

1 **Draft NIST Special Publication 800-184**

2

3 **Guide for**
4 **Cybersecurity Event Recovery**

5

6

7

8

9

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Matthew Smith
Greg Witte
Karen Scarfone

10

11

12

13

14

15

16

17

18

19

20 **C O M P U T E R S E C U R I T Y**

21

22

23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56

Draft NIST Special Publication 800-184

Guide for Cybersecurity Event Recovery

Michael Bartock
Murugiah Souppaya
*Computer Security Division
Information Technology Laboratory*

Matthew Smith
Greg Witte
*G2, Inc.
Annapolis Junction, MD*

Jeffrey Cichonski
*Applied Cybersecurity Division
Information Technology Laboratory*

Karen Scarfone
*Scarfone Cybersecurity
Clifton, VA*

June 2016



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

57

Authority

58 This publication has been developed by NIST in accordance with its statutory responsibilities under the
59 Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law
60 (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines,
61 including minimum requirements for federal information systems, but such standards and guidelines shall
62 not apply to national security systems without the express approval of appropriate federal officials
63 exercising policy authority over such systems. This guideline is consistent with the requirements of the
64 Office of Management and Budget (OMB) Circular A-130.

65 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory
66 and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should
67 these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of
68 Commerce, Director of the OMB, or any other federal official. This publication may be used by
69 nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States.
70 Attribution would, however, be appreciated by NIST.

71 National Institute of Standards and Technology Special Publication 800-184
72 Natl. Inst. Stand. Technol. Spec. Publ. 800-184, 39 pages (June 2016)
73 CODEN: NSPUE2

74

75 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
76 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
77 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
78 available for the purpose.

79 There may be references in this publication to other publications currently under development by NIST in accordance
80 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,
81 may be used by federal agencies even before the completion of such companion publications. Thus, until each
82 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For
83 planning and transition purposes, federal agencies may wish to closely follow the development of these new
84 publications by NIST.

85 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to
86 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
87 <http://csrc.nist.gov/publications>.

88

89 **Public comment period: June 6 through July 11, 2016**

90 All comments are subject to release under the Freedom of Information Act (FOIA).

91 National Institute of Standards and Technology
92 Attn: Computer Security Division, Information Technology Laboratory
93 100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930
94 Email: csf-recover@nist.gov

95

96

Reports on Computer Systems Technology

97 The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology
98 (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's
99 measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of
100 concept implementations, and technical analyses to advance the development and productive use of
101 information technology. ITL's responsibilities include the development of management, administrative,
102 technical, and physical standards and guidelines for the cost-effective security and privacy of other than
103 national security-related information in federal information systems. The Special Publication 800-series
104 reports on ITL's research, guidelines, and outreach efforts in information system security, and its
105 collaborative activities with industry, government, and academic organizations.

106

Abstract

107 In light of an increasing number of cybersecurity events, organizations can improve resilience by ensuring
108 that their risk management processes include comprehensive recovery planning. Identifying and
109 prioritizing organization resources helps to guide effective plans and realistic test scenarios. This
110 preparation enables rapid recovery from incidents when they occur and helps to minimize the impact on
111 the organization and its constituents. Additionally, continually improving that recovery planning by
112 learning lessons from past events, including those of other organizations, helps to ensure the continuity of
113 important mission functions. This publication provides tactical and strategic guidance regarding the
114 planning, playbook developing, testing, and improvement of recovery planning. It also provides an
115 example scenario that demonstrates guidance and informative metrics that may be helpful for improving
116 resilience of the information systems.

117

Keywords

118 cyber event; cybersecurity; Cybersecurity Framework (CSF); Cybersecurity National Action Plan
119 (CNAP); Cybersecurity Strategy and Implementation Plan (CSIP); metrics; planning; recovery; resilience

120

Acknowledgments

121 The authors wish to thank their colleagues from NIST and industry who reviewed drafts of this document
122 and contributed to its technical content.

123

Trademark Information

124 All trademarks or registered trademarks belong to their respective organizations.

125

126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166

Table of Contents

- Executive Summary 1**
- 1. Introduction 2**
 - 1.1 Background2
 - 1.2 Purpose and Scope3
 - 1.3 Audience3
 - 1.4 Document Structure3
- 2. Planning for Cyber Event Recovery 5**
 - 2.1 Enterprise Resiliency5
 - 2.2 Recovery Planning Prerequisites7
 - 2.3 Recovery Planning Prerequisites8
 - 2.3.1 Planning Document Development 8
 - 2.3.2 Process and Procedure Development 9
 - 2.3.3 Determination of Recovery Initiation/Termination Criteria and Goals Security
10
 - 2.3.4 Root Cause and Containment Strategy Determination11
 - 2.4 Recovery Communications12
 - 2.5 Sharing Recovery Insights13
 - 2.6 Summary of Recommendations13
- 3. Continuous Improvement15**
 - 3.1 Validating Recovery Capabilities15
 - 3.2 Improving Recovery and Security Capabilities17
 - 3.3 Summary of Recommendations17
- 4. Recovery Metrics19**
- 5. Building the Playbook21**
- 6. An Example of a Data Breach Cyber Event Recovery Scenario23**
 - 6.1 Pre-Conditions Required for Effective Recovery23
 - 6.2 Tactical Recovery Phase23
 - 6.2.1 Initiation24
 - 6.2.2 Execution24
 - 6.2.3 Termination25
 - 6.3 Strategic Recovery Phase25
 - 6.3.1 Planning and Execution25
 - 6.3.2 Metrics26
 - 6.3.3 Recovery Plan Improvement26

List of Appendices

- Appendix A— CSF Core Components and SP 800-53r4 Controls Supporting Recovery ..27**
- Appendix B— Acronyms and Other Abbreviations31**
- Appendix C— References32**

167 **Executive Summary**

168 Organizations used to focus their information security efforts on cybersecurity (cyber) event defense, but
169 adversaries have modified their attack techniques to make protection much more difficult, including
170 taking advantage of weaknesses in processes and people instead of just exploiting weaknesses in
171 technologies. As a result, the number of major cyber events continues to increase sharply every year.¹
172 Over the last few years, there has been widespread recognition that some cyber events cannot be stopped.
173 As a result, organizations have started to enhance their cyber event detection and response capabilities.
174 Organizations are continuously improving their prevention capabilities with modern technology and tools
175 while augmenting their cyber event detection and response capabilities.

176 In 2015, members of the Federal Government reviewed cybersecurity capabilities and, as documented in
177 the Cybersecurity Strategy and Implementation Plan (CSIP) [2], identified significant inconsistencies in
178 cyber event response capabilities among federal agencies. The CSIP also stated that agencies must
179 improve their response capabilities. Although there are existing federal policies, standards, and guidelines
180 on cyber event handling, none of them focuses solely on improving security recovery capabilities, nor is
181 the fundamental information captured in a single document. The previous recovery content tends to be
182 spread out in documents such as security, contingency, disaster recovery, and business continuity plans.

183 Recovery is one part of the enterprise risk management process lifecycle; for example, the *Framework for*
184 *Improving Critical Infrastructure Cybersecurity* [3], better known as the Cybersecurity Framework
185 (CSF), defines five functions: Identify, Protect, Detect, Respond, and Recover.² These functions are all
186 critical for a complete defense and may be executed simultaneously instead of occurring sequentially. At
187 a more fundamental level, the Recover function has a significant effect in shaping the other functions by
188 informing them with realistic data. Recovery can be described in two phases focused on separate tactical
189 and strategic outcomes. The immediate tactical recovery phase is largely achieved through the execution
190 of the recovery playbook planned prior to the incident (with input from Detect and other CSF functions as
191 required). The second phase is more strategic, and it focuses on the continuous improvement of all the
192 CSF functions to mitigate the likelihood and impact of future incidents (based on the lessons learned from
193 the incident as well as from other organizations and industry practices).

194 This document is not an operational playbook, but provides guidance to help organizations plan and
195 prepare recovery from a cyber event and integrate the processes and procedures into their enterprise risk
196 management plan. This document is not intended to be used as a playbook by organizations responding to
197 an active cyber event, but as a guide to develop their recovery plan in form of customized playbooks. As
198 referred to in this document, a playbook is an action plan that documents actionable set of steps an
199 organization can follow to successfully recover from a cyber event. While many fundamental activities
200 are similar for organizations of different sizes and from different industry sectors, each playbook can
201 focus on a unique type of cyber event and can be organization-specific, tailored to fit the dependencies of
202 its people, processes, and technologies. If an active cyber event is discovered, organizations that do not
203 have in-house expertise to execute a playbook can seek assistance from a trustworthy external party with
204 experience in incident response and recovery, such as through the Department of Homeland Security
205 (DHS) or an Information Sharing and Analysis Organization (ISAO), or a reputable commercial managed
206 security services provider.

¹ For more information on the number of cyber events occurring within federal agencies, see Government Accountability Office (GAO) 15-714, September 2015 [1].

² Throughout this paper, there are references to the five CSF functions to help organize the material. CSF is one of many informative references that organizations might use to prepare for recovery; see Appendix C for additional examples.

207 1. Introduction

208 1.1 Background

209 The Cybersecurity Strategy and Implementation Plan (CSIP) [2] defines *recover* as “the development and
210 implementation of plans, processes, and procedures for recovery and full restoration, in a timely manner,
211 of any capabilities or services that are impaired due to a cyber event.” A *cyber event* is a specific
212 cybersecurity incident or set of related cybersecurity incidents that result in the successful compromise of
213 one or more information systems. In the simplest cases, recovering from a cyber event might involve a
214 system administrator rebuilding a system or restoring data from a backup. But in most cases, recovery is
215 far more complex, involving combinations of people, processes, and technologies. The status of recovery
216 is usually better expressed as a gradient, with different degrees of progress toward recovery at any given
217 time for different systems or system components, than a binary state of recovered or not recovered.

