MIND THE GAP (ANALYSIS) FOR ISO 27001:2022

James Keenan
BU Lead, Information Security

David Nutbrown
Principal Auditor ISO27001

OUR PURPOSE

IS TO HELP CUSTOMERS DELIVER PRODUCTS THE WORLD CAN **TRUST**

NQA is a **world leading certification body** with global operations.

NQA specialises in certification in **high technology** and engineering sectors.

AMERICA'S NO.1
Certification body in **Aerospace** sector

TOP 3 IN THE UK
ISO 9001, ISO 14001, ISO 45001, ISO 27001

CHINA'S NO.1
Certification body in **Automotive** sector

GLOBAL NO.1
Certification body in **telecommunications** and **Automotive** sector

GLOBAL NO.3
Certification body in **Aerospace** sector

UK'S NO.2
Certification body in **Aerospace** sector

nqa.
NEVER STOP IMPROVING

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

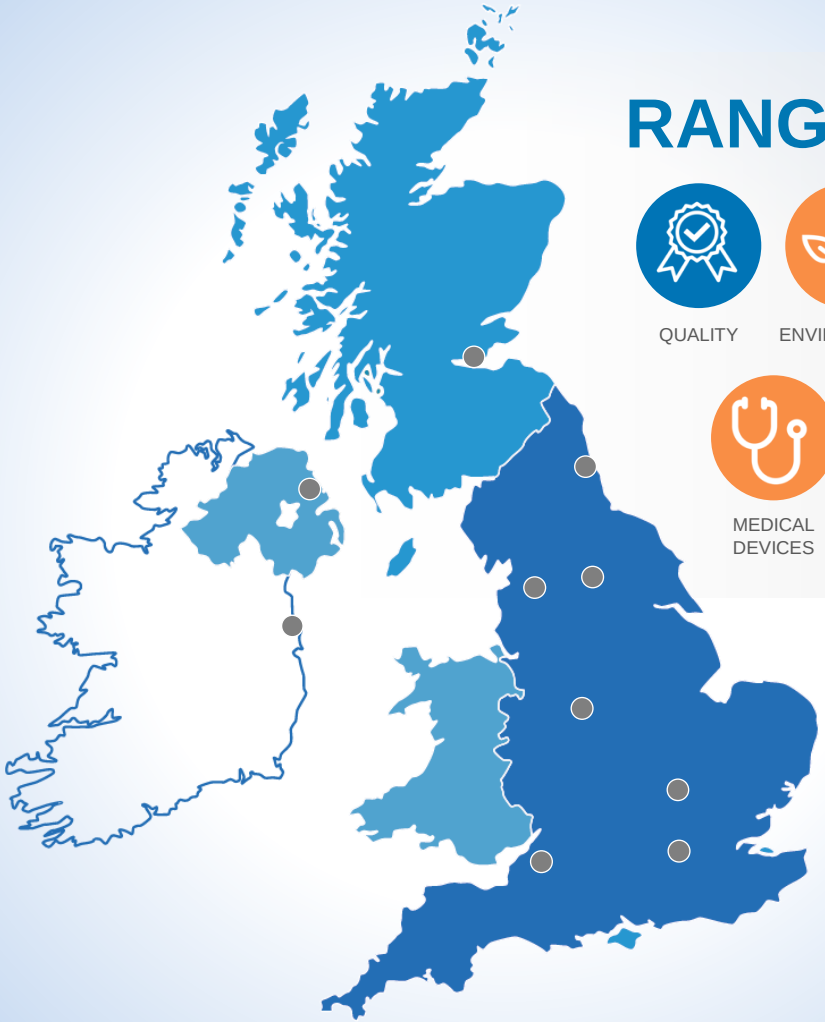

RISK MANAGEMENT


MEDICAL DEVICES

NATIONWIDE TRAINING SERVICES

ACCREDITED COURSES

- Virtual Learning
- e-Learning / Live Webinars
- In-house Training
- Public Training Nationwide Locations



RANGE OF COURSES

- QUALITY
- ENVIRONMENT
- ENERGY
- HEALTH AND SAFETY
- INFORMATION SECURITY
- MEDICAL DEVICES
- BUSINESS CONTINUITY
- AEROSPACE
- INTEGRATED MANAGEMENT

- **e-Learning** Introduction
- **1 day** Introduction Courses
- **2 day** Implementation Courses
- **2 day** Internal Auditor – NQA or IRCA
- **5 day** Lead Auditor – NQA or IRCA

CQI | IRCA
APPROVED TRAINING PARTNER

nqa.


nqa.
ISO 27001
INFORMATION SECURITY MANAGEMENT
UKAS
MANAGEMENT SYSTEMS
0015


nqa.

