nqa.

a kiwa company

# WEBINAR: Understanding the ISO 27001 Controls and Annex A

15th October 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

# PRESENTER INFORMATION

**SARAH CLYDE**
NQA Tutor (ISMS)

## KEY INFORMATION

- 20 years in IT and Information Security
- **ISO 27001** & **ISO 22301** Lead Auditor
- ISACA Silver Member:
  - **CISM** (Certified Information Security Manager)
  - **CRISC** (Certified in Risk and Information Systems Control)
  - CGEIT (Certified in the Governance of Enterprise IT)
- COBIT 2019 / ITIL 4 certificates
- Member of the Institute of Leadership (MIoL)

# WEBINAR AGENDA

## OBJECTIVES

- Provide an overview of ISO 27001:2022 Annex A and its control structure
- Recognise the changes introduced in the 2022 revision, including the 4 control themes
- Explain the relationship between the clauses and the controls
- Highlight how Annex A supports a risk-based approach to information security

## OUTCOMES

- Appreciate the role of Annex A in supporting an Information Security Management System (ISMS)
- Identify the four themes and examples of controls within each theme
- Understand the difference between the mandatory requirements and the selectable controls within Annex A
- Relate the Annex A controls to practical scenarios in your own organisations

# WHAT IS ISO 27001?

## INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

- An **internationally recognised standard** for managing information security
- Focuses on protecting the Confidentiality, Integrity and Availability (**CIA**) of information, in all forms (digital, printed and verbal)
- Follows a **risk-based approach** to security
- Aligns with the **PDCA** (Deming) cycle - Plan, Do, Check, Act
- Split into **clauses** (mandatory requirements) and **information security controls** (Annex A)

# WHAT IS ANNEX A?

## INFORMATION SECURITY CONTROLS REFERENCE

- A table containing a list of **93** commonly used **information security controls**
- The controls are grouped into **4 themes**:

  - **Organisational**
  - **People**
  - **Physical**
  - **Technological**

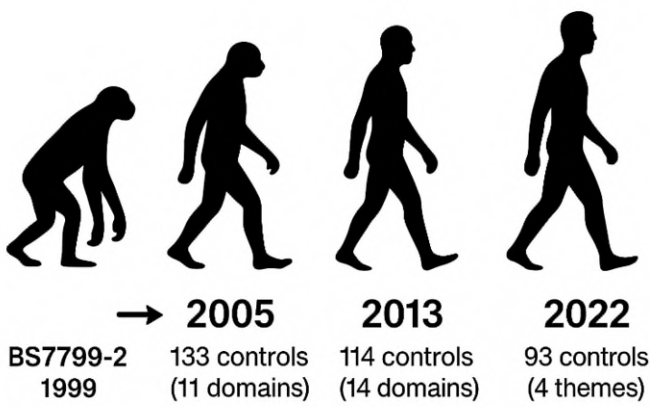
- The controls in ISO 27001 are directly derived and aligned with those listed in **ISO 27002:2022** clauses 5 to 8
- Information security controls are **designed to treat information security risks**

# EVOLUTION OF ANNEX A CONTROLS

| | |
|---|---|
| ISO 27001:2005 → 133 controls | 11 domains |
| ISO 27001:2013 → 114 controls | 14 domains |
| **ISO 27001:2022 → 93 controls** | **4 themes** |

## KEY DIFFERENCES:

- A reduction in the overall volume of control references
- Themes have replaced domains, simplifying the structure
- 11 new controls introduced to bring it up to date



