NQA ISO 27001:2022 TRANSITION

James Keenan
BU Lead, Information Security

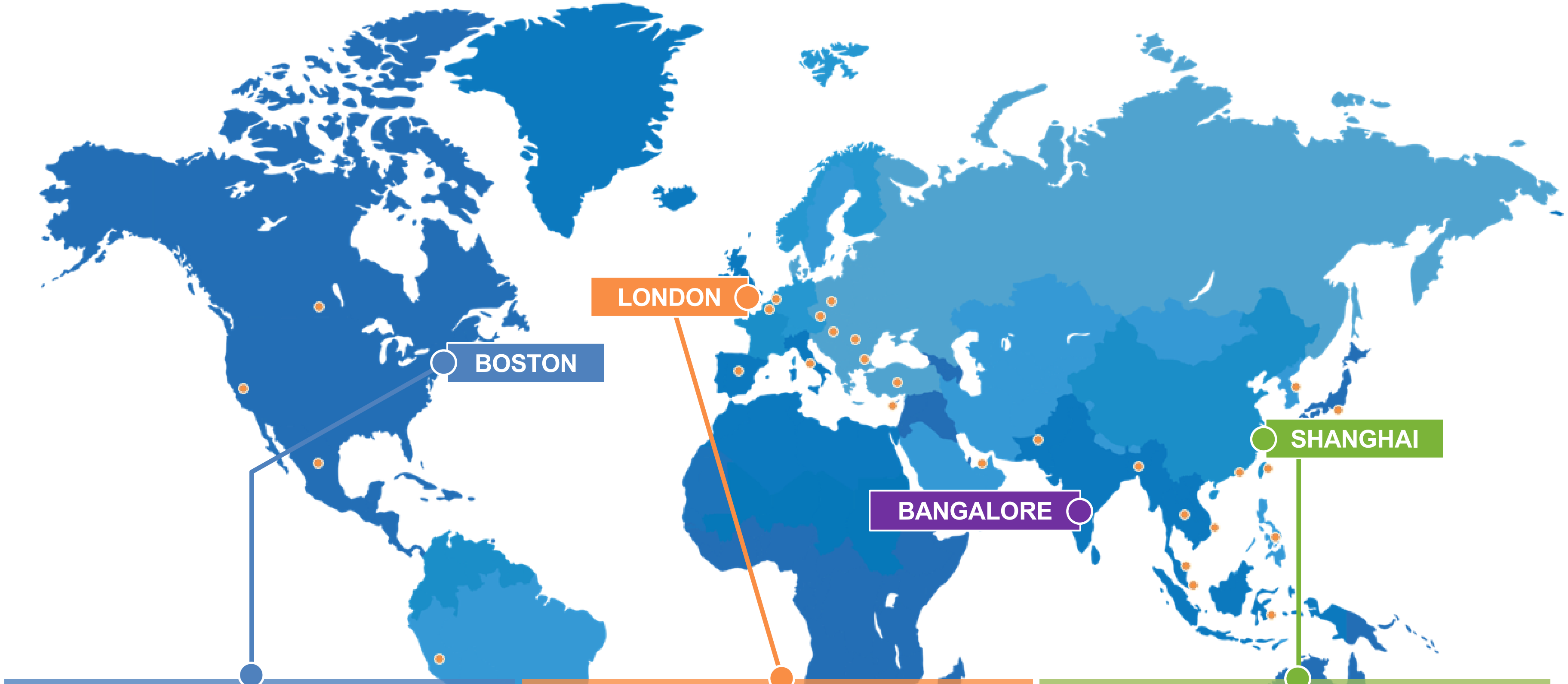
David Nutbrown
Principal Auditor ISO 27001

