# ISO/IEC 27001:2013 > ISO/IEC 27001:2022
# Control Mapping

Die typische Lebensdauer einer ISO-Norm beträgt fünf Jahre. Nach diesem Zeitraum wird entschieden, ob die Norm gültig bleiben kann, überarbeitet werden muss oder zurückgezogen werden sollte. Im Jahr 2018 wurde beschlossen, dass die ISO/IEC 27002:2013 überarbeitet werden sollte. Der Entwurf wurde veröffentlicht und am 15. Februar 2022 angekündigt.

Die im Anhang A aufgeführte Maßnahmen („Controls“) wurden aktualisiert und neu strukturiert. Dabei wurde die Zahl der Controls von 114 auf 93 reduziert. Die Controls sind in der ISO/IEC 27001:2022 in vier statt wie bisher in 14 Abschnitte unterteilt:

| ISO/IEC 27001:2013 | | ISO/IEC 27001:2022 | |
|---|---|---|---|
| **A.5** | **Information security policies** | **5** | **Organizational controls** |
| A.5.1.1 | Policies for information security | 5.1 | Policies for information security |
| A.5.1.2 | Review of the policies for information security | | |
| **A.6** | **Organization of information security** | **5** | **Organizational controls** |
| A.6.1.1 | Information security roles and responsibilities | 5.2 | Information security roles and responsibilities |
| A.6.1.2 | Segregation of duties | 5.3 | Segregation of duties |
| A.6.1.3 | Contact with authorities | 5.5 | Contact with authorities |
| A.6.1.4 | Contact with special interest groups | 5.6 | Contact with special interest groups |
| **Neu** | | **5.7** | **Threat intelligence** |
| A.6.1.5 | Information security in project management | 5.8 | Information security in project management |
| A.14.1.1 | Information security requirements analysis and specification | | |
| **A.6** | **Organization of information security** | **8** | **Technological controls** |
| A.6.2.1 | Mobile devices (Moved to Asset management) | 8.1 | User endpoint devices |

| | | | |
|---|---|---|---|
| A.11.2.8 | Unattended user equipment | | |
| **A.6** | **Organization of information security** | **6** | **People Controls** |
| A.6.2.2 | Teleworking | 6.7 | Remote working |
| **A.7** | **Human Resources Security** | **6** | **People Controls** |
| A.7.1.1 | Screening | 6.1 | Screening |
| A.7.1.2 | Terms and conditions of employment | 6.2 | Terms and conditions of employment |
| A.7.2.1 | Management responsibilities | 5.4 | Management responsibilities |
| A.7.2.2 | Information security awareness, education, and training | 6.3 | Information security awareness, education, and training |
| A.7.2.3 | Disciplinary process | 6.4 | Disciplinary process |
| A.7.3.1 | Termination or change of employment responsibilities | 6.5 | Responsibilities after termination or change of employment |
| **A.8** | **Asset Management** | **5** | **Organizational controls** |
| A.8.1.1 | Inventory of assets | 5.9 | Inventory of information and other associated assets |
| A.8.1.2 | Ownership of assets | | |
| A.8.1.3 | Acceptable use of assets | 5.10 | Acceptable use of assets and other associated information assets |
| A.8.2.3 | Handling of assets | | |
| A.8.1.4 | Return of assets | 5.11 | Return of assets |
| A.8.2.1 | Classification of information | 5.12 | Classification of information |
| A.8.2.2 | Labeling of information | 5.13 | Labeling of Information |
| **A.8** | **Asset Management** | **7** | **Physical controls** |
| A.8.3.1 | Management of removable media | 7.10 | Storage media |
| A.8.3.2 | Disposal of media | | |
| A.8.3.3 | Physical media transfer | | |