218 Recovery is one part of the enterprise risk management process lifecycle; for example, the *Framework for*
219 *Improving Critical Infrastructure Cybersecurity* [3], better known as the Cybersecurity Framework
220 (CSF), defines five functions: Identify, Protect, Detect, Respond, and Recover.³ These functions are all
221 critical for a complete defense and may be executed simultaneously instead of occurring sequentially. At
222 a more fundamental level, the Recover function has a significant effect in shaping the other functions by
223 informing them with realistic data. Recovery can be described in two phases focused on separate tactical
224 and strategic outcomes. The immediate tactical recovery phase is largely achieved through the execution
225 of the recovery playbook planned prior to the incident (with input from Detect and other CSF functions as
226 required). The second phase is more strategic, and it focuses on the continuous improvement of all the
227 CSF functions to mitigate likelihood and impact of future incidents (based on the lessons learned from the
228 incident as well as from other organizations and industry practices).

229 In 2015, members of the Federal Government reviewed cybersecurity capabilities and, as documented in
230 the CSIP, identified significant inconsistencies in cyber event response capabilities among federal
231 agencies. The CSIP also stated that agencies must improve their response capabilities. Although there are
232 existing federal policies, standards, and guidelines on cyber event handling, none of them has focused
233 solely on improving cybersecurity recovery capabilities, nor is the fundamental information captured in a
234 single document. The previous recovery content tends to be spread out in documents such as security,
235 contingency, disaster recovery, and business continuity plans.

236 Organizations used to focus their information security efforts on cyber event protection, but adversaries
237 have modified their attack techniques to make protection much more difficult, including taking advantage
238 of weaknesses in processes and people instead of just exploiting weaknesses in technologies. As a result,
239 the number of cyber events continues to increase sharply every year.⁴ Over the last few years, there has
240 been widespread recognition that some cyber events cannot be stopped. As a result of this risk
241 recognition, organizations have started to enhance their cyber event detection and response capabilities.
242 Organizations are continuously improving their prevention capabilities with modern technology and tools
243 while augmenting their cyber event detection and response capabilities.

244 The increased emphasis on detection and response has an important implication leading to greater
245 awareness of and desire for cyber event recovery. If the assumption is that cyber events will happen, then
246 recovery from those cyber events will also be needed. Recovery has also become more important to

³ Throughout this paper, there are references to the five CSF functions to help organize the material. CSF is one of many informative references that organizations might use to prepare for recovery; see Appendix C for additional examples.

⁴ For more information on the number of cyber events occurring within federal agencies, see Government Accountability Office (GAO) 15-714, September 2015 [1].

247 organizations because of the dependence on information technology (IT) for providing core business
248 capabilities and meeting organizational missions. Organizations need to be prepared at all times to resume
249 normal operations in a secure and timely fashion when cyber events occur.

250 Every organization has experienced some instances of cyber events and performed corresponding
251 recovery actions. Recovery brings together numerous processes and activities throughout the
252 organization, such as business continuity and disaster recovery planning and plan execution.

253 **1.2 Purpose and Scope**

254 The purpose of this document is to support federal agencies in a technology-neutral way in improving
255 their cyber event recovery plans, processes, and procedures, with the goal of agencies resuming normal
256 operations more quickly. This document extends, and does not replace, existing federal guidelines
257 regarding incident response by providing actionable information specifically on preparing for cyber event
258 recovery and achieving continuous improvement of recovery capabilities. It points readers to existing
259 guidance for recovery of information technology.⁵

260 While the scope of this document is US federal agencies, the information provided should be useful to
261 any organization in any industry sector that wishes to have a more flexible and comprehensive approach
262 to recovery.

263 This document is not an operational playbook, but provides guidance to help organizations plan and
264 prepare recovery from a cyber event and integrate the processes and procedures into their enterprise risk
265 management plan. It is not intended to be used as a playbook by organizations responding to an active
266 cyber event, but as a guide to develop their recovery plan in form of customized playbooks prior to the
267 active event. As referred to in this document, a playbook is a plan that documents actionable set of steps
268 an organization can follow to successfully recover from a cyber event. While many fundamental activities
269 are similar for organizations of different size and industry sector, each playbook can focus on a unique
270 type of cyber event and an organization's specific and tailored needs to fit the dependencies of its people,
271 processes, and technology. If an active cyber event is discovered, organizations that do not have in-house
272 expertise to execute a playbook can seek assistance from a trustworthy external party with experience in
273 incident response and recovery, such as through the Department of Homeland Security (DHS) or an
274 Information Sharing and Analysis Organization (ISAO), or a reputable commercial security services
275 provider.

276 **1.3 Audience**

277 This document is intended for individuals with decision making responsibilities related to cyber event
278 recovery. Examples include chief information officers (CIOs), chief information security officers
279 (CISOs), and authorizing officials for systems.

280 **1.4 Document Structure**

281 The remainder of the document is structured as follows:

⁵ Many organizations are also highly dependent upon Operational Technology (OT), including Industrial Control System (ICS) and other Cyber-Physical System (CPS) components, for delivery of services. This white paper is primarily focused upon IT, but the considerations provided may apply to OT and may be useful for planning and execution of OT recovery activities and also the future application of other types of technology, such as that described as the "Internet of Things".

- 282 • Section 2 describes the need for effective recovery planning in advance of a cyber event. The
283 section provides information about improving enterprise resiliency, recovery processes and
284 procedures, recovery communications, and insight sharing.
- 285 • Section 3 provides guidance for achieving continuous improvement of the organization's
286 recovery processes and security posture. It emphasizes the need to validate recovery capabilities
287 using a variety of techniques, including asking personnel for feedback on recovery plans, policies,
288 and procedures, and periodically conducting exercises and tests that address real-world recovery.
- 289 • Section 4 gives examples of recovery metrics that may help organizations to measure their
290 recovery performance and monitor their recovery performance over time.
- 291 • Section 5 summarizes the recommendations introduced in earlier sections to develop a recovery
292 playbook which is composed of a tactical and strategic phase.
- 293 • Section 6 provides an example of a data breach cyber event recovery scenario that demonstrates
294 the application of guidance in earlier sections.
- 295 • Appendix A provides mappings from the recovery processes and activities to the Cybersecurity
296 Framework and related NIST Special Publication (SP) 800-53 security controls.
- 297 • Appendix B provides a list of acronyms and abbreviations that appear in the paper.
- 298 • Appendix C includes a list of external references that will provide additional information for the
299 reader.
- 300

301 2. Planning for Cyber Event Recovery

302 Effective planning is a critical component of an organization’s preparedness for cyber event recovery. As
303 part of an ongoing organizational information security program, recovery planning enables participants to
304 understand system dependencies, critical personnel identities such as crisis management and incident
305 management roles, arrangements for alternate communication channels, alternate services, alternate
306 facilities, and many other elements of business continuity. Planning also enables the organization to
307 explore “what if” scenarios, which might be largely based on recent cyber events that have negatively
308 impacted other organizations, in order to develop customized playbooks. Thinking about each scenario
309 helps the organization to evaluate the potential impact, planned response activities, and resulting recovery
310 processes long before an actual cyber event takes place. These exercises help identify gaps that can be
311 addressed long before a crisis situation, reducing business impact of the gaps. Such scenarios also help to
312 exercise both technical and non-technical aspects of recovery such as personnel considerations, legal
313 concerns, and facility issues.

314 This section describes the importance of cyber event recovery planning, including its integration
315 throughout security operations. This section also provides guidance for improving cyber event recovery
316 planning. The primary purpose of this guidance is to help organizations be better prepared to develop a
317 plan and playbooks to recover from cyber events and thus have greater resiliency. Section 5 provides
318 guidance on developing a playbook, while Section 6 provides a playbook example.

319 2.1 Enterprise Resiliency

320 As IT has become increasingly pervasive, nearly every organization has become highly dependent upon it
321 for delivery of services. Recovering normal operations for these services after a cyber event is often not a
322 binary activity. Organizations must understand how to be resilient, planning how to operate in a
323 diminished capacity or restore services over time based on services’ relative priorities. The DHS Risk
324 Lexicon [4] defines resilience as the “ability to resist, absorb, recover from or successfully adapt to
325 adversity or a change in conditions.” Taking resiliency into consideration throughout the enterprise
326 security lifecycle, everything from planning technology acquisitions and developing procedures to
327 executing recovery and restoration efforts, is critical to minimizing the impact of a cyber event upon an
328 organization. This lifecycle is likely to contain similar elements across most organizations, although the
329 scale and activities within each element may differ depending upon the size and resources of the
330 enterprise.

331 While this document is primarily focused on recovering from a cybersecurity event, it is important to
332 understand that the Cyber Incident Response Plan (CIRP)⁶ should be developed as part of a larger
333 Business Continuity Plan (BCP). The BCP may include other plans and procedures for ensuring minimal
334 impact to business functions, for example Disaster Recovery Plans and Crisis Communication plans.
335 NIST SP 800-61 Revision 2 defines CIRPs as the documents that “establish procedures to address cyber
336 attacks against an organization’s information system(s).” While many publications, including NIST SP
337 800-34 [6], provide useful advice for recovering a single information system or set of systems from
338 natural and manmade events, there is a clear need for organizations to be prepared to recover from a
339 significant cyber event that impacts their core business functions and impact their ability to support their
340 mission.

