed changes 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*; and
- Comments by approximately 800 attendees at a workshop on April 6-7, 2016.

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 draft Framework Version 1.1.

This Version 1.1 Draft 2 was prompted and informed by:

- Over 120 comments on a January 10, 2017, proposed first draft Version 1.1; and
- Comments and discussion by approximately 500 attendees at a workshop held on May 16-17, 2017.

Beyond key refinements, clarifications, and enhancements from the first draft, revisions in this draft include:

Update	Description of Update
<u>Clarifications and revisions to cybersecurity measurement language</u>	<u>Revised and retitled Section 4.0 to emphasize the correlation of business results to cybersecurity risk management. This section now highlights the multiple uses of measurement, with an emphasis on the role of measurements in self-assessment. The new title is <i>Self-Assessing Cybersecurity Risk with the Framework</i>.</u>
<u>Clarification of the use of the Framework to manage cybersecurity within supply chains</u>	<u>Refined Section 3.3 <i>Communicating Cybersecurity Requirements with Stakeholders</i> to help users better understand managing cybersecurity within supply chains and to incorporate that information into the External Participation property of Implementation Tiers.</u>
<u>Refinements to better account for authorization, authentication, and identity proofing</u>	<u>Added a Subcategory to address authentication and some language refinements were made within the Identity Management and Access Control Category.</u>
<u>Consideration of Coordinated Vulnerability Disclosure</u>	<u>A Subcategory related to the vulnerability disclosure lifecycle was added.</u>

<u>Removal of Federal Alignment Section</u>	<u>With publication of U.S. Federal policy, memorandum, and guidance (e.g., Executive Order 13800, OMB Memorandum M-17-25, and the draft NIST Interagency Report 8170) on Cybersecurity Framework use, federal applicability statements are no longer needed in the Framework publication.</u>
---	--

26 A more detailed review of Version 1.1 refinements, clarifications, and enhancements can be
27 found in Appendix D.

28 NIST is seeking public comment on this Framework Version 1.1 Draft 2, specifically regarding
29 the following:

- 30 • Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity
31 ecosystem (threats, vulnerabilities, risks, practices, technological approaches), including
32 those developments in the Roadmap items?
- 33 • For those using Version 1.0, would the proposed changes affect their current use of the
34 Framework? If so, how?
- 35 • For those not currently using Version 1.0, would the proposed changes affect their
36 decision about using the Framework? If so, how?

37 Feedback and comments should be directed to cyberframework@nist.gov. After reviewing
38 public comments regarding the Version 1.1 Draft 2, NIST intends to publish a final Framework
39 Version 1.1 in early calendar year 2018.

40

41 **Table of Contents**

42 [Note to Reviewers on the Update and Next Steps](#) ii

43 [Executive Summary](#) 1

44 [1.0 Framework Introduction](#) 3

45 [2.0 Framework Basics](#)..... 8

46 [3.0 How to Use the Framework](#)..... 18

47 [4.0 Self-Assessing Cybersecurity Risk with the Framework](#)..... 26

48 [Appendix A: Framework Core](#)..... 28

49 [Appendix B: Glossary](#)..... 53

50 [Appendix C: Acronyms](#) 56

51 [Appendix D: Revisions and Updates](#) 57

52 [Note to Reviewers on the Update and Next Steps](#) ii

53 [Executive Summary](#) 1

54 [1.0 Framework Introduction](#) 3

55 [2.0 Framework Basics](#)..... 7

56 [3.0 How to Use the Framework](#)..... 14

57 [4.0 Self-Assessing Cybersecurity Risk with the Framework](#)..... 21

58 [Appendix A: Framework Core](#)..... 23

59 [Appendix B: Glossary](#)..... 46

60 [Appendix C: Acronyms](#) 49

61 [Appendix D: Revisions and Updates](#) 50

62 **List of Figures**

63 [Figure 1: Framework Core Structure](#) 9

64 [Figure 2: Notional Information and Decision Flows within an Organization](#) 17

65 [Figure 3: Cyber Supply Chain Relationships](#)..... 22

66 [Figure 1: Framework Core Structure](#) 7

67 [Figure 2: Notional Information and Decision Flows within an Organization](#) 13

68 [Figure 3: Cyber Supply Chain Relationships](#)..... 17

69 **List of Tables**

70 [Table 1: Function and Category Unique Identifiers](#) 29

71	Table 2: Framework Core	30
72	Table 3: Framework Glossary	53
73	Table 4: Changes in Framework Version 1.1	57
74	Table 1: Function and Category Unique Identifiers	24
75	Table 2: Framework Core	25
76	Table 3: Framework Glossary	46
77	Table 4: Changes in Framework Version 1.1	50

78

Executive Summary

79 The national and economic security of the United States depends on the reliable functioning of
80 critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of
81 critical infrastructure systems, placing the Nation’s security, economy, and public safety and
82 health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company’s
83 bottom line. It can drive up costs and ~~impact~~affect revenue. It can harm an organization’s ability
84 to innovate and to gain and maintain customers.

85

86 ~~To better address these risks, the President issued Executive Order 13636, “Improving Critical~~
87 ~~Infrastructure Cybersecurity,” on February 12, 2013, which established that “[i]t is the Policy of~~
88 ~~the United States to enhance the security and resilience of the Nation’s critical infrastructure and~~
89 ~~to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity~~
90 ~~while promoting safety, security, business confidentiality, privacy, and civil liberties.” In~~
91 ~~enacting this policy, the Executive Order calls for the development of a voluntary risk-based~~
92 ~~Cybersecurity Framework—a set of industry standards and best practices to help organizations~~
93 ~~manage cybersecurity risks. The resulting Framework, created through collaboration between~~
94 ~~government and the private sector,~~To better address these risks, the Cybersecurity Enhancement
95 Act of 2014¹ (CEA) statutorily updated the role of the National Institute of Standards and
96 Technology (NIST) to include identifying and developing cybersecurity risk frameworks for
97 voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify
98 “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including
99 information security measures and controls that may be voluntarily adopted by owners and
100 operators of critical infrastructure to help them identify, assess, and manage cyber risks.” This
101 formalized NIST’s previous work developing Framework version 1.0 under Executive Order
102 13636, “Improving Critical Infrastructure Cybersecurity” (February 2013), and provided
103 guidance for future Framework evolution. The Framework that was developed under EO 13636
104 and continues to evolve according to CEA uses a common language to address and manage
105 cybersecurity risk in a cost-effective way based on business needs without placing additional
106 regulatory requirements on businesses.

107 The Framework focuses on using business drivers to guide cybersecurity activities and
108 considering cybersecurity risks as part of the organization’s risk management processes. The
109 Framework consists of three parts: the Framework Core, the Framework Profile, and the
110 Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities,
111 outcomes, and informative references that are common across sectors and critical infrastructure
112 sectors, providing. Elements of the Core provide detailed guidance for developing individual
113 organizational Profiles. Through use of ~~the~~ Profiles, the Framework will help ~~the~~an organization
114 to align and prioritize its cybersecurity activities with its business requirements, risk tolerances,
115 and resources. The Tiers provide a mechanism for organizations to view and understand the

¹See 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>.

116 characteristics of their approach to managing cybersecurity risk, which will help in prioritizing
117 and achieving cybersecurity objectives.

118 ~~The Executive Order also requires that the Framework include a methodology to protect~~
119 ~~individual privacy and civil liberties when critical infrastructure organizations conduct~~
120 ~~cybersecurity activities. While processes and existing needs will differ, the Framework can assist~~
121 ~~organizations in incorporating privacy and civil liberties as part of a comprehensive~~
122 ~~cybersecurity program.~~

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

128 The Framework provides a common organization and structure to today’s multiple approaches to
129 cybersecurity by assembling standards, guidelines, and practices that are working effectively ~~in~~
130 ~~industry~~ today. Moreover, because it references globally recognized standards for cybersecurity,
131 the Framework can ~~also be used by organizations located outside the United States and can~~ serve
132 as a model for international cooperation on strengthening critical infrastructure cybersecurity.

