CQI | IRCA

LEADING QUALITY SINCE 1919

ISO/IEC 27001 – What the latest edition means for you

22 November 2022

Richard Green – Founder and Managing Director
Kingsford Consultancy Services Limited

Agenda

CQI | IRCA
LEADING QUALITY SINCE 1919

1. Welcome, introductions, objectives
2. The changes
3. The implications
4. Future trends
5. Opportunity for questions

CQI | IRCA
LEADING QUALITY SINCE 1919

Welcome, introductions and objectives

Welcome and introductions

CQI | IRCA
LEADING QUALITY SINCE 1919

Richard Green

MD of Kingsford Consultancy Services Limited

Former Head of Technical Services CQI/IRCA

BS and ISO Standards writer – IST/33/1 and JTC 1/SC 27/WG 1

ISMS Lead Auditor (CB) and CQI ISMS Technical Assessor

bcs Chartered IT Professional

Webinar objectives

CQI | IRCA
LEADING QUALITY SINCE 1919

As a result of attending this seminar you will be able to:

1. explain the purpose of information security (IS) management and ISO/IEC 27001
2. identify what has changed between the second edition (ISO/IEC 27001:2013) and the third edition (ISO/IEC 27001:2022)
3. determine the implications of the changes for those who use this standard

CQI | IRCA
LEADING QUALITY SINCE 1919

The changes

The changes

CQI | IRCA
LEADING QUALITY SINCE 1919

What is Information Security Management?

'Preservation of confidentiality, integrity and availability of information' – ISO/IEC 27000:2018

What is an Information Security Management system?

'Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security'

The changes

CQI | IRCA
LEADING QUALITY SINCE 1919

What does an ISMS consist of?

‘Policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets’
(ISO/IEC 27000:2018 – clause 4.2.1 Overview and principles)

What is an information asset?

‘a definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation’.

