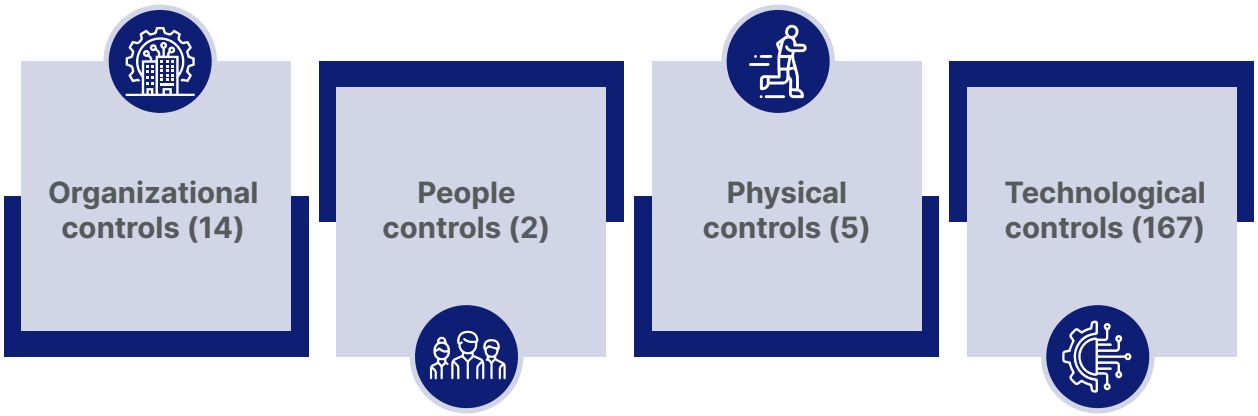
Quick-Start Guide

ISO/IEC 27040: 2024
Storage Security

CONTINUITY

ISO/IEC 27040:
2024 Edition – Storage Security

- Update to ISO/IEC 27040:2015: https://www.iso.org/standard/80194.html
- 220 security guidelines
- 188 controls that establish a baseline set of storage security controls
- Notable examples of mandatory items:
  - Enforce logging
  - Eliminate insecure, outdated features and protocols
  - Minimal strength / currency requirements for encryption
  - Apply minimum security features (limit access, client types, limit vendor access)
  - Safe sanitization



Who's affected

Organizations that have embraced the ISO 27001 family of standards

- With ISO 27001:2022 coming into effect, and 27002 giving credence to 27040 – this is likely to come up in near-term audits

Organizations in regulated industries around the world

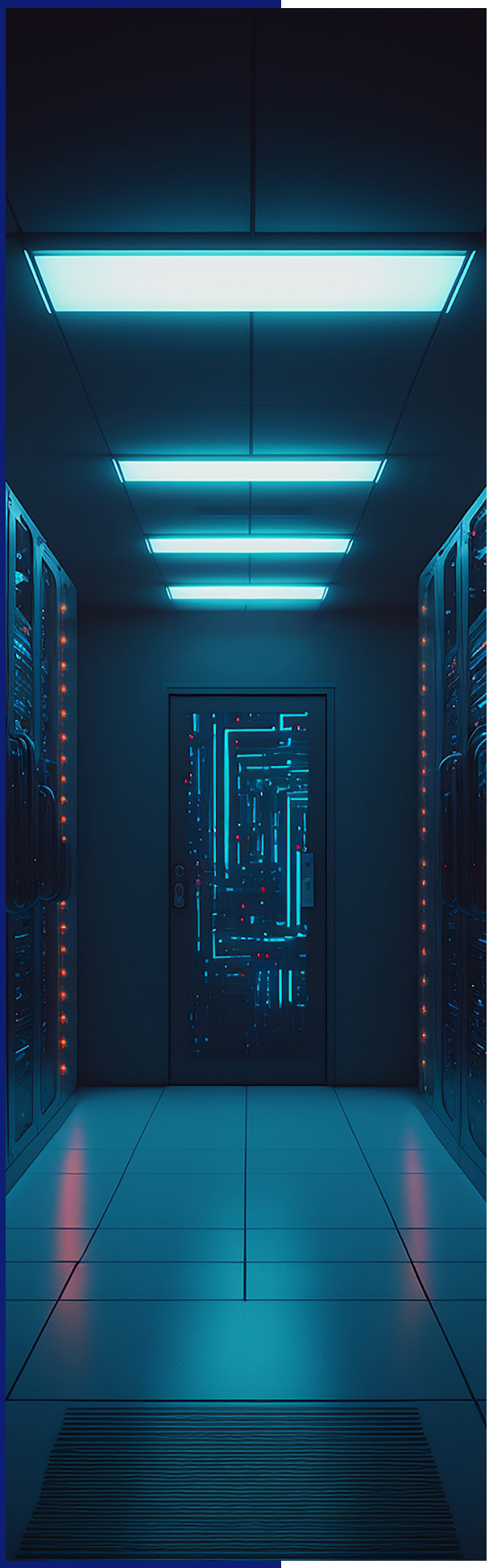
- With the weight that ISO carries, once new guidance becomes publicly available, national authorities and auditors will likely enhance expectations

