ISO/IEC 27002:2022

A practical overview

All attendees will be on mute for the duration of the webinar.

Throughout the webinar, please ask questions using the chat function.

The recording and slides for this webinar will be made available on our website.

Enjoy the webinar!

For more information:

✉ hello@dspanz.org

www www.dspanz.org

dspanz.

digital service providers
australia new zealand

Acknowledgement of Country

Belinda Stewart

DSPANZ Director & GNGB Director

Leveraging a wealth of leadership experience in compliance and data security, specialising in scoping, project management, consultation, and customised solutions. Bringing a unique perspective to the optimisation of Payroll, Time & Attendance, and HR processes. Recognised for the ability to devise innovative solutions, driving efficiency and ensuring compliance in business operations.

Dushyant Sanathara

Head of Digital Trust, APAC - BSI

Drawing on his extensive leadership experience technology and background in e-business and business management, bringing a distinctive perspective to the convergence of technology and Governance, Risk, and Compliance. Widely recognised for his capacity to craft innovative solutions that enhance outcomes and propel business achievements.

dspanz.

digital service providers
australia new zealand

Lucas Roe

Governance Risk & Compliance Practice Lead - InfoTrust

Over 15 years of expertise, excelling in assessing and proposing practical security strategies aligned with industry standards. Specialising in security architecture and advisory services, providing clients with practical solutions to effectively mitigate security risks. Possesses extensive knowledge in designing, implementing, and leading security advisory services, contributing to the management of effective cybersecurity programs.

Charles Gillman

Chief Information Security Officer - Super Choice

With over two decades of expertise in Information Security, specialising in financial services. Led security teams at major institutions and held CISO roles in diverse settings, offering a comprehensive perspective from a background as a penetration tester. Provides practical solutions for current and emerging cybersecurity threats.

ISO/IEC 27002:2022

Welcome Dushyant

dspanz.

digital service providers
australia new zealand

What is a transition?

Transition is used when a standard has changed and released as a new version created. In this case, clients certified to the existing standard (ISO 27001:2013) must transition to the new version of the standard (ISO 27001:2022).

Key Transition Issues

What	Date/Impact
Updated standard issue date	Published October 24th 2022
First assessments against new standard	November 2022
General availability of certification to new standard	Depends on Accreditation Bodies. RvA, Accredia, ANAB, CNAS Completed – others in progress
Availability of training	ISO27002:2022 – available now ISO27001:2022 – available now
Last date for initial/recertification audits against 2013 version	**18 months from publication (April 2024)**
All certificates against 2013 withdrawn	3 years from publication (October 2025)
Transition audit duration	Depends on size/complexity Can be performed alongside an annual audit

Key Transition Dates

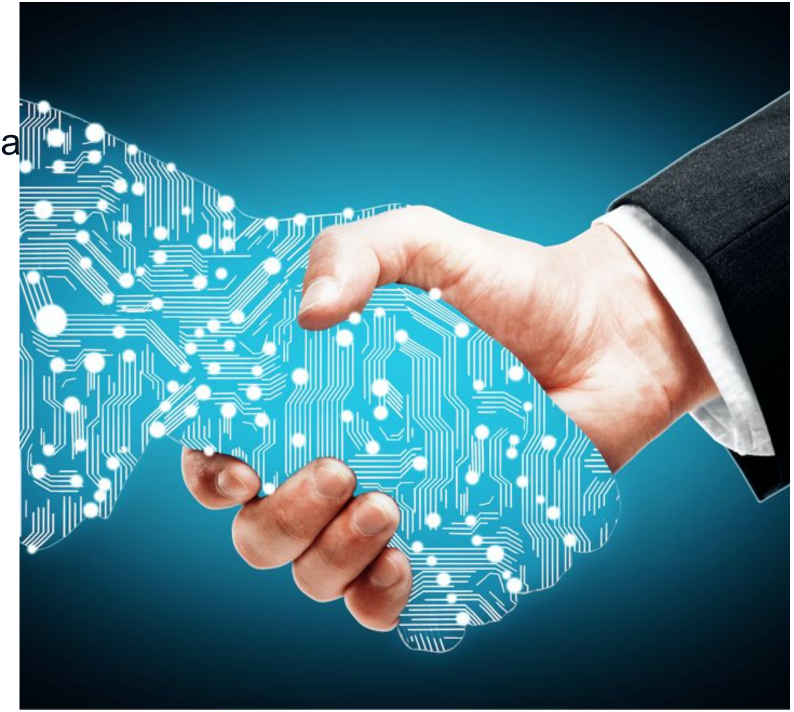
Transition end date – 31st October 2025

Please ensure that all transition audits are booked no later than 31st August 2025 to allow 8 weeks for NCR closures, technical review and cert issue.

