Statement of Applicability - SoA

What is SoA?

SoA stands for Statement of Applicability. It is a statement of the level of security the organization has decided and why.

The SoA document thus supports why the organization do one thing in one area, and another thing in another area. All based on the organization's risk assessment. The SoA document can be seen as a status statement for the organization's work with information security and as documentation of decisions on selected and deselected regarding security efforts.

Usage

Overview of selected and deselected control items and actions and overview of the responsible of the controls.

Also remember to update ISMS audit plan if areas are selected or deselected.

Process

P: Working with controls - Visma Enterprise A/S

ISO/IEC 27001:2013 Annex A controls			Applicable	Responsible (owner of control - udførende af kontrol)	Remarks (with justification for exclusions)	*Selected controls and reasons for selection				Status on control implementation
						LR	CO	BR /BP	RRA	
Clause	**Sec**	**Control Objective /Control**								
5 Security Policies	**5.1**	**Management direction for information security**								
	5.1.1	Policies for information	Yes	The Information Security Officer is responsible for preparing, maintaining, and monitoring the implementation of this policy. The management is responsible for approving the policies.			CO	BP	RRA	Implemented
	5.1.2	Review of the policies for information security	Yes	Information Security			CO	BP	RRA	Implemented

6 Organisation of information security	**6.1**	**Internal organisation**								
	6.1.1	Information security roles and responsibilities	Yes	Information Security			CO	BP	RRA	Implemented
	6.1.2	Segregation of duties	Yes	Operations			CO	BP	RRA	Implemented
	6.1.3	Contact with authorities	Yes	Information Security Legal		LR	CO	BP	RRA	Implemented
	6.1.4	Contact with special interest groups	Yes	Legal			CO	BP	RRA	Implemented
	6.1.5	Information security in project management	Yes	Product Development			CO	BP	RRA	Implemented
	6.2	**Mobile devices and teleworking**								Implemented
	6.2.1	Mobile device policy	Yes	Information Security			CO	BP	RRA	Implemented
	6.2.2	Teleworking	Yes	Information Security			CO	BP	RRA	Implemented
7 Human resource security	**7.1**	**Prior to employment**								
	7.1.1	Screening	Yes	HR		LR	CO	BP	RRA	Implemented
	7.1.2	Terms and conditions of employment	Yes	HR			CO	BP	RRA	Implemented
	7.2	**During employment**								Implemented
	7.2.1	Management responsibilities	Yes	HR Information Security			CO	BP	RRA	Implemented
	7.2.2	Information security awareness, education and training	Yes	HR Information Security			CO	BP	RRA	Implemented
	7.2.3	Disciplinary process	Yes	HR			CO	BP	RRA	Implemented
	7.3	**Termination and change of employment**								
	7.3.1	Termination or change of employment responsibilities	Yes	HR			CO	BP	RRA	Implemented
8 Asset management (sammen)	**8.1**	**Responsibility for assets**								
	8.1.1	Inventory of assets	Yes	Information Security			CO	BP	RRA	Implemented
	8.1.2	Ownership of assets	Yes	Information Security			CO	BP	RRA	Implemented
	8.1.3	