133 The Framework offers a flexible way to address cybersecurity, including cybersecurity’s effect
134 on physical, cyber, and people domains. It is applicable to organizations relying on technology,
135 whether their cybersecurity focus is primarily on information technology (IT), industrial control
136 systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including
137 the Internet of Things (IoT). Applied to the people domain, the Framework can assist
138 organizations in addressing cybersecurity as it affects the privacy of customers, employees, and
139 other parties.

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

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

152 Expanded and more effective use and sharing of best practices of this voluntary Framework isare
153 the next steps to improve the cybersecurity of our Nation’s critical infrastructure – providing
154 evolving guidance for individual organizations, while increasing the cybersecurity posture of the
155 Nation’s critical infrastructure ~~as a whole~~ and the broader economy and society.

156 1.0 Framework Introduction

157 The national and economic security of the United States depends on the reliable functioning of
158 its critical infrastructure. To strengthen the resilience of this infrastructure, President Obama
159 issued Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity,” on
160 February 12, 2013. This Executive Order calls for the Cybersecurity Enhancement Act of 2014²
161 (CEA) statutorily updated the role of the National Institute of Standards and Technology (NIST)
162 to “facilitate and support the development of a voluntary Cybersecurity Framework
163 (“Framework”) that provides a “” cybersecurity risk frameworks. Through CEA, NIST must
164 identify “a prioritized, flexible, repeatable, performance-based, and cost-effective approach” to
165 manage cybersecurity risk for those processes, including information, and systems directly
166 involved in the delivery security measures and controls that may be voluntarily adopted by
167 owners and operators of critical infrastructure services. The Framework, developed in
168 collaboration with industry, provides to help them identify, assess, and manage cyber risks.” This
169 formalized NIST’s previous work developing Framework version 1.0 under Executive Order
170 13636, “Improving Critical Infrastructure Cybersecurity,” issued in February 2013³, and
171 provided guidance to an organization on managing cybersecurity risk, for future Framework
172 evolution.

173 Critical infrastructure⁴ is defined in the EO U.S. Patriot Act of 2001⁵ as “systems and assets,
174 whether physical or virtual, so vital to the United States that the incapacity or destruction of such
175 systems and assets would have a debilitating impact on security, national economic security,
176 national public health or safety, or any combination of those matters.” Due to the increasing
177 pressures from external and internal threats, organizations responsible for critical infrastructure
178 need to have a consistent and iterative approach to identifying, assessing, and managing
179 cybersecurity risk. This approach is necessary regardless of an organization’s size, threat
180 exposure, or cybersecurity sophistication today.

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

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 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>

191 and safety of individuals, ~~and~~ the environment, communities, and the broader economy and
192 society should be considered.

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

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

206 ~~To ensure extensibility~~ The Framework remains effective and enables support technical innovation,
207 ~~the Framework because it~~ is technology neutral. ~~The Framework relies on, while also referencing~~
208 a variety of existing standards, guidelines, and practices ~~to enable critical infrastructure providers~~
209 ~~to achieve resilience~~ that evolve with technology. By relying on those global standards,
210 guidelines, and practices developed, managed, and updated by industry, the tools and methods
211 available to achieve the Framework outcomes will scale across borders, acknowledge the global
212 nature of cybersecurity risks, and evolve with technological advances and business requirements.
213 The use of existing and emerging standards will enable economies of scale and drive the
214 development of effective products, services, and practices that meet identified market needs.
215 Market competition also promotes faster diffusion of these technologies and practices and
216 realization of many benefits by the stakeholders in these sectors.

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

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

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

230 ~~Just as the Framework is not industry-specific, the~~ While the Framework has been developed to
231 improve cybersecurity risk management as it relates to critical infrastructure, it can be used by
232 organizations in any sector of the economy or society. It is intended to be useful to companies,

233 [government agencies, and not-for-profit organizations regardless of their focus or size. The](#)
234 common taxonomy of standards, guidelines, and practices that it provides also is not country-
235 specific. Organizations outside the United States may also use the Framework to strengthen their
236 own cybersecurity efforts, and the Framework can contribute to developing a common language
237 for international cooperation on critical infrastructure cybersecurity.

238 **1.1 Overview of the Framework**

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

- 243 • The [Framework Core](#) is a set of cybersecurity activities, desired outcomes, and
244 applicable references that are common across critical infrastructure sectors. The Core
245 presents industry standards, guidelines, and practices in a manner that allows for
246 communication of cybersecurity activities and outcomes across the organization from the
247 executive level to the implementation/operations level. The Framework Core consists of
248 five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.
249 When considered together, these Functions provide a high-level, strategic view of the
250 lifecycle of an organization’s management of cybersecurity risk. The Framework Core
251 then identifies underlying key Categories and Subcategories for each Function, and
252 matches them with example Informative References such as existing standards,
253 guidelines, and practices for each Subcategory.
- 254 • [Framework Implementation Tiers](#) (“Tiers”) provide context on how an organization
255 views cybersecurity risk and the processes in place to manage that risk. Tiers describe the
256 degree to which an organization’s cybersecurity risk management practices exhibit the
257 characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and
258 adaptive). The Tiers characterize an organization’s practices over a range, from Partial
259 (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive
260 responses to approaches that are agile and risk-informed. During the Tier selection
261 process, an organization should consider its current risk management practices, threat
262 environment, legal and regulatory requirements, business/mission objectives, and
263 organizational constraints.
- 264 • A [Framework Profile](#) (“Profile”) represents the outcomes based on business needs that an
265 organization has selected from the Framework Categories and Subcategories. The Profile
266 can be characterized as the alignment of standards, guidelines, and practices to the
267 Framework Core in a particular implementation scenario. Profiles can be used to identify
268 opportunities for improving cybersecurity posture by comparing a “Current” Profile (the
269 “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an
270 organization can review all of the Categories and Subcategories and, based on business
271 drivers and a risk assessment, determine which are most important; [theyit](#) can add
272 Categories and Subcategories as needed to address the organization’s risks. The Current
273 Profile can then be used to support prioritization and measurement of progress toward the
274 Target Profile, while factoring in other business needs including cost-effectiveness and
275 innovation. Profiles can be used to conduct self-assessments and communicate within an
276 organization or between organizations.

277 1.2 Risk Management and the Cybersecurity Framework

278 Risk management is the ongoing process of identifying, assessing, and responding to risk. To
279 manage risk, organizations should understand the likelihood that an event will occur and the
280 resulting impact. With this information, organizations can determine the acceptable level of risk
281 for delivery of services achieving its organizational objectives and can express this as their risk
282 tolerance.

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

294 The Framework is adaptive to provide a flexible and risk-based implementation that can be used
295 with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk
296 management processes include International Organization for Standardization (ISO)
297 31000:2009⁶, ISO/IEC 27005:2011⁷, National Institute of Standards and Technology (NIST)
298 Special Publication (SP) 800-39⁸, and the *Electricity Subsector Cybersecurity Risk Management*
299 *Process* (RMP) guideline⁹.

300 1.3 Document Overview

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

- 302 • [Section 2](#) describes the Framework components: the Framework Core, the Tiers, and the
303 Profiles.
- 304 • [Section 3](#) presents examples of how the Framework can be used.
- 305 • [Section 4 describes how to use the Framework for self-assessing and demonstrating](#)
306 [cybersecurity through measurements.](#)
- 307 • [Appendix A](#) presents the Framework Core in a tabular format: the Functions, Categories,
308 Subcategories, and Informative References.

