NQA ISO 27001:2022 TRANSITION

James Keenan
BU Lead, Information Security

David Nutbrown
Principal Auditor ISO 27001

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

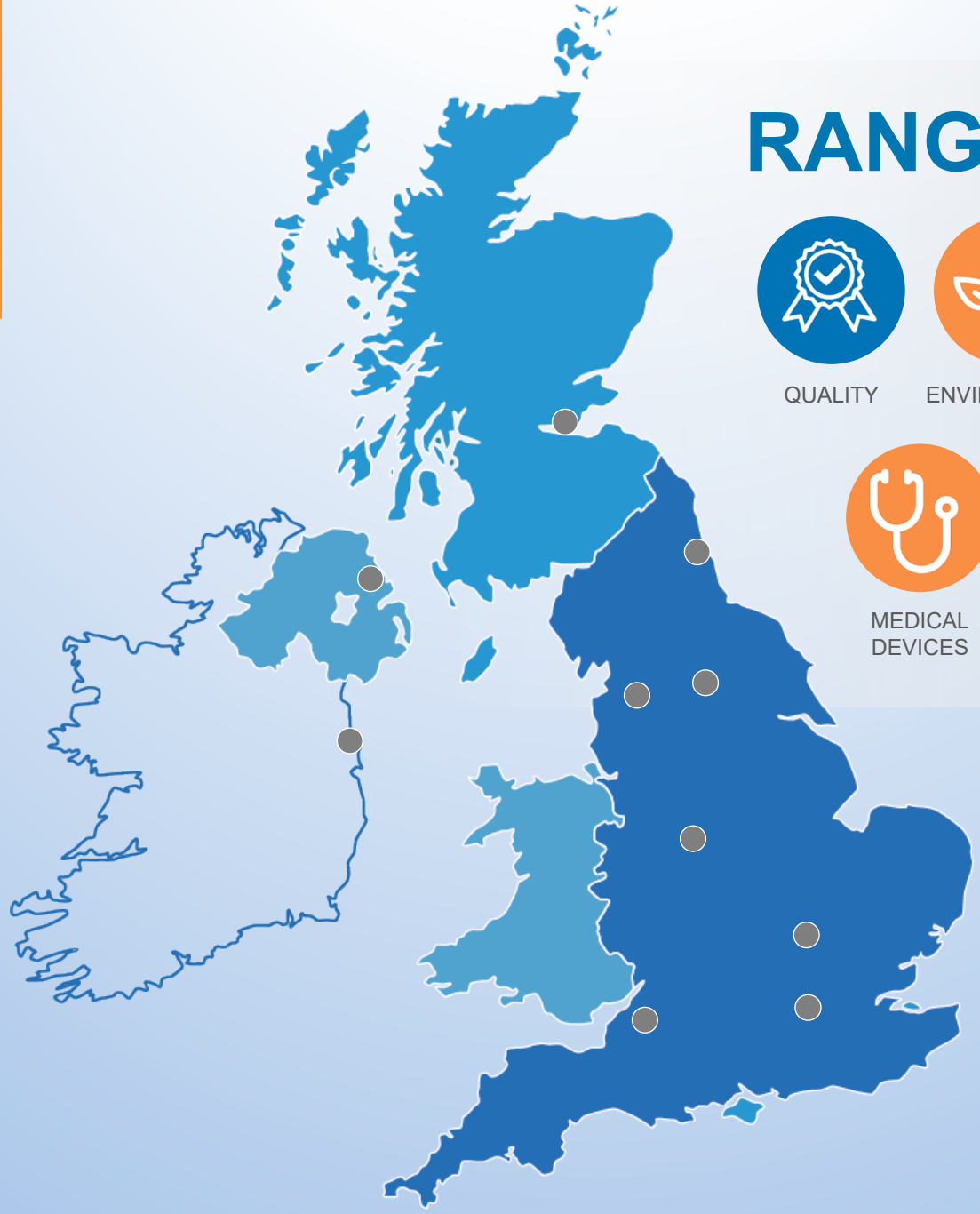

RISK MANAGEMENT


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

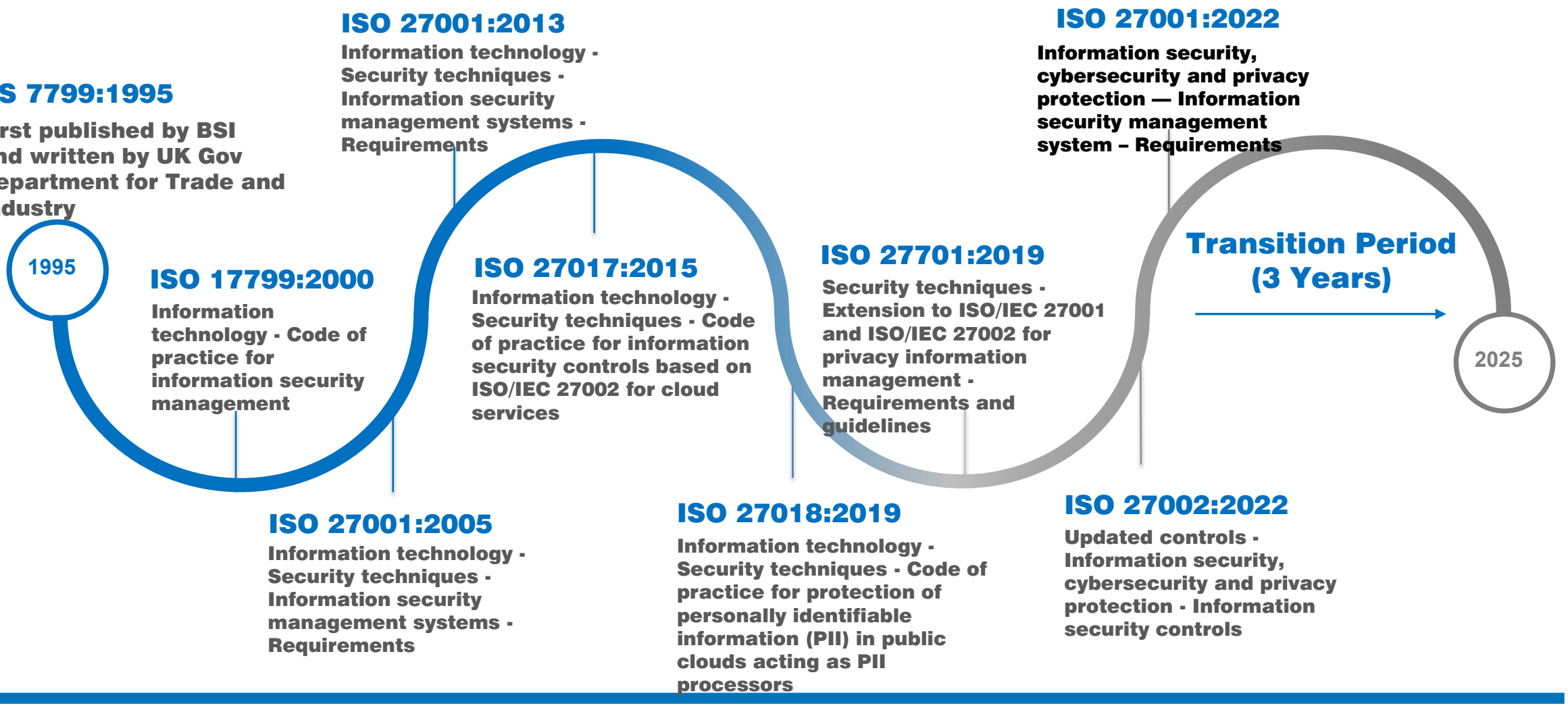
- **e-Learning** Introduction
- **1 day** Introduction Courses
- **2 day** Implementation Courses
- **2 day** Internal Auditor – NQA or IRCA
- **5 day** Lead Auditor – NQA or IRCA
- **Advanced** Training

CQI | IRCA
APPROVED TRAINING PARTNER

nqa.

nqa.
NEVER STOP IMPROVING

THE HISTORY OF ISO 27001



nqa
NEVER STOP IMPROVING

LANDSCAPE CHANGES

What are the main threats affecting the security of a business and its data?