| | | | |
|---|---|---|---|
| **A.9** | **Access Control** | **5** | **Organizational controls** |
| A.9.1.1 | Access control policy | 5.15 | Access Control |
| A.9.1.2 | Access to networks and network services | | |
| A.9.2.1 | User registration and de-registration | 5.16 | Identity Management |
| A.9.2.2 | User access provisioning | 5.18 | Access rights |
| A.9.2.5 | Review of access rights | | |
| A.9.2.6 | Removal or adjustment of access rights | | |
| **A.9** | **Access Control** | **8** | **Technological controls** |
| A.9.2.3 | Management of privileged access rights | 8.2 | Privileged access rights |
| **A.9** | **Access Control** | **5** | **Organizational controls** |
| A.9.2.4 | Management of secret authentication information of users | 5.17 | Authentication of information |
| A.9.3.1 | Use of secret authentication information | | |
| **A.9** | **Access Control** | **8** | **Technological controls** |
| A.9.4.1 | Information access restriction | 8.3 | Information access restriction |
| A.9.4.2 | Secure log-on procedures | 8.5 | Secure authentication |
| **A.9** | **Access Control** | **5** | **Organizational controls** |
| A.9.4.3 | Password management system | 5.17 | Authentication of information |
| **A.9** | **Access Control** | **8** | **Technological controls** |
| A.9.4.4 | Use of privileged utility programs | 8.18 | Use of privileged utility programs |
| A.9.4.5 | Access control to program source code | 8.4 | Access to source code |
| **A.10** | **Cryptography** | **8** | **Technological controls** |
| A.10.1.1 | Policy on the use of cryptographic controls | 8.24 | Use of cryptography |
| A.10.1.2 | Key management | | |

| A.11 | Physical and environmental security | 7 | Physical controls |
|---|---|---|---|
| A.11.1.1 | Physical security perimeter | 7.1 | Physical security perimeter |
| A.11.1.2 | Physical entry controls | 7.2 | Physical entry controls |
| A.11.1.6 | Delivery and loading areas | | |
| A.11.1.3 | Securing offices, rooms, and facilities | 7.3 | Securing offices, rooms, and facilities |
| Neu | | 7.4 | Physical security monitoring |
| A.11.1.4 | Protecting against external and environmental threats | 7.5 | Protecting against physical and environmental threats |
| A.11.1.5 | Working in secure areas | 7.6 | Working in secure areas |
| A.11.2.1 | Equipment siting and protection | 7.8 | Equipment siting and protection |
| A.11.2.2 | Supporting utilities | 7.11 | Supporting utilities |
| A.11.2.3 | Cabling security | 7.12 | Cabling security |
| A.11.2.4 | Equipment maintenance | 7.13 | Equipment maintenance |
| A.11.2.5 | Removal of assets | 7.10 | Storage media |
| A.11.2.6 | Security of equipment and assets off-premises | 7.9 | Security of assets off-premises |
| A.11.2.7 | Secure disposal or reuse of equipment | 7.14 | Secure disposal or reuse of equipment |
| A.11.2.8 | Unattended user equipment | 8.1 | User endpoint devices |
| A.11.2.9 | Clear desk and clear screen policy | 7.7 | Clear desk, clear screen policy |
| **A.12** | **Operations security** | **5** | **Organizational controls** |
| A.12.1.1 | Documented operating procedures | 5.37 | Documented operating procedures |
| **A.12** | **Operations security** | **8** | **Technological controls** |
| A.12.1.2 | Change management | 8.32 | Change management |
| A.12.1.3 | Capacity management | 8.6 | Capacity management |
| A.12.1.4 | Separation of development, testing and operational environments | 8.31 | Separation of development, test, and production environments |

| | | | |
|---|---|---|---|
| A.12.2.1 | Controls against malware | 8.7 | Protection against malware |
| A.12.3.1 | Information backup | 8.13 | Information backup |
| A.12.4.1 | Event logging | 8.15 | Logging |
| A.12.4.2 | Protection of log information | | |
| A.12.4.3 | Administrator and operator logs | | |
| Neu | | 8.16 | Monitoring activities |
| A.12.4.4 | Clock synchronization | 8.17 | Clock synchronization |
| A.12.5.1 | Installation of software on operational systems | 8.19 | Installation of software on operational systems |
| A.12.6.1 | Management of technical vulnerabilities | 8.8 | Management of technical vulnerabilities |
| Neu | | 8.9 | Configuration management |
| Neu | | 8.10 | Information deletion |
| Neu | | 8.11 | Data masking |
| Neu | | 8.12 | Data leakage prevention |
| **A.13** | **Communications security** | **8** | **Technological controls** |
| A.13.1.1 | Network controls | 8.20 | Network controls |
| A.13.1.2 | Security of network services | 8.21 | Security of network services |
| A.13.1.3 | Segregation in networks | 8.22 | Segregation in networks |
| Neu | | 8.23 | Web filtering |
| **A.13** | **Communications security** | **5** | **Organizational controls** |
| A.13.2.1 | Information transfer policies and procedures | 5.14 | Information transfer |
| A.13.2.2 | Agreements on information transfer | | |
| A.13.2.3 | Electronic messaging | | |