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. http://www.iso.org/iso/catalogue_detail?csnumber=56742

⁸ Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. <http://csre.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf><http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

⁹ U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012. <http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf><https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf>

309
310
311
312

- [Appendix B](#) contains a glossary of selected terms.
- [Appendix C](#) lists acronyms used in this document.
- [Appendix D is a detailed listing of updates between the Framework Version 1.0 and the current draft of Version 1.1.](#)

313 2.0 Framework Basics

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

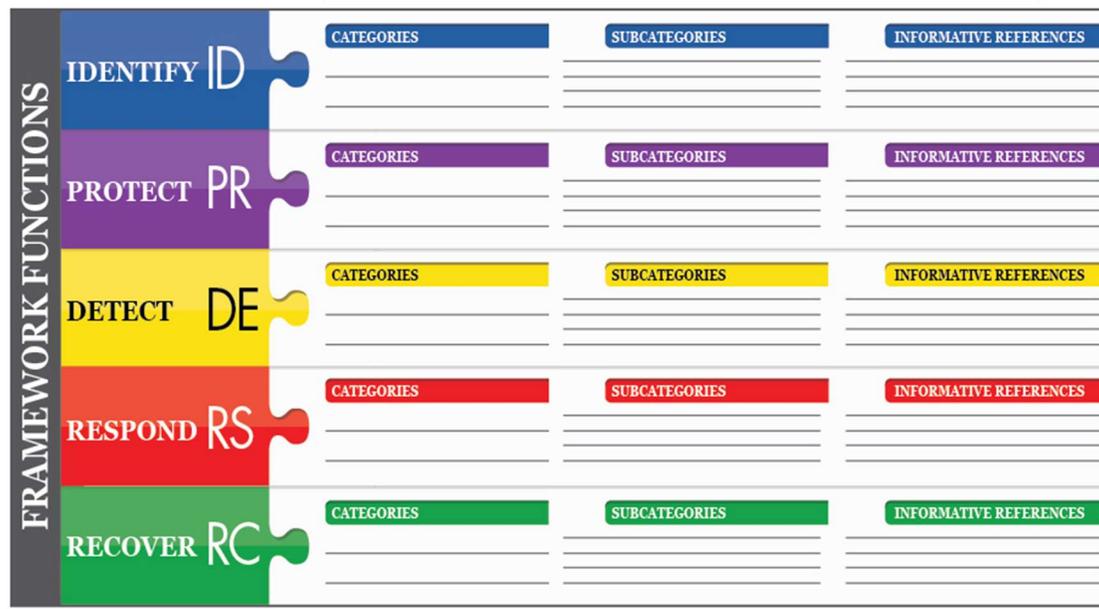
322 2.1 Framework Core

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

328

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

329



330

Figure 1: Framework Core Structure

331 The Framework Core elements work together as follows:

- 332 • **Functions** organize basic cybersecurity activities at their highest level. These Functions
333 are Identify, Protect, Detect, Respond, and Recover. They aid an organization in
334 expressing its management of cybersecurity risk by organizing information, enabling risk
335 management decisions, addressing threats, and improving by learning from previous
336 activities. The Functions also align with existing methodologies for incident management
337 and help show the impact of investments in cybersecurity. For example, investments in
338 planning and exercises support timely response and recovery actions, resulting in reduced
339 impact to the delivery of services.
- 340 • **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes
341 closely tied to programmatic needs and particular activities. Examples of Categories
342 include “Asset Management,” “[Identity Management and Access Control](#),” and
343 “Detection Processes.”

- 344 • **Subcategories** further divide a Category into specific outcomes of technical and/or
345 management activities. They provide a set of results that, while not exhaustive, help
346 support achievement of the outcomes in each Category. Examples of Subcategories
347 include “External information systems are catalogued,” “Data-at-rest is protected,” and
348 “Notifications from detection systems are investigated.”
- 349 • **Informative References** are specific sections of standards, guidelines, and practices
350 common among critical infrastructure sectors that illustrate a method to achieve the
351 outcomes associated with each Subcategory. The Informative References presented in the
352 Framework Core are illustrative and not exhaustive. They are based upon cross-sector
353 guidance most frequently referenced during the Framework development process.¹⁰

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

- 358 • **Identify** – Develop ~~the~~an organizational understanding to manage cybersecurity risk to
359 systems, assets, data, and capabilities.

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

- 366 • **Protect** – Develop and implement ~~the~~ appropriate safeguards to ensure delivery of
367 critical infrastructure services.

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

¹⁰ NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at <http://www.nist.gov/cyberframework/>.

- **Detect** – Develop and implement ~~the~~ 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 ~~the~~ appropriate activities to take action regarding a detected cybersecurity ~~event-~~incident.

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

- **Recover** – 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-~~incident.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity ~~event~~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. ~~The Tiers range~~Ranging from Partial (Tier 1) to Adaptive (Tier 4) ~~and~~, Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices ~~and~~. 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 necessarily 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 should receive additional resources. Progression to higher Tiers is encouraged when ~~such a change would reduce cybersecurity risk and be a~~ cost-benefit analysis indicates a feasible and cost-effective. Successful implementation

414 ~~of the Framework is based upon achievement reduction of the outcomes described in the~~
415 ~~organization's Target Profile(s) and not upon Tier determination cybersecurity risk.~~

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

422 The Tier definitions are as follows:

423 **Tier 1: Partial**

- 424 • *Risk Management Process* – Organizational cybersecurity risk management practices are
425 not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner.
426 Prioritization of cybersecurity activities may not be directly informed by organizational
427 risk objectives, the threat environment, or business/mission requirements.
- 428 • *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk
429 at the organizational level ~~and an organization-wide approach to managing cybersecurity~~
430 ~~risk has not been established.~~ The organization implements cybersecurity risk
431 management on an irregular, case-by-case basis due to varied experience or information
432 gained from outside sources. The organization may not have processes that enable
433 cybersecurity information to be shared within the organization.
- 434 • ~~*External Participation*—An organization may not have the processes in place to~~
435 ~~participate in coordination or collaboration with other entities.~~ *External Participation* –
436 The organization does not understand its role in the larger ecosystem with respect to its
437 dependencies and dependents. The organization does not collaborate with or receive
438 information (e.g., threat intelligence, best practices, technologies) from other entities
439 (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor
440 does it share information. The organization is generally unaware of the cyber supply
441 chain risks of the products and services it provides and that it uses.

442 **Tier 2: Risk Informed**

- 443 • *Risk Management Process* – Risk management practices are approved by management
444 but may not be established as organizational-wide policy. Prioritization of cybersecurity
445 activities and protection needs is directly informed by organizational risk objectives, the
446 threat environment, or business/mission requirements.
- 447 • *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at
448 the organizational level, but an organization-wide approach to managing cybersecurity
449 risk has not been established. ~~Risk-informed, management-approved processes and~~
450 ~~procedures are defined and implemented, and staff has adequate resources to perform~~
451 ~~their cybersecurity duties.~~ Cybersecurity information is shared within the organization on
452 an informal basis. Consideration of cybersecurity in organizational objectives and
453 programs may occur at some but not all levels of the organization. Cyber risk assessment
454 of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- 455 • *External Participation* – ~~The~~ Generally, the organization knows/understands its role in the
456 larger ecosystem with respect to its own dependencies or dependents, but ~~has not~~
457 ~~formalized its capabilities to interact both.~~ The organization collaborates with and

458 receives some information from other entities and generates some of its own
459 information, but may not share information externally with others. Additionally, the
460 organization is aware of the cyber supply chain risks associated with the products and
461 services it provides and that it uses, but does not act consistently or formally upon those
462 risks.

463 Tier 3: Repeatable

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

487 Tier 4: Adaptive

- 488 • *Risk Management Process* – The organization adapts its cybersecurity practices based on
489 lessons learned and predictive indicators derived from previous and current cybersecurity
490 activities, including lessons learned and predictive indicators. Through a process of
491 continuous improvement incorporating advanced cybersecurity technologies and
492 practices, the organization actively adapts to a changing cybersecurity landscape threat
493 and technology landscapes and responds in a timely and effective manner to evolving
494 and, sophisticated threats in a timely manner.
- 495 • *Integrated Risk Management Program* – There is an organization-wide approach to
496 managing cybersecurity risk that uses risk-informed policies, processes, and procedures
497 to address potential cybersecurity events. The relationship between cybersecurity risk and
498 organizational objectives is clearly understood and considered when making decisions.
499 Senior executives monitor cybersecurity risk in the same context as financial risk and
500 other organizational risks. The organizational budget is based on an understanding of the

501 current and predicted risk environment and risk tolerance. Business units implement
502 executive vision and analyze system-level risks in the context of the organizational risk
503 tolerances. Cybersecurity risk management is part of the organizational culture and
504 evolves from an awareness of previous activities, ~~information shared by other sources,~~
505 and continuous awareness of activities on their systems and networks. The organization
506 can quickly and efficiently account for changes to business/mission objectives in how
507 risk is approached and communicated. ~~External Participation—The organization manages~~
508 ~~risk and actively shares information with partners to ensure that accurate, current~~
509 ~~information is being distributed and consumed to improve cybersecurity before a~~
510 ~~cybersecurity event occurs.~~

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

521 **2.3 Framework Profile**

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

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

535 Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be
536 addressed to meet cybersecurity risk management objectives. An action plan to address these
537 gaps can contribute to the roadmap described above. Prioritization of gap mitigation is driven by
538 the organization’s business needs and risk management processes. This risk-based approach
539 enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve
540 cybersecurity goals in a cost-effective, prioritized manner.

