

2

3 **Security Guidelines for Storage**
4 **Infrastructure**
5

6
7 **Ramaswamy Chandramouli**
8 **Doron Pinhas**
9

10
11
12
13
14 This publication is available free of charge from:
15 <https://doi.org/10.6028/NIST.SP.800-209-draft>
16
17

18 **C O M P U T E R S E C U R I T Y**
19

20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

Draft NIST Special Publication 800-209
Security Guidelines for Storage
Infrastructure

Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

Doron Pinhas
Continuity Software
New York, NY

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-209-draft>

July 2020



U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

40
41
42
43
44
45
46

47

Authority

48 This publication has been developed by NIST in accordance with its statutory responsibilities under the
49 Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law
50 (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including
51 minimum requirements for federal information systems, but such standards and guidelines shall not apply
52 to national security systems without the express approval of appropriate federal officials exercising policy
53 authority over such systems. This guideline is consistent with the requirements of the Office of Management
54 and Budget (OMB) Circular A-130.

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

61 National Institute of Standards and Technology Special Publication 800-209
62 Natl. Inst. Stand. Technol. Spec. Publ. 800-209, 65 pages (July 2020)
63 CODEN: NSPUE2

64 This publication is available free of charge from:
65 <https://doi.org/10.6028/NIST.SP.800-209-draft>

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

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

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

79

80 **Public comment period: July 21, 2020 through August 31, 2020**

81

82

83

84

85

86

87

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-209-comments@nist.gov

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

88

Reports on Computer Systems Technology

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

99

100

Abstract

101 Storage technology, just like its computing and networking counterparts, has evolved from
102 traditional storage service types, such as block, file, and object. Specifically, the evolution has
103 taken two directions: one along the path of increasing storage media capacity (e.g., tape, HDD,
104 SSD) and the other along the architectural front, starting from direct attached storage (DAS) to
105 the placement of storage resources in dedicated networks accessed through various interfaces and
106 protocols to cloud-based storage resource access, which provides a software-based abstraction
107 over all forms of background storage technologies. Accompanying the evolution is the increase
108 in management complexity, which subsequently increases the probability of configuration errors
109 and associated security threats. This document provides an overview of the evolution of the
110 storage technology landscape, current security threats, and the resultant risks. The main focus of
111 this document is to provide a comprehensive set of security recommendations that will address
112 the threats. The recommendations span not only security management areas that are common to
113 an information technology (IT) infrastructure (e.g., physical security, authentication and
114 authorization, change management, configuration control, and incident response and recovery)
115 but also those specific to storage infrastructure (e.g., data protection, isolation, restoration
116 assurance, and encryption).

117

118

Keywords

119 storage area network; network attached storage; storage array; file storage service; block storage
120 service; object storage service; storage virtualization; software-defined storage; hyper-converged
121 storage; data protection; cloud storage; backup; replication.

122

123

Acknowledgements

124 [TBD]

125

Call for Patent Claims

126 This public review includes a call for information on essential patent claims (claims whose use
127 would be required for compliance with the guidance or requirements in this Information
128 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
129 directly stated in this ITL Publication or by reference to another publication. This call also
130 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
131 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

132 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
133 in written or electronic form, either:

134 a) assurance in the form of a general disclaimer to the effect that such party does not hold
135 and does not currently intend holding any essential patent claim(s); or

136 b) assurance that a license to such essential patent claim(s) will be made available to
137 applicants desiring to utilize the license for the purpose of complying with the guidance
138 or requirements in this ITL draft publication either:

139 i. under reasonable terms and conditions that are demonstrably free of any unfair
140 discrimination; or

141 ii. without compensation and under reasonable terms and conditions that are
142 demonstrably free of any unfair discrimination.

143 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
144 on its behalf) will include in any documents transferring ownership of patents subject to the
145 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
146 the transferee, and that the transferee will similarly include appropriate provisions in the event of
147 future transfers with the goal of binding each successor-in-interest.

148 The assurance shall also indicate that it is intended to be binding on successors-in-interest
149 regardless of whether such provisions are included in the relevant transfer documents.

150 Such statements should be addressed to: sp800-209-comments@nist.gov
151 with Subject: sp800-209 PATENT CLAIMS
152

153 **Executive Summary**

154 Storage, computing, and networking form the three fundamental building blocks of an
155 information technology infrastructure. Just like computing and network technologies, the storage
156 technology has also evolved over the years. Higher capacity storage media and storage system
157 architecture are the two fronts on which the storage technology has evolved. The developments
158 on the second front have enabled the storage services to support many new and evolving
159 computing use cases but have also introduced storage management complexity and many
160 security challenges.

161 Just like computing and networking, the current landscape of storage infrastructure consists of a
162 mixture of legacy and advanced systems. With this in mind, this document provides an overview
163 of the storage technology landscape, including traditional storage services (e.g., block, file, and
164 object storage), storage virtualization, storage architectures geared for virtualized server
165 environments, and storage resources hosted in the cloud. Descriptions of various threats to the
166 storage resources are also included, as well as analysis of the risks to storage infrastructure and
167 the impacts of these threats.

168
169 The primary purpose of this document is to provide a comprehensive set of security
170 recommendations for the current landscape of the storage infrastructure. The security focus areas
171 span those that are common to the entire IT infrastructure, such as physical security,
172 authentication and authorization, change management, configuration control, incident response,
173 and recovery. Within these areas, security controls that are specific to storage technologies, such
174 as network-attached storage (NAS) and storage area networks (SAN), are also covered. In
175 addition, security recommendations specific to storage technologies are provided for the
176 following areas of operation in the storage infrastructure:

- 177 • Data protection
- 178 • Isolation
- 179 • Restoration assurance
- 180 • Encryption

| | | |
|-----|---|-----------|
| 181 | Table of Contents | |
| 182 | Executive Summary | iv |
| 183 | 1 Introduction | 1 |
| 184 | 1.1 Scope..... | 2 |
| 185 | 1.2 Target Audience..... | 3 |
| 186 | 1.3 Relationship to other NIST Guidance Documents | 3 |
| 187 | 1.4 Organization of this Document..... | 3 |
| 188 | 2 Data Storage Technologies: Background..... | 4 |
| 189 | 2.1 Block Storage Service..... | 5 |
| 190 | 2.2 File Storage Service..... | 5 |
| 191 | 2.3 Object Storage Service | 6 |
| 192 | 2.4 Content-addressable Storage (CAS) Service | 7 |
| 193 | 2.5 Higher-level Data Access Service..... | 7 |
| 194 | 2.6 Software-defined Storage | 7 |
| 195 | 2.7 Storage Virtualization | 8 |
| 196 | 2.8 Storage for Virtualized Servers | 8 |
| 197 | 2.9 Converged and Hyper-Converged Storage..... | 9 |
| 198 | 2.10 Storage Infrastructure in Cloud | 10 |
| 199 | 2.11 Storage Management | 11 |
| 200 | 2.11.1 Data Classification or Categorization..... | 11 |
| 201 | 2.11.2 Data Sanitization | 11 |
| 202 | 2.11.3 Data Retention | 12 |
| 203 | 2.11.4 Data Protection..... | 12 |
| 204 | 2.11.5 Enhancing Performance – Data Reduction | 13 |
| 205 | 2.11.6 Security Controls | 14 |
| 206 | 3 Threats, Risks, and Attack Surfaces | 15 |
| 207 | 3.1 Threats..... | 15 |
| 208 | 3.1.1 Credential Theft..... | 15 |
| 209 | 3.1.2 Cracking Encryption | 15 |
| 210 | 3.1.3 Infection of Malware and Ransomware | 16 |
| 211 | 3.1.4 Backdoors and Unpatched Vulnerabilities | 16 |
| 212 | 3.1.5 Privilege Escalation | 16 |

| | | | |
|-----|----------|---|-----------|
| 213 | 3.1.6 | Human Error and Deliberate Misconfiguration..... | 17 |
| 214 | 3.2 | Risks to Storage Infrastructure | 17 |
| 215 | 3.2.1 | Data Breach | 17 |
| 216 | 3.2.2 | Data Exposure..... | 18 |
| 217 | 3.2.3 | Unauthorized Data Alteration and Addition..... | 18 |
| 218 | 3.2.4 | Data Corruption | 19 |
| 219 | 3.2.5 | Compromising Backups..... | 19 |
| 220 | 3.2.6 | Data Obfuscation and Encryption | 19 |
| 221 | 3.2.7 | Data Availability and Denial of Service | 20 |
| 222 | 3.2.8 | Tampering of Storage-Related Log and Audit Data..... | 20 |
| 223 | 3.2.9 | Mapping of Threats to Risks..... | 20 |
| 224 | 3.3 | Attack Surfaces..... | 21 |
| 225 | 3.3.1 | Physical Access | 22 |
| 226 | 3.3.2 | Access to Storage OS | 22 |
| 227 | 3.3.3 | Access to Management Hosts | 23 |
| 228 | 3.3.4 | Management APIs, Management Software, In-band Management | 23 |
| 229 | 3.3.5 | Storage Clients | 23 |
| 230 | 3.3.6 | Storage Network (Tap Into, Alter to Gain Access)..... | 23 |
| 231 | 3.3.7 | Compute Environment of Key Individuals – Storage Admins | 24 |
| 232 | 3.3.8 | Electricity Network..... | 24 |
| 233 | 4 | Security Guidelines for Storage Deployments | 25 |
| 234 | 4.1 | Physical Storage Security | 25 |
| 235 | 4.2 | Data Protection | 26 |
| 236 | 4.2.1 | Data Backup and Recovery | 26 |
| 237 | 4.2.2 | Replication..... | 27 |
| 238 | 4.2.3 | Point-in-Time Copies and Snapshots | 28 |
| 239 | 4.2.4 | Continuous Data Protection..... | 28 |
| 240 | 4.3 | Authentication and Data Access Control..... | 28 |
| 241 | 4.3.1 | Authentication Recommendations | 29 |
| 242 | 4.3.2 | Password Recommendations | 29 |
| 243 | 4.3.3 | Account Management Recommendations | 30 |
| 244 | 4.3.4 | Privilege and Session Management Recommendations | 31 |
| 245 | 4.3.5 | SAN-Specific Recommendations | 32 |
| 246 | 4.3.6 | File and Object Access Recommendations | 33 |

247 4.4 Audit Logging 34

248 4.5 Preparation for Data Incident Response and Cyber Recovery 36

249 4.6 Guidelines for Network Configuration 36

250 4.6.1 SAN 37

251 4.6.2 IP Network 38

252 4.6.3 Protocols 40

253 4.7 Isolation 41

254 4.8 Restoration Assurance 43

255 4.9 Encryption 45

256 4.10 Administrative Access 47

257 4.11 Configuration Management 50

258 **5 Summary and Conclusions 53**

259 **References 54**

260

261 **1 Introduction**

262 Storage, computing, and networking form the three fundamental building blocks of any
263 information technology (IT) infrastructure. The storage infrastructure has evolved over the years
264 to become feature-rich in areas such as performance and efficiency due to developments on two
265 fronts. One is the area of storage media, which features solid-state drives (SSD) with high
266 capacity and storage efficiency features (e.g., deduplication, compression, etc.) compared to
267 hard-disk drives (HDD). The second is in the area of storage system architecture using concepts
268 such as storage virtualization. However, development on this second front has also introduced a
269 great deal of management complexity, including the task of providing security assurance.

270 Briefly tracing the history of storage system architecture shows that the earliest form of digital
271 storage infrastructure is direct-attached storage (DAS) where the storage element or device (e.g.,
272 tape, hard disk) is directly attached to the host server without any intervening network. The next
273 evolution of the storage infrastructure is one where the storage resources are intelligently pooled,
274 located across the network, accessed through networking protocols, and accessible by multiple
275 hosts or servers. This type of storage infrastructure is the only way that the data access needs of
276 distributed systems can be supported since application components that need to share data are in
277 different nodes of a network. In this stage of evolution, the storage infrastructure has taken on
278 two forms, depending on the type of networking protocol. In one form, the storage resource is
279 simply a node in a network using common networking technology (e.g., LAN, WAN), while in
280 the other, there is a dedicated network for communicating with all storage resources (e.g., Fibre
281 Channel). An example of the former is network-attached storage (NAS), which provides file-
282 level access to heterogeneous clients across a network using higher level protocols, such as NFS
283 or SMB/CIFS. The latter is exemplified by the storage area network (SAN), which uses a
284 specialized, high-speed network (e.g., Fibre-Channel) that provides block-level access to storage.

285 A variation of the traditional enterprise storage infrastructure is the emergence of converged and
286 hyper-converged systems (HCI). A converged system involves a preconfigured package of
287 software and hardware in a single hardware chassis for simplified management. However, with a
288 converged infrastructure, the compute, storage, and networking components are discrete and can
289 be separated. Just like a converged system, an HCI combines storage, computing, and
290 networking into a single hardware unit or chassis and has built in a layer of abstraction for
291 managing all three components. In fact, it includes a common software console or management
292 tool for managing all three components. It also includes a hypervisor for virtualized computing,
293 software-defined storage, and virtualized networking bundled together to run on standard, off-
294 the-shelf hardware. The integrated storage systems, hosts, and networking switches are designed
295 to be managed as a single system across all instances of a hyperconverged infrastructure. Further,
296 each hardware unit can be configured to be a node of a cluster to create pools of shared storage
297 resources, thus providing the advantage of a centralized enterprise storage infrastructure.

298 The next wave of storage evolution involves the introduction of cloud storage, which offers a
299 highly scalable and durable set of storage services that are completely software-defined. Cloud
300 storage services often include:

- 301 • Block storage services, which expose software-defined block devices that can be
302 presented to virtual hosts running in the cloud
- 303 • Object storage services, which can be mapped to hosts, applications, or even other cloud
304 services
- 305 • Scalable shared filesystems, which can allow a scalable set of hosts to access the same
306 file system at a high speed
- 307 • A variety of replication, caching, archiving, mirroring, and point-in-time copy services to
308 all of the above

309 Additional cloud services—such as managed database services, data lakes, memory caches, and
310 messages queues—are also offered, all of which can store stateful and transient data. However,
311 experts are divided over whether to classify them as storage services in and of themselves.

312 Another type of storage infrastructure is the one that contains interfaces to support the data
313 storage needs of emerging stateful applications that are designed using microservices-based
314 architecture and deployed using containers organized into clusters with container orchestration
315 platforms. These platforms have a standard plug-in mechanism by way of a container storage
316 interface (CSI) that connects the clusters configured by them to different types of persistent
317 storage implementations.

318 **1.1 Scope**

319 This document provides security recommendations for the following storage technologies:

- 320 • Traditional enterprise storage technologies classified based on storage service interface
321 type (e.g., block, file, and object)
- 322 • Storage systems that have a layer of software abstraction (e.g., software-designed storage
323 and storage virtualization)
- 324 • Storage systems designed exclusively for virtualized server environments (eg., storage for
325 VMs and containers, converged and hyperconverged storage systems)
- 326 • Storage systems designed with APIs for cloud access

327 The security recommendations span the following operations:

- 328 • Operations that are carried out for other infrastructures (e.g., computing and networking)
329 but the specific tasks are applicable to storage infrastructure, such as physical security,
330 authentication and authorization, audit logging, network configuration, isolation,
331 configuration control, and change management
- 332 • Operations that are unique to storage infrastructure, such as data protection and
333 restoration assurance

334 1.2 Target Audience

335 The target audience for the security recommendations discussed in this document includes:

- 336 • Chief Security Officer (CSO) or Chief Technology Officer (CTO) of an IT department in
337 a private enterprise, government agency, or a cloud service provider who wishes to
338 formulate enterprise- or data center-wide policies for the entire infrastructure, including
339 storage infrastructure
- 340 • System or storage administrators who have to set up specific deployment configurations
341 for storage, converged, or virtualized systems

342 1.3 Relationship to other NIST Guidance Documents

343 This guidance document focuses on a particular type of infrastructure that provides access to all
344 data resources/services, similar to how the computing infrastructure provides access to
345 computing services and the networking infrastructure provides access to communication
346 services. Hence, some of the security guidance and recommendations related to computing and
347 networking are relevant security strategies for the storage infrastructure discussed in this
348 document. These common recommendations are either included here through a brief description
349 or incorporated by reference. The relevant NIST documents containing recommendations that
350 span all infrastructures (i.e., computing, networking, and storage) are:

- 351 • SP 800-125A, Revision 1, *Security Recommendations for Server-based Hypervisor Platforms*
352 (2018)
- 353 • SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*
354 (2016)

355 1.4 Organization of this Document

356 The organization of this document is as follows:

- 357 • Section 2 provides an overview of traditional enterprise storage technologies, storage
358 access technologies that provide a level of abstraction, storage architectures tailored for
359 virtualized server environments, and APIs for accessing storage resources in the cloud.
360 This section also provides an overview of certain general principles of storage
361 administration.
- 362 • Section 3 explores the threats to storage infrastructure and associated risks. Apart from
363 generic threats such as privilege escalation, credential theft, cracking encryption,
364 malware, and ransomware, storage infrastructure-specific threats such as unauthorized
365 storage configuration changes are also discussed. The resulting risks to storage
366 infrastructure (e.g., data breach, data exposure, unauthorized data alteration and addition,
367 data corruption, data obfuscation and encryption, and tampering of storage-related log
368 and audit data) are also analyzed based on the possibility of the realization of these
369 threats and their impacts.
- 370 • Section 4 provides the core material for the publication. It details security
371 recommendations for all facets of storage infrastructure management.

372

2 Data Storage Technologies: Background

374 Data storage technology encompasses the devices, objects (e.g., storage elements, storage arrays,
375 storage network switches or storage media), and processes (e.g., protocols and interfaces) used to
376 store computer data in non-volatile (durable) form. Hence, this technology can be viewed upon
377 from the following two taxonomies:

- 378 • **Based on location of storage resource:** The storage device is directly attached to the
379 storage client or host computer and called the direct-attached storage (DAS), or there is a
380 network separating the host computer and the storage device (networked storage).
- 381 • **Based on storage type (access type):** This classification is based on the service interface
382 offered by the storage system that is used by the client software. Examples include block-
383 based storage (block storage service), file-based storage (file storage service), and object-
384 based storage (object storage service).

385 In DAS, the storage device can be either an integral part of the computer (attached to the bus) or
386 external storage (attached to a computer port, such as serial or USB).