| A.13 | Communications security | 6 | People Controls |
|---|---|---|---|
| A.13.2.4 | Confidentiality or nondisclosure agreements | 6.6 | Confidentiality or nondisclosure agreements |
| **A.14** | **System and software acquisition, development, and maintenance** | **8** | **Technological controls** |
| A.14.1.1 | Information security requirements, analysis, and specifications | 5.8 | Information security in project management |
| A.14.1.2 | Securing applications services on public networks | 8.26 | Application security requirements |
| A.14.1.3 | Protecting application transactions | | |
| A.14.2.1 | Secure development policy | 8.25 | Secure development lifecycle |
| A.14.2.2 | System change control procedures | 8.32 | Change management |
| A.14.2.5 | Security system engineering principles | 8.27 | Secure system architecture and engineering principles |
| Neu | | 8.28 | Secure coding |
| A.14.2.6 | Secure development environment | 8.31 | Separation of development, test, and production environments |
| A.14.2.7 | Outsourced development | 8.30 | Outsourced development |
| A.14.2.8 | System security testing | 8.29 | Security testing in development and acceptance |
| A.14.2.9 | System acceptance testing | | |
| A.14.3.1 | Protection of test data | 8.33 | Test information |
| **A.15** | **Supplier relationships** | **5** | **Organizational controls** |
| A.15.1.1 | Information security in supplier relationships | 5.19 | Information security in supplier relationships |
| A.15.1.2 | Addressing security within supplier agreements | 5.20 | Addressing security within supplier agreements |
| A.15.1.3 | Information and communication technology supply chain | 5.21 | Managing information security in the ICT supply chain |

| | | | |
|---|---|---|---|
| A.15.2.1 | Monitoring and review of supplier services | 5.22 | Monitoring, review, and change management of supplier services |
| A.15.2.2 | Managing changes to supplier services | | |
| Neu | | 5.23 | Information security for use of cloud services |
| **A.16** | **Incident Management** | **5** | **Organizational controls** |
| A.16.1.1 | Responsibilities and procedures | 5.24 | Information security incident management planning and prep |
| **A.16** | **Incident Management** | **6** | **People Controls** |
| A.16.1.2 | Reporting information security events | 6.8 | Information security event reporting |
| A.16.1.3 | Reporting information security weaknesses | | |
| **A.16** | **Incident Management** | **5** | **Organizational controls** |
| A.16.1.4 | Assessment of and decision on information security events | 5.25 | Assessment and decision on information security events |
| A.16.1.5 | Response to information security incidents | 5.26 | Response to information security incidents |
| A.16.1.6 | Learning from information security incidents | 5.27 | Learning from information security incidents |
| A.16.1.7 | Collection of evidence | 5.28 | Collection of evidence |
| **A.17** | **Information security aspects of business continuity** | **5** | **Organizational controls** |
| A.17.1.1 | Planning information security continuity | 5.29 | Information security during disruption |
| A.17.1.2 | Implementing information security continuity | | |
| A.17.1.3 | Verify, review, and evaluate information security continuity | | |
| Neu | | 5.30 | ICT Readiness for business continuity |

| | | | |
|---|---|---|---|
| **A.17** | **Information security aspects of business continuity** | **8** | **Technological controls** |
| A.17.2.1 | Availability of information processing facilities | 8.14 | Redundancy of information processing facilities |
| **A.18** | **Compliance** | **5** | **Organizational controls** |
| A.18.1.1 | Identification of applicable legislative and contractual requirements | 5.31 | Identification of applicable legislative and contractual requirements |
| A.18.1.5 | Regulation of cryptographic controls | | |
| A.18.1.2 | Intellectual property rights | 5.32 | Intellectual property rights |
| A.18.1.3 | Protection of records | 5.33 | Protection of records |
| A.18.1.4 | Privacy and protection of personally identifiable information | 5.34 | Privacy and protection of PII |
| A.18.2.1 | Independent review of information security | 5.35 | Independent review of information security |
| A.18.2.2 | Compliance with security policies and standards | 5.36 | Compliance with security policies and standards |
| A.18.2.3 | Technical compliance review | | |