541 **2.4 Coordination of Framework Implementation**

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

- 544 • Executive
- 545 • Business/Process
- 546 • Implementation/Operations

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

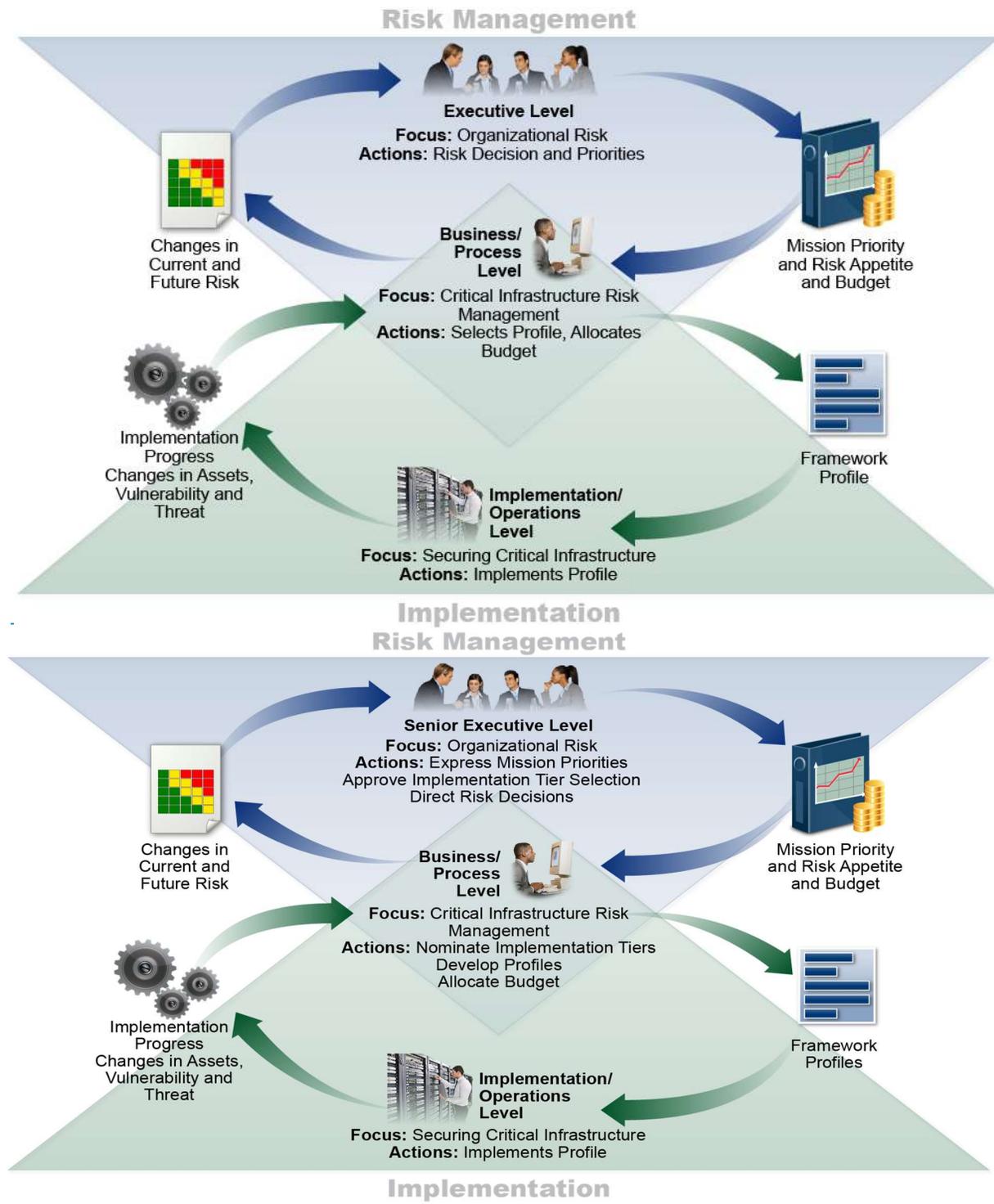


Figure 2: Notional Information and Decision Flows within an Organization

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. Utilizing 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 design, build/buy, deploy, operate, and decommission. The design phase should account for cybersecurity requirements as a part of a larger multi-disciplinary systems engineering process.¹¹ 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 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

¹¹ NIST Special Publication 800-160 - *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>

595 and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve
596 certain outcomes. The organization can use this information to reprioritize resources.

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

604 **3.2 Establishing or Improving a Cybersecurity Program**

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

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

615 **Step 2: Orient.** Once the scope of the cybersecurity program has been determined for the
616 business line or process, the organization identifies related systems and assets, regulatory
617 requirements, and overall risk approach. The organization then [identifiesconsults sources to](#)
618 [identify](#) threats ~~to~~, and vulnerabilities ~~of~~, [applicable to](#) those systems and assets.

619 **Step 3: Create a Current Profile.** The organization develops a Current Profile by indicating
620 which Category and Subcategory outcomes from the Framework Core are currently being
621 achieved. [If an outcome is partially achieved, noting this fact will help support subsequent steps.](#)

622 **Step 4: Conduct a Risk Assessment.** This assessment could be guided by the organization’s
623 overall risk management process or previous risk assessment activities. The organization
624 analyzes the operational environment in order to discern the likelihood of a cybersecurity event
625 and the impact that the event could have on the organization. It is important that organizations
626 [seek to incorporateidentify](#) emerging risks and [use cyber](#) threat [information from internal](#) and
627 [vulnerability dataexternal](#) sources to [facilitategain](#) a ~~robust~~[better](#) understanding of the likelihood
628 and impact of cybersecurity events.

629 **Step 5: Create a Target Profile.** The organization creates a Target Profile that focuses on the
630 assessment of the Framework Categories and Subcategories describing the organization’s desired
631 cybersecurity outcomes. Organizations also may develop their own additional Categories and
632 Subcategories to account for unique organizational risks. The organization may also consider
633 influences and requirements of external stakeholders such as sector entities, customers, and

634 business partners when creating a Target Profile. [The Profile should appropriately reflect criteria](#)
635 [within the target Implementation Tier.](#)

636 **Step 6: Determine, Analyze, and Prioritize Gaps.** The organization compares the Current
637 Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to
638 address ~~those~~ gaps ~~that draws upon~~ [reflecting](#) mission drivers, ~~a cost/benefit analysis, costs~~ and
639 ~~understanding of risk benefits, and risks~~ – to achieve the outcomes in the Target Profile. The
640 organization then determines resources, [including funding and workforce](#), necessary to address
641 the gaps. Using Profiles in this manner [encourages](#) the organization to make informed
642 decisions about cybersecurity activities, supports risk management, and enables the organization
643 to perform cost-effective, targeted improvements.

644 **Step 7: Implement Action Plan.** The organization determines which actions to take ~~in regards~~
645 to [address](#) the gaps, if any, identified in the previous step. It then ~~monitors~~ [adjusts](#) its current
646 cybersecurity practices [against in order to achieve](#) the Target Profile. For further guidance, the
647 Framework identifies example Informative References regarding the Categories and
648 Subcategories, but organizations should determine which standards, guidelines, and practices,
649 including those that are sector specific, work best for their needs.

650 An organization may repeat the steps as needed to continuously assess and improve its
651 cybersecurity. For instance, organizations may find that more frequent repetition of the orient
652 step improves the quality of risk assessments. Furthermore, organizations may monitor progress
653 through iterative updates to the Current Profile, subsequently comparing the Current Profile to
654 the Target Profile. Organizations may also [utilize](#) this process to align their cybersecurity
655 program with their desired Framework Implementation Tier.

