

BS EN ISO/IEC 27040:2016



BSI Standards Publication

Information technology — Security techniques — Storage security (ISO/IEC 27040:2015)



National foreword

This British Standard is the UK implementation of EN ISO/IEC 27040:2016. It is identical to ISO/IEC 27040:2015. It supersedes BS ISO/IEC 27040:2015 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee IST/33, IT - Security techniques to Subcommittee IST/33/4, Security Controls and Services.

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 92352 4

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2015.

Amendments issued since publication

Date	Text affected
30 September 2016	This corrigendum rennumbers BS ISO/IEC 27040:2015 as BS EN ISO/IEC 27040:2016

English Version

Information technology - Security techniques - Storage
security (ISO/IEC 27040:2015)

Technologie de l'information - Techniques de sécurité -
Sécurité de stockage (ISO/IEC 27040:2015)

Informationstechnik - IT-Sicherheitsverfahren -
Speichersicherheit (ISO/IEC 27040:2015)

This European Standard was approved by CEN on 19 June 2016.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of ISO/IEC 27040:2015 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27040:2016.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2017, and conflicting national standards shall be withdrawn at the latest by February 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27040:2015 has been approved by CEN as EN ISO/IEC 27040:2016 without any modification.

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	7
5 Overview and concepts	11
5.1 General	11
5.2 Storage concepts	12
5.3 Introduction to storage security	12
5.4 Storage security risks	14
5.4.1 Background	14
5.4.2 Data breaches	15
5.4.3 Data corruption or destruction	16
5.4.4 Temporary or permanent loss of access/availability	16
5.4.5 Failure to meet statutory, regulatory, or legal requirements	17
6 Supporting controls	17
6.1 General	17
6.2 Direct Attached Storage (DAS)	17
6.3 Storage networking	18
6.3.1 Background	18
6.3.2 Storage Area Networks (SAN)	18
6.3.3 Network Attached Storage (NAS)	23
6.4 Storage management	24
6.4.1 Background	24
6.4.2 Authentication and authorization	26
6.4.3 Secure the management interfaces	27
6.4.4 Security auditing, accounting, and monitoring	28
6.4.5 System hardening	30
6.5 Block-based storage	31
6.5.1 Fibre Channel (FC) storage	31
6.5.2 IP storage	31
6.6 File-based storage	32
6.6.1 NFS-based NAS	32
6.6.2 SMB/CIFS-based NAS	33
6.6.3 Parallel NFS-based NAS	33
6.7 Object-based storage	34
6.7.1 Cloud computing storage	34
6.7.2 Object-based Storage Device (OSD)	35
6.7.3 Content Addressable Storage (CAS)	36
6.8 Storage security services	37
6.8.1 Data sanitization	37
6.8.2 Data confidentiality	40
6.8.3 Data reductions	42

7	Guidelines for the design and implementation of storage security	43
7.1	General	43
7.2	Storage security design principles	43
7.2.1	Defence in depth	43
7.2.2	Security domains	44
7.2.3	Design resilience	45
7.2.4	Secure initialization	45
7.3	Data reliability, availability, and resilience	45
7.3.1	Reliability	45
7.3.2	Availability	46
7.3.3	Backups and replication	46
7.3.4	Disaster Recovery and Business Continuity	47
7.3.5	Resilience	48
7.4	Data retention	48
7.4.1	Long-term retention	48
7.4.2	Short to medium-term retention	49
7.5	Data confidentiality and integrity	50
7.6	Virtualization	52
7.6.1	Storage virtualization	52
7.6.2	Storage for virtualized systems	53
7.7	Design and implementation considerations	54
7.7.1	Encryption and key management issues	54
7.7.2	Align storage and policy	55
7.7.3	Compliance	55
7.7.4	Secure multi-tenancy	56
7.7.5	Secure autonomous data movement	57
	Annex A (normative) Media sanitization	60
	Annex B (informative) Selecting appropriate storage security controls	75
	Annex C (informative) Important security concepts	96
	Bibliography	109

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *Security techniques*.

Introduction

Many organizations face the challenge of implementing data protection and security measures to meet a wide range of requirements, including statutory and regulatory compliance. Too often the security associated with storage systems and infrastructure has been missed because of misconceptions and limited familiarity with the storage technology, or in the case of storage managers and administrators, a limited understanding of the inherent risks or basic security concepts. The net result of this situation is that digital assets are needlessly placed at risk of compromise due to data breaches, intentional corruption, being held hostage, or other malicious events.

Data storage has matured in an environment where security has been a secondary concern due to its historical reliance on isolated connectivity, specialized technologies, and the physical security of data centres. Even as storage connectivity evolved to use technologies such as storage protocols over Transmission Control Protocol/Internet Protocol (TCP/IP), few users took advantage of either the inherent security mechanisms or the recommended security measures.

This International Standard provides guidelines for storage security in an organization, supporting in particular the requirements of an Information Security Management System (ISMS) according to ISO/IEC 27001. This International Standard recommends the information security risk management approach as defined in ISO/IEC 27005. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.

This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

The objectives for this International Standard are the following:

- help draw attention to the risks;
- assist organizations in better securing their data when stored;
- provide a basis for auditing, designing, and reviewing storage security controls.

It is emphasized that ISO/IEC 27040 provides further detailed implementation guidance on the storage security controls that are described at a basic standardized level in ISO/IEC 27002.

It should be noted that this International Standard is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Information technology — Security techniques — Storage security

1 Scope

This International Standard provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Storage security is relevant to anyone involved in owning, operating, or using data storage devices, media, and networks. This includes senior managers, acquirers of storage product and service, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security or storage security, storage operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design, and implementation of the architectural aspects of storage network security.

This International Standard provides an overview of storage security concepts and related definitions. It includes guidance on the threat, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other International Standards and technical reports that address existing practices and techniques that can be applied to storage security.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ITU-TY.3500 | ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27005, and the following apply.

3.1

block

unit in which data is *stored* ([3.50](#)) and retrieved on disk and tape *devices* ([3.14](#))

3.2 **clear**

sanitize (3.38) using logical techniques on data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user

3.3 **compression**

process of removing redundancies in digital data to reduce the amount that should be *stored* (3.50) or transmitted

[SOURCE: ISO/TR 12033:2009, 3.1]

Note 1 to entry: For *storage* (3.43), lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.

3.4 **cryptographic erase**

method of *sanitization* (3.37) in which the encryption key for the encrypted *target data* (3.52) is *sanitized* (3.38), making recovery of the decrypted *target data* (3.52) infeasible

3.5 **cryptoperiod**

defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys in a given system can remain in effect

[SOURCE: ISO 16609:2004, 3.9]

3.6 **data at rest**

data *stored* (3.50) on stable *non-volatile storage* (3.30)

3.7 **data breach**

compromise of security that leads to the accidental or unlawful *destruction* (3.13), loss, alteration, unauthorized disclosure of, or access to protected data transmitted, *stored* (3.50), or otherwise processed

3.8 **data in motion**

data being transferred from one location to another

Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device).

3.9 **data integrity**

property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.10 **deduplication**

method of reducing *storage* (3.43) needs by eliminating redundant data, which is replaced with a pointer to the unique data copy

Note 1 to entry: Deduplication is sometimes considered a form of *compression* (3.3).

3.11 **degauss**

render data unreadable by applying a strong magnetic field to the media

3.12

destruct

sanitize (3.38) using physical techniques that make recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for *storage* (3.43) of data

Note 1 to entry: *Disintegrate* (3.15), *incinerate* (3.21), *melt* (3.25), *pulverize* (3.34), and *shred* (3.41) are destruct forms of *sanitization* (3.37).

3.13

destruction

result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible or prohibitively expensive to recover

3.14

device

mechanical, electrical, or electronic contrivance with a specific purpose

[SOURCE: ISO/IEC 14776-372:2011, 3.1.10]

3.15

disintegrate

destruct (3.12) by separating media into its component parts

3.16

Electronically Stored Information

data or information of any kind and from any source, whose temporal existence is evidenced by being *stored* (3.50) in, or on, any electronic medium

Note 1 to entry: Electronically Stored Information (ESI) includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations, and other electronic formats commonly found on a computer. ESI also includes system, application, and file-associated *metadata* (3.26) such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, *storage devices* (3.45) and *storage elements* (3.47).