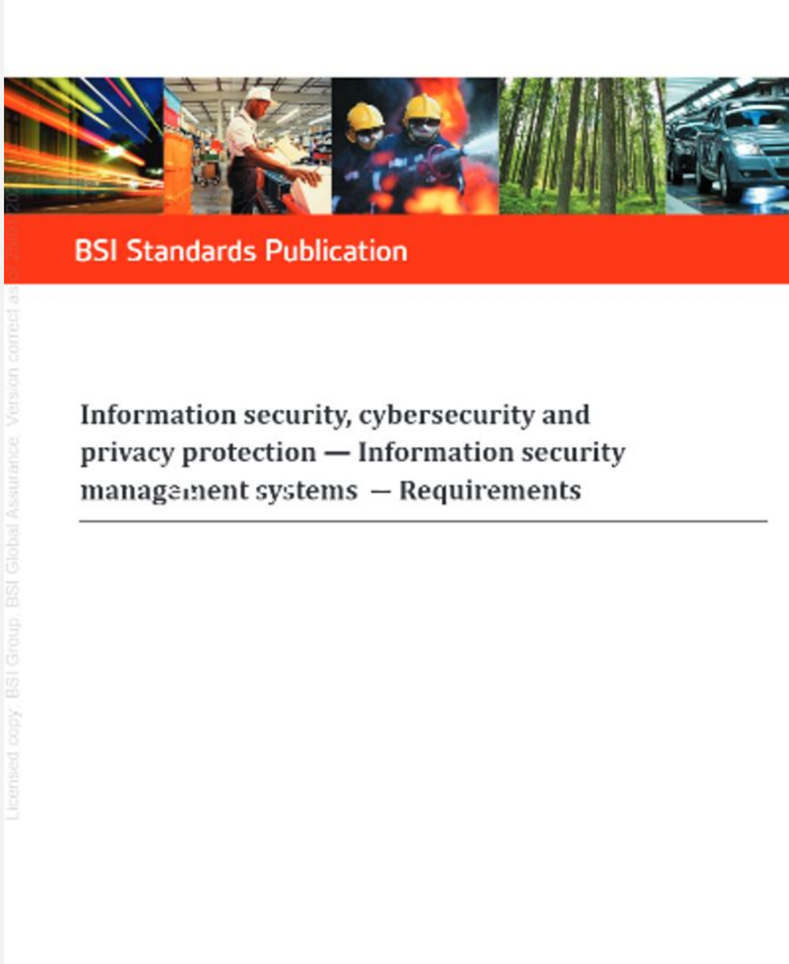
From 1st May 2024, all initial and recertification audits shall be conducted using ISO/IEC 27001:2022.

Introducing Digital Trust – thinking beyond traditional cybersecurity

"Digital trust is about instilling confidence in an organization, that empowers the people, the systems and the technology to ensure their safety, security, compliance, privacy and ethica requirements."



Key changes and transition process

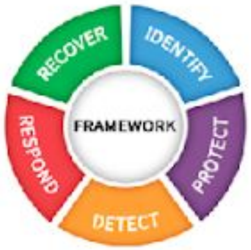


BSI Standards Publication

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Why is ISO/IEC 27001 Changing?

- The way we live and work has changed
- The cybersecurity industry has matured



ISO/NIST Cybersecurity Concepts

- New harmonized approach to ISO Management System Standards

NEWS

18% of Remote Workers Have Suffered a Security Breach Since Lockdown

August 30, 2020

Survey shows relying on VPN
attacks.

The BYOD effect: the security risks of using personal devices for work

By Lucy Wright

CORE

THE BYOD EF
The security ris
using personal
for work

The rise of smartphones and tablets has meant
working from home, you can log on to your dev
remote working in 2020 means its more impor
device, also known as Bring Your Own Device (

In our recent survey of more than 200 IT decisi
security breach

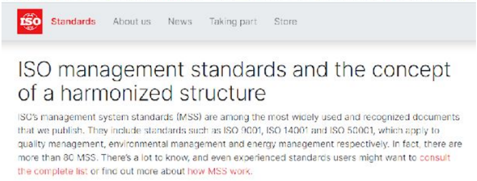
But with remote working here to stay and BYO

TECHNOLOGY

After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users

April 9, 2021 · 11:50 PM ET

EMMA BOWMAN



ISO management standards and the concept of a harmonized structure

ISO's management system standards (MSS) are among the most widely used and recognized documents that we publish. They include standards such as ISO 9001, ISO 14001 and ISO 50001, which apply to quality management, environmental management and energy management respectively. In fact, there are more than 80 MSS. There's a lot to know, and even experienced standards users might want to consult the complete list or find out more about how MSS work.

ISO/IEC 27001 Structure and Key Areas of Change

Changes

- 3 key changes to main body of document – clarification on processes
- Annex A: Controls - updated in line with ISO/IEC 27002:2022
- Editorial changes throughout document
- Other changes – further clarifications throughout main body of document

1. Introduction
2. References
3. Terms & Definitions
4. Context of the organization
    1. Organization & context
    2. Needs & expectations
    3. Scope of ISMS
    4. ISMS
5. Leadership
    1. Leadership & Commitment
    2. Policy
    3. Organization

ISO/IEC 27001 Structure and Key Areas of Change

6. Planning
    1. Risks & opportunities
    2. Objectives
    3. Planning of changes
7. Support
    1. Resources
    2. Competence
    3. Awareness
    4. Communication
    5. Documented information

8. Operation
    1. Planning and control
    2. Risk assessment
    3. Risk treatment
9. Performance evaluation
    1. Monitoring, measurement, analysis and evaluation
    2. Internal audit
    3. Management review
10. Improvement
    1. Non-conformity and corrective action
    2. Continual Improvement

Annex A: Reference controls

Key Clause Changes and Inclusions:

Clause	Change in Requirement
4.4 – Information Security Management System	The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

Key Clause Changes and Inclusions:

