



Index for ISO/IEC 27040:2015

Version 1.0

ABSTRACT: The ISO/IEC 27040:2015 (Information technology - Security techniques - Storage security) standard provides detailed technical guidance on controls and methods for securing storage systems and ecosystems. Until late in the development of this standard, the drafts included a detailed index that significantly enhanced the usability of the standard. Unfortunately, this index was lost as part of the ISO publication process. This custom-developed index, which is perfectly aligned with the published standard, can be used to quickly locate terms and concepts throughout the standard.

Publication of this SNIA Technical Proposal has been approved by the SNIA. This document represents a stable proposal for use as agreed upon by the Security TWG. The SNIA does not endorse this proposal for any other purpose than the use described. This proposal may not represent the preferred mode, and the SNIA may update, replace, or release competing proposal at any time. If the intended audience for this release is a liaison standards body, the future support and revision of this proposal may be outside the control of the SNIA or originating Security TWG. Suggestion for revision should be directed to <http://www.snia.org/feedback/>.

SNIA Technical Proposal

February 17, 2015

USAGE

The SNIA hereby grants permission for individuals to use this document for personal use only, and for corporations and other business entities to use this document for internal use only (including internal copying, distribution, and display) provided that:

1. Any text, diagram, chart, table or definition reproduced shall be reproduced in its entirety with no alteration, and,
2. Any document, printed or electronic, in which material from this document (or any portion hereof) is reproduced shall acknowledge the SNIA copyright on that material, and shall credit the SNIA for granting permission for its reuse.

Other than as explicitly provided above, you may not make any commercial use of this document, sell any or this entire document, or distribute this document to third parties. All rights not explicitly granted are expressly reserved to SNIA.

Permission to use this document for purposes other than those enumerated above may be requested by e-mailing tcmd@snia.org. Please include the identity of the requesting individual and/or company and a brief description of the purpose, nature, and scope of the requested use.

DISCLAIMER

The information contained in this publication is subject to change without notice. The SNIA makes no warranty of any kind with regard to this specification, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The SNIA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this specification.

Suggestions for revisions should be directed to <http://www.snia.org/feedback/>.

Copyright © 2015 SNIA. All rights reserved. All other trademarks or registered trademarks are the property of their respective owners.

Revision History

Revision	Date	Sections	Originator:	Comments
V1.0 R0	1/22/2015	All	Eric Hibbard	Initial Draft
V1.0 R1	2/17/2015	All	Eric Hibbard	Address TWG ballot comments

Suggestion for changes or modifications to this document should be submitted at <http://www.snia.org/feedback/>.

Index

- access
 - accidental, 15
 - unauthorized, 2, 14, 15, 16, 17, 18, 27, 35, 47, 77, 83, 89
- access control, 13, 17, 21, 26, 31, 32, 33, 35, 36, 39, 49, 52, 53, 55, 56, 57, 81, 82, 83, 90, 91, 92, 93, 94, 97, 98, 102
- Access Control Entry, 7
- Access Control List, 7, 21, 22, 23, 32, 34, 44, 77, 78, 82, 87, 98
- accessibility, 16
- accidental
 - access, 15
 - alteration, 15
 - configuration changes, 15
 - data loss, 15, 18, 77
 - destruction, 2, 15
 - disclosure, 15
 - loss of media, 15
- accidents, 48
- accountability, 25, 29, 43, 49, 56, 58, 80, 87, 90, 100
- accreditation, 52, 91
- ACE. *See* Access Control Entry
- ACL. *See* Access Control List
- Advanced Encryption Standard, 7, 41
- Advanced Technology Attachment, 7, 39, 60, 64, 66, 67, 68, 71, 99, 110
- AES. *See* Advanced Encryption Standard
- alteration
 - accidental, 15
 - unauthorized, 16
 - unlawful, 2, 15, 16
- ANSI INCITS 400, 36, 110
- ANSI INCITS 458, 36, 110
- ANSI INCITS 461, 105, 110
- ANSI INCITS 462, 22, 110
- ANSI INCITS 463, 104, 105, 110
- ANSI INCITS 470, 31, 104, 110
- ANSI INCITS 482, 110
- ANSI INCITS 496, 18, 102, 111
- ANSI INCITS 521, 111
- arbitrated loop, 12, 28, 57
- archiving, 21
- ATA. *See* Advanced Technology Attachment
- attack
 - history, 49, 90
 - surface, 12
 - vector, 24
- attacks, 27, 43, 45, 48, 52, 79, 87, 88, 91, 99
 - adversarial, 47, 89
 - Denial of Service, 14, 16
 - indirect, 27, 32, 79, 82
 - intentional, 16
 - laboratory, 60
 - malicious, 16
 - malware, 15
 - non-malicious, 16
 - slow, 48, 49, 90
- audit log, 58, 94
 - data, 30, 80
 - entries, 26, 30, 49, 52, 80, 90, 91, 101
 - infrastructure, 41
 - material, 52, 91
 - records, 29, 80
 - trail, 38
- audit logging, 26, 28, 29, 30, 56, 57, 80, 93, 94, 100, 101
- audit logs, 17, 26, 56, 93
- audit trail, 39, 85
- authentication, 20, 22, 23, 25, 26, 27, 29, 31, 32, 33, 35, 36, 37, 48, 74, 77, 78, 79, 82, 83, 96, 97, 102, 103, 104, 105, 108