387 Networked storage is broadly classified based on the type of access, such as network-attached
388 storage (NAS), which provides file-level access across the network, and storage area network
389 (SAN) whose protocols provide block-level access across the network. Further, in SAN, either
390 the entire network stack can be comprised of storage-specific protocols (e.g., fibre channel), or it
391 may consist of storage-specific protocols running over (or encapsulated within) common
392 networking protocols (e.g., iSCSI by design running over TCP/IP, Fibre channel over IP [FCIP],
393 Fibre channel over Ethernet [FCoE]).

394 Since SAN is a specialized, high-speed network for block-level network access to storage, a
395 more detailed look at its variants is warranted. The variants are the results of different types of
396 network stacks with different protocols in certain layers of the stack. The building block of SAN-
397 based systems typically include (a) host computers (clients); (b) topology, most of which involve
398 switches (called SAN Fabric); and (c) storage devices/arrays, with all three components
399 interconnected using various network stacks.

400 Based on the above descriptions, SANs can be broadly classified as:

- 401 a. Fibre Channel SAN
- 402 b. IP SAN
- 403 c. Fibre channel over Ethernet (FCoE)
- 404 d. NVMe over Fabrics

405 A Fibre Channel SAN is a network stack with five layers (i.e., FC0 through FC4, unlike the
406 seven-layer OSI stack). The logical storage resource addressed by Fibre Channel SAN is called
407 the logical unit number (LUN).

408 iSCSI [1,2] and Fibre Channel over TCP/IP (FCIP) are examples of IP SANs since they use the
409 IP protocol at the network layer, as in the former, or to encapsulate the Fibre Channel frame in an
410 IP packet, as in the latter.

411 In FCoE, the Fibre Channel frame is encapsulated in Ethernet packets. The type of traffic (data
412 and commands) carried in all three categories of SAN is SCSI.

413 NVMe is the standard host controller interface for systems using PCI Express (PCIe)-based solid
414 state drives (SSDs). The NVMe over Fabrics (NVMe-oF) specification defines a protocol
415 interface and related extensions that enable the NVMe commands to be transmitted over other
416 interconnects, including RDMA, Fibre Channel, and TCP. NVMe-oF extends the NVMe
417 deployment from a local host to a remote host for a scale-out NVMe storage system.

418 The hardware that connects the host computer (client) to storage devices is called the SAN
419 fabric. The type of connection is called a topology. There are three kinds of topologies in SAN:
420 point-to-point (two devices are directly connected), arbitrated loop, and switched fabric. In
421 switched fabric, there is a set of hardware switches (acting as one big logical switch) separating
422 the host computer and the storage resources. Since all variants of SAN run Fibre Channel
423 protocol, the SAN fabric is synonymous with Fibre Channel fabric.

424 The taxonomy based on storage, access, or service type includes block, file, and object types or
425 services. Since the choice of a storage service is dictated by the specific IT system use case (e.g.,
426 volume of data, control required over data, required performance, nature of data representation),
427 this document will present an overview of storage technology in terms of these services
428 (synonymous with storage/access types).

429 **2.1 Block Storage Service**

430 A block storage service offers an interface that reads and writes fixed-size blocks of data,
431 typically offering high bandwidth, low latency access to storage devices at the block level [3].
432 Each storage device in a block-level storage system can be controlled as an individual hard drive,
433 and the blocks are managed by the host OS. Block storage protocols like SCSI, SATA,
434 iSCSI, Fibre Channel, and FCoE (Fibre Channel over Ethernet) are utilized to transport the
435 storage blocks from the storage resources to the client system [4].

436 This type of service is offered by DAS. Across the network, this service is provided by SAN
437 protocols, such as iSCSI and Fibre Channel [5]. All variations of SAN—such as FC, FCIP,
438 FCoE, iSCSI, and FC-VNMe—provide block storage service. Here, the remote storage devices
439 are presented as if they are locally attached to the host system on which storage client software is
440 running.

441 **2.2 File Storage Service**

442 This type of service projects storage resources in the form of file system model with files
443 contained in directories within volumes. The different variations of this service and their
444 associated protocols are:

- 445 • Network-attached storage (NAS) with NFS protocol (current version is NFS 4.2 [6]) – A
446 module that is part of the protocol implementation system, called the NFS client driver,
447 mounts the volumes that are relevant for the client in its environment. The volume can be
448 shared by multiple clients. Behind the scenes, files can be encrypted and replicated by

449 making redundant copies. The files or folders can also be shared from either a dedicated
450 appliance (typically referred to as a “NAS device” or “NAS array”) or from any host running
451 the NFS server service.

- 452 • NAS with SMB/CIFS protocol connection – This is provided by a LAN-attached file server,
453 just like those that provide NFS protocol connection, but with the standard SMB protocol
454 that is found in the network stack of operating systems used in personal computers and
455 workstations.
- 456 • NAS with multi-protocol support – There are file service storage offerings that support multi-
457 protocol exports of a folder or filesystem (e.g., both NFS and CIFS, concurrently). Each of
458 these may have slightly different access control structures (i.e., ACL/permissions
459 specifications), and some conflicts in access control rights may have to be resolved during
460 access requests.
- 461 • NAS with parallel NFS protocol – This is provided through a clustered collection of storage
462 servers (instead of a single NFS server) that slices and/or strips data and metadata at the back
463 end while providing dynamic, distributed client connections at the front end across the set of
464 clustered hosts. The parallel NFS system is implemented either by (a) partitioning filesystem
465 namespace and assigning storage resources (i.e., files) that belong to different namespaces to
466 different servers (called symmetric cluster) or (b) splitting functionality across servers (called
467 asymmetric cluster) by having a primary fileserver provide the directory information for the
468 location of secondary storage servers, the data contained in them, and the method to access
469 them.

470 This service is used for large-scale content repositories (because of its scalability), media stores,
471 and development environments [7].

472 **2.3 Object Storage Service**

473 An object storage service presents data as flexible-size data containers called objects, unlike the
474 fixed-size blocks offered by block storage service. The interface it provides is called the object-
475 based storage device (OSD) interface. Each object has both data (a linear sequence of bytes) and
476 metadata (an extensible set of attributes describing the object) as well as a unique object
477 identifier (OID). The OSD interface contains commands to create and delete objects, read and
478 write bytes to and from individual objects, and set and get attributes (metadata) on objects.
479 Hence, the object storage model is also called a key-value model, with the value as the object.
480 The user-specified metadata can be arbitrary in number and potentially far higher than what is
481 possible with standard file systems. The objects are organized in a flat, non-hierarchical
482 namespace (unlike file systems with a hierarchical namespace) called a storage pool, bucket, or
483 container.

484 An OSD interface is agnostic to the type of storage hardware and can span multiple storage
485 devices, thus making it highly scalable. The interface is typically a network-accessible REST
486 API, so the client applications have to be designed to make API calls.

487 The OSD interface is useful for accessing and modifying unstructured data, such as images,
488 where modification involves replacing the whole object with a new version.

489 **2.4 Content-addressable Storage (CAS) Service**

490 This is a specialized form of object-based storage that is intended for storing the content digests
491 of documents to enable users to retrieve those documents without having to know the location of
492 the actual data or the number of copies. Hence, a CAS service exposes the digest generated by a
493 cryptographic hash function (e.g., SHA-1 or SHA-256) pertaining to the document it refers to.

494 CAS is used for retrieving documents with short- and medium-term retention requirements.

495 **2.5 Higher-level Data Access Service**

496 There are data access services that provide data at a higher level of abstraction than that of basic
497 storage types (files, blocks, or objects). These services can only be accessed through clients
498 specifically built to access data at the same level of abstraction (e.g., SQL database clients).
499 These services are available both in enterprise data centers and in the clouds. The following are
500 some of these higher-level data access services:

- 501 • NoSQL database services
- 502 • SQL database services
- 503 • Messaging queue storage services

504 NoSQL database services enable the storage and retrieval of unstructured data, such as images,
505 videos, documents, and large binary objects. Unstructured data has higher logical structures and
506 representations than basic storage types in order to facilitate faster storage and retrievals. They
507 include key-value store, multi-modal database, graph database, and others.

508 SQL database services enable the storage and retrieval of structured data that is typically in a
509 tubular format (also called relational tables). The access is enabled through a standardized
510 interactive programming language called Structured Query Language (SQL) [ISO/IEC
511 9075:2016 Database languages – SQL]. Current SQL databases can not only store data using
512 relational tables/views but also other structures, such as XML, JSON, and BLOBs.

513 Messaging queue storage services are specialized services for the storage and retrieval of data
514 from messaging queue infrastructures. These infrastructures are used by distributed applications
515 whose components communicate asynchronously through subscription to a message queueing
516 system. In addition to providing access to persistent data, this service also facilitates specialized
517 operations, such as stream processing where events relating to multiple message storage and
518 retrieval by distributed system components can be analyzed to discover patterns.

519 **2.6 Software-defined Storage**

520 Software-defined storage (SDS) is a storage architecture [8] that separates the storage hardware
521 from the software that manages the storage infrastructure and automates its configuration. In
522 other words, the storage capabilities and services are separated from the storage hardware.
523 Advantages of this separation include the following:

- 524 • Use of heterogeneous storage hardware without the issues of interoperability

- 525 • Enabling of functions such as deduplication, replication, snapshots, and thin provisioning
- 526 using industry-standard server hardware
- 527 • Automatic and efficient allocation of pooled storage resources to match the application
- 528 needs of the enterprise

529 The following service capabilities are expected of the software managing the hardware storage
530 resources in a software-define storage system [9]:

- 531 • Decouple storage policy management from the storage hardware;
- 532 • Support heterogeneous storage environments;
- 533 • Allow for the ability to add new storage capabilities across all platforms and not just to
- 534 individual arrays; and
- 535 • Ensure that the storage software understands and leverages the capabilities of all storage
- 536 hardware.

537 **2.7 Storage Virtualization**

538 Storage virtualization allows the capacity of multiple storage devices or arrays to be pooled
539 (abstracted) so that they can be managed as one entity. Virtualization can aggregate and manage
540 storage resources as logical storage across a wide range of physical storage devices (physical
541 storage) in large networks (e.g., SAN) or data centers. This technique provides the flexibility to
542 change the logical to physical relationship over time and mask the details of physical storage
543 resources [10]. The following are some scenarios where storage virtualization is deployed:

- 544 • Portions of multiple physical disk drives can be presented as a single mirrored logical
545 volume (using a logical volume manager in a host or storage array). Further, the
546 composition of physical disk drives in the mirrored volume can be changed.
- 547 • Sensing changes to access patterns, drives on which data is stored can be changed (e.g.,
548 store frequently accessed information on high performance drives), thus providing an
549 automatic tiering functionality.

550 In addition to logical volumes and masking, other techniques for storage virtualization include
551 zoning, use of host-bus adapters, RAID, and the use of distributed file systems or objects [11].
552 The benefits of storage virtualization are scalability, performance, redundancy, and increased
553 storage resource utilization.

554 **2.8 Storage for Virtualized Servers**

555 A virtualized server is one where a single physical server runs multiple computing stacks (each
556 consisting of an OS and applications) called virtual machines (VMs) with the use of a software
557 called the hypervisor. Storage infrastructure specifically designed to support virtualized servers
558 is often called virtualization-aware storage or VM-aware storage. In most environments, this
559 infrastructure is managed together with the VMs rather than as separately managed LUNs.

560 A key driver for building this VM-aware storage is to enable policy-based provisioning of
561 storage resources at the VM-level through the hypervisor (which controls the allocation of all
562 resources to VMs) so as to meet data access QoS requirements for the applications hosted on the

563 VMs. Another feature of this architecture is the ability to decouple VM storage from the
564 individual hypervisor, thereby enabling an advanced virtual infrastructure function, such as live
565 migration of VMs from one hypervisor to another, as well as enabling automated failover of a
566 VM between hypervisors.

567 If the storage network infrastructure used to connect virtual machines to storage resources is
568 implemented as a SAN, such a VM-aware storage system can be called a server-based SAN or
569 virtual SAN (VSAN), although there is a specific commercial product offering by that name. A
570 VSAN can be implemented on a cluster of virtualized servers by aggregating the direct-attached
571 storage in the various nodes (virtualized servers) within the cluster and then treating that storage
572 as a shared SAN resource. Each virtualized server that participates in the VSAN must have at
573 least one SATA or SAS hard drive that is dedicated to SAN storage. Additionally, some
574 implementations may have at least one solid-state drive (SSD) in the virtualized server used as a
575 read/write cache or for tiering storage.

576 Since the management functions in a VM-aware storage infrastructure are enabled using
577 software, they can be looked upon as a subset of SDS tailored for virtualized server
578 environments. The key factor in a VM-aware storage environment is that the storage components
579 are managed together with the VMs rather than as separately managed volumes or LUNs (logical
580 unit numbers) [12]. One of the limitations of VSAN compared to general-purpose SAN is that it
581 is only used for storing data related to VMs and is not multi-purpose. However, some
582 commercial implementations also allow physical hosts to use VSAN volumes.

583 **2.9 Converged and Hyper-Converged Storage**

584 In a converged architecture, the storage, memory, networking, and virtualization software are
585 preconfigured and pre-installed for fast deployment in a single box (e.g., a Rack containing one
586 or more physical hosts, storage resources [DAS or storage arrays], and network components). A
587 hyperconverged architecture takes the level of abstraction one step further where the individual
588 storage components associated with the physical hosts are virtualized to build up a common
589 storage pool, which is shared among all of the VMs or containers through the software-defined
590 storage (SDS) management software [13]. Therefore, a VM or a container hosted on one physical
591 host, say H(i), may use the storage associated with a different physical host, say H(j). As a
592 consequence, the SDS over a shared storage hyperconverged platform introduces a storage
593 network where the storage access is carried out over the network in the form of remote disk
594 access through popular storage networking protocols, such as the iSCSI.

595 A hyperconverged storage or hyperconverged integrated system (HCI) is one where hardware
596 required for compute, network, and storage are tightly coupled. All primary storage management
597 functions—together with other functional capabilities such as backup, recovery, replication,
598 deduplication, and compression—are delivered via the management software layer of the HCI
599 vendor and/or hardware along with compute provisioning. Examples include Nutanix, Scale
600 Computing, Cisco (HyperFlex), and SimpliVity [14]. The tight integration of the hardware
601 comes about due to HCI vendors working with storage device manufacturers to create a storage
602 solution that is tailored to their software stack as original equipment or as part of an industry-
603 accepted reference architecture.

604

605 In this system, some of the CPU used for computing has to be shared for performing storage
606 management functions. The overall management software stack may include a compute node, a
607 hypervisor, and Virtual SAN (VSAN) software, depending on the deployment environment (e.g.,
608 virtualized infrastructure, virtual desktops, unstructured data stores, high performance
609 computing) [15]. A common deployment scenario is one where the application environment
610 consists of microservices-based applications implemented using VMs and/or containers. The
611 expected features in an HCI solution include [16]:

612

- Support for multiple hypervisors
- Data protection features, such as always-on deduplication and compression across
614 primary storage and backup
- Management control through a single pane of glass or a central dashboard
- Ability to provide QoS storage requirements based on application needs

613

614

615

616

617

618 Offering application processing capabilities in the storage controller of the storage device (e.g.,
619 NVMe SSD) using a system on a chip (SoC) is one approach for hyperconverged storage
620 architecture. Another approach is to provide an add-in storage card (that can provide SSD or raw
621 flash storage) with an embedded CPU for running applications with them connected directly to
the hosting server's PIC bus and running NVMe protocol [17].

622

2.10 Storage Infrastructure in Cloud

623

624 Storage systems in the cloud may be either standards-based or proprietary and may include
625 object-, block-, or file-based services. The technical reasons for enterprises using storage systems
in the cloud are [18]:

626

- To accommodate new demand for storage resources without building an additional data
627 center
- To respond to changes in demand for storage, such as peaks and valleys
- The need for immediate storage capacity
- Increasing management complexity of on-premise storage infrastructure

628

629

630

631

Storage systems based in the cloud provide several sophisticated data services [19]:

632

- Collaboration capability – Includes features such as (a) notifications when files are
633 changed by others, (b) file sharing with the ability to set editing and view-only
634 permissions, (c) simultaneous editing, and (d) change tracking and versioning
- Data integration and analytics capability – Ability to integrate data resident on several
635 cloud sources, perform complex analytics, and either instantly serve the extracted
636 information or store it in a persistent storage for later access by cloud service customers
- Advanced data protection services, including replication, mirroring, archiving, auditing,
637 encryption

638

639

640

Cloud storage services often include:

641

- Block storage services that expose software-defined block devices that can be presented
642 to virtual hosts running in the cloud

642

- 643 • Object storage services that can be mapped to hosts, applications, or even other cloud
644 services
- 645 • Scalable shared filesystems that can allow a scalable set of hosts to access the same
646 filesystem at a high speed
- 647 • A variety of replication, caching, archiving, mirroring, and point-in-time copy services to
648 all of the above

649 Additional cloud services (e.g., managed database services, data lakes, memory caches,
650 messages queues) are also offered, all of which can store stateful and transient data. However,
651 experts are divided over whether to classify them as storage services in and of themselves.

652 **2.11 Storage Management**

653 Storage management refers to all activities geared toward ensuring reliability, resilience,
654 performance, and the security of storage resources through the use of management tools and
655 processes. Since storage security is the central focus of this document, this chapter will focus on
656 all activities not related to security controls (and associated recommendations), which are
657 deferred to Chapter 4. The non-security control-related activities that are followed as state of
658 practice are:

- 659 • Data Classification or Categorization
- 660 • Data Sanitization
- 661 • Data Retention
- 662 • Data Protection
- 663 • Performance Enhancement – Data Reduction
- 664 • Security Controls

665 **2.11.1 Data Classification or Categorization**

666 Enterprise data can be classified along several dimensions, such as:

- 667 • Sensitive vs. non-sensitive
- 668 • Frequently accessed vs. non-frequently accessed
- 669 • Productions vs. development

670 The sensitive vs. non-sensitive classification is required to enable provisioning of appropriate
671 security controls (e.g., authentication, authorization, encryption, key management, sanitization
672 etc.) Further, the sensitive category may require sub-categories based on regulations applicable
673 to the data, such as PII, HIPPA-related, and PCI. The frequently accessed vs. non-frequently
674 accessed classification is required to provision the appropriate storage media (e.g., SSD vs
675 HDD). The production vs. development classification may be required for both media selection
676 and security controls.