341 The categories of the CSF Identify function are particularly useful for planning, testing, and implementing
342 the organization’s recovery strategy, including asset management, business environment, governance, risk

⁶ NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* [5], provides guidance on establishing a cyber incident response capability and plan.

343 assessment, and risk management strategy. Among the first steps in planning the recovery strategy is to
344 identify and document the key personnel that will be responsible for defining the recovery criteria and
345 associated plans, and to ensure that all these personnel understand their roles and responsibilities. Note
346 that there may be multiple levels of stakeholders and roles – each organizational tier may need to identify
347 key stakeholders. Responsibilities of these stakeholders may be quite different for a cyber event as
348 compared to a physical event (e.g., a natural disaster).

349 Each organization has a broad array of assets (e.g., people, information, infrastructure, facilities) that
350 enable the governance, management, and use of IT to accomplish the enterprise mission. For recovery
351 planning and execution, the organization needs a reliable source of information regarding its people,
352 process, and technology assets, and the assets of external partners that are connected to or associated with
353 enterprise resources. The organization should create and maintain a complete inventory as reflected in a
354 configuration management database for large organizations or at a minimum a list of the assets that enable
355 it to achieve its mission, along with all dependencies among these assets. This understanding may be
356 informed by several existing planning documents, including Business Impact Analysis (BIA)
357 assessments, Service/Operations Level Agreements (SLAs/OLAs), and Dependency Maps with a
358 particular focus on security dependencies that can administer or operate the asset.

359 While all assets are valuable, they do not all have the same potential impact to the organization if they
360 become unavailable or experience reduced capability. The organization should document and maintain
361 the categorizations of its people, process, and technology assets based upon their relative importance. The
362 prioritization of assets is critical given that many agencies and organizations do not have sufficient
363 resources to protect all assets to the same level of rigor and must prioritize their high-value assets, which
364 must be recovered to support the mission.

365 Many federal information systems are already categorized based upon the criteria in Federal Information
366 Processing Standards (FIPS) 199 and 200 [7]; organizations can add to this by categorizing their other
367 assets as well. Prioritizing resources by their relative importance to meeting the organization's mission
368 objectives is an important driver for determining the sequence and timeline for restoration activities
369 during or after a cyber event. This prioritization also helps the organization to consider categories of
370 recovery events, including cyber events, and to plan appropriate mitigation steps for each category.

371 Understanding recovery objectives relies upon understanding the interdependencies among resources. For
372 example, it is frequently necessary to recover an identity or authentication server before recovering files,
373 messaging, and data stored and processed on servers across the infrastructure. There may also be less
374 obvious dependencies, such as a person taking the result of a computation from system A and mailing it
375 to someone else, who then manually enters it into system B. These dependencies need to be considered
376 when setting objectives for recovery time and establishing the sequence for recovering systems.

377 Furthermore, these dependencies should be categorized by organizational value. Other considerations
378 include applicable regulatory, legal, environmental, and operational requirements. These relationships
379 should be mapped to understand how the organization's critical services are dependent on a tiered
380 structure of support. For example, an organization's electronic mail services may be dependent on
381 Lightweight Directory Access Protocol (LDAP) services and/or network services. If an event causes the
382 LDAP or network services to be degraded, then mail services will likewise be degraded. Similarly, there
383 may be acquisition dependency considerations (alternate facilities, backup communication lines, spare
384 equipment, staffing surge support) that should be included in the planning. By understanding how each
385 service affects the organization's mission or business, staff can prioritize recovery efforts to best optimize
386 resilience.

387 2.2 Recovery Planning Prerequisites

388 The Cybersecurity Framework provides a high-level mechanism for an organization to understand and
389 improve its security posture by building upon capabilities that have already been implemented. The
390 framework functions Identify, Detect, Protect, and Respond all work together in a concurrent manner and
391 directly inform the Recover function. Information gathered and understood in the Identify function can
392 provide a substantial amount of understanding about the organizations systems and the dependencies they
393 require in order to provide business functions to support the mission.

394 Much of the planning and documentation for recovering from a cybersecurity event needs to be in place
395 before the cyber event occurs. The Identify function of the cybersecurity framework helps the
396 organization identify critical systems such as high-value assets – Information on which systems are
397 critical to the organization’s mission that must be recovered first as part of the Response activity. These
398 assets should be identified and assessed prior to an incident in the Identify activity so that the assets and
399 the security dependencies are well understood and correctly prioritized in the recovery guidance and
400 playbook(s). Planning may be informed by threat modeling, as described in draft NIST SP 800-154,
401 *Guide to Data-Centric System Threat Modeling* [8]. This publication describes this activity as “a form of
402 risk assessment that models aspects of the attack and defense sides of a particular logical entity, such as a
403 piece of data, an application, a host, a system, or an environment. The fundamental principle underlying
404 threat modeling is that there are always limited resources for security and it is necessary to determine how
405 to use those limited resources effectively.” The outcome of the threat model exercise helps the
406 organization identify grouping of data, applications, and systems with various level of priorities and
407 criticality. This results in a functional and security dependency map that can help the organization risk
408 management team prioritize the implementation of adequate security protection mechanism, the incident
409 response team react efficiently during a cyber event and identify the root cause when possible, and the
410 recovery team return the business capabilities in a prioritized and orderly manner. Additionally,
411 organizations should evaluate the use of containment principles to isolate access to business resources that
412 do not need to be closely integrated with high value asset (HVA) resources. An example of this
413 containment would be to restrict production workstations used to browse the internet and access email
414 from access or managing the HVAs.

415 Other proactive recovery assessments should help identify and enable the understanding of security
416 dependencies, particularly high value assets. This allows the response team to understand the key
417 components that define the organization’s root(s) of trust in any operational environment:

- 418 • Organizations should have a good understanding of the system boundaries, trust relationships,
419 and identities that exist in their environment. Without clear definition and understanding of
420 identities, it will be difficult to be confident in the effectiveness of a recovery. For example, if a
421 directory is recovered but an adversary has access to an account to manage it, then the adversary
422 can persist access despite the efforts expended during the recovery. The adversary can use any
423 security dependency to persist, such as a service account with administrative privileges, a
424 forgotten/undocumented administrative account, an authorized management tool with installed
425 agents, or a public key infrastructure component used for authentication.
- 426 • Once an organization has a handle on the identities in its environment, it must ensure that they
427 have the proper access controls applied to them, especially in regards to the management and
428 control of the infrastructure. Without well-defined and maintained access control an organization
429 cannot have full confidence that its infrastructure is properly secured. For example, if after
430 recovery an adversary can still access the infrastructure that manages an organization’s
431 environment then they can make changes such that they can exploit the organization again. It is

432 critical that proper access controls are in place for the management of an organization's
433 infrastructure.

- 434 • Data integrity is the key driver and leads to confidence of the data. The organization has
435 implemented sound processes and tools to protect the integrity of the business mission critical
436 data and control and management of the infrastructure data. This will include mechanism to
437 validate the data, monitor and detect it changes, and replication and backup based on
438 organization's defined frequency. Once trust in the management and control data has been
439 established, then the focus can shift to the integrity of the business, customer, employee, and
440 partner data.

441 Without a good understanding of the functional and security dependencies, any tailored recovery plan is
442 less likely to be effective at disrupting and eradicating the adversary.

443 **2.3 Recovery Planning Prerequisites**

444 A critical component of cyber event recovery is having guidance and playbooks that support the asset
445 prioritizations and recovery objectives identified in Section 2.1 and 2.2. This aligns with the first category
446 of CSF's Recover function - Recovery Planning (RC.RP). Recovery planning leads to the development of
447 recovery processes and procedures that are flexible enough to ensure timely restoration of systems and
448 other assets affected by future cyber events, and also comprehensive enough to have modular components
449 for frequently used procedures represented in a playbook, such as reestablishing control of accounts and
450 systems from advanced adversaries. The recommendations presented in this section cover selected aspects
451 of recovery process and procedures planning; the fictional scenarios in Section 6 illustrate how those are
452 helpful during actual recovery activity.

453 **2.3.1 Planning Document Development**

454 A recovery plan provides a method to document and maintain specific strategies and decisions regarding
455 the approved means for implementing and conducting business recovery processes. NIST SP 800-53
456 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [9],
457 includes recovery-relevant controls that apply to all federal systems.

458 While the details of a recovery plan need to be developed by each organization, a typical recovery plan
459 includes the following topics:

- 460 • Service level agreements – Relevant service/operation/organization level agreement details –
461 Information about existing written commitments to provide a particular level of service (e.g.,
462 availability percentage, maximum allowable downtime, guaranteed bandwidth provision). This
463 may include pre-established external engagement contract support that can assist and augment the
464 organization's recovery team in the event of a major cyber event.
- 465 • Authority – Documented name and point of contact information for two or more management
466 staff members who may activate the plan.
- 467 • Recovery team membership – Point of contact information for designated members of the team
468 who have reviewed, exercised, and are prepared to implement the plan.
- 469 • Specific recovery details and procedures – Documented system details that apply to the given
470 information system, with diagrams where applicable. These details may prescribe specific

471 recovery activities to be performed by the recovery team, including application restoration details
472 or methods to activate alternate means of processing (e.g., backup servers, failover site).

473 • Out of band communications – Ability to communicate with critical business, IT, and IT security
474 stakeholders, including external parties like incident response and recovery teams, without using
475 existing production systems, which are frequently monitored by advanced adversaries.