Transition Information

TRANSITION DEADLINE

October 31st 2025

BOOKINGS

NQA is now taking bookings.

DAYS

Transition will be 1 day on top of the usual audit you choose.

RECERTIFICATION

Recertification would be the ideal time to transition.

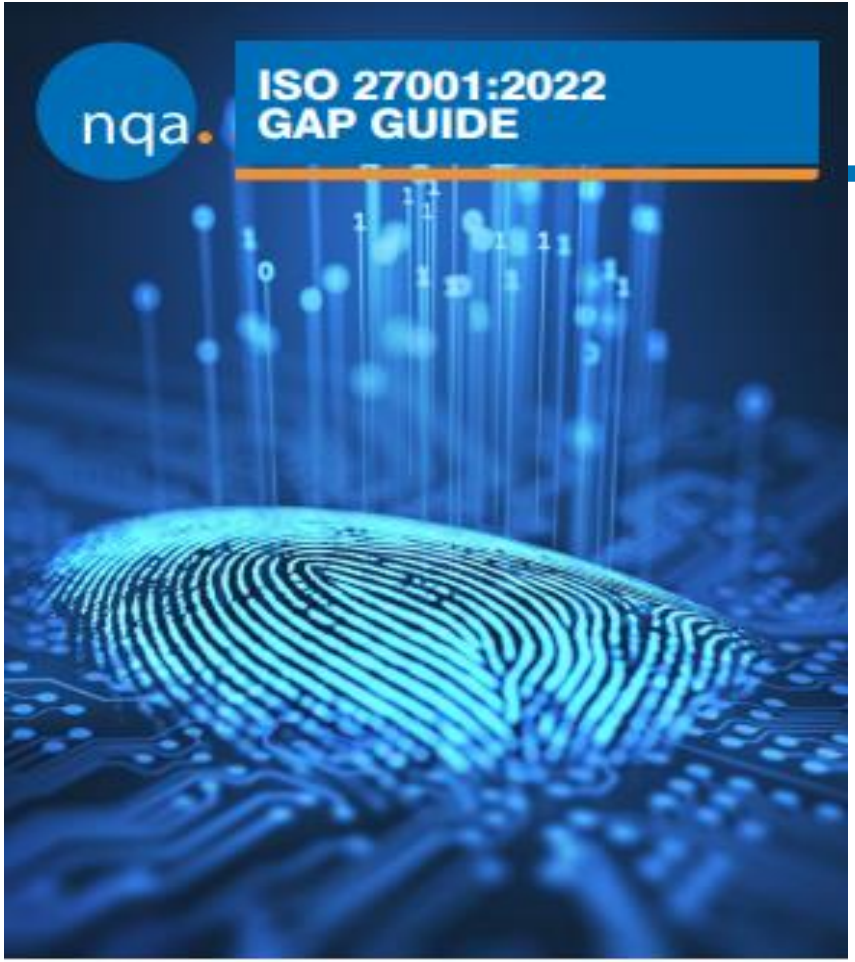
CONTACT US

For more information about your specific timeline and details contact out team.

www.nqa.com

0800 052 2424


nqa.
ISO 27001:2022
GAP GUIDE
nqa.
ISO 27001:2022
CLIENT GAP ANALYSIS TOOL



53,000 CERTIFICATES GLOBALLY · 100% INDEPENDENT FEES · 1000's EMPLOYED · AVERAGE CUSTOMER PARTNERSHIP 10 YEARS · 100 OPERATING COUNTRIES · CARBON NEUTRAL

nqa.