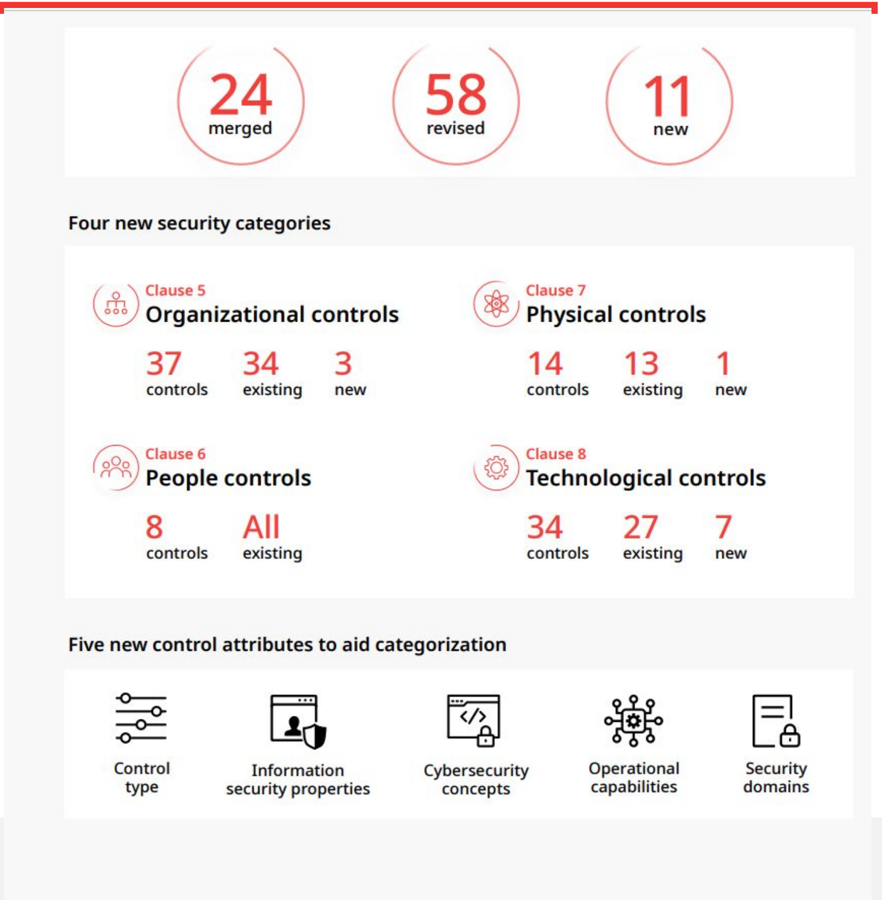
Clause	Change in Requirement
6.3 *New* – Planning of Changes	When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

Key Clause Changes and Inclusions:

Clause	Change in Requirement
8.1 Operational Planning and Control	The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: ▪ establishing criteria for the processes; ▪ implementing control of the processes in accordance with the criteria. Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

New Controls Structure

- **Controls**
114 in 14 groups » now 93 in 4 groups
- **Organization, People, Physical, Technological**
- **11 new controls, 24 merged + 58 maintained**
- **Full review of Annex A, Risk Assessment, SoA**
- **ISO/IEC 27002:2022**
  - Updated implementation guidance
  - Control purpose
  - Attributes
  - **Confidentiality Integrity Availability**
  - **Identify Protect Detect Respond Recover**



24 merged

58 revised

11 new

Four new security categories

Clause 5
Organizational controls

37	34	3
controls	existing	new

Clause 7
Physical controls

14	13	1
controls	existing	new

Clause 6
People controls

8	All
controls	existing

Clause 8
Technological controls

34	27	7
controls	existing	new

Five new control attributes to aid categorization

Control type

Information security properties

Cybersecurity concepts

Operational capabilities

Security domains

Controls Maintained – Total 58 (People - A6)

27001:2022 Control	27001:2013 Control	Control Title
A6.1	**A07.1.1**	Screening
A6.2	**A07.1.2**	Terms and definitions of employment
A6.3	**A07.2.2**	Information security awareness, education and training
A6.4	**A07.2.3**	Disciplinary process
A6.5	**A07.3.1**	Responsibilities after termination or change of employment
A6.6	**A13.2.4**	Confidentiality or non-disclosure agreements
A6.7	**A06.2.2**	**Remote working**

Controls Maintained – Total 58 (People - A6)

27001:2022 Control	27001:2013 Control	Control Title
A7.1	**A11.1.1**	Physical security perimeters
A7.3	**A11.1.3**	Securing offices, rooms and facilities
A7.5	**A11.1.4**	Protecting against physical and environmental threats
A7.6	**A11.1.5**	Working in secure areas
A7.7	**A11.2.9**	Clear desk and clear screen
A7.8	**A11.2.1**	Equipment siting and protection
A7.9	**A11.2.6**	**Security of assets off-premises**
A7.11	**A11.2.2**	Supporting utilities
A7.12	**A11.2.3**	Cabling security
A7.13	**A11.2.4**	Equipment maintenance
A7.14	**A11.2.7**	Secure disposal or re-use of equipment

Merged controls

ISO/IEC 27001:2013	ISO/IEC 27001:2022	ISO/IEC 27001:2013	ISO/IEC 27001:2022
A05.1.1, A05.1.2	A5.01	A16.1.2, A16.1.3	A6.08
A06.1.5, A14.1.1	A5.08	A11.1.2, A11.1.6	A7.02
A08.1.1, A08.1.2	A5.09	A08.3.1, A08.3.2, A08.3.3, A11.2.5	A7.10
A08.1.3, A08.2.3	A5.10	A06.2.1, A11.2.8	A8.01
A13.2.1, A13,2,2, A13.3.3	A5.14	A12.6.1, A18.2.3	A8.08
A09.1.1, A09.2.2	A5.15	A12.4.1, A12.4.2, A12.4.3	A8.15
A09.2.4, A09.2.5, A09.2.6	A5.17	A12.5.1, A12.6.2	A8.19
A09.2.2, A09.2.5, A09.2.6	A5.18	A10.1.1, A10.1.2	A8.24
A15.1.1, A15.1.2	A5.22	A14.1.2, A14.1.3	A8.26
A17.1.1, A17.1.2, A17.1.3	A5.29	A14.2.8, A14.2.9	A8.29
A18.1.1, A18.1.5	A5.31	A12.1.4, A12.2.6	A8.31
A18.2.2, A18.2.3	A5.36	A12.1.2, A14.2.2, A14.2.3, A14.2.4	A8.32