677 **2.11.2 Data Sanitization**

678 Sanitization is the process of rendering previously written data in the storage media irretrievable,
679 such that there is reasonable assurance that the data cannot be easily retrieved or reconstructed

680 [10]. There are three methods for sanitization: (a) clear (i.e., overwrite of the existing data), (b)
681 purge (i.e., using a strong magnetic field for magnetic media degaussing, cryptographic erase for
682 encrypted data), and (c) destroy (i.e., physical destruction of the media, such as burning,
683 pulverizing, etc.). Factors that determine the type of sanitization include the category of
684 information in the media, the nature of the media (magnetic or optic), and the reuse plans for the
685 media.

686 **2.11.3 Data Retention**

687 While data sanitization is the last activity in the data governance framework, there may be
688 situations where data needs to be retained for a short-, medium- (i.e., less than 10 years), or long-
689 term duration. This may be due to operational, legal, regulatory, or statutory requirements.

690 **2.11.4 Data Protection**

691 Data protection is an umbrella term for all activities that ensure that data is accessible, usable,
692 uncorrupted, and available for all authorized purposes with an acceptable level of performance
693 and is handled in accordance with compliance requirements, including privacy and all physical,
694 administrative, and technical means to provide assurance against accidental or intentional
695 disclosure, modification, or destruction.

696
697 The range of objectives and associated activities provides a taxonomy for classifying data
698 protection activities under three facets: storage, privacy, and information assurance/security [20].
699 The activities related to privacy are outside of the scope of this document since privacy-related
700 laws and regulations differ by countries and communities of interest. The activities related to
701 information assurance/security are predominantly technical controls, and each of them needs a
702 dedication session for discussion of their details. Hence, in this section, only storage-related data
703 protection activities/controls are discussed. These controls are:

- 704 • Data backup and recovery,
- 705 • Replication technologies,
- 706 • Continuous data protection, and
- 707 • Point-in-time copies and snapshots.

708 Backup is an operation wherein data stored in storage devices is accessed by production systems
709 and periodically copied to another set of storage devices (some of which may be offline).
710 Because of the changing nature of data content, a backup taken at an earlier time is often made
711 obsolete by the backup taken at a later time. Backups can either be “file backups,” which back up
712 a select portion of the data in a storage device (often based on logical data structures, such as
713 files, directories, data under a database schema, etc.), or “image backups,” which contain the
714 entire content of a particular device (e.g., an individual LUN).

715 Data replication is the process of writing the same data to two separate locations (i.e., two
716 separate storage systems) [18]. Replication is often used as part of the data recovery process and
717 involves copying data from one site to another. Generally, there are two types of replication:
718 synchronous and asynchronous. Synchronous replication involves the real-time copying of data

719 from site A (e.g., a production platform) to site B (e.g., a specially designated DR site).
720 Asynchronous replication involves time delay and may be performed continuously or using a
721 designed frequency for writing data from site A to site B. The time delay and frequency are
722 dictated by the enterprise's disaster recovery policy and are described in terms of specific RTO
723 (recovery time objective) and RPO (recovery point objective) goals. Specific point-in-time
724 replicas are designated as archives for fast recovery and a wide variety of other uses, such as
725 cloning production data for testing purposes.

726

727 Data protection involves activities and mechanisms that span the entire storage lifecycle. These
728 phases include [21]:

729

- Data at rest/at the endpoint – on a server or client device
- Data in transit – between storage devices, client to server, server to server
- Data in use – during viewing, modifying, or synchronizing between devices
- Data traveling outside of the security perimeter – during downloads, etc.

730

731

732

733 Continuous data protection (CDP) is a form of backup that supports a fine-grained recovery and
734 improved RPO. Unlike traditional backup, where copies of the data are performed periodically,
735 changed blocks in CDP are continually transmitted to the target storage environment, which
736 captures or journals the changes over time. In this respect, CDP resembles replication. However,
737 unlike replication, CDP will typically allow “playback” of the copied data to previous points in
738 time using a variety of techniques (e.g., byte-by-byte, pre-determined bookmarks, past versions,
739 etc.)

740 A snapshot is a point-in-time copy of a defined collection of data. Snapshots are a way to create
741 distinct “point-in-time” views of a data set, capturing the state of the data and ignoring those that
742 are in a state of flux. Snapshots are often “thin,” meaning that they store only the individual
743 blocks changed from a given point in time in reference to the source data. This often means that
744 if the primary data is unavailable, the snapshots will not be usable.

745 **2.11.5 Enhancing Performance – Data Reduction**

746 Data reduction is the process of reducing the amount of data stored and transmitted in an effort to
747 reduce costs and improve efficiency. The two common approaches to data reduction are data
748 deduplication and compression. Both of these approaches can be used together.

749 Data compression (sometimes performed in hardware) seeks to reduce the amount of data by
750 encoding it with a known algorithm to produce a representation of data that uses fewer bits of
751 storage than the unencoded representation [10]. Data compression is used in tape backups and
752 during remote data replication in network gateways to reduce the bandwidth requirements for
753 disaster recovery (DR) and business continuity (BC) operations. Interoperability is a key
754 requirement for data compression since the encoding and subsequent reading system may be
755 different.

756 Data deduplication attempts to replace multiple copies of data with references to a shared copy.
757 It works by eliminating identical blocks of storage. For example, if a storage system has 500

758 identical blocks, the storage array will store just one copy, thereby eliminating the need to store
759 the other 499 copies [18]. This can take place at the storage device level, the transmission stage,
760 and the file system level.

761 **2.11.6 Security Controls**

762 Security controls—such as encryption, authentication, and authorization—are applicable to many
763 of the storage management and protection activities described in the previous sections. As stated
764 earlier, these security controls form part of the security recommendations of this document and
765 are detailed in Chapter 4.
766

767 **3 Threats, Risks, and Attack Surfaces**

768 This section provides background information regarding storage system security threats, risks,
769 and attack surfaces (where risks are the possible outcomes or goals of threats, and attack surfaces
770 are the possible means through which risks can manifest).

771 **3.1 Threats**

772 A threat is the adverse potential of an insecure state. Threats will often have a 1:1 correlation to
773 *types of attack* or *types of exploitable vulnerability*. The following sections provides a brief
774 overview of storage infrastructure-related threats.

775 **3.1.1 Credential Theft**

776 Credentials are used to verify the identity of users, authenticate them, and grant access to storage
777 systems and tools. Different forms of credentials exist, including physical keys, tokens and cards,
778 passwords, digital private keys, session cookies, digital certificates on websites, and more.
779 However, all of them are vulnerable to hackers using the right tools or techniques. The most
780 widely used and easily compromised are login-password credentials, which generate a significant
781 amount of risk to any organization. Credential theft is a growing industry within the
782 cybercriminal ecosystem. The market for credential theft is extremely broad with very high
783 potential as a result of the proliferation of cheap malware kits available online, a global increase
784 in active stealer campaigns, and ever more sophisticated tactics, techniques, and procedures
785 implemented by cybercriminals [22]. Password length and complexity alone are often
786 insufficient protection against an attack. In fact, almost all effective methods of credential theft
787 (other than password spray and brute force cracking) involve stealing the user's exact password
788 rather than randomly guessing it. Modern ransomware often scrapes passwords from the data sets
789 it has captured. Along with phishing and list cleaning via ransomware, keystroke logging—in
790 which malware virtually watches a user type in their password—is another method of credential
791 theft that works regardless of password complexity [23]. In many cases, login credentials are
792 stored within storage infrastructure. If this data is not properly encrypted at rest, and the storage
793 infrastructure is compromised, a hacker can gain access to a multitude of user credentials.

794 **3.1.2 Cracking Encryption**

795 Encryption is used to secure data at rest and in transit. In addition, encryptions are also used to
796 secure the sessions in which data at rest or in transit is managed and controlled. Encryption
797 algorithms make use of randomness to create keys or other key components. Encryptions can
798 have a range of weaknesses, from weak encryption algorithms and weak key generators to
799 server-side vulnerabilities, leaked keys, fundamental design flaws of bugs, and backdoors [24].
800 It is not only important to use strong encryption but to also properly secure the encryption keys.
801 When it comes to key generation, the same key should not be created twice. Some attacks aim to
802 disrupt the random number generator so that it issues the same random number for key
803 generation twice in a row [25].

804 3.1.3 Infection of Malware and Ransomware

805 Malware is the general term for any program that is designed to damage, disrupt, or hack a
806 device, whereas ransomware is a particular type of malware that blocks access to data until a
807 ransom fee is paid to its creator. Malware compromises a system, slowing down its basic
808 functions and breaching its security. It can be used to steal data, control a device/system, and
809 harvest the system's resources for illegal activities. Malware can infect a system in several ways.
810 Similar to viruses, it can be transmitted via file sharing, downloading free software, email
811 attachments, using compromised portable storage devices, and visiting infected websites [26].
812 Malware can be mistakenly installed on a storage management host and consequently cause
813 harm such as credential theft, privilege escalation, data corruption/loss/alteration, compromise
814 future backups, and more. In general, malware will use OS vulnerabilities to install itself and
815 perform various actions, meaning that more common operating systems will be more likely
816 attacked. For this reason, it would be easier to attack the storage management system than the
817 storage device itself.

818 Ransomware is a form of malware that encrypts the data in the storage systems, rendering it
819 unusable. The attacker then demands a ransom to restore access to the data upon payment. In
820 some cases, the attacker will publish confidential data that was collected from the storage system
821 to create urgency.

822 3.1.4 Backdoors and Unpatched Vulnerabilities

823 Backdoors and unpatched vulnerabilities could be used either directly or indirectly to bypass
824 other security controls.

825 Backdoors are software mechanisms or capabilities *intentionally* created by vendors or
826 individual contributors (and, in rare occasions, by states or malicious actors) for reasons often
827 considered legitimate by the author (e.g., to improve support, debugging, national security, etc.).
828 Given their dangerous potential, backdoors are not officially documented and are meant to be
829 known to a restricted set of individuals. However, over time, their existence could be
830 intentionally or unintentionally leaked or discovered by the public.

831 Unpatched vulnerabilities are *unintended* software side effects or dependencies not caught by
832 QA that present a security risk.

833 Once vulnerabilities are known—and especially if they are discovered in software versions that
834 are still publicly supported—vendors typically issue a software fix in the form of a patch or a
835 new version that closes the gap.

836 3.1.5 Privilege Escalation

837 Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight to gain
838 elevated access to resources that are normally protected from an application or user [27]. It is
839 highly linked to backdoors and vulnerabilities, and some might even consider it a sub-case.
840 Privilege escalation occurs in two forms: 1) vertical privilege escalation (also known as privilege
841 elevation), where a lower privilege user or application accesses functions or content reserved for

842 higher privilege users or applications, and 2) horizontal privilege escalation, where a normal user
843 accesses functions or content reserved for other normal users. In storage systems, this type of
844 threat can result in a wide variety of risks, including data corruption, data alteration, data loss,
845 and more. For example, an attacker can use elevated privileges to gain access to a storage system
846 and delete storage volumes and modify access configuration. The attack can also compromise
847 backup copies of the data (e.g., synchronous/asynchronous copies, snapshots) or the generation
848 of future backups. The privilege escalation itself can occur on various levels, such as the storage
849 components (e.g. storage array, host/client), the networking devices (e.g. the switch), or the
850 management systems (e.g. storage management systems).

851 **3.1.6 Human Error and Deliberate Misconfiguration**

852 Even with the existence of security controls, users may end up with a technically allowed storage
853 configuration that still presents an unacceptable exposure (e.g., mapping a restricted object
854 storage pool to a public network, stopping replication or backup for maintenance without
855 reenabling it afterwards). Such omission could be unintentional (i.e., an error) or deliberate (i.e.,
856 a sabotage).

857 Human errors take different forms, and some are significantly more difficult to identify or
858 prevent than others:

- 859 • Typos
- 860 • Lack of knowledge or unfamiliarity with internal security baselines and vendor best
861 practices
- 862 • Miscommunication between individuals or teams
- 863 • Errors related to the orchestration or automation of storage infrastructure
 - 864 ○ Direct, such as bugs in scripts and manifests
 - 865 ○ Indirect, such as unrealized software dependencies

866 **3.2 Risks to Storage Infrastructure**

867 Security risk is defined as:

868 “...the extent to which an entity is threatened by a potential circumstance or
869 event. Risk typically is a function of: (i) the adverse impacts that would arise if
870 the circumstance or event occurs; and (ii) the likelihood of occurrence.
871 Information system-related security risks arise from the loss of confidentiality,
872 integrity, or availability of information or information systems. These risks reflect
873 the potential adverse impacts to organizational operations (including mission,
874 functions, image, or reputation), organizational assets, individuals, other
875 organizations, and the Nation.” [28]

876 **3.2.1 Data Breach**

877 An incident that involves sensitive, protected, or confidential information being copied,
878 transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information
879 may include credit card numbers and associated data, personal health information, customer data,

880 company trade secrets, matters of national security, or any other proprietary or sensitive
881 information.

882 Data breaches can originate from an external source, such as a hacker or cybercriminal, or from
883 an internal source, such as a malicious insider or disgruntled employee. Data breaches can be
884 performed in a covert manner with traces being concealed or entirely removed or in a manner
885 that can be easily identified, whether this was deliberate or due to a lack of sophistication. The
886 impact of data breaches can span a wide range, from inconvenience to users to the devastating
887 exposure of sensitive/confidential data, resulting in irreparable damage to the reputation and
888 operational health of the organization.

889 **3.2.2 Data Exposure**

890 An incident that involves the inadvertent exposure of otherwise confidential information.
891 Sensitive data exposure occurs as a result of not adequately protecting a data asset (e.g., a file,
892 database, network share, object store) where information is stored. This might be the result of a
893 multitude of root causes, such as weak (or lack of) encryption, software flaws, loss of custody of
894 removable media, incorrect or too relaxed access limitations, or user data upload to an incorrect
895 location. Different types of data can be exposed in a sensitive data exposure. Banking account
896 numbers, credit card numbers, healthcare data, session tokens, Social Security numbers, home
897 addresses, phone numbers, dates of birth, and user account information like usernames and
898 passwords are some of the types of information that can be left exposed [29]. Unlike *Data*
899 *Breach*, which involves an active action by a malicious actor, data exposure can occur by
900 mistake, such as when data is left exposed in a database, host, or other storage infrastructure for
901 anyone or specific unauthorized users to see. Examples of data exposure include transmitting
902 confidential information to the wrong recipient, mistakenly making sensitive data available for
903 search on a public search engine, mistakenly configuring access control to allow read permission
904 to sensitive information to unauthorized users/user groups, placing data in publicly available
905 object stores, using weak cryptographic algorithms or keys, not implementing hashed and salted
906 password practices (which is a form of cryptography similar to encryption), and other unsecure
907 data storage practices [29].

908 **3.2.3 Unauthorized Data Alteration and Addition**

909 Unauthorized data alteration or addition is an incident that involves the illegal, unauthorized, or
910 fraudulent alteration of data. It is the process of modifying data before or after it is entered into
911 the system. In this case, the attacker gains access to the data storage infrastructure and modifies
912 the data in a way that will force future transactions to use inaccurate information. Data alteration
913 and addition can originate from both an external and internal source in a covert and/or easily
914 identifiable manner. In certain cases, this type of risk is realized using the “salami attack”
915 method, in which the attacker steals a little bit at a time over a long period of time from a large
916 number of transactions (e.g., by rounding up small sums). The impacts of data alteration and
917 addition can range from the loss of funds to permanent damage to reputation and trust.

918 **3.2.4 Data Corruption**

919 Data corruption refers to errors in data that occur during writing, reading, storage, transmission,
920 or processing and which introduce unintended changes to the original data. In general, when data
921 corruption occurs, a file containing that data will produce unexpected results when accessed by
922 the system or the related application. Results could range from a minor loss of data to a system
923 crash. For example, if a document file is corrupted, when a person tries to open that file with a
924 document editor, they may get an error message, and the file might not be opened or might open
925 with some or all of the data rendered unintelligible. Some types of malware may intentionally
926 corrupt files as part of their payloads, usually by overwriting them with inoperative or garbage
927 code, while a non-malicious virus may also unintentionally corrupt files when it accesses them.

928 **3.2.5 Compromising Backups**

929 The backup, or archiving of copies, of data assets is important to enable the recovery of said
930 assets when they are damaged or lost. Satisfactory recovery is possible only if the backup copies
931 are generated correctly with an appropriate retention and currency, stored in a secure manner,
932 and accessible in a manner that allows timely restoration. Since these prerequisites are
933 codependent, backup is sensitive to multiple failures. For example, incorrect configuration could
934 involve a live database backup performed without applying techniques to ensure consistency or
935 write-order fidelity. Insufficient currency or retention could mean that at least some portion of
936 the data, past or new, will be unrecoverable. An attacker, therefore, has a high motivation to
937 target not only a “primary” data asset but also its copies. When existing copies cannot be
938 compromised, another viable attack strategy could be to interfere with the backup process itself,
939 thereby gradually “poisoning” future copies. When enough time has passed, the attacker can
940 return to the original goal of compromising the primary data assets, knowing that the only
941 available copies for recovery are too old.

942 Another type of “poisoning” strategy is to specifically infect backup copies of compute or
943 application assets, such as OS images, software packages, or even source code repositories. This
944 way, when an individual component or even an entire environment is rebuilt in an attempt to
945 battle an infection, at least some portions of the malware will be included in the restored
946 environment, allowing the attacker to quickly inflict more damage.

947 **3.2.6 Data Obfuscation and Encryption**

948 The reversible obfuscation and/or encryption of data results in data becoming unavailable to the
949 user or organization unless it is decrypted using an encryption key. This type of risk is
950 commonly used in ransomware attacks. Ransomware is a form of malware that encrypts the
951 victim’s data while demanding a ransom to restore access to the data upon payment. Originally
952 targeting data/files on users’ computers or enterprise servers, ransomware has evolved to also
953 include other storage components, such as NAS and backup appliances [30]. Data obfuscation
954 and encryption typically originate from an external source but could also potentially originate
955 from an internal one. Since it is reversible and commonly used as part of ransomware attacks, it
956 is meant to be identified and is commonly accompanied by a threat and ransom instructions. The

957 impact of data obfuscation and encryption can range from the loss of funds to permanent damage
958 to reputation and trust.