centralized, 26, 31, 48, 79, 81, 97
 entity, 26, 27, 35, 79
 external, 35, 84, 96, 97
 factor, 96
 multi-factor, 4, 26, 27, 79, 96
 mutual, 31, 81, 96, 103, 105
 strong, 7, 26, 27, 33, 35, 79, 83
 authenticity, 28, 30, 36, 55, 56, 58, 84, 92, 93
 authorization, 23, 25, 26, 27, 33, 35, 37, 79, 97, 102
 autonomous data movement, 13, 14, 58, 94, 95
 sanitization, 58
 availability, 4, 6, 13, 14, 15, 16, 24, 28, 37, 45, 46, 48, 65, 69, 75, 76, 88, 105
 application, 18
 data, 46, 48, 52, 88
 designs, 46, 88
 high, 46
 objective, 53
 objectives, 92
 priorities, 76
 backups, 12, 13, 14, 16, 18, 34, 38, 42, 46, 47, 52, 57, 73, 77, 85, 88, 89
 LAN-free, 32
 BC. *See* Business Continuity
 BCM. Business Continuity Management
 breach notifications, 17, 38
 Business Continuity, 7, 13, 14, 18, 42, 43, 47, 50, 51, 86, 89, 90
 Business Continuity Management, 7, 47
 CAS. *See* Content Addressable Storage
 CDMI. *See* Cloud Data Management Interface
 CDP. *See* Continuous Data Protection
 certificate of sanitization, 38, 39, 85
 chain of custody, 28, 30, 38, 49, 56, 80, 90, 93
 chain of trusted individuals, 47, 89
 Challenge Handshake Authentication Protocol, 7, 26, 31, 81
 CHAP. *See* Challenge Handshake Authentication Protocol
 CIFS. *See* Common Internet File System
 circulation
 unauthorized, 76
clear, 2, 5, 13, 31, 32, 35, 37, 38, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 84, 85
 cloud computing, 34
 storage, 13, 23, 34, 35, 83
 Cloud Data Management Interface, 7, 35, 44, 83, 84, 87, 109
 authenticate entities, 83
 clients, 35
 Deletion, 35, 84
 Domains, 35, 84
 Hold, 84
 Holds, 35
 logging, 35
 sanitization, 84
 security authenticate entities, 35
 security capabilities, 35, 83
 security logging, 84
 cloud service provider, 34, 35, 83, 84
 cluster
 asymmetric, 33, 34, 83
 fault tolerant, 12
 highly scalable, 32
 Network Attached Storage, 23, 33
 symmetric, 33, 34, 83
 CNA. *See* Converged Network Adaptor
 Common Internet File System, 7, 23, 24, 33, 44, 78, 82, 83, 87
 apply ACLs, 33

