WEBINAR: Back To Basics ISO 27001

Linda Porter

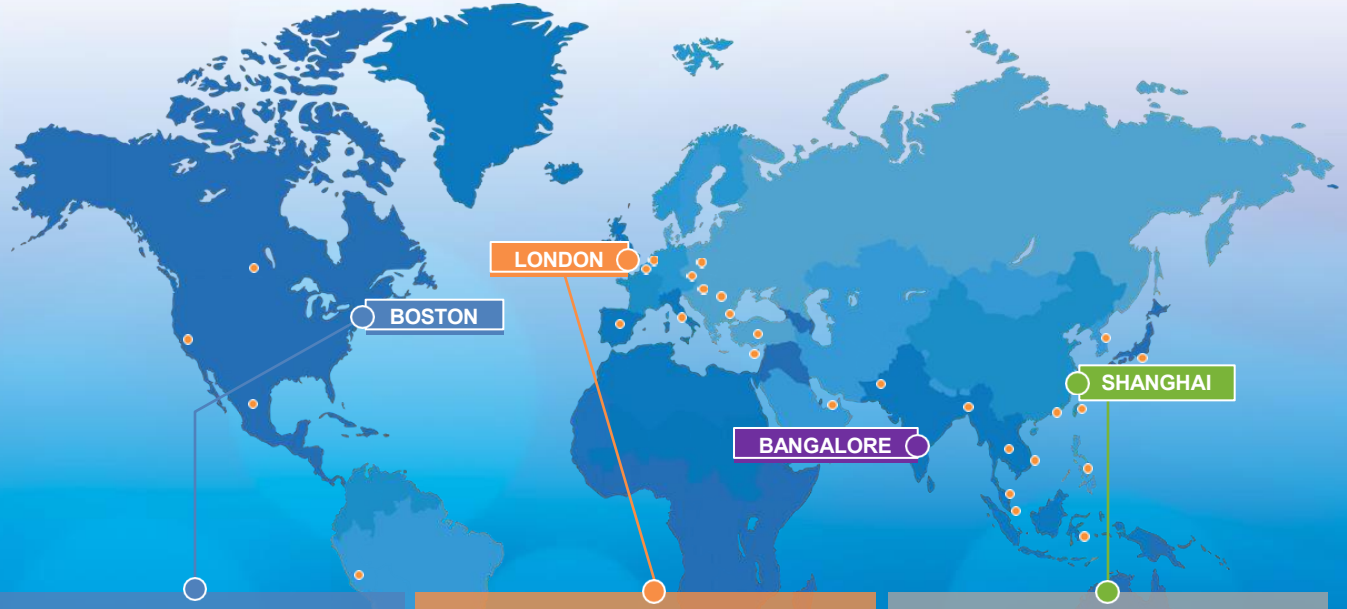
28th July 2025

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.
a kiwa company

WEBINAR AGENDA

OBJECTIVES

- Understand the core principles of ISO 27001
- Break down key components of an Information Security Management System (ISMS)
- Explore why ISO 27001 matters now more than ever
- Provide practical tips for implementation or refresh

OUTCOME

- Be able to explain the purpose and structure of ISO 27001
- Identify the mandatory clauses and key Annex A control categories
- Understand how to apply risk-based thinking to information security
- Recognise common challenges and how to avoid them

What is ISO 27001

ISO 27001 is the International Standard describing the best practices for an Information Security Management System (ISMS).

It provides a systematic approach to managing sensitive company information so that it remains secure.

Requires formulation of procedures and practices including:

- Risk Management Monitoring and Analysis of your management system
- Identifying and generating improvements

Common Misconception: “ISO 27001 is just cyber security stuff.”

ISO 27001 is not just about cyber security or IT systems, it’s a comprehensive management framework that helps organisations of any type identify, assess, and control risks related to information assets.

Importantly, ISO 27001 does not promise to make security breaches impossible. Instead, it ensures that a structured, risk-based approach is in place to manage and reduce information security risks in a consistent, ongoing manner.

nqa.
a kiwa company

Why It's Important

Data is a critical asset, and breaches are costly. ISO 27001 promotes shared responsibility across the organisation, helping us stay secure, compliant, and smart in how we work.