24
merged
controls

Merged where existing controls are inseparable or closely related

Controls Merged – New Statements

27001:2022 Control	27001:2013 Control	Control Name	Old Statement(s)	New Statement
A5.1	**A05.1.1, A05.1.2**	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	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.
A5.8	**A06.1.5, A14.1.1**	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project. The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Information Security shall be integrated into project management

Controls Merged – New Statements

27001:2022 Control	27001:2013 Control	Control Name	Old Statement(s)	New Statement
A5.17	**A09.2.4, A09.3.1, A09.4.3**	Authentication information	The allocation of secret authentication information shall be controlled through a formal management process Users shall be required to follow the organization's practices and use of secret authentication information Password management systems shall be interactive and shall ensure quality passwords	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on the appropriate handling of authentication information
A5.18	**A09.2.2, A09.2.5, A09.2.6**	Access rights	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services Assets owners shall review users' access rights at regular intervals The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change	Access rights to information in order associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control

11 New Controls

27001:2022 Control	27001:2013 Control	Control Title
A5.7	**New**	Threat intelligence
A5.23	**New**	Information security for use of cloud services
A5. 30	**New**	ICT readiness for business continuity
A7.4	**New**	Physical security monitoring
A8.9	**New**	Configuration management
A8. 10	**New**	Information deletion
A8.11	**New**	Data masking
A8.12	**New**	Data leakage prevention
A8.16	**New**	Monitoring activities
A8.23	**New**	Web filtering
A8.28	**New**	Secure coding

A5.7 – Threat Intelligence

- Control: “Information relating to information security threats shall be collected and analyzed to produce threat intelligence”.

- Purpose: To provide awareness of the organization’s threat environment so that appropriate mitigation actions can be taken.

- Security Domains: Defense and Resilience

- Supporting Standards: ISO 27701, ISO 31000, and ISO 22301

A5.7 – ISO 27002:2022 - Implementation Guidance

Collect and Analyze Threats

- Existing Threats
- Emerging Threats

Divide into three layers

- Strategic (High-level info about the changing (Players and types)
- Tactical (Methodologies, tools and technologies involved)
- Operational (Details about attacks, including technical indicators)

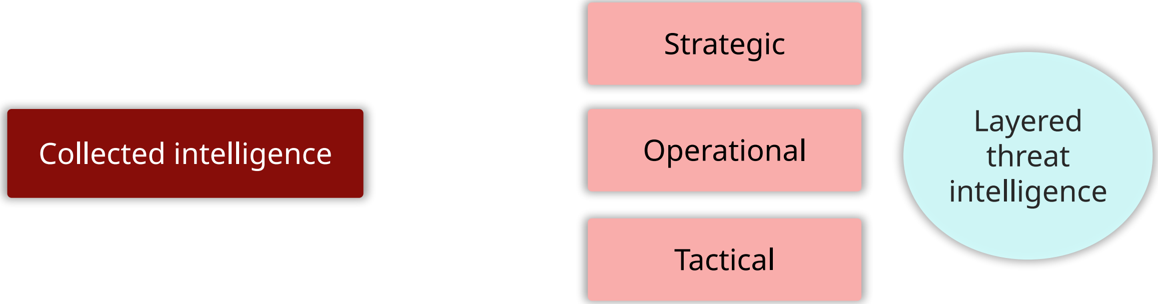
Understand

- Relevant for the protection of the Organization
- Insightful (Accurate and understanding of the threat landscape)
- Contextual (time, where they occur, previous experiences)
- Actionable (Act quickly and effectively)

Define and Analyze

- Objectives for threat intelligence production
- Identify stakeholders (internal and external) to support your production
- Collect information and analyze information
- Implement a process to include the info obtained and add them to the risk management

Control A.5.7 threat intelligence - Summary



- Intelligence shall be relevant, insightful, contextual and actionable
- Establish activities to identify, vet, select, collect, process, analyse and communicate relevant information
- Consider internal and external threats

A5.23 – 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.

- Security Domains: Governance and Protection

- Additional Standards: ISO/IEC 17788, ISO/IEC 17789 and ISO/IEC 22123-1

- Supporting Standards : ISO/IEC 27017 and ISO/IEC 27018

ISO/IEC 27001:2022 Annex A new control:

A5.23 – 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

Supporting Standards

ISO 22301, ISO 27017, ISO 27018, ISO 17788 / 17789, and ISO 22123-1

A5.23 – ISO 27002:2022 - Implementation Guidance

Identify Type

- Cloud Services User
- Cloud Services Provider
- Both

Define

- Requirements
- Criteria and Scope of Cloud Service Usage
- Roles and Responsibilities
- Controls managed by the provider and by the customer
- How to obtain and analyze IS capabilities provided and controls implemented by the providers
- How to manage controls, interfaces and changes

Agree

- Provisioning of solutions – best practice in Industry for architecture and infrastructure
- Manage Access Controls to meet the requirements of the organization
- Dedicated support in case of Information Security incidents
- Backup of Data and Configuration information
- Returning information (Configuration files, source code and data owned by the organization)

Further guidance on InfoSec for Cloud Users/Providers ISO 27017:2021

- Standard created for Cloud Service Customers and Cloud Service Providers
- Provides robust control over Cloud Services
- Based on ISO/IEC 27002* (guidance)
- 32 Controls – extra guidance:
  - All 32 apply to Cloud Users
  - 30 apply to Cloud Providers
- 7 additional controls
  - 5 apply to Cloud Users
  - All 7 apply to Cloud Providers

BS EN ISO/IEC 27017:2021

BSI Standards Publication

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

*

A5.30 – 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.