- auditing, 33, 83
 - enable, 24, 78
 - strong authentication, 33, 83
 - unauthenticated access, 33, 82
- compliance, vi, 14, 17, 28, 29, 30, 37, 38, 52, 55, 56, 80, 85, 91, 93, 100, 102, 103
 - requirements, 12, 14, 24, 43, 52
- compression**, 2, 13, 42, 49, 50, 55, 86, 90, 92
- confidentiality, 40, 41, 50, 58, 60, 63, 75, 76, 104, 108
 - appropriate measures, 22
 - attacking, 4
 - breach of, 17
 - capabilities, 40
 - Common Transport, 104
 - components, 20
 - encryption, 40, 53
 - ensure adequate, 14
 - ESP_Header, 31
 - FC frame, 102
 - frame, 102
 - key management, 40
 - measures, 56, 78, 93
 - mechanisms, 30, 80
 - privacy requirements, 53, 76, 92
 - risks, 28, 37, 85
 - sanitization, 25, 85, 99
- configuration changes
 - accidental, 15
- Content Addressable Storage, 7, 12, 36, 84
- Continuous Data Protection, 7, 12, 38, 46, 47, 52, 85
- Converged Network Adaptor, 7, 20, 44
- corruption
 - data, 15, 16, 18, 27, 52, 77
 - hardware-based, 16
 - intentional, vi, 18, 77
 - unauthorized, 15
- cryptographic erase**, 2, 38, 39, 57, 60, 62, 63, 64, 65, 66, 67, 68, 69, 71, 72, 73, 74, 85, 86, 94, 99, 100
- cryptographic hash, 36
- cryptoperiod**, 2, 42, 49, 52, 86, 90, 91
- CT_Authentication, 102, 104
- curation, 49
- DAC. *See* Discretionary Access Control
- DAS. *See* Direct Attached Storage
- data at rest**, 2, 5, 13, 14, 17, 20, 31, 32, 33, 34, 35, 41, 51, 52, 53, 57, 77, 82, 83, 84, 89, 91, 93, 94
- data authenticity, 12, 49, 56, 90, 93
- data breach**, vi, 2, 5, 15, 20, 38, 51, 53, 57, 86
 - potential forms, 15
 - storage-oriented, 15
- data corruption, 15, 16, 18, 27, 52, 77
- data destruction, 2, 15, 16, 27, 52, 55, 92
- data in motion**, 2, 13, 14, 20, 40, 41, 86
- data integrity**, 2, 13, 16, 22, 35, 40, 46, 48, 49, 52, 56, 78, 90, 91, 93
- Data Lifecycle Management, 58
- data loss
 - accidental, 15, 18, 77
 - intentional, 18, 77
- data path, 27
 - diverse, 57, 94
 - multiple, 18, 57, 94
 - redundant, 45
- data protection, vi, 14, 18, 24, 38, 40, 46, 49, 52, 57, 62, 85, 90
 - backups, 12, 13, 14, 16, 18, 32, 34, 38, 42, 46, 47, 52, 57, 73, 77, 85, 88, 89
 - Continuous Data Protection, 7, 12, 38, 46, 47, 52, 85
 - mechanisms, 16, 38, 46, 85, 88
 - methods, 41

- replication, 38, 42, 46, 47, 50, 52, 57, 85, 88, 89, 94
- snapshots, 13
- strategy, 13
- systems, 12
- data reduction, 13, 42, 51, 86, 90
- technologies, 13, 42, 49, 50
- data sensitivity, 44
- DDoS. *See* Distributed Denial of Service
- deduplication**, 2, 13, 42, 49, 50, 55, 56, 86, 90, 92, 93
- defence in depth, 43
- degauss**, 2, 38, 60, 63, 64, 65, 66, 67, 71, 100
- denial of access, 27
- Denial of Service, 8, 14, 16
- deconstruct**, 3, 4, 5, 6, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72
- disintegrate, 3, 60, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72
- incinerate, 3, 4, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72
- melt, 3, 4, 60
- pulverize, 3, 5, 60, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72
- shred, 3, 6, 60, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 72
- destruction**, 3, 17, 28, 30, 39, 60, 66, 67, 80, 100
 - accidental, 2, 15, 16
 - data, 2, 15, 16, 27, 52, 55, 92
 - keys, 41
 - media, 60
 - unauthorized, 6, 15, 16
 - unlawful, 2, 15, 16
- DH-CHAP. *See* Diffie Hellman – Challenge Handshake Authentication Protocol
- Diffie Hellman – Challenge Handshake Authentication Protocol, 8, 26, 103
- Diffie-Hellman Challenge
 - Handshake Authentication Protocol, 102
- digital signature, 40
- Direct Attached Storage, 8, 12, 17, 18, 77
- Disaster Recovery, 8, 13, 14, 18, 38, 42, 47, 49, 50, 51, 86, 89, 90
- Disaster Recovery Planning, 8, 47
- disclosure
 - accidental, 15, 61
 - public, 15
 - unauthorized, 2, 6, 15, 16, 41, 56, 76, 93
- Discretionary Access Control, 7, 97
- disintegrate**, 3, 60, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72
- Distributed Denial of Service, 8, 14
- DNS. *See* Domain Name System
- Domain Name System, 8, 27, 29, 79, 82
- DoS. *See* Denial of Service
- DR. *See* Disaster Recovery
- DRP. Disaster Recovery Planning
- EHR. *See* Electronic Healthcare Record
- Electronic Healthcare Record, 8, 37, 85
- Electronically Stored Information**, 3, 6, 8, 11
- Encapsulating Security Payload, 8, 104, 110
- encryption**, 13, 14, 17, 18, 20, 26, 31, 32, 33, 35, 36, 38, 40, 41, 42, 47, 48, 49, 50, 51, 52, 54, 55, 86, 91, 92, 99, 104
 - at rest, 13, 14, 23, 31, 32, 33, 34, 35, 41, 47, 51, 52, 53, 57, 82, 83, 84, 86, 89, 91, 94
 - CDP, 47
 - in motion, 13, 23, 40, 41, 47, 52, 57, 86, 89, 91, 94
 - key, 15, 25, 42, 46, 54, 74, 86, 88