The changes

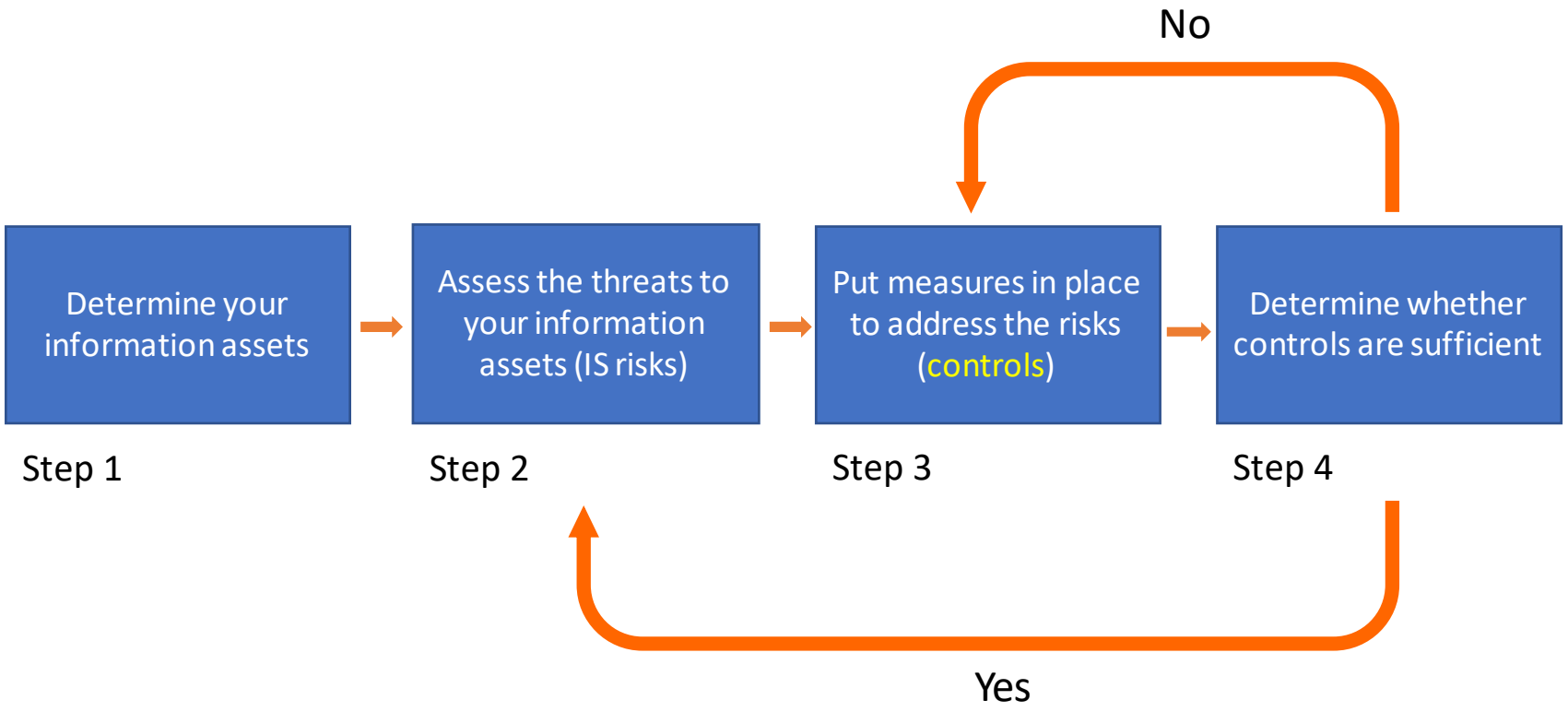
Examples of information assets

Strategies, goals and objectives	Patents, copyrights, trademarks	Project Management Information	Customer Lists
Training and development materials	Marketing Plans	Sales Plans	Operational procedures and work instructions
Decision support tools/techniques	Financial reports and budgets	Research and development outcomes	Legal & Compliance Performance

Note – these are 'enterprise' assets – ISMS is NOT an ICT function, it's an organizational function

