ISO 27001: Key Changes at a glance

ISO 27001 Background:

ISO 27001 is the international standard for information security. It sets out the specification for an effective ISMS (information security management system). ISO 27001's best-practice approach helps organisations manage their information security by addressing people, processes and technology. The focus of the standard is to protect and safeguard the confidentiality, availability and integrity of information.

ISO 27001:2022 – Why the Change?

Management system standards are reviewed periodically to ensure they remain relevant and up to date with business needs and challenges. For information security management systems, technology is a rapidly changing area, and so are the threats, and as such, the minimum controls needed for security and privacy also need to evolve to remain current.

The new version of the ISO 27001 addresses duplication by merging several controls in the 2013 version of the standard to simplify the process of implementing and maintaining an ISMS. By 31st October 2025 (3 years after publication of ISO 27001:2022) all organisations that are already certified must have completed the transition to the updated version ISO 27001 and hold an updated ISO 27001:2022 certificate. From the 31st of October 2023, (12 months after publication of ISO 27001:2022), any new certificates issued must be to ISO 27001:2022.

Centre for Assessment Ltd.
Jul, 2023 - 3 min read
www.centreforassessment.co.uk

A UKAS-accredited body, we provide certification to ISO and sector-specific Standards, as well as specialist training services.

CfA Centre for Assessment

Key Changes:

The key changes in the standard are within Annex A, which include:

- The merging of 24 controls
- The revision of 58 controls
- The addition of 11 new controls

114 controls have now been reduced to 93 and organised into:

- Organisations (37 controls, A5)
- People (8 Controls, A6)
- Physical (14 Controls, A7)
- Technological (34 Controls, A8)

Many of the controls in ISO 27001:2022 can be mapped to ISO 27001:2013 controls, but the following are seen as new controls that will require specific focus:

- **Threat intelligence** – understanding attackers and their methods in the context of your IT landscape.
- **Information security for the use of cloud services** – the introduction through operation to exit strategy regarding cloud initiatives now needs to be considered comprehensively.
- **ICT readiness for business continuity** – the requirements for the IT landscape should be derived from the overall business processes and the ability to recover operational capabilities.
- **Physical security monitoring** – the use of alarm and monitoring systems to prevent unauthorised physical access has gained more emphasis.
- **Configuration management** – hardening and secure configuration of IT systems.
- **Information deletion** – compliance with external requirements, such as data protection deletion concepts needs to be implemented.
- **Data masking** – using techniques that mask data, such as anonymisation and pseudonymisation, to bolster your data protection.
- **Data leakage prevention** – taking steps to help prevent sensitive data from being leaked.
- **Monitoring activities** – monitoring network security and application behaviour to detect any network anomalies.
- **Web filtering** – a focus on preventing users from viewing specific URLs containing malicious code.
- **Secure coding** – the use of tools, commenting, tracking changes, and avoiding insecure programming methods to ensure secure coding.

CfA Centre for Assessment

centreforassessment.co.uk
0161 237 4080 | sales@centreforassessment.co.uk
Lee House, 90 Great Bridgewater Street, Manchester, M1 5JW