- modes of operations, 40, 41, 86, 109, 111
- point of, 5, 14, 41, 50, 51, 90
- proof of, 17, 41, 51, 100
- ESI. *See* Electronically Stored Information
- ESP. *See* Encapsulating Security Payload
- ESP_Header, 31, 40, 81, 102, 104
- Ethernet, 22, 78
- event logging, 28, 29, 80, 100
 - centralized, 28, 80
 - external, 28, 80
 - program, 28
- event signing, 30
- evidentiary data, 56
- fault-tolerance, 47, 89
- FC. *See* Fibre Channel
- FCAP. *See* Fibre Channel Certificate Authentication Protocol
- FCEAP. *See* Fibre Channel Extensible Authentication Protocol
- FCIP. *See* Fibre Channel over TCP/IP
- FCoE. *See* Fibre Channel over Ethernet
- FCP. *See* Fibre Channel Protocol
- FCPAP. *See* Fibre Channel Password Authentication Protocol
- FCS. *See* Fixed Content Storage
- FC-SP. *See* Fibre Channel – Security Protocol
- FC-SP Zoning, 21, 44, 77, 105
- FDE. *See* Full Disk Encryption
- Fibre Channel**, 3, 8, 13, 18, 19, 21, 22, 27, 31, 65, 68, 79, 81, 102, 104
 - fabric, 102
 - fabrics, 102
 - frames, 22, 102, 104
 - interface, 18
 - port, 101
 - storage, 31
- Storage Area Network, 22
- switch, 101
- topologies, 21
- traffic, 104
- Fibre Channel – Security Protocol, 8, 18, 27, 31, 79, 81, 102, 111
 - policy, 21, 77
 - Zoning, 21, 44, 77, 105
- Fibre Channel Certificate Authentication Protocol, 8, 102
- Fibre Channel Extensible Authentication Protocol, 8, 102
- Fibre Channel over Ethernet, 8, 13, 19, 22, 78
- Fibre Channel over TCP/IP, 8, 22, 78, 110
- Fibre Channel Password Authentication Protocol, 8, 102
- Fibre Channel Protocol**, 3, 8, 19, 21, 26, 31
- filesystem, 13, 32
 - encryption, 50
 - exported, 32, 33
 - namespace, 33, 34, 83
 - network, 82
- Fixed Content Storage, 8, 36
- Full Disk Encryption, 8, 18, 77
- Galois/Counter Mode, 8, 41, 111
- gateway**, 3, 19, 21, 42, 77, 78
- GCM. *See* Galois/Counter Mode
- HAMR. *See* Heat Assisted Magnetic Recording
- Hard Disk Drive, 8, 12, 17, 39, 41, 53, 64, 65, 67
- HBA. *See* Host Bus Adapter
- HDD. *See* Hard Disk Drive
- Heat Assisted Magnetic Recording, 8, 66
- Host Bus Adapter, 8, 20, 21, 41, 44, 50, 86, 101
- hypervisor, 30, 53, 81, 92
- ICT Readiness for Business Continuity, 9, 47
- IDS. *See* Intrusion Detection System

