Statement of Applicability - SoA

Last updated and approved on 8 January 2026

This Statement of Applicability lists all ISO/IEC 27001:2022 Annex A controls and identifies their applicability to Visma Enterprise A/S based on legal requirements (LR), contractual obligations (CO), business requirements (BR), best practice (BP), or results from risk assessments (RA). These applicability criteria serve as the justification for inclusion or exclusion of each control.

Visma Enterprise A/S has implemented all Annex A controls.

Annex A Control (ISO/IEC 27002:2022)		Applicability (LR/CO/BR/BP/RA)	Status on control implementation
5.1	Policies for information security	CO;BP;RA	Implemented
5.2	Information security roles and responsibilities	CO;BP;RA	Implemented
5.3	Segregation of duties	CO;BP;RA	Implemented
5.4	Management responsibilities	CO;BP;RA	Implemented
5.5	Contact with authorities	LR;CO;BP;RA	Implemented
5.6	Contact with special interest groups	CO;BP;RA	Implemented
5.7	Threat intelligence	CO;BP;RA	Implemented
5.8	Information security in project management	CO;BP;RA	Implemented
5.9	Inventory of information and other associated assets	CO;BP;RA	Implemented

5.10	Acceptable use of information and other associated assets	CO;BP;RA	Implemented
5.11	Return of assets	CO;BP;RA	Implemented
5.12	Classification of information	LR;CO;BP;RA	Implemented
5.13	Labelling of information	CO;BP;RA	Implemented
5.14	Information transfer	CO;BP;RA	Implemented
5.15	Access control	CO;BP;RA	Implemented
5.16	Identity management	CO;BP;RA	Implemented
5.17	Authentication information	CO;BP;RA	Implemented
5.18	Access rights	CO;BP;RA	Implemented
5.19	Information security in supplier relationships	LR;CO;BR;BP;RA	Implemented
5.20	Addressing information security within supplier agreements	LR;CO;BR;BP;RA	Implemented
5.21	Managing information security in the ICT supply chain	CO;BR;BP;RA	Implemented

5.22	Monitoring, review and change management of supplier services	LR;CO;BP;RA	Implemented
5.23	Information security for use of cloud services	LR;CO;BP;RA	Implemented
5.24	Information security incident management planning and preparation	LR;CO;BP;RA	Implemented
5.25	Assessment and decision on information security events	CO;BP;RA	Implemented
5.26	Response to information security incidents	CO;BP;RA	Implemented
5.27	Learning from information security incidents	CO;BP;RA	Implemented
5.28	Collection of evidence	CO;BP;RA	Implemented
5.29	Information security during disruption	CO;BR;BP;RA	Implemented
5.30	ICT readiness for business continuity	CO;BR;BP;RA	Implemented
5.31	Legal, statutory, regulatory and contractual requirements	LR;CO;BP;RA	Implemented
5.32	Intellectual property rights	CO;BP;RA	Implemented
5.33	Protection of records	LR;CO;BP;RA	Implemented

5.34	Privacy and protection of personal identifiable information (PII)	LR;CO;BP;RA	Implemented
5.35	Independent review of information security	CO;BP;RA	Implemented
5.36	Compliance with policies, rules and standards for information security	CO;BP;RA	Implemented
5.37	Documented operating procedures	CO;BP;RA	Implemented
6.1	Screening	LR;CO;BP;RA	Implemented
6.2	Terms and conditions of employment	CO;BP;RA	Implemented
6.3	Information security awareness, education and training	CO;BP;RA	Implemented
6.4	Disciplinary process	CO;BP;RA	Implemented
6.5	Responsibilities after termination or change of employment	CO;BP;RA	Implemented
6.6	Confidentiality or non-disclosure agreements	CO;BP;RA	Implemented
6.7	Remote working	CO;BP;RA	Implemented
6.8	Information security event reporting	LR;CO;BP;RA	Implemented

7.1	Physical security perimeters	CO;BP;RA	Implemented
7.2	Physical entry	CO;BP;RA	Implemented
7.3	Securing offices, rooms and facilities	CO;BP;RA	Implemented
7.4	Physical security monitoring	CO;BP;RA	Implemented
7.5	Protecting against physical and environmental threats	CO;BP;RA	Implemented
7.6	Working in secure areas	CO;BP;RA	Implemented
7.7	Clear desk and clear screen	CO;BP;RA	Implemented
7.8	Equipment siting and protection	CO;BP;RA	Implemented
7.9	Security of assets off-premises	CO;BP;RA	Implemented
7.10	Storage media	CO;BP;RA	Implemented
7.11	Supporting utilities	CO;BP;RA	Implemented
7.12	Cabling security	CO;BP;RA	Implemented
7.13	Equipment maintenance	CO;BP;RA	Implemented
7.14	Secure disposal or re-use of equipment	CO;BP;RA	Implemented

8.1	User end point devices	CO;BP;RA	Implemented
8.2	Privileged access rights	CO;BP;RA	Implemented
8.3	Information access restriction	CO;BP;RA	Implemented
8.4	Access to source code	CO;BP;RA	Implemented
8.5	Secure authentication	CO;BP;RA	Implemented
8.6	Capacity management	CO;BP;RA	Implemented
8.7	Protection against malware	CO;BP;RA	Implemented
8.8	Management of technical vulnerabilities	CO;BP;RA	Implemented
8.9	Configuration management	CO;BP;RA	Implemented
8.10	Information deletion	LR;CO;BP;RA	Implemented
8.11	Data masking	LR;CO;BP;RA	Implemented
8.12	Data leakage prevention	BP;RA	Implemented
8.13	Information backup	CO;BP;RA	Implemented
8.14	Redundancy of information processing facilities	CO;BR;BP;RA	Implemented
8.15	Logging	CO;BR;BP;RA	Implemented

8.16	Monitoring activities	CO;BR;BP;RA	Implemented
8.17	Clock synchronization	CO;BP;RA	Implemented
8.18	Use of privileged Utility programs	CO;BP;RA	Implemented
8.19	Installation of software on operational systems	CO;BP;RA	Implemented
8.20	Networks security	CO;BP;RA	Implemented
8.21	Security of network services	CO;BP;RA	Implemented
8.22	Segregation of networks	CO;BP;RA	Implemented
8.23	Web filtering	BP;RA	Implemented
8.24	Use of cryptography	CO;BP;RA	Implemented
8.25	Secure development life cycle	CO;BP;RA	Implemented
8.26	Application security requirements	LR;CO;BP;RA	Implemented
8.27	Secure system architecture and engineering principles	CO;BP;RA	Implemented
8.28	Secure coding	CO;BP;RA	Implemented
8.29	Security testing in development and acceptance	CO;BP;RA	Implemented

8.30	Outsourced development	CO;BP;RA	Implemented
8.31	Separation of development, test and production environments	CO;BP;RA	Implemented
8.32	Change management	CO;BP;RA	Implemented
8.33	Test information	CO;BP;RA	Implemented
8.34	Protection of information systems during audit testing	CO;BP;RA	Implemented