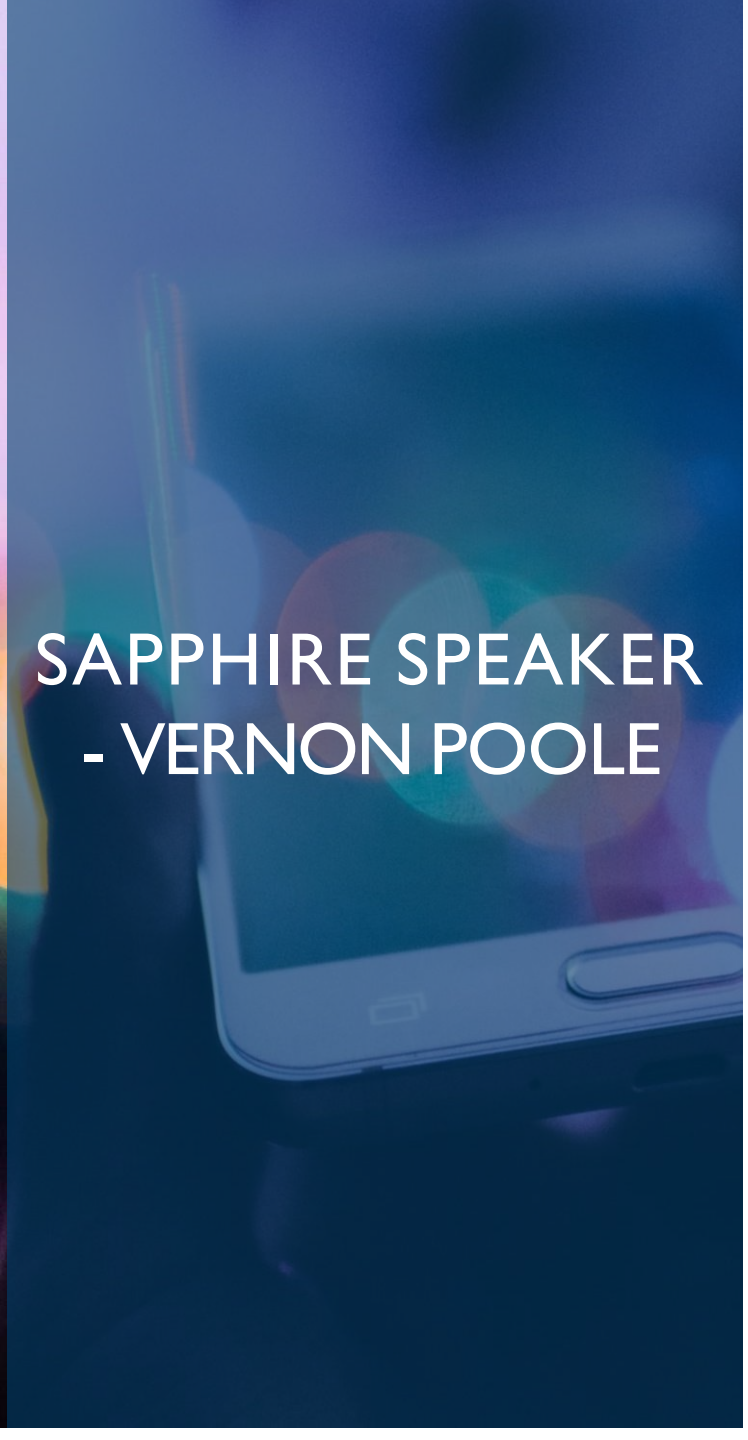
ISO/IEC 27002: 2022 WHAT DOES THE REVISED STANDARD MEAN TO YOU?

BCS – ISSG: 27 April 2022

Vernon Poole – CRISC, CISM & CGEIT



SAPPHIRE SPEAKER - VERNON POOLE

bcs The Chartered Institute for IT
Information Security Specialist Group

- Recognised trainer in Information Security Management.
- Member of UK/International ISO User Groups & presenter at the first International 27001 Day – January 2022.
- ISO27001/2 Expert with over 30 years experience.
- Head of Business Consultancy at Sapphire.

SAPPHIRE™

AGENDA

- The revised ISO/IEC 27002 standard (set of controls).
- Changes to the guiding principles.
- New and revised controls.
- New perspectives/attributes added to each control.
- Why you should adopt the changes.
- Standard Benefits

ISO27002 REVISION 2022 STATUS

- New & enhanced title – ISO/IEC 27002 standard (Information security, cyber security, and privacy protection – information security controls).

- The publication date was 15 February 2022.

- Certified organisations will have up to 2 years to transition to the revised standard once ISO27001has been updated - an Advisory Guide for external auditors is being provided.