959 **3.2.7 Data Availability and Denial of Service**

960 In a data availability or denial-of-service incident, the data client cannot gain access to some or
961 all of their data. A data availability disruption risk can occur due to purposeful or unintended
962 damage to the communication path or access configuration. The damage can be physical, such as
963 a disconnection along the communication path, or logical, such as the misconfiguration of an
964 endpoint of network components. For example, an attacker can delete the SAN masking settings
965 of a block storage device or suspend the export setting in NFS so that clients will be unable to
966 access their data. Although the damage may be reversible (e.g., by restoring the settings that
967 were deleted), it may cause temporary disruptions and downtime for the system or service. A
968 denial-of-service (DoS) attack will also achieve disruption to data availability by flooding the
969 targeted machine or resource with superfluous requests in an attempt to overload systems and
970 prevent some or all legitimate requests from being fulfilled. DoS attacks could potentially impact
971 not only individual data assets and clients but also an entire fabric.

972 **3.2.8 Tampering of Storage-Related Log and Audit Data**

973 The tampering of storage-related log and audit data is where an attacker deletes or modifies log
974 data to prevent an effective audit trail in an effort to conceal the attack (in real-time or
975 afterwards) or to mislead the people investigating attacks with false information. The logs can be
976 partially modified, such as by modifying the timestamp. The impact of this risk is that the
977 attacker/attack can remain unnoticed by security systems that rely on log data. During this
978 period, the attacker can perform additional lateral movements that may jeopardize the data and/or
979 service. For example, a brute force attack to log into a sensitive system may be concealed by
980 deleting the login attempts from the logs. Another form of this risk involves tampering with the
981 logging mechanism itself (e.g., disabling it, filling up all free space with synthetic messages,
982 convincing clients to send log data to rouge log servers, etc.).

983 **3.2.9 Mapping of Threats to Risks**

984 The following table provides a mapping of threats discussed in Section 3.1 to the risk outcomes
985 discussed in Section 3.2.

986

| Threats – Insecure States and Adversary Capabilities | <i>Occurrence – Risk Outcomes</i> |
|--|---|
| Privilege escalation | <p><i>Application system</i> – Data breach, data exposure, unauthorized data alteration, data corruption</p> <p><i>Administrative system</i> – Compromise of existing and future backups, ransomware attack, DoS attack, tamper storage-related log and audit data, unsafe storage configuration parameters</p> |
| Credential theft | Depending on whether user credentials or administrator credentials are compromised, all risk outcomes for privilege escalation apply to this threat. |
| Cracking encryption | Data breach and exposure of (a) data at rest, (b) data in transit, and (c) user/administrator session data |
| Infection of malware and ransomware | <p>Malware can enable other threats – Privilege escalation, credential theft</p> <p>Malware, depending on where it is present – application systems or administrative systems can impact all risk outcomes in Section 3.2</p> |
| Backdoors and unpatched vulnerabilities | Depends on the nature of the vulnerability, but in many cases, all risk outcomes for privilege escalation apply to this threat |
| Human error and deliberate misconfiguration | Depending on its type and scope, misconfiguration can impact all risk outcomes in Section 3.2 |

987 **3.3 Attack Surfaces**

988 Attack surfaces are defined as “the sum of the different points (the “attack vectors”) where an
 989 unauthorized user (the “attacker”) can try to enter data into or extract data from an environment”
 990 [31]. This section will list common digital and physical attack surfaces that are related to storage
 991 infrastructure.

992 3.3.1 Physical Access

993 Physical access to storage infrastructure involves physical intrusion into the data center, its
994 perimeter, communication infrastructure (including cabling), or physical objects in transit (e.g.,
995 physical hosts, storage arrays, hard drives, tapes). Such intrusion is performed in order to access,
996 steal, or damage the data or prevent its availability. The physical intrusion can occur by “overt
997 access” in which the attacker will masquerade as someone who belongs in the situation (e.g., by
998 playing the part of a cleaning employee, technician, or building maintenance personnel).

999 “Tailgating” is another way to access restricted areas in the data center. For example, an intruder
1000 gains entry to a network operations center by carrying a tray of food. Although the data center is
1001 protected by biometrics, the staff may open the door for the intruder and the food. Other
1002 intruders may simply follow employees in. Physical access protection is essentially the last line
1003 of defense. An intruder who gains access to storage infrastructure can ultimately steal, duplicate,
1004 harm, or destroy media and data. An intruder can also connect to the storage system port, insert a
1005 removable media to a physical port that may be used for firmware updates or to a management
1006 terminal, access data, and damage it. However, even if the storage system is well-protected by
1007 physical restrictions, an attacker can physically target additional components of the storage
1008 infrastructure that may be less protected, such as switches and management terminals. The
1009 attacker can target the data ports to intercept the data itself or the management ports.
1010 Communication cables are also a vulnerability. A sophisticated attacker can potentially tap into
1011 the storage communication by physically accessing the cables. Another physical access method
1012 involves replacing peripheral components, such as the keyboard and mouse, with infected
1013 components (e.g., infiltrating an infected keyboard that includes a “keylogger” component that
1014 transmits sensitive data, such as usernames/passwords, or infects the system with malware). An
1015 additional form of physical access is accessing removable media that is transported between
1016 storage sites. In some cases, companies back up large amounts of data on removable media and
1017 then transport this removable media to a remote DR site. The removable media can potentially be
1018 compromised or intercepted in transit.

1019 3.3.2 Access to Storage OS

1020 Access to a storage OS attack surface involves intrusion into a storage device by exploiting
1021 operating system vulnerabilities. The term “storage OS” refers to all of the operating systems
1022 that are related to the storage infrastructure. This includes storage arrays, switches, data
1023 protection appliances, and storage virtualization appliances. In many cases, the operating systems
1024 running these devices are based on a version of the Linux/Unix operating system, which is
1025 generally more closed or secure than general-purpose OS distributions. However, all operating
1026 systems include security vulnerabilities and are therefore regularly updated with security updates
1027 and patches. In addition, any operating system has configurations that may influence its security.
1028 An attacker can gain access to the storage OS by a variety of methods, from a local login process
1029 (using a standard protocol, such as SSH, ‘rshell,’ ‘telnet,’ etc.) through remote login using TCP-
1030 IP or through an OS vulnerability.

1031 **3.3.3 Access to Management Hosts**

1032 Most storage components are managed or configured through computing devices called
1033 management hosts, which run an operating system that is usually some variation of a commercial
1034 OS. By infiltrating the management host with malware or through an OS vulnerability, an
1035 attacker can, for example, hack an executable, read cached data, install a memory tap that reads
1036 data from the memory, install malware, and gain access to the related storage array and/or its
1037 configuration. Consequently, through the management host, an attacker can realize most related
1038 risks, including data corruption, data loss, data alteration, compromising of future backups,
1039 tampering log and audit data, and more. Access to management hosts provides the attacker with
1040 the ability to cause almost unlimited damage to the entire domain that is being managed by the
1041 management host.

1042 **3.3.4 Management APIs, Management Software, In-band Management**

1043 Storage infrastructure components expose management software UI, APIs, and other in-band or
1044 out-of-band management protocols for administering the devices and managing data storage. In
1045 some cases, the device has a management interface (e.g. SOAP or REST API) and, in parallel,
1046 management software that is installed on a management host. All of these interfaces create a
1047 variety of attack surfaces. For example, an attacker can access a storage device by impersonating
1048 the management host or software through the management API. In this case, the attacker does
1049 not need to infiltrate the management software in order to gain access to the management
1050 capabilities. Some equipment allows in-band access via the data links (e.g., Fiber Channel paths).
1051 The storage device allows in-band management access through the same connection plane used
1052 for providing the storage service. By doing so, it opens yet another attack surface, which can be
1053 exploited by attackers that can impersonate a storage client while sending management
1054 commands.

1055 **3.3.5 Storage Clients**

1056 Storage clients are compute components, or applications installed on compute components, that
1057 use the storage protocol to read/write data from a storage object or network. If a storage client is
1058 compromised, the attacker can potentially read the data that is consumed by the storage client,
1059 write data to the storage device or object, and encrypt data. In addition, if in-band access to the
1060 storage is enabled, the attacker impersonating the storage client can send management
1061 commands. Archiving systems may sometimes use a storage client to gain access to data in order
1062 to create backups. If the storage client is compromised, the attacker can also harm future
1063 backups. In this scenario, the attacker can then wait for a while, harming the ability of the
1064 organization to defend itself because it will not be able to use its compromised backups.

1065 **3.3.6 Storage Network (Tap Into, Alter to Gain Access)**

1066 When storage clients consume data from the storage systems, the data is transferred through a
1067 variety of storage network components (i.e., data in transit), such as storage switches, cables, and
1068 extenders. If such components are compromised, the attacker can tap into the data path and copy,
1069 view, reroute, or steal data. In addition, the attacker can read configuration data, management

1070 traffic, or other metadata (e.g., if the data in transit may include user credentials, encryption
1071 keys, and more). By compromising a network component, an attacker can also potentially
1072 perform data corruption, alteration, or addition by modifying the payload. Another form of attack
1073 is “man in the middle” (MITM), specifically Fibre Channel man-in-the-middle attacks. The
1074 purpose of the MITM is to sniff data, alter it, or bypass encryption and authentication
1075 mechanisms. A switch will only transmit information to the correct port, not allowing any other
1076 ports to see any communication that is not theirs. An entity using IP, such as a switch or an
1077 operating system, will send out ARP (Address Resolution Protocol) requests when it is trying to
1078 communicate with other entities. The issue with ARP is that any malicious entity could send out
1079 an ARP reply instead of the actual server. Since there is no authentication with ARP, similar to
1080 how there is no authentication with PLOGI in Fibre Channel fabrics, an entity receiving an ARP
1081 reply from an attacker would update their routing table with the incorrect information.
1082 Furthermore, even if a node did not send out an ARP request, which would request the MAC
1083 address of a specific IP address, it could potentially receive an ARP reply and update its own
1084 routing table. For example, an attacker could send out ARP replies to the entire network
1085 segment, telling each entity that the MAC address of the router, which is 172.16.1.1, is actually
1086 the MAC address of the malicious entity. When one node tries to communicate to any other node
1087 by going through the default router, it will actually be going to the malicious entity first since it
1088 is using the MAC address of the malicious entity for layer 2 routing [32].

1089 **3.3.7 Compute Environment of Key Individuals – Storage Admins**

1090 Storage administrators sometimes have remote access to the storage infrastructure. For example,
1091 the storage admin may have a computer that is remotely connected to the storage’s management
1092 host. The compute environment of such key individuals can be exploited to gain access to and
1093 compromise the storage infrastructure. For example, an attacker can install malware on this
1094 compute environment that will, in turn, install a key logger that allows for the interception of
1095 login credentials. This compute environment is therefore a potential attack surface.

1096 **3.3.8 Electricity Network**

1097 Since storage infrastructure is connected to the electricity grid, the electricity network may
1098 potentially become an attack surface. A huge spike in electrical current, such as the kind caused
1099 by lightning, can potentially damage and even erase data that is stored in electromagnetic discs.
1100 Voltage fluctuations that correspond to keystrokes create noise in the ground line. The ground
1101 line noise can be intercepted by a hacker connected to a nearby power socket. Another method is
1102 through a malware dubbed *PowerHammer*, which can stealthily exfiltrate data from air-gapped
1103 computers using power lines. This malware exfiltrates data from a compromised machine by
1104 regulating its power consumption, which can be controlled through the workload of the device’s
1105 CPU. Sensitive pieces of information, such as passwords and encryption keys, can be stolen one
1106 bit at a time by modulating changes in the current flow. In the line level variant of this attack, the
1107 attacker intercepts the bits of data exfiltrated by the malware by tapping the compromised
1108 computer’s power cable. In the phase level attack, the attacker collects the data from the main
1109 electrical service panel. The data can be harvested using a non-invasive tap that measures the
1110 emissions on power cables and then converted to a binary form via demodulation and decoding
1111 [33].

1112 4 Security Guidelines for Storage Deployments

1113 4.1 Physical Storage Security

1114 Physical security is fundamental to the overall safeguarding of any IT infrastructure. Most
1115 software-based security controls can be compromised if an attacker gains access to the physical
1116 facility and equipment.

1117 In many regards, physical security requirements for storage infrastructure are identical to those
1118 of other infrastructure elements like computers and network equipment (e.g., facility security,
1119 surveillance, transportation, etc.). These are well covered by multiple publications, including
1120 NIST SP 800-171 [34]. Additional valuable discussion regarding media disposal and destruction
1121 is available in ISO 27040 ([10]).

1122 It is, therefore, beyond the scope of this document to cover all physical storage security aspects.
1123 Rather, focused guidance is provided for physical security aspects that are unique to storage
1124 infrastructure or are less emphasized in other publications.

1125 **PS-SS-R1 – Media security measures:**

- 1126 (a) Follow general recommendations, NIST SP 800-171, Section 3.8 (including protection,
1127 access restriction, sanitization, marking, transportation, cryptography, removable media,
1128 confidentiality, disposal).
- 1129 (b) Lifecycle management should include purchasing media from a trusted source.
- 1130 (c) Physical media and backups of sensitive data, which are used for data protection, should be
1131 stored in sufficiently distant locations, away from the primary storage.
- 1132 (d) For sensitive information, a comprehensive inventory of storage media (cataloging) must be
1133 kept to track its location, ownership, capacity, and other relevant configuration attributes.
1134 Particular attention should be paid to tracking the actual content of media, including:
- 1135 • Sensitivity level
 - 1136 • Classification (what type of data it stores, what applications and business services it
1137 relates to)
 - 1138 • Encryption level
 - 1139 • Potential impact if compromised or stolen (e.g., compromise of financial or medical
1140 information; leak of passwords, certificates, or encryption keys).
 - 1141 • Mitigation/contingency steps or procedures to employ (e.g., including changing
1142 passwords, re-issue keys, re-encrypt data, notify relevant stake holders)
 - 1143 • Dependencies between the data and other application
- 1144 (e) Consider using advanced tracking controls on sensitive removable media, such as RFID tags,
1145 GPS tracking devices, tamper protection, and for extremely sensitive information triggered
1146 self-destruction mechanism (self-activated and/or remotely controlled).

1147 **PS-SS-R2 – Protect all sensitive administrative equipment:** Sensitive workstations, which can
1148 be used to obtain administrative access to storage infrastructure, must be managed using
1149 corporate-approved security controls for access, surveillance, and auditing, including physical
1150 security. If possible, the same security measures required to protect the data itself should apply to

1151 the management workstations. This includes workstations located outside of the facility storing
1152 the data as well as work-from-home environments, when used.

1153 **PS-SS-R3 – Ensure that the data sanitization approach is sufficiently broad:** Certain
1154 elements capable of storing sensitive information are sometimes overlooked when disposing of
1155 storage equipment, including non-volatile memory and cache objects (often found in storage
1156 arrays), firmware/BIOS settings, and HBA-level settings (which can contain WWNs, masking,
1157 IP addresses, passwords). Ensure that all of those elements are considered.

1158 **4.2 Data Protection**

1159 Section 2.11.4 discusses the objectives and associated activities of data protection, the three
1160 facets based on the range of objectives, and primary controls from the point of the view of the
1161 storage facet. To reiterate, these controls are:

- 1162 • Data backup and recovery,
- 1163 • Replication technologies,
- 1164 • Continuous data protection, and,
- 1165 • Point-in-time copies and snapshots.

1166 The security recommendations in this section provide the due diligence aspects associated with
1167 implementing each of the controls above. Each recommendation has a unique identifier with
1168 format DP-SS-Rx, where DP stands for data protection, SS stands for secure storage, and Rx for
1169 the recommendation sequence.

1170 **4.2.1 Data Backup and Recovery**

1171 **DP-SS-R1:** The backup plan or policy should be established prior to deployment and should
1172 include, at the minimum, the following:

- 1173 (a) Type of backup (e.g., full or incremental/differential, the use of CDP, versioning, replication,
1174 and point-in-time copies as part of the backup scheme)
- 1175 (b) Frequency of backup (in particular, to meet RPOs)
- 1176 (c) Retention period
- 1177 (d) Types of media to be used
- 1178 (e) Encryption requirements (in particular, backup encryption methods used should be at least as
1179 secure as those applicable to protected data)
- 1180 (f) Other protection requirements, such as digital signing, location, facility security (including
1181 fire, explosion, and magnetic interference protection), immutability and locking, and a
1182 minimum number of copies per backup set and their geographic distribution
- 1183 (g) Reference to applicable regulatory frameworks with appropriate controls
- 1184 (h) Restore procedures

1185 **DP-SS-R2:** The backup plan or policy should be comprehensive enough to:
1186 (a) Cover all data assets of the enterprise irrespective of where they reside (i.e., on-premise or in
1187 the cloud)
1188 (b) Be organized by the type of data involved (e.g., Tier 1, Tier 2, etc.)
1189 (c) Consider data integrity at the application and business process levels (e.g., if two components
1190 must be recovered to the same point in time to function properly, then federated consistency
1191 mechanisms or equivalent should be planned and implemented)
1192 (d) Consider the required restoration speed to meet business or regulatory requirements (e.g., for
1193 mission critical data with requirements for fast recovery or RTO, consider the use of point-
1194 in-time copies, such as snapshots of clones, as opposed to tape or over-WAN recovery)

1195 **DP-SS-R3:** In addition to a backup plan or policy, standard operating procedures relating to the
1196 backup should:

1197 (a) Monitor the execution of backups based on policy and associated notification mechanisms.
1198 (b) Periodically test backups (at least monthly for critical data) to verify their integrity and their
1199 ability to be restored.
1200 (c) Ensure copy hygiene. An up-to-date recovery catalog should be kept for each copy that
1201 records which anti-malware tools it has been scanned with and what the results of the scans
1202 were. For sensitive data, it is further recommended to periodically scan at least a subset of
1203 past copies with current anti-malware tools to identify “poisoned” copies.
1204 (d) Periodically review (at least annually) the backup plan and operations procedures.
1205 (e) Maintain an audit trail that provides the information necessary to ensure conformance of the
1206 backup operations consistent with the policy.
1207 (f) Employ special controls when necessary (e.g., refreshing old, at risk, retired media by
1208 copying to new one).

