ISO/IEC 27040

ISO/IEC 27040:2024 — Information technology — Security techniques — **Storage security** *(second edition)*

Abstract

"[ISO/IEC 27040:2024] provides detailed technical requirements and guidance on how organizations can achieve 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 of data both while stored in information and communications technology (ICT) systems and while in transit across the communication links associated with storage. Storage security includes the security of devices and media, management activities related to the devices and media, applications and services, and controlling or monitoring user activities during the lifetime of devices and media, and after end of use or end of life.

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 products and services, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information or storage security, storage operation, or who are responsible for an organization's overall security programme 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.

[ISO/IEC 27040:2024] provides an overview of storage security concepts and related definitions. It includes requirements and guidance on the threats, 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."

[Source: ISO/IEC 27040:2024]

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

Introduction

Information deserves to be adequately protected while in storage, as well as when created, communicated, processed, used and disposed of. The standard guides the purchasers and users of **computer storage technologies** to determine and treat the associated information risks.

Scope and purpose

The standard concerns the security of data storage devices and media, security of management activities related to the devices and media, applications/services, and end-users, in addition to security of the information being transferred across the communication links associated with storage.

The standard describes information risks associated with data storage, and controls to mitigate the risks. It aims to:

- Draw attention to common risks associated with the confidentiality, integrity and availability of information on various data storage technologies;
- Encourage organisations to improve their protection of stored information using suitable information security controls; and
- Improve assurance, for example by facilitating reviews or audits of the information security controls protecting stored data.

The information security issues associated with backup/disaster recovery locations and cloud storage are covered, as well as those associated with primary/local storage on a variety of data storage technologies, media and subsystems (*e.g.* DAS, SAN, NAS, CAS, FC and OSD).

Media sanitisation (destruction of data stored on various computer storage media) is also covered.

The standard is unusually detailed. It mentions a number of specific storage technologies which is also unusual for the ISO27k standards that are mostly generic and hence timeless.

Status of the standard

The *first* edition was published in **2015**.

The *second* edition was published in January **2024**.

Personal comments

Resilience aspects of digital storage are covered in the standard - an important information security concept that (in my considered opinion) deserves much more emphasis *throughout* ISO27k. After all, information security involves protecting/ensuring the *availability* of important and valuable information, information technologies and information services, right?

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799