Overview of new security controls in ISO 27002:2022

Author: Rhand Leal

WHITE PAPER

Advisera

Making certification simple.

Table of Contents

Introduction

ISO 27002 has gone through the process of change – the old 2013 revision with 114 security controls is transformed into a more modern standard with 93 controls and better structure, and the new ISO 27002:2022 was published on February 15, 2022.

This standard is a supporting standard for ISO 27001, the world's leading information security standard, and on October 25, 2022, the ISO 27001:2022 was published, aligning its Annex A with ISO 27002.

In other words, the controls in ISO 27001 and ISO 27002 are exactly the same; the only difference is that ISO 27002 provides detailed guidance on how the controls could be implemented.

This white paper highlights the key changes in the 2022 revisions of ISO 27001 & ISO 27002 compared to the 2013 revisions of those standards.

Structure of sections

Rather than the 14 sections of the previous version, ISO 27002:2022 now has only four sections and two annexes:

- Organizational controls (clause 5): This section contains all controls related to various organizational issues, comprising 37 controls.
- People controls (clause 6): This section focuses on controls related to human resources security, comprising 8 controls.
- Physical controls (clause 7): This section focuses on controls related to the physical environment, comprising 14 controls.
- Technological controls (clause 8): This section focuses on controls related to technological solutions, comprising 34 controls.
- Annex A – Using attributes: This annex provides a matrix of all the new controls, and it compares their attributes and provides suggestions on how the controls might be used according to their attributes.
- Annex B – Correspondence with ISO/IEC 27002:2013: This annex provides a mapping between controls from this version and the controls from the previous 2013 edition.

The reduced number of sections, and the addition of an annex with guidance on how to use the controls, makes it easier to understand the applicability of controls and designation of responsibilities.

Number of controls

This new version has reduced the number of controls from 114 to 93. Technological advancements, and an improvement in the understanding of how to apply security practices, are the reasons for the change in the number of controls.

The changed controls are listed further in this white paper.

Elements of each control

Each control in the new version of ISO 27002 has two new elements in its structure:

- Attribute table: A table presenting the set of attributes associated with the control (see next section for explanation).
- Purpose: Rationale for applying the control, i.e., why a control needs to be implemented (e.g., to ensure integrity, to define roles, etc.).
- These added elements make it easier for those choosing or analyzing the controls to find out information to better understand how to sort and justify the use of a control. For example, from the attribute table, an organization can identify all controls of a preventive nature (e.g., 5.1 Policies for Information Security and 8.25 Secure Development Life Cycle) and work with them in an integrated way. Through Purpose you can better explain to others the need for implementing a control, as well as evaluate its adequacy to treat specific risks.
- The elements that already existed in the old ISO 27002 and remain in this new revision of the standard are:
- Control title: the name of the control.
- Control: a description of what needs to be accomplished to be compliant with the control.
- Guidance: tips on how the control should be implemented.
- Other information: complementary information to understand the control and references to other documents for consultation.

Controls attributes

From our point of view, this is the change that brings the most value for this new version of the standard, because it provides a standardized way to sort and filter controls against different criteria.

Attributes for each control are as follows:

- Control types: Preventive, Detective, and Corrective.
- Information security properties: Confidentiality, Integrity, and Availability.
- Cybersecurity concepts: Identify, Protect, Detect, Respond, and Recover.
- Operational Capabilities: 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 management, Continuity, Supplier relationships security, Legal and compliance, Information security event management, and Information security assurance.

- Security domains: Governance and ecosystem, Protection, Defense, and Resilience.
- These attributes will make it easier to understand which controls are applicable according to criteria relevant to the business (i.e., not related only to information security), as well as the integration of ISO 27002 controls to other similar security frameworks, like NIST Risk Management Framework.