- Security Domains: Resilience

- Supporting Standards : ISO/IEC 27031, ISO 22301, ISO 22313, ISO/TS 22317 (for BIA)

A7.4 – ISO 27002:2022 - Implementation Guidance

Define

- ICT readiness for Business Continuity Management
- Use BIA process with impact types and criteria

Identify

- Prioritized activities which should be assigned a recovery time objective (RTO
- Resources needed to support prioritized activities
- Performance and capacity requirements

Implement

- Aadequate organizational structure
- ICT continuity plans, including response and recovery procedures
- Regular test and evaluation of plans for effectiveness

Next Steps ISO 27001:2022 Transition

Step 1: Understand the Changes

- Get standards: 27001:2022 and 27002:2022
- **BSI On-demand and classroom training available now**

Step 2: Check the Impact on your Organization

- **Gap assessment**
- Update Risk Assessment

Step 3: Implement the Changes

- Review controls
- Update SOA
- Implement applicable changes
- **Readiness review**

Step 4: Transition your Certification

- **Schedule transition audit with BSI**
- Can be combined with annual audit

bsi ISO/IEC 27001 Information Security Management CERTIFIED

ISO/IEC 27002:2022

Welcome Lucas & Charles

dspanz.
digital service providers
australia new zealand

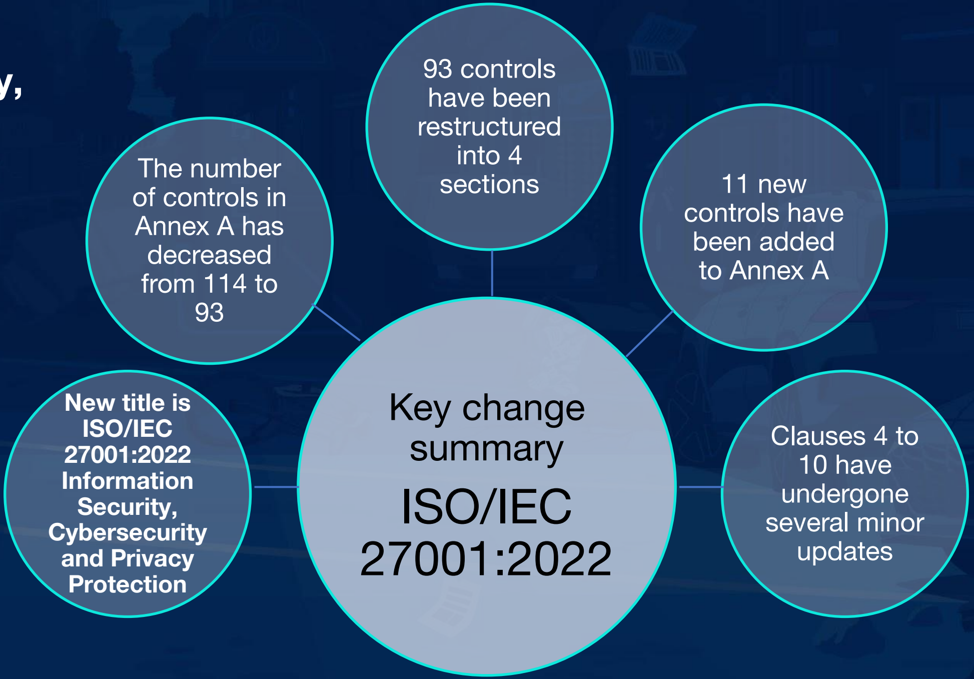
KEY CHANGES TO ISO/IEC 27001:2022

ISO/IEC 27001:2022 - Information Security, Cybersecurity & Privacy Protection

Whilst the Standard refers to information security throughout, security professionals and interested parties should be considering both cyber security and privacy. Determining privacy protections helps achieve security outcomes.

Scope & context of interested parties

Clause 4.3c in the 2022 update has been added; to clarify which requirements of interested parties will be addressed through the Information Security Management System (ISMS).



Key change summary ISO/IEC 27001:2022

93 controls have been restructured into 4 sections

The number of controls in Annex A has decreased from 114 to 93

11 new controls have been added to Annex A

New title is ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection

Clauses 4 to 10 have undergone several minor updates

InfoTrust

ISO 27002 CONTROLS OVERVIEW

ISO 27002 (Annex A)

Organisational Controls

37 organisational controls that cover your governance, management, Information Security Management System controls

People Controls

8 controls to ensure your giving through right support and training to keep your company safe

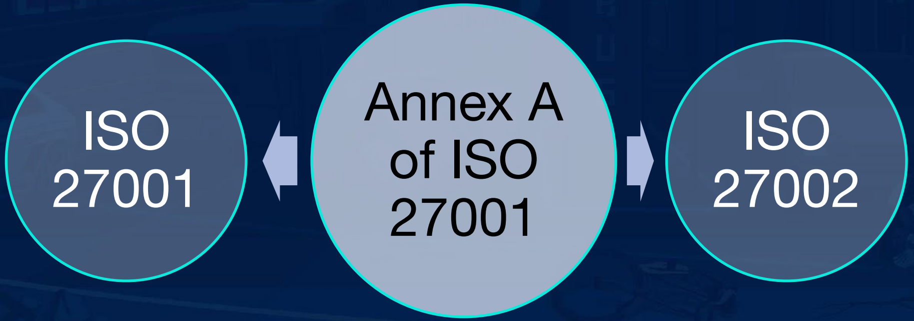
Physical Controls

14 controls covering the main security controls to protect your physical locations and equipment

Technological Controls

34 technical controls to secure your networks, applications, data and all things technical

RELATIONSHIP BETWEEN ISO 27001 & 27002



1. Identify risk in ISMS and relevant controls for risk management

2. Establish, implement, monitor, review and improve controls

CHANGES TO 27001 CLAUSES (4-10)

CLAUSE 6.1.3 CHANGES

Clause 6.1.3 has been updated to now reference Annex A as containing a list of possible information security controls.