476 • Communication plan – Any specific notification and/or escalation procedures that apply to this
477 information system. As an example, some systems impact users outside of the organization, and
478 legal, public relations, and human resources personnel may need to be engaged to manage
479 expectations and information disclosure about the incident and recovery progress.

480 • Off-site storage details – Details regarding any arrangement for storing specific records or media
481 at an offline or offsite location. This is particularly critical given the credible threat of
482 ransomware that encrypts data and holds the decryption key hostage for payment.

483 • Operational workarounds – Approved workaround procedures if the information system is not
484 able to be restored within the recovery time objective (RTO).

485 • Facility recovery details – Information relevant to resilience of a physical facility such as an
486 office location or a data center. Such details might include personnel notification processes,
487 alternate location information, and communications circuit details.

488 • Infrastructure, hardware, and software – Details regarding access to the infrastructure, hardware,
489 and software to provide intermediary services used during the recovery process. Examples
490 include an identity management system, a recovery network, a messaging system, and a staging
491 system to validate the integrity of recovered data from backups and restore the system in order to
492 instantiate trust in the infrastructure.

493 Cyber event recovery planning may be documented in a recovery plan and/or other organizational plans.
494 For example, NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to*
495 *Federal Information Systems: A Security Life Cycle Approach* [10] describes system security planning
496 documents that may have useful information for recovery planning purposes. NIST SP 800-34 Revision
497 1, *Contingency Planning Guide for Federal Information Systems* [6], details various types of contingency
498 plans, pointing out that “information system contingency planning represents a broad scope of activities
499 designed to sustain and recover critical system services following an emergency event.” The intention of
500 cyber event recovery planning is not to duplicate all of this information in another document, but to
501 ensure that all necessary information is documented, readily accessible, and actionable.

502 **2.3.2 Process and Procedure Development**

503 In accordance with the approved agency-wide information security program, the organization should
504 develop and implement the actual recovery processes that will help ensure timely restoration of
505 capabilities or services affected by cyber events.

506 An approach to this may incorporate:

507 • Recovery guidance and playbook with major phases to include procedures, stages, and well-
508 defined exit criteria for each stage, such as notification of key stakeholders

509 • Specific technical processes and procedures that are expected to be used during a recovery

510 This allows for both a flexible approach that can adapt to different situations as well as the required
511 technical specificity to ensure key actions are carried out in a high quality manner. Procedures should be
512 automated as much as possible to reduce errors in a challenging operating environment, which is typical
513 of recovery operations.

514 Based upon the catalog of services, infrastructures, and applications, and the recovery objectives defined,
515 the recovery planning team should determine specific continuity requirements in order to identify the
516 possible strategic business and technical options. The team may also be able to identify ways in which
517 automation could aid in the recovery. Engaging stakeholders in this activity helps ensure that recovery
518 participants understand their roles, and it also improves repeatability and consistency of recovery
519 processes. In addition to building and improving rapport among the team members, involvement in this
520 modeling will remind business system owners of the realistic threats and help integrate cybersecurity
521 thinking.

522 Part of the recovery planning should include organizational trade-off discussions regarding resource
523 requirements and costs for each strategic technical recovery option. The discussions provide an
524 opportunity to consider how achieving resilience objectives (e.g., 99.99% uptime) occurs at a resource
525 cost (e.g., cost of available spare equipment and/or facilities.) Such discussions may be aided by the
526 application of recovery metrics, described in Section 4 of this document. Additionally, the criticality of
527 the asset to the organization should be included in the trade-off discussions.

528 Recovery teams should integrate specific recovery procedures based upon the processes used within the
529 organization. Such procedures may include technical actions such as restoring systems from clean
530 backups, rebuilding systems from scratch, enhancing the identity management system and trust boundary,
531 replacing compromised files with clean versions, installing patches, changing passwords, and tightening
532 network perimeter security (e.g., firewall rulesets, boundary router access control lists). Procedures may
533 also include non-technical actions that involve changes to business processes, human behavior and
534 knowledge, and IT policies and procedures.

535 Effective recovery will include ongoing use and improvement of both technical and non-technical actions.

536 **2.3.3 Determination of Recovery Initiation/Termination Criteria and Goals Security**

537 Depending on the severity and nature of the incident and recovery operations, the decision to initiate
538 recovery processes may not be made by the recovery personnel, but by the organization's incident
539 response team, CISO, business owners, and/or other personnel involved in decision making for
540 addressing cyber events. Agreement and coordination of this criteria, especially involving timing, is
541 critically important to achieving successful recovery. For example, starting recovery before the
542 investigation response has achieved key understandings of the adversary's footprint and objective may
543 alert the adversary that an infiltration has been discovered, triggering a change in tactics that would defeat
544 the recovery operation. Such a change could mean the loss of indicators and visibility of the adversary's
545 activities, resulting in a reduced ability to discover impacted resources.

546 A coordinated response will help achieve a balance between effective forensic investigation and business
547 service restoration. This balance is a unique decision based on the balance between identification of the
548 root cause analysis and rapid restoration of services and systems to operational status. To achieve that
549 balance, the organization should formally define and document the conditions under which the recovery
550 plan is to be invoked, who has the authority to invoke the plan, and how recovery personnel will be
551 notified of the need for recovery activities to be performed.

552 As described above, full recovery or restoration may not be the immediate goal. Achieving resilience
553 might mean that a given resource is able to continue operation in a diminished capacity, such as during a

554 denial of service attack or a destructive attack on a group of systems. Resilience can also mean containing
555 adversary access or damage to a contained set of resources or limiting reputational and brand damage of
556 the organization. Organizational recovery teams may be able to learn from internal resources (or through
557 external partners, such as the United States Computer Emergency Readiness Team (US-CERT) or Sector
558 Coordinating Councils) specific methods for successfully absorbing or adapting to adverse conditions.
559 Such a solution might include an alternative or a partial restoration as an interim measure. In complex
560 situations, recovery may have many levels, and while operational status should be progressing back to
561 normal, occasionally a step backward will be needed before achieving other steps forward, such as taking
562 a key system offline to perform recovery measures before conducting recovery actions on other systems.

563 Organizations should define key milestones for meeting intermediate recovery goals and terminating
564 active recovery efforts. Frequently, it is not possible or practical to achieve 100 percent recovery in a
565 timely fashion, such as determining which offline virtual machine images have been compromised and
566 should be replaced with clean backups. It is recommended to put security controls in place to
567 automatically identify affected systems in the future and alert personnel so that recovery and any other
568 necessary actions can be initiated. An organization in such a situation might declare this recovery
569 operation to be terminated when this automated system is in place, pending discovery of another active
570 incident. Section 4 provides a more detailed discussion of metrics related to recovery initiation,
571 intermediate goals, and termination.

572 **2.3.4 Root Cause and Containment Strategy Determination**

573 Identifying the root cause(s) of a cyber event is important to planning the best response, containment, and
574 recovery actions. While knowing the full root cause is always desirable, adversaries are incentivized to
575 hide their methods, so discovering the full root cause is not always achievable.

576 Before execution of recovery efforts start in earnest, the investigation should achieve two key objectives
577 to be considered sufficient:

- 578 • Basic knowledge of the adversary's objective (access specific data, systems, or communications)
579 or incident response subject matter expert (SME) confirmation that the adversary's objective is
580 not apparent.
- 581 • High confidence in either understanding the technical mechanisms the adversary is using to
582 persist access to the environment or confirming non-persistence intent. Most targeted attacks that
583 are part of a large campaign involve multiple types of well-concealed persistence mechanisms.

584 Without these objectives being met during the investigation, the recovery procedure has a high chance of
585 being ineffective or inefficient (in terms of resources and other costs). The investigation for the final root
586 cause may continue in parallel to the recovery after these objectives have been met, as the adversary may
587 change or evolve tactics and persistence mechanisms. Note that some scenarios such as ransomware or
588 extortion threats of system and information destruction may impose an external deadline on achieving
589 these objectives, forcing the organization to use incomplete information for the objectives in the recovery.

590 Organizations should adjust their incident detection and response policies, processes, and procedures to
591 emphasize sufficient root cause determination. While the search for the root cause may continue
592 separately, there are instances where recovery will be initiated before that cause is determined. Effective
593 recovery depends on ensuring that all portions of a cyber event are addressed, so if one or more
594 vulnerabilities or misconfigurations are overlooked (e.g., compromised account credentials used to restore
595 critical services), the recovery personnel may inadvertently leave weaknesses in place that adversaries can
596 immediately exploit again. Elimination and containment failures might permit portions of a compromise

597 to remain on the organization's systems, causing further damage without the adversary even acting. The
598 investigation of root cause can also be valuable in identifying previously unknown systemic weaknesses
599 that should be addressed throughout the enterprise. An example of this is a previously unknown access
600 path to an asset via a security dependency like a system management tool or security scanning service
601 account.

602 Once a resource is targeted and attacked, it is often targeted again or other resources within the
603 organization are attacked in a similar manner. Once organizations detect an attack, they should deploy
604 protection, detection, and response processes to other interconnected systems in the organization, as well
605 as the affected systems, to minimize the attack's propagation across the infrastructure. The speed with
606 which this response needs to occur should be set through business risk-based decision making that takes
607 into account the potential negative impact of disrupting operations versus the risk of the systems being
608 compromised. Containment can help isolate the adversary from the untrusted assets and potentially isolate
609 compromised assets from recovered or rebuilt assets.