Pre-2013	2022
• Hactivism • Script Kiddies • DoS/DDoS • Web Defacement • SQL Injections • Malware and Spyware	• High Value Data Theft • Ransomware • Organised Criminal Gangs • State Sponsored • Sophisticated Phishing • APTs • Cryptojacking

nqa
NEVER STOP IMPROVING

ISO 27001:2022 CLAUSES 4-10

New Requirement	Phase	Clause(s)	Activity	*(Client to Complete) Evidence of compliance*	*Complete) Has the Client Demonstrated they have Met the requirements of this clause?*		*(Assessor to Complete) Comments if Required*
					Yes	*No*	
A more explicit requirement for ensuring that interested parties and 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?				

nqa
NEVER STOP IMPROVING

ISO 27001:2022 CHANGES

- Information Security Policies
- Organisation of Information Security
- HR Security
- Asset Management
- Access Control
- Cryptographic Controls
- Physical Security
- Operational Security
- Communication Security
- System Acquisition, development and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Security Aspects of Business Continuity
- Compliance

nqa
NEVER STOP IMPROVING

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

nqa
NEVER STOP IMPROVING

ISO 27001:2022 NEW CONTROLS

Organisational Controls

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

Physical Controls

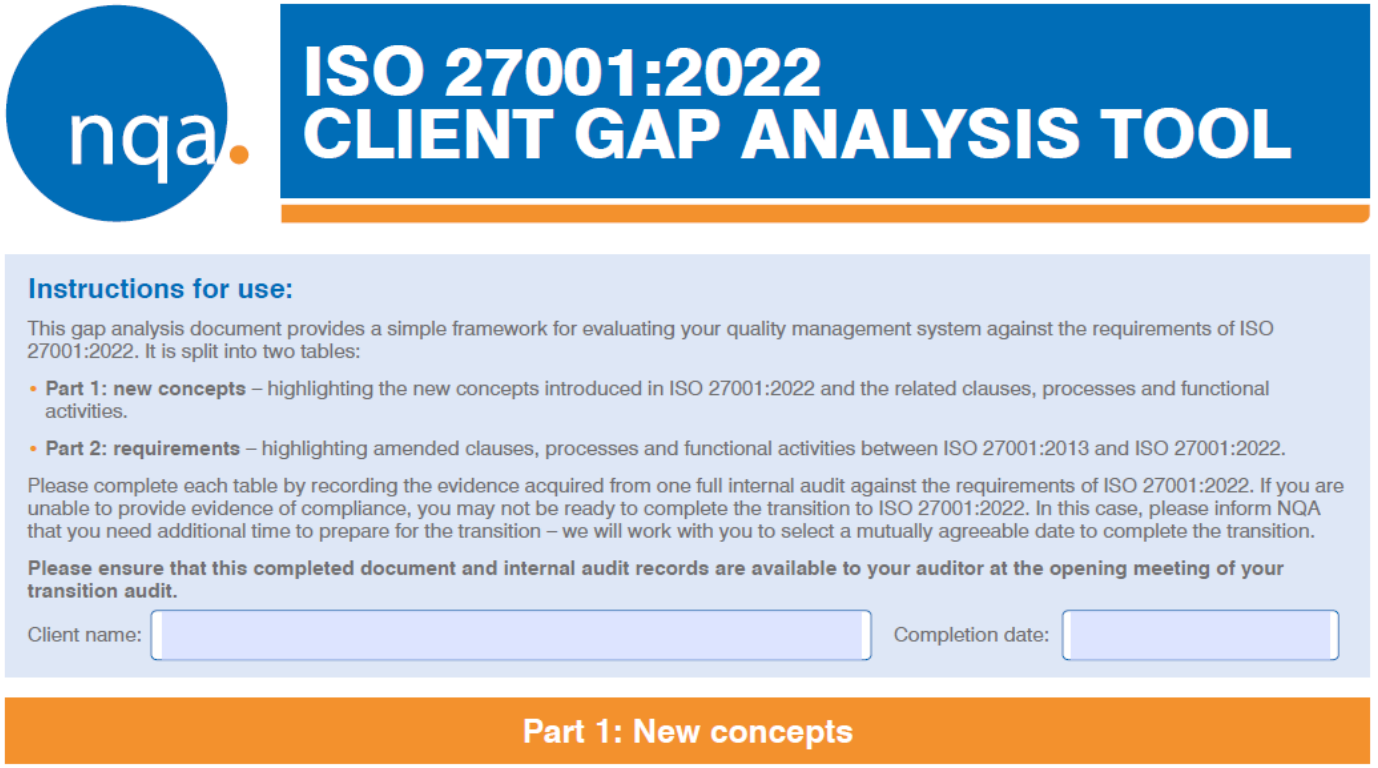
- 7.4 Physical Security Monitoring

Technical 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

NEVER STOP IMPROVING

ISO 27001:2022 NQA GAP TOOL



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

NEVER STOP IMPROVING

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 ☐	

NEVER STOP IMPROVING

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	

NEVER STOP IMPROVING

ISO 27001:2022 NQA GAP TOOL

New requirement	Phase	Control(s)	Activity
Security considerations and controls for cloud services.	Plan	5.23	Do you use any cloud services?
			How do you determine which cloud services are required by your organization and which cloud model is the best fit (IaaS, PaaS, SaaS, etc.)?
			What controls do you have in place to monitor the performance/effectiveness of your cloud service provider?
			Have you planned for changes to or termination of your cloud service(s) provider? What are your processes 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 ☐	

NEVER STOP IMPROVING

ISO 27001:2022 NQA GAP TOOL

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 ☐	

STATEMENT OF APPLICABILITY

- May be remapped