This update differs from it originally containing a comprehensive list of control objectives. This ensures more flexibility if additional information security controls are needed; can be included.

CLAUSES 6.2 & 6.3 CHANGES

Changes to clause 6.2 were made to focus on clarity.

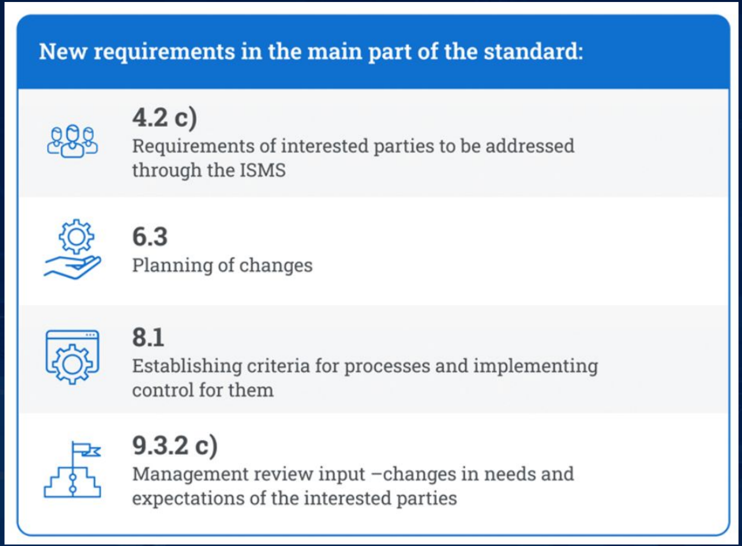
It was also updated to explicitly confirm that information security objectives should be monitored and be available as documented information when planning to achieve them. Clause 6.3 has been newly added to confirm when you make changes to the ISMS, to carry it out in a planned manner.

CLAUSES 9.2 & 9.3 SEPARATED

Clause 9.2 have been separated into sub clauses 9.2.1 "General" and 9.2.2 "Internal audit programme".

Clause 9.3 has been shifted into three new separate sub clauses. 9.3.1 "General", 9.3.2 "Management review inputs", and 9.3.3 "Management review results".

These changes were intended for ease and clarity of reading.



New requirements in the main part of the standard:

4.2 c)
Requirements of interested parties to be addressed through the ISMS

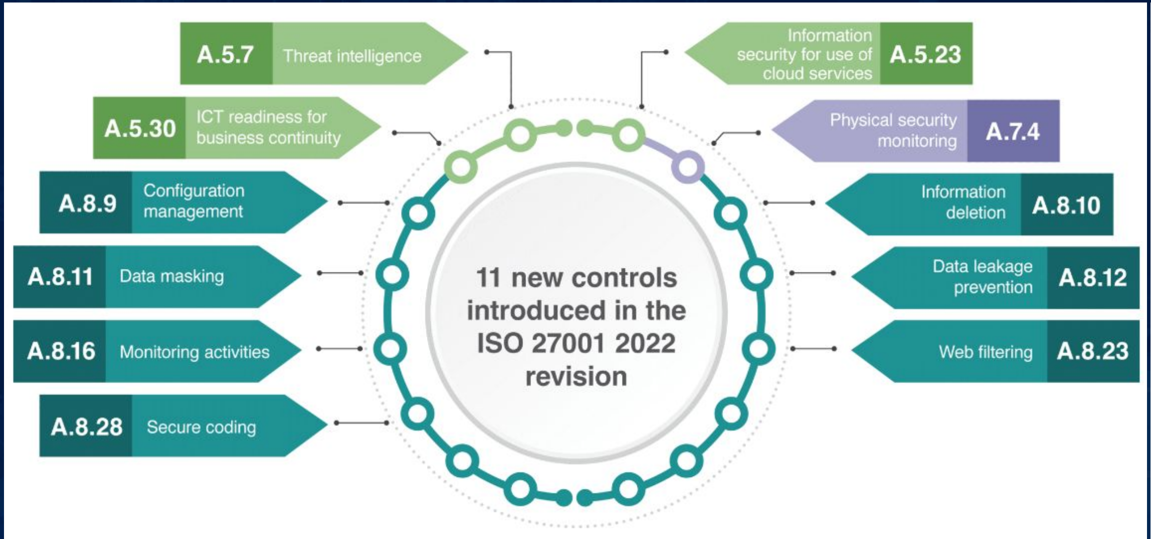
6.3
Planning of changes

8.1
Establishing criteria for processes and implementing control for them

9.3.2 c)
Management review input –changes in needs and expectations of the interested parties