3.17

Fibre Channel

serial I/O interconnect capable of supporting multiple protocols, including access to open system *storage* (3.43), access to mainframe *storage* (3.43), and networking

Note 1 to entry: Fibre Channel supports point to point, arbitrated loop, and switched topologies with a variety of copper and optical links running at speeds from 1 gigabit per second to over 10 gigabits per second.

3.18

Fibre Channel Protocol

serial Small Computer System Interface (SCSI) transport protocol used on *Fibre Channel* (3.17) interconnects

3.19

gateway

device (3.14) that converts a protocol to another protocol

3.20

in-band

communication or transmission that occurs within a previously established communication method or channel

Note 1 to entry: The communications or transmissions often take the form of a separate protocol, such as a management protocol over the same medium as the primary data protocol.

3.21

incinerate

destruct ([3.12](#)) by burning media completely to ashes

3.22

malware

malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity, or availability

Note 1 to entry: Viruses and Trojan horses are examples of malware.

[SOURCE: ISO/IEC 27033-1:2009, 3.22]

3.23

Mean Time Between Failures

expected time between consecutive failures in a system or component

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1713, modified — The term was capitalized.]

3.24

Mean Time To Repair

expected or observed duration to return a malfunctioning system or component to normal operations

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1714, modified — The term was capitalized.]

3.25

melt

destruct ([3.12](#)) by changing media from a solid to a liquid state generally by the application of heat

3.26

metadata

data that define and describe other data

[SOURCE: ISO/IEC 11179-1:2004, 3.2.16]

3.27

multi-factor authentication

authentication using two or more of the following factors:

- knowledge factor, “something an individual knows”;
- possession factor, “something an individual has”;
- biometric factor, “something an individual is or is able to do”.

[SOURCE: ISO 19092:2008, 4.42]

3.28

multi-tenancy

allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.27]

3.29

Network Attached Storage

storage device ([3.45](#)) or system that connects to a network and provide file access services to computer systems

3.30

non-volatile storage

storage ([3.43](#)) that retains its contents even after power is removed

3.31

out-of-band

communication or transmission that occurs outside of a previously established communication method or channel

3.32

over provisioning

technique used by *storage elements* (3.47) and *storage devices* (3.45) in which a subset of the available media is exposed through the interface

Note 1 to entry: *Storage media* (3.48) is used internally and independently by the *storage element* (3.47) to improve performance, endurance, or reliability.

3.33

point of encryption

location within the Information and Communications Technology (ICT) infrastructure where data are encrypted on its way to *storage* (3.43) and, conversely, where data are decrypted when accessed from *storage* (3.43)

Note 1 to entry: The point of encryption is only applicable for *data at rest* (3.6).

3.34

pulverize

destruct (3.12) by grinding media to a powder or dust

3.35

purge

sanitize (3.38) using physical techniques that make recovery infeasible using state of the art laboratory techniques, but which preserves the *storage media* (3.48) in a potentially reusable state

3.36

reliability

ability of a system or component to perform its required functions under stated conditions for a specified period of time

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.2467, modified — The second definition from ISO/IEC 9126-1:2001 and the cf. entry were not included.]

3.37

sanitization

process or method to *sanitize* (3.38)

3.38

sanitize

render access to *target data* (3.52) on *storage media* (3.48) infeasible for a given level of effort

Note 1 to entry: *Clear* (3.2), *purge* (3.35), and *destruct* (3.12) are actions that can be taken to *sanitize* (3.38) *storage media* (3.48).

3.39

secure multi-tenancy

type of *multi-tenancy* (3.28) that employs security controls to explicitly guard against *data breaches* (3.7) and provides validation of these controls for proper governance

Note 1 to entry: Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment.

Note 2 to entry: In very secure environments even the identity of the tenants is kept secret.

3.40

security strength

number associated with the amount of work that is required to break a cryptographic algorithm or system

3.41
shred

destruct (3.12) by cutting or tearing media into small particles

3.42
single point of failure

element or component of a system, a path in a system, or a system that, if it fails, the whole system or an array of systems are unable to perform their primary functions

Note 1 to entry: A single point of failure is often considered a design flaw associated with a critical element.

3.43
storage

device (3.14), function, or service supporting data entry and retrieval

3.44
Storage Area Network

network whose primary purpose is the transfer of data between computer systems and *storage devices* (3.45) and among *storage devices* (3.45)

Note 1 to entry: A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, *storage devices* (3.45), and computer systems so that data transfer is secure and robust.

3.45
storage device

any *storage element* (3.48) or aggregation of *storage elements* (3.47), designed and built primarily for the purpose of data *storage* (3.43) and delivery

3.46
storage ecosystem

complex system of interdependent components that work together to enable *storage* (3.43) services and capabilities

Note 1 to entry: The components often include *storage devices* (3.45), storage elements (3.47), storage networks, storage management, and other Information and Communications Technology (ICT) infrastructure.

3.47
storage element

component that is used to build *storage devices* (3.45) and which contributes to data *storage* (3.43) and delivery

Note 1 to entry: Common examples of a storage element include a disk or tape drive.

3.48
storage medium
storage media

material on which *Electronically Stored Information* (3.16) or digital data are or can be recorded

3.49
storage security

application of physical, technical, and administrative controls to protect storage systems and infrastructure as well as the data *stored* (3.50) within them

Note 1 to entry: Storage security is focused on protecting data (and its storage infrastructure) against unauthorized disclosure, modification, or destruction while assuring its availability to authorized users.

Note 2 to entry: These controls may be preventive, detective, corrective, deterrent, recovery, or compensatory in nature.

**3.50
store**

record data on *volatile storage* (3.53) or *non-volatile storage* (3.30)

**3.51
strong authentication**

authentication by means of cryptographically derived credentials

[SOURCE: ISO/TS 22600-1:2006, 2.23]

**3.52
target data**

information subject to a given process, typically including most or all information on a piece of *storage media* (3.48)

**3.53
volatile storage**

storage (3.43) that fails to retain its contents after power is removed

**3.54
weak key**

key that interacts with some aspect of a particular cipher's definition in such a way that it weakens the *security strength* (3.40) of the cipher

4 Symbols and abbreviated terms

ACE	Access Control Entry
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
ATA	Advanced Technology Attachment
BC	Business Continuity
BCM	Business Continuity Management
CAS	Content Addressable Storage
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining Message authentication code
CDMI	Cloud Data Management Interface
CDP	Continuous Data Protection
CHAP	Challenge Handshake Authentication Protocol
CIFS	Common Internet File System
CLI	Command Line Interface
CNA	Converged Network Adaptor
DAC	Discretionary Access Control

DAS	Direct Attached Storage
DDoS	Distributed Denial of Service
DH-CHAP	Diffie Hellman – Challenge Handshake Authentication Protocol
DES	Data Encryption Standard
DLM	Data Lifecycle Management
DMZ	De-Militarized Zone
DNS	Domain Name System
DoS	Denial of Service
DR	Disaster Recovery
DRP	Disaster Recovery Planning
EHR	Electronic Healthcare Record
ESI	Electronically Stored Information
ESP	Encapsulating Security Payload
FC	Fibre Channel
FC-SP	Fibre Channel – Security Protocol
FCAP	Fibre Channel Certificate Authentication Protocol
FCEAP	Fibre Channel Extensible Authentication Protocol
FCIP	Fibre Channel over TCP/IP
FCoE	Fibre Channel over Ethernet
FCP	Fibre Channel Protocol
FCPAP	Fibre Channel Password Authentication Protocol
FCS	Fixed Content Storage
FDE	Full Disk Encryption
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HAMR	Heat Assisted Magnetic Recording
HBA	Host Bus Adapter
HDD	Hard Disk Drive
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
ID	Identifier

IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
ILM	Information Lifecycle Management
I/O	Input/Output
IP	Internet Protocol
IPS	Intrusion Prevention System
IPOCM	Incident Preparedness and Operational Continuity Management
IPsec	Internet Protocol Security
IRBC	ICT Readiness for Business Continuity
iSCSI	Internet Small Computer Systems Interface
ISL	Inter-Switch Link
ISMS	Information Security Management System
iSNS	Internet Storage Name Service
KEK	Key Encryption Key
KMIP	Key Management Interoperability Protocol
LAN	Local Area Network
LBA	Logical Block Address
LDAP	Lightweight Directory Access Protocol
LUN	Logical UNit
MAC	Mandatory Access Control
MD5	Message-Digest algorithm 5
MEK	Media Encryption Key
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card

NIS	Network Information Service
NPIV	N_Port_ID Virtualization
NTLM	NT LAN Manager
NTP	Network Time Protocol
NVM	Non-Volatile Memory
OASIS	Organization for the Advancement of Structured Information Standards
OID	Object Identifier
OSD	Object-based Storage Device
PCIe	Peripheral Component Interconnect express
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
pNFS	parallel Network File System
PRNG	Pseudo-Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RBAC	Role-Based Access Control
REST	REpresentational State Transfer
RNG	Random Number Generator
ROM	Read-Only Memory
RPC	Remote Procedure Call
SAN	Storage Area Network
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLP	Service Locator Protocol
SMB	Server Message Block
SMI-S	Storage Management Initiative – Specification
SNIA	Storage Networking Industry Association

SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SSC	Security Subsystem Class
SSD	Solid State Drive
SSH	Secure SHell
SSHD	Solid State Hard Drive
SSO	Single Sign-On
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VSAN	Virtual Storage Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WORM	Write Once Read Many
WWN	World Wide Name
WWPN	World Wide Port Name
XEX	Xor-Encrypt-Xor
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing

5 Overview and concepts

5.1 General

Computer data storage or information storage, often called storage, refers to computer components, storage elements, storage devices, and storage media that retain Electronically Stored Information (ESI) or digital data. While both volatile and non-volatile forms of storage exist, this International Standards is concerned primarily with non-volatile storage. Storage is a core function and fundamental component of computers.

To secure storage infrastructure, a clear understanding of the storage technologies and concepts are necessary. In addition, the types of security controls and insight into how they impact and interact with the storage technologies are also important. Finally, the threats to this infrastructure and the major risks arising from these threats are factored into any efforts to secure storage infrastructure or individual storage systems.

5.2 Storage concepts

In the past, storage was simply seen as Hard Disk Drives (HDD) and tape drives attached to a computer to store data. This approach, commonly called Direct Attached Storage (DAS), is still in use within enterprise data centres as well as Small Office/Home Office (SOHO) environments. Alternate approaches based on the use of networking technology for storage have emerged as highly sophisticated technologies became available to provide solutions for managing, connecting, protecting, securing, sharing, and optimizing the storage of data. These solutions become more feasible and cost effective as storage technology evolved from non-intelligent internal and external DAS to intelligent networked storage. The use of networking in these solutions increases the attack surface of these solutions and requires additional attention be paid to their security.

Contemporary storage solutions include some or all of the following elements:

- storage arrays with storage network interfaces;
- Network Attached Storage (NAS);
- Content Addressable Storage (CAS);
- Object-based Storage Devices (OSD);
- backup/recovery systems, Continuous Data Protection (CDP), etc. (i.e., data protection systems).

Storage has become a prominent and independent layer of Information and Communications Technology (ICT) infrastructure in enterprise class and midrange computing environments. The requirements for these environments frequently exceed simple data storage capabilities. Examples of applications and functions driving the emergence of new storage technology include:

- sharing of vast storage resources (measured in petabytes and exabytes) between multiple systems via networks;
- backups that don't require use of a Local Area Network (LAN);
- remote, disaster tolerant, on-line mirroring of mission critical data;
- clustering of fault tolerant applications and related systems around a single copy of data;
- long-term retention of sensitive or high-value business information;
- distributed database and file systems;
- support for regulatory and legal compliance requirements;
- support for centralized data repositories for rapid recovery (e.g., backups) and archiving.

5.3 Introduction to storage security

Storage security is concerned with the physical, technical and administrative controls as well as the preventive, detective and corrective controls associated with storage systems and infrastructure as outlined in [5.2](#). Storage security can also force the introduction of specialized technologies such as:

- media sanitization;
- virtualization security;
- self-encrypting storage devices (see [C.3](#)) like HDD, Solid State Drives (SSD), and Solid State Hard Drive (SSHD);
- key management services;
- data authenticity and integrity services;

- data in motion protections (encryption and data reduction);
- directory services and other user management systems.

To better understand the security issues and implications for storage, one should know both how and why the storage technologies are used. As a starting point, consider the following:

- The storage systems can function as nodes within storage networks, which can be based on, but not limited to technologies like Transmission Control Protocol/Internet Protocol (TCP/IP), Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), and InfiniBand. The potential threats can vary significantly based on the networking technology as well as the topologies used.
- When stored, the data is typically represented and accessed as either block data or as files/objects; there are significant differences between these two types of storage methods. Likewise, the security measures associated with each can have radical differences, especially with access controls, encryption, and data integrity.
- As part of normal storage operations, many storage device types have more internal media capability than is exposed through the interface. SSDs and SSHDs often are typically over provisioned, where data may be moved internally between physical media areas to improve write latencies. HDDs often contain spare areas where data may be moved internally between physical media areas when there is a temporary access problem. User data may remain on such areas even after the device is written through its interface. Such devices may not be cleared by overwrites through the interface.
- Storage management is both an element of the storage infrastructure as well as an operation performed on many of the systems. It is common to have privileged users applying configuration changes, provisioning storage, tuning, monitoring, etc. this infrastructure. Some of the management can be performed remotely as well as involve third parties such as vendor support personnel.
- Data availability and integrity are key factors in an organization's storage architecture, so it is important for security to be complementary rather than a trade-off and that it not negate high-availability measures by introducing choke-points and additional single points of failure.
- Many organizations implement elaborate data resiliency strategies, which are integral to their Disaster Recovery (DR) and Business Continuity (BC) plans. Security mechanisms like data at rest encryption have to be implemented carefully to ensure that resiliency strategies are not impacted.
- Virtualization within storage can take many forms and be implemented at different points within the storage infrastructure. This virtualization can mask the physical details associated with the presentation of storage (e.g., a Logical Unit or filesystem to a server), mask the true capacity of a device, perform policy-driven autonomous data movement (like tiered storage), or completely abstract the storage infrastructure (like cloud computing storage). Balancing the security and virtualization so they can coexist requires careful planning and selection of the right technologies.
- Data growth rates in some organizations are driving increased use of data storage technologies. As an alternative to acquiring additional storage, organizations are employing data reduction technologies such as compression and deduplication. However, these data reduction technologies can be impacted by data at rest encryption mechanisms, and they in turn, can introduce data integrity problems during DR and BC operations.
- As part of the normal data protection strategy, many copies of data end up getting created (e.g., replicated between systems and sites, backups, snapshots, etc.). These copies need to be protected appropriately while they are in use, and then properly sanitized when their usefulness has ended.
- Sensitive and high-value data often need to be protected when transmitted between systems, using mechanisms like the Internet Protocol Security (IPsec). IPsec can have detrimental impacts to the use of certain technologies like Network Address Translation (NAT), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), or other systems that look deeper into network traffic frames. Whether to rely on IPsec or other in motion protection protocols can hinge on the trade-offs of potentially neutralizing the value of other technologies or where in the network it is to be deployed.

- Many organizations are implementing data at rest encryption to protect sensitive and high-value data. The specific cryptographic mechanisms and the point of encryption are important factors in the actual data protection as well as meeting compliance requirements.
- Successful use of encryption is often predicated on proper management of keying material throughout its lifecycle. This includes correct generation of keys, secure storage and transmittal of key material, replicating keys as part of the normal strategy to ensure availability of the data, and proper disposal of the keying material when it is no longer needed. The sensitivity and importance of the data to be protected may also factor into the key management approach.