IEEE 1619.1-2007, 41, 110
 IEEE 1619.2-2010, 40, 110
 IEEE 1619-2007, 40, 41, 110
 IETF RFC 1813, 24, 110
 IETF RFC 3195, 29, 110
 IETF RFC 3530, 24, 110
 IETF RFC 3720, 22, 110
 IETF RFC 3723, 22, 110
 IETF RFC 3821, 22, 110
 IETF RFC 4303, 104, 110
 IETF RFC 4595, 104, 110
 IETF RFC 5246, 40, 110
 IETF RFC 5424, 29, 110
 IETF RFC 5425, 29, 110
 IETF RFC 5426, 29, 110
 IETF RFC 5427, 29, 110
 IETF RFC 5661, 24, 110
 IETF RFC 5663, 34, 110
 IETF RFC 5848, 29, 110
 IETF RFC 6012, 29, 110
 IETF RFC 6071, 40, 110
 IETF RFC 6587, 29, 110
 IETF RFC 7146, 22, 110
 IKE. *See* Internet Key Exchange
 ILM. *See* Information Lifecycle Management
 immutability, 52, 58, 91
 immutable, 52
in-band, 3, 17, 18, 27, 29, 79
incinerate, 3, 4, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72
 InfiniBand, 13, 19
 Information Lifecycle Management, 9, 58
 Information Security Management System, vi
 integrity, 4, 13, 14, 28, 40, 41, 48, 49, 52, 58, 75, 76, 90, 91, 94
 algorithm, 40
 log, 30, 80
 services, 12
 verification, 52
 intentional
 attacks, 16
 circumvention of security, 16
 corruption, vi, 77
 data loss, 18, 77
 Internet Key Exchange, 9, 40, 41, 86, 102, 104, 110
 Internet Protocol Security, 9, 13, 22, 24, 26, 31, 36, 40, 41, 78, 79, 84, 86, 110
 Internet Small Computer Systems Interface, 9, 19, 22, 26, 31, 44, 78, 81, 87, 110
 initiator, 31, 81
 interfaces, 22, 78
 network, 22
 security, 31
 Internet Storage Name Service, 9, 32, 82
 Intrusion Detection System, 9, 13, 27, 79
 Intrusion Prevention System, 9, 13, 27, 79
 IPS. *See* Intrusion Prevention System
 IPsec. *See* Internet Protocol Security
 IRBC. ICT Readiness for Business Continuity
 iSCSI. *See* Internet Small Computer Systems Interface
 iSNS. *See* Internet Storage Name Service
 ISO 16175-1, 48, 109
 ISO 16175-2, 48, 109
 ISO 16175-3, 48, 109
 ISO 16609, 2, 109
 ISO 19092, 4
 ISO 7498-2, 2, 109
 ISO Guide 73, 109
 ISO/IEC 10116, 40, 41, 109
 ISO/IEC 11179-1, 4, 111
 ISO/IEC 11770, 40, 41, 109
 ISO/IEC 14776-372, 3, 111
 ISO/IEC 15408, 51
 ISO/IEC 17788, 1, 4, 56
 ISO/IEC 17826, 35, 109
 ISO/IEC 19790, 51, 74, 109

ISO/IEC 24759, 74, 109
 ISO/IEC 24775, 57, 109
 ISO/IEC 27000, 1
 ISO/IEC 27001, vi, 1, 43, 55, 75, 93
 ISO/IEC 27002, vi, 17, 26, 28, 30,
 37, 40, 43, 46, 55, 75, 93, 96,
 111
 ISO/IEC 27003, 109
 ISO/IEC 27005, vi, 1, 14, 43, 75, 76
 ISO/IEC 27031, 47, 109
 ISO/IEC 27033, 18
 ISO/IEC 27033-1, 4, 109
 ISO/IEC 27033-2, 25, 44, 109
 ISO/IEC 27033-3, 109
 ISO/IEC 27037, 56, 109
 ISO/IEC/IEEE 24765, 4, 5, 110
 ISO/PAS 22399, 47, 109
 ISO/TR 10255, 48, 109
 ISO/TR 12033, 2
 ISO/TR 18492, 48, 109
 ISO/TS 22600-1, 7
 isolation, 54, 101
 logical, 21, 27, 79
 physical, 21, 22, 27, 79
 secure, 57, 93
 KEK. *See* Key Encryption Key
 Kerberos, 23, 24, 32, 33, 78, 82, 83,
 97
 key backup, 55, 92
 Key Encryption Key, 9, 73, 74
 key escrow, 54, 92
 key management, 14, 26, 40, 41,
 42, 43, 50, 52, 54, 55, 57, 87,
 91, 92, 94, 109, 111
 centralized, 50, 86
 frameworks, 41
 guidance, 40
 purpose, 40
 services, 12
 specifications, 40
 Key Management Interoperability
 Protocol, 9, 41, 42, 57, 86, 94,
 111
 KMIP. *See* Key Management
 Interoperability Protocol
 LAN. *See* Local Area Network
 LBA. *See* Logical Block Address
 LDAP. *See* Lightweight Directory
 Access Protocol
 least privilege, 21, 27, 56, 57, 78,
 79, 93, 94
 legal, 15, 38, 56, 76
 holds, 52, 58, 94
 requirements, 12, 15, 17, 49,
 55, 90
 Lightweight Directory Access
 Protocol, 9, 33, 83, 97
 Local Area Network, 9, 12, 22, 27,
 32, 33, 44, 78, 79, 87
 logging, 29, 35, 80
 CDMI, 35, 84
 centralized, 101
 event, 28, 29, 80, 100
 policy, 28, 30, 80
 protocols, 29
 security, 49, 90
 Logical Block Address, 9, 39, 99
 Logical Unit, 9, 13, 19, 20, 31, 38,
 54, 81, 101
 loss, 16, 37, 49, 85
 of access, 15
 of availability, 15, 16
 of control, 41
 of data, 15, 16
 of information, 15
 of media, 15, 41, 86
 unlawful, 2, 15
 LUN. *See* Logical Unit
 LUN mapping, 20, 31, 81
 LUN masking, 19, 20, 31, 81
 MAC. Mandatory Access Control
malware, 4, 30, 52
 against, 83
 attack, 15
 guard against, 33, 82
 protection, 30, 35, 45, 52, 81,
 91
 Mandatory Access Control, 9, 97
Mean Time Between Failures, 4,
 9, 45