ISO 27001:2022 CLIENT GAP ANALYSIS TOOL

Instructions for use:

This gap analysis document provides a simple framework for evaluating your quality management system against the requirements of ISO 27001:2022. It is split into two tables:

- **Part 1: new concepts** – highlighting the new concepts introduced in ISO 27001:2022 and the related clauses, processes and functional activities.
- **Part 2: requirements** – highlighting amended clauses, processes and functional activities between ISO 27001:2013 and ISO 27001:2022.

Please complete each table by recording the evidence acquired from one full internal audit against the requirements of ISO 27001:2022. If you are unable to provide evidence of compliance, you may not be ready to complete the transition to ISO 27001:2022. In this case, please inform NQA that you need additional time to prepare for the transition – we will work with you to select a mutually agreeable date to complete the transition.

Please ensure that this completed document and internal audit records are available to your auditor at the opening meeting of your transition audit.

Client name: Completion date:

Part 1: New concepts

Tip: Ensure that these new concepts have been deployed in a manner that supports the **Process Approach** and **Risk-Based Thinking**.

New requirement	Phase	Clause(s)	Activity
A more explicit requirement for ensuring that interested parties, their needs and expectations relevant to the ISMS have been identified.	Identify	4.2.a.b.c)	Have you identified interested parties relevant to the ISMS, their relevant requirements and which of these will be addressed by 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 ☐	

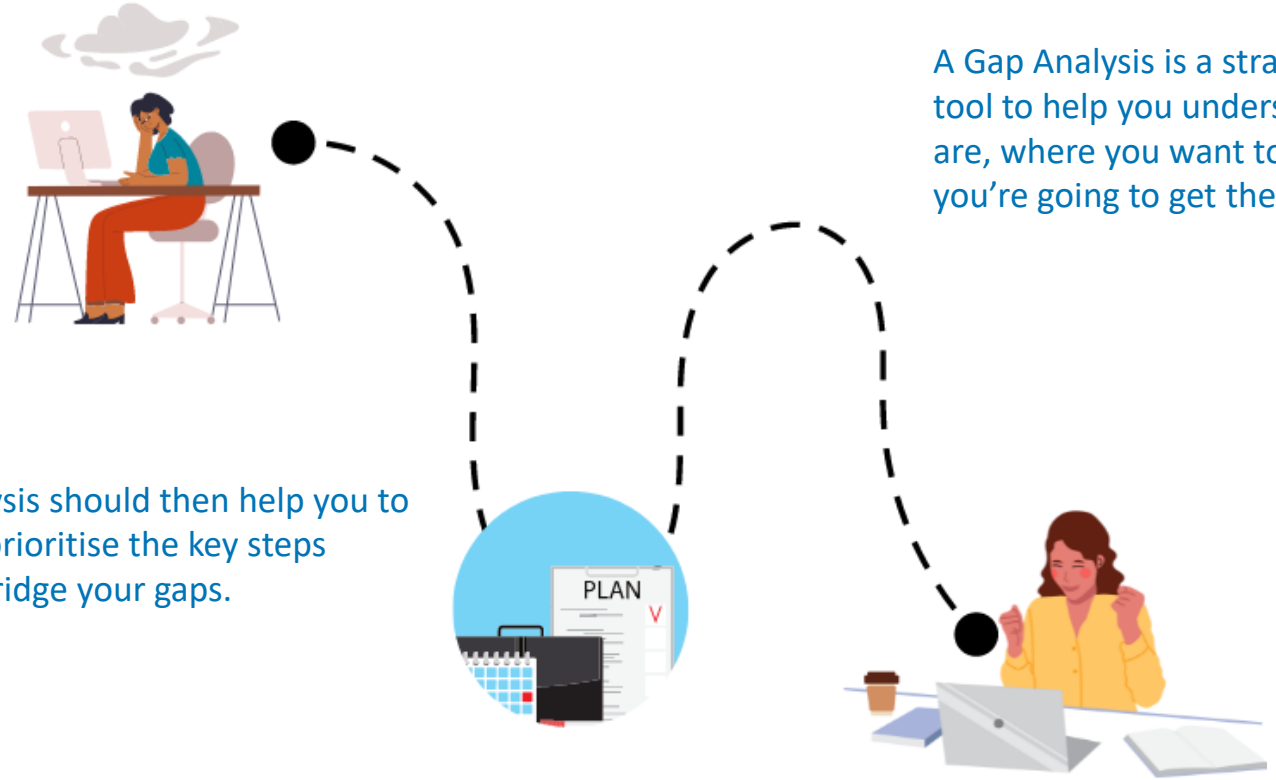
New requirement	Phase	Clause(s)	Activity
New requirement for the adoption of a process approach (where before this was implied).	Identify	4.4	Has planning for the information security management system determined the processes of your organization and interactions with the ISMS?