Ensuring adequate confidentiality, integrity, and availability of data stored and accessed on current and emerging storage technologies requires a concerted effort within this layer of ICT. Many of these security efforts will focus on:

- protecting storage management (operations and interfaces);
- ensuring adequate credential and trust management;
- protecting data backup and recovery resources;
- data in motion protection;
- data at rest protection;
- data availability protection;
- Disaster Recovery and Business Continuity support;
- proper sanitization and disposal;
- secure autonomous data movement;
- secure multi-tenancy.

5.4 Storage security risks

5.4.1 Background

Storage security risk is created by an organization's use of specific storage systems or infrastructures. Storage security risk arises from:

- a) threats targeting the information handled by the storage systems and infrastructure;
- b) vulnerabilities (both technical and non-technical); and
- c) impact of successful exploitation of vulnerabilities by threats.

Risk management is a key concept in information security. According to ISO/IEC 27005, "the information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. Business Continuity planning)." The information security risk management process presented in ISO/IEC 27005 consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.

Threats for storage systems and infrastructure include, but are not limited to:

- unauthorized usage;
- unauthorized access;
- liability due to regulatory non-compliance;
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on storage;

- corruption/modification and destruction of data;
- data leakage/breaches;
- theft or accidental loss of media;
- malware attack or introduction;
- improper treatment or sanitization after end-of-use.

These threats can give rise to a wide assortment of risks. However, for storage systems and infrastructure the risks associated with data breaches, data corruption or destruction, temporary or permanent loss of access/availability, and failure to meet statutory, regulatory, or legal requirements are the major concerns.

5.4.2 Data breaches

A data breach can be one of the results of a security compromise and it can take many forms. Unauthorized access or disclosure of protected information are two commonly recognized forms of data breaches, but it is important to understand that lesser known forms can include accidental or unlawful destruction, loss, or alteration of data.

Depending on the volume and type of information involved (e.g., personally identifiable information, protected health information, etc.) and the applicable laws and regulations, a data breach can expose the organization to significant risk arising from costs involved in investigating the data breach, making requisite notifications to affected individuals, litigation expenses, regulatory fines and other legal penalties as well as brand damage accruing from the public disclosure of the data breach.

There are economic and security risks to the entity that has lost their or others' secured information, in that the loss of the information could include things such as:

- secrets or confidential information (e.g., passwords, encryption keys, etc.);
- intellectual property or other sensitive business information;
- Personally Identifiable Information (PII);
- financial account or record information;
- personally identifiable health record information.

Untrusted or unauthorized entities seeking this leaked or spilled information can be of a broad range of sources, be well funded and have diverse motivations.

[Table 1](#) summarizes the storage-based security threats that are more likely to occur and lists the forms of data breaches that can result from these compromises.

Table 1 — Storage-oriented data breaches

Security threats	Potential forms of data breach
Theft of storage element or media	Unlawful access, unlawful disclosure, unlawful data loss, unlawful data destruction
Loss of storage element or media	Unauthorized access, unauthorized disclosure, accidental data loss, accidental data destruction
Loss of data	Unlawful, unauthorized, or accidental data destruction or corruption
Accidental configuration changes (e.g., storage management, storage/network resources, incorrect patch management, etc.) by authorized personnel	Accidental access, accidental disclosure, accidental data destruction, accidental data alteration

Table 1 (continued)

Security threats	Potential forms of data breach
Malicious configuration changes (storage management, storage/network resources, application tampering, etc.) by external or internal adversaries	Unlawful access, unlawful disclosure, unlawful data destruction, unlawful data alteration
Privileged user abuses by authorized users (e.g., inappropriate data snooping)	Unlawful/unauthorized access or disclosure
Malicious data tampering by external or internal adversaries	Unlawful data destruction or alteration
Denial of service attacks	Unauthorized data destruction, loss, or alteration
Malicious monitoring of network traffic	Unlawful/unauthorized disclosure

5.4.3 Data corruption or destruction

Data corruption is the deterioration or damage of computer data (i.e., unintended changes to the original data) caused by human, hardware and software error. It can occur during writing, reading, storage, transmission, or processing. Data corruption may only affect a small, but important, portion of data or metadata that can allow for recovery under the right conditions; it could also result in permanent data loss if the root cause is allowed to persist. Data destruction on the other hand results in data loss, which can be permanent if data protection mechanisms like backups have not been employed. Both data corruption and destruction can be the result of unintentional or intentional events, and in the latter case, they can be further categorized as malicious or non-malicious.

Events such as fire, flood, power outages, programming bugs and user errors are all examples of general, unintentional sources of data corruption and destruction. Background radiation, head crashes, and aging or wear of the storage hardware are additional sources of problems that are more storage centric. Hardware-based data corruption can generally be detected by the use of checksums, and can often be corrected by the use of error correcting codes, but these “silent corrections” can lead to other problems if storage is not managed well (i.e., temporary correctable errors can turn into permanent ones as the storage device or media deteriorates).

Intentional attacks/events of a malicious nature can be perpetrated by external parties or insiders with the purpose of making some or all of the affected data unusable or destroyed. In this context, unusable could mean that unauthorized modifications have been applied, modifications are suspected, or the data can be encrypted with an unknown key or mechanism. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as “getting the job done,” but the impact on the data can be as devastating as malicious attacks.

Employing appropriate mechanisms to detect and remedy data corruption is an important way of maintaining data integrity. Likewise, detecting data loss and recovering this data using data protection mechanisms can guard against the total loss of data.

5.4.4 Temporary or permanent loss of access/availability

Availability is concerned with assuring that there is no or limited denial of authorized access¹⁾ to storage elements, storage network elements, stored information, information flows, services, and applications. In general, data availability is achieved through redundancy of where the data is stored and how it can be reached.

Loss of availability can often be attributed to a problem with one or more of the following:

- reliability;
- accessibility;

1) Within this context, “limited denial of authorized access” means that data continues to be available at a required level of performance within a specified timeframe.

- timeliness.

5.4.5 Failure to meet statutory, regulatory, or legal requirements

Organizations can incur significant liabilities and penalties for non-compliance with statutory, regulatory, or legal requirements. Requirements can vary significantly in different jurisdictions, and for multi-national organizations, country specific legislation has a greater influence on information security requirements.

Common compliance issues include:

- breach of country specific privacy requirements;
- unlawful transfer of data (i.e., moving restricted data out of particular jurisdiction);
- breach of confidentiality;
- non-conformance with an organization's policies (e.g., sanitization);
- inadequate data retention and protection;
- insufficient evidence of security (e.g., audit logs, proof of encryption/sanitization, etc.).

These non-compliance issues can result in costly sanctions and remediation (e.g., breach notifications).

6 Supporting controls

6.1 General

[Clause 6](#) provides the controls that *support* storage security technical architectures, their related technical controls, and other controls (technical and non-technical) that are applicable not just to storage. Information on many of these types of controls can be found in ISO/IEC 27002. The controls that are especially important with regard to the use of storage are expanded upon in clauses [6.2](#) to [6.8](#) below. They address securing direct attached storage, storage networks, the management of storage network security, technical controls for different types of storage (block, file, and object-based storage), and storage security services. Data sensitivity, criticality, and value can also be an important consideration in selecting and using controls, so [Annex B](#) and specifically [B.1.2](#) should also be consulted.

6.2 Direct Attached Storage (DAS)

A DAS device is a storage element (e.g., HDD, tape, etc.) that is directly connected to a computer without a storage network in between (i.e., no network device like a hub, router, or switch between the two). DAS devices can take the form of internal storage (i.e., an integral part of the computer system) or external storage (i.e., auxiliary storage). In addition, they are typically dedicated to the system to which they are attached; a DAS device can be shared between multiple computers, as long as it provides multiple interfaces (ports) that allow concurrent and direct access.