Mean Time To Failure, 9, 45

Mean Time To Repair, 4, 9, 45

Media Encryption Key, 9, 64, 65, 68, 69, 73, 74, 100

media sanitization, 12, 18, 35, 38, 39, 55, 56, 57, 60, 71, 72, 73, 77, 92, 93, 94, 99, 111

MEK. *See* Media Encryption Key

melt, 3, 4, 60

metadata, 3, 4, 16, 23, 36, 49, 52, 56, 93

modem, 27, 28, 80

modes of operations, 40, 41, 86, 109, 111

modification
 unauthorized, 6, 16

MTBF. *See* Mean Time Between Failure

MTTF. *See* Mean Time to Failure

MTTR. *See* Mean Time to Repair

multi-factor authentication, 4, 26, 27, 79, 96

multi-tenancy, 4, 5, 53, 56, 92
 secure, 5, 14, 56, 57, 93

N_Port_ID Virtualization, 10, 21, 54, 77, 92, 101

namespace, 33, 34, 83

NAS. *See* Network Attached Storage

natural disasters, 48

Network Attached Storage, 4, 9, 12, 23, 50
 cluster, 23, 32, 33
 NFS-based, 24, 28, 31, 32, 33, 82
 pNFS-based, 33, 83
 security controls, 23
 SMB/CIFS-based, 33, 34, 82
 with SAN-attach, 32

Network File System, 9, 23, 24, 32, 33, 34, 44, 78, 82, 87, 110

Network Time Protocol, 10, 27, 29, 79

NFS. *See* Network File System

NIST FIPS 140-2, 51, 111

NIST FIPS 197, 40, 111

NIST SP 800-38A, 40, 111

NIST SP 800-38C, 40, 111

NIST SP 800-38D, 40, 111

NIST SP 800-38E, 40, 111

NIST SP 800-57 Part 1, 40, 111

NIST SP 800-57 Part 2, 40, 111

NIST SP 800-67, 40, 111

NIST SP 800-88, 111

non-repudiation, 56, 93

NPIV. *See* N_Port_ID Virtualization

NT LAN Manager, 10, 24, 33, 78, 83

NTLM. *See* NT LAN Manager

NTP. *See* Network Time Protocol

Object-based Storage Device, 10, 12, 23, 35, 36, 84, 110

OSD. *See* Object-based Storage Device

over provisioning, 5, 13

Parallel Network File System, 10, 23, 33, 34, 83, 110

passwords, 15, 71, 81, 96
 strong, 26, 79

patches, 30, 44, 45, 81, 87

path failover, 46

PCIe. *See* Peripheral Component Interconnect Express

Peripheral Component Interconnect Express, 10, 19

Personally Identifiable Information, 10, 15, 37, 55, 85, 92

PII. *See* Personally Identifiable Information

PKI. *See* Public Key Infrastructure

pNFS. *See* Parallel Network File System

point of encryption, 5, 14, 41, 50, 51, 90

point-in time copies, 56, 93

point-to-point, 21

policy, 43, 55, 93
 backups, 73
 data retention, 28, 35, 84
 for storage, 28, 55, 92

- logging, 28, 30, 80
- retention, 80
- sanitization, 17, 73
- security, 1
- port binding, 19
- preservation orders, 56
- privacy, 51, 56, 91
 - breach of, 17
 - requirements, 17, 35, 53, 76, 92
 - threats, 48
- privilege escalation, 26, 29, 79
- privileged
 - access rights, 26
 - operations, 29
 - user, 13, 16, 26, 56, 58, 93, 94
 - user controls, 27, 79
- PRNG. *See* Pseudo-Random Number Generator
- proof, 47, 89
 - of encryption, 17, 41, 51, 100
 - of sanitization, 17, 37, 38, 39, 58, 85
- provenance, 38, 49, 90
- Pseudo-Random Number Generator, 10, 39, 42
- Public Key Infrastructure, 10, 43, 87, 97
- pulverize**, 3, 5, 60, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72
- purge**, 5, 37, 38, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 85, 100
- RADIUS. *See* Remote Authentication Dial In User Service
- RAID. *See* Redundant Array of Independent Disks
- RAM. *See* Random Access Memory
- Random Access Memory, 10, 61, 72
- Random Number Generator, 10, 86
- RBAC. *See* Role-based Access Control
- Read-Only Memory, 10, 61, 72
- Rec. ITU-T X.1601, 34
- Rec. ITU-T Y.3500, 1, 4, 56
- reconnaissance, 27
- recovery plan, 54, 92
- redundancy, 45, 48, 88, 89
- Redundant Array of Independent Disks, 10, 46, 52
- redundant components, 46
- regulatory, 15
 - compliance, vi. 14, 30, 80
 - requirements, vi. 12, 15, 17, 49, 55, 75, 90
- reliability**, 5, 16, 45, 47, 48, 88, 89
- remote access, 26, 27, 79
- Remote Authentication Dial In User Service, 10, 26, 33, 83, 97
- Remote Procedure Call, 10, 24
- replication, 38, 46, 47, 52, 57, 85, 88, 89, 94
 - out of region, 50
 - remote, 42
 - security, 47
- resilience, 47, 48, 89
- resiliency, 13, 46
- retention, 49, 56, 100
 - cloud data, 35
 - data, 17, 51, 52, 55, 56, 80, 91, 92, 93
 - drivers, 49
 - event log data, 30
 - long-term, 12, 34, 48, 90
 - medium-term, 37, 49, 90
 - metadata, 49
 - periods, 49, 52
 - policy, 28, 35, 80, 84
 - requirements, 80
 - short-term, 49, 90
- right of erasure, 35
- right to be forgotten, 35
- risk, vi. 11, 15, 28, 37, 41, 49, 50, 54, 63, 85
 - acceptance, 14, 71
 - assessment, 14, 43, 50, 75, 76
 - communication, 14
 - management, vi. 1, 14, 109
 - mitigation, 1, 20, 43, 47, 65, 99