New controls

Here are the 11 controls that are completely new:

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

Renamed controls

A total of 23 controls have had their names changed for the sake of easier understanding; however, their essence remained the same as in the old standard:

ISO/IEC 27002:2013 control	ISO/IEC 27002:2022 control
6.2.2 Teleworking	6.7 Remote working
9.2.1 User registration and de-registration	5.16 Identity management
9.2.3 Management of privileged access rights	8.2 Privileged access rights
9.4.2 Secure log-on procedures	8.5 Secure authentication
9.4.5 Access control to program source code	8.4 Access to source code
7.3.1 Termination or change of employment responsibilities	6.5 Responsibilities after termination or change of employment
11.1.1 Physical security perimeter	7.1 Physical security perimeters
11.2.6 Security of equipment and assets off-premises	7.9 Security of assets off-premises
11.2.9 Clear desk and clear screen policy	7.7 Clear desk and clear screen
12.2.1 Controls against malware	8.7 Protection against malware
12.7.1 Information systems audit controls	8.34 Protection of information systems during audit testing
13.1.1 Network controls	8.20 Networks security
13.1.3 Segregation in networks	8.22 Segregation of networks
14.2.1 Secure development policy	8.25 Secure development life cycle
14.2.5 Secure system engineering principles	8.27 Secure system architecture and engineering principles
14.3.1 Protection of test data	8.33 Test information
15.1.1 Information security policy for supplier relationships	5.19 Information security in supplier relationships

ISO/IEC 27002:2013 control	ISO/IEC 27002:2022 control
15.1.2 Addressing security within supplier agreements	5.20 Addressing information security within supplier agreements
15.1.3 Information and communication technology supply chain	5.21 Managing information security in the ICT supply chain
16.1.1 Responsibilities and procedures	5.24 Information security incident management planning and preparation
16.1.4 Assessment of and decision on information security events	5.25 Assessment and decision on information security events
17.2.1 Availability of information processing facilities	8.14 Redundancy of information processing facilities
18.1.4 Privacy and protection of personally identifiable information	5.34 Privacy and protection of PII

These changes will help keep the focus on information security aspects of processes and activities, reducing the effort for implementing and maintaining the Information Security Management System.

Excluded controls: none

Although the number of controls has been reduced, no controls were excluded in this new version, only merged for the sake of better understanding.

Merged controls

A total of 57 controls have been merged into 24 new controls:

ISO/IEC 27002:2013 control	ISO/IEC 27002:2022 control
5.1.1 Policies for information security 5.1.2 Review of the policies for information security	5.1 Policies for information security
6.1.5 Information security in project management 14.1.1 Information security requirements analysis and specification	5.8 Information security in project management
6.2.1 Mobile device policy 11.2.8 Unattended user equipment	8.1 User end point devices
8.1.1 Inventory of assets 8.1.2 Ownership of assets	5.9 Inventory of information and other associated assets
8.1.3 Acceptable use of assets 8.2.3 Handling of assets	5.10 Acceptable use of information and other associated assets
8.3.1 Management of removable media 8.3.2 Disposal of media 8.3.3 Physical media transfer 11.2.5 Removal of assets	7.10 Storage media
9.1.1 Access control policy 9.1.2 Access to networks and network services	5.15 Access control
9.2.2 User access provisioning 9.2.5 Review of user access rights 9.2.6 Removal or adjustment of access rights	5.18 Access rights
9.2.4 Management of secret authentication information of users 9.3.1 Use of secret authentication information 9.4.3 Password management system	5.17 Authentication information
10.1.1 Policy on the use of cryptographic controls 10.1.2 Key management	8.24 Use of cryptography
11.1.2 Physical entry controls 11.1.6 Delivery and loading areas	7.2 Physical entry
12.1.2 Change management 14.2.2 System change control procedures 14.2.3 Technical review of applications after operating platform changes 14.2.4 Restrictions on changes to software packages	8.32 Change management
12.1.4 Separation of development, testing and operational environments 14.2.6 Secure development environment	8.31 Separation of development, test and production environments
12.4.1 Event logging 12.4.2 Protection of log information 12.4.3 Administrator and operator logs	8.15 Logging
12.5.1 Installation of software on operational systems 12.6.2 Restrictions on software installation	8.19 Installation of software on operational systems

ISO/IEC 27002:2013 control	ISO/IEC 27002:2022 control
12.6.1 Management of technical vulnerabilities 18.2.3 Technical compliance review	8.8 Management of technical vulnerabilities
13.2.1 Information transfer policies and procedures 13.2.2 Agreements on information transfer 13.2.3 Electronic messaging	5.14 Information transfer
14.1.2 Securing application services on public networks 14.1.3 Protecting application services transactions	8.26 Application security requirements
14.2.8 System security testing 14.2.9 System acceptance testing	8.29 Security testing in development and acceptance
15.2.1 Monitoring and review of supplier services 15.2.2 Managing changes to supplier services	5.22 Monitoring, review and change management of supplier services
16.1.2 Reporting information security events 16.1.3 Reporting information security weaknesses	6.8 Information security event reporting
17.1.1 Planning information security continuity 17.1.2 Implementing information security continuity 17.1.3 Verify, review and evaluate information security continuity	5.29 Information security during disruption
18.1.1 Identification of applicable legislation and contractual requirements 18.1.5 Regulation of cryptographic controls	5.31 Legal, statutory, regulatory and contractual requirements
18.2.2 Compliance with security policies and standards 18.2.3 Technical compliance review	5.36 Conformance with policies, rules and standards for information security