These storage elements have limited data access and management interfaces (the latter is usually in-band). As such, the options for securing DAS tend to be limited and include:

- DAS tends to be small in physically size and may be located in office environment where they can be subjected to malicious attacks (e.g., stolen, destruction, unauthorized access, etc.), so DAS should be physically secured.
- To avoid unauthorized access of sensitive and high value data on DAS, some form of encryption should be used to protect the data at rest, including:
 - Storage elements with integrated encryption and access control capabilities, also known as Self-Encrypting Drives (SEDs);

- Computer-based or application-based encryption, including Full Disk Encryption (FDE).
- Media sanitization (see [6.8.1.2](#) and [Annex A](#) for additional information) should be used on all DAS involved with sensitive or high value data with either of the following:
 - Use the integrated sanitization functionality in the storage elements;
 - Use computer-based or application-based sanitization.
- If possible, authentication such as Fibre Channel – Security Protocol – 2²⁾ (FC-SP-2) AUTH-A Authentication (see [C.7.2](#)) should be used to prevent unauthorized access to sensitive and high value data;
- To guard against accidental or intentional data loss or corruption, backups of the DAS contents should be made on a regular basis.

6.3 Storage networking

6.3.1 Background

With the possible exception of DAS, networking plays an important role in storage infrastructures and these networks can include common networking technologies (e.g., LAN and WAN), storage-specific network protocols that use those technologies, as well as storage-specific technologies (e.g., Fibre Channel). In the case of the former, the security guidance offered in ISO/IEC 27033 is instrumental in protecting storage resources that utilize these technologies. The storage-specific network protocols and technologies are addressed in this International Standard.

Storage systems use networking for three primary purposes: 1) storage and retrieval of data, 2) protection of data, and 3) management of storage systems. None of the uses mandate a particular networking technology or approach. For example, some storage management can be performed over the same Fibre Channel interface (i.e., in-band) used by a server to access data and simultaneously over a TCP/IP connection to the management interface of the storage system.

6.3.2 Storage Area Networks (SAN)

6.3.2.1 General

A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of servers, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. SANs can also span multiple sites.

SANs are often used to improve application availability (e.g., multiple data paths), enhance application performance (e.g., off-load storage functions, use separate networks, etc.), increase storage utilization and effectiveness (e.g., consolidate storage resources, tiered storage, etc.), and improve data protection and security. In addition, SANs typically play an important role in an organization's DR and BC activities (see [Figure 1](#)).

2) FC-SP-2 is specified in ANSI INCITS 496-2012, *Information Technology - Fibre Channel - Security Protocols - 2 (FC-SP-2)*

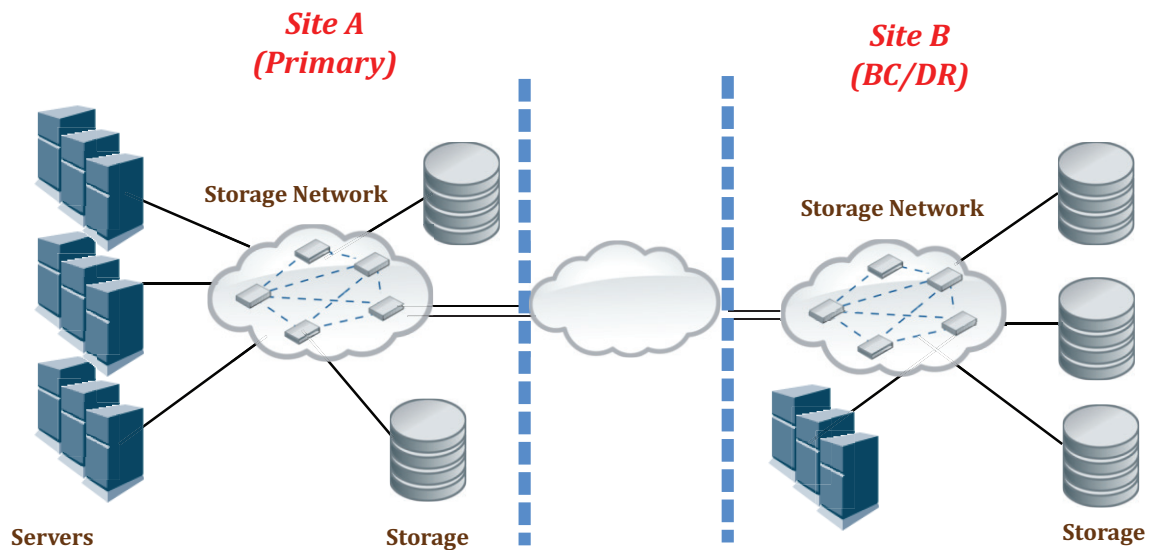


Figure 1 — Storage Area Network (SAN) example

A SAN presents storage devices (such as disk arrays and tape libraries) to a server operating system such that to the server, the storage appears to be locally attached. This simplified presentation of storage to a server is accomplished through the use of different types of virtualization.

SANs are commonly based on Fibre Channel (FC) technology that utilizes the Fibre Channel Protocol (FCP) for open systems and proprietary variants for mainframes. In addition, the use of Fibre Channel over Ethernet (FCoE) makes it possible to move FC traffic across existing high-speed Ethernet infrastructure and converges storage and IP protocols onto a single cable transport and interface. Other technologies like Internet Small Computing System Interface (iSCSI), commonly used in small and medium sized organization as a less expensive alternative to FC, and InfiniBand, commonly used in high performance computing environments, can also be used. Interconnects like Serial Attached SCSI (SAS) and Peripheral Component Interconnect express (PCIe) that leverage extenders and switches are beginning to take on characteristics of a SAN as well.³⁾ In addition, it is possible to move data between different SAN technologies through the use of gateways (see [Figure 2](#)).

Security controls relevant to a SAN are grouped into the following categories:

- **Access Control:** Access control on a SAN is implemented through application of zoning, Logical Unit (LUN) masking, and port binding mechanisms:
 - **Port Binding:** Globally unique identifiers known as World Wide Names (WWN) are used for identification in a SAN. Port binding is a SAN security mechanism that associates a physical port ID and the WWN of the connected device. This association can mitigate snooping attempts by a potential adversary and should be used when possible.
 - **Zoning:** A SAN fabric can be segmented into separate zones to restrict the visibility of portions of a SAN to specific servers and storage devices. Soft zoning is based on limiting SAN fabric nameserver responses to queries based on the assumption that servers will not contact storage devices that are not discovered via the nameserver. Hard zoning uses physical port numbers on SAN switches to restrict traffic forwarding and is a more secure zoning method because it does not rely on correct server behaviour and in particular is not vulnerable to spoofing of server identity.

³⁾ This International Standard does not provide guidance specific to InfiniBand, SAS, or PCIe, but the general guidance is applicable.

