Sophos Low Business Impact

Statement of Applicability

Legend (for Selected Controls and Reasons for controls selection)

LR: legal or regulatory requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment

Statement of Applicability

Version No.:	**2.0**	**Annex A Controls Summary**	
Approved Date:	**13 June 2024**	**Applicable**	**92**
Approved By:	**Chelsea Steiner**	**Not Applicable**	**1**

2013 Version Annex A	27001:2022 Annex A Control Number	Control Title	Control Applicable?	Justification for Inclusions of Control	Control Implemented?	Justification for Exclusions of Control
	5	**Organizational Controls**				
5.1.1, 5.1.2	5.1	Policies for information security	Yes	Business Requirements (Policy/Procedures)	Yes	
6.1.1	5.2	Information security roles and responsibilities	Yes	Business Requirements (Policy/Procedures)	Yes	
6.1.2	5.3	Segregation of duties	Yes	Business Requirements (Policy/Procedures)	Yes	
7.2.1	5.4	Management responsibilities	Yes	Business Requirements (Policy/Procedures)	Yes	
6.1.3	5.5	Contact with authorities	Yes	Business Requirements (Policy/Procedures)	Yes	
6.1.4	5.6	Contact with special interest groups	Yes	Business Requirements (Policy/Procedures)	Yes	
New	5.7	Threat intelligence	Yes	Business Requirements (Policy/Procedures)	Yes	
6.1.5, 14.1.1	5.8	Information security in project management	Yes	Business Requirements (Policy/Procedures)	Yes	
8.1.1, 8.1.2	5.9	Inventory of information and other associated assets	Yes	Business Requirements (Policy/Procedures)	Yes	
8.1.3, 8.2.3	5.10	Acceptable use of information and other associated assets	Yes	Business Requirements (Policy/Procedures)	Yes	
8.1.4	5.11	Return of assets	Yes	Business Requirements (Policy/Procedures)	Yes	
8.2.1	5.12	Classification of information	Yes	Business Requirements (Policy/Procedures)	Yes	
8.2.2	5.13	Labelling of information	Yes	Business Requirements (Policy/Procedures)	Yes	
13.2.1, 13.2.2, 13.2.3	5.14	Information transfer	Yes	Business Requirements (Policy/Procedures)	Yes	
9.1.1, 9.1.2	5.15	Access control	Yes	Business Requirements (Policy/Procedures)	Yes	

9.2.1	5.16	Identity management	Yes	Business Requirements (Policy/Procedures)	Yes	
9.2.4, 9.3.1, 9.4.3	5.17	Authentication information	Yes	Business Requirements (Policy/Procedures)	Yes	
9.2.2, 9.2.5, 9.2.6	5.18	Access rights	Yes	Business Requirements (Policy/Procedures)	Yes	
15.1.1	5.19	Information security in supplier relationships	Yes	Business Requirements (Policy/Procedures)	Yes	
15.1.2	5.20	Addressing information security within supplier agreements	Yes	Business Requirements (Policy/Procedures)	Yes	
15.1.3	5.21	Managing information security in the ICT supply chain	Yes	Business Requirements (Policy/Procedures)	Yes	
15.2.1, 15.2.2	5.22	Monitoring, review and change management of supplier services	Yes	Business Requirements (Policy/Procedures)	Yes	
New	5.23	Information security for use of cloud services	Yes	Business Requirements (Policy/Procedures)	Yes	
16.1.1	5.24	Information security incident management planning and preparation	Yes	Business Requirements (Policy/Procedures)	Yes	
16.1.4	5.25	Assessment and decision on information security events	Yes	Business Requirements (Policy/Procedures)	Yes	
16.1.5	5.26	Response to information security incidents	Yes	Business Requirements (Policy/Procedures)	Yes	
16.1.6	5.27	Learning from information security incidents	Yes	Business Requirements (Policy/Procedures)	Yes	
16.1.7	5.28	Collection of evidence	Yes	Business Requirements (Policy/Procedures)	Yes	
17.1.1, 17.1.2, 17.1.3	5.29	Information security during disruption	Yes	Business Requirements (Policy/Procedures)	Yes	
New	5.30	ICT readiness for business continuity	Yes	Business Requirements (Policy/Procedures)	Yes	
18.1.1, 18.1.5	5.31	Legal, statutory, regulatory and contractual requirements	Yes	Legal/Regulatory Requirements	Yes	
18.1.2	5.32	Intellectual property rights	Yes	Legal/Regulatory Requirements	Yes	
18.1.3	5.33	Protection of records	Yes	Legal/Regulatory Requirements	Yes	
18.1.4	5.34	Privacy and protection of PII	Yes	Legal/Regulatory Requirements	Yes	
18.2.1	5.35	Independent review of information security	Yes	Legal/Regulatory Requirements	Yes	