656 3.3 Communicating Cybersecurity Requirements with Stakeholders

657 The Framework provides a common language to communicate requirements among
658 interdependent stakeholders responsible for the delivery of essential critical infrastructure
659 [products and](#) services. Examples include:

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

673 [Communication is especially important among stakeholders up and down supply chains. Supply](#)
674 [chains are a complex, globally distributed, and interconnected set of resources and processes](#)

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

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

683 A primary objective of cyber SCRM is to identify, assess, and mitigate “products and services
684 that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to
685 poor manufacturing and development practices within the cyber supply chain¹².” Cyber SCRM
686 activities may include:

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

694 As depicted in Figure 3, cyber SCRM encompasses technology suppliers and buyers, as well as
695 non-technology suppliers and buyers, where technology is minimally composed of information
696 technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected
697 devices more generally, including the Internet of Things (IoT).

¹² NIST Special Publication 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf><http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf>

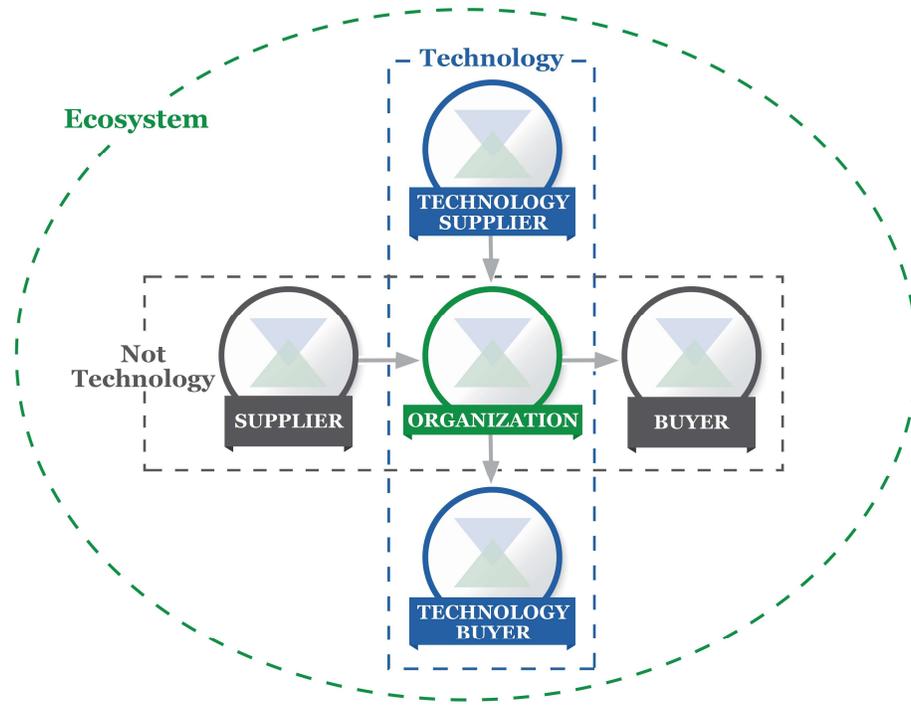


Figure 3: Cyber Supply Chain Relationships

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

703 In the figure above, “Buyer” refers to the people or organizations that consume a given product
 704 or service from an organization, including both for-profit and not-for-profit organizations.
 705 “Supplier” encompasses product and service providers that are used for an organization’s
 706 internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to
 707 the Buyer. These terms are applicable for both technology-based and non-technology-based
 708 relationships.

709 Whether considering individual Subcategories of the Core or the comprehensive considerations
 710 of a Profile, the Framework offers organizations and their partners a method to help ensure the
 711 new product or service meets critical security outcomes. By first selecting outcomes that are
 712 relevant to the context (e.g., transmission of Personally Identifiable Information (PII), mission
 713 critical service delivery, data verification services, product or service integrity) the organization
 714 then can evaluate partners against those criteria. For example, if a system is being purchased that
 715 will monitor OT for anomalous network communication, availability may be a particularly
 716 important cybersecurity objective to achieve and should drive a Technology Supplier evaluation
 717 against applicable Subcategories (e.g., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6,
 718 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 cyber SCRM (Section 3.3) in that it may not be possible to impose a set of cybersecurity requirements on the supplier. Instead, 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 analysis, so a product or service with known gaps to the Target Profile may be evaluated.

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.

3.5.6 Methodology to Protect Privacy and Civil Liberties

This section describes a methodology ~~as required by the Executive Order~~ to address individual privacy and civil liberties implications that may result from cybersecurity operations. 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 ~~may give rise to these~~ engender privacy and civil liberties considerations. ~~Consistent with Section 3.4, technical~~ 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 ~~implications may arise~~ when personal information is used, collected, processed, maintained, or disclosed ~~in connection with an organization's cybersecurity activities.~~ Some examples ~~of activities that bear privacy or civil liberties considerations may~~ 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 ~~activities such as~~ some types of incident detection or monitoring that may ~~impact~~ inhibit freedom of expression or association.

The government and ~~its~~ agents ~~of the government~~ have a ~~direct~~ responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below,

761 government or ~~its~~ ~~agents of the government~~ that own or operate critical infrastructure should
762 have a process in place to support compliance of cybersecurity activities with applicable privacy
763 laws, regulations, and Constitutional requirements.

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

772 As organizations assess the Framework Core in [Appendix A](#), the following processes and
773 activities may be considered as a means to address the above-referenced privacy and civil
774 liberties implications:

775 **Governance of cybersecurity risk**

- 776 • An organization's assessment of cybersecurity risk and potential risk responses considers
777 the privacy implications of its cybersecurity program
- 778 • Individuals with cybersecurity-related privacy responsibilities report to appropriate
779 management and are appropriately trained
- 780 • Process is in place to support compliance of cybersecurity activities with applicable
781 privacy laws, regulations, and Constitutional requirements
- 782 • Process is in place to assess implementation of the [foregoing above](#) organizational
783 measures and controls

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

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

789 **Awareness and training measures**

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

794 **Anomalous activity detection and system and assets monitoring**

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

797 **Response activities, including information sharing or other mitigation efforts**

- 798 • Process is in place to assess and address whether, when, how, and the extent to which
799 personal information is shared outside the organization as part of cybersecurity
800 information sharing activities
- 801 • Process is in place to conduct a privacy review of an organization's cybersecurity
802 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.

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 operate setting 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.

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. 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 both security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives. While it is sometimes important to determine whether or not an organizational objective was achieved through lagging measurement, leading measurements of whether a cybersecurity risk may occur, and the impact it might have, are typically more important to determining likelihood of accomplishing an organizational objective.

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

847 **Appendix A: Framework Core**

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

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

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

873 Additional supporting material relating to the Framework can be found on the NIST website at
874 <http://www.nist.gov/cyberframework/>.

875
876

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

877

Table 2: Framework Core

Function	Category	Subcategory	Informative References
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 <u>businessorganizational</u> objectives and the organization’s risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CEIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CEIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	CEIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04 , DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, <u>time</u> , and software) are prioritized based on their classification, criticality, and business value	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01 , BAI04.02 , BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06 , APO13.01 , DSS06.03

Function	Category	Subcategory	Informative References
		third-party stakeholders (e.g., suppliers, customers, partners) are established	ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	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, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2- NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established <u>for all operating states (e.g. under duress/attack, during recovery, normal operations)</u>	COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-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 information security policy is established	CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all families

Function	Category	Subcategory	Informative References
	management of cybersecurity risk.	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	CIS CSC 19 COBIT 5 APO01.02 , APO10.03 , APO13.1202 , DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PS-7 , PM-1, PS-7PM-2
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	CIS CSC 19 COBIT 5 MEA03BAI02.01 , MEA03.01 , MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2 , A.18.1.3 , A.18.1.4 , A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	COBIT 5 EDM03.02 , APO12.02 , APO12.05 , DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2 , PM-3 , PM-7 , PM-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	CCIS CSC 4 COBIT 5 APO12.01 , APO12.02 , APO12.03 , APO12.04 , DSS05.01 , DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2 , CA-7 , CA-8 , RA-3 , RA-5 , SA-5 , SA-11 , SI-2 , SI-4 , SI-5	
	ID.RA-2: Threat and vulnerability information 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, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4	