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

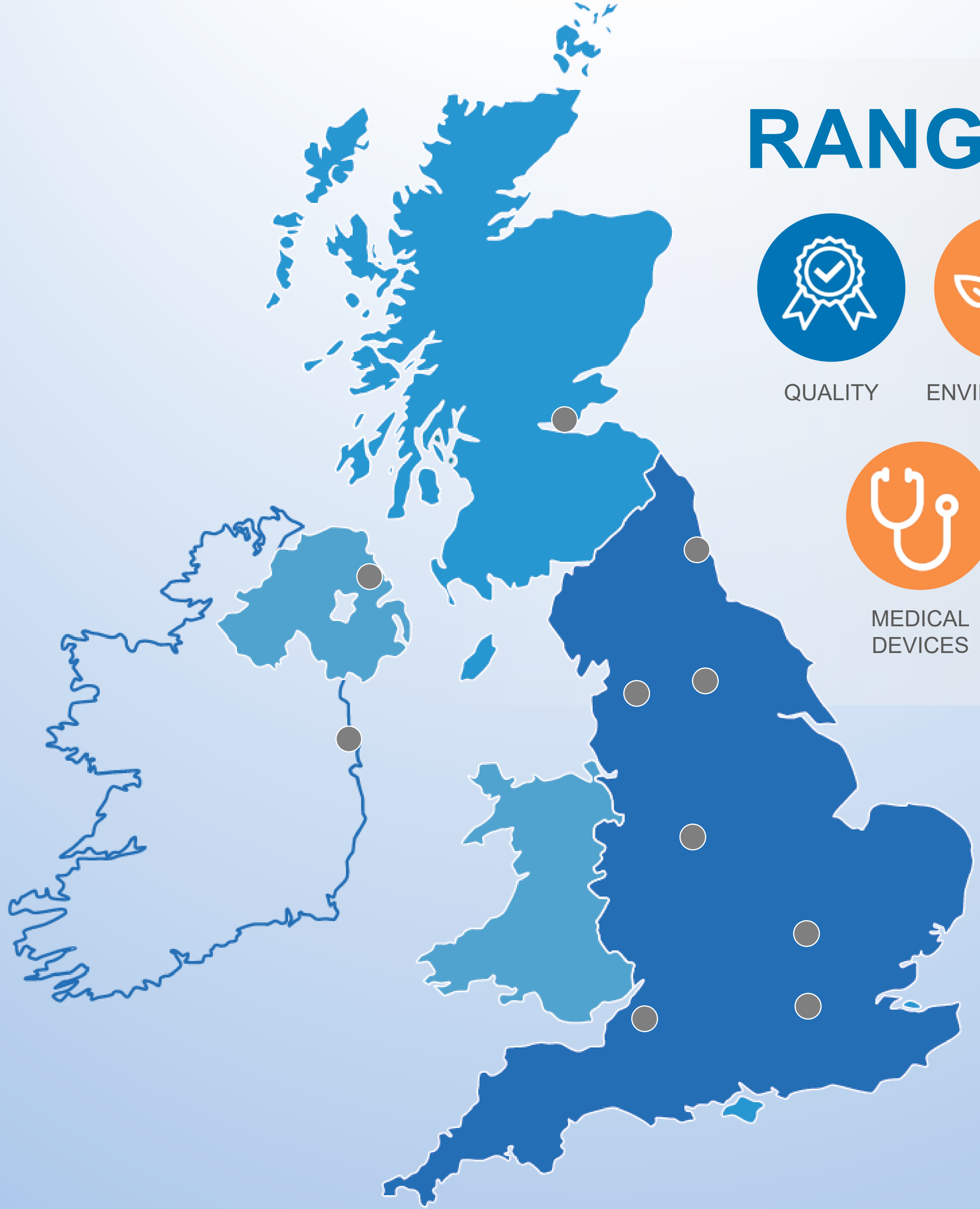
We specialize in management systems certification for:

