

Key Differences between ISO 27001:2022 and 27001:2013

Annex A Control Type	ISO/IEC 27001:2022 Annex A Identifier	ISO/IEC 27001:2013 Annex A Identifier	Annex A Name
Organisational Controls	Annex A 5.1	Annex A 5.1.1 Annex A 5.1.2	Policies for Information Security
Organisational Controls	Annex A 5.2	Annex A 6.1.1	Information Security Roles and Responsibilities
Organisational Controls	Annex A 5.3	Annex A 6.1.2	Segregation of Duties
Organisational Controls	Annex A 5.4	Annex A 7.2.1	Management Responsibilities
Organisational Controls	Annex A 5.5	Annex A 6.1.3	Contact With Authorities
Organisational Controls	Annex A 5.6	Annex A 6.1.4	Contact With Special Interest Groups
Organisational Controls	Annex A 5.7	NEW	Threat Intelligence
Organisational Controls	Annex A 5.8	Annex A 6.1.5 Annex A 14.1.1	Information Security in Project Management
Organisational Controls	Annex A 5.9	Annex A 8.1.1 Annex A 8.1.2	Inventory of Information and Other Associated Assets
Organisational Controls	Annex A 5.10	Annex A 8.1.3 Annex A 8.2.3	Acceptable Use of Information and Other Associated Assets
Organisational Controls	Annex A 5.11	Annex A 8.1.4	Return of Assets
Organisational Controls	Annex A 5.12	Annex A 8.2.1	Classification of Information
Organisational Controls	Annex A 5.13	Annex A 8.2.2	Labelling of Information
Organisational Controls	Annex A 5.14	Annex A 13.2.1 Annex A 13.2.2 Annex A 13.2.3	Information Transfer
Organisational Controls	Annex A 5.15	Annex A 9.1.1 Annex A 9.1.2	Access Control
Organisational Controls	Annex A 5.16	Annex A 9.2.1	Identity Management

Annex A Control Type	ISO/IEC 27001:2022 Annex A Identifier	ISO/IEC 27001:2013 Annex A Identifier	Annex A Name
Organisational Controls	Annex A 5.17	Annex A 9.2.4 Annex A 9.3.1 Annex A 9.4.3	Authentication Information
Organisational Controls	Annex A 5.18	Annex A 9.2.2 Annex A 9.2.5 Annex A 9.2.6	Access Rights
Organisational Controls	Annex A 5.19	Annex A 15.1.1	Information Security in Supplier Relationships
Organisational Controls	Annex A 5.20	Annex A 15.1.2	Addressing Information Security Within Supplier Agreements
Organisational Controls	Annex A 5.21	Annex A 15.1.3	Managing Information Security in the ICT Supply Chain
Organisational Controls	Annex A 5.22	Annex A 15.2.1 Annex A 15.2.2	Monitoring, Review and Change Management of Supplier Services
Organisational Controls	Annex A 5.23	NEW	Information Security for Use of Cloud Services
Organisational Controls	Annex A 5.24	Annex A 16.1.1	Information Security Incident Management Planning and Preparation
Organisational Controls	Annex A 5.25	Annex A 16.1.4	Assessment and Decision on Information Security Events
Organisational Controls	Annex A 5.26	Annex A 16.1.5	Response to Information Security Incidents
Organisational Controls	Annex A 5.27	Annex A 16.1.6	Learning From Information Security Incidents
Organisational Controls	Annex A 5.28	Annex A 16.1.7	Collection of Evidence
Organisational Controls	Annex A 5.29	Annex A 17.1.1 Annex A 17.1.2 Annex A 17.1.3	Information Security During Disruption
Organisational Controls	Annex A 5.30	NEW	ICT Readiness for Business Continuity
Organisational Controls	Annex A 5.31	Annex A 18.1.1 Annex A 18.1.5	Legal, Statutory, Regulatory and Contractual Requirements
Organisational Controls	Annex A 5.32	Annex A 18.1.2	Intellectual Property Rights
Organisational Controls	Annex A 5.33	Annex A 18.1.3	Protection of Records
Organisational Controls	Annex A 5.34	Annex A 18.1.4	Privacy and Protection of PII
Organisational Controls	Annex A 5.35	Annex A 18.2.1	Independent Review of Information Security

