nqa.

ISO 27001:2022 GAP GUIDE

53,000 CERTIFICATES GLOBALLY

100% TRANSPARENT FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OVER 100 OPERATING COUNTRIES

CARBON NEUTRAL

INTRODUCTION

This document provides an overview of the key changes between the 2013 and 2022 version of ISO 27001. New requirements are shown below. You will need to prepare for change and adapt your information security management system to meet the new requirements and transitional timelines. This document should be used in conjunction with the NQA Gap Analysis tool.

STRUCTURE OF ISO 27001:2022

The structure of ISO 27001:2022 follows the high level structure defined in Annex SL:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Annex A

5. Organizational controls
6. People controls
7. Physical controls
8. Technological controls

OUR VALUES

We will help you understand the changes, interpret the new concepts and how they impact your ISMS.

Keep updated with the changes at www.nqa.com

Please get in touch if you have any questions.

GAP GUIDE AND GUIDANCE

CLAUSE	REQUIREMENT	GAP
4 Context of the organization		
4.2	Understanding the needs and expectations of interested parties	This control now explicitly requires your organization to be able to demonstrate which of your interested parties' relevant requirement will be addressed through the ISMS.
4.4	Information Security Management System (ISMS)	There is now a focus on your processes and how they interact with the ISMS.
5 Leadership		
5.3	Organizational roles, responsibilities and authorities	This clause now contains an explicit requirement to communicate roles, responsibilities and authorities within your organization.
6 Planning		
6.2.d	Information security objectives and planning to achieve them	Information security objectives must be established at relevant levels within your organization. ISO 27001:2022 requires objectives and progress towards achieving them to be monitored.
6.3	Planning of changes	This is a new requirement. Be prepared to demonstrate how you plan any changes to the ISMS.
9 Performance evaluation		
9.3.2.c	Management review inputs	During mangement review, you are now expected to review any changes to the needs and expectations of your relevant interested parties.

ANNEX A

CLAUSE	REQUIREMENT	GAP
5 Organizational controls		
5.7	Threat intelligence	A completely new control which requires organizations to collect information relating to information security threats, and to analyse this information in order to produce threat intelligence. Organizations may wish to consider where they will collect information from and how they determine that the information is relevant to their own needs.
5.23	Information security for use of cloud services	This is a new control that requires organizations to have processes in place in order to ensure that they have specified, managed and administered security concepts as they relate to the cloud services they have deployed. You must also consider security matters when planning your exit from cloud services.
5.30	ICT readiness for business continuity	This control requires that you identify ICT continuity requirements in a business continuity situation. You will be expected to show objective evidence that ICT readiness has been fully integrated into you business continuity plan, including testing of ICT readiness.
7 Physical controls		
7.4	Physical security monitoring	Although physical security controls are not a new concept, the standard now introduces the requirement to monitor your premises continuously (in and out of normal business hours,) for unauthorised physical access.

ANNEX A

CONTROL	REQUIREMENT	GAP

8 Technological controls

8.9	Configuration management	Configuration management of networks and systems must now be established, implemented, monitored and reviewed. This will include identifying threats, weaknesses and vulnerabilities to security configurations.
8.10	Information deletion	This control requires information that is no longer required to be securely deleted when it is out of date or no longer required.
8.11	Data masking	A new requirement that sensitive data is protected using techniques above and beyond an organization's regular security controls and protocols. The information to be masked may be due to a legal, statutory, contractual or regulatory requirement.
8.12	Data leakage prevention	This new control requires data leakage prevention measures to be implemented in order to prevent/detect unauthorised access, transfer or extraction of information.
8.16	Monitoring activities	This control is an extension of 'ISO 27001:2013 A.12.4 Logging and monitoring'. In this latest edition, organizations are required to monitor networks and systems for anomolous behaviour, having understood what 'normal' behaviour/usage looks like. There is also a requirement to show how you react to potential security incidents.
8.23	Web filtering	This is a new control with the requirement for users to be blocked from accessing external websites that may contain malicious content or content that is not commensurate with organizational policies.
8.28	Secure coding	Organizations are required to ensure that secure coding principles have been designed, implemented and are being followed thorughout the development lifecycle.

Statement of applicability

Your Statement Of Applicability (SOA) must contain the necessary controls and justification for their inclusion, whether the necessary controls are implmented or not and the justification for any excluded controls.