18.2.2, 18.2.3	5.36	Compliance with policies, rules and standards for information security	Yes	Legal/Regulatory Requirements	Yes	
12.1.1	5.37	Documented operating procedures	Yes	Business Requirements (Policy/Procedures)	Yes	
	6	**People Controls**				
7.1.1	6.1	Screening	Yes	Business Requirements (Policy/Procedures)	Yes	
7.1.2	6.2	Terms and conditions of employment	Yes	Business Requirements (Policy/Procedures)	Yes	
7.2.2	6.3	Information security awareness, education and training	Yes	Business Requirements (Policy/Procedures)	Yes	
7.2.3	6.4	Disciplinary process	Yes	Business Requirements (Policy/Procedures)	Yes	
7.3.1	6.5	Responsibilities after termination or change of employment	Yes	Business Requirements (Policy/Procedures)	Yes	
13.2.4	6.6	Confidentiality or non-disclosure agreements	Yes	Business Requirements (Policy/Procedures)	Yes	
6.2.2	6.7	Remote working	Yes	Business Requirements (Policy/Procedures)	Yes	
16.1.2, 16.1.3	6.8	Information security event reporting	Yes	Business Requirements (Policy/Procedures)	Yes	
	7	**Physical Controls**				
11.1.1	7.1	Physical security perimeters	Yes	Business Requirements (Policy/Procedures)	Yes	
11.1.2, 11.1.6	7.2	Physical entry	Yes	Business Requirements (Policy/Procedures)	Yes	
11.1.3	7.3	Securing offices, rooms and facilities	Yes	Business Requirements (Policy/Procedures)	Yes	
New	7.4	Physical security monitoring	Yes	Business Requirements (Policy/Procedures)	Yes	
11.1.4	7.5	Protecting against physical and environmental threats	Yes	Business Requirements (Policy/Procedures)	Yes	
11.1.5	7.6	Working in secure areas	Yes	Business Requirements (Policy/Procedures)	Yes	
11.2.9	7.7	Clear desk and clear screen	Yes	Business Requirements (Policy/Procedures)	Yes	
11.2.1	7.8	Equipment siting and protection	Yes	Business Requirements (Policy/Procedures)	Yes	
11.2.6	7.9	Security of assets off-premises	Yes	Business Requirements (Policy/Procedures)	Yes	

8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Storage media	Yes	Business Requirements (Policy/Procedures)	Yes	
11.2.2	7.11	Supporting utilities	Yes	Business Requirements (Policy/Procedures)	Yes	
11.2.3	7.12	Cabling security	Yes	Business Requirements (Policy/Procedures)	Yes	
11.2.4	7.13	Equipment maintenance	Yes	Business Requirements (Policy/Procedures)	Yes	
11.2.7	7.14	Secure disposal or re-use of equipment	Yes	Business Requirements (Policy/Procedures)	Yes	
	8	**Technological Controls**				
6.2.1, 11.2.8	8.1	User endpoint devices	Yes	Business Requirements (Policy/Procedures)	Yes	
9.2.3	8.2	Privileged access rights	Yes	Business Requirements (Policy/Procedures)	Yes	
9.4.1	8.3	Information access restriction	Yes	Business Requirements (Policy/Procedures)	Yes	
9.4.5	8.4	Access to source code	Yes	Business Requirements (Policy/Procedures)	Yes	
9.4.2	8.5	Secure authentication	Yes	Business Requirements (Policy/Procedures)	Yes	
12.1.3	8.6	Capacity management	Yes	Business Requirements (Policy/Procedures)	Yes	
12.2.1	8.7	Protection against malware	Yes	Business Requirements (Policy/Procedures)	Yes	
12.6.1, 18.2.3	8.8	Management of technical vulnerabilities	Yes	Business Requirements (Policy/Procedures)	Yes	
New	8.9	Configuration management	Yes	Business Requirements (Policy/Procedures)	Yes	
New	8.10	Information deletion	Yes	Business Requirements (Policy/Procedures)	Yes	
New	8.11	Data masking	Yes	Business Requirements (Policy/Procedures)	Yes	
New	8.12	Data leakage prevention	Yes	Business Requirements (Policy/Procedures)	Yes	
12.3.1	8.13	Information backup	Yes	Business Requirements (Policy/Procedures)	Yes	
17.2.1	8.14	Redundancy of information processing facilities	Yes	Business Requirements (Policy/Procedures)	Yes	
12.4.1, 12.4.2, 12.4.3	8.15	Logging	Yes	Business Requirements (Policy/Procedures)	Yes	

New	8.16	Monitoring activities	Yes	Business Requirements (Policy/Procedures)	Yes	
12.4.4	8.17	Clock synchronization	Yes	Business Requirements (Policy/Procedures)	Yes	
9.4.4	8.18	Use of privileged utility programs	Yes	Business Requirements (Policy/Procedures)	Yes	
12.5.1, 12.6.2	8.19	Installation of software on operational systems	Yes	Business Requirements (Policy/Procedures)	Yes	
13.1.1	8.20	Networks security	Yes	Business Requirements (Policy/Procedures)	Yes	
13.1.2	8.21	Security of network services	Yes	Business Requirements (Policy/Procedures)	Yes	
13.1.3	8.22	Segregation of networks	Yes	Business Requirements (Policy/Procedures)	Yes	
New	8.23	Web filtering	Yes	Business Requirements (Policy/Procedures)	Yes	
10.1.1, 10.1.2	8.24	Use of cryptography	Yes	Business Requirements (Policy/Procedures)	Yes	
14.2.1	8.25	Secure development life cycle	Yes	Business Requirements (Policy/Procedures)	Yes	
14.1.2, 14.1.3	8.26	Application security requirements	Yes	Business Requirements (Policy/Procedures)	Yes	
14.2.5	8.27	Secure system architecture and engineering principles	Yes	Business Requirements (Policy/Procedures)	Yes	
New	8.28	Secure coding	Yes	Business Requirements (Policy/Procedures)	Yes	
14.2.8, 14.2.9	8.29	Security testing in development and acceptance	Yes	Business Requirements (Policy/Procedures)	Yes	
14.2.7	8.30	Outsourced development	No	Business Requirements (Policy/Procedures)	No	Sophos does not outsource development.
12.1.4, 14.2.6	8.31	Separation of development, test and production environments	Yes	Business Requirements (Policy/Procedures)	Yes	
12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Change management	Yes	Business Requirements (Policy/Procedures)	Yes	
14.3.1	8.33	Test information	Yes	Business Requirements (Policy/Procedures)	Yes	
12.7.1	8.34	Protection of information systems during audit testing	Yes	Business Requirements (Policy/Procedures)	Yes	