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 ☐	

New requirement	Phase	Clause(s)	Activity
Explicit requirement for top management to ensure that information security roles, responsibilities and authorities are communicated within the organization.	Action	5.3	Have top management established (and are they supportive of,) a mechanism for communicating responsibilities and authorities for roles relevant to information security within the organization?

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 ☐	

Gap Analysis Definition

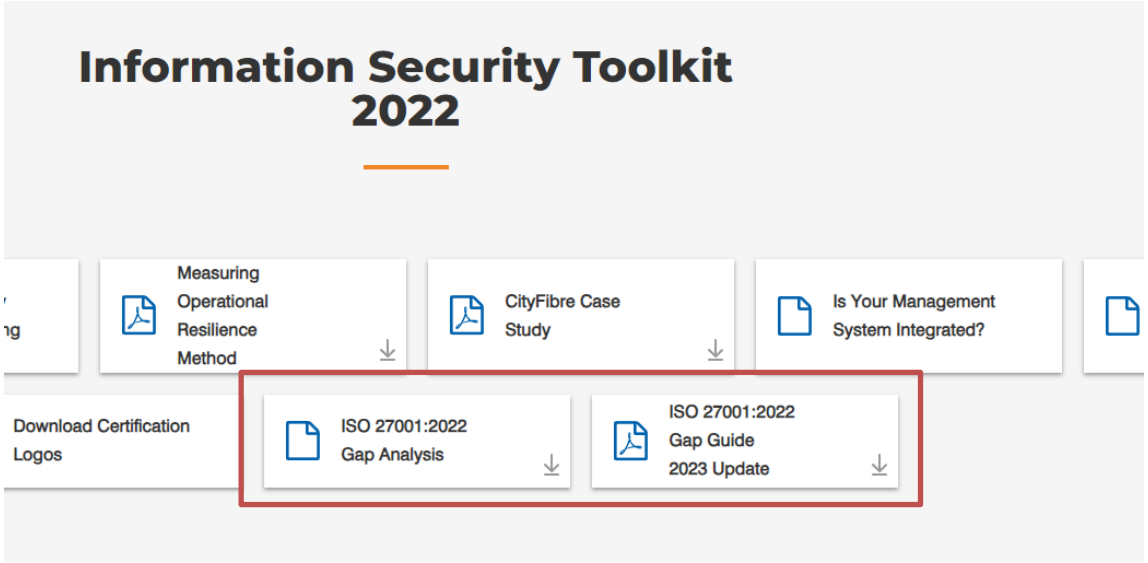


A Gap Analysis is a strategic planning tool to help you understand where you are, where you want to be and how you're going to get there.

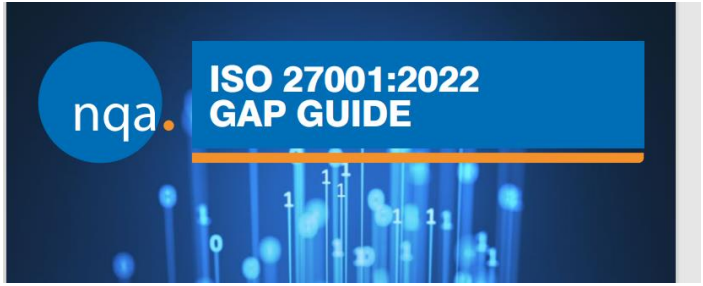
Any gap analysis should then help you to identify and prioritise the key steps required to bridge your gaps.