ISO/IEC 27002 & ISO/IEC 27001

- ISO/IEC 27002 is the set of controls deployed by ISO/IEC 27001 – Certification Process which will outline the 'themes' & controls in Annex A.

- Time will be required to amend ISO27001 with the revised Annex A (potentially a 2022 amendment to the 2013 version) – estimated to be in late 2022 so it is not anticipated that organisations could get certified to the changes until early 2023. For certified organisations, the transition period is estimated to end in mid 2024.

- What is clear is that the changes proposed are highly significant for all organisations (large & small or in the public or private sector) - a standard that addresses information security, cyber security and privacy is a game changer.

ISO/IEC 27002 Revision: A Simplified Approach

14 guiding principles will become 4 ‘themes’.

1. IS Policy
2. Organising IS
3. Asset Management
4. Human Resources Security
5. Physical/Environmental Security
6. Operations Security
7. Communications Security
8. Access Control
9. Cryptography
10. Information Systems Acquisition & Development
11. Supplier Relationships
12. IS Incident Management
13. IS aspects of BCM
14. Compliance

1. Organisational Controls
2. People Controls
3. Physical Controls
4. Technological Controls

ISO/IEC 27002 Revision: New Control Structure (Modernised)

114 controls will now be 93 controls:

- 58 are updated
- 24 merged controls
- 11 new controls added

Note: 35 remain the same as the current version

Where the grouping of controls are as follows:

1. Organisational Controls (37) including 3 new controls.
2. People Controls (8) – no new controls.
3. Physical Controls (14) including 1 new control.
4. Technological Controls (34) including 7 new controls.

ISO/IEC 27002 Revision: Updated Controls (Examples)

- ‘Teleworking’ becomes ‘Remote working’.
- ‘User registration/de-registration’ becomes ‘Identity management’.
- ‘Secure log-on procedures’ becomes ‘Secure authentication’.
- ‘Controls against malware’ becomes ‘Protection against malware’.

Such renaming will provide easier understanding in developing the organisation’s Information Security Management System (ISMS).

ISO/IEC 27002 Revision: Merged Controls (Examples)

- ‘Management of removable media, disposal of media, physical media transfer and removal of assets’ is merged into ‘Storage Media’

- ‘User access provisioning, review of user access rights, removal or adjustment of access rights’ is merged into ‘Access Rights’

- ‘Change management, system change control procedures, technical review of applications after operations platform changes, restrictions on changes to software packages’ is merged into ‘Change Management’

Such merging makes its simpler to follow and is more efficient.

ISO/IEC 27002 Revision: New Controls (11)

1. Threat Intelligence (O)
2. Information security for cloud services (O)
3. ICT readiness for business continuity (O)
4. Physical security monitoring (P)
5. Configuration management (T)
6. Information deletion (T)
7. Data masking (T)
8. Data leakage prevention (T)
9. Monitoring activities (T)
10. Web filtering (T)
11. Secure coding principles (T)

Where:-

O = Organisational

P = Physical

T = Technological

ISO/IEC 27002 Revision: 1. Organisational Controls (IS Forum)

- Policy
- Organising Security – roles/responsibilities; identity & access management, etc.
- Asset Management inc. threat intelligence.
- Supplier Relationships inc. IS for use of cloud services (ISO27017:2021 controls).
- Incident Management.
- BCP inc. ICT continuity planning .
- Compliance.

ISO/IEC 27002 Revision; 2. People Controls (HR)

- Screening.
- Terms and conditions of employment.
- Information security awareness, education and training.
- Disciplinary process.
- Responsibilities after termination or change of employment.
- Confidentiality or non-disclosure agreements.
- Remote working.
- Information security event reporting.

ISO/IEC 27002 Revision: 3. Physical Controls (Facilities Management)

- Physical security perimeter.
- Physical entry controls.
- Securing offices, rooms & facilities.
- Physical security monitoring.
- Protecting against physical & environmental threats.
- Working in secure areas.
- Clear desk and clear screen.
- Equipment siting and protection.
- Security of assets off-premises.
- Storage media.

- Supporting utilities.
- Cabling security.
- Equipment maintenance.
- Secure disposal or re-use of equipment.

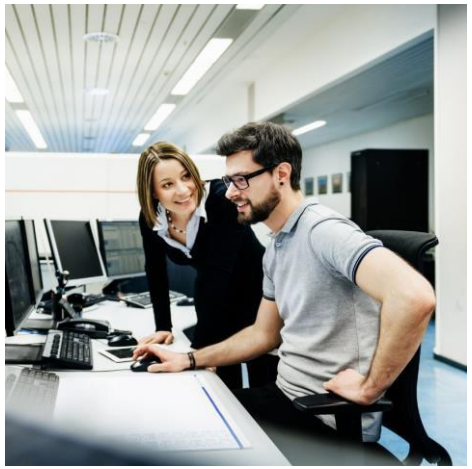
ISO/IEC 27002 Revision: 4. Technological Controls (IT/IS)

- Endpoint devices.
- Controls on privileged access & secure authentication.
- Cryptographic Controls.
- Operations Security inc. configuration management; information deletion; data masking; data leakage prevention; and monitoring activities.
- Communications Security inc. web filtering.
- Development Security inc. secure coding principles.