# ORGANISATIONAL CONTROLS

## POLICIES, GOVERNANCE (OVERSIGHT), PROCESSES AND COMPLIANCE:

5.1 Policies for information security

5.2 Information security roles and responsibilities

5.3 Segregation of duties

5.4 Management responsibilities

5.5 Contact with authorities

5.6 Contact with special interest groups

**5.7 Threat intelligence**

5.8 Information security in project management

5.9 Inventory of information and other associated assets

5.10 Acceptable use of information and other associated assets

5.11 Return of assets

5.12 Classification of information

5.13 Labelling of information

5.14 Information transfer

5.15 Access control

5.16 Identity management

5.17 Authentication information

5.18 Access rights

5.19 Information security in supplier relationships

5.20 Addressing information security within supplier agreements

5.21 Managing information security in the ICT supply chain

5.22 Monitoring, review and change management of supplier services

**5.23 Information security for use of cloud services**

5.24 Information security incident management planning and preparation

5.25 Assessment and decision on information security events

5.26 Response to information security incidents

5.27 Learning from information security incidents

5.28 Collection of evidence

5.29 Information security during disruption

**5.30 ICT readiness for business continuity**

5.31 Identification of legal, statutory, regulatory and contractual requirements

5.32 Intellectual property rights

5.33 Protection of records

5.34 Privacy and protection of PII

5.35 Independent review of information security

5.36 Compliance with policies and standards for information security

5.37 Documented operating procedures

# PEOPLE CONTROLS

## HUMAN FACTOR SECURITY - FOCUS ON PERSONNEL AND BEHAVIOURS:

6.1 Screening

6.2 Terms and conditions of employment

6.3 Information security awareness, education and training

6.4 Disciplinary process

6.5 Responsibilities after termination or change of employment

6.6 Confidentiality or non-disclosure agreements

6.7 Remote working

6.8 Information security event reporting

# PHYSICAL CONTROLS

## PHYSICAL PROTECTION OF INFORMATION, FACILITIES AND EQUIPMENT:

7.1 Physical security perimeter

7.2 Physical entry controls

7.3 Securing offices, rooms and facilities

**7.4 Physical security monitoring**

7.5 Protecting against physical and environmental threats

7.6 Working in secure areas

7.7 Clear desk and clear screen

7.8 Equipment siting and protection

7.9 Security of assets off-premises

7.10 Storage media

7.11 Supporting utilities

7.12 Cabling security

7.13 Equipment maintenance

7.14 Secure disposal or re-use of equipment

# TECHNOLOGICAL CONTROLS

## PROTECTING DIGITAL INFORMATION AND NETWORKS USING TECHNICAL SAFEGUARDS:

8.1 User endpoint devices

8.2 Privileged access rights

8.3 Information access restriction

8.4 Access to source code

8.5 Secure authentication

8.6 Capacity management

8.7 Protection against malware

8.8 Management of technical vulnerabilities

**8.9 Configuration management**

**8.10 Information deletion**

**8.11 Data masking**

**8.12 Data leakage prevention**

8.13 Information backup

8.14 Redundancy of information processing facilities

8.15 Logging

**8.16 Monitoring activities**

8.17 Clock synchronisation

8.18 Use of privileged utility programs

8.19 Installation of software on operational systems

8.20 Network controls

8.21 Security of network services

8.22 Segregation in networks

**8.23 Web filtering**

8.24 Use of cryptography

8.25 Secure development life cycle

8.26 Application security requirements

8.27 Secure system architecture and engineering principles

**8.28 Secure coding**

8.29 Security testing in development and acceptance

8.30 Outsourced development

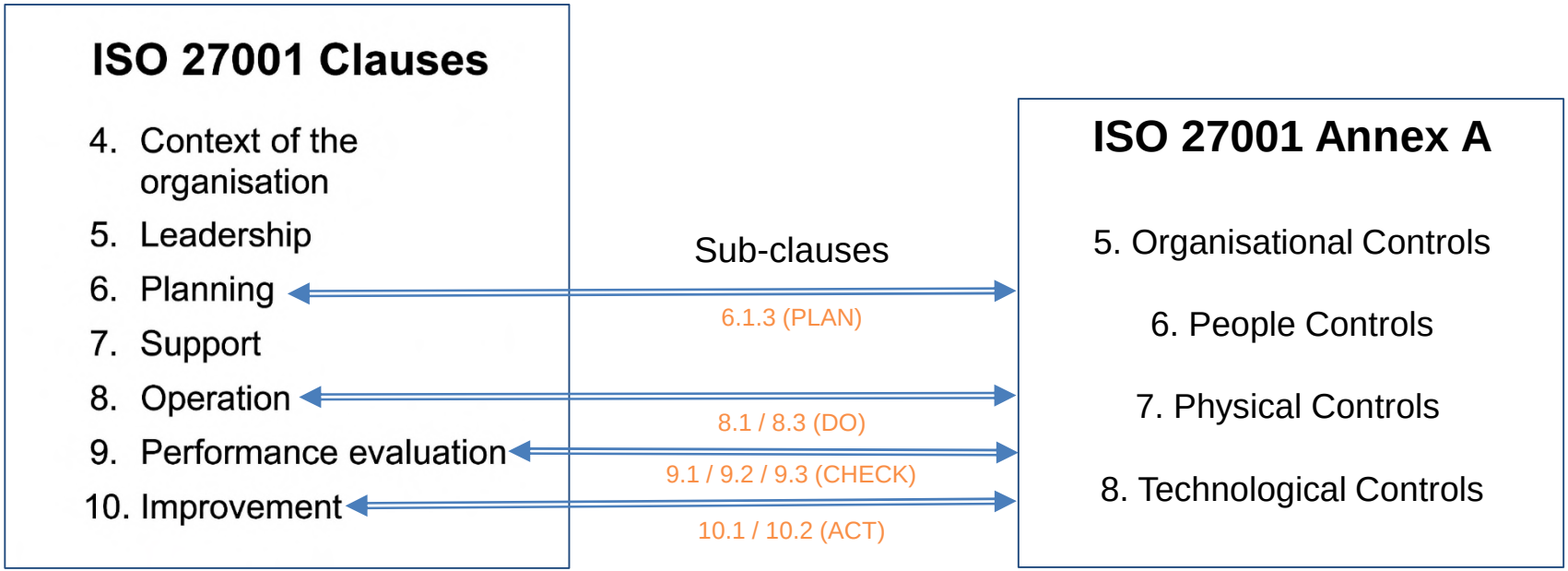
8.31 Separation of development, test and production environments