Other organizations, even those with no external oversight

- Who seek to reduce their exposure to cyber attacks, increase the resiliency of their storage and backup systems, and be better assured they can successfully recover.

Highlights of the new ISO/ IEC 27040

- Use multi-factor authentication
- Use cyber-attack recovery backups & data immutability protections
- Include storage in vulnerability management programs
- Apply vendor-recommended security configurations
- Leverage robust and highly attack-resistant security infrastructures (e.g. zero trust architectures) that are centrally-managed and monitored
- NVMe Security



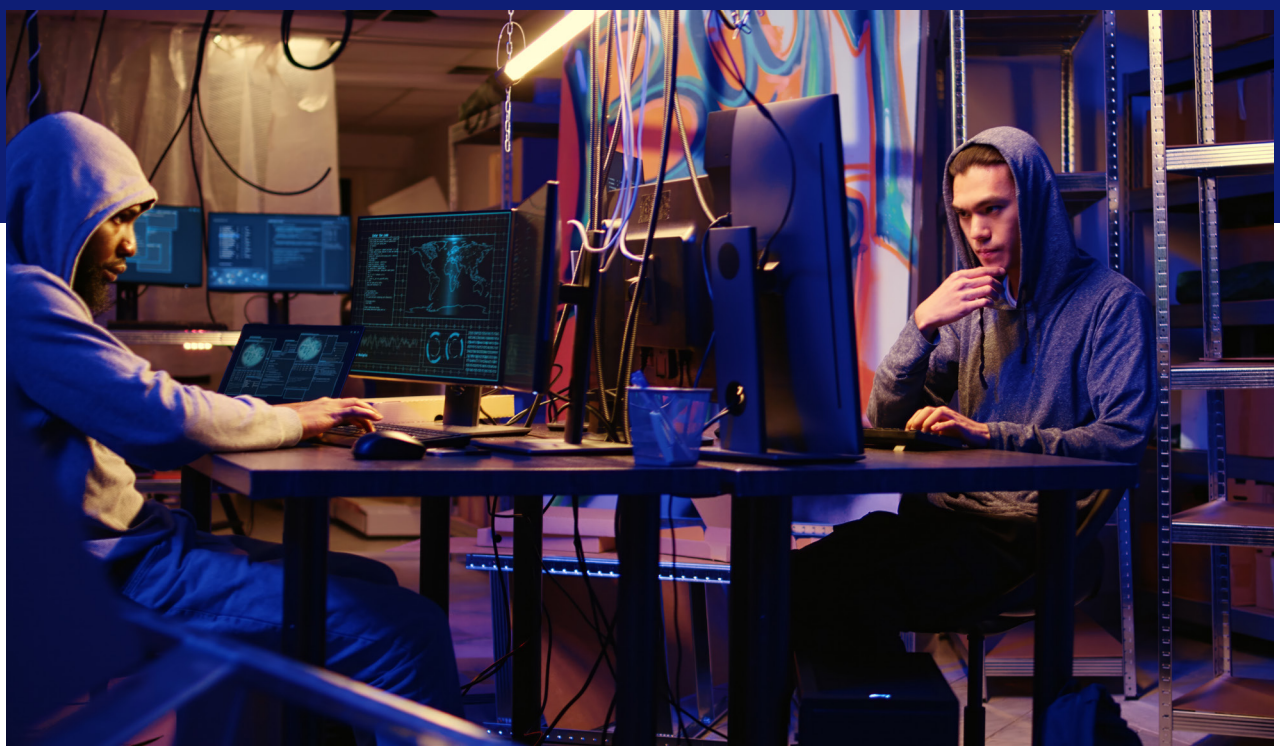
How StorageGuard helps you comply with ISO/IEC 27040