The changes

Information asset protection process



The changes

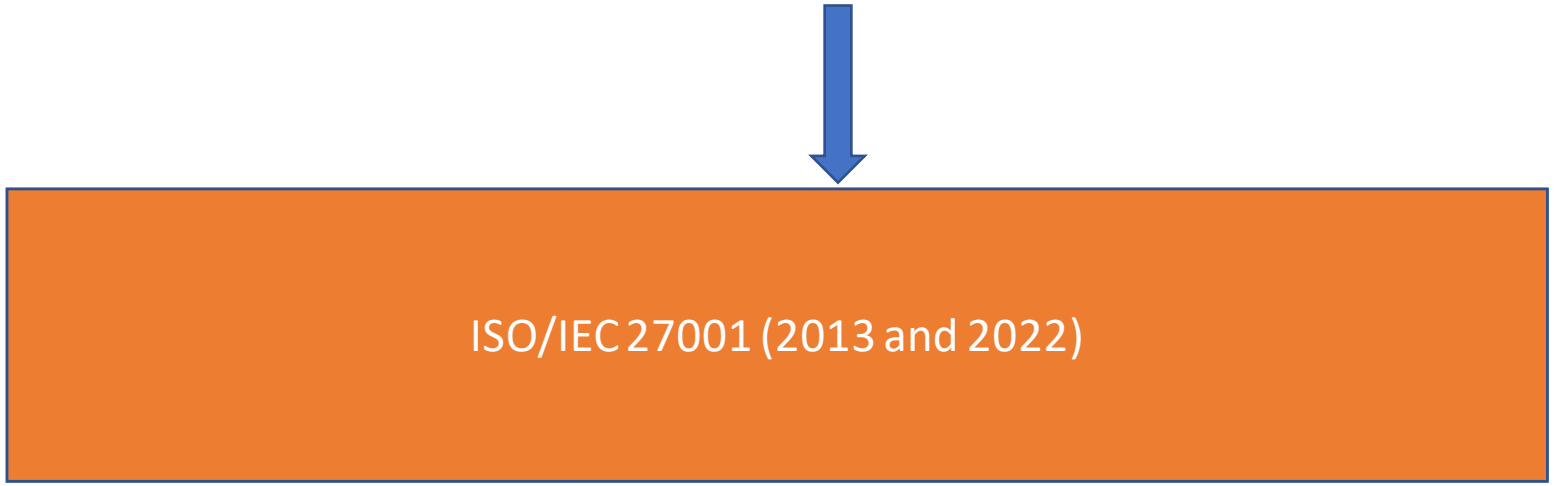
CQI | IRCA
LEADING QUALITY SINCE 1919

Controls

'a measure that is modifying risk' – ISO/IEC 27000:2018

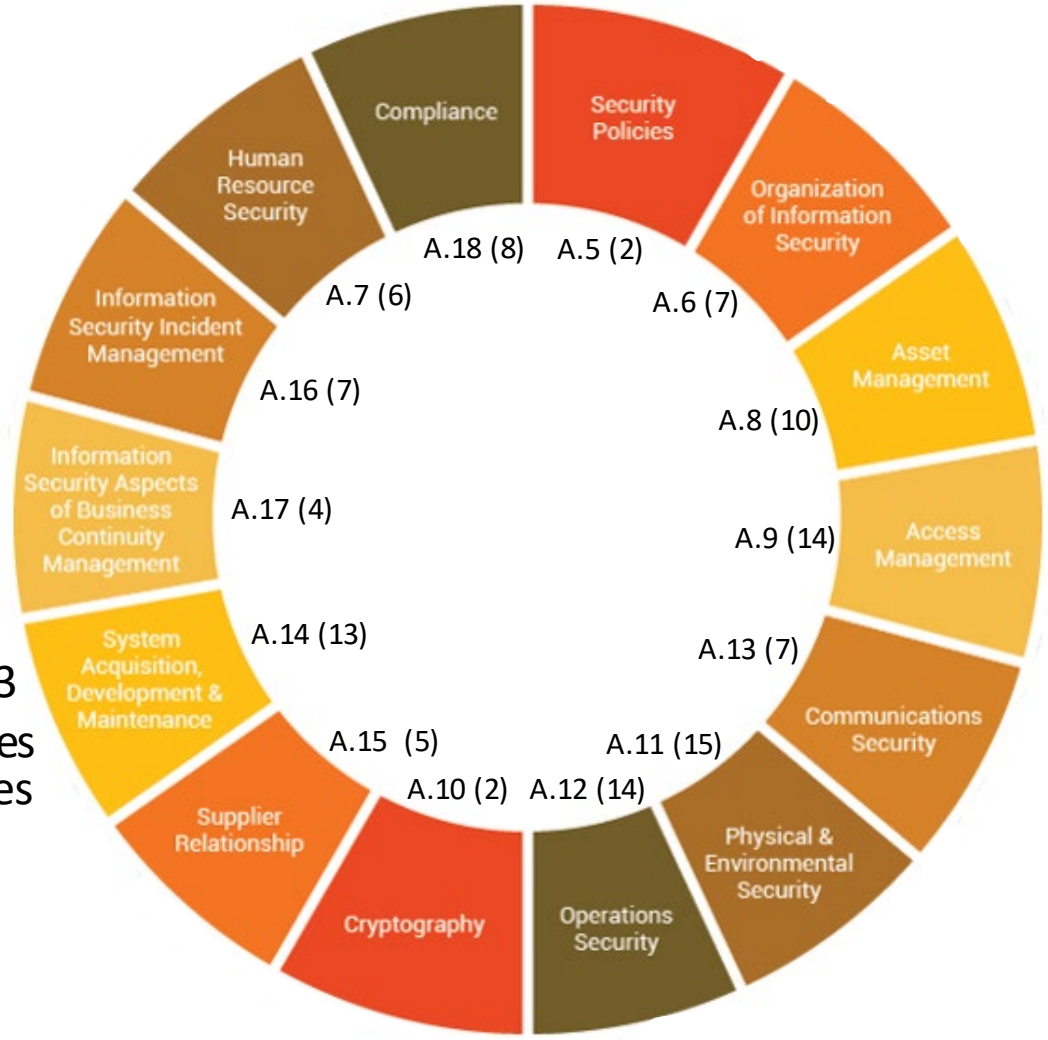
ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection — Information security controls