8.32 Change management

8.33 Test information

8.34 Protection of information systems during audit testing

# LINKAGE BETWEEN CLAUSES AND CONTROLS



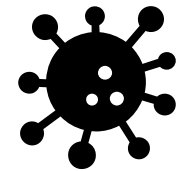
# CONTROL SELECTION

## RISK TREATMENT – CLAUSE 6.1.3

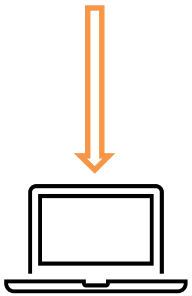
- Perform risk assessment and select appropriate risk treatment options
- **Determine the controls** necessary for the risk treatment options considering the risk assessment results:
  - Controls can be selected from any source (e.g., ISO 27002)
  - Controls can be designed by the organisation
- Compare the selected controls with those listed in Annex A to **verify that no necessary controls have been omitted** (NOTE – ANNEX A is not an exhaustive list - additional controls can be applied where necessary)
- Produce a Statement of Applicability (**SoA**) to include:
  - The necessary controls
  - The justification for inclusion / exclusion
  - Whether the necessary controls are implemented or not

# CONTROL COMBINATIONS EXAMPLE

## TO MITIGATE THE RISK OF **A MALWARE INFECTION ON AN END-USER DEVICE** THE FOLLOWING CONTROLS COULD BE CONSIDERED:



VIRUS



LAPTOP

### TECHNOLOGICAL

- 8.1 User endpoint devices
- 8.7 Protection against malware
- 8.8 Management of technical vulnerabilities
- 8.9 Configuration management
- 8.16 Monitoring activities
- 8.19 Installation of software on operational systems
- 8.23 Web filtering

### ORGANISATIONAL

- 5.1 Policies for information security
- 5.7 Threat intelligence
- 5.24 Information security incident management planning and preparation

### PEOPLE

- 6.3 Information security awareness, education and training
- 6.8 Information security event reporting

### PHYSICAL

- 7.8 Equipment siting and protection

When determining controls, consider how they interact with one another. Controls to mitigate a single risk can be:

- **Complementing Controls**
- **Converging Controls**
- **Compensating Controls**

# ATTRIBUTES (ISO/IEC 27002:2022)

- Can be used to used to filter, sort or present controls in different views
- Can also help with mapping controls to other frameworks and standards

| ATTRIBUTE | DESCRIPTION |
|---|---|
| Control Type | How the control modifies risk in the relation to an information security incident (Preventive, Detective and Corrective) |
| Information Security Properties | Which properties of information security the control is designed to preserve (Confidentiality, Integrity and Availability) |
| Cyber Security Concepts | How the controls align to cyber security concepts (Identify, Protect, Detect, Respond and Recover) |
| Operational Capabilities | To view the controls from the perspective of the information security capabilities (Governance, Asset Management, Information Protection, Human Resource Security, Physical Security, System and Network Security, Application Security, Secure Configuration, Identity & Access Management, Threat and Vulnerability Management, Continuity, Supplier Relationships Security, Legal & Compliance, Information Security & Event Management and Information Security Assurance) |
| Security Domains | To view the controls from the perspective of 4 information security domains (Governance and Ecosystem, Protection, Detection and Resilience) |

# CONCLUSION

- Annex A provides a list of **common control references** that can be used to modify or maintain risk
- Annex A is **a flexible tool kit** to support an organisation's unique risk landscape
- The 2022 update reflects **modern threats and technologies**, making it more relevant than ever
- The security controls referenced in Annex A can be used independently, but they work more effectively as part of a **structured information security management system**
- Annex A empowers organisations to build **resilient, risk-focused, and compliant security practices**

# SUMMARY OF LEARNINGS

- Gained a clearer understanding of the structure of ISO 27001 Annex A
- Recognised the shift from domains to themes and the rationale behind the 2022 update
- Appreciate how Annex A supports a risk-based approach to information security
- Understood how the controls can be applied to mitigate real-world information security incidents
- Gained an awareness of the control attributes and how they can be used in practical terms

# TRAINING OFFERED

| STANDARD | TRAINING |
| --- | --- |
| **ISO 27001** | NQA ISO 27001 Understanding Annex A Controls |
| **ISO 27001** | Introduction, Implementation, Internal Auditor, Lead & Lead Auditor Conversion Courses (CQI & IRCA) |
| **ISO 27701** | Introduction and Implementation |
| **ISO 42001** | 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:
training@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