

DIN EN ISO/IEC 27040:2017-03 (E)

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

Contents		Page
European foreword.....		4
Foreword.....		5
Introduction.....		6
1	Scope	7
2	Normative references	7
3	Terms and definitions	7
4	Symbols and abbreviated terms	13
5	Overview and concepts	17
5.1	General.....	17
5.2	Storage concepts.....	18
5.3	Introduction to storage security.....	18
5.4	Storage security risks.....	20
5.4.1	Background.....	20
5.4.2	Data breaches.....	21
5.4.3	Data corruption or destruction.....	22
5.4.4	Temporary or permanent loss of access/availability.....	22
5.4.5	Failure to meet statutory, regulatory, or legal requirements.....	23
6	Supporting controls	23
6.1	General.....	23
6.2	Direct Attached Storage (DAS).....	23
6.3	Storage networking.....	24
6.3.1	Background.....	24
6.3.2	Storage Area Networks (SAN).....	24
6.3.3	Network Attached Storage (NAS).....	29
6.4	Storage management.....	30
6.4.1	Background.....	30
6.4.2	Authentication and authorization.....	32
6.4.3	Secure the management interfaces.....	33
6.4.4	Security auditing, accounting, and monitoring.....	34
6.4.5	System hardening.....	36
6.5	Block-based storage.....	37
6.5.1	Fibre Channel (FC) storage.....	37
6.5.2	IP storage.....	37
6.6	File-based storage.....	38
6.6.1	NFS-based NAS.....	38
6.6.2	SMB/CIFS-based NAS.....	39
6.6.3	Parallel NFS-based NAS.....	39
6.7	Object-based storage.....	40
6.7.1	Cloud computing storage.....	40
6.7.2	Object-based Storage Device (OSD).....	41
6.7.3	Content Addressable Storage (CAS).....	42
6.8	Storage security services.....	43
6.8.1	Data sanitization.....	43
6.8.2	Data confidentiality.....	46
6.8.3	Data reductions.....	48

7	Guidelines for the design and implementation of storage security	49
7.1	General.....	49
7.2	Storage security design principles.....	49
7.2.1	Defence in depth.....	49
7.2.2	Security domains.....	50
7.2.3	Design resilience.....	51
7.2.4	Secure initialization.....	51
7.3	Data reliability, availability, and resilience.....	51
7.3.1	Reliability.....	51
7.3.2	Availability.....	52
7.3.3	Backups and replication.....	52
7.3.4	Disaster Recovery and Business Continuity.....	53
7.3.5	Resilience.....	54
7.4	Data retention.....	54
7.4.1	Long-term retention.....	54
7.4.2	Short to medium-term retention.....	55
7.5	Data confidentiality and integrity.....	56
7.6	Virtualization.....	58
7.6.1	Storage virtualization.....	58
7.6.2	Storage for virtualized systems.....	59
7.7	Design and implementation considerations.....	60
7.7.1	Encryption and key management issues.....	60
7.7.2	Align storage and policy.....	61
7.7.3	Compliance.....	61
7.7.4	Secure multi-tenancy.....	62
7.7.5	Secure autonomous data movement.....	63
	Annex A (normative) Media sanitization	65
	Annex B (informative) Selecting appropriate storage security controls	81
	Annex C (informative) Important security concepts	101
	Bibliography	114