1209 **DP-SS-R4:** The data protection configuration management (including backup, point-in-time
1210 copies, and replication) should be centrally managed and separated from the data consumption
1211 plane. In particular, servers and clients should not be allowed to change their own data protection
1212 configuration.

1213 **4.2.2 Replication**

1214 **DP-SS-R5:** In both synchronous and asynchronous replication, the same level of data protection
1215 (e.g., encryption of data at rest, access restrictions) that is used in the primary storage should be
1216 carried over to the secondary storage.

1217 **DP-SS-R6:** The confidentiality of data in transit during replication should be protected using
1218 encryption.

1219 **DP-SS-R7:** When synchronous replication is critical, the primary storage server should have a
1220 feature to disallow any writes (or accept any write transaction request) on the data it stores if its
1221 synchronization with the secondary storage server is lost, and it should only resume processing
1222 when synchronization is restored.

1223 **DP-SS-R8:** Obsolete replicas should be removed to reduce the attack surface.

1224 4.2.3 Point-in-Time Copies and Snapshots

1225 **DP-SS-R9:** When point-in-time copies, such as snapshots, are used as part of the backup
1226 scheme, they should be configured accordingly:

- 1227 (a) To meet the recovery point objective (RPO) requirements of the target data sets in the
1228 snapshot. For example, if the business or compliance standards require that no more than five
1229 minutes of committed data could be lost in recovery, then the snapshot interval must be five
1230 minutes or less.
- 1231 (b) To meet retention requirements. For example, if hourly copies are required for at least 48
1232 hours, ensure that a sufficient number of hourly snapshots is preserved.

1233 **DP-SS-R10:** Obsolete snapshots and clones should be removed to reduce the attack surface.

1234 4.2.4 Continuous Data Protection

1235 **DP-SS-R11 – Security considerations for using CDP:** Other than the functional benefits (e.g.,
1236 improved RPO, finer-grained retention), the use of CDP or similar techniques (e.g., versioning of
1237 source data or replicas in AWS S3, Azure Blob) can also assist in improving forensics, when
1238 applicable. Replaying to previous versions of data can help one learn more about the attack
1239 profile and, in particular, better estimate attack times.

1240 4.3 Authentication and Data Access Control

1241 Storage infrastructure systems are administered by designated users who use various accounts to
1242 access these systems. The administrative users and their management hosts constitute an
1243 important attack surface that can be exploited by attackers. Since the individuals managing
1244 storage systems and infrastructure are generally privileged users, the allocation and use of
1245 privileged access rights should be restricted and controlled. Inappropriate use of system
1246 administration privileges can be a major contributory factor to the failures or breaches of storage
1247 systems.

1248 A least privilege model that leverages specific roles should be implemented. According to ISO
1249 Standard ISO/IEC 27040 [10], the following roles should be implemented and used within
1250 storage technologies:

- 1251 • **Security Administrator** – This role has view and modify rights to establish and manage
1252 accounts, create and associate roles/permissions for audit logging configurations and
1253 contents (audit log event entries can never be changed), establish trust relationships with
1254 IT infrastructure (e.g., shared secrets for RADIUS), manage certificate and key stores,
1255 manage encryption and key management, and set access controls.
- 1256 • **Storage Administrator** – This role has view and modify rights for all aspects of the
1257 storage system. No access is granted to security-related elements or data.
- 1258 • **Security Auditor** – This role has view rights that allow for entitlement reviews,
1259 verification of security parameters and configurations, and inspections of audit logs. No
1260 access is granted to the storage, configuration, or data.

- 1261 • **Storage Auditor** – This operator-like role has view rights that allow for the verification
1262 of storage parameters and configurations and inspections of health/fault logs. No access
1263 is granted to security-related elements or data.

1264 **4.3.1 Authentication Recommendations**

1265 **AC-SS-R1 – Unique Identifier for all users:** All administrators should have a unique identifier
1266 for their personal use only. This requirement is important for accountability and audit purposes
1267 as well as for the ability to control access on the individual user level.

1268 **AC-SS-R2 – A centralized authentication solution:** A centralized authentication solution (e.g.,
1269 such as Active Directory, Remote Authentication Dial-In User Service [RADIUS], single sign-
1270 on [SSO]) should be deployed to enable the close monitoring and control of user access and to
1271 ensure uniform enforcement of the organization’s authentication policies. The use of the
1272 authentication and permissions management module that comes with the storage product should
1273 be avoided and preferably disabled.

1274 **AC-SS-R3 – Configuration of authentication servers:**

- 1275 (a) The designation of servers to perform authentication services should be strictly controlled,
1276 and their validity should be periodically checked to detect and prevent the introduction of any
1277 rogue or unauthorized authentication servers.
1278 (b) There should be multiple authentication servers to ensure availability and avoid single points
1279 of failure.

1280 **AC-SS-R4 – Secure connection to centralized authentication server:** All communication
1281 between the centralized authentication server and the authenticating clients should be secured
1282 through protocols such as TLS.

1283 **AC-SS-R5 – Use of multi-factor authentication:** Access configuration to storage infrastructure
1284 components that store mission-critical data should be protected using a minimum of two-factor
1285 authentication.

1286 **4.3.2 Password Recommendations**

1287 **AC-SS-R6 – Secure password policies should cover service accounts:** The secure password
1288 policies should be applied not only to individual accounts but also to service accounts (e.g.,
1289 SNMP, NDMP) and accounts used by automation tools. Some vendor publications suggest at
1290 least 16 randomized characters for NDMP and 20 for SNMP.

1291 **AC-SS-R7 – Password Length:** A good passphrase should have at least 15, preferably 20,
1292 characters.

1293 **AC-SS-R8 – Password Complexity:** A good passphrase should combine uppercase and
1294 lowercase letters, digits, and special characters. They should not be similar to usernames and
1295 should not include repeated character sequences.

1296 **AC-SS-R9 – Password expiration:** Expiry times should be set for all passwords. Passwords for
1297 administrative accounts should be set shorter than user words.

1298 **AC-SS-R10 – Password reuse:** Users should be prohibited from reusing at least the four
1299 previous passwords (or more) based on organizational risk factors.

1300 **AC-SS-R11 – Password caching:**

1301 (a) Passwords should not be cached on the server, desktop, or any other system.

1302 (b) Sufficiently short TTL or an equivalent control mechanism should be employed to guarantee
1303 that changes are propagated quickly throughout the network.

1304 **AC-SS-R12 – Saving passwords:** Passwords should not be saved anywhere in cleartext (e.g.,
1305 not in files) or in scripts. Furthermore, enabling storage management applications to locally
1306 remember users and passwords for automatic login should never be used, even if passwords are
1307 stored encrypted, unless managed through an authorized central authentication service, such as
1308 LDAP SSO.

1309 **AC-SS-R13 – Eliminate or change default passwords:** The default passwords that come with
1310 system installation or deployment must be immediately changed.

1311 **4.3.3 Account Management Recommendations**

1312 **AC-SS-R14 – Use of accounts unassociated with system users:** Accounts not associated with
1313 any system user (e.g., not in an active directory, such as “guest,” “anonymous,” “nobody”)
1314 should be disabled. In situations where they need to be used, they should not be mapped to any
1315 system user, and all of their default configurations (e.g., password, privileges) should be changed
1316 to conform to organization-wide policies.

1317 **AC-SS-R15 – Account lockout:** Users should be temporarily or permanently locked out after a
1318 certain number (preferably three) of unsuccessful login attempts.

1319 **AC-SS-R16 – A local user account for emergency purposes:** A single local user account
1320 should be maintained for access to storage resources in order to provide emergency-only access
1321 if the centralized authentication system is down. This account should conform to all
1322 organizational policies (e.g., password length, complexity).

1323 **AC-SS-R17 – Eliminate or disable default user accounts:** The default user accounts that come
1324 with the storage system installations should be eliminated or disabled immediately. When there
1325 is a justified reason to keep any of those accounts, review and change its privileges to the
1326 minimum required.

1327 **AC-SS-R18 – Limit local and default user accounts:** As much as possible, eliminate the use of
1328 local and default accounts. In situations where this is not possible:

- 1329 (a) Limit the use of such accounts and the privileges they have.
- 1330 (b) Password policies should apply to all user, local, and default accounts, including those with
1331 administrative rights.
- 1332 (c) An exception for password expiration may be considered for the emergency account if its use
1333 is only allowed during a real emergency and providing that the password changes after each
1334 incident.

1335 **4.3.4 Privilege and Session Management Recommendations**

1336 **AC-SS-R19 – Roles and responsibilities configuration:** At a minimum, the four roles in the
1337 ISO Standard ISO/IEC 27040 [10] must be implemented for all access to storage resources (i.e.,
1338 Security Administrator, Storage Administrator, Security Auditor, Storage Auditor) See Section
1339 4.2 for more details.

1340 **AC-SS-R20 – Separate roles of administrative account types:** A critical aspect of storage
1341 security is to separate administrative control planes. (For example, if attackers gain control over
1342 a host or compromise a host admin role, they could not trivially compromise its data assets,
1343 backups, and replicas.) At a minimum, this includes:

- 1344 (a) The privileges required for *data management* (e.g., create and map a volume or share) and
1345 *data protection* (e.g., configure, stop, and delete backup) should be assigned to different
1346 roles.
- 1347 (b) The privileges required for *data management* and *host administration* should be assigned to
1348 different roles.

1349 **AC-SS-R21 – The privileges assigned to any role should adhere to the principle of “least
1350 privilege”:** The permissions assigned to a role should be no more than what is required to
1351 perform the functions designated for that role.

1352 **AC-SS-R22 – Enable session expiration/timeout:** All inactive open sessions between the client
1353 and a storage infrastructure system should be terminated through an automatic logout. This
1354 recommendation is applicable to all accounts that access the storage infrastructure (e.g., CLIs,
1355 APIs, etc.) but is especially important and mandatory for admin accounts.

1356 **AC-SS-R23 – Implement a “message of the day” and “login banner” notice:** The “message
1357 of the day” or “login banner” notice should appear on every login to any storage infrastructure
1358 component or system via UI, CLI, or API (if applicable). The message should include a legal
1359 notice and a warning that the user is accessing a restricted system with sensitive data, as well as
1360 any additional warnings and meaningful messages, according to the organization’s security and
1361 privacy policies.

1362 **AC-SS-R24 – Eliminate unnecessary replication trust between storage devices:** When arrays
1363 do not have shared replicated volumes, disable the replication trust relationship between them.

1364 4.3.5 SAN-Specific Recommendations

1365 The topic of SAN-related access control involves multiple aspects. Some overlap with *Network*
1366 *Configuration* and *Administrative Access*, which are covered in other sections.

1367 To eliminate repetition:

- 1368 • Access control recommendations closely related to the *network infrastructure* (e.g.,
1369 switch, port, HBAs, and NICs configuration; additional zoning guidelines) and *protocols*
1370 are discussed in Section 4.6.
- 1371 • Administrative access is discussed in Section 4.10.
- 1372 • Data-related access control is discussed in this section.

1373 For a complete appreciation of all access control aspects, please refer to all three sections.

1374 **AC-SS-R25 – LUN access control:** The set of hosts that can access a set of SAN storage
1375 devices must be restricted through zoning (software or hardware) and masking to the minimum
1376 required access.

1377 **AC-SS-R26 – LUN copy and replica access control:** The set of hosts that can access a set of
1378 SAN-replicated LUNs, Snapshots, and other types of point in time copies of LUNs should be
1379 similarly restricted through zoning and masking to the minimum required access. Note that in
1380 many cases, a host granted access to a device should not be allowed to access a copy.

1381 **AC-SS-R27:** The default zone should always be configured as “deny all.”

1382 **AC-SS-R28:** The zoning should be implemented in a switched SAN fabric based on sound logic,
1383 particularly as it relates to the separation of environments and traffic type, such as the following
1384 which should be separated to the maximum possible extent:

- 1385 (a) Separation based on environment: *development* vs. *test* vs. *production*, etc.
- 1386 (b) Type of traffic: data access vs. management vs. replication vs. backup
- 1387 (c) Type of hosts: *virtualized* vs. *physical*
- 1388 (d) Storage device type: *tape* vs. *disk*

1389 **AC-SS-R29:** When software zoning is implemented, care should be taken to ensure that a host
1390 can only connect to storage devices provided by the simple name server (SNS) (by looking it up
1391 at the software zoning table) and not directly using device discovery.

1392 **AC-SS-R30 – Ensure allowlisting of devices that can join fabric:** The policy specification
1393 feature in SAN that enables the creation of an allowlist of switches, arrays, and hosts that can
1394 join the fabric must be leveraged where applicable and carefully configured.

1395 4.3.6 File and Object Access Recommendations

1396 **AC-SS-R31 – Restricting access to storage objects to the minimum possible:** Follow the
1397 principle of least privilege, including:

- 1398 (a) Access to storage objects for all protocols (e.g., CIFS, SMB, NFS, and object storage
1399 such as Amazon S3 and Azure Blob) should be restricted based on client IPs and/or
1400 relevant subnets, and the ports/protocols should be required.
- 1401 (b) If supported, finer-grained access control mechanisms (e.g., by role, ID, labels, accounts,
1402 VPC, VPC endpoints, etc.) must also be used.
- 1403 (c) Prefer granting access to centrally managed users and roles only, such as Active
1404 Directory and IAM, and not to local users of the specific system.
- 1405 (d) Make sure that the default access to any share is set to “deny all” or equivalent.
- 1406 (e) Disable or remove default shares unless they have a specific purpose, in which case
1407 review and adjust access rights to the minimum required.
- 1408 (f) Provide the minimal access rights (e.g., read, write, execute, modify, delete, view ACLs,
1409 change ACLs, etc.), which could typically be adjusted individually.
- 1410 (g) Prefer using ACLs in addition to the native OS user, group, or admin permission models.

1411 **AC-SS-R32 – Avoid permitting anonymous, null, guest, or “public access” users:** Such users
1412 are typically able to perform network discovery without the need to authenticate. If it is
1413 absolutely essential to have this type of user, make sure it is mapped to the “nobody” user group
1414 and not to ID 0.

1415 **AC-SS-R33 – Regularly audit file and object security settings:** Perform regular audits of all
1416 the security settings mentioned above.

1417 **AC-SS-R34 – Scan files with anti-malware tools on-access:** Every time a file is accessed, it
1418 should first be scanned with anti-malware tools to ensure that it has not been compromised.

1419 **AC-SS-R35 – Granular permission assignment:** For file and object sharing systems (e.g.,
1420 NFS, CIFS, S3 buckets, etc.), prefer granting permissions at a finer level of granularity rather
1421 than a coarser one (e.g., file or object over folder or label, over share or bucket).

1422 **AC-SS-R36 – In NFS, avoid sharing with execute-as-root allowed:** While executing
1423 mounting, the “nosuid” option should be used to prevent programs from being executed as a root
1424 user on the client. In general, NFS clients should not be allowed to run “suid” and “sgid”
1425 programs on exported file systems.

1426 **AC-SS-R37:** In NFS, for files that are to be used in the “read only” mode, the mount
1427 configuration for corresponding NFS shares should always have the “noexec” option.

1428 **AC-SS-R38 – Export of administrative file systems should not be allowed:** This includes the
1429 ‘/’ filesystems, restricted OS/storage array system folders, etc.

1430 **AC-SS-R39 – When CIFS is used, “Full Control” permissions should not be granted** to any
1431 user since the recipient can use it to modify the permissions, thus resulting in the leakage of
1432 privileges.

1433 **AC-SS-R40 – Enable multi-factor authentication delete/lock**, when supported, to sensitive
1434 objects in object storage.

1435 **4.4 Audit Logging**

1436 Storage infrastructure components generate event log entries for a wide range of transactions or
1437 events. These event log entries have to be recorded in some manner for event logging. From a
1438 security or compliance perspective, it is important to capture those event log entries that are
1439 necessary to demonstrate proof of operations (e.g., encryption and retention), enforcement of
1440 accountability and traceability, meeting evidentiary requirements, and adequate monitoring of
1441 systems. This subset of general event logging is commonly called audit logging.

1442 The following audit logging events are relevant for security purposes:

- 1443 • **Management events** (i.e., what a human did) are always of interest.
- 1444 • **Blocked attempts to grant** access (to storage, login sessions, etc.) are most often of
1445 interest.
- 1446 • **Data access events** are usually of limited interest, except in situations where critical files
1447 and directories need to be tightly monitored.
- 1448 • **Control events and data access events** are typically of the least interest (they can
1449 provide useful information during root cause analysis after an incident and are important
1450 in extremely sensitive environments).

1451 Deficiencies in security logging and analysis allow attackers to hide their location, malicious
1452 software, and activities on victim machines. Even if the victims know that their systems have
1453 been compromised, without protected and complete logging records, they are blind to the details
1454 of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack
1455 may go unnoticed indefinitely, and the particular damages done may be irreversible. Sometimes,
1456 logging records are the only evidence of a successful attack. Many organizations keep audit
1457 records for compliance purposes, but attackers rely on the fact that such organizations rarely look
1458 at the audit logs, and they do not know that their systems have been compromised. Because of
1459 poor or nonexistent log analysis processes, attackers sometimes control victim machines for
1460 months or years without anyone in the target organization knowing, even though evidence of the
1461 attack can be obtained in unexamined log files.

1462 Based on the criticality of event log data for attack detection and forensic investigation, the
1463 following are the security recommendations for implementing audit logging capabilities. Each
1464 recommendation has a unique identifier with format AL-SS-Rx, where AL stands for audit
1465 logging, SS stands for secure storage, and Rx stands for the recommendation sequence.

1466 **AL-SS-R1 – Enable logging of all storage infrastructure components:** Storage systems and
1467 devices should participate in audit logging, and all significant storage management events should
1468 be collected.

1469 **AL-SS-R2 – Ensure that all of the device’s time is synchronized with a reliable, external**
1470 **time source, such as an NTP service:** An NTP service is critical for time synchronization. If the
1471 NTP service is disabled, dependent systems may suffer from inaccurate timestamps on messages,
1472 events and alerts, inconsistent time across different devices, and subsequent failure to perform
1473 log analysis, correlation, anomaly detection or forensics. Establishing and using a common,
1474 accurate time source across the environment helps ensure that event records from different
1475 sources can be correlated.