The changes

Controls



ISO/IEC 27001:2013

14 control categories
35 control objectives
114 controls

Organizational controls (37)	People controls (8)
Physical controls (14)	Technological controls (34)

ISO/IEC 27001:2022

4 control 'themes'
0 control objectives
93 controls – 82 based on existing
+ 11 new

The changes

CQI | IRCA
LEADING QUALITY SINCE 1919

Controls (new)

- Treat Intelligence
- Information security for use of cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Monitoring activities
- Web filtering
- Secure coding

The changes

A.5 Information security policies		
A.5.1 Management direction for information security		
Objective: To provide management direction and support for IS in accordance with business requirements and relevant laws and regulations		
A.5.1.1	Policies for IS	Control A set of policies for IS shall be defined, approved by management, published and communicated to employees and external parties
A.5.1.2	Review of the policies for IS	Control The policies for IS shall be review at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness

A.5 Organizational controls		
A.5.1	Policies for IS	Control Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

The changes

Controls

The third edition of ISO/IEC 27002 also identifies whether each 27001 control:

Is a [corrective] [preventive] [detective] control

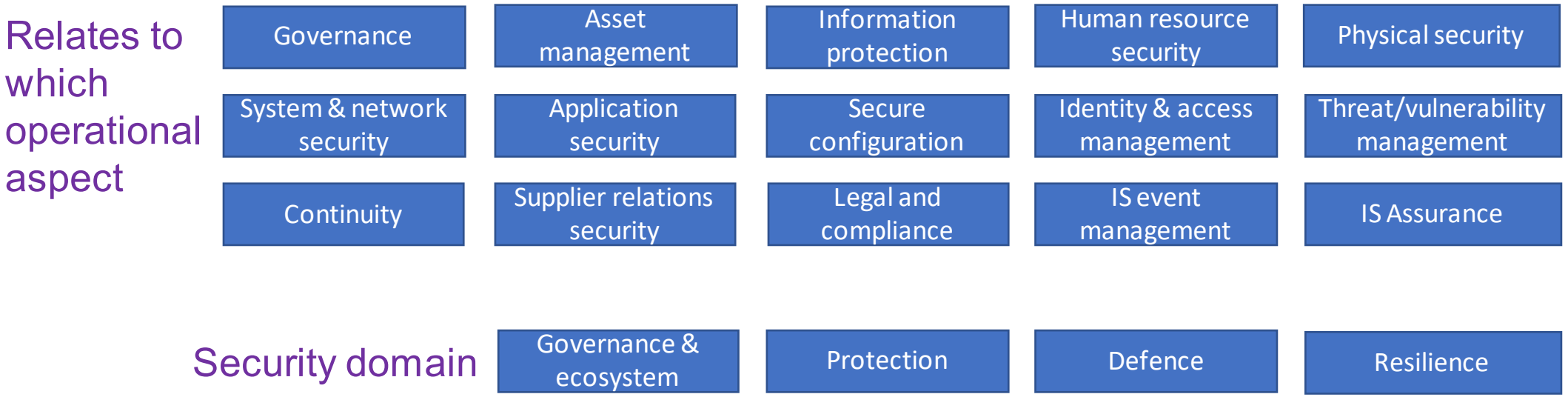
Seeks to support the [confidentiality] [integrity] [availability] of information assets

Exists to [identify] [protect] [detect] [respond] [recover] from IS threats

The changes

Controls

The third edition of ISO/IEC 27002 also identifies whether each 27001 control:



ISO/IEC 27002:2022 annex B contains 2 useful tables mapping the 2022 controls to the 2013 controls and vice versa.

