MSECB

Presentation of **ISO/IEC 27002:2022** Controls

Contents

New Controls

11 new controls have been added to the ISO/IEC 27002:2022

ISO/IEC 27002:2022 Controls

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

Merged controls

57 controls from the 2013 version, 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
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
13.2.1 Information transfer policies and procedures **13.2.2** Agreements on information transfer **13.2.3** Electronic messaging	**5.14** Information transfer
9.1.1 Access control policy **9.1.2** Access to networks and network services	**5.15** Access control
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
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
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

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
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** Compliance with policies, rules and standards for information security
16.1.2 Reporting information security events **16.1.3** Reporting information security weaknesses	**6.8** Information security event reporting
11.1.2 Physical entry controls **11.1.6** Delivery and loading areas	**7.2** Physical entry
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
6.2.1 Mobile device policy **11.2.8** Unattended user equipment	**8.1** User endpoint devices
12.6.1 Management of technical vulnerabilities **18.2.3** Technical compliance review	**8.8** Management of technical vulnerabilities
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
10.1.1 Policy on the use of cryptographic controls **10.1.2** Key management	**8.24** Use of cryptography
14.1.2 Securing application services on public networks **14.1.3** Protecting application services transactions	**8.26** Application security requirements

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
14.2.8 System security testing **14.2.9** System acceptance testing	**8.29** Security testing in development and acceptance
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
12.1.2 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

Renamed controls

23 controls have changed their names. However, their purpose is the same as in the previous 2013 version.

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
9.2.1 User registration and de-registration	**5.16** Identity management
15.1.1 Information security policy for supplier relationships	**5.19** Information security in supplier relationships
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
18.1.4 Privacy and protection of personally identifiable information	**5.34** Privacy and protection of PII
7.3.1 Termination or change of employment responsibilities	**6.5** Responsibilities after termination or change of employment

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
6.2.2 Teleworking	**6.7** Remote working
11.1.1 Physical security perimeter	**7.1** Physical security perimeters
11.2.9 Clear desk and clear screen policy	**7.7** Clear desk and clear screen
11.2.6 Security of equipment and assets off-premises	**7.9** Security of assets off-premises
9.2.3 Management of privileged access rights	**8.2** Privileged access rights
9.4.5 Access control to program source code	**8.4** Access to source code
9.4.2 Secure log-on procedures	**8.5** Secure authentication
12.2.1 Controls against malware	**8.7** Protection against malware
17.2.1 Availability of information processing facilities	**8.14** Redundancy of information processing facilities
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
12.7.1 Information systems audit controls	**8.34** Protection of information systems during audit testing

Same name, different control number

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
7.2.1 Management responsibilities	**5.4** Management responsibilities
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
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
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

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
12.1.1 Documented operating procedures	Documented operating procedures
7.1.1 Screening	**6.1** Screening
7.1.2 Terms and conditions of employment	**6.2** Terms and conditions of employment
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
13.2.4 Confidentiality or non-disclosure agreements	**6.6** Confidentiality or non-disclosure agreements
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
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
9.4.1 Information access restriction	**8.3** Information access restriction
12.1.3 Capacity management	**8.6** Capacity management

ISO/IEC 27002:2013 Control	**ISO/IEC 27002:2022** Control
12.3.1 Information backup	**8.13** Information backup
12.4.4 Clock synchronization	**8.17** Clock synchronization
9.4.4 Use of privileged utility programs	**8.18** Use of privileged utility programs
13.1.2 Security of network services	**8.21** Security of network services
14.2.7 Outsourced development	**8.30** Outsourced development

To learn more about the updated ISO/IEC 27002:2022, **click here,**

MSECB

info@msecb.com
www.msecb.com

in f