A-Trust GmbH
1030 Wien, Landstraßer Hauptstraße 1b, E02

Statement of Applicability (SoA)

SoA incl. mapping ISO27002 2013 ↔ 2022

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name	Applicable	Implemented (yes/no)
5.1	05.1.1, 05.1.2	Policies for information security	yes	yes
5.2	06.1.1	Information security roles and responsibilities	yes	yes
5.3	06.1.2	Segregation of duties	yes	yes
5.4	07.2.1	Management responsibilities	yes	yes
5.5	06.1.3	Contact with authorities	yes	yes
5.6	06.1.4	Contact with special interest groups	yes	yes
5.7	New	Threat intelligence	yes	yes
5.8	06.1.5, 14.1.1	Information security in project management	yes	yes
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets	yes	yes
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets	yes	yes
5.11	08.1.4	Return of assets	yes	yes
5.12	08.2.1	Classification of information	yes	yes
5.13	08.2.2	Labelling of information	yes	yes
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer	yes	yes
5.15	09.1.1, 09.1.2	Access control	yes	yes

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name	Applicable	Implemented (yes/no)
5.16	09.2.1	Identity management	yes	yes
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information	yes	yes
5.18	09.2.2, 09.2.5, 09.2.6	Access rights	yes	yes
5.19	15.1.1	Information security in supplier relationships	yes	yes
5.20	15.1.2	Addressing information security within supplier agreements	yes	yes
5.21	15.1.3	Managing information security in the ICT supply chain	yes	yes
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services	yes	yes
5.23	New	Information security for use of cloud services	yes	yes
5.24	16.1.1	Information security incident management planning and preparation	yes	yes
5.25	16.1.4	Assessment and decision on information security events	yes	yes
5.26	16.1.5	Response to information security incidents	yes	yes
5.27	16.1.6	Learning from information security incidents	yes	yes
5.28	16.1.7	Collection of evidence	yes	yes
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption	yes	yes
5.30	New	ICT readiness for business continuity	yes	yes
5.31	18.1.1, 18.1.5	Legal, statutory, regulatory and contractual requirements	yes	yes

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name	Applicable	Implemented (yes/no)
5.32	18.1.2	Intellectual property rights	yes	yes
5.33	18.1.3	Protection of records	yes	yes
5.34	18.1.4	Privacy and protection of PII	yes	yes
5.35	18.2.1	Independent review of information security	yes	yes
5.36	18.2.2, 18.2.3	Compliance with policies, rules and standards for information security	yes	yes
5.37	12.1.1	Documented operating procedures	yes	yes
6.1	07.1.1	Screening	yes	yes
6.2	07.1.2	Terms and conditions of employment	yes	yes
6.3	07.2.2	Information security awareness, education and training	yes	yes
6.4	07.2.3	Disciplinary process	yes	yes
6.5	07.3.1	Responsibilities after termination or change of employment	yes	yes
6.6	13.2.4	Confidentiality or non-disclosure agreements	yes	yes
6.7	06.2.2	Remote working	yes	yes
6.8	16.1.2, 16.1.3	Information security event reporting	yes	yes
7.1	11.1.1	Physical security perimeters	yes	yes
7.2	11.1.2, 11.1.6	Physical entry	yes	yes
7.3	11.1.3	Securing offices, rooms and facilities	yes	yes
7.4	New	Physical security monitoring	yes	yes
7.5	11.1.4	Protecting against physical and environmental threats	yes	yes

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name	Applicable	Implemented (yes/no)
7.6	11.1.5	Working in secure areas	yes	yes
7.7	11.2.9	Clear desk and clear screen	yes	yes
7.8	11.2.1	Equipment siting and protection	yes	yes
7.9	11.2.6	Security of assets off-premises	yes	yes
7.1	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media	yes	yes
7.11	11.2.2	Supporting utilities	yes	yes
7.12	11.2.3	Cabling security	yes	yes
7.13	11.2.4	Equipment maintenance	yes	yes
7.14	11.2.7	Secure disposal or re-use of equipment	yes	yes
8.1	06.2.1, 11.2.8	User endpoint devices	yes	yes
8.2	09.2.3	Privileged access rights	yes	yes
8.3	09.4.1	Information access restriction	yes	yes
8.4	09.4.5	Access to source code	yes	yes
8.5	09.4.2	Secure authentication	yes	yes
8.6	12.1.3	Capacity management	yes	yes
8.7	12.2.1	Protection against malware	yes	yes
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities	yes	yes
8.9	New	Configuration management	yes	yes
8.1	New	Information deletion	yes	yes
8.11	New	Data masking	yes	yes
8.12	New	Data leakage prevention	yes	yes

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name	Applicable	Implemented (yes/no)
8.13	12.3.1	Information backup	yes	yes
8.14	17.2.1	Redundancy of information processing facilities	yes	yes
8.15	12.4.1, 12.4.2, 12.4.3	Logging	yes	yes
8.16	New	Monitoring activities	yes	yes
8.17	12.4.4	Clock synchronization	yes	yes
8.18	09.4.4	Use of privileged utility programs	yes	yes
8.19	12.5.1, 12.6.2	Installation of software on operational systems	yes	yes
8.20	13.1.1	Networks security	yes	yes
8.21	13.1.2	Security of network services	yes	yes
8.22	13.1.3	Segregation of networks	yes	yes
8.23	New	Web filtering	yes	yes
8.24	10.1.1, 10.1.2	Use of cryptography	yes	yes
8.25	14.2.1	Secure development life cycle	yes	yes
8.26	14.1.2, 14.1.3	Application security requirements	yes	yes
8.27	14.2.5	Secure system architecture and engineering principles	yes	yes
8.28	New	Secure coding	yes	yes
8.29	14.2.8, 14.2.9	Security testing in development and acceptance	yes	yes
8.3	14.2.7	Outsourced development	yes	yes
8.31	12.1.4, 14.2.6	Separation of development, test and production environments	yes	yes

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name	Applicable	Implemented (yes/no)
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management	yes	yes
8.33	14.3.1	Test information	yes	yes
8.34	12.7.1	Protection of information systems during audit testing	yes	yes