- 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

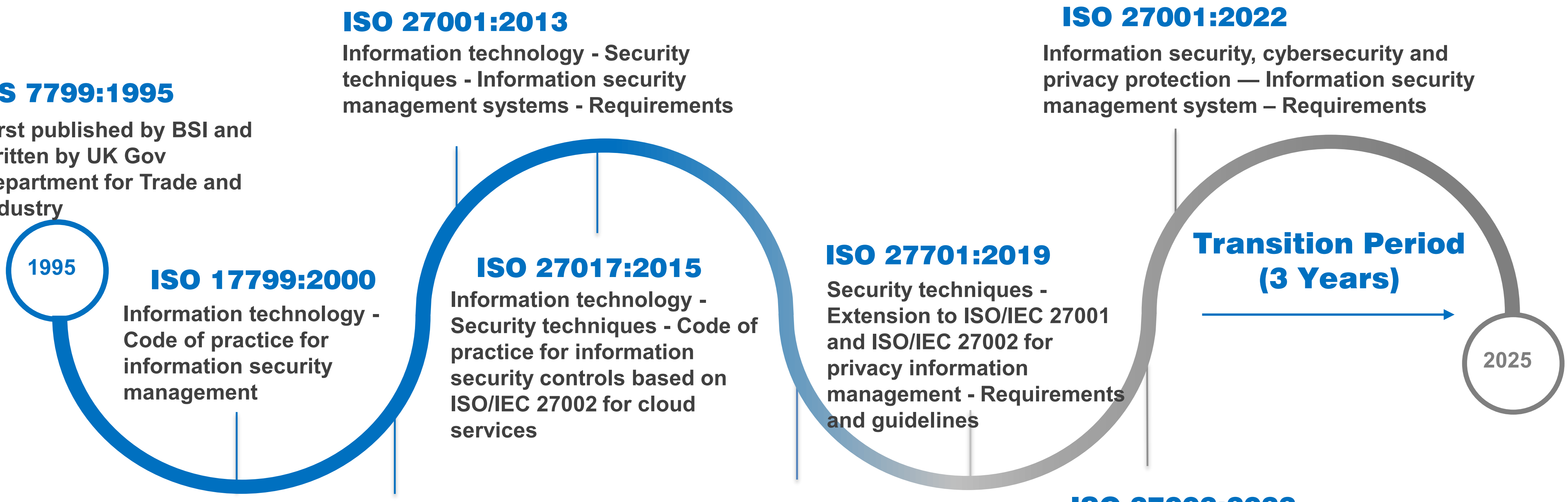
- QUALITY
- ENVIRONMENT
- ENERGY
- HEALTH AND SAFETY
- INFORMATION SECURITY
- MEDICAL DEVICES
- BUSINESS CONTINUITY
- AEROSPACE
- INTEGRATED MANAGEMENT

- **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

CQI | IRCA APPROVED TRAINING PARTNER

nqa.

THE HISTORY OF ISO 27001



BS 7799:1995

First published by BSI and written by UK Gov Department for Trade and Industry

ISO 17799:2000

Information technology - Code of practice for information security management

ISO 27001:2005

Information technology - Security techniques - Information security management systems - Requirements

ISO 27001:2013

Information technology - Security techniques - Information security management systems - Requirements

ISO 27017:2015

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

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 27701:2019

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

ISO 27001:2022

Information security, cybersecurity and privacy protection — Information security management system – Requirements

ISO 27002:2022

Updated controls - Information security, cybersecurity and privacy protection - Information security controls