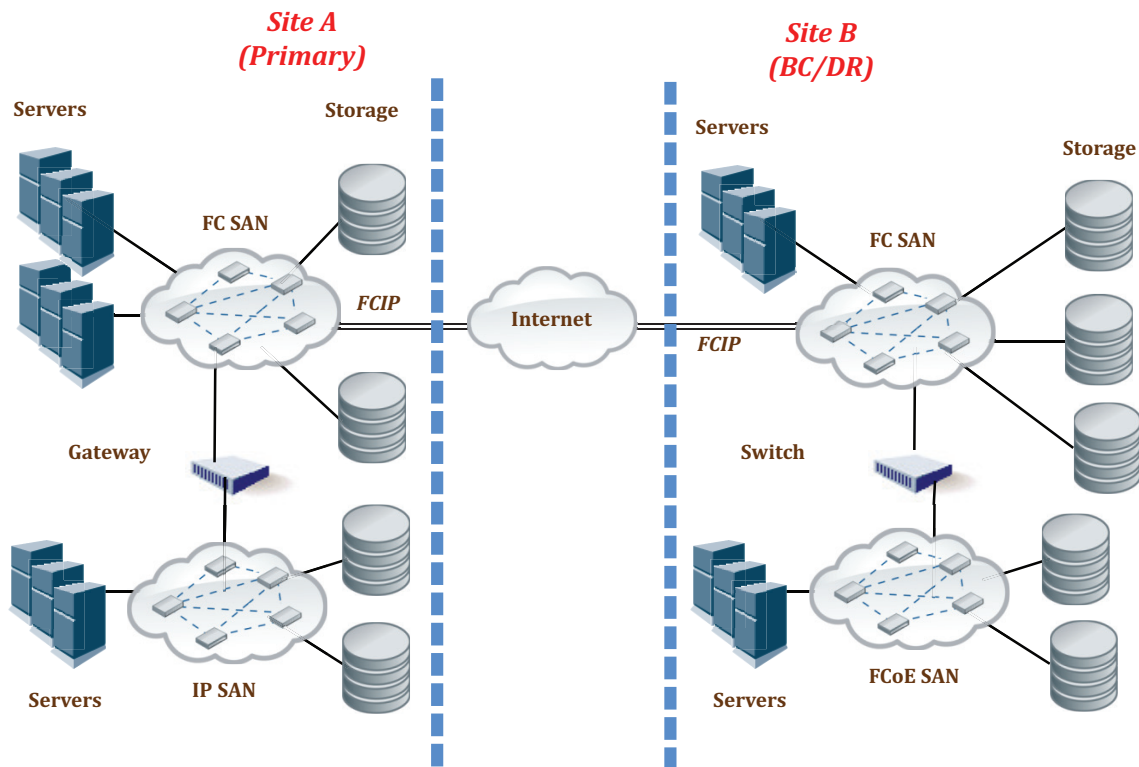


Figure 2 — Storage Area Network (SAN) example

- **LUN masking and mapping:** A storage device can be divided into different logical units (LUNs) that are identified by logical unit numbers. LUN mapping refers to the assignment of a number to a LUN, and it typically takes place in a storage array, but it can also occur as part of a redirection (initial address to a new address) in the switch, Host Bus Adapter (HBA) or Converged Network Adaptors (CNA), and virtualization layer. LUN masking refers to making a LUN visible to some servers and not visible to others.
- **Authentication:** For SANs it is important for a switch to verify the identity of other switches in the SAN with whom it communicates. If switch authentication is not implemented a rogue switch could join a SAN and potentially compromise SAN data. Likewise, the nodes in a SAN (e.g., storage devices and servers) need to employ authentication to guard against data breaches.
- **Encryption:** There are two major components of data confidentiality on a SAN: 1) data in motion and 2) data at rest. Sensitive and high-value data needs to be cryptographically protected in SANs when it is in motion as well as when it is at rest on a storage device. This can require the use of special purpose hardware that can encrypt the data that is being sent to a storage device. Refer to [6.8.2.2](#) for additional guidance on protection of data in motion and [6.8.2.3](#) for guidance on protection of data at rest.

A defence in depth strategy (see [7.2.1](#)) helps to mitigate the risk associated with failure of one security control (possible single point of failure) compromising the assets under protection.

Physical and logical isolation of storage elements within a SAN can also play an important role, and can take the form of:

- Physical isolation including:
 - segregate production from other system classes (e.g., Quality Assurance, Development);
 - where possible, avoid network connections between classes (e.g., a production server connected to both the production and development networks);
 - segregate networks and storage by class where appropriate;
 - physically separate systems in each class.
- isolate storage devices from other data centre devices, if practical.
- Logical isolation including:
 - segregate storage traffic from normal server traffic using:
 - available network controls to create independent logical domains on common physical infrastructure;
 - trust and access controls to manage membership in the logical domains.
 - segregate storage management traffic from all other traffic;
 - ensure that configurations of network gateways maintain appropriate network segregation.

6.3.2.2 Fibre Channel SAN

Fibre Channel is a multi-gigabit-speed network technology used for block-based storage. There are three major Fibre Channel topologies, describing how a number of ports are connected together: point-to-point (two devices are directly connected), arbitrated loop, and switched fabric. Switched fabric topologies along with the Fibre Channel Protocol (FCP), which is the interface protocol used to transmit SCSI traffic on this network technology, are the more interesting from a security perspective.

Fabric administrators should take steps to:

- Control FCP node access including:
 - restrict server access on the switches using techniques such as Access Control Lists (ACLs), binding lists, and FC-SP-2 fabric policies (see [C.7.1](#));
 - use NPIV (N_Port_ID Virtualization) enabled HBAs to assign individual N_Port_IDs to virtual servers.
- Implement switch-based controls including:
 - restrict switch interconnections using techniques such as ACLs, binding lists, and FC-SP-2 fabric policies (see [C.7.1](#));
 - zoning should be used in FC SAN fabrics with a preference for hard zoning;
 - determine whether basic zoning is a strong enough security measure for the target environment, and if it is not, use stronger techniques like FC-SP Zoning (see [C.7.5](#)) where supported by the vendor;
 - disable unused ports;
 - carefully use default zones and zone sets (assume a least privilege posture).
- Interconnect storage networks securely by configuring switches, extenders, routers, and gateways necessary to meet requirements.

Subclause [6.5.1](#) provides guidance on block-based Fibre Channel storage.

6.3.2.3 IP SAN

Internet SCSI (iSCSI), described in IETF RFC 3720, is a connection-oriented command/response protocol that runs over TCP, and it is used to access disk, tape and other devices.

Control iSCSI network access and protocols by:

- avoiding connecting iSCSI interfaces to general purpose LANs; segregate for security and performance;
- using Virtual Local Area Networks (VLANs) when the use of physically isolated LANs is not an option.

Fibre Channel over TCP/IP (FCIP), defined in IETF RFC 3821, is a pure Fibre Channel encapsulation protocol. It allows the interconnection of islands of Fibre Channel Storage Area Networks through IP-based networks to form a unified Storage Area Network.

FCIP network access and protocols controls should be controlled by:

- setting up the peer-to-peer relationship between FCIP entities, recognizing that the security policies will be applied uniformly;
- using a private IP network exclusively by the FCIP entities whenever possible.

Implement IPsec security measures in conjunction with FCIP by:

- performing cryptographic authentication and data integrity at a minimum;
- protecting sensitive data by appropriate confidentiality measures.

IETF RFC 3723, *Securing Block Storage Protocols over IP* provides additional useful information on both iSCSI and FCIP. Subclause [6.5.2](#) provides guidance on block-based IP storage. In addition, IETF RFC 7146, *Securing Block Storage Protocols over IP: RFC 3723 Requirements Update for IPsec v3* provides important security updates to IETF RFCs 3720, 3723, and 3821.

6.3.2.4 FCoE SAN

Fibre Channel over Ethernet (FCoE) is a protocol specification⁴⁾ to encapsulate Fibre Channel frames in Ethernet packets. The Ethernet network that supports FCoE is required to be a lossless Ethernet network,⁵⁾ with switching devices that have internal architectures designed to offer a no-drop packet capability and network flow control mechanisms to enable lossless transmission of packets across the Ethernet infrastructure.

FCoE SANs should be protected by:

- leveraging the Fibre Channel security mechanisms (see [C.7](#));
- protecting against Ethernet broadcast storms (e.g., allocation of adequate input buffering) that can cause throughput and timeout issues;
- using ACLs to control network access (e.g., denying specific computers from unnecessary or unwanted traffic);
- using FCoE VLANs when the use of physically isolated LANs is not an option.

4) FCoE is specified in ANSI INCITS 462-2010, *Information Technology - Fibre Channel - Backbone - 5 (FC-BB-5)*

5) These networks are full duplex, IEEE 802.3 networks that support 802.3x PAUSE and Jumbo frames to encapsulate the 2 kilobyte FC frames.

6.3.3 Network Attached Storage (NAS)

6.3.3.1 General

Network Attached Storage (NAS) is a data storage technology that provides file-level access to heterogeneous clients over a network. NAS enables a file system physically residing on one server or device to be accessed by remote client computers, appearing to users as a local file system. NAS systems are typically designed and build specifically for NAS purposes, but general purpose server computers can also be used.

NAS systems can be implemented as individual storage servers or as a clustered collection of storage servers that dynamically distributes client connections by slicing or striping data and metadata across the clustered storage servers (see [Figure 3](#)); parallel NFS (pNFS) systems are examples of clustered NAS systems.