NQA Gap Analysis Material

We do not require you to use our tool



NQA ISO 27001:2022 Gap Guide



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.

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.

The Gap guide is to be used as a companion to the Gap Tool which should add context.

NQA ISO 27001:2022 Gap Tool

NEVER STOP IMPROVING

Part 1: New concepts

Tip: Ensure that these new concepts have been deployed in a manner that supports the **Process Approach** and **Risk-Based Thinking**.

New requirement	Phase	Clause(s)	Activity
A more explicit requirement for ensuring that interested parties, their needs and expectations relevant to the ISMS have been identified.	Identify	4.2.a.b.c)	Have you identified interested parties relevant to the ISMS, their relevant requirements and which of these will be addressed by 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 ☐	

Part 1 – Introduces new concepts

Part 2 – Focusses on the requirements of the standard, not the new requirements

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 ☐	

Why do we insist on the Gap Analysis being performed and a Gap Tool being presented to the auditor?

Simply – this will provide part of the evidence supporting the auditor's decision as to whether certification to has been recommended or not.

The Gap tool will be uploaded into your client notes and be made available for scrutiny if required by UKAS.

NEVER STOP IMPROVING

NQA ISO 27001:2022 Gap Tool (Part 1)

New requirement	Phase	Clause(s)	Activity
Changes in the needs and expectations of interested parties are to be addressed during management review.	**Action**	**9.3.2.c)**	Are the needs and expectations of interested parties (relevant to the ISMS) reviewed during MR?

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)*
Management Review Minutes - xx/xx/2023, agenda item 4. Management Review Minutes (template)	Yes ☐	No ☐	

NEVER STOP IMPROVING

NQA ISO 27001:2022 Gap Tool

New requirement	Phase	Clause(s)	Activity
Changes in the needs and expectations of interested parties are to be addressed during management review.	**Action**	**9.3.2.c)**	**Are the needs and expectations of interested parties (relevant to the ISMS) reviewed during MR?**

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)*
Management Review Minutes - xx/xx/2023, agenda item 4. Management Review Minutes (template)	Yes ✓	No	

NEVER STOP IMPROVING

NQA ISO 27001:2022 Gap Tool

New requirement	Phase	Clause(s)	Activity
Changes in the needs and expectations of interested parties are to be addressed during management review.	**Action**	**9.3.2.c)**	**Are the needs and expectations of interested parties (relevant to the ISMS) reviewed during MR?**

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)*
Management Review Minutes - xx/xx/2023, agenda item 4. Management Review Minutes (template)	Yes ✓	No	Reviewed Management Review Minutes xx/x/2023. Agenda item 4 adresses 'Changes to the needs and expecttions of interested parties'. The following changes have been noted ....

NEVER STOP IMPROVING

NQA ISO 27001:2022 Gap Tool

New requirement	Phase	Control(s)	Activity
Monitoring activities	**Action**	**8.16**	**Are your networks monitored for anomalous behaviour?**
	Plan	**8.16**	**If/when detected, how is anomalous behaviour evaluated and reported?**

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)*
SIEM installed Event logs and SIEM dashboard Information Security Analyst Roles and Responsibilities Information Security Incident Reporting Record.	Yes ✓	No	Observed SIEM inputs and outputs and interviewed Information Security Analyst

nqa.
NEVER STOP IMPROVING

Q&A

nqa.
NEVER STOP IMPROVING

TAKE THE NEXT STEP

FURTHER SUPPORT

Call
0800 052 2424

Email:
info@nqa.com

Visit LinkedIn
or Twitter
@NQAGlobal

To find out more information on certification, the training we offer or to receive top class support please get in touch.

Visit our website:
www.nqa.com

Check out our
latest blogs
nqa.com/blog

Sign up to our
e-zine, InTouch:
nqa.com/signup

nqa.
NEVER STOP IMPROVING

THANK YOU

Warwick House | Houghton Hall Park | Houghton Regis | Dunstable | LU5 5ZX | United Kingdom
0800 052 2424 | | www.nqa.com