LANDSCAPE CHANGES

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

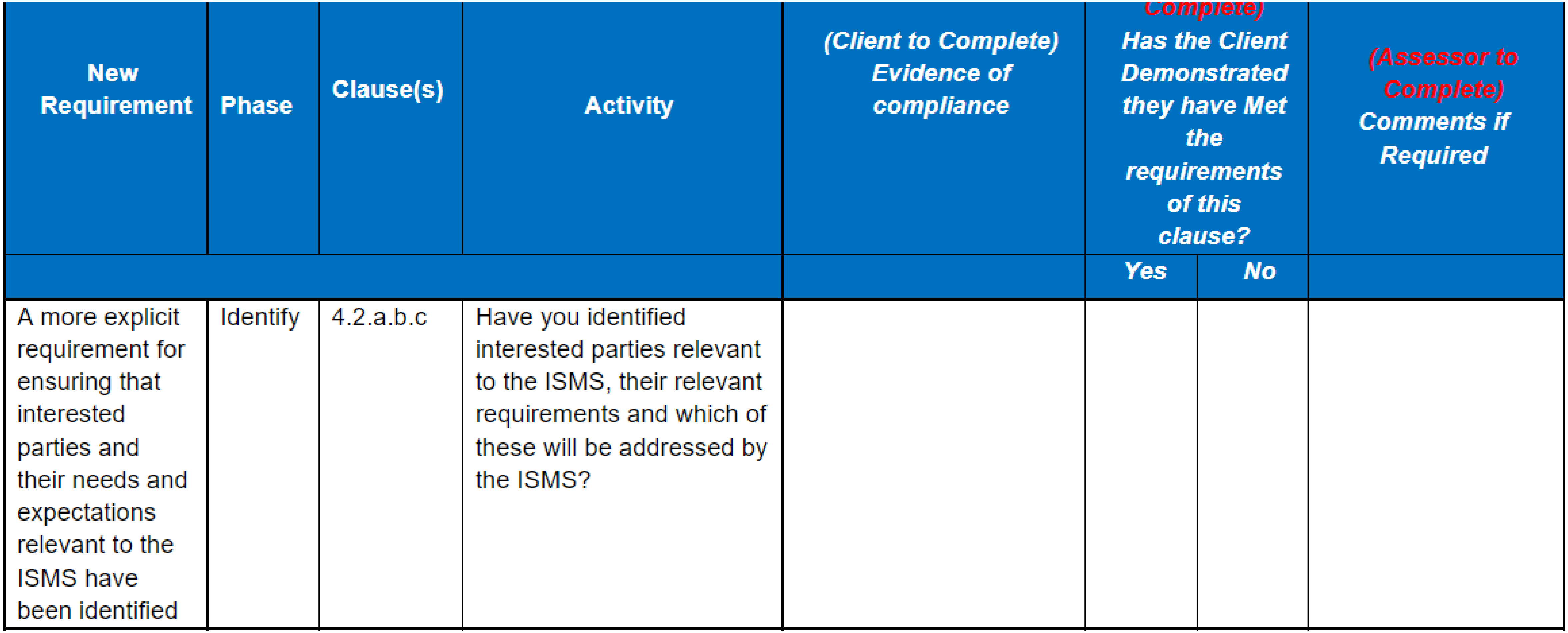
Pre-2013

- Hactivism
- Script Kiddies
- DoS/DDoS
- Web Defacement
- SQL Injections
- Malware and Spyware

2022

- High Value Data Theft
- Ransomware
- Organised Criminal Gangs
- State Sponsored
- Sophisticated Phishing
- APTs
- Cryptojacking

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?				

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

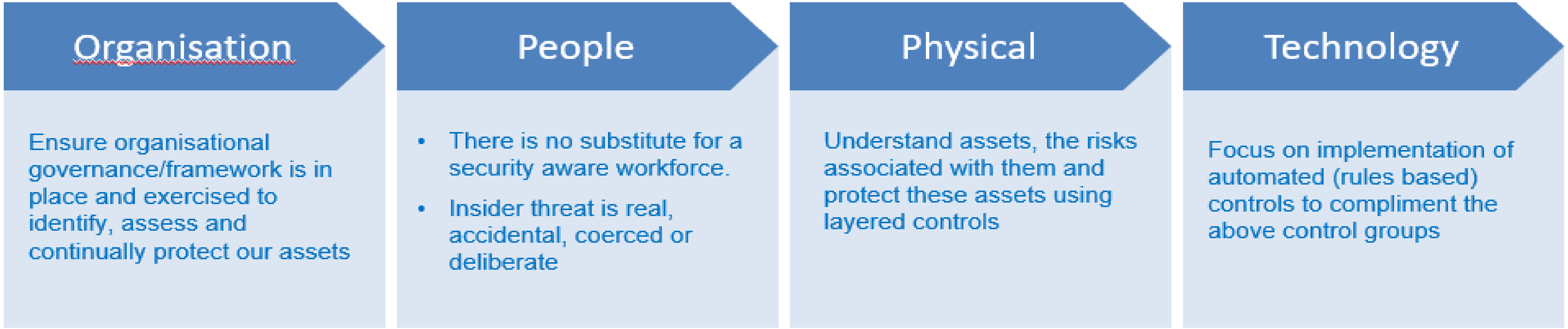
Supplier Relationships

Information Security Incident Management

Security Aspects of Business Continuity

Compliance

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

nqa.
NEVER STOP IMPROVING

ISO 27001:2022 NEW CONTROLS

Infosec and Cloud Services

- Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.
- To specify and manage information security for the use of cloud services.
- Understand and address risks associated with cloud storage/services.

DATA LEAKAGE PREVENTION

- Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.
- To detect and prevent the unauthorised disclosure and extraction of information by individuals or systems.

nqa.
NEVER STOP IMPROVING

ISO 27001:2022 NEW CONTROLS

MONITORING ACTIVITIES

- Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
- To detect anomalous behaviour and potential information security incidents.
- Horizon Scanning and understanding the norm vs the abnormal.