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 SI-5 , PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14 , PM-9, PM-11, SA-14
		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.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9
	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, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9

Function	Category	Subcategory	Informative References
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9
		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 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11, SA-14
	<p>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.</p>	<p>ID.SC-1: <u>Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders</u></p>	<p>CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9</p>
<p>ID.SC-2: <u>Identify, prioritize and assess suppliers and third-party partners of information systems, components and services using a cyber supply chain risk assessment process</u></p>		<p>COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9</p>	
<p>ID.SC-3: <u>Suppliers and third-party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.</u></p>		<p>COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9</p>	

Function	Category	Subcategory	Informative References
		<p><u>ID.SC-4: Suppliers and third-party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted</u></p>	<p><u>COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05</u> <u>ISA 62443-2-1:2009 4.3.2.6.7</u> <u>ISA 62443-3-3:2013 SR 6.1</u> <u>ISO/IEC 27001:2013 A.15.2.1, A.15.2.2</u> <u>NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12</u></p>
		<p><u>ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers</u></p>	<p><u>CIS CSC 19, 20</u> <u>COBIT 5 DSS04.04</u> <u>ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11</u> <u>ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4</u> <u>ISO/IEC 27001:2013 A.17.1.3</u> <u>NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9</u></p>
<p>PROTECT (PR)</p>	<p><u>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.</u></p>	<p><u>PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices and users and processes</u></p>	<p><u>CIS CSC 1, 5, 15, 16</u> <u>COBIT 5 DSS05.04, DSS06.03</u> <u>ISA 62443-2-1:2009 4.3.3.5.1</u> <u>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9</u> <u>e43, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3</u> <u>NIST SP 800-53 Rev. 4 AC-1, AC-2, IA Family-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11</u></p>
		<p><u>PR.AC-2: Physical access to assets is managed and protected</u></p>	<p><u>COBIT 5 DSS01.04, DSS05.05</u> <u>ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8</u> <u>ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.3-1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8</u> <u>NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-98</u></p>
		<p><u>PR.AC-3: Remote access is managed</u></p>	<p><u>CIS CSC 12</u></p>

Function	Category	Subcategory	Informative References
			<p>COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.21, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-17-1, AC17, AC-19, AC-20, SC-15</p>
		<p>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties</p>	<p>CCIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24</p>
		<p>PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate</p>	<p>CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7</p>
		<p>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions when appropriate</p>	<p>CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3</p>

Function	Category	Subcategory	Informative References
		<p>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)</p>	<p>CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11</p>
	<p>Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>PR.AT-1: All users are informed and trained</p>	<p>CEIS CSC 917, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13</p>
		<p>PR.AT-2: Privileged users understand roles and responsibilities</p>	<p>CEIS CSC 95, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13</p>
		<p>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities</p>	<p>CEIS CSC 917 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16</p>
		<p>PR.AT-4: Senior executives understand roles and responsibilities</p>	<p>CEIS CSC 917, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2; NIST SP 800-53 Rev. 4 AT-3, PM-13</p>

Function	Category	Subcategory	Informative References
<p>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.</p>		<p>PR.AT-5: Physical and information security personnel understand roles <u>&and</u> responsibilities</p>	<p>CEIS CSC 917 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2; NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13</p>
		<p>PR.DS-1: Data-at-rest is protected</p>	<p>CEIS CSC 4713, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28</p>
		<p>PR.DS-2: Data-in-transit is protected</p>	<p>CEIS CSC 4713, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12</p>
		<p>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition</p>	<p>CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009-4 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16</p>
		<p>PR.DS-4: Adequate capacity to ensure availability is maintained</p>	<p>CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5</p>
		<p>PR.DS-5: Protections against data leaks are implemented</p>	<p>CEIS CSC 4713</p>

Function	Category	Subcategory	Informative References
			<p>COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02</p> <p>ISA 62443-3-3:2013 SR 5.2</p> <p>ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</p>
		<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>	<p>CIS CSC 2, 3</p> <p>COBIT 5 APO01.06, BAI06.01, DSS06.02</p> <p>ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8</p> <p>ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4</p> <p>NIST SP 800-53 Rev. 4 SC-16, SI-7</p>
		<p>PR.DS-7: The development and testing environment(s) are separate from the production environment</p>	<p>CIS CSC 18, 20</p> <p>COBIT 5 BAI03.08, BAI07.04</p> <p>ISO/IEC 27001:2013 A.12.1.4</p> <p>NIST SP 800-53 Rev. 4 CM-2</p>
		<p>PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity</p>	<p>COBIT 5 BAI03.05</p> <p>ISA 62443-2-1:2009 4.3.4.4.4</p> <p>ISO/IEC 27001:2013 A.11.2.4</p> <p>NIST SP 800-53 Rev. 4 SA-10, SI-7</p>
		<p>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</p>	<p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)</p>

Function	Category	Subcategory	Informative References
	protection of information systems and assets.	<p>PR.IP-2: A System Development Life Cycle to manage systems is implemented</p>	<p>CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8SI-12, SI-13, SI-14, SI-16, SI-17</p>
		<p>PR.IP-3: Configuration change control processes are in place</p>	<p>CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01, BAI01.06 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</p>
		<p>PR.IP-4: Backups of information are conducted, maintained, and tested periodically</p>	<p>CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9</p>
		<p>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met</p>	<p>COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18</p>
		<p>PR.IP-6: Data is destroyed according to policy</p>	<p>COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2</p>

Function	Category	Subcategory	Informative References
			<p>ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7</p> <p>NIST SP 800-53 Rev. 4 MP-6</p>
		<p>PR.IP-7: Protection processes are continuously improved</p>	<p>COBIT 5 APO11.06, APO12.06, DSS04.05</p> <p>ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8</p> <p>ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10</p> <p>NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6</p>
		<p>PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties</p>	<p>COBIT 5 BAI08.04, DSS03.04</p> <p>ISO/IEC 27001:2013 A.16.1.6</p> <p>NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4</p>
		<p>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</p>	<p>CIS CSC 19</p> <p>COBIT 5 APO12.06, DSS04.03</p> <p>ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1</p> <p>ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3</p> <p>NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17</p>
		<p>PR.IP-10: Response and recovery plans are tested</p>	<p>CIS CSC 19, 20</p> <p>COBIT 5 DSS04.04</p> <p>ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11</p> <p>ISA 62443-3-3:2013 SR 3.3</p> <p>ISO/IEC 27001:2013 A.17.1.3</p> <p>NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14</p>
		<p>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)</p>	<p>CIS CSC 5, 16</p> <p>COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05</p> <p>ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3</p> <p>ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4</p>

Function	Category	Subcategory	Informative References
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.			NIST SP 800-53 Rev. 4 PS-Family-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: A vulnerability management plan is developed and implemented	CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components isare performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets isare performed and logged in a timely manner, with approved and controlled tools	COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, 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 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.43.3.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
	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, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, APO13.04, DSS05.06

Function	Category	Subcategory	Informative References
			<p>ISA 62443-3-3:2013 SR 2.3</p> <p>ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9</p> <p>NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8</p>
		<p>PR.PT-3: Access to systems and assets is controlled, incorporating theThe principle of least functionality is incorporated by configuring systems to provide only essential capabilities</p>	<p>CIS CSC 3, 11, 14</p> <p>COBIT 5 DSS05.02, DSS05.05, DSS06.06</p> <p>ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4</p> <p>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7</p> <p>ISO/IEC 27001:2013 A.9.1.2</p> <p>NIST SP 800-53 Rev. 4 AC-3, CM-7</p>
		<p>PR.PT-4: Communications and control networks are protected</p>	<p>CIS CSC 78, 12, 15</p> <p>COBIT 5 DSS05.02, APO13.01</p> <p>ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6</p> <p>ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3</p> <p>NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43</p>
		<p>PR.PT-5: <u>Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations)</u></p>	<p>COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05</p> <p>ISA 62443-2-1:2009 4.3.2.5.2</p> <p>ISA 62443-3-3:2013 SR 7.1, SR 7.2</p> <p>ISO/IEC 27001:2013 A.17.1.2, A.17.2.1</p> <p>NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6</p>