Organizations are to have mapped their previous SOA to the requirements of ISO 27001:2022. Use of attributes, which is not mandated, may be introduced in order to better understand controls and how they address areas of risk identified by your organization.

Risk assessments/register

Your assessor will want to see evidence that risk assessments/registers have been updated to take into account the new controls that have been introduced by ISO 27001:2022.

NEXT STEPS

Preparing for your ISO 27001 transition

- Organizations must transition their **management system** in accordance with the requirements to ISO 27001:2022 before their transition audit is conducted. This should include any documentation changes, along with evidence of any new or changed process requirements.
- Of note, organizations must conduct an internal audit and management review of the new requirements prior to the NQA transition audit being conducted.
- Organizations may have a transition gap assessment conducted by NQA prior to their official transition audit. This could be conducted in conjunction with an earlier ISO 27001:2013 surveillance, or at any other stand-alone time prior to their transition audit.

Your ISO 27001 transition audit

- All organizations must have a transition audit to confirm the implementation of the new standard. The transition audit may be conducted in conjunction with an existing audit, or may be a stand-alone audit.
- If the transition audit is conducted in conjunction with an existing surveillance (i.e. transition surveillance,) or recertification audit (i.e. transition re-assessment,) additional time will be added to the audit duration in order to cover the new requirements introduced by ISO 27001:2022.
- If a stand-alone audit is carried out for the transition audit, the duration will be calculated on an individual organization basis.

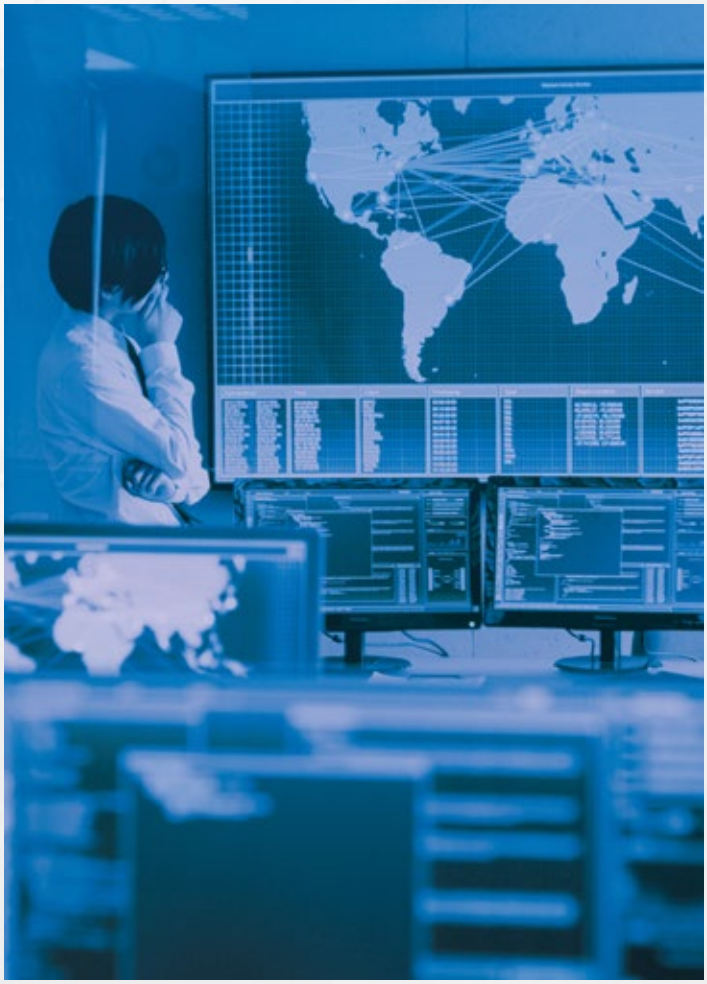
Note: *Specific transition audit durations will depend on your organization's size and the complexity of the ISMS. NQA will advise you of your specific transition audit duration.*

Revised ISO 27001:2022 certificates

As with any audit, non-conformances identified during a transition audit will require a corrective action plan to be submitted and approved. An updated ISO 27001:2022 certification will be issued following corrective action approval.

Updated ISO 27001:2022 certificate issuance and validity will be as follows:

- **Transition surveillance**
  The organization's existing 'Valid Until Date' will be maintained.
- **Transition re-assessment**
  A new 'Valid Until Date' will be issued for the renewed three year period.
- **Stand-alone transition**
  The organization's existing 'Valid Until Date' will be maintained.



nqa.

www.nqa.com