The changes

CQI | IRCA
LEADING QUALITY SINCE 1919

Requirements

- Substantively unchanged, reordering of words, restructuring of paragraphs, updating of cross references to other standards (e.g. ISO 31000)
- Incorporates changes driven by annex SL's harmonised structure
- 4.4 – ISMS Mgt System - more explicitly calls for a process approach 'including the processes needed and their interactions'
- New requirement to monitor progress against achievement of ISMS objectives
- New subclause 6.3 – planning of changes (to ISMS) – these need to be controlled

The changes

CQI | IRCA
LEADING QUALITY SINCE 1919

Requirements

- Reduction in bullets relating to 7.4 communication (5 to 4)
- 9.2 Internal Audit -> 9.2.1 General + 9.2.2 Internal Audit programme
- 9.3 Management Review -> 9.3.1 General +9.3.2 Management Review Inputs + 9.3.3 Management Review Outputs
- 10.1 Nonconformity and corrective action -> 10.2
- 10.2 Continual improvement -> 10.1

CQI | IRCA
LEADING QUALITY SINCE 1919

The implications

Implications - Implementers

- You have three years to transition (IAF communique – 'from last day of month published' – October 2022)
- You will need to update your SoA/risk treatment plans based on the new control set
- You may need to revise existing processes / introduce new processes to evidence the new control set
- You may need to update MS references (revised control numbers, requirement numbers)
- You may need to provide additional training to staff – awareness, competence.
- Talk to your certification bodies, they will assist you

Implications - Auditors

CQI | IRCA
LEADING QUALITY SINCE 1919

- Upskill as necessary to enable you to audit the new control set
- CQI encourages its' ISMS auditors to attend a transition course but will accept self transition through appropriate study
- More details of the transition requirements to follow in due course.

Implications – Training Providers

- Revisit course materials – e.g. delegate manuals, case studies, exercises to determine whether any changes are necessary
- For CQI IRCA ATP's note:

  ISMS training course criteria have been revised

  ISMS A/LA and conversion course examinations and solution papers have been revised ('transition' markers)

CQI | IRCA
LEADING QUALITY SINCE 1919

Future trends

Future trends (ISO 2021 survey)

CQI | IRCA
LEADING QUALITY SINCE 1919

Sector	ISO/IEC 27001:2013 certificates	
1. Information technology	10,644	+5%
2. Transport, storage, communications	6,909	+1,014%
3. Other services	1,693	+24%
4. Engineering services	630	+14%
5. Financial, real estate, renting	645	+58%
6. Wholesale, retail, repair of goods	562	+39%
7. Construction	527	+26%
8. Electrical and optical equipment	477	+23%

% change since ISO 2020 survey

Future trends (ISO 2021 survey)

CQI | IRCA
LEADING QUALITY SINCE 1919

Country	Certificates	%change(2020)	sites/cert
1. China	18,446	+48%	1.00
2. Japan	6,587	+16%	2.69
3. UK	5,256	+57%	1.65
4. India	2,775	+24%	2.17
5. Italy	1,924	+5%	1.80
6. USA	1,742	+64%	2.59
7. Germany	1,673	+31%	2.08
8. Netherlands	1,508	+13%	1.61

% change since ISO 2020 survey

CQI | IRCA

LEADING QUALITY SINCE 1919

Any questions?

Question time

Any feedback or questions?

Thanks

CQI | IRCA
LEADING QUALITY SINCE 1919

rgreen@kingsfordconsultancyservices.co.uk

kingsfordconsultancyservices.co.uk


CQI
IRCA
LEADING QUALITY SINCE 1919
Thanks for joining us