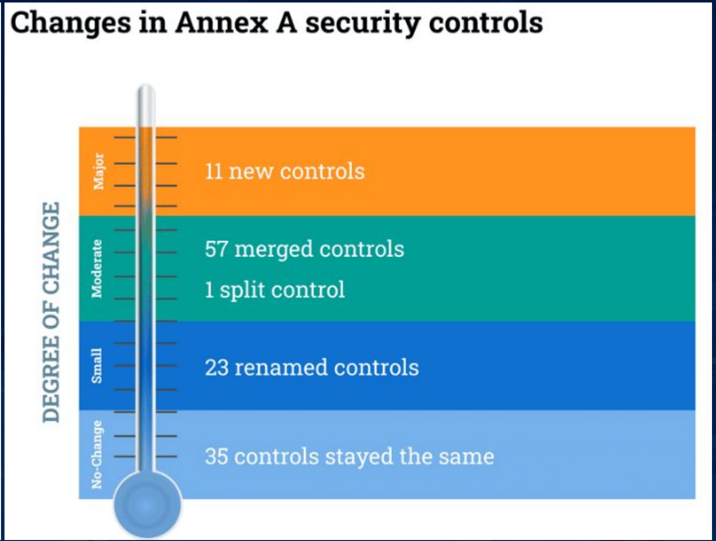
InfoTrust

CHANGES TO ISO 27002



11 new controls introduced in the ISO 27001 2022 revision

- A.5.7 Threat intelligence
- A.5.23 Information security for use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Information deletion
- A.8.11 Data masking
- A.8.12 Data leakage prevention
- A.8.16 Monitoring activities
- A.8.23 Web filtering
- A.8.28 Secure coding



Changes in Annex A security controls

CHANGES TO ISO 27002 (CONT.)

Threat Intelligence (5.7)	Organisations should gather and use threat intelligence to proactively identify, assess, and mitigate potential cybersecurity threats.
Information Security for Use of Cloud Services (5.23)	Organisations should implement appropriate security measures when using cloud services to ensure the confidentiality, integrity, and availability of their information assets.
ICT Readiness for Business Continuity (5.30)	Organisations should ensure that their ICT infrastructure and resources are resilient and can support business continuity in the event of disruptions or disasters.
Physical Security Monitoring (7.4)	Organisations should continuously monitor physical security controls to detect and respond to unauthorised access or other security incidents.
Configuration Management (8.9)	Organisations should establish and maintain a configuration management process to ensure that IT systems are configured securely and consistently.
Information Deletion (8.10)	Organisations should implement procedures for securely deleting information when it is no longer needed or required.
Data Masking (8.11)	Organisations should consider using data masking techniques to protect sensitive data when it is used for testing or development purposes.
ICT Security Assessment and Testing (8.23)	Organisations should regularly assess and test the effectiveness of their ICT security controls to identify and address vulnerabilities.
Incident Management (A.6.1.2)	Organisations should establish and maintain an incident management process to effectively respond to cybersecurity incidents.
Cybersecurity Awareness and Training (A.6.2.1)	Organisations should provide cybersecurity awareness and training to their employees to educate them about cybersecurity risks and best practices.
Supplier Relationships (A.15)	Organisations should manage supplier relationships to ensure suppliers adhere to appropriate security requirements.

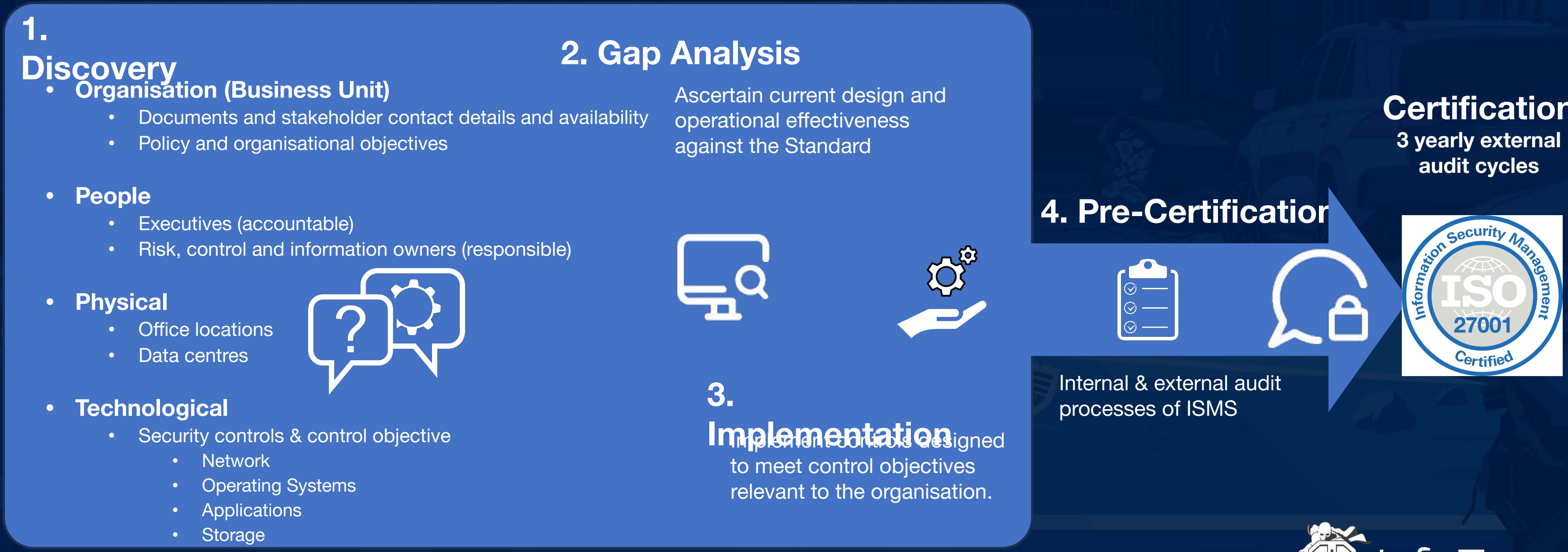
InfoTrust

A PHASED APPROACH

An overview of initial **discovery and gap analysis activities** aligned with ISO/IEC 27001:2022 are summarized below.

Determining an organisation’s objectives, people, physical locations and technological controls frames activities and effort required to meet the Standard. Designing and maintaining and ISMS requires significant effort.