610 **2.4 Recovery Communications**

611 Planning for and implementing effective recovery communications are critical success factors for
612 achieving organization resilience. This is included in CSF category Recovery Communications (RC.CO),
613 which has the following described outcome: "Restoration activities are coordinated with internal and
614 external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems,
615 victims, other CSIRTs, and vendors." Recovery communications includes non-technical aspects of
616 resilience such as management of public relation issues and organizational reputation.

617 The recovery team should develop a comprehensive recovery communications plan. Effective
618 communications planning is important for numerous reasons, including:

- 619 • Statements made in the heat of recovery may have significant legal and/or regulatory impact and
620 must be worded carefully. Understanding, from a legal perspective, what may be said to whom
621 and when will require extensive planning and advance discussion. There may be specific
622 requirements regarding what may be released to outside organizations, including the media.
- 623 • Key stakeholders need to know sufficient information so that they understand their
624 responsibilities during the recovery stage and can maintain confidence in the recovery team's
625 abilities. Planning, testing, and ongoing improvement will help define the appropriate messaging
626 for each type of stakeholder (e.g., external partner, customer, manager).
- 627 • Individual members of the recovery team may not have sufficient information to provide accurate
628 and timely reporting of recovery status and activities. For example, while the team may
629 understand that a recovery time objective will be missed, members may not be aware of a manual
630 workaround being implemented. Agreement in advance on who will report information to whom
631 is a critical aspect of the communications plan.

632 For these reasons, teams need to plan in advance for recovery communications and ensure that lessons
633 learned from internal and external events are integrated into the improvement processes. Communications
634 considerations should be fully integrated into recovery policies, plans, processes, and procedures. The
635 recovery team should consider establishing guidelines regarding what information may and/or should be
636 shared with each type of constituent. For example, providing too much information or inaccurate
637 information may do more harm than good, and insufficient information sharing could lead to further harm
638 to the organization's reputation. When updates are being delivered to enable decision making, the updates

639 should contain the necessary actionable information that will help the organization more effectively reach
640 the ultimate goal of resuming normal operations and maintaining that state.

641 Recovery teams should consider specific types of stakeholders in regard to communications planning,
642 including internal personnel (various IT teams, incident response personnel, senior management, business
643 unit owners, legal, human resources, privacy representatives, board of directors, etc.) and external parties
644 (computer security incident response teams (CSIRTs), business partners, customers, regulators, credit
645 reporting agencies, law enforcement, press/media, analysts, insurers, etc.) The organization should ensure
646 that current points of contact for each type of stakeholder are established and maintained to minimize
647 delays during the recovery process. It is important to note that for effective recovery, communications
648 should occur continuously across the tactical and strategic phases.

649 Some methods of communications may be unavailable (or undesirable) during recovery activities. For
650 example, if the network has been compromised, email communications may be unwise. Recovery teams
651 should be prepared for alternate means of secure and reliable communication, and should practice such
652 scenarios as part of ongoing improvement.

653 **2.5 Sharing Recovery Insights**

654 As stated in draft NIST SP 800-150, *Guide to Cyber Threat Information Sharing* [11], organizations are
655 encouraged to share actionable information about cyber threats with other organizations. For example, an
656 organization that has just recovered from a major new threat could document its recovery steps and share
657 them with others so that those organizations could recover from the same threat or similar threats much
658 more quickly, or in some cases could detect cyber events more quickly and perhaps prevent them
659 altogether. Sharing recovery insights has become necessary in response to adversaries sharing their
660 methodologies, tools, and other information with each other for mutual benefit. Organizations can
661 similarly benefit by sharing recovery information.

662 Organizations should not share recovery information until after they have performed the necessary
663 planning and preparation activities, such as defining their information sharing goals, objectives, and
664 scope, and establishing information sharing rules. See NIST SP 800-150 for more information on
665 planning and preparatory activities.

666 **2.6 Summary of Recommendations**

667 The following are the key recommendations presented throughout Section 2:

- 668 • Understand how to be prepared for resilience at all times, planning how to operate in a
669 diminished capacity or restore services over time based on their relative priorities.
- 670 • Identify and document the key personnel who will be responsible for defining recovery criteria
671 and associated plans, and ensure these personnel understand their roles and responsibilities.
- 672 • Create and maintain a list of the people, process, and technology assets that enable the
673 organization to achieve its mission (including external resources), along with all dependencies
674 among these assets. Document and maintain categorizations for these assets based on their
675 relative importance and interdependencies to enable prioritization of recovery efforts.
- 676 • Develop comprehensive plan(s) for recovery that support the prioritizations and recovery
677 objectives, and use the plans as the basis of developing recovery processes and procedures that
678 ensure timely restoration of systems and other assets affected by future cyber events. The plan(s)

- 679 should ensure that underlying assumptions (e.g., availability of core services) will not undermine
680 recovery, and that processes and procedures address both technical and non-technical activity
681 affecting people, processes, and technologies.
- 682 • Develop, implement, and practice the defined recovery processes, based upon the organization's
683 recovery requirements, to ensure timely recovery team coordination and restoration of capabilities
684 or services affected by cyber events.
 - 685 • Formally define and document the conditions under which the recovery plan is to be invoked,
686 who has the authority to invoke the plan, and how recovery personnel will be notified of the need
687 for recovery activities to be performed.
 - 688 • Define key milestones for meeting intermediate recovery goals and terminating active recovery
689 efforts.
 - 690 • Adjust incident detection and response policies, processes, and procedures to ensure that recovery
691 does not hinder effective response (e.g., by alerting an adversary or by erroneously destroying
692 forensic evidence).
 - 693 • Develop a comprehensive recovery communications plan, and fully integrate communications
694 considerations into recovery policies, plans, processes, and procedures.
 - 695 • Clearly define recovery communication goals, objectives, and scope, including information
696 sharing rules and methods. Based upon this communications plan, consider sharing actionable
697 information about cyber threats with relevant organizations, such as those described in NIST SP
698 800-150.

699 **3. Continuous Improvement**

700 Cyber event recovery planning is not a one-time activity. The plans, policies, and procedures created for
701 recovery should be continually improved by addressing lessons learned during recovery efforts⁷ and by
702 periodically validating the recovery capabilities themselves. This is reflected in CSF category
703 Improvements (RC.IM), which states, “Recovery planning and processes are improved by incorporating
704 lessons learned into future activities.” Similarly, recovery should be utilized as a mechanism for
705 identifying weaknesses in the organization’s technologies, processes, and people that should be addressed
706 to improve the organization’s security posture and the ability to meet its mission. Since the outcome of
707 these types of identifications will help define long-term goals for the organization, continuous
708 improvement of the recovery plan is part of the strategic phase. This section provides insights into
709 improving an organization’s recovery capabilities and security posture.

710 **3.1 Validating Recovery Capabilities**

711 Validating recovery capabilities refers to ensuring that the technologies, processes, and people involved in
712 recovery efforts are well prepared to work together to effectively and efficiently recover normal business
713 operations from disruptive cyber events.

714 There are several ways to validate recovery capabilities. The simplest method is to ask all of the
715 individuals who may be involved in response efforts to provide input on the recovery plans, policies, and
716 procedures. Although these documents should have already taken into account pertinent information and
717 insights provided by key business owners and IT staff members, many other individuals may have
718 responsibilities involving response efforts that are affected by these documents. In particular, the
719 individuals who will participate in hands-on recovery efforts should have the opportunity to review the
720 recovery documents related to their areas of responsibility so that they can comment on how realistic the
721 expectations are and what their primary concerns are. For example, an individual may lack the tools or
722 training to recover a particular system within the expected time period. The appropriate personnel should
723 then decide how to best address these concerns.

724 In some cases, recovery concerns can be addressed by conducting exercises or tests. Exercises and tests
725 should be performed periodically to help the organization’s real-world recovery capabilities, building
726 organizational “muscle memory” and identifying areas for improvement. Although it is tempting to avoid
727 tests in favor of exercises because of the possible disruption that tests can cause to operations, it is
728 generally much better to identify an unexpected operational issue during testing than during an actual
729 cyber event because more resources should be available to address the issue during testing. Some
730 organizations have found it helpful to intentionally introduce system failures as part of daily operations to
731 ensure that participants are always resilient and ready for a cyber event. An example of a potential test is
732 disconnecting a critical system with high availability to ensure that failover occurs gracefully, with
733 operations automatically switching to a hot spare. Organizations should use a combination of exercises
734 and tests for recovery capability validation.

735 Recovery teams should practice a realistic scenario in a table top exercise where at least one member of
736 each team is part of the adversary group that provides realistic obstacles and complexities for the defense
737 and recovery team to navigate. Another practice is to use a newly discovered cyber event scenario
738 described in the news to develop or customize a playbook exercising the recovery plan documentation.
739 Adding realism like this will increase visibility of gaps in the organization proactively that can be
740 resolved as part of continuous improvement to increase effectiveness in a real incident recovery.

⁷ For more information on this, see the CSF Recovery function named Improvements (RC.IM).

741 Exercises and tests can provide several benefits related to recovery, including the following:

- 742 • The exercise or test itself will remind participants of known risk scenarios and help them consider
743 what actions they might take in a real cyber event.
- 744 • Exercise and test results will help confirm or refute assumptions that were made in planning,
745 particularly regarding how realistic the recovery targets are.
- 746 • Exercises and tests will spotlight gaps and inefficiencies in the processes that should be addressed
747 to ensure smooth responses in real-world cyber events.
- 748 • Personnel, especially those with new recovery-related responsibilities, will receive training
749 through exercises and tests in recovery practices.