- Operational attributes can help

ISO 27002:2017 - ISO 27002:2022 MAPPING TOOL

The below mapping document outlines the relationship between the previous ISO 27002 controls and their 2022 counterparts.

		INFORMATION SECURITY CODE OF PRACTICE ISO 27002:2017		INFORMATION SECURITY CODE OF PRACTICE ISO 27002:2022
5	INFORMATION SECURITY POLICY	MERGED ISO27002:2017 CONTROLS	CONTROL REFERENCE	
5.1.1	Policies for Information Security	5.1.1, 5.1.2	5.1	Policies for information security
5.1.2	Review of the policies for information security	5.1.1, 5.1.2	5.1	Policies for information security
6.1	Internal Organisation			
6.1.1	Information security roles and responsibilities		5.2	Information security roles and responsibilities
6.1.2	Segregation of duties		5.3	Segregation of duties
6.1.3	Contact with authorities		5.5	Contact with authorities
6.1.4	Contact with special interest groups		5.6	Contact with special interest groups
			5.7 (new)	Threat intelligence
6.1.5	Information security in project management	6.1.5, 14.1.1	5.8	Information security in project management
6.2	Mobile devices and teleworking			
6.2.1	Mobile device policy		8.1	User endpoint devices
6.2.2	Teleworking		6.7	Remote working
7.1	Prior to employment			
7.1.1	Screening		6.1	Screening
7.1.2	Terms and conditions of employment		6.2	Terms and conditions of employment

#Governance	A.6 Organisation of information security
#Asset_management	A.8 Asset management
#Information_protection	
#Human_resource_security	A.7 Human resources security
#Physical_security	A.11 Physical and environmental security
#System_and_network_security	A.13 Communications security
#Application_security	A.14 Acquisition, development and maintenance
#Secure_configuration	
#Identity_and_access_management	A.9 Access control
#Threat_and_vulnerability	
#Continuity	A.17 Business continuity
#Supplier_relationships_security	A.15 Supplier relationships
#Legal_and_compliance	A.18 Compliance
#Information_security_event_management	A.16 Incident management
#Information_security_assurance	

ISO 27001:2022 Transition Policy - Timeline

Transition period begins

All current existing certificates to ISO 27001:2013 will expire three years from 31st Oct 2022

Transition period ends

Certificates for ISO 27001:2013 will no longer be valid from 01 Nov 2025

NQA to book future recertification audits as transitions

Any remaining transition audits should be completed (allowing suitable time for corrective actions and certificates to be issued).

nqa.