- Risk Management: Helps identify and address information security risks.
- Regulatory Compliance: Assists in meeting legal, regulatory, and contractual obligations (e.g., GDPR).
- Trust & Reputation: Builds confidence with customers, stakeholders, and partners.
- Competitive Advantage: Demonstrates a strong commitment to information security.
- Incident Reduction: Reduces the likelihood and impact of security breaches

nqa.
a kiwa company

Structure and Key Clauses of ISO 27001

Key Clauses	Description
Clause 4: Context of the Organisation	Understanding internal/external issues, stakeholders, and ISMS scope.
Clause 5: Leadership	Top management commitment, policy, roles, and responsibilities.
Clause 6: Planning	Risk assessment, treatment plans, and ISMS objectives.
Clause 7: Support	Resources, awareness, communication, documented information.
Clause 8: Operation	Operational planning and control, risk treatment execution.
Clause 9: Performance Evaluation	Monitoring, measurement, analysis, internal audits, and management reviews.
Clause 10: Improvement	Continual improvement, nonconformity handling, and corrective actions.

Annex A

Annex A Controls (updated in ISO 27001:2022):

- Organisational controls
- People controls
- Physical controls
- Technological controls

Where the Risk Controls are found!

Can be augmented by controls not specifically listed within your ISMS.

Common Implementation Mistakes

Treating it as an IT-only project
- Involve departments such as HR, Legal, Operations ISMS spans the whole business.

Copy-pasting templates without customisation
- Tailor policies and procedures to your actual environment and risk profile.

Focusing too much on documentation
- Ensure that procedures are actually implemented and followed, not just written.

Ignoring top management involvement
- Leadership must actively support and review the ISMS.

Inadequate risk assessment
- Use a structured, repeatable method to identify, assess, and treat risks.

Not training employees
- Provide security awareness training regularly across the organization.

Steps Toward ISO 27001 Certification

Before engaging a Certification Body (CB), conduct internal preparation, typically starting with a gap analysis to assess what's already in place. If existing policies align with ISO 27001, there's no need to start from scratch.

- Define your scope: Boundaries of what your ISMS will cover
- Complete Risk Assessment:
  - Identify risk owner
  - Consider Annex A controls to be used.
    - Risks can also be opportunities
  - Identify assets, threats, vulnerabilities, and apply controls
- Develop Required Documentation: Policies, procedures, Statement of Applicability (SoA), risk treatment plan, etc.
- Audit, Review and Improve – PDCA!
- External audits – stage one and stage two

Conclusion

- ISO 27001 is a framework for managing information security risks not just an IT or cyber security tool.
- It treats data as a critical asset and helps reduce the risk and cost of data breaches.
- Responsibility is organisation-wide, not limited to the IT department.
- ISO promotes smart, secure, and efficient ways of working.
- Before talking to a Certification Body (CB), conduct a gap analysis to identify what's already in place.
- Leverage existing policies, like risk management, rather than starting from scratch.
- ISO 27001 helps organisations achieve compliance, resilience, and trust.

Training Offered

STANDARD	TRAINING
ISO 27001	ISO 27001 E-learning Level 1 | Introduction Online – In your own time
ISO 27001	CQI and IRCA ISO 27001 Internal Auditor (A2574) Level 2 | Intermediate Thursday 4th – Friday 5th September 2025
ISO 27001	CQI and IRCA ISO 27001 Lead Auditor (A2573) Level 3 | Advanced Monday 22nd – Friday 26th September 2025
ISO 9001	ISO 9001 E-Learning Level 1 | Introduction Online – In your own time

TRAINING OFFERED

Privacy Information Pathway

ISO 27701
Introduction & Implementation

Information Security Pathway

ISO 27001
E-Learning → ISO 27001
Introduction & Implementation → ISO 27001
Internal Auditor → ISO 27001
Lead Auditor

Cloud Pathway

ISO 27001
E-Learning → ISO 27018
E-Learning

Certification And Training Services

We specialize in management systems certification for:

QUALITY

AEROSPACE (QUALITY)

AUTOMOTIVE (QUALITY)

SUSTAINABILITY

ENERGY

HEALTH AND SAFETY

INFORMATION RESILIENCE

FOOD SAFETY

RISK MANAGEMENT

MEDICAL DEVICES

FURTHER SUPPORT

Call
0800 052 2424

Email:
info@nqa.com

Visit LinkedIn
@NQA

To find out more information on verification, 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. Sustainability Simplified

Podcast
NQA's Sustainability Simplified
NQA Global Certification Body

Q&A