750 Recovery exercises and tests should be formally implemented at a frequency that makes sense for the
751 organization, and the results should be recorded to help inform organizational cybersecurity activities.
752 Organizations should set realistic objectives, with specific roles and responsibilities, for exercising and
753 testing recovery capabilities to verify their ability to adequately manage cybersecurity risk. It may also be
754 helpful to get assistance from a trustworthy external party with experience in such exercises, such as
755 through DHS or an Information Sharing and Analysis Organization (ISAO).

756 An important aspect of improving recovery processes and procedures is a realistic and comprehensive
757 review of the results of the exercise or test. By understanding what worked and what did not, the recovery
758 planners can identify areas for improvement, not only in the specific plan being tested but also in the
759 planning processes themselves. As identified by the COBIT 5 Framework [12], the following may result
760 from a post-exercise or post-test debrief:

- 761 • Validate assumptions made regarding current business operational and strategic objectives.
- 762 • Consider whether a revised business impact assessment may be required.
- 763 • Recommend and communicate changes in policy, plans, procedures, infrastructure, and roles and
764 responsibilities for management approval and processing via the change management process.
- 765 • Review the recovery plan to consider the impact of new or major changes to enterprise
766 organization, business processes, outsourcing arrangements, technologies, infrastructure,
767 operating systems, and application systems.
- 768 • Define and maintain training requirements and plans for those performing continuity planning,
769 impact assessments, risk assessments, media communication, and incident response.
- 770 • Ensure that the training plans consider frequency of training and training delivery mechanisms.
- 771 • Develop competencies based on practical training, including participation in exercises and tests.
- 772 • Monitor skills and competencies based on the exercise and test results.

773 The following resources may be useful for gaining a better understanding of exercises and tests:

- 774 • NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
775 [13]

- 776 • NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems* [6]
- 777 • NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* [14]
- 778 • NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* [5]

779 **3.2 Improving Recovery and Security Capabilities**

780 In addition to identifying potential improvements to recovery capabilities through reviews by personnel
781 and periodic tests and exercises, organizations should also identify improvements from lessons learned
782 during actual cyber event recovery actions. These lessons learned help drive improvements not only to
783 recovery itself, but also to the organization's security operations, policies, etc.

784 Improvements to the recovery capabilities themselves should be documented by measuring and analyzing
785 current and past cyber event recovery efforts to identify the most important issues, such as major
786 problems that caused significant delays in recovery or minor problems that occurred repeatedly. To gain
787 the most benefit, analysis should consider events' impact on the enterprise rather than just on individual
788 systems. The organization should then determine how available resources can best be spent to address
789 these issues. In some cases, the organization can adapt approaches to these issues previously taken by
790 other organizations.

791 Improving the organization's security posture by analyzing lessons learned from actual cyber event
792 recovery actions takes two forms. Short-term improvements can be achieved through identification of
793 low-level issues, such as a particular system not being patched often enough, which enabled it to be
794 compromised while other similar systems stayed secure. Long-term improvements to the organization's
795 security posture can be achieved through identification of high-level issues, such as providing inputs on
796 commonly seen system security issues to organizational risk assessment and management activities,
797 which in turn inform the enterprise information security program. This can lead to the acquisition of new
798 security technologies, the redesign of operational processes, or the initiation of other major changes to
799 how the organization conducts and secures its operations.

800 The individuals participating in recovery actions may find it challenging to balance the need to restore
801 normal operations quickly with the need to immediately document issues they encounter instead of
802 documenting such issues after recovery concludes. The former expedites the resolution of the current
803 cyber event, while the latter may help expedite the resolution of future cyber events and potentially
804 prevent some cyber events from ever occurring in the first place. Individuals should strive to document
805 issues to the extent necessary during recovery so that they have enough information to expand on their
806 documentation later in the recovery process or immediately after recovery is achieved. The longer
807 individuals wait to document lessons learned, the less likely it is that the lessons learned will be
808 documented accurately and completely.

809 **3.3 Summary of Recommendations**

810 The following are the key recommendations presented throughout Section 3:

- 811 • Gather feedback for the recovery plans and capabilities from those stakeholders that will have a
812 role in recovery activities.
- 813 • Formally implement cyber event recovery exercises and tests at a frequency that makes sense for
814 the organization, recording the results to help inform organizational cybersecurity activities.
815 These events should include realistic objectives, with specific roles and responsibilities, for

- 816 exercising and testing recovery capabilities to verify the ability to adequately manage
817 cybersecurity risk.
- 818 • Continually improve cyber event recovery plans, policies, and procedures by addressing lessons
819 learned during recovery efforts and by periodically validating the recovery capabilities
820 themselves.
 - 821 • Use recovery as a mechanism for identifying weaknesses in the organization's technologies,
822 processes, and people that should be addressed to improve the organization's security posture and
823 the ability to meet its mission.
 - 824 • At a minimum, validate recovery capabilities by soliciting input from individuals with recovery
825 responsibilities and conducting exercises and tests.
 - 826 • Strive to have recovery personnel document issues to the extent necessary during recovery so that
827 they have enough information to expand on their documentation later in the recovery process or
828 immediately after recovery is achieved.

829 4. Recovery Metrics

830 Throughout the process of planning, exercising, and executing recovery activities as described in earlier
831 sections, the collection of specific metrics may help improve recovery and inform continuous
832 improvement. It may be beneficial to determine these metrics in advance, both to understand what should
833 be measured and to implement the processes to collect relevant data. This process also requires the ability
834 to determine where the metrics that have been identified can be most beneficial to the recovery activity
835 and identify which activities cannot be measured in an accurate and repeatable way. It is important that
836 restoring business functions remains the primary task at hand, while the collection of recovery metrics is
837 designed in a way such that the metric data is an automated output of the recovery activities. Metrics can
838 be detrimental to recovery if they hinder the recovery process, cause a rushed/incomplete investigation, or
839 create additional obstacles for recovery team efficiency. It is critical to ensure metrics provide useful
840 information that supports actionable improvement without being detrimental to recovery.

841 The majority of recovery metrics will be used to improve the quality of recovery actions within the
842 organization, such as to improve specific aspects or to perform a cost/benefit analysis of a particular
843 approach. Other metrics might be used as part of compulsory reporting (such as in response to an inquiry
844 from an external authority) or for information sharing (such as might be responsibly shared with US-
845 CERT). In each case, determining in advance what will be measured and which measures may be shared
846 will aid the organization's recovery efforts. As with the previously described communications plans,
847 sharing of metrics must be done with caution and should occur only with the approval of appropriate
848 organizational stakeholders, including senior managers, legal representatives, and regulatory compliance
849 personnel.

850 Organizations should decide when and how to use metrics during recovery because they can be either a
851 benefit or a hindrance. For well-defined and repeatable activities, metrics can help measure progress as
852 well as provide valuable feedback to improve the activity. For example, the replacement of user laptops
853 because of a malware infection may be commonplace and routine within a large organization. The
854 organization will have a well-defined process for recovering from the malware infection on a single
855 laptop, and metrics can be used to measure the time, cost, and other important information. On the other
856 hand, for events that are anomalous there might not be well-defined recovery procedures, so there would
857 not be predefined metrics to use. In this case, it could be unclear which metrics to gather, or metrics could
858 be misused, leading to a false sense of recovery. Because of these different types of situations,
859 organizations should give careful consideration as to when and how they will use recovery metrics.

860 Many organizations also face major incidents where adversaries gain full administrative access to most or
861 all IT assets in the enterprise during the course of the attack. The value of metrics in these cases may be
862 diminished, as these types of events should be rare once effective defenses and responses are
863 implemented. In the most extreme instances, a cyber event may be so severe that the issue is
864 unrecoverable and results in the loss of the financial viability of the organization itself. While such
865 occasions may be rare, it may be helpful for the organization to determine a "point of no return".

866 The following table provides some considerations regarding aspects of cyber event recovery, describing a
867 general area to be measured and some example metrics (e.g., cost, time, damage assessment, number of
868 incidents). It is important to note that resilience is a highly subjective area of cybersecurity, so comparing
869 recovery metrics among organizations or even within a single entity may produce misleading results.

870

Table 4-1: Example Recovery Metrics

Recovery Area	Example Metrics
<p>Assessing Incident Damage and Cost Consider both direct and indirect costs; recovery damage and costs may be important evidence as part of a legal action.</p>	<ul style="list-style-type: none"> • Costs due to the loss of competitive edge from the release of proprietary or sensitive information • Legal costs • Hardware, software, and labor costs to execute the recovery plan • Costs relating to business disruption such as system downtime (for example, lost employee productivity, lost sales, etc.) • Other consequential damages such as loss of brand reputation or customer trust from the release of customer data
<p>Organizational Risk Assessment Improvement</p>	<ul style="list-style-type: none"> • Frequency and/or scope of recovery exercises and tests • Number of significant IT-related incidents that were not identified in risk assessment • System dependencies accurately identified • Identified gaps during the recovery exercises or tests that help inform and drive the improvement in the other functions of the CSF
<p>Quality of Recovery Activities</p>	<ul style="list-style-type: none"> • Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of IT services meeting uptime requirements • Percent of successful and timely restoration from backup or alternate media copies • Number of recovery efforts that have achieved recovery objectives

871

872 **5. Building the Playbook**

873 The information gathering and planning activities the organization has conducted provide a substantial
874 understanding of the mission supporting information systems as well as any dependencies, and intricacies
875 surrounding them. A foundational understanding of all of this information is critical for business
876 functions to remain operational when operating under normal conditions. In the event of a cybersecurity
877 event, this information becomes even more paramount, and these processes and procedures need to be
878 presented in an actionable manner in order to effectively restore business functions quickly and
879 holistically. The playbook is a way to express tasks and processes required to recover from an event in a
880 way that provides actions and milestones specifically relevant for each organizations systems.