monitoring and review, 14
 profile, 5
 security, 15
 storage security, 14, 43
 tolerance, 44, 49, 90
 treatment, 14
 RNG. *See* Random Number Generator
 Role-based Access Control, 10, 97
 roles, 26, 27, 43, 56, 79, 87, 93, 97, 98
 ROM. *See* Read-Only Memory
 RPC. *See* Remote Procedure Call
 SAN. *See* Storage Area Network
 sanctions, 17, 38
sanitization, 5, 14, 25, 35, 37, 38, 39, 51, 53, 56, 58, 60, 61, 62, 63, 65, 66, 67, 69, 71, 72, 73, 74, 85, 99, 100
 after end-of-use, 15, 38, 85
 application-based, 18
 autonomous data movement, 58, 95
 CDMI, 84
 certificate of, 38, 39, 85
 cloud computing, 83
 computer-based, 18
 costly and time consuming, 37
 cryptographic erase, 73, 86, 99
 encryption keys, 72
 integrated functionality, 18
 logical, 31, 32, 38, 81, 82, 85
 media, 12, 18, 35, 37, 38, 39, 55, 56, 57, 60, 71, 72, 73, 77, 92, 93, 94, 99, 111
 media-aligned, 31, 32, 81, 82
 method, 38, 60, 61, 62, 63, 67, 68, 72
 policy, 17, 73
 proof of, 17, 37, 38, 39, 58, 85
 rapid, 31, 32, 81, 82
 record, 85
 record of, 38
 verification, 39, 86
sanitize, 2, 3, 5, 13, 38, 39, 56, 57, 58, 60, 61, 62, 64, 67, 68, 69, 71, 72, 73, 74, 85, 93, 94, 100
 clear, 2, 5, 13, 31, 32, 35, 37, 38, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 84, 85
 destruct, 3, 4, 5, 6, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72
 disintegrate, 3, 60, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72
 incinerate, 3, 4, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72
 key, 73, 74, 100
 melt, 3, 4, 60
 pulverize, 3, 5, 60, 61, 62, 63, 65, 67, 68, 69, 70, 71, 72
 purge, 5, 37, 38, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 85, 100
 shred, 3, 6, 60, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 72
 SAS. *See* Serial Attached SCSI
 SCSI. *See* Small Computer System Interface
 secret-sharing, 49
 secure initialization, 45, 88
secure multi-tenancy, 5, 14, 56, 57, 93
 Secure Shell, 11, 27, 79
 Security Association Management Protocol, 102
 security domain, 28, 44, 87, 88
 Security Information and Event Management, 10, 29, 80
security strength, 5, 7, 50, 51, 57, 73, 91, 94
 SED. *See* Self-Encrypting Drives
 Self-Encrypting Drives, 10, 17, 41, 51, 74, 77, 91, 98, 99, 100
 separation of duties, 27, 52, 91
 Serial Attached SCSI, 10, 19, 65, 68
 Server Message Block, 10, 23, 24, 33, 78, 82, 83