THREAT INTELLIGENCE

- Information relating to information security threats should be collected and analysed to produce threat intelligence.
- To provide awareness of the organisation's threat environment so that the appropriate mitigation actions can be taken.
- Allow risk assessed decision making when determining security control measures

NEVER STOP IMPROVING

ISO 27001:2022 NEW CONTROLS

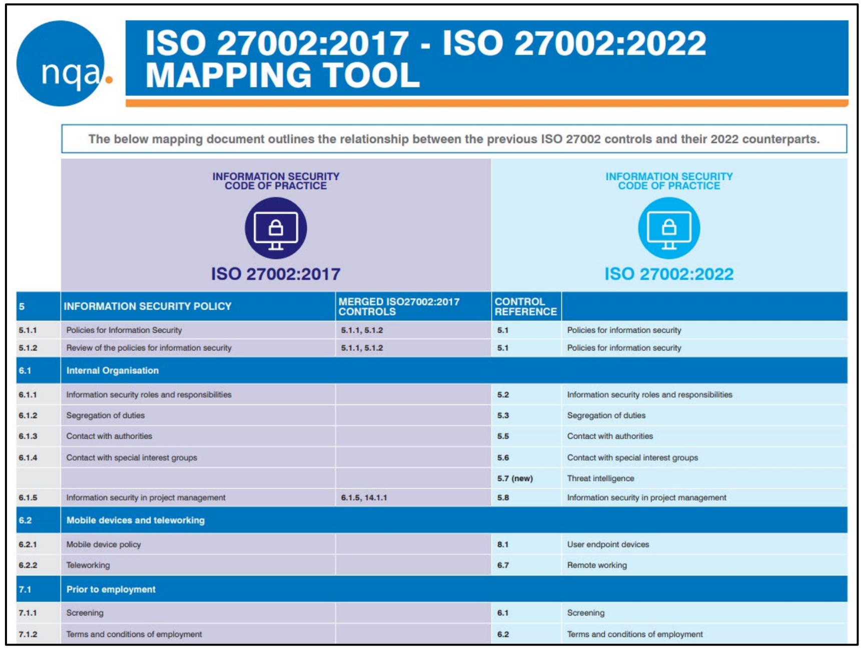
ICT READINESS FOR BC

- ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.
- To ensure the availability of the organisation's information and other associated assets during disruption.

nqa.
NEVER STOP IMPROVING

STATEMENT OF APPLICABILITY

- May be remapped
- Operational attributes can help



nqa.

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	

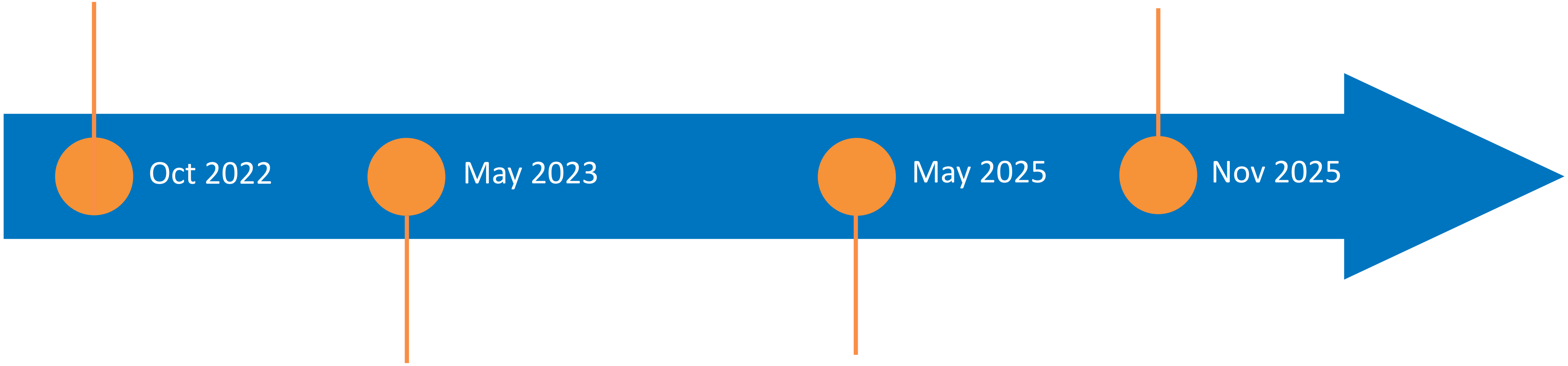
ISO 27001:2022 TRANSITION POLICY - TIMELINE

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).

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

NEVER STOP IMPROVING

Q&A

TAKE THE NEXT STEP

INFORMATION. SECURED.

Discover how NQA can help you achieve your information security goals with an ISO 27001 / ISO 27701 training course.

Book your place here!

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