881 This section summarizes the recommendations described in the previous sections. The goal is to to
882 provide a consolidated list of items that can be included in a playbook. The recovery activities can be
883 organized in two phases. The initial and tactical recovery phase is largely achieved through the execution
884 of the playbook developed as part of the planning efforts for cyber event recovery, which not only
885 prepares the organization for the recovery actions themselves, but also depends on the activities
886 performed during the protection, detection, and response functions of the enterprise risk management
887 lifecycle process. The actions can be organized into initiation, execution, and termination stages. The
888 second phase is more strategic; it focuses on the continuous improvement of the organization risk
889 management process lifecycle driven by the recovery activities. The second phase focuses on reducing the
890 organization's attack surface and minimizing cyber threats. The actions can be further organized into the
891 planning and execution stage, metrics stage, and recovery improvement stage. The lessons learned
892 identify the gaps and help inform the planning and execution of the other CSF functions.

893 The tactical recovery phase will depend on performing the following actions before and during the cyber
894 event:

- 895 • Create and maintain a list of the people, process, and technology assets that enable the
896 organization to achieve its mission (including external resources), along with all dependencies
897 among these assets. The creation of a map or diagram of the dependencies will help in planning
898 the order of restoration.
- 899 • Document and maintain categorizations for all assets based on their relative importance and
900 interdependencies to confidently prioritize recovery efforts.
- 901 • Identify and document the key personnel who will be responsible for defining recovery criteria
902 and associated plans, and ensure these personnel understand their roles and responsibilities.
- 903 • Ensure that the correct underlying assumptions (e.g., availability of core services, trustworthiness
904 of directory services, adversary's motivation is well understood) are made during the initiation of
905 the recovery in order to prevent an ineffective recovery.
- 906 • Define and document the conditions under which the recovery plan is to be invoked, who has the
907 authority to invoke the plan, and how recovery personnel will be notified of the need for recovery
908 activities to be performed. Additionally, define key milestones, intermediate recovery goals, and
909 criteria for finalizing active recovery efforts.
- 910 • Ensure initial restoration planning addresses the need for the recovery efforts to be tactical in
911 nature in order to prevent recovery from negatively affecting the incident response (e.g., by
912 alerting an adversary or by erroneously destroying forensic evidence).

- 913 • Examine the cyber event to determine the extent that recovery must be carried out, and initiate the
914 corresponding plan for recovery accordingly.
- 915 • Develop a comprehensive recovery communications plan, while clearly defining recovery
916 communication goals, objectives, and scope, including information sharing rules and methods.
917 Based upon this communications plan, consider sharing actionable information about cyber
918 threats with relevant organizations, such as those described in NIST SP 800-150.
- 919 • Gather feedback for the recovery plans and capabilities from those stakeholders that will have a
920 role in recovery activities.
- 921 • Formally implement cyber event recovery exercises and tests at a frequency acceptable for the
922 organization. These events should include realistic objectives, with specific roles and
923 responsibilities, for exercising and testing recovery capabilities. Based on the results of these
924 recovery activities the organizations should update cyber event recovery plans, policies, and
925 procedures. They should also use the information learned from recovery activities to improve the
926 organization's cybersecurity posture, ensuring the ability to meet its mission.
- 927 • Vet recovery capabilities by soliciting input from individuals with recovery responsibilities and
928 conducting exercises and tests.
- 929 • Execute the tailored playbook that has been created during the cyber event.
- 930 • Continually document issues during recovery so that there is enough information to expand on
931 documentation and improve capabilities later in the recovery process or immediately after
932 recovery is achieved.
- 933 • Implement monitoring for events, signatures, etc. to alert the organization about known malicious
934 behavior. Monitor the artifacts and evidence found during detection and response. This
935 monitoring will extend into the strategic phase.
- 936 The strategic recovery phase will depend on performing the following actions before and during the cyber
937 event:
- 938 • Develop and implement an improvement plan for the organization's overall security posture
939 based on tactical phase results.
- 940 • Continually execute communications plans to inform appropriate internal and external
941 stakeholders of the progress of the recovery effort. Internal stakeholders should be notified of any
942 improvements that need to be made to people, processes, and procedures, while external
943 stakeholders will need to be notified of any impact to them.
- 944 • Review defined milestones, goals, and metrics gathered throughout the tactical phase. This
945 information can help quantify the effectiveness of the recovery effort, as well as identify areas
946 that need improvement.
- 947 These actions are general recommendations that can be tailored in order to fit each organization's specific
948 requirements. The next section applies these recommendations in a data breach cyber event recovery
949 scenario.

950 **6. An Example of a Data Breach Cyber Event Recovery Scenario**

951 This section presents a scenario that illustrates how, using the guidelines provided in earlier sections of
952 this document, organizations can effectively recover from cyber events and subsequently use information
953 gained during recovery to improve cybersecurity processes. The scenario is not meant to be all inclusive
954 or exhaustive of cyber events, but to provide a means to demonstrate how to apply the document's
955 recommendations for a specific situation.

956 This scenario describes an organization that has experienced a breach of its network. Anomalous activity
957 was detected during recent log reviews, indicating that a malicious actor used stolen credentials to gain
958 access to one or more critical business and IT infrastructure systems. While the method of entry and the
959 specific type of attack are not directly relevant to the recovery team, it is important to note that such a
960 breach jeopardizes the trustworthiness of the business unit and IT management systems.

961 For this scenario, network monitoring equipment confirms that a significant amount of personally
962 identifiable information (PII) has been exfiltrated. Additionally, there is the possibility that customer
963 financial data has been stolen.

964 **6.1 Pre-Conditions Required for Effective Recovery**

965 The organization understood the need to be prepared and conducted planning to operate in a diminished
966 condition. The recovery plan includes the following critical elements:

- 967 • Development of a set of formal recovery processes;
- 968 • Determination of the criticality of organizational resources (e.g., people, facilities, technical
969 components, external services) that are required to achieve the organization's mission(s);
- 970 • Creation of functional and security dependency maps that helps to understand the order of
971 restoration priority;
- 972 • Identification and selection of technology and key personnel who will be responsible for defining
973 and implementing recovery criteria and associated plans;
- 974 • A comprehensive recovery communications plan with fully integrated internal and external
975 communications considerations, including information sharing criteria informed by
976 recommendations in NIST SP 800-150 [11]; and
- 977 • Periodic training and exercises to practice the defined recovery processes, based upon the
978 organization's recovery requirements, to ensure timely recovery team coordination and
979 restoration of capabilities or services affected by cyber events.

980 Because the organization has formally implemented cyber event recovery exercises and tests with realistic
981 scenarios and clear roles and responsibilities, the organization is prepared to tackle the recovery task with
982 limited assistance from external entities.

983 **6.2 Tactical Recovery Phase**

984 The following steps summarize the activities of the recovery team in the tactical recovery phase.

985 6.2.1 Initiation

- 986 • The incident response team informs the recovery team about the event.
- 987 • The recovery team meets to determine the criticality and impact of the cyber event to formulate
988 an approach and set of specific actions.
- 989 • Understanding that initiation of the recovery might alert the adversary, planning and tactical
990 recovery operations such as monitoring are increased. This is accomplished by heightening the
991 network defenses to look for lateral movements based a set of indicators of compromises that
992 have been generated by the incident response team. This helps validate the adversary's presence
993 on impacted systems.
- 994 • The incident response and recovery teams work collaboratively to understand the adversary's
995 motivation and identify the adversary's footprint on the infrastructure, command and control
996 channels, and tools and techniques.
- 997 • Based upon the criteria in the recovery playbook, the defined personnel determine that the
998 recovery process is ready to begin because the team has a good understanding of the situation. All
999 parties defined in the playbook are informed that the recovery activities have been initiated.
- 1000 • It was determined that network-based communications (e.g., email) may be insecure and cannot
1001 be trusted. The team agrees to use in-person meetings and telephone conversations as alternate
1002 means of communication.
- 1003 • The recovery team is briefed by the incident response team and understands which accounts and
1004 systems have been compromised. Without alerting the adversary, the team is able to contain them
1005 and regain control of the underlying management infrastructure.
- 1006 • Based on prioritization of mission critical systems, the recovery team determines the order in
1007 which systems will be restored. The team uses the dependency map to build the restoration plan.
- 1008 • The backup hardware, software, and data are inventoried, and responsible personnel are
1009 accounted as reflected in the recovery plan.

1010 6.2.2 Execution

- 1011 • The recovery team begins to execute the restoration by validating and implementing remediation
1012 countermeasures in coordination with the incident response team and other information security
1013 personnel to ensure that the underlying system weaknesses are not re-introduced, and to minimize
1014 the likelihood that the adversary can pivot within the organization. High-value assets are the key
1015 components and are handled first.
- 1016 • The organization continues to execute its recovery plan, restoring additional business services and
1017 communicating, in accordance with the pre-existing communications criteria and in coordination
1018 with the legal and public affairs offices, regarding the restoration status.
- 1019 • During restoration, the recovery team tracks the actual time that critical services were unavailable
1020 or diminished, comparing the actual outage with agreed-upon service levels and recovery times.
1021 Organizational managers are advised regarding objectives that may not or will not be

1022 accomplished, and the team considers the impact so that proactive actions may take place (e.g.,
1023 routing traffic to a pre-arranged alternate service provider with pre-approved notification pages.)