ISO/IEC 27002 Revision: Addition of Attributes for each Control

Each control can be viewed from several perspectives (attributes) - not mandatory:

1. Control Type (preventive; detective or corrective).
2. IS Properties (C, I or A).
3. Cyber Security Concepts (Identify; Protect; Detect; Respond or Recover).
4. Operational Capabilities - 15 (Governance; Asset management; Information protection; HR security; Physical security; System & network security; Application security; Secure configuration; Identity & access management; Threat & vulnerability management; Continuity; Supplier Relationships security; Legal & compliance; IS event management; and Security assurance).
5. Security Domains (Governance & Ecosystem, Protection, Defence, Resilience).



You can set up your own attribute groupings e.g., GDPR or specific regulatory requirements.

ISO/IEC 27002 Revision: Control Format

Each control will have a new 'Purpose' outlined and revised 'Guidance' (with sub- headings where required) & 'Other Information' where:

- Purpose is the rationale for applying the control.
- Guidance is detailed explanations on how the control should be implemented.
- Other Information is further guidance to understand the control with references to other documents for consultation.

These improvements make it easier in choosing and justifying the use of appropriate controls.

ISO/IEC 27002 Revision: Control Format Example

5.1 Policies for information security

CONTROL	IS	CYBERSECURITY	OPERATIONAL CAPABILITIES	SECURITY DOMAINS
Preventative	C,I, A	Identify	Governance	Governance & Ecosystem; Resilience

Control
Policies for information security should be defined, approved by…

Purpose (New Section)
To ensure continuing suitability, adequacy, and effect…

Guidance (with subheadings where appropriate)
At the highest level, organizations should define an "information security policy"…

Other Information – see the following reference material….

ISO/IEC 27002 Revision: Standard Annexes

There are two excellent Annexes:

<u>Annex A – matrix outlining the attributes for each control</u>
This annex has a comprehensive coverage of each attribute value for each control - useful in Risk Assessment and allocating CIA to each threat.

<u>Annex B – matrix comparison with the ISO27002:2013</u>
This annex allows organisations to see where current controls have been reallocated or merged, plus the addition of new controls.

Why you should adopt the ISO/IEC 27002 Revision.

- Organisations are undertaking digital transformation, utilising cloud services, and adjusting to hybrid working as a result of COVID.
- At the same time, cybercriminals are continuing to find ways to exploit vulnerabilities as the threat landscape grows.
- This standard will assist in the identification, implementation and management of up-to-date information security controls. These controls cover processes, policies, procedures, and management structures to address the growing cyber threats and risks.
- Adopting this standard will enable you to identify appropriate and proportionate controls that are sustainable and work to increase the overall appropriateness of your ISMS - helping to create an 'security culture' that is vital to protect your information and staff.

What changes are required to adopt the ISO/IEC 27002 Revision.

- Organisations can still utilise the existing policies/procedures – there will be tailoring required to adjust to the revised focus/amendments.

- The calibration to the new attribute types enables organisations to present the ISMS from different perspectives – information security, cyber security and/or privacy – very useful depending how your organisation is set up or needs to report based on different stakeholders.

- The new controls will need to be accommodated/adhered to and the structure of the ISMS refined accordingly.

- Risk Assessment Process (Statement of Applicability) & Internal Audit Checklists will need to recalibrated to the revised arrangements.

- All organisations will need to educate their staff (management & users) into the revised way of addressing the ISMS in readiness for external audit.

ISO/IEC 27002 Revision: Enhanced Benefits for the Organisation

- Provides you with competitive edge.
- Protects and enhances your reputation.
- Reduces financial penalties/losses associated with data breaches.
- Ensures compliance with business, legal, contractual & regulatory requirements.

The ISO/IEC 27002 can help you to achieve the following benefits

bcs The Chartered Institute for IT
Information Security Specialist Group

- Compliance with the revised requirements.
- Improved Communication & Awareness.
- Enhanced Staff Skills.
- Increased Productivity / Service Delivery.
- Increased Operational Efficiency.
- Reduced Legal Costs
- Reduced Risk to your business.
- Increased Trust in your business.

SAPPHIRE™

THANK YOU

ISO/IEC 27001/2 can help you to protect your data from prying eyes.

QUESTIONS?

Contact Details: vernon.poole@sapphire.net