These merges were considered either because related controls are natural steps of a bigger process, or because more efficient security could be achieved by considering them in a single control.

Split controls

There is only one control that was split: *18.2.3 Technical compliance review* was split into *5.36 Conformance with policies, rules and standards for information security* and *8.8 Management of technical vulnerabilities*.

Controls that have stayed the same

These 35 controls remained the same, only changing their control number:

ISO/IEC 27002:2013 control	ISO/IEC 27002:2022 control
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
7.1.1 Screening	6.1 Screening
7.1.2 Terms and conditions of employment	6.2 Terms and conditions of employment
7.2.1 Management responsibilities	5.4 Management responsibilities
7.2.2 Information security awareness, education and training	6.3 Information security awareness, education and training
7.2.3 Disciplinary process	6.4 Disciplinary process
8.1.4 Return of assets	5.11 Return of assets
8.2.1 Classification of information	5.12 Classification of information
8.2.2 Labelling of information	5.13 Labelling of information
9.4.1 Information access restriction	8.3 Information access restriction
9.4.4 Use of privileged utility programs	8.18 Use of privileged utility programs
11.1.3 Securing offices, rooms and facilities	7.3 Securing offices, rooms and facilities
11.1.4 Protecting against external and environmental threats	7.5 Protecting against external and environmental threats
11.1.5 Working in secure areas	7.6 Working in secure areas

ISO/IEC 27002:2013 control	ISO/IEC 27002:2022 control
11.2.1 Equipment siting and protection	7.8 Equipment siting and protection
11.2.2 Supporting utilities	7.11 Supporting utilities
11.2.3 Cabling security	7.12 Cabling security
11.2.4 Equipment maintenance	7.13 Equipment maintenance
11.2.7 Secure disposal or re-use of equipment	7.14 Secure disposal or re-use of equipment
12.1.1 Documented operating procedures	5.37 Documented operating procedures
12.1.3 Capacity management	8.6 Capacity management
12.3.1 Information backup	8.13 Information backup
12.4.4 Clock synchronization	8.17 Clock synchronization
13.1.2 Security of network services	8.21 Security of network services
13.2.4 Confidentiality or non-disclosure agreements	6.6 Confidentiality or non-disclosure agreements
14.2.7 Outsourced development	8.30 Outsourced development
16.1.5 Response to information security incidents	5.26 Response to information security incidents
16.1.6 Learning from information security incidents	5.27 Learning from information security incidents
16.1.7 Collection of evidence	5.28 Collection of evidence
18.1.2 Intellectual property rights	5.32 Intellectual property rights
18.1.3 Protection of records	5.33 Protection of records
18.2.1 Independent review of information security	5.35 Independent review of information security

Implications for the ISMS

If you already have your Information Security Management System implemented according to ISO 27001, you don't have to worry too much for now – no matter which changes the new ISO 27002 revision has brought, there will be a transition period of three years for certified companies, starting October 25, 2022.

Check out ISO 27001 compliance software

To automate your compliance with ISO 27001/ISO 27002 security controls, sign up for a free trial of Conformio, the leading ISO 27001 compliance software.

References

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls

About the author

Rhand Leal has 16 years of experience in information security, and for six years he continuously maintained a certified Information Security Management System based on ISO 27001.

Rhand holds an MBA in Business Management from Fundação Getúlio Vargas. His certifications include ISO 27001 Lead Auditor, ISO 9001 Lead Auditor, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), and others. He is a member of the ISACA Brasília Chapter.

Advisera Expert Solutions Ltd
for electronic business and business consulting

Our offices:
Zavizanska 12, 10000 Zagreb, Croatia
Via Maggio 1 C, Lugano, CH-6900, Switzerland
275 Seventh Ave, 7th Floor, New York, 10001, U.S.

Email: support@advisera.com

Making certification simple