ISO 27002:2022 – A GUIDE TO THE CHANGES

Tim Pinnell

NEVER STOP IMPROVING

YOUR PRESENTER

KEY INFO

- 45 minute webinar
- Questions in the chat box
- Q&A at the end
- Recording of webinar circulated shortly

Tim Pinnell

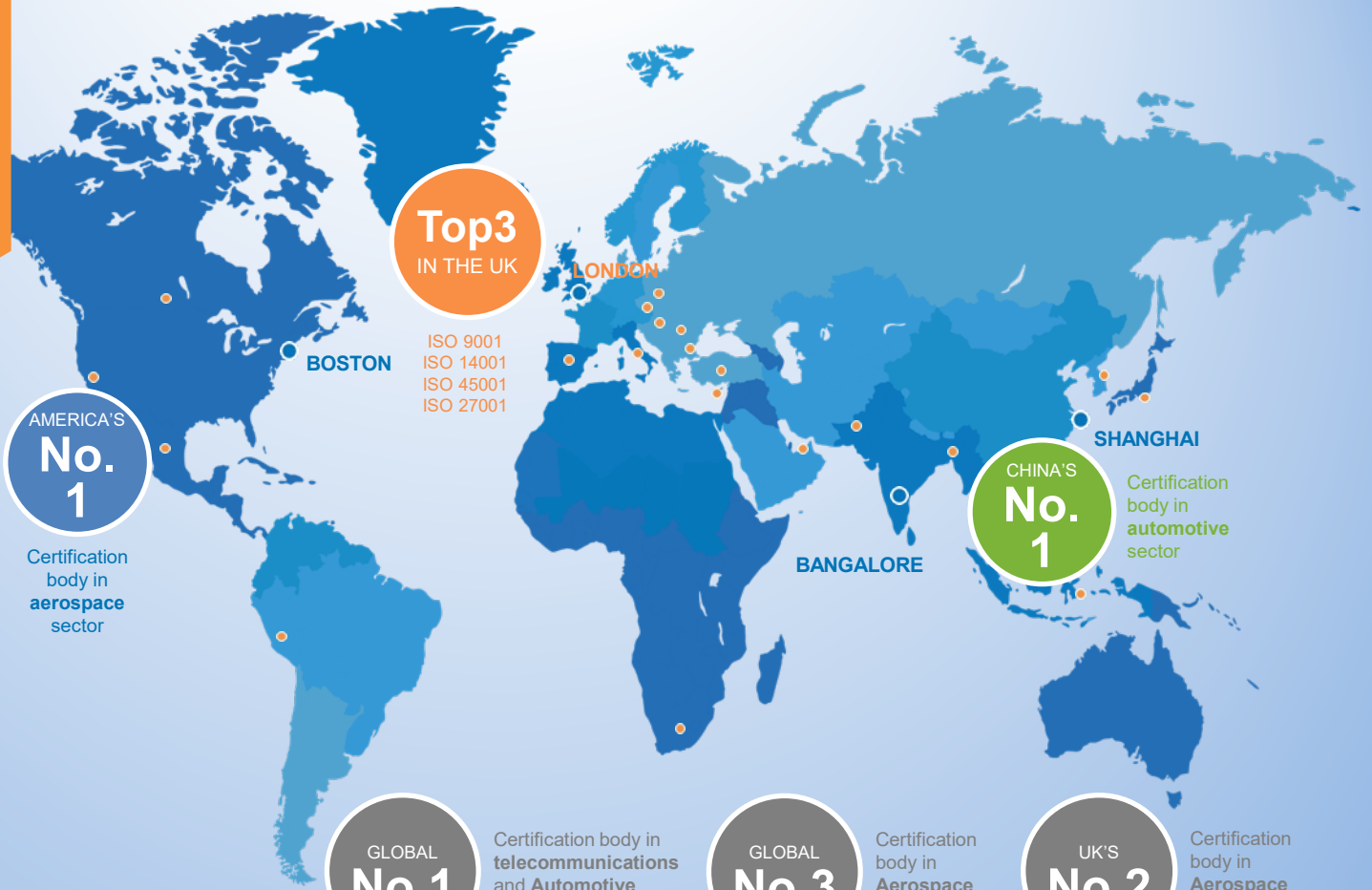
BSc, MSc, PCIP, CIPP/E, CISMP, Information Security

NQA Information Security Assurance Manager

Tim has worked in telecommunications cyber and information security for over twenty years. From the early World Wide Web days to today's globally connected information services, Tim brings a wealth of experience in security, compliance and governance. Throughout his career he has played a leading role in adopting, consulting and implementing information security compliance standards, including ISO 27001, PCIDSS and Cyber Essentials, helping organizations understand the risks facing their businesses and the controls needed to mitigate them.

