CERTIFICATION AND TRAINING SERVICES

We specialize in management systems certification for:

QUALITY	AEROSPACE (QUALITY)	AUTOMOTIVE (QUALITY)	ENVIRONMENT	ENERGY

HEALTH AND SAFETY	INFORMATION RESILIENCE	FOOD SAFETY	RISK MANAGEMENT	MEDICAL DEVICES

THE HISTORY OF ISO 27001

nqa.
NEVER STOP IMPROVING

ISO 27001:2013
Information technology - Security techniques - Information security management systems - Requirements

ISO 27001:2022
Information security, cybersecurity and privacy protection — Information security management system —Requirements

BS 7799:1995
First published by BSI and written by UK Gov Department for Trade and Industry

1995

ISO 17799:2000
Information technology - Code of practice for information security management

ISO 27017:2015
Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO 27701:2019
Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines

Transition Period (3 Years)

2025

ISO 27001:2005
Information technology - Security techniques - Information security management systems - Requirements

ISO 27018:2019
Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO 27002:2022
Updated controls - Information security, cybersecurity and privacy protection - Information security controls

About ISO 27001:2022

ISO 27001:2022 brings significant updates to information security management, aimed at aligning with the evolving digital landscape and strengthening defenses against cybersecurity threats. These updates reflect a more streamlined and risk-focused approach, including substantial changes in the Annex A - control structure.

The 14 control domains from ISO 27001:2013 have been reorganised into four key categories—organisational, people, physical, and technological controls and eleven new controls have been added, covering critical areas like threat intelligence, secure coding, and cloud security, to reflect today's heightened security demands. The number of Annex A controls now stands at 93 compared to 114 in the previous edition.

For organisations preparing to transition, these structural changes will require a careful review and adjustment of their ISMS.

Notable Changes

- **4.2 Understanding the needs and expectations of interested parties**

- **4.4 Information security management system**

- **5.3 Organisational roles, responsibilities and authorities**

- **6.2.d Information security objectives and planning to achieve them**

- **6.3 Planning of changes**

- **9.3.2.c Management review inputs**

ISO 27001:2022 CHANGES

Organisation

Ensure organisational governance/framework is in place and exercised to identify, assess and continually protect our assets

People

- There is no substitute for a security aware workforce.
- Insider threat is real, accidental, coerced or deliberate

Physical

Understand assets, the risks associated with them and protect these assets using layered controls

Technology

Focus on implementation of automated (rules based) controls to compliment the above control groups

ISO 27001:2022 NEW CONTROLS

- **5.7 Threat Intelligence**
- **5.23 Information Security for use of Cloud Services**
- **5.30 ICT Readiness for Business Continuity**

Organisational Controls

- **7.4 Physical Security Monitoring**

Physical Controls

- **8.9 Configuration Management**
- **8.10 Information Deletion**
- **8.11 Data Masking**
- **8.12 Data Leakage Prevention**
- **8.16 Monitoring Activities**
- **8.23 Web Filtering**
- **8.28 Secure Coding**

Technical Controls

ISO 27001:2022 NQA GAP TOOL

ISO 27001:2022 NQA GAP TOOL

New requirement	Phase	Clause(s)	Activity
Information security objectives are to be monitored.	Assess	6.2.d)	Have you established how information security objectives are to be monitored and whom shall be responsible for this?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Clause(s)	Activity
Changes to the ISMS are to be planned.	Plan	6.3	Have you established a process for managing changes to the ISMS? How are changes authorised?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022 NQA GAP TOOL

New requirement	Phase	Clause(s)	Activity
Information security objectives are to be monitored.	Assess	6.2.d)	Have you established how information security objectives are to be monitored and whom shall be responsible for this?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
KPIs relating to objectives are captured monthly. The ISMS manager collates the information and reports to the c-suite monthly - see monthly powerpoint slides	Yes ✓	No ☐	

New requirement	Phase	Clause(s)	Activity
Changes to the ISMS are to be planned.	Plan	6.3	Have you established a process for managing changes to the ISMS? How are changes authorised?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
Any changes to the ISMS must be approved by the senior process owner - changes are recorded in our Change Management Log	Yes ✓	No ☐	

ISO 27001:2022 NQA GAP TOOL

nqa.
NEVER STOP IMPROVING

Part 2: ISO 27001:2022 Requirements

Tip: Ensure that you can demonstrate that each requirement of ISO 27001:2022 has been addressed within the ISMS.

ISO 27001:2022			ISO 27001:2022 cross reference and the significant changes from the 2013 version	
4.1 Understanding the organization and its context			No change: Have you determined your external and internal issues that are relevant to and affect the ISMS?	
Evidence of compliance (Client to complete)	**Has the client demonstrated they have met the requirements of this clause?** (Assessor to complete)		**Comments if required** (Assessor to complete)	
	Yes ☐	No ☐		

➤ May be remapped

ISO 27001:2022 Transition Policy – transition Approach

- Clients can transition their systems at surveillance or recertification audits

- Certification will be granted for ISO 27001:2022 in alignment with their existing cycle
  - Transition at surveillance: the previous valid until date (VUD) will be maintained
  - Transition at recertification: 3 years will be granted

Clients which have their ISO 27001 VUD restricted to less than 3 years due to the transition period (31 Oct 2025) will have the balance of their 3 year cycle reinstated at transition

ISO 27001:2022 Transition Policy – MR & IA

- Clients are to undertake a Management Review and Internal Audit to the new requirements of ISO 27001:2022

- As a minimum, the client must have completed a formal gap analysis using the document mentioned above and reviewed the output with Top Management at management review or an equivalent mechanism

- Completion of the NQA ISO 27001:2022 gap analysis form is mandatory

27001:2022 - Transition

- We offer a range of tools and advice such as:

- Gap Analysis Tool (Client to complete) to help teams assess their systems against the new standard and guide them through any necessary updates.

- Webinars. Cover the subject area and are interactive with Q and A sessions.

- Blogs and news articles covering everything from understanding the updates to common FAQs.

- Training Courses to ensure the candidate has the knowledge necessary for a seamless transition.