Annex A Control Type	ISO/IEC 27001:2022 Annex A Identifier	ISO/IEC 27001:2013 Annex A Identifier	Annex A Name
Organisational Controls	Annex A 5.36	Annex A 18.2.2 Annex A 18.2.3	Compliance With Policies, Rules and Standards for Information Security
Organisational Controls	Annex A 5.37	Annex A 12.1.1	Documented Operating Procedures
People Controls	Annex A 6.1	Annex A 7.1.1	Screening
People Controls	Annex A 6.2	Annex A 7.1.2	Terms and Conditions of Employment
People Controls	Annex A 6.3	Annex A 7.2.2	Information Security Awareness, Education and Training
People Controls	Annex A 6.4	Annex A 7.2.3	Disciplinary Process
People Controls	Annex A 6.5	Annex A 7.3.1	Responsibilities After Termination or Change of Employment
People Controls	Annex A 6.6	Annex A 13.2.4	Confidentiality or Non-Disclosure Agreements
People Controls	Annex A 6.7	Annex A 6.2.2	Remote Working
People Controls	Annex A 6.8	Annex A 16.1.2 Annex A 16.1.3	Information Security Event Reporting
Physical Controls	Annex A 7.1	Annex A 11.1.1	Physical Security Perimeters
Physical Controls	Annex A 7.2	Annex A 11.1.2 Annex A 11.1.6	Physical Entry
Physical Controls	Annex A 7.3	Annex A 11.1.3	Securing Offices, Rooms and Facilities
Physical Controls	Annex A 7.4	NEW	Physical Security Monitoring
Physical Controls	Annex A 7.5	Annex A 11.1.4	Protecting Against Physical and Environmental Threats
Physical Controls	Annex A 7.6	Annex A 11.1.5	Working In Secure Areas
Physical Controls	Annex A 7.7	Annex A 11.2.9	Clear Desk and Clear Screen
Physical Controls	Annex A 7.8	Annex A 11.2.1	Equipment Siting and Protection
Physical Controls	Annex A 7.9	Annex A 11.2.6	Security of Assets Off-Premises
Physical Controls	Annex A 7.10	Annex A 8.3.1 Annex A 8.3.2 Annex A 8.3.3 Annex A 11.2.5	Storage Media

Annex A Control Type	ISO/IEC 27001:2022 Annex A Identifier	ISO/IEC 27001:2013 Annex A Identifier	Annex A Name
Physical Controls	Annex A 7.11	Annex A 11.2.2	Supporting Utilities
Physical Controls	Annex A 7.12	Annex A 11.2.3	Cabling Security
Physical Controls	Annex A 7.13	Annex A 11.2.4	Equipment Maintenance
Physical Controls	Annex A 7.14	Annex A 11.2.7	Secure Disposal or Re-Use of Equipment
Technological Controls	Annex A 8.1	Annex A 6.2.1 Annex A 11.2.8	User Endpoint Devices
Technological Controls	Annex A 8.2	Annex A 9.2.3	Privileged Access Rights
Technological Controls	Annex A 8.3	Annex A 9.4.1	Information Access Restriction
Technological Controls	Annex A 8.4	Annex A 9.4.5	Access to Source Code
Technological Controls	Annex A 8.5	Annex A 9.4.2	Secure Authentication
Technological Controls	Annex A 8.6	Annex A 12.1.3	Capacity Management
Technological Controls	Annex A 8.7	Annex A 12.2.1	Protection Against Malware
Technological Controls	Annex A 8.8	Annex A 12.6.1 Annex A 18.2.3	Management of Technical Vulnerabilities
Technological Controls	Annex A 8.9	NEW	Configuration Management
Technological Controls	Annex A 8.10	NEW	Information Deletion
Technological Controls	Annex A 8.11	NEW	Data Masking
Technological Controls	Annex A 8.12	NEW	Data Leakage Prevention
Technological Controls	Annex A 8.13	Annex A 12.3.1	Information Backup
Technological Controls	Annex A 8.14	Annex A 17.2.1	Redundancy of Information Processing Facilities
Technological Controls	Annex A 8.15	Annex A 12.4.1 Annex A 12.4.2 Annex A 12.4.3	Logging
Technological Controls	Annex A 8.16	NEW	Monitoring Activities
Technological Controls	Annex A 8.17	Annex A 12.4.4	Clock Synchronization
Technological Controls	Annex A 8.18	Annex A 9.4.4	Use of Privileged Utility Programs
Technological Controls	Annex A 8.19	Annex A 12.5.1 Annex A 12.6.2	Installation of Software on Operational Systems
Technological Controls	Annex A 8.20	Annex A 13.1.1	Networks Security
Technological Controls	Annex A 8.21	Annex A 13.1.2	Security of Network Services
Technological Controls	Annex A 8.22	Annex A 13.1.3	Segregation of Networks

Annex A Control Type	ISO/IEC 27001:2022 Annex A Identifier	ISO/IEC 27001:2013 Annex A Identifier	Annex A Name
Technological Controls	Annex A 8.23	NEW	Web filtering
Technological Controls	Annex A 8.24	Annex A 10.1.1 Annex A 10.1.2	Use of Cryptography
Technological Controls	Annex A 8.25	Annex A 14.2.1	Secure Development Life Cycle
Technological Controls	Annex A 8.26	Annex A 14.1.2 Annex A 14.1.3	Application Security Requirements
Technological Controls	Annex A 8.27	Annex A 14.2.5	Secure System Architecture and Engineering Principles
Technological Controls	Annex A 8.28	NEW	Secure Coding
Technological Controls	Annex A 8.29	Annex A 14.2.8 Annex A 14.2.9	Security Testing in Development and Acceptance
Technological Controls	Annex A 8.30	Annex A 14.2.7	Outsourced Development
Technological Controls	Annex A 8.31	Annex A 12.1.4 Annex A 14.2.6	Separation of Development, Test and Production Environments
Technological Controls	Annex A 8.32	Annex A 12.1.2 Annex A 14.2.2 Annex A 14.2.3 Annex A 14.2.4	Change Management
Technological Controls	Annex A 8.33	Annex A 14.3.1	Test Information
Technological Controls	Annex A 8.34	Annex A 12.7.1	Protection of Information Systems During Audit Testing

Revision #1

Created 2026-01-06 19:18:22 UTC by Vlad Birgauanu

Updated 2026-01-06 19:18:58 UTC by Vlad Birgauanu