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.

nqa.

nqa.

NEVER STOP IMPROVING

50,000
CERTIFICATES
GLOBALLY

100%
ALL INCLUSIVE
FEES

1000+
EMPLOYEES
WORLDWIDE

10
YEARS
AVERAGE
CUSTOMER
PARTNERSHIP

OVER **90**
OPERATING
COUNTRIES

WHAT WE WILL COVER TODAY

- A quick overview of 27002
- The changes to 27002
- New controls
- ISMS implications
- Implications for other 27k standards
- Transition timelines
- Q&A

nqa.
NEVER STOP IMPROVING

THE STANDARD: ISO 27002

nqa.
NEVER STOP IMPROVING

ISO 27001 & ISO 27002

Management System - Requirements

ISO 27001:2013
Information security management systems - Requirements

Management System
4. Context
5. Leadership
6. Planning
7. Support
8. Operations
9. Performance
10. Improvement

Annex A (114 controls)
5. Policies
6. Organisation
7. Human resources
8. Asset management
9. Access Control
10. Cryptography
11. Physical
12. Operations
13. Communications
14. Dev and maintenance
15. Suppliers
16. Incidents
17. Business Continuity
18. Compliance

Code of practice - Guidance

ISO 27002:2017
Code of practice for information security controls

114 controls
5. Policies
6. Organisation
7. Human resources
8. Asset management
9. Access Control
10. Cryptography
11. Physical
12. Operations
13. Communications
14. Dev and maintenance
15. Suppliers
16. Incidents
17. Business Continuity
18. Compliance

nqa.
NEVER STOP IMPROVING

REQUIREMENTS VS. GUIDANCE

Management System - Requirements

ISO 27001:2013
Information security management systems - Requirements

A.8.2.2	Labelling of information	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Code of practice - Guidance

ISO 27002:2017
Code of practice for information security controls

8.2.2 Labelling of information

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

"Implementation guidance"

Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established in 8.2.1. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information to reduce workloads. Employees and contractors should be made aware of labelling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information

Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and metadata are a common form of labelling.

Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.

nqa.
NEVER STOP IMPROVING

THE CHANGES ISO27002:2022

THE CHANGES TO 27002: TITLE

2017	Information technology – Security techniques – Code of practise for information security controls (ISO/IEC 27002:2013)
2022	Information security, cybersecurity and privacy protection – Information security controls

NEVER STOP IMPROVING

THE CHANGES TO 27002: CONTROL GROUPS

2017

14 Control Groups

Control Groups	
5. Policies	12. Operations
6. Organisation	13. Communications
7. Human resources	14. Dev and maintenance
8. Asset management	15. Suppliers
9. Access Control	16. Incidents
10. Cryptography	17. Business Continuity
11. Physical	18. Compliance

2022

4 Themes

Theme clauses	
5. Organisational	7. Physical
6. People	8. Technology

THE CHANGES TO 27002: NO GROUP OBJECTIVES

2017

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

THE CHANGES TO 27002: CONTROLS

2017 114 controls

19 controls consolidated
11 new controls
n deleted controls?

2022 93 controls

THE CHANGES TO 27002: ATTRIBUTES

Attributes are used to create different views of the controls

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identity #Protect #Detect #Respond #Recover	#Governance #Asset_management #Information_protection #Human_resource_security #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability #Continuity #Supplier_relationships_security #Legal_and_compliance #Information_security_event_management #Information_security_assurance	#Governance_and_Ecosystem #Protection #Defence #Resilience

THE CHANGES TO 27002: ATTRIBUTES

Attributes are used to create different views of the controls

8.6 Capacity management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_Ecosystem #Protection

Control

The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

THE CHANGES TO 27002: ATTRIBUTES

You can create your own attributes
You can ignore those in the standard

For example:

1. Assign risk references to the controls treating specific risks
2. Maturity implementation level
3. Implementation state
4. Responsible department

Control	Treating risk	Implementation maturity	Implementation state	Responsible department	Information security properties	Operational capabilities
5.7 Threat intelligence	#6 #15	#Level_2	#Partially_implemented	#CISO	#Confidentiality #Integrity #Availability	#Threat_and_vulnerability_management
5.8 Information security in project management	#2	#Level_3	#Fully_implemented	#CISO #CSO	#Confidentiality #Integrity #Availability	#Governance

nqa.
NEVER STOP IMPROVING

NEW CONTROLS

THE CHANGES TO 27002: NEW CONTROLS

5.7 Threat intelligence

Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

THE CHANGES TO 27002: NEW CONTROLS

5.23 Information security for use of cloud services

Control

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Purpose

To specify and manage information security for the use of cloud services.