Function	Category	Subcategory	Informative References
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		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 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.16.1.1 , A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated collected and correlated from multiple sources and sensors	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The	DE.CM-1: The network is monitored to detect potential cybersecurity events	CIS CSC 4 CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05 , DSS05.07

Function	Category	Subcategory	Informative References
	information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.		ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		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 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	CIS CSC 5, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8
		DE.CM-5: Unauthorized mobile code is detected	CIS CSC 7, 8 COBIT 5 DSS05.01 ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	CEIS CSC 519 COBIT 5 APO01.02 , DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	COBIT 5 DSS06.01 , MEA03.03 , MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2 , A.18.2.3 NIST SP 800-53 Rev. 4 AC-25 , CA-2, CA-7, PM-14 , SA-18 , SI-4, PM-14
		DE.DP-3: Detection processes are tested	COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14 , SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated to appropriate parties	CIS CSC 19 COBIT 5 APO08.04 , APO12.06, DSS02.05 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Detection processes are continuously improved	COBIT 5 APO11.06, APO12.06 , DSS04.05 ISA 62443-2-1:2009 4.4.3.4		

Function	Category	Subcategory	Informative References
			ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events/incidents .	RS.RP-1: Response plan is executed during or after an event/incident	CIS CSC 19 COBIT 5 APO12.06 , BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include 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 , APO01.02 , APO12.03 ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events/Incidents are reported consistent with established criteria	CIS CSC 19 COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2, Clause 7.4 , Clause 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, 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 4.3.4.5.5 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Function	Category	Subcategory	Informative References
<p>Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.</p>		<p>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</p>	<p>CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, SI-5</p>
		<p>RS.AN-1: Notifications from detection systems are investigated</p>	<p>CIS CSC 4, 6, 8, 19 COBIT 5 DSS02.04, DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4</p>
		<p>RS.AN-2: The impact of the incident is understood</p>	<p>COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4</p>
		<p>RS.AN-3: Forensics are performed</p>	<p>COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4</p>
		<p>RS.AN-4: Incidents are categorized consistent with response plans</p>	<p>CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8</p>
		<p>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)</p>	<p>CIS CSC 4, 19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15</p>

Function	Category	Subcategory	Informative References
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate resolve the incident.	RS.MI-1: Incidents are contained	CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	CIS CSC 4, 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		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.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	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 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events incidents.	RC.RP-1: Recovery plan is executed during or after an event a cybersecurity incident
Improvements (RC.IM): Recovery planning and processes are improved by incorporating		RC.IM-1: Recovery plans incorporate lessons learned	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10

Function	Category	Subcategory	Informative References
	lessons learned into future activities.		NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	COBIT 5 APO12.06 , BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as 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.6.1.4, Clause 7.4
		RC.CO-2: Reputation after an event is repaired	COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4

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/Pages/default.aspx>
- ~~Council on CyberSecurity (CCS) Top 20 CIS~~ Critical Security Controls (~~CSC~~ [for Effective Cyber Defense \(CIS Controls\)](https://www.cisecurity.org)):
~~<http://www.counciloncybersecurity.org>~~<https://www.cisecurity.org>
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*:
<http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243><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 Security Requirements and Security Levels*:
<http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420><https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785>
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: ~~NIST Special Publication 800-53 Revision 4~~, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January ~~15, 2014~~ [22, 2015](#)).

<http://dx.doi.org/10.6028/NIST.SP.800-53r4>. Informative References are only mapped to the control level, though any control enhancement might be found useful in achieving a subcategory outcome.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References ~~represent a general correspondence and~~ are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

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

1 Appendix B: Glossary

2 This appendix defines selected terms used in the publication.

3 **Table 3: Framework Glossary**

<u>Buyer</u>	<u>The people or organizations that consume a given product or service.</u>
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,” “ <u>Identity Management and Access Control</u> ,” 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).
<u>Cybersecurity Incident</u>	<u>A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.</u>
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.”

<u>Supplier</u>	<u>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.</u>
<u>Taxonomy</u>	<u>A scheme of classification.</u>

4

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

CCS	Council on CyberSecurity
CEA	Cybersecurity Enhancement Act of 2014
COBIT	Control Objectives for Information and Related Technology
DCS	Distributed Control System
CPS	Cyber-Physical Systems
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
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SP	Special Publication

29 Appendix D: Revisions and Updates

30 Changes incorporated into the Framework Version 1.1 Draft 2 are displayed in Table 4.

31

32

Table 4: Changes in Framework Version 1.1

<u>PAGE(S)</u>	<u>CHANGE</u>
<u>p. ii</u>	<u>A ‘Note to Reviewers on the Update and Next Steps’ was added to give readers a quick glance to the updates made and to request comments.</u>
<u>p. iv</u>	<u>The ‘Table of Contents’ was modified to reflect all changes relative to the current draft of Version 1.1 update.</u>
<u>pp. 5-6</u>	<u>The ‘Executive Summary’ was modified to more clearly present the Framework, the development process, and next steps.</u>
<u>p. 7</u>	<u>Section 1.0 ‘Framework Introduction’ was updated to include the current chartering documents for Framework.</u>
<u>p. 7</u>	<u>Section 1.0 ‘Framework Introduction’ was updated to reflect security implications of a broadening use of technology (e.g. ICS/CPS/IoT) and to more clearly define Framework uses.</u>
<u>p. 10</u>	<u>Section 1.3 ‘Document Overview’ was modified to reflect the additional section and appendix added with this update.</u>
<u>p. 11</u>	<u>Figure 1: ‘Framework Core Structure’ was visually updated.</u>
<u>sic passim</u>	<u>The term “cybersecurity event” has been categorized into two separate concepts: cybersecurity event and cybersecurity incident. The difference is an incident may require a response and recovery, whereas an event may not have a response or recovery associated with it. An organization is expected to have many more events than incidents.</u>
<u>p. 13</u>	<u>Section 2.2 ‘Framework Implementation Tiers’ - Paragraph 3 was modified to clarify the relationship between Tiers and Profiles during Tier selection.</u>
<u>pp. 14-16</u>	<u>Section 2.2 ‘Framework Implementation Tiers’ - Cyber Supply Chain Risk Management (C-SCRM) was incorporated into the “External Participation” portion of the Tiers definitions. The updated “External Participation” portions of the Tiers reflect both C-SCRM and elements of information sharing.</u>
<u>p. 14</u>	<u>Section 2.2 ‘Framework Implementation Tiers’ - Tier 2 ‘Risk Informed’ - Paragraph 2 was modified for clarification to include: “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.”</u>

<u>PAGE(S)</u>	<u>CHANGE</u>
p. 15	<p>Section 2.2 ‘Framework Implementation Tiers’ - Tier 3 ‘Repeatable’ - Paragraph 2 was modified for clarification to include:</p> <p>“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.”</p>
p. 15	<p>Section 2.2 ‘Framework Implementation Tiers’ - Tier 4 ‘Adaptive’ - Paragraph 2 was modified for clarification to include:</p> <p>“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.”</p>
p. 15	<p>Section 2.2 ‘Framework Implementation Tiers’ - Tier 4 ‘Adaptive’ - Paragraph 2 was modified for clarification to include:</p> <p>“The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.”</p>
p. 17	<p>Figure 2 - The actions outlined for the ‘Senior Executive Level’ and the ‘Business/Process Level’ were modified.</p>
p. 18	<p>Section 3.0 ‘How to Use the Framework’ was modified to include the following phrase to show the connection between the Framework and the product development life cycle:</p> <p>“The Framework can be applied throughout the life cycle phases of design, build/buy, deploy, operate, or decommission. The design phase should account for cybersecurity requirements as a part of a larger multi-disciplinary systems engineering process. 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 on-going 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 one or more systems are decommissioned.”</p>
p. 19	<p>Section 3.2 ‘Establishing or Improving a Cybersecurity Program’ - Step 1: ‘Prioritize and Scope’ was modified to clarify Tier usage with the following:</p> <p>“Risk tolerances may be reflected in a target Implementation Tier.”</p>
p. 19	<p>Section 3.2 ‘Establishing or Improving a Cybersecurity Program’ - Step 2: ‘Orient’ was modified to now read as follows:</p>