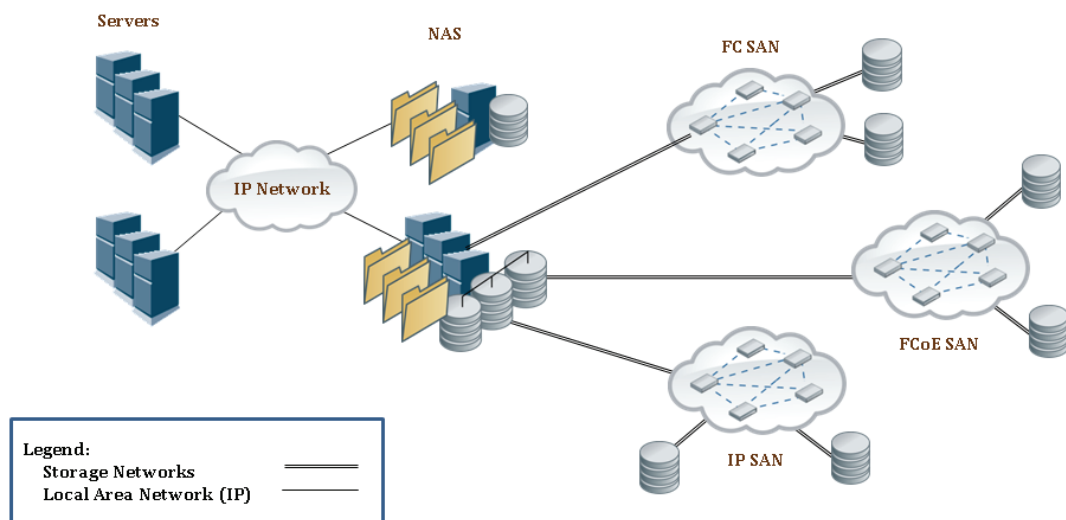


Figure 3 — Network Attached Storage (NAS) Example

Common file system implementations include the Network File System (NFS) and Server Message Block (SMB)/ Common Internet File System (CIFS), but other technologies like Object-based Storage Device (OSD) and cloud computing storage exist as well.

Security controls relevant to NAS are grouped into the following categories:

- authorization controls, such as ACLs, that restrict users' access to file and folder resources provided by the NAS device;
- encryption of data, both in motion and at rest; and
- authentication controls, such as Kerberos, for verifying the identity of users attempting to access NAS data.

Refer to [6.6](#) for further implementation guidance on NAS and file-based storage.

6.3.3.2 Network File System (NFS)

NFS is a client/server application, communicating with a Remote Procedure Call (RPC)-based protocol. Multiple versions of NFS are specified and in use, including NFS version 3 (specified in IETF RFC 1813), NFS version 4 (specified in IETF RFC 3530), and NFS version 4.1 (specified in IETF RFC 5661). From a security perspective, NFS version 3 (NFSv3) is considered less secure and extra care should be exercised when it is used with sensitive or high-value data.

The following networking guidance is applicable to NFS-based NAS and should be used:

- control NFS network access and protocols by:
 - enabling NFS only if needed. This will eliminate it as a possible attack vector available to an intruder;
 - using NFSv4 (or later versions) whenever possible and limit NFSv3 usage;
 - filtering client and management access by IP address for additional security.
- encrypt client data access (e.g., IPsec) when necessary.

6.3.3.3 SMB/CIFS

Server Message Block (SMB) 3.0—the successor to CIFS (Common Internet File System), itself the successor to SMB 1.0—is a protocol intended to provide an open cross-platform mechanism for client systems to request file services from server systems over a network. It is based on the standard SMB protocol widely in use by personal computers and workstations running a wide variety of operating systems.

The following networking guidance is applicable to SMB/CIFS-based NAS and should be used:

- use later versions of the SMB protocol;
- turn off low-security session negotiation protocols, such as NT LAN Manager (NTLM) v1, LanMan and plaintext, and use NTLM v2 or Kerberos instead;
- maintain up-to-date patch levels;
- use SMB signing;
- maintain Active Directory (AD) services securely;
- use one-way trusts, from leaf domains to parent domains, when possible;
- control SMB/CIFS network access and protocols by:
 - enabling SMB/CIFS only if needed. This will eliminate it as a possible attack vector available to an intruder;
 - encrypting client data access when necessary.

6.4 Storage management

6.4.1 Background

Storage networks and infrastructure elements are complex architectures that can impose stringent management demands on administrators. To address these demands, organizations implement storage infrastructure management tools and processes to ensure availability and performance of all storage elements, greater data protection and security, centralized auditing, and meeting compliance requirements (see [Figure 4](#)).

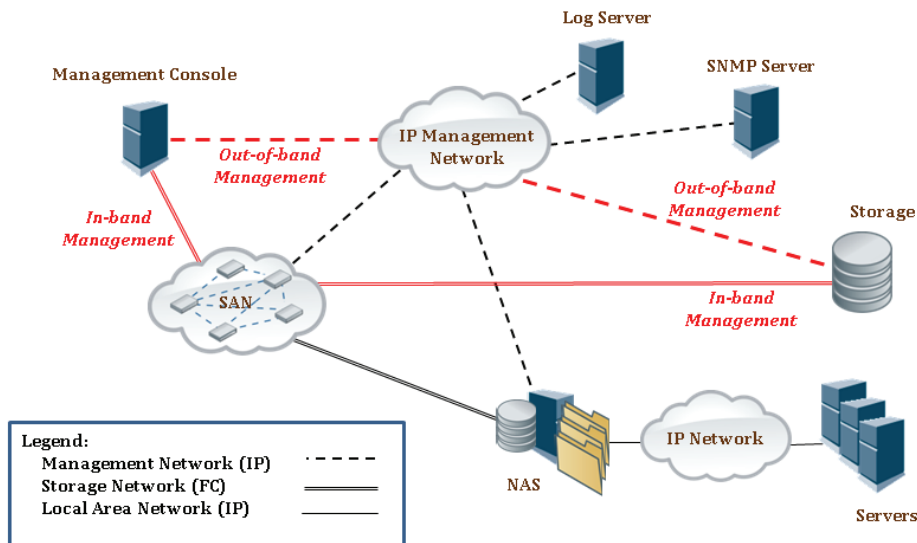


Figure 4 — Storage Management Example

Like the network management description in ISO/IEC 27033-2, storage management also refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, provisioning and sanitization of storage systems.

- Operation deals with keeping the storage (and the services that the storage infrastructure provides) up and running smoothly. It includes monitoring the storage to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the storage infrastructure and how they are assigned. It includes all the “housekeeping” that is necessary to keep the storage under control.
- Maintenance is concerned with performing repairs and upgrades - for example, when equipment has to be replaced, when a storage array needs a microcode update, or when a new switch is added to a storage network. Maintenance also involves corrective and preventive measures to make the storage run “better,” such as adjusting device configuration parameters.
- Provisioning deals with initializing and equipping a system to prepare it to provide services.
- Sanitization deals with preserving the confidentiality of information remaining on media when it is removed from service or re-purposed by rendering the data unreadable (e.g., by overwriting it with random data, destroying the encryption keys for encrypted data or physically destroying the device).

Performing these storage management activities securely, requires controls associated with authentication and authorization (6.4.2), protecting the storage management interfaces (6.4.3), maintaining accountability and traceability of systems and users (6.4.4), and ensuring the underlying systems used for storage management are adequately hardened (6.4.5). Guidance for each of these topics is provided in the subclauses within this clause 6.4.

6.4.2 Authentication and authorization

6.4.2.1 Authentication

The individuals managing storage systems and infrastructure are generally privileged users. According to ISO/IEC 27002:2013, 9.2.3 the allocation and use of privileged access rights should be restricted and controlled. Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems. To help mitigate these threats, secure log-on procedures as described in ISO/IEC 27002:2013, 9.4.2 with additional authentication measures (see [C.1](#)) may be necessary, including but not limited to:

- all users should have a unique identifier (user ID) for their personal use only;
- a suitable authentication technique should be chosen to substantiate the claimed identity of a user by using:
 - strong passwords (increased minimum number of characters, increased complexity, etc.) with a reduced period of use;
 - strong authentication (e.g., a challenge response protocol); or
 - multi-factor authentication, such as biometric data (e.g. finger-print verification, signature verification) and use of hardware tokens (e.g., smart cards).
- for all remote access, use strong authentication or multi-factor authentication along with secure channels;
- when possible, use a centralized authentication solution (e.g., Remote Authentication Dial In User Service or RADIUS, Single Sign-on or SSO, etc.) for improved monitoring and control;
- use multi-factor authentication when managing sensitive and high-value data;
- disable login to the root account. Remotely log all privilege escalation operations.