THE CHANGES TO 27002: NEW CONTROLS

5.30 ICT readiness for business continuity

Control

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Purpose

To ensure the availability of the organization's information and other associated assets during disruption.

THE CHANGES TO 27002: NEW CONTROLS

7.4 Physical security monitoring

Control

Premises should be continuously monitored for unauthorized physical access.

Purpose

To detect and deter unauthorized physical access.

THE CHANGES TO 27002: NEW CONTROLS

8.9 Configuration management

Control

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

Purpose

To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

THE CHANGES TO 27002: NEW CONTROLS

8.10 Information deletion

Control

Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

Purpose

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

THE CHANGES TO 27002: NEW CONTROLS

8.11 Data masking

Control

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Purpose

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

THE CHANGES TO 27002: NEW CONTROLS

8.12 Data leakage prevention

Control

Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

THE CHANGES TO 27002: NEW CONTROLS

8.16 Monitoring activities

Control

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Purpose

To detect anomalous behaviour and potential information security incidents.

THE CHANGES TO 27002: NEW CONTROLS

8.23 Web filtering

Control

Access to external websites should be managed to reduce exposure to malicious content.

Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

THE CHANGES TO 27002: NEW CONTROLS

8.28 Secure coding

Control

Secure coding principles should be applied to software development.

Purpose

To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.

nqa.
NEVER STOP IMPROVING

ISMS IMPLICATIONS

RISK ASSESSMENT & TREATMENT

- You will need to review your risk assessment

ISO 27001: Clause 8.2

The organisation shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur.

- You will need to review your SoA and risk treatment plan:-

ISO 27001: Clause 6.1.3

b) Determine all controls that are necessary to implement the information security risk treatment options

c) Compare the controls determined in 6.1.3 b) with those in Annex A and verify that no necessary controls have been omitted

d) Produce a statement of applicability

e) Formulate an information security risk treatment plan

NEVER STOP IMPROVING

STATEMENT OF APPLICABILITY

You will need to remap

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	

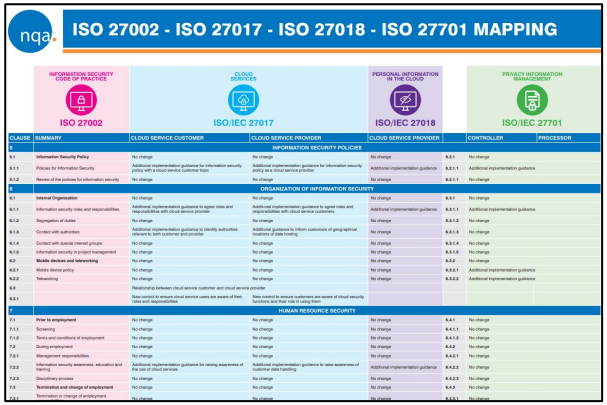
IMPLICATIONS FOR OTHER STANDARDS

NEVER STOP IMPROVING

ISO 27017
CLOUD SERVICES SECURITY

Cloud Services Customer	
33	5
It extends the controls in **27002**	and provides new controls
31	7
Cloud Services Provider	

There are no plans to change these standards



ISO 27701
PRIVACY INFORMATION MANAGEMENT

ISO 27018
PROCESSOR CLOUD PRIVACY

PII Processors	
It extends the controls in **27002**	and provides new controls
16	13 – Security 12 - Privacy

PII Controllers		
6	37	31
It extends the clauses in **27001**	It extends the controls in **27002**	and provides new controls
6	37	18
PII Processors		

nqa.
NEVER STOP IMPROVING

TRANSITION TIMELINE

TIMELINE TBC

Transition period begins

All current existing certificates to ISO 27001:2013 will expire two years from the last day of the month of the release and publication of the updated version of ISO 27001.

Transition period ends

Certificates for ISO 27001:2013 will no longer be valid

CB's must cease conducting initial and recertification audits. As such, all initial and recertification audits occurring after this date must be conducted against the updated version.

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

nqa.
NEVER STOP IMPROVING

Q&A

nqa.
NEVER STOP IMPROVING

THANK YOU

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