Companies currently Certified have until November 2025 to align with the new requirements of the Standard.



1. Discovery

- **Organisation (Business Unit)**
  - Documents and stakeholder contact details and availability
  - Policy and organisational objectives
- **People**
  - Executives (accountable)
  - Risk, control and information owners (responsible)
- **Physical**
  - Office locations
  - Data centres
- **Technological**
  - Security controls & control objective
    - Network
    - Operating Systems
    - Applications
    - Storage

2. Gap Analysis

Ascertain current design and operational effectiveness against the Standard

3. Implementation

Implement controls designed to meet control objectives relevant to the organisation.

4. Pre-Certification

Internal & external audit processes of ISMS

Certification

3 yearly external audit cycles

InfoTrust

PRAGMATIC MIGRATION ADVICE

Upgrading or migrating to the ISO 27001:2022 framework can seem daunting. With careful planning and careful execution the process can be made efficient and effective. An ISMS needs to work to meet your objectives.

PLAN FOR A MIGRATION

Allocate Ample Time and Resources
Don't underestimate the time required for a seemingly simple migration. Allocate sufficient resources and plan for potential roadblocks. The complexity of your organization's ISMS and the number of changes required will influence the overall timeline.

Initiate Migration Promptly Begin the migration process immediately after your latest audit concludes to maintain momentum and avoid last-minute rushes. This ensures you stay on track for recertification under the new standard.

Get support

Ensure you have the information security skills and capabilities needed.

LEVERAGE USEFUL RESOURCES

Use Tools Download and utilize the ISO27001:2013 to ISO27001:2022 mapping tool to streamline comparison and identification of changes. These tools can significantly reduce the manual effort involved in mapping controls between the two versions of the standard.

Understand Control Mapping
Recognise the many-to-one mapping of old controls to new controls, such as merging three old controls into one new control. This understanding will help you optimise your migration efforts and avoid unnecessary duplication of work.

ASSESS NEW ANNEX A CONTROLS

Assess Control Relevance and SOA Inclusion
Evaluate the relevance and risk reduction potential of new Annex A controls. Prioritize controls based on specific risks and consider formally documenting them in the Statement of Applicability (SOA).

Optimise Control Implementation:
Explore efficient methods for implementing new controls

- Leverage existing controls
- Implement *and enforce* policy updates
- Evaluate capacity to design and manage controls

EMBRACE CONTINOUS IMPROVEMENT

Establish Continuous Monitoring
Establish continuous monitoring processes to ensure your ISMS remains aligned with ISO 27001:2022 requirements and adapts to evolving threats and risks.

Conduct Regular Reviews and Updates Schedule regular reviews of your ISMS to identify any areas for improvement and make necessary updates to maintain compliance and effectiveness.

Foster a culture of security awareness: Continuously educate and train your teams on awareness and best practices to minimise human error and enhance the skills of your teams.

NEW ISO27002 CONTROLS - IMPLEMENTATION GUIDANCE

- **A.5.7 Threat intelligence**
  - Open-source threat feeds
  - Threat intelligence platforms allowing aggregation, sharing and receiving of threat intel with other organisations are available.
- **A.5.23 Information security for use of cloud services**
  - Embed requirements to manage cloud service risks into Supplier Security Policies and supporting artefacts.
  - Gain a clear understanding of your Identity & Access Management strategy and existing services available and used.
  - Use tools to monitor and continually assess your cloud security posture, identify misconfigurations, and enforce security policies.
- **A.5.30 ICT readiness for business continuity**
  - Business Impact Analyses, Business Continuity Planning and testing schedules.
- **A.7.4 Physical security monitoring**
  - Cameras, alarms and access control systems to monitor and restrict access to physical premises processing sensitive information. Confirm third parties responsible for these controls are aware of their responsibilities.
- **A.8.9 Configuration management**
  - Define configuration baselines using CIS, OWASP or other relevant security standards. Make use of tooling and configuration reviews available to better understand device configuration
  - Utilise tools like Ansible that can be used for configuration management, deployment and orchestration
- **A.8.10 Information deletion**
  - Define and enforce an achievable Disposal & Destruction Policy, aligned with retention requirements known.

InfoTrust

NEW ISO27002 CONTROLS - IMPLEMENTATION GUIDANCE

- **A.8.11 Data masking**
  - Access controls to restrict unauthorised access to sensitive data
  - Use of data anonymisation tools or techniques (tokenisation, encryption, hashing techniques) to protect or restrict exposure of sensitive data.
- **A.8.12 Data leakage prevention**
  - DLP strategies encompass a broad range of control objectives
  - Understanding identities and access management risks assist in effectively achieving DLP objectives
- **A.8.16 Monitoring activities**
  - Logging & Monitoring Policy & Procedure
  - SIEM Tool to collect, analyse and monitor data from various sources
- **A.8.23 Web filtering**
  - Numerous Web Application Firewall (WAF) solutions available
  - Use of inbound or outbound proxies to filter and restrict web traffic
  - Open-source web content filtering tool that can be used to block websites based on URL, category, content, and user group.
- **A.8.28 Secure coding**
  - Develop secure coding guidelines if you develop software
  - Enforce secure coding practices throughout software development lifecycle (SDLC); effective use of static and dynamic analysis tools can reduce time to ensure security objectives are met.

ISO/IEC 27002:2022

Group Q&A

dspanz.

digital service providers
australia new zealand

Feedback Survey

If you are unable to access the form, please contact hello@dspanz.org

dspanz.

digital service providers
australia new zealand

Thank you for joining us

The recording and slides for this webinar will be made available on DSPANZ website.

For more information:

✉ hello@dspanz.org

www www.dspanz.org

dspanz.

digital service providers
australia new zealand