NEVER STOP IMPROVING

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 strongly encouraged 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**

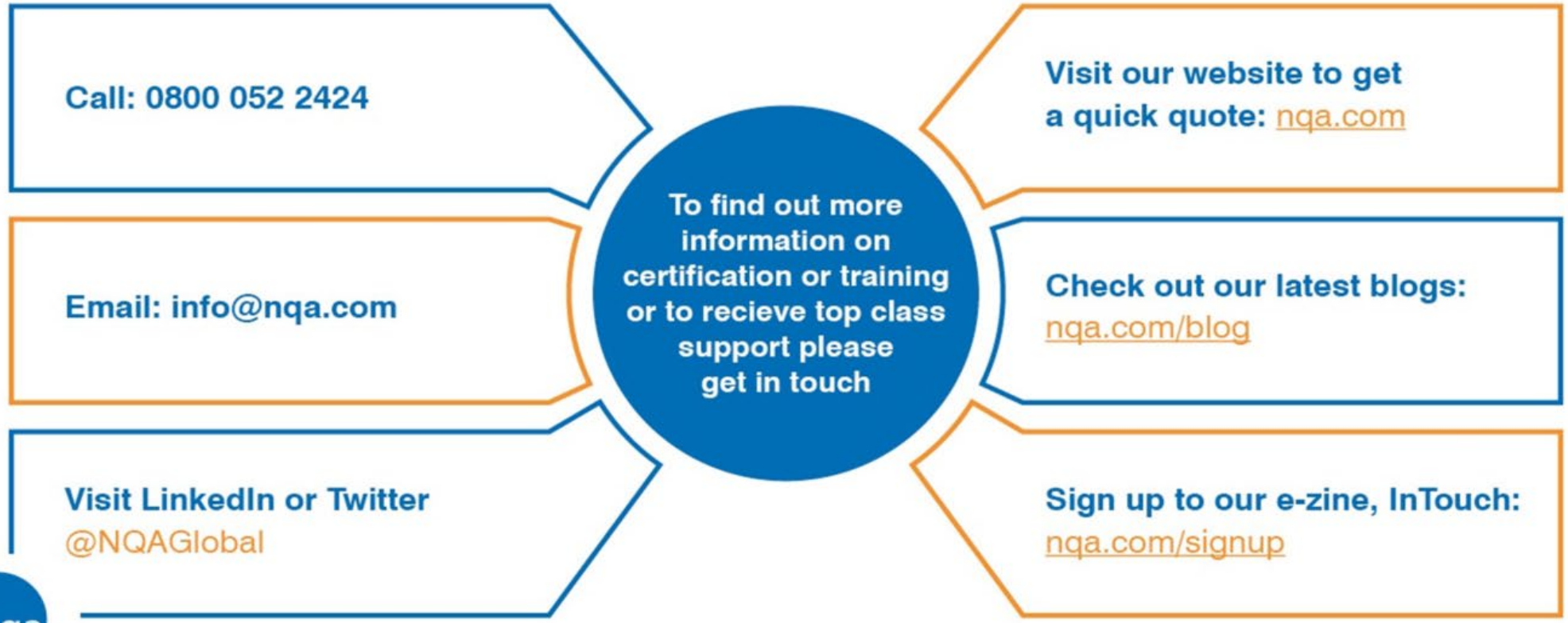
THANK YOU
ANY QUESTONS?

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

nqa.com/signup | youtube.com/nqamovies | twitter.com/NQAGlobal | linkedin.com/company/nqa-global

nqa.
NEVER STOP IMPROVING

FURTHER SUPPORT



nqa.
NEVER STOP IMPROVING