Required by ISO, Provided by StorageGuard

- Ensure adequate storage protection expertise
- Ensure adequate storage security expertise
- Perform system hardening
- Apply vendor-recommend security configurations
- Include storage in vulnerability management programs

Tech controls required by ISO, audited (and potentially enforced) by StorageGuard

Control	ID
TC-BBFC-G01 Using FC LUN masking and mapping	10.9.1
TC-BBFC-G02 Using FCP for SCSI security measures	10.9.1
TC-BBFC-G03 Using data at rest encryption for FC storage	10.9.1
TC-CNFD-G11 Providing end-to-end security protections for data in motion	10.5.4.1
TC-CNFD-G15 Limiting plaintext exposure of plaintext keys	10.5.5
TC-CNFD-G16 Using centralized key management infrastructure	10.5.5
TC-CNFD-R01 Use cryptography with at least 128 bits of security strength	10.5.3
TC-CNFD-R02 TLS minimum requirements	10.5.4.2
TC-CNFD-R03 IPsec minimum requirements	10.5.4.3
TC-DSGN-G01 Adhering to core security design principles	10.2.1
TC-FBNF-G01 Securing data on NFS servers	10.10.2
TC-FBNF-R01 Apply NFS access controls	10.10.2
TC-FBNF-R02 Restrict NFS client behaviours	10.10.2
TC-FBSM-G01 Securing data on SMB servers	10.10.3
TC-FBSM-R01 Minimum acceptable SMB protocol	10.10.3
TC-FBSM-R02 Apply SMB access controls	10.10.3
TC-FBSM-R03 Restrict SMB client behaviours	10.10.3
TC-FCSS-G01 Controlling FCP node access	10.8.2.2
TC-FCSS-G02 Using FC switch-based controls	10.8.2.2
TC-FCSS-G03 Configuring FC device to meet security requirements	10.8.2.2
TC-HARD-G03 Ensuring completeness of storage audit logging	10.3.2