- apply ACLS, 33
 - enable, 24, 78
- Service Locator Protocol, 10, 27, 32, 79, 82
- shred**, 3, 6, 60, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 72
- SIEM. *See* Security Information and Event Management
- signature, 26, 39, 96
 - digital, 40, 107
- silent corrections, 16
- Simple Network Management Protocol, 11, 27, 57, 94
- single point of failure**, 6, 13, 20, 45, 46, 88
- Single Sign-on, 11, 26, 97
- SLP. *See* Service Locator Protocol
- Small Computer System Interface, 3, 10, 21, 39, 60, 65, 66, 67, 68, 71, 99
- SMB. *See* Server Message Block
- SMI-S. *See* Storage Management Initiative – Specification
- snapshots, 13
- SNMP. *See* Simple Network Management Protocol
- Solid State Drive, 11, 12, 13, 39, 60, 68, 69, 73, 74
- Solid State Hard Drive, 11, 12, 13, 60, 64, 65
- SSD. *See* Solid State Drive
- SSH. *See* Secure Shell
- SSHD. *See* Solid State Hard Drive
- SSO. *See* Single Sign-on
- Storage Area Network**, 6, 10, 18, 19, 20, 21, 22, 32, 44
- storage device**, 3, 4, 6, 11, 12, 16, 18, 19, 20, 21, 32, 35, 39, 41, 42, 44, 55, 57, 63, 64, 65, 66, 68, 69, 71, 72, 73, 74, 77, 87, 88, 92, 99, 100
- storage ecosystem, 6, 47, 55, 89, 92, 93
- storage element**, 3, 6, 11, 16, 17, 18, 21, 24, 44, 50, 57
- storage management, 13, 14, 16, 25, 57, 79, 94, 109
 - in-band, 18
 - logging, 28
 - remote, 79
 - roles, 27
 - segregate traffic, 21, 77
 - threats, 15
- Storage Management Initiative – Specification, 10, 57, 94, 111
- storage security**, vi, 1, 6, 28, 42, 43
 - architecture, 43
 - concepts, 1
 - controls, 17, 52
 - design, 45
 - design and implementation, 43, 46
 - design rules, 44
 - introduction, 12
 - relevance, 1
 - risk, 14
 - scope, 1
 - services, 37
 - threats, 43
- switched fabric, 21
- syslog, 29, 57, 94, 110
- target data, 2, 5, 7, 39, 60, 72, 73, 100
- TCG
 - Enterprise SSC, 64, 65, 68, 69, 111
 - Opal SSC, 64, 65, 68, 69, 111
- TCP wrappers, 27, 79
- threats, 1, 11, 13, 14, 15, 26, 43, 44, 52, 75, 87
 - privacy, 48
 - storage security, 43
- timeliness, 17
- timestamp, 3, 29
- TLS. *See* Transport Layer Security
- topologies, 3, 13, 18, 21
- traceability, 25, 49, 56, 58, 90

Transport Layer Security, 11, 26,
 27, 29, 34, 35, 40, 41, 57, 79,
 86, 94, 110
 unauthorized
 access, 2, 14, 15, 16, 17, 18, 27,
 35, 47, 77, 83, 89
 alteration, 16
 circulation, 76
 corruption, 15
 destruction, 6, 15, 16
 disclosure, 2, 6, 15, 16, 41, 56,
 76, 93
 modification, 6
 modifications, 16
 usage, 14
 Universal Serial Bus, 11, 65, 67, 68,
 69
 unlawful
 alteration, 2, 15, 16
 destruction, 2, 15, 16
 loss, 2, 15
 transfer of data, 17
 usage
 unauthorized, 14
 USB. *See* Universal Serial Bus
 vendor
 maintenance, 27, 28, 79, 80
 support personnel, 13
 vendors
 implement functionality, 31,
 32, 33, 35, 36, 37, 40, 45,
 52, 57, 59
 trusted, 47, 89
 Virtual Local Area Network, 11, 22,
 27, 44, 78, 79, 88
 Virtual Machine, 11, 53, 54, 92
 Virtual Private Network, 11, 27, 79
 virtual storage, 53, 91
 Virtual Storage Area Network, 11,
 44, 88
 virtualization, 13, 19, 20, 35, 53
 security, 12
 server, 38, 53, 92
 storage, 52, 53, 91
 VLAN. *See* Virtual Local Area
 Network
 VM. *See* Virtual Machine
 VPN. *See* Virtual Private Network
 VSAN. *See* Virtual Storage Area
 Network
weak key, 7, 42, 86
 World Wide Name, 11, 19, 31, 81
 World Wide Port Name, 11, 54,
 101
 WORM. *See* Write Once Read Many
 Write Once Read Many, 11, 30, 52,
 55, 81, 91, 92
 WWN. *See* World Wide Port Name,
 See World Wide Name
 XTS-AES, 41
 zoning, 19, 29, 44, 88, 101
 basic, 21, 77
 FC-SP Zoning, 21, 77, 102, 105
 hard, 19, 21, 77
 secure, 19
 soft, 19