1024 • Designated staff document any issues that arise, and newly identified dependencies, to help
1025 expand on documentation later in the recovery process or immediately after recovery is achieved.
1026 Indicators of compromises are continuously captured, updated, and documented. Restoration
1027 techniques, tools, and procedures are customized and refined to the current cyber event.

1028 • While the services are being restored, other members of the recovery team work with business
1029 unit managers and senior leadership, in coordination with representatives from HR and legal, to
1030 discuss appropriate notification activities. Using the pre-agreed recovery communications plan,
1031 the team drafts notices for employees, for customers affected by financial and/or privacy
1032 information leaks, and for the public. As a critical component of this step, additional surge
1033 support has been added to the customer support center and customers are kept abreast of the
1034 status of recovery, sharing status accurately while abiding by the pre-agreed decisions regarding
1035 what information may be shared with whom, and when.

1036 • Additional recovery steps are initialized, including external interactions and services such as pre-
1037 arranged credit monitoring services and additional customer support staff, to help restore
1038 confidence and to protect constituents.

1039 • The recovery team asks the Security Operations Center (SOC) and in particular the incident
1040 response team and external subject matter experts to confirm that the newly rebuilt servers are not
1041 susceptible to the original issue and are ready to be restored to service. The team validates the
1042 restored assets are fully functional and meet the security posture required by the organization
1043 security team before it receives approval to restore network operations and make the servers
1044 publicly available.

1045 **6.2.3 Termination**

1046 • The personnel determine that termination criteria have been met, declares the end of the tactical
1047 recovery event, and confirms, in consultation with business/system owners, that restoration has
1048 fully occurred.

1049 • The team stands down and staff returns to executing their normal job functions.

1050 • The SOC continues to monitor the infrastructure for potential persistency of malicious activities
1051 and continue to inform the incident response and recovery team. The goal is to make sure the
1052 organization has fully eradicated the adversary from the infrastructure and has exclusive control
1053 of the operational environment.

1054 • The recovery team finalizes the metrics collected during the event.

1055 **6.3 Strategic Recovery Phase**

1056 The following steps summarize the activities performed during the strategic recovery phase.

1057 **6.3.1 Planning and Execution**

1058 • The recovery continues to support the various communication teams as they interact within the
1059 internal users and public customers.

- 1060 • The recovery teams close the loop with the external entities who have been involved during the
1061 tactical phase.
- 1062 • A plan is developed to include longer-term goals that have to be met to fully correct the root
1063 causes. These actions will involve vetting and approval from the management, business units, and
1064 IT teams, as they will include changes in the business workflows, the IT architecture, and
1065 operation of the assets. This plan includes eliminating legacy technology that can no longer be
1066 protected adequately, and adopting enhanced and modern protection and detection mechanisms.
1067 An example key finding for this event is the need to encrypt employee data in one of the payroll
1068 systems that was breached.
- 1069 • The IT team, with assistance from the recovery team, will start the execution and implementation
1070 of the long-term improvement plan once the changes to the architecture and enhanced capabilities
1071 have been approved and funded by the organization.

1072 **6.3.2 Metrics**

- 1073 • Upon formal completion of the event, the recovery team meets for an after-action review. During
1074 that meeting, members of the recovery team consider metrics that were gathered during the event
1075 (e.g., review of recovery objective assumptions, efficacy of training, additional plans required).
- 1076 • The debriefing reviews the efficacy key milestones that were developed in planning activities,
1077 including those that identified interim recovery goals, to share with the team. The team reviewed
1078 other relevant metrics regarding assumptions made, recovery objective performance, and
1079 stakeholder communications achievement.

1080 **6.3.3 Recovery Plan Improvement**

- 1081 • Comparison of the performance of the team during the recovery against the estimated
1082 performance defined in the the plans enables the organization planners to consider what
1083 adjustments should be made to the plans. Hopefully there will not be a recurrence of the issues,
1084 but the organization must continue to always be prepared.
- 1085 • These post-recovery steps help to continually improve cyber event recovery plans, policies, and
1086 procedures by addressing lessons learned during recovery efforts and by periodically validating
1087 the recovery capabilities themselves.

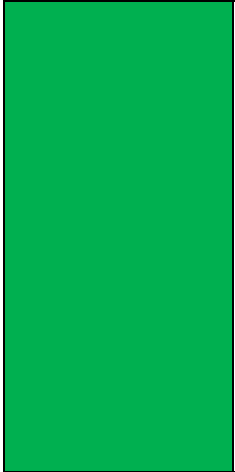
1088 **Appendix A—CSF Core Components and SP 800-53r4 Controls Supporting Recovery**

1089 This appendix provides mappings from the recovery processes and activities to the Cybersecurity
 1090 Framework [3] and related NIST Special Publication (SP) 800-53 Revision 4 [9] security controls.

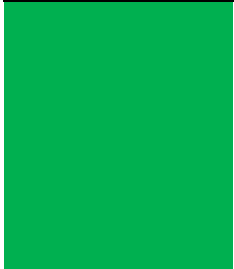
Function	Category	Subcategory	SP 800-53r4 Controls
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	ID.AM-3: Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6, PM-8
	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-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	CP-2, CP-11, SA-14, SA-13
		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 management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established

Function	Category	Subcategory	SP 800-53r4 Controls
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ID.RA-3: Threats, both internal and external, are identified and documented</p>	<p>RA-3, SI-5, PM-12, PM-16</p>
		<p>ID.RA-4: Potential business impacts and likelihoods are identified</p>	<p>RA-2, RA-3, PM-9, PM-11, SA-14</p>
		<p>ID.RA-6: Risk responses are identified and prioritized</p>	<p>PM-4, PM-9</p>
	<p>Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis</p>	<p>PM-8, PM-9, PM-11, SA-14</p>
<p>PROTECT (PR)</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 protection of information systems and assets.</p>	<p>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained</p>	<p>CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p>
		<p>PR.IP-4: Backups of information are conducted, maintained, and tested periodically</p>	<p>CP-4, CP-6, CP-9</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>CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, IR-10, PE-17</p>
		<p>PR.IP-10: Response and recovery plans are tested</p>	<p>CP-4, IR-3, IR-7, PM-14</p>

Function	Category	Subcategory	SP 800-53r4 Controls
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	AC-4, CA-3, CM-2, SI-4
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	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	CP-2, CP-3, IR-3, IR-8
	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	CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	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.	RC.RP-1: Recovery plan is executed during or after an event	CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	CP-2, IR-4, IR-8

Function	Category	Subcategory	SP 800-53r4 Controls
	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	[Not currently included in SP 800-53 R4]
		RC.CO-2: Reputation after an event is repaired	[Not currently included in SP 800-53 R4]
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	CP-2, IR-4

1091



1092 **Appendix B—Acronyms and Other Abbreviations**

1093 Selected acronyms and other abbreviations used in the guide are defined below.

BIA	Business Impact Analysis
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNAP	Cybersecurity National Action Plan
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical System
CSF	Cybersecurity Framework
CSIP	Cybersecurity Strategy and Implementation Plan
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
GAO	Government Accountability Office
HR	Human Resources
ICS	Industrial Control System
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
ITL	Information Technology Laboratory
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OLA	Operations Level Agreement
OT	Operational Technology
PHI	Protected Health Information
PII	Personally Identifiable Information
RTO	Recovery Time Objective
SLA	Service Level Agreement
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

1094

1095 **Appendix C—References**

1096 This appendix lists the references for the document.

- [1] Government Accountability Office (GAO), GAO 15-714, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, September 2015. <http://www.gao.gov/products/GAO-15-714> [accessed 6/6/16]
- [2] Office of Management and Budget (OMB), *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, OMB Memorandum 16-04, October 30, 2015. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf> [accessed 6/6/16]
- [3] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014. <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> [accessed 6/6/16]
- [4] Department of Homeland Security (DHS), *DHS Risk Lexicon, 2010 Edition*, September 2010. <https://www.dhs.gov/dhs-risk-lexicon> [accessed 6/6/16]
- [5] National Institute of Standards and Technology (NIST), NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012. <http://dx.doi.org/10.6028/NIST.SP.800-61r2>
- [6] National Institute of Standards and Technology (NIST), NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010. <http://dx.doi.org/10.6028/NIST.SP.800-34r1>
- [7] Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>, <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf> [accessed 6/6/16]
- [8] National Institute of Standards and Technology (NIST), Draft NIST SP 800-154, *Guide to Data-Centric System Threat Modeling*, March 2016. http://csrc.nist.gov/publications/drafts/800-154/sp800_154_draft.pdf [accessed 6/6/16]
- [9] Joint Task Force Transformation Initiative, NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). <http://dx.doi.org/10.6028/NIST.SP.800-53r4>
- [10] Joint Task Force Transformation Initiative, NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 (including updates as of June 5, 2014). <http://dx.doi.org/10.6028/NIST.SP.800-37r1>

- [11] National Institute of Standards and Technology (NIST), Second Draft NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, April 2016.
http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf [accessed 6/6/16]
- [12] ISACA, COBIT version 5. <https://www.isaca.org/cobit> [accessed 6/6/16]
- [13] National Institute of Standards and Technology (NIST), NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.
<http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf> [accessed 6/6/16]
- [14] National Institute of Standards and Technology (NIST), NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008.
<http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf> [accessed 6/6/16]

1097