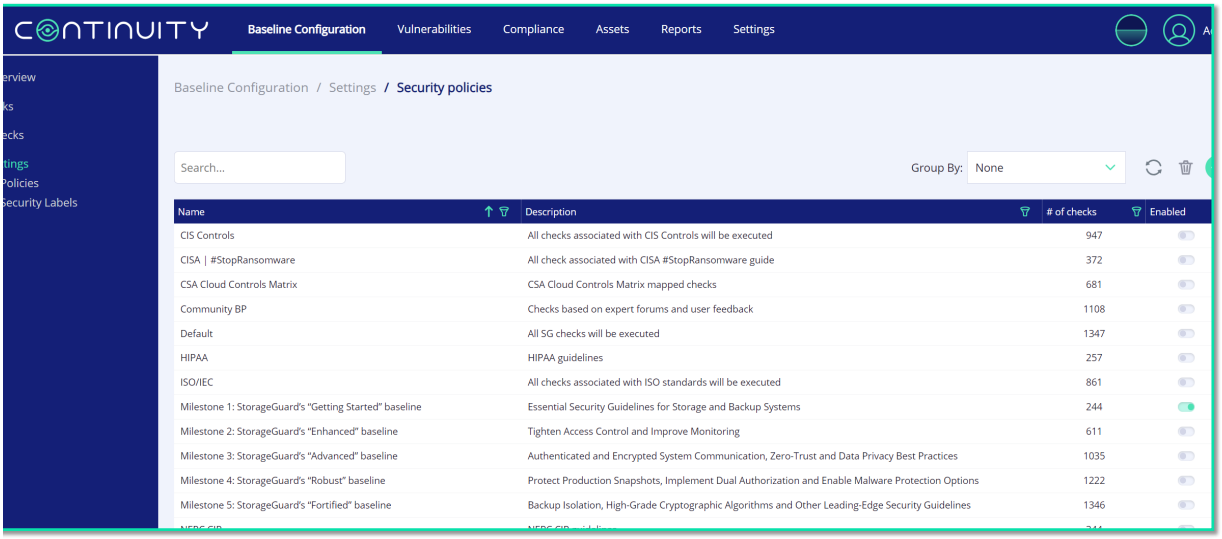
Control	ID
TC-HARD-G04 Implementing appropriate monitoring of storage	10.3.2
TC-HARD-G05 Using log retention and protection for storage	10.3.2
TC-HARD-R01 Perform logging on storage	10.3.2
TC-IPSS-G01 Using iSCSI network access and protocols	10.8.2.3
TC-IPSS-G02 Using FCIP network access and protocols	10.8.2.3
TC-IPSS-G03 Using IPsec to secure FCIP	10.8.2.3
TC-MGMT-G01 Using centralized authentication solutions	10.4.2.1
TC-MGMT-G02 Using multi-factor authentication	10.4.2.1
TC-MGMT-G03 Disabling login to the root or admin account	10.4.2.1
TC-MGMT-G04 Remotely logging all privilege escalation operations	10.4.2.1
TC-MGMT-G06 Separating security and non-security roles	10.4.2.2
TC-MGMT-G07 Securing the network interfaces to management software/firmware	10.4.3
TC-MGMT-R01 Minimum user authentication measures	10.4.2.1

Control	ID
TC-MGMT-R02 Secure the remote management	10.4.3
TC-MGMT-R03 Restrict vendor remote management	10.4.3
TC-MGMT-R04 Restrict dial-up access use	10.4.3
TC-MGMT-R05 Secure IPMI	10.4.3
TC-NASP-G01 Using NFS network access and protocols	10.8.3.2
TC-NASP-G02 Using encryption to secure NFS	10.8.3.2
TC-NASP-G03 Using SMB network access and protocols	10.8.3.3
TC-OBSS-G01 Using transport security for object-based storage transactions	10.12
TC-OBSS-G02 Using data at rest encryption for object-based storage	10.12
TC-OBSS-G03 Enabling data immutability for object-based storage	10.12
TC-PROT-G02 Using data backup measures and operations securely	10.14.2
TC-PROT-G03 Using cyber-attack recovery backups	10.14.2
TC-PROT-G04 Using data replication measures and operations securely	10.14.3
TC-PROT-G05 Using snapshots in conjunction with backups	10.14.4
TC-PROT-G06 Using snapshot security	10.14.4
And hundreds more	

> Due to the specialized nature of storage technologies, storage systems are not always included in an organization's vulnerability management program...
>
> many of the tools used to identify vulnerabilities do not provide extensive coverage of storage operating systems and applications.

StorageGuard Baselines

Ensuring you remain ISO/IEC 27040 compliant - with StorageGuard



www.continuitysoftware.com