- 1476 (a) Ensure that an NTP service is enabled on all devices.
- 1477 (b) In particular, log servers, monitor time synchronization validity, and handle alerts at a
1478 high priority.
- 1479 (c) Ensure that devices are configured to synchronize time with a time source server, such as
1480 an NTP server.
- 1481 (d) Ensure that the configured time source servers for each device are secure and approved
1482 for use by information security.
- 1483 (e) Ensure time source server redundancy by using at least three synchronized time sources.
1484 It is also important to distribute the servers across multiple geographies so that a localized
1485 outage will not impact the entire service.
- 1486 (f) Use authentication for a time source client and server communication to ensure that the
1487 server is a trusted server.
- 1488 (g) Use access control options, such as “ntpd” access restrictions, to restrict access to the
1489 time source servers.

1490 **AL-SS-R3 – Collect logs in a centralized fashion:** For example, utilize syslog, AWS
1491 CloudTrail, or Azure Operational Insights. By writing logs to central log servers, the risk of
1492 those logs being lost or altered is lowered since they are more secure within the internal network.

- 1493 (a) Ensure that log servers are approved. To ensure that storage infrastructure components
1494 transmit their log event data to the desired syslog server(s), ensure that the syslog server
1495 IP address is correct and that the configured syslog server is authorized/approved.
- 1496 (b) Ensure log server redundancy. Deploy multiple syslog servers to ensure continuous
1497 logging and prevent a single point of failure.
- 1498 (c) Maintain at least one off-site copy for each log.

1499 **AL-SS-R4 – Ensure complete audit logging:** Ensure that all types of events and all storage-
1500 related objects, sites, accounts, etc., are included in the audit logging:

- 1501 (a) Ensure audit logging for read-only API calls in sensitive environments.
- 1502 (b) To prevent loss of entries if the logging process is stopped and restarted before all entries
1503 are written, ensure that logging is configured to be written in real time to disk with no
1504 buffers in place and sent over TCP (not UDP).
- 1505 (c) Ensure that all denied access attempts to services, ports, files, objects, or devices are
1506 logged.
- 1507 (d) For sensitive information, enable full logging of all data access activity.

1508 **AL-SS-R5 – Ensure sufficient audit log retention and protection:**

- 1509 (a) Retain historical logs for a sufficiently long period of time, as it often takes a while to
1510 notice that a compromise has occurred or is occurring.

- 1511 (b) Ensure sufficient storage space and proactively monitor free space and unusual growth
1512 rates of log data to prevent log destinations from filling up. A known attack pattern
1513 involves filling up logs first to disrupt forensics, and appropriate monitoring can help
1514 identify such attacks in real time.
- 1515 (c) Ensure that archived log data is safe from tampering (e.g., using immutable storage,
1516 object locking, MFA delete).
- 1517 (d) Restrict access to log data and servers. Consider using separate roles or accounts to
1518 manage them.
- 1519 (e) Enable encryption since access to log data can provide attackers with valuable insight
1520 into assets and possible attack vectors.

1521 **4.5 Preparation for Data Incident Response and Cyber Recovery**

1522 Storage-related incidents should be handled as an integral part of the organization incident
1523 response process, including aspects such as isolation, root-cause-analysis, defining a response
1524 plan, testing, periodical process review and refresh, etc.

1525 The following recommendations incorporate specific aspects that should be considered with
1526 respect to storage infrastructure and data assets.

1527 **IR-SS-R1 – Develop a response plan for storage component compromise:** Consider the
1528 following elements in organizational analysis, isolation, remediation, restoration, and testing
1529 procedures:

- 1530 (a) Compromise of an entire array or an entire cloud-based storage asset (e.g., SAN, NAS,
1531 object store, elastic file system)
- 1532 (b) Compromise of a backup system
- 1533 (c) Compromise of an individual storage element (e.g., share, LUN)
- 1534 (d) Compromise of a SAN fabric switch

1535 **IR-SS-R2 – Ensure immutability of recovery assets during incident management:** In
1536 conjunction with the guidance provided in Section 4.7 below regarding the protection of cyber
1537 recovery copies, ensure that those copies remain isolated during incident management.

1538 **IR-SS-R3 – Validate the hygiene of recovered compute components:** Ensure that recovered
1539 executables, applications, containers, and OS images are free from infection prior to deploying
1540 them in production.

1541 **4.6 Guidelines for Network Configuration**

1542 As previously mentioned, the topic of storage-related networking involves multiple aspects,
1543 some of which overlap with *Data Access Control*, *Administrative Access*, and *Encryption*, which
1544 have been covered in other sections. To eliminate repetition, this document discusses:

- 1545 • Certain network recommendations closely related to data access control in Section 4.3,
1546 • Network- and protocol-related encryption recommendations in Section 4.9,
1547 • Certain network recommendations closely related to administrative access in Section
1548 4.10, and

- 1549 • *Network infrastructure* (e.g., switch, port, HBA and NICs configuration, zoning
1550 guidelines, etc.) and *protocols* in this section.

1551 For a complete appreciation of all network configuration aspects, please refer to all sections.

1552 Each recommendation has a unique identifier with the format NC-SS-Rx, where NC stands for
1553 Network Configuration, SS stands for secure storage, and Rx stands for the recommendation
1554 sequence.

1555 **4.6.1 SAN**

1556 **NC-SS-R1 – Ensure that switches are authenticated:** Ensure that storage switches are
1557 authenticated before joining the network.

1558 **NC-SS-R2 – Ensure the use of an approved PKI mechanism:** Use an approved and certified
1559 central key management (PKI) system for the management of switch certificates rather than the
1560 devices' self-signed certificates.

1561 **NC-SS-R3 – A blended approach to zoning:** This is preferable to simply zoning using a single
1562 type (i.e., host, switch, and storage device):

- 1563 (a) Host-based zoning mechanisms control what storage resources or devices are visible to
1564 an application on a host as well as the devices that it can access. At the lowest level, the
1565 masking capability in a host bus adapter's (HBA) firmware or driver must be used to
1566 control whether the host may interact with any storage device. At the next level, OS
1567 capabilities must be used to control which devices the host tries to mount as a storage
1568 volume. Finally, the centralized management software for volume management,
1569 clustering, and the file system must be utilized to control device access by applications.
1570 (b) In switch-based zoning, the switches (especially the FC switches) should have the
1571 capability to specify which devices on which ports can access other devices or ports.
1572 Port-based zoning uses hardware to enforcing zoning and is therefore also called "hard
1573 zoning." In other words, switches must support zone control at the level of port WWNs
1574 rather than at the switch (node) WWN level.
1575 (c) In storage device-based zoning, the storage array is configured with a list that shows
1576 which hosts (even more specifically, which HBA ports) can access which LUNs and on
1577 which ports. Access requests from unlisted hosts or HBA ports are ignored or rejected.
1578 (d) If the zone set feature is available, it should be leveraged. This will help to create
1579 multiple zones dedicated to a particular purpose, such as testing, dynamic
1580 reconfiguration, testing, backup, and maintenance.

1581 **NC-SS-R4 – Prefer masking as close to the data as possible** and as far from the data consumer
1582 or client as possible (e.g., favor array over switch masking, core switch over edge switch, and
1583 switch over HBA).

1584 **NC-SS-R5 – A copy of the zone configuration file should be kept** outside of the SAN switches
1585 to enable redeployment upon erroneous or malicious corruption or deletion.

1586 **NC-SS-R6 – Limit switch management capabilities to the minimum necessary:**

1587 (a) When implementing the SAN fabric, there should be well-defined policies that specify
1588 and minimize the set of switches that are authorized to distribute configuration data
1589 (while providing acceptable redundancy).

1590 (b) Any unnecessary configuration management permissions and services, password
1591 distribution, should not be enabled.

1592 **NC-SS-R7 – Considerations for using soft vs. hard zoning:**

1593 • **Soft zoning** – Soft zoning uses filtering implemented in Fibre Channel switches to
1594 prevent ports from being seen from outside of their assigned zones. The security
1595 vulnerability in soft zoning is that the ports are still accessible if the user in another zone
1596 correctly guesses the Fibre Channel address. In this case, the FC switch will place a host
1597 WWN in a zone without evaluating the port numbers it is connected to in the FC switch.
1598 PWWN identification is considered more secure than port number identification (used in
1599 hard zoning) because any device physically connected to a port could grant storage
1600 access to an unauthorized host. If the SAN spans facilities with different physical security
1601 controls, and if there is a risk that physical ports could be accessed by unauthorized
1602 individuals, soft zoning may be preferable.

1603 • **Hard zoning** – Hard zoning uses physical port numbers on SAN switches, thereby
1604 physically blocking access to a zone from any device outside of the zone. This type of
1605 zoning protects from WWN spoofing attacks as it does not rely on host identity. If the
1606 organization's physical access is thoroughly protected (i.e., it is improbable that an
1607 intruder will access a physical port), this method may be preferable.

1608 **NC-SS-R8 – Limit which SAN Fibre Channel physical and logical ports can be used for**
1609 **management** on all SAN switches and storage arrays.

1610 **NC-SS-R9 – Limit communication between switches:** Limit communication between SAN
1611 switches based on security policies while ensuring that switches can only communicate with
1612 switches that are necessary.

1613 **NC-SS-R10 – Persistently disable unused SAN ports** to prevent the accidental or deliberate
1614 connection of unauthorized equipment

1615 **4.6.2 IP Network**

1616 **NC-SS-R11 – IP storage network separation:** When it comes to storage-related
1617 communication over IP networks, sound logic should be applied to the separation of
1618 environments and traffic type (at both layer 2 and later 3) to the maximum possible extent.

- 1619 (a) Type of traffic: data access protocols vs. management vs. replication vs. backup vs. host
1620 and application networking
- 1621 (b) In sensitive environments, further separate management traffic of different solutions,
1622 vendors, and technologies (e.g., use separate layer 2 and 3 subnets for managing each
1623 array technology, Server-Based SAN, switch technology, storage virtualization, etc.).
- 1624 (c) Data access protocols (e.g., iSCSI vs. NFS vs. proprietary vendor protocols, such as
1625 Server-based SAN).
- 1626 (d) Type of servers or hosts accessing data: virtualized hosts vs. physical hosts

1627 **NC-SS-R12 – IP or Ethernet management ports of SAN switches should reside in an**
1628 **isolated subnet**, including separation from subnets used for data access between hosts and
1629 storage and for host-to-host communication.

1630 **NC-SS-R13 – Enable device IP access control:** With respect to IP network accessibility,
1631 security features should be turned on for all storage devices regulating IPs and port/protocols,
1632 where applicable. This includes but is not limited to built-in Firewall rules, IP Filtering, and
1633 access lists in order to:

- 1634 (a) Control data access between hosts or applications and the storage objects they use.
1635 (b) Separately control management IP traffic between management hosts and applications
1636 and the relevant storage management interfaces they manage.

1637 **NC-SS-R14 – Enable network IP access control:** Restriction should be applied at the network
1638 level (e.g., routing, firewall, access lists, VPC security groups, server-based SAN clients) to
1639 allow all traffic types (e.g., data-access and management traffic) only to allowed IP addresses
1640 and TCP/UDP ports and protocols:

- 1641 (a) Between hosts or applications and the storage objects they use.
1642 (b) Between management hosts and applications and the relevant storage management
1643 interfaces of storage objects they manage.

1644 **NC-SS-R15 – Block any public access to storage objects**, particularly from the internet.
1645 Additionally, ensure that sufficient controls are implemented, such as:

- 1646 (a) Minimizing access
1647 (b) Using physically and logically separate storage subnets and, preferably, separate storage
1648 devices and pools
1649 (c) Considering protection from denial-of-service attacks
1650 (d) Cached copies (e.g., using CDN, replicas, and proxies) retaining at least the same security
1651 characteristics as the source data
1652 (e) Considering regulatory requirements (e.g., confidentiality, storage location restrictions,
1653 etc.)
1654 (f) Any additional applicable security controls (e.g., encryption, authentication, etc.)

1655 **NC-SS-R16 – Ensure that internal IP addresses for SNMP:** When configuring SNMP, ensure
1656 that all traffic is directed to valid and internal IP addresses as destinations.

1657 **NC-SS-R17 – Consider the use of isolated non-routable VLAN for server-based SAN:** To
1658 protect the data storage environment and mitigate security concerns, consider using non-routable
1659 VLAN for server-based SAN.

1660 **4.6.3 Protocols**

1661 **NC-SS-R18 – Disable unsecure versions of file access protocols:** Outdated, unrecommended,
1662 or unsecured protocol versions, such as SMB v1 or NFS 1 and 2, should be blocked. If possible,
1663 disable these protocols on both the client side and the server side.

1664 **NC-SS-R19 – SNMP security:**

- 1665 (a) Disable SNMP if not required.
- 1666 (b) Change the default, known community strings, even if SNMP is not enabled. The
1667 configured strings should meet the organizational password policy.
- 1668 (c) Use different community strings for devices that differ in levels of confidentiality.
- 1669 (d) Use at least SNMP version 3.
- 1670 (e) Enforce the use of SNMP authentication and privacy (encryption) features.
- 1671 (f) Do not configure SNMP with read-write access unless it is absolutely needed. In this
1672 case, limit and control the use of read-write SNMP.
- 1673 (g) Use access control lists to control access through SNMP to devices.
- 1674 (h) Ensure that SNMP traps are sent to authorized, intended managers.
- 1675 (i) Refer to DHS CISA TA17-156A [35] for additional guidance.

1676 **NC-SS-R20 – Ensure the authenticity of directory, domain, and similar services (e.g., AD,
1677 DNS, LDAP):** Actively and periodically review service configurations in all storage elements
1678 (e.g., devices, switches, management workstations, management software) to make sure that the
1679 approved ones are used, and remediate any discrepancies.

1680 **NC-SS-R21 – Considerations for using standard and non-standard TCP/IP or UDP ports:**
1681 Most applications and services have a default TCP/IP or UDP port that is used to connect to the
1682 application or service. However, since it is usually possible to configure which logical ports will
1683 be used by the various applications and services, the pros and cons of using non-standard ports
1684 should be considered.

- 1685 • **Pros** – Using non-standard ports helps obfuscate the application or service as hackers
1686 will not know which port to use.
- 1687 • **Cons** – Alternately, using non-standard ports can make it difficult for security scanning
1688 tools to identify suspicious activities since they are designed to expect specific behaviors
1689 on standard ports.

1690 **NC-SS-R22:** Enable FIP snooping filters on FCoE VLANs to prevent unauthorized access to
1691 data.

1692 **NC-SS-R23 – Limit iSCSI ports:** Hosts on the iSCSI network should be prevented from
1693 accessing any TCP ports other than the those designated for iSCSI on that network.

1694 **NC-SS-R24 – Use iSCSI authentication:** Use one of the supported methods to authenticate
1695 iSCSI initiators upon opening a session (e.g., CHAP, SRP, Kerberos, SPKM-1/2). When using
1696 CHAP, prefer using two-way authentication over one-way authentication.

1697 **NC-SS-R25 – Use of NDMP security features:** When NDMP is used to transport data from
1698 storage arrays to backup systems, ensure that NDMP security features are used, including:

- 1699 (a) Access control over which hosts can initiate NDMP sessions
- 1700 (b) The challenge response authentication (do not use the plaintext authentication option)
- 1701 (c) Log NDMP connection attempts
- 1702 (d) An NDMP password that meets the organizational password policy (e.g., length,
1703 complexity, etc.)
- 1704 (e) Restricted NDMP-related rights that require user only
- 1705 (f) Encrypted NDMP control connections
- 1706 (g) NDMP throttling per session or per server

1707 **NC-SS-R26 – Use of LDAP SSL:** Use LDAP over SSL when setting up Active Directory
1708 options for storage systems.

1709 **NC-SS-R27 – Additional protocols:** When additional protocols such as SymAPI, SMI-S, GNS,
1710 and others are used, further consider adapting the recommendations in Sections 4.6.2 and 4.6.3
1711 for their use. In particular:

- 1712 (a) Isolate traffic for data access and management from other environments;
- 1713 (b) Limit TCP / UDP ports; and
- 1714 (c) Enable encryption.

1715 **4.7 Isolation**

1716 When production data is damaged or lost, organizations should be able to recover it using
1717 replicated or backed up data copies. If the damage is the result of a malicious attack, and the
1718 attackers were also able to compromise the backup data copies, the attack on the production
1719 environment can have a devastating effect since the organization does not have the ability to
1720 recover. To provide wide support for recovery from various scenarios, sufficient isolation must
1721 be guaranteed between data assets, classes, and storage systems holding recovery data, in
1722 particular.

1723 In this context, organizations should maintain at least two separate types of data protection
1724 copies of their data:

- 1725 • **Non-malicious recovery copies** – To be used in the event of a natural disaster, hardware
1726 failure, human error, etc. These can include local copies (e.g., snapshots taken before
1727 performing maintenance), DR copies, long-term backups, and others. The “closer” the
1728 copy is to the production environment, the more likely it is to be mapped to systems for
1729 the purpose of testing and DR.
- 1730 • **Cyber-attack recovery copies** – Reserved for the event of a cyber-attack and should be
1731 hardened, locked, and kept in isolation. These copies should not be impacted by *anything*,

1732 including cases wherein production volumes or other types of copies have been
1733 compromised.

1734 The purpose of isolation is to make the cyber-attack recovery copies and systems inaccessible
1735 and independent from the production environment. Other levels of isolation (e.g., between long-
1736 term backup and production/DR) may be highly advantageous.

1737 The following security recommendations apply to the creation of these copies and the associated
1738 management system.

1739 **IS-SS-R1 – Ensure separated storage systems:**

- 1740 (a) Cyber-attack recovery copies should be created on designated separated storage
1741 environments. In private clouds, this implies physically separated storage systems. In
1742 public clouds, this implies separate accounts (or equivalent).
1743 (b) Long-term backup systems should be separated from production data storage systems.

1744 **IS-SS-R2 – Ensure separate management systems:** Storage systems that store cyber-attack
1745 recovery copies should be managed from designated management systems, which are separated
1746 from the production environment and other data protection mechanisms. It should not be possible
1747 to access them with regular credentials (including production and regular backup). The system
1748 should be hosted on a dedicated host that is only connected to an isolated network.