<u>PAGE(S)</u>	<u>CHANGE</u>
	<u>“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 <i>consults sources to identify threats and vulnerabilities applicable to those systems and assets.</i>”</u>
<u>p. 19</u>	<u>Section 3.2 ‘Establishing or Improving a Cybersecurity Program’ - Step 3: ‘Create a Current Profile’ was modified to include: “If an outcome is partially achieved, noting this fact will help support subsequent steps.”</u>
<u>p. 19</u>	<u>Section 3.2 ‘Establishing or Improving a Cybersecurity Program’ - Step 4: ‘Conduct a Risk Assessment’ was modified to now read as follows: “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 <i>identify emerging risks and use cyber threat information from both internal and external sources to gain a better</i> understanding of the likelihood and impact of cybersecurity events.”</u>
<u>p. 20</u>	<u>Section 3.2 ‘Establishing or Improving a Cybersecurity Program’ - Step 5: ‘Create a Target Profile’ was modified to include: “The Profile should appropriately reflect criteria within the target Implementation Tier.”</u>
<u>p. 20</u>	<u>Section 3.2 ‘Establishing or Improving a Cybersecurity Program’ - Step 6: ‘Determine, Analyze, and Prioritize Gaps’ was modified to now read as follows: “The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps - <i>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.</i> Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.”</u>
<u>p. 20</u>	<u>Section 3.3 ‘Communication Cybersecurity Requirements with Stakeholders’ - an additional bullet was added which reads: “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.”</u>
<u>pp. 20-22</u>	<u>Section 3.3 ‘Communicating Cybersecurity Requirement with Stakeholders’ was modified to include Cyber SCRM.</u>
<u>p. 22</u>	<u>Figure 3: ‘Cyber Supply Chain Relationships’ was added to depict concepts in 3.3.</u>
<u>p. 23</u>	<u>Section 3.4 ‘Buying Decisions’ was added to demonstrate an example of using the Framework.</u>

<u>PAGE(S)</u>	<u>CHANGE</u>
p. 23	Section 3.5 ‘Identifying Opportunities for New or Revised Informative References’ (previously Section 3.4) was moved to accommodate an additional section.
p. 23	Section 3.6 ‘Methodology to Protect Privacy and Civil Liberties’ (previously Section 3.5) was moved to accommodate an additional section.
p. 23	Section 3.6 ‘Methodology to Protect Privacy and Civil Liberties’ - a portion of this section was modified to now read as follows: <u>“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 impact freedom of expression or association.”</u>
p. 24	Section 3.6 ‘Methodology to Protect Privacy and Civil Liberties’ - Authentication was added to “Approaches to identifying, authenticating , and authorizing individuals to access organizational assets and systems”. Also, the subsequent bullet now includes reference to Identity Management.
pp. 25-26	Section 4.0 ‘Self-Assessing Cybersecurity Risk with the Framework’ was added to clarify the relationship between measurements and the Framework.
p. 28	Table 1: ‘Function and Category Unique Identifiers’ was updated to include an additional Category (ID.SC) Supply Chain Risk Management.
pp. 29-49	Table 2: ‘Framework Core’ - The Informative References have been updated pursuant to the most recent version of each reference document.
p. 29	Table 2: ‘Framework Core’ - Subcategory ID.AM-5 was modified to now read as follows: <u>“Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value”.</u>
p. 30	Table 2: ‘Framework Core’ - Subcategory ID.BE-5 was modified to now read as follows: <u>“Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)”.</u>
p. 31	Table 2: ‘Framework Core’ - Subcategory ID.RA-2 was modified to clarify the specific type of data received and now reads as follows: <u>“Cyber threat intelligence is received from information sharing forums and sources”.</u>
pp. 33-34	Table 2: ‘Framework Core’ - Category ID.SC: ‘Supply Chain Risk Management’ and subsequent Subcategories (ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, ID.SC-5) and Informative References were added.

<u>PAGE(S)</u>	<u>CHANGE</u>
p. 34	Table 2: 'Framework Core' - Category PR.AC: 'Access Control' was retitled to "Identity Management, Authentication and Access Control" and now reads: "Access to physical and logical assets and associated facilities is limited to authorized users, processes, or and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions."
p. 34	Table 2: 'Framework Core' - Subcategory PR.AC-1 was modified to now read as follows: "Identities and credentials are <i>issued, managed, verified, revoked, and audited</i> for authorized devices, and users, <i>and processes</i> ".
p. 35	Table 2: 'Framework Core' - Subcategory PR.AC-4 was modified to now read as follows: "Access permissions <i>and authorizations</i> are managed, incorporating the principles of least privilege and separation of duties".
pp. 35-36	Table 2: 'Framework Core' - Subcategories PR.AC-6 and PR.AC-7 and their subsequent Informative References were added.
p. 38	Table 2: 'Framework Core' - Subcategory PR.DS-8 and the subsequent Informative References were added.
p. 38	Table 2: 'Framework Core' - Subcategory PR.IP-1 was modified to now read as follows: "A baseline configuration of information technology/industrial control systems is created and maintained <i>incorporating appropriate security principles (e.g. concept of least functionality)</i> ".
p. 42	Table 2: 'Framework Core' - Subcategory PR.PT-3 was modified to now read as follows: "The principle of least functionality is incorporated by configuring systems to provide only essential capabilities".
p. 42	Table 2: 'Framework Core' - Subcategory PR.PT-5 and the subsequent Informative References were added.
p. 43	Table 2: 'Framework Core' - Subcategory DE.AE-3 was modified to now read as follows: "Event data are <i>collected</i> and correlated from multiple sources and sensors".
p. 46	Table 2: 'Framework Core' - Subcategory RS.CO-2 was modified to now read as follows: " <i>Incidents</i> are reported consistent with established criteria".
p. 47	Table 2: 'Framework Core' - Subcategory RS.AN-5 and the subsequent Informative References were added.
p. 48	Table 2: 'Framework Core' - Subcategory RC.RP-1 was modified to now read as follows: "Recovery plan is executed during or after a <i>cybersecurity incident</i> ".
p. 49	Appendix A: "Framework Core" - The following sentence was added to clarify the nature of Informative References:

<u>PAGE(S)</u>	<u>CHANGE</u>
	<u>“Informative References are not exhaustive, in that not every element (e.g., control, requirement) of a given Informative Reference is mapped to Framework Core Subcategories.</u>
<u>p. 50</u>	<u>Appendix B: ‘Glossary’ - was modified to include the term ‘Buyer’ with the definition: “The people or organizations that consume a given product of service”.</u>
<u>p. 50</u>	<u>Appendix B: ‘Glossary’ - was modified to include the term ‘Cybersecurity Incident’ with the definition: “A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.”</u>
<u>p. 52</u>	<u>Appendix B: ‘Glossary’ - was modified to include the term ‘Supplier’ with the definition: “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.”</u>
<u>p. 52</u>	<u>Appendix B: ‘Glossary’ - was modified to include the term ‘Taxonomy’ with the definition: “A scheme of classification.”</u>
<u>p. 53</u>	<u>Appendix C: ‘Acronyms’ - was modified to include CEA - Cybersecurity Enhancement Act of 2014.</u>
<u>p. 53</u>	<u>Appendix C: ‘Acronyms’ - was modified to include CPS - Cyber-Physical Systems.</u>
<u>p. 53</u>	<u>Appendix C: ‘Acronyms’ – was modified to include IoT - Internet of things.</u>
<u>p. 53</u>	<u>Appendix C: ‘Acronyms’ - was modified to include ISAO - Information Sharing and Analysis Organization.</u>
<u>p. 53</u>	<u>Appendix C: ‘Acronyms’ - was modified to include OT - Operational Technology.</u>
<u>p. 53</u>	<u>Appendix C: ‘Acronyms’ - was modified to include PII - Personally Identifiable Information.</u>
<u>p. 53</u>	<u>Appendix C: ‘Acronyms’ - was modified to include SCRM - Supply Chain Risk Management.</u>