In addition to user authentication, storage systems sometimes employ entity authentication, which is the process by which an agent in a distributed system gains confidence in the identity of a communication partner. This entity authentication can take place in Transport Layer Security (TLS) and IPsec connections as well as within storage protocols (e.g., Challenge Handshake Authentication Protocol with iSCSI, Diffie-Hellman Challenge Handshake Authentication Protocol within FCP, etc.). When possible, these entity authentication mechanisms should be used. Additional guidance is provided in the sections that address these mechanisms.

6.4.2.2 Authorization and access control

Within market sectors like financial services and healthcare there are trends to align authorization and access control (see [C.2](#)) to a least-privilege model that leverages specific roles. The following roles should be implemented and used within storage technologies:

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

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

Each storage management transaction should be associated with a “security” or “storage” role. These roles can be important controls to ensure separation of duties with respect to management capabilities.

6.4.3 Secure the management interfaces

Protecting the management interfaces from unauthorized access and reconnaissance is of paramount importance. Unauthorized access to management interfaces, occurring due to failure to implement appropriate controls, could result in data destruction, corruption, and denial of access.

Management interfaces for storage systems can take on several physical forms including serial ports (e.g., RS-232, DB9, DB25, etc.), local area networks, modems, and even the technologies used for the data path (e.g., Fibre Channel). Hybrid interfaces (e.g., serial ports plugged into a console concentrator that provides an interface on a LAN) are also relatively common. To protect these physical interfaces organization should:

- restrict physical access to management interfaces;
- disable and disconnect serial management ports when not in use;
- segregate LAN interfaces used for management from other LAN traffic, noting that physical isolation is preferred, but logical isolation (such as VLANs) should be used at a minimum.

In addition to the physical interfaces, storage systems employ a variety of software and firmware to enable management of storage system. These software interfaces can include simple Command Line Interfaces (CLI), Web-based Graphical User Interfaces (GUI), support for the Simple Network Management Protocol (SNMP), and server-based proxies that handle in-band management (i.e., over the data path). To secure these software/firmware interfaces, organizations should:

- use firewalls and TCP wrappers to restrict access to management networks to authorized systems and protocols;
- use entity authentication to establish trust relationships between storage systems and the management systems (e.g., using FC-SP-2 AUTH-A to authenticate the entities performing in-band management as described in [C.7.1](#));
- leverage IDS and IPS mechanisms to identify anomalous behaviours and guard against them;
- use ICT infrastructure (Domain Name System or DNS, Service Locator Protocol or SLP, Network Time Protocol or NTP) with appropriate security controls to avoid indirect attacks;
- employ appropriate privileged user controls, including authentication (see [6.4.2.1](#)), authorization (see [6.4.2.2](#)), and secure auditing/monitoring (see [6.4.4](#));
- ensure that operating systems and applications are current and sufficiently hardened against attacks (see [6.4.5](#)).

When storage systems are managed remotely, the following additional security measures should be used:

- use secure channels for all remote access (Virtual Private Network or VPN, TLS, Secure Shell or SSH, Hypertext Transfer Protocol Secure or HTTPS);
- employ strong authentication or multi-factor authentication;
- restrict privileges to the minimum needed (i.e., least privilege);

The organization should devise organizational and technical controls to restrict the management interface used for remote (non-local) vendor maintenance sessions. Remote vendor maintenance

operations conducted by individuals communicating through an external network such as the Internet impose significant risks, not only regarding availability, but also integrity and confidentiality.

Technical controls should restrict communication traffic (i.e. systems, ports, and protocols) to the minimum required for remote vendor maintenance operations. After the accessing party is authenticated, additional controls at the access point should be devised to authorize the vendor maintenance session. These include accepting, asking for approval, or denying the requested session. Appropriate logs containing audit records of vendor actions should be generated.

The organization should restrict dial-up access lines to authorized accessing parties. This includes enforcing a modem call-back protocol and disabling connection establishment until vendor requests a maintenance session and the request is authorized by the organization.

6.4.4 Security auditing, accounting, and monitoring

Compliance regulations and contractual clauses often include monitoring and reporting requirements. Event logging and systems accounting are key capabilities (see [C.5](#)) to help address these requirements. Of these two, event logging is probably the more useful from a storage security perspective because it can be used both real-time and as part of an incident investigation. As such, storage systems and infrastructure need to participate in the organization's event logging program (see also ISO/IEC 27002:2013, 12.4 for relevant guidance).

The following logging guidance is applicable to storage systems and should be used:

- include storage in the logging policy such that:
 - with regard to storage systems and devices, the following elements of policy should be addressed:
 - storage systems and devices should participate in audit logging;
 - all *significant* storage management events should be collected;
 - log data is preserved;
 - log data is archived and retained according to log data retention policy; and
 - the device time is synchronized with a reliable, external source.
 - the logging policy (see also [7.7.2](#)) should include evidentiary expectations (authenticity, chain of custody, etc.).
- employ external or centralized event logging to a trusted⁶⁾ remote source by:
 - implementing centralized⁷⁾ audit logging to collect events from all sources in a single repository;
 - establishing and using a common, accurate time source across the environment to assure that event records from different sources can be correlated;
 - avoiding use of device resident logs for anything other than system health monitoring and debugging because they are more easily subjected to tampering or destruction, there is limited storage space available for logs, and they preclude the use of centralized automated analysis, alerting, and archiving;
 - natively logging events to one, and preferably multiple,⁸⁾ external log servers;

6) A trusted external event logging source is an IT security management product located in a dedicated security zone or domain and is assumed to enforce its security functions correctly.

7) Centralization in this context should not be interpreted as meaning that all audit logging within an organization has to use a common infrastructure. It is more important to have storage systems/ecosystems within a single security domain use a common audit logging infrastructure.

8) Some logging protocols use unreliable network protocols such as User Datagram Protocol (UDP) and therefore log messages may be lost due to network or server performance. Sending messages to multiple log servers can help mitigate this risk.

- using standard logging protocols like syslog⁹⁾ that support reliable delivery and secure transports (e.g., TLS);
- having devices configured to log events as they occur (i.e., no buffering) when the primary drivers for audit logging are compliance, accountability, or security;
- implementing an analysis protocol to correlate audit log records across event sources to identify significant security events that provide indication of security incidents;
- ensuring that the storage logging is factored into Security Information and Event Management (SIEM) solutions, when such technology is deployed.
- ensure complete event logging
 - once the types of events to be logged have been determined, then all occurrences of these events should be logged (whether in-band or out-of-band);
 - the following kinds of events should be logged (a minimum set of security events):
 - failed and successful logon attempts;
 - failed file and object access attempts for sensitive and high-value data;
 - account and group profile additions, changes, and deletions;
 - changes to system security configurations (e.g., audit logging, network filtering, zoning changes);
 - changes to security server usage (e.g., syslog, Network Time Protocol or NTP, Domain Name System or DNS, authentication);
 - system shutdown and restarts;
 - privileged operations (i.e., administrator initiated changes);
 - use of sensitive utilities (e.g., privilege escalation commands);
 - access to critical data files;
 - movement of virtual servers between physical servers.
 - each log entry should include:
 - a timestamp (date and time);
 - a severity level;
 - the source of the log entry (distinguishing name, IP address, etc.);
 - an event ID as well as a textual description (necessary to enable localization/internationalization of events – where the event ID remains the same but the textual description could be translated to different languages); and

destinations reduces the risk of inadvertent loss.

9) Syslog is defined in IETF RFC 5424 with additional details contained in IETF RFC 3195, IETF RFC 5425, IETF RFC 5426, IETF RFC 5427, IETF RFC 5848, IETF RFC 6012, and IETF RFC 6587.