1749 **IS-SS-R3 – Ensure restricted access:**

- 1750 (a) Cyber-attack recovery copies and their systems should not be accessible to regular IT
1751 staff, only to a single person (e.g. CISO) or to a very narrow group of executives or
1752 security managers who use credentials separate from those used for other day-to-day
1753 duties. This ensures that if the credentials of an IT admin are compromised, the attacker
1754 cannot use those credentials to access the cyber-attack recovery copies. This restricted
1755 team can have access to the cyber-attack recovery copies, but an even smaller subset
1756 should have administrative rights that include granting permissions to other users.
1757 (b) Access rights to long-term backup should be separate from those used to perform other
1758 storage administration duties (e.g., SAN management, storage allocation, etc.) and should
1759 include the use of separate user IDs, accounts, and credentials.

1760 **IS-SS-R4 – Ensure off-site storage:** Cyber-attack recovery copies should be stored off-site and
1761 not where the production data is stored. This ensures that if the attacker has physical access to
1762 the production site or manages to compromise the physical site, they would not be able to access
1763 or compromise the cyber-attack recovery copy.

1764 **IS-SS-R5 – Ensure the use of an independent, full baseline copy:** Backup systems often
1765 make use of incremental backups that capture changes to the data relative to a baseline copy.
1766 These incremental copies cannot be used during recovery without the baseline copy. For certain
1767 types of backup schemes, such as snapshots, only incremental copies are used (i.e., the baseline
1768 copy is the production data itself).

1769 To handle a recovery scenario properly, dependencies between copies must be accounted for,
1770 and sufficient isolation between different types of copies must be maintained. In particular:

- 1771 (a) Replicated disaster recovery copies should have no dependencies on production baseline
1772 data;
- 1773 (b) Long-term backups should have no dependency on production and disaster recovery
1774 baseline data; and
- 1775 (c) Cyber-attack recovery copies should have no dependency on production and disaster
1776 recovery baseline data.

1777 **IS-SS-R6 – Disable all unneeded services and protocols:** Unneeded services and protocols
1778 should be disabled on cyber-attack recovery storage systems. Disabling all web access and
1779 relying only on API or CLI for management are recommended.

1780 **IS-SS-R7 – Ensure independence from hosts and applications:**

- 1781 (a) Cyber-attack recovery copies should not be mounted, exported, or mapped to a host or
1782 application. During recovery, if needed, Cyber-attack recovery copies should preferably be
1783 restored (pushed) into an isolated staging (or “air-gapped”) environment and not directly to
1784 the target hosts or applications. A less secure option is to allow the target hosts or
1785 applications limited read-only access (e.g., mapping or mounting) during restore only, and
1786 remove such access as soon as restore is complete.
- 1787 (b) Long-term backups should not be mounted, exported, or mapped to a host or application.

1788 **IS-SS-R8 – Consider setting up an air gap:** Organizations should consider setting up an air gap
1789 around the cyber-attack recovery copies. For example, certain storage vendors enable shutting
1790 down data ports and opening them during a limited time for the periodic sync with the
1791 production system.

1792 **IS-SS-R9 – Perform periodic audits:** The above recommendations should be checked as part of
1793 a periodic audit to ensure that there are no configuration gaps/drifts that may compromise the
1794 isolation of the cyber-attack recovery copy.

1795 **IS-SS-R10 – Consider the use of immutable storage,** which could help further isolate and
1796 protect recovery data (e.g., retention locking, vault locking, immutability policies, etc.).

1797 **4.8 Restoration Assurance**

1798 In order to ensure successful recovery from a cyber-attack, it is not enough to have a process in
1799 places. Organizations must also verify that all components of critical data assets are protected
1800 and can be restored faithfully, consistently, and completely and that the speed and currency of
1801 restoration are aligned with business and regulatory requirements. In many cases, organizations
1802 have backups of their critical systems but do not regularly check whether this backup can
1803 actually be used to restore the system. However, due to configuration drifts, changes in the
1804 environment, or even a malicious attack that compromises the backups, they are faced with a
1805 reality in which they cannot use the backed-up data to recover. The following security
1806 recommendations apply for obtaining restoration assurance.

1807 **RA-SS-R1 – Ensure the completeness of cyber-attack recovery copies:** All storage elements
1808 that contain components of critical data assets should be protected and backed up in a cyber-
1809 attack recovery copy. This includes components such as storage volumes, critical file systems,
1810 databases, software images, certificates, encryption keys, startup files, catalog info, ACLs, and
1811 configuration files.

1812 **RA-SS-R2 – Protect all dependent components:** Dependent components, such as Active
1813 Directory or DNS, should be protected to enable full recovery.

1814 **RA-SS-R3 – Ensure the availability of all relevant software and hardware components:** In
1815 order to recover, make sure that all of the relevant software and hardware components (e.g.,
1816 drivers, firmware, etc.) used to run the system are backed up, protected, and available for a
1817 restore operation.

1818 **RA-SS-R4 – Ensure that selected backup technology and media matches RTO**
1819 **requirements:** Recovery speed (RTO) should be examined holistically, including all dependent
1820 and related components (e.g., data, configuration files, encryption keys) while also balancing the
1821 actual recovery speed that is required with the cost that it would take to align all of the dependent
1822 components to enable this expected recovery speed.

1823 **RA-SS-R5 – Test restore to ensure required RTO:** Perform a test restore to ensure that it is
1824 completed successfully and that it meets the required timeframe.

1825 **RA-SS-R6 – Ensure that remote replicas meet the RPO:** Set a recovery point objective
1826 (RPO), which is the amount of data that can be lost following a failure, and ensure that remote
1827 replicas meet this objective.

1828 **RA-SS-R7 – Ensure that remote replicas meet the retention requirements:** Set the data
1829 retention requirement, which is the amount of time that data will be backed up. Based on this
1830 requirement, ensure that the system creates the relevant number of copies with the relevant
1831 refresh rate.

1832 **RA-SS-R8 – Ensure that remote replicas are in good health:** Periodically ensure that the
1833 remote replicas are in good health. This includes checking that there are no relevant errors in the
1834 log and that they are in a healthy state.

1835 **RA-SS-R9 – Enable the separate restoration of data and application:** Separating the data
1836 from the applications will allow for the data to be restored without restoring infected code or
1837 software.

1838 **RA-SS-R10 – Document DR plan, resources, mapping to production, flow, and test**
1839 **procedures:** A disaster recovery plan should be written, including all of the resources, its
1840 mapping to production, flows, and test procedures. These documents should be backed up as
1841 well.

1842 **RA-SS-R11 – Ensure cyber hygiene:** For mission critical information, cyber-attack recovery
1843 copies should be scanned with various anti-malware scanning tools for known vulnerabilities and

1844 anomalies. Ideally, all copies should be scanned. If that is not possible, scan a subset of the
1845 copies, and keep a record of those copies scanned and secure. Cyber hygiene includes antivirus,
1846 anti-malware, vulnerability scanning, and security analytics.

1847 **RA-SS-R12 – Perform periodic audits:** The above recommendations should be checked as part
1848 of a periodic audit to ensure that systems can be restored according to the defined RTO/RPO
1849 requirements.

1850 **4.9 Encryption**

1851 Encryption is the conversion of data from a readable form (i.e., plaintext) into an obfuscated
1852 form (i.e., ciphertext) that cannot be easily understood by unauthorized people. In storage
1853 systems, the encryption of sensitive information should be implemented end to end, including:

- 1854 • **Data at rest** – Data that is physically or logically stored in the storage infrastructure (e.g.,
1855 tapes, disks, optical media) should be encrypted. A comprehensive approach should be
1856 taken that incorporates not only the data itself but also metadata, which can include
1857 access permissions, labels, paths, and journaling information.
- 1858 • **Data in transit** – When the data is transferred between storage elements (e.g., read or
1859 written by a client, replicated between storage devices or pools, transmitted in server-
1860 based SAN, Storage vMotion) and in transit throughout the network, it should be
1861 encrypted.
- 1862 • **Administrative access** – This includes connections through standard and proprietary
1863 protocols and APIs to configure or control storage elements, storage networking, and
1864 data.

1865 There are a few different types of encryption algorithms that encrypt information and facilitate
1866 the encryption process. Asymmetric, symmetric, and hashing formulas are the common methods
1867 to enable encryption, with a few variations.

1868 The following encryption guidance is applicable to storage infrastructure and should be used:

1869 **EN-SS-R1 – Ensure that secure TLS and SSL levels are used:** Certain versions are considered
1870 insecure (e.g., TLS 1.0 includes a means by which a TLS implementation can downgrade the
1871 connection to SSL 3.0, thus weakening security and exposing it to the POODLE vulnerability):

- 1872 (a) Enable TLS 1.3 and 1.2, which are the most recent versions of TLS.
- 1873 (b) Ensure that SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 are disabled across all storage
1874 infrastructure components.

1875 **EN-SS-R2 – Ensure robust hash algorithms and message authentication codes (MAC):** Do
1876 not use weak hash algorithms, such as MD5 and SHA1. Strong algorithms, such as PBKDF2 or
1877 HMAC-SHA-256, should be used instead. Refer to NIST Special Publication 800-107 and NIST
1878 Special Publication 800-132 for additional guidance.

1879 **EN-SS-R3 – Disable the use of cleartext protocols (e.g., HTTP, Telnet, FTP, or RSH):**
1880 Cleartext protocols are vulnerable to sniffing, interception, and other attacks as they do not
1881 encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information.

1882 **EN-SS-R4 – Ensure that storage management API sessions are encrypted:** Storage
1883 management APIs and CLIs are used for administrative access to storage systems. For some of
1884 the storage systems, the encryption of API and CLI client sessions is controlled in specific per-
1885 vendor configuration options within the management software or the API/CLI software
1886 component.

1887 **EN-SS-R5 – Ensure that administrative access sessions are encrypted:** Administrative
1888 sessions over HTTP should use SSL (HTTPS). CLI access should be encrypted using SSH rather
1889 than Telnet. The authentication during API access should not use cleartext, and the session itself
1890 should be encrypted.

1891 **EN-SS-R6 – Enable FIPS mode for FIPS-based environments:** FIPS 140-2 specifies that a
1892 cryptographic module should be a set of hardware, software, firmware, or some combination of
1893 those that implements cryptographic functions or processes, including cryptographic algorithms
1894 and, optionally, key generation, and is contained within a defined cryptographic boundary. FIPS
1895 specifies certain crypto algorithms as secure, and it also identifies which algorithms should be
1896 used if a cryptographic module is to be called FIPS-compliant. Organizations that are FIPS-
1897 compliant should ensure that FIPS mode is enabled in their FIPS-compliant storage infrastructure
1898 components.

1899 **EN-SS-R7 – Ensure that sensitive data is encrypted at rest:** At-rest encryption protects
1900 against a variety of data-related risks (including unauthorized access, compromise in case of
1901 media loss or theft, etc.) and should be enabled for sensitive data. Certain considerations should
1902 be applied:

- 1903 • **Infrastructure encryption** (e.g., the use of built-in encryption capabilities provided by a
1904 drive, storage array, or cloud storage, whether using the vendor keys or organization-
1905 provided keys) can protect against device loss, misplacement, or theft but is not
1906 considered an effective control against:
 - 1907 ○ **In-band attacks** – When an attacker can compromise a host already mapped to
1908 the storage (or when the storage can be mapped using legitimate means to an
1909 unauthorized host).
 - 1910 ○ Administrators or attackers gaining elevated right – Who can remove encryption.
- 1911 • **Application-level encryption** – Data is encrypted at its source, presenting ciphertext
1912 only to the storage infrastructure and administrators. While generally considered more
1913 secure, application-level encryption comes at a (sometimes considerable) cost:
 - 1914 ○ **Data-reduction mechanisms are impacted** – For example, compression and
1915 dedupe can be drastically less effective.
 - 1916 ○ Management is more complex.

1917 **EN-SS-R8 – Ensure that data in transit is encrypted:**

- 1918 (a) **Block over Fibre Channel:** Use Fiber Channel link encryption to encrypt data between
1919 SAN ports. When supported, use end-to-end (host to storage) encryption (FC-SP-2
1920 compliant).
- 1921 (b) **Block over IP:** IP storage traffic is subject to the same security risks as regular IP
1922 networks. By default, block-over IP protocols do not provide data confidentially,

1923 integrity, and authentication per packet. When using block-over IP protocols (e.g., iSCSI,
 1924 FCIP, iFCP or iSNS, proprietary protocols), configure IPsec to ensure per-packet
 1925 authentication, integrity, and confidentiality.

1926 (c) **File and object storage access:** Ensure that data encryption in-flight options are enabled
 1927 (for backup systems) and that data remote replication is encrypted. For file access, ensure
 1928 that data is transmitted and encrypted using mechanisms such as SMB encryption and
 1929 NFS Kerberos. Ensure that objects are accessed through HTTPS with TLS.

1930 (d) Particular attention should be paid to enable encryption on all connectivity segments that
 1931 extend network communication beyond the boundaries of a physically protected domain
 1932 (e.g., an ISL link between two physically separated datacenters, IP traffic over WAN or
 1933 the internet).

1934 **EN-SS-R9 – Ensure that internal storage communication is encrypted:** Storage systems
 1935 often have subsystems and components that communicate with each other, such as nodes,
 1936 managers, and witness devices. Ensure that internal communication between subsystems is
 1937 properly encrypted. This can also be extended to communication with gateway servers, policy
 1938 servers, and antivirus servers.

1939 **4.10 Administrative Access**

1940 Administrative access is required to control and managed a wide spectrum of storage elements,
 1941 including arrays, network and fabric, management tools, backup, replication, and cloud storage.
 1942 Administrative access can be based on a direct connection to the storage component and through
 1943 a management software. Both connection types can involve various interfaces, including a
 1944 management UI, CLI, and API.

1945 Securing administrative access is critical, as most storage risks discussed in Section 3.2 above,
 1946 including the most devastating, could materialize if not well-controlled.

1947 Certain other sections in this chapter include aspects that overlap with Administrative Access.
 1948 To eliminate repetition, additional relevant recommendations can be found in:

- 1949 • Section 4.9 above, regarding encryption
- 1950 • Section 4.3 above, regarding data-related access controls, part of which may also apply to
 1951 administration

1952 The following security guidelines are recommended for the configuration of administrative
 1953 access.

1954 **AA-SS-R1 – Network access to management ports** of the SAN switches should be limited to
 1955 devices and administrators specifically assigned to manage the switches through a mechanism
 1956 such as an access control list (ACL).

1957 **AA-SS-R2 – Control and limit the devices and components that have administrative**
 1958 **capabilities to the minimum required:** This includes CLI servers, management consoles, API
 1959 gateways, witness hosts, and storage devices with control permissions. In particular:

- 1960 (a) Actively discover components that have storage administration capabilities to make sure that
 1961 only authorized ones have them. Remove unnecessary ones, if found, and debrief.
 1962 (b) Remove unnecessary rights and capabilities from authorized devices.
- 1963 **AA-SS-R3 – Implement the least-privileges approach:** Limit the rights of users with
 1964 administrative rights to the minimum required. This includes the minimal actions that the user
 1965 can carry out while also limiting the scope of these permissions to include only the relevant
 1966 systems or regions. Full administrative rights should only be granted to users who require these
 1967 rights.
- 1968 **AA-SS-R4 – Limit monitoring tools’ access rights:** Service accounts, such as monitoring tools,
 1969 should be limited to read-only and metadata-only access.
- 1970 **AA-SS-R5 – Use IP filtering on storage systems:** Most storage systems offer the ability to
 1971 manage the list of hosts that are allowed to administer the system. This capability should be used
 1972 to explicitly restrict management rights to designated and documented hosts using IP filters.
- 1973 **AA-SS-R6 – Authenticate/authorize all CLI/API access:** CLI/API usage should be subject to
 1974 authentication and authorization processes. In cases where it is not possible to perform
 1975 authentication or authorization, secure the unauthorized access with additional security measures,
 1976 such as using privilege management tools to restrict control to the minimum required commands
 1977 and objects.
- 1978 **AA-SS-R7 – Favor API access control over CLI/shell access:** API access is more restricted
 1979 than CLI/shell access. For example, through the CLI access, it is potentially possible to access
 1980 the system’s underlying operating system and file system, which can be used to access configure
 1981 files. CLI also often includes features that are not documented yet can be found through research
 1982 on the web.
- 1983 **AA-SS-R8 – Restrict management consoles OS privileges:** Management consoles should not
 1984 run as root users but rather as storage-designated accounts (see also **AC-SS-R20**). Their web
 1985 service should be hardened to meet the minimum standards of other web-application servers in
 1986 the organization.
- 1987 **AA-SS-R9 – Restrict host storage control privileges:** In certain shared data configurations
 1988 (e.g., clusters, geo-clusters, scale-sets, or storage virtualization infrastructure), hosts are granted
 1989 administrative access to storage to control shared cluster data resource allocation and behavior.
 1990 When such administrative access is necessary, restrict the scope and privileges granted to hosts
 1991 to the maximum possible extent:
- 1992 (a) Only to the particular elements (e.g., LUNs, shares, files, objects) that the hosts need to
 1993 control
 1994 (b) Only to the specific actions that the hosts need to perform
- 1995 **AA-SS-R9 – Command device or gatekeeper configuration:** Certain storage arrays allow in-
 1996 band administrative control to hosts that have access to special block devices (e.g., “command

1997 device,” ”gatekeeper”). Commands are transferred using I/O operations on those special devices.
 1998 When used, the following security guidelines are recommended apply:

- 1999 (a) **Limit the use of control devices to the minimum possible** – If feasible, eliminate the
 2000 use of such devices completely (e.g., using API access instead). If not, ensure that they
 2001 are mapped to required hosts only (e.g. management hosts).
- 2002 (b) **Scan for control devices** – Perform network scanning to discover control devices, and
 2003 ensure that they are mapped to the required and authorized hosts only.

2004 **AA-SS-R10 – Disable or limit call home or remote access:** Storage infrastructure systems may
 2005 have the ability to send certain telemetry and diagnostic data back to the manufacturer, such as
 2006 logs. In some cases, they even enable remote connection to the system by the manufacturer with
 2007 administrative rights. These mechanisms are in place to allow the manufacturer to investigate
 2008 and resolve technical issues. These capabilities could potentially be exploited by hackers and
 2009 should be disabled if they are not required. However, if they are required, they should be limited
 2010 and controlled by implementing the following settings:

- 2011 (a) **Change the default credentials** – Modify the default credentials used for the remote
 2012 connection.
- 2013 (b) **Limit permissions** - Limit access permissions to only the minimal level required.
- 2014 (c) **Enforce encryption** – The remote session should be encrypted.
- 2015 (d) **Limit access with an “allow list”** – Manage access with an access list that limits access
 2016 by specific IPs and specific users.
- 2017 (e) **Fully logged** – All remote access should be fully logged for auditing purposes.
- 2018 (f) **Enable built-in data obfuscation features** – This is applicable for those storage devices
 2019 that allow obfuscating sensitive data, such as IP addresses, WWNs, device names, and
 2020 usernames.
- 2021 (g) **Limit the scope of data sent** to the minimum required
- 2022 (h) **Review and approve** – Periodically evaluate the data that is occasionally or
 2023 automatically being sent to the vendor, and ensure that it does not contain sensitive
 2024 information, such as IP addresses, usernames, or the actual content of storage devices.
- 2025 (i) **Authorize each connection** – If possible, implement a mechanism that will ask
 2026 permission before allowing each connection.
- 2027 (j) When remote access by the vendor is performed through a gateway device, server, or
 2028 appliance, take particular care to secure and restrict access to the gateway system.
- 2029 (k) Consider the use of dedicated (private) links to the vendor over the use of the internet.

2030 **AA-SS-R11 – Limit network access for management:** In addition to separating management
 2031 from other traffic (see Sections 4.6 and 4.7), in sensitive environments, it is recommended to
 2032 further control access to management networks, including mechanisms such as:

- 2033 (a) Using VPN, IP-SEC, or one or more “jump servers” (or “login proxies,” which are dedicated
 2034 servers in the management network that are the only ones accessible from outside of the
 2035 network and can serve to connect to other servers after proper authentication and
 2036 authorization).
- 2037 (b) Enhanced logging, tracing, and session recording.

2038 **AA-SS-R12 – Secure and protect core storage management files and binaries:** Storage
2039 management software often includes configuration files that present various options to control
2040 how the storage system would operate, including undocumented options. Such sensitive
2041 directories and files should be kept with appropriate limited permission and with correct
2042 ownership and group membership. This includes:

- 2043 • Configuration files outlining users and roles, network settings, consistency groups, device
2044 groups, and other storage options. The configuration files that define consistency and
2045 device groups are often automatically propagated from central management hosts to other
2046 hosts that are attached to the managed storage system. Thus, if compromised, it can affect
2047 multiple systems.
- 2048 • Scripts to control starting, monitoring, and stopping storage management services and
2049 daemons as well as the binaries themselves should be kept in a secure way.

2050 Apply the following controls to critical files:

- 2051 (a) Restrict access and permissions, and control ownership of key folders and files.
- 2052 (b) For sensitive environments, consider monitoring for content changes in such files to
2053 prevent unauthorized ones.

2054 **4.11 Configuration Management**

2055 The purpose of configuration management is to provide visibility and control over settings,
2056 behavior, and the physical and logical attributes of storage assets throughout their life cycle. In
2057 the context of storage security, this involves:

- 2058 • Maintaining comprehensive and current inventory,
- 2059 • Managing change, and
- 2060 • Ensuring that the configuration continually meets the organization’s security baselines
2061 and current industry best-practices and that it is free of known risks.

2062 To this end, appropriate controls, policies, processes, and tools are required. The following
2063 paragraphs contain guidelines applicable to achieving those ends.

2064 **CM-SS-R1 – Create a comprehensive inventory of all storage devices:** This includes
2065 identifying the name, address, location, and software, firmware, or driver versions for all storage
2066 components, including:

- 2067 • Arrays
- 2068 • Storage virtualization systems
- 2069 • Management consoles
- 2070 • Witness hosts
- 2071 • Hosts installed with storage management software and/or plugins
- 2072 • Data protection appliances
- 2073 • Backup clients and servers
- 2074 • Storage network switches
- 2075 • Storage adapters or “HBA”
- 2076 • I/O multipathing software

- 2077 • Pairing of primary and (replication) destination storage systems
- 2078 • Designated backup servers for hosts or off-site backup
- 2079 • Tape libraries and drives

2080 **CM-SS-R2 – Create a comprehensive inventory of all data and configuration assets:** This
2081 includes identifying logical data components and data access configurations through the
2082 following assets:

- 2083 • Storage pools, LUNs, masking, and zoning
- 2084 • Initiators and initiator groups
- 2085 • File shares and ACLs
- 2086 • Object storage pools, buckets, etc.
- 2087 • Replicas and snapshots
- 2088 • Backup catalogue and access rights
- 2089 • Backup sets (on-premises, archived, virtualized in the cloud, on tapes, archive appliances,
2090 etc.)
- 2091 • Users, groups, roles, and rights
- 2092 • Host access configuration to storage assets (e.g., LUNs, file shares, global file systems,
2093 object storage)
- 2094 • Images of storage software, virtual appliances, etc.

2095 **CM-SS-R3 – Create a comprehensive storage security policy,** either as a dedicated policy or
2096 as part of the organization’s security policy. It should include configuration baselines for storage
2097 systems and could be based on:

- 2098 • Recommendations from this publication and cited sources
- 2099 • Storage-related security standards internal to the organization
- 2100 • Relevant vendor security-best practices

2101 **CM-SS-R4 – Keep the storage security policy current:** The storage security policy should be
2102 reviewed and updated periodically (at least annually). The security baseline should be updated
2103 with the latest vendor and industry recommendations available for storage systems and/or
2104 specific storage devices (preferably on a quarterly basis, at least).

2105 **CM-SS-R5 – Periodically and proactively assess configuration compliance to storage**
2106 **security policy:**

- 2107 (a) Make sure that the actual configuration meets the storage security baselines, and identify
2108 gaps.
- 2109 (b) Track the remediation of gaps in a timely manner.
- 2110 (c) Consider developing KPIs to track the compliance to storage security baselines based on
2111 types of data, their organization function, and their sensitivity.

2112 **CM-SS-R6 – Create a storage change management process** as a dedicated process or as part
2113 of the organization’s general change management process. It should cover:

- 2114 (a) Planning, reviewing, and approving storage configuration changes;
- 2115 (b) Updating environment documentation and inventory (e.g., infrastructure, data,
2116 configuration); and
- 2117 (c) Assessing compliance to relevant security baselines following any change to the sensitive
2118 storage environment.

2119 **CM-SS-R7 – Detect unauthorized storage security changes:** There should be a process for
2120 detecting unauthorized changes, prompt remediation, and thorough debriefing

2121 **CM-SS-R8 – Software updates and patches:**

- 2122 (a) **Release updates** – There should be a process for periodically updating storage software
2123 to the latest stable and secure storage release available. This includes management
2124 software, API and CLI packages, array and HBA firmware versions, and OS drivers.
- 2125 (b) **Important security updates and patches** – There should be a process to proactively and
2126 frequently install important and urgent storage security fixes and patches.

2127 **CM-SS-R9 – Network topology documentation:** Maintain current storage-related network
2128 documentation, including drawings (SAN and IP).

2129 **CM-SS-R10 – Ensure the propagation of SAN security configuration changes:** Many
2130 security changes are not automatically or reliably propagated across all switches in the fabric.
2131 There should be a process for enforcement and validation that all such changes are distributed
2132 and activated throughout the fabric.
2133

2134 **5 Summary and Conclusions**

2135 Starting with an overview of the storage technology landscape, this document has discussed the
2136 threats and resulting risks to the safe utilization of resources. It then provided detailed security
2137 recommendations for the secure deployment, configuration, and operation of storage resources in
2138 various security focus areas. These focus areas spanned the following:

- 2139 • Focus areas that are common to all IT infrastructures, such as physical security,
2140 authentication and authorization, audit logging, network configuration, change management,
2141 incidence response and recovery, administrative access, and configuration management.
- 2142 • Focus areas that are specific to storage infrastructures, such as data protection, confidentiality
2143 protection using encryption, isolation, and restoration assurance.

2144 Along with compute (encompassing OS and host hardware) and network infrastructures, storage
2145 infrastructure is one of the three fundamental pillars of IT. However, compared with its
2146 counterparts, it has received relatively limited attention when it comes to security, even though
2147 data compromise can have as much of a negative impact on an enterprise as security breaches in
2148 compute and network infrastructures. The comprehensive security recommendations for storage
2149 infrastructures in this document seek to close that gap.

2150 Building an effective risk management program for storage infrastructure based on the security
2151 controls described in this document and tightly integrating it with existing cybersecurity
2152 frameworks [36] could significantly improve an organization's resilience to data breaches.

2153 **References**

- 2154 [1] Storage Networking Industry Association (2020) *What is iSCSI?* Available at
2155 <https://www.snia.org/education/what-is-iscsi>
- 2156 [2] Chadalapaka M, Satran J, Meth K, Black D (2014) Internet Small Computer System
2157 Interface (iSCSI) Protocol (Consolidated). (Internet Engineering Task Force (IETF)
2158 Network Working Group), IETF Request for Comments (RFC) 7143.
2159 <https://tools.ietf.org/html/rfc7143>
- 2160 [3] International Organization for Standardization/International Electrotechnical Commission
2161 (2020) ISO/IEC TS 23167:2020 – *Information technology – Cloud Computing –*
2162 *Common technologies and techniques* (ISO, Geneva, Switzerland). Available at
2163 <https://www.iso.org/standard/74805.html>
- 2164 [4] Webopedia (2020) *Block-level storage*. Available at
2165 <https://www.webopedia.com/TERM/B/block-level-storage.html>
- 2166 [5] TechTarget (2018) *Fibre Channel*. Available at
2167 <https://searchstorage.techtarget.com/definition/Fibre-Channel>
- 2168 [6] Haynes T (2016) Network File System (NFS) Version 4 Minor Version 2 Protocol.
2169 (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for
2170 Comments (RFC) 7862. <https://tools.ietf.org/html/rfc7862>
- 2171 [7] Black D, Glasgow J, Faibish S (2012) Parallel NFS (pNFS) Block Disk Protection.
2172 (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for
2173 Comments (RFC) 6688. <https://tools.ietf.org/html/rfc6688>
- 2174 [8] Webopedia (2020) *SDS – software defined storage*. Available at
2175 https://www.webopedia.com/TERM/S/software-defined_storage_sds.html
- 2176 [9] The Channel Company (2013) *Software-defined Storage Strategy*. Available at
2177 [https://www.crn.com/news/storage/240150933/emc-outlines-software-defined-storage-](https://www.crn.com/news/storage/240150933/emc-outlines-software-defined-storage-strategy-plans-product-release-this-year.htm?itc=xbodyjk)
2178 [strategy-plans-product-release-this-year.htm?itc=xbodyjk](https://www.crn.com/news/storage/240150933/emc-outlines-software-defined-storage-strategy-plans-product-release-this-year.htm?itc=xbodyjk)
- 2179 [10] International Organization for Standardization/International Electrotechnical Commission
2180 (2020) ISO/IEC 27040:2015 – *Information technology – Security Techniques – Storage*
2181 *Security* (ISO, Geneva, Switzerland). Available at
2182 <https://www.iso.org/standard/44404.html>
- 2183 [11] SDxCentral (2015) *What is Storage Virtualization?*. Available at
2184 [https://www.sdxcentral.com/data-center/storage/definitions/what-is-storage-](https://www.sdxcentral.com/data-center/storage/definitions/what-is-storage-virtualization/)
2185 [virtualization/](https://www.sdxcentral.com/data-center/storage/definitions/what-is-storage-virtualization/)
- 2186 [12] Webopedia (2020) *VM-aware storage*. Available at
2187 https://www.webopedia.com/TERM/V/vm-aware_storage.html

- 2188 [13] Azeem SA, Sharma S (2019) Study of Converged Infrastructure & Hyper Converged
2189 Infrastructure As Future of Data Centre. *International Journal of Advanced Computer*
2190 *Research* 8(5):900. <https://doi.org/10.26483/ijarcs.v8i5.3476>
- 2191 [14] Gartner (2016) *Magic Quadrant for Integrated Systems*. Available at
2192 <https://www.gartner.com/document/3471517?ref=ddisp&refval=3500917>
- 2193 [15] Gartner (2019) *Magic Quadrant for Hyperconverged Infrastructure*. Available at
2194 <https://www.gartner.com/document/3975501?ref=ddisp&refval=3975577>
- 2195 [16] Gartner (2016) *Critical Capabilities for Integrated Systems*. Available at
2196 <https://www.gartner.com/document/3500917?ref=ddisp&refval=3471517>
- 2197 [17] Gartner (2018) *Cool Vendors in Storage Technologies*. Available at
2198 <https://www.gartner.com/document/3893182?ref=solrAll&refval=240504932>
- 2199 [18] ActualTechMedia (2017) *2017 State of Storage in Virtualization*. Available at
2200 [https://www.actualtechmedia.com/wp-content/uploads/2018/01/ActualTech-Media-](https://www.actualtechmedia.com/wp-content/uploads/2018/01/ActualTech-Media-Survey-Report-finalv1.pdf)
2201 [Survey-Report-finalv1.pdf](https://www.actualtechmedia.com/wp-content/uploads/2018/01/ActualTech-Media-Survey-Report-finalv1.pdf)
- 2202 [19] Trust Radius (2020) *Cloud Storage Systems*. Available at
2203 <https://www.trustradius.com/cloud-storage>
- 2204 [20] Storage Networking Industry Association (2018) *Storage Security: Data Protection*
2205 Available at [https://www.snia.org/sites/default/files/security/SNIA-Data-Protection-](https://www.snia.org/sites/default/files/security/SNIA-Data-Protection-TechWhitepaper.pdf)
2206 [TechWhitepaper.pdf](https://www.snia.org/sites/default/files/security/SNIA-Data-Protection-TechWhitepaper.pdf)
- 2207 [21] Galibus T, Krasnoproshin VV, De Oliveira Albuquerque R, Pignaton de Freitas E (2016)
2208 *Elements of Cloud Storage Security* (Springer Nature, Switzerland AG)
- 2209 [22] Blueliv (2018) *Credential theft: the business impact of stolen credentials*.
2210 [https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-](https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/credential-theft/credential-theft-blog-news-and-articles-blueliv/)
2211 [blueliv/credential-theft/credential-theft-blog-news-and-articles-blueliv/](https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/credential-theft/credential-theft-blog-news-and-articles-blueliv/)
- 2212 [23] JumpCloud (2019) *Credential Theft: How It Works and How to Mitigate It*. Available at
2213 <https://jumpcloud.com/blog/credential-theft-mitigation/>
- 2214 [24] MalwarebytesLABS (2018) *Encryption 101: How to break encryption*. Available at
2215 [https://blog.malwarebytes.com/threat-analysis/2018/03/encryption-101-how-to-break-](https://blog.malwarebytes.com/threat-analysis/2018/03/encryption-101-how-to-break-encryption/)
2216 [encryption/](https://blog.malwarebytes.com/threat-analysis/2018/03/encryption-101-how-to-break-encryption/)
- 2217 [25] TechNadu (2018) *How is Encryption cracked?*. [https://www.technadu.com/how-is-](https://www.technadu.com/how-is-encryption-cracked/36616/)
2218 [encryption-cracked/36616/](https://www.technadu.com/how-is-encryption-cracked/36616/)
- 2219 [26] Available at <https://www.vpnmentor.com/blog/difference-between-malware-ransomware/>

- 2220 [27] Wikipedia (2020) *Privilege escalation*. Available at
2221 https://en.wikipedia.org/wiki/Privilege_escalation
- 2222 [28] Joint Task Force (2020) Security and Privacy Controls for Information Systems and
2223 Organizations. (National Institute of Standards and Technology, Gaithersburg, MD),
2224 Draft NIST Special Publication (SP) 800-53, Rev. 5. Available at
2225 <https://doi.org/10.6028/NIST.SP.800-53r5-draft>
- 2226 [29] Norton (2020) *Sensitive data exposure: What is it and how it's different from a data*
2227 *breach*. Available at [https://us.norton.com/internetsecurity-privacy-sensitive-data-](https://us.norton.com/internetsecurity-privacy-sensitive-data-exposure-how-its-different-from-data-breach.html)
2228 [exposure-how-its-different-from-data-breach.html](https://us.norton.com/internetsecurity-privacy-sensitive-data-exposure-how-its-different-from-data-breach.html)
- 2229 [30] MSSPAlert (2019) *Ransom Attacks Target Backups, NAS (Network Attached Storage)*.
2230 Available at ([https://www.msspalert.com/cybersecurity-news/attacks-target-nas-](https://www.msspalert.com/cybersecurity-news/attacks-target-nas-backups/)
2231 [backups/](https://www.msspalert.com/cybersecurity-news/attacks-target-nas-backups/))
- 2232 [31] Wikipedia (2020) *Attack Surface*. Available at
2233 https://en.wikipedia.org/wiki/Attack_surface
- 2234 [32] TechTarget-SearchITChannel (2007) *Fibre Channel man-in-the-middle attacks*.
2235 Available at [https://searchitchannel.techtarget.com/feature/Fibre-Channel-man-in-the-](https://searchitchannel.techtarget.com/feature/Fibre-Channel-man-in-the-middle-attacks)
2236 [middle-attacks](https://searchitchannel.techtarget.com/feature/Fibre-Channel-man-in-the-middle-attacks)
- 2237 [33] Security Week (2018) *Hackers Can Stealthily Exfiltrate Data vis Power Lines*. Available
2238 at <https://www.securityweek.com/hackers-can-stealthily-exfiltrate-data-power-lines>
- 2239 [34] Ross RS, Pillitteri V, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled
2240 Unclassified Information in Nonfederal Systems and Organizations. (National Institute of
2241 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171,
2242 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-171r2>
- 2243 [35] Department of Homeland Security (2017) *Reducing the Risk of SNMP Abuse*. Available
2244 at <https://us-cert.cisa.gov/ncas/alerts/TA17-156A>
- 2245 [36] National Institute of Standards and Technology (2018) Framework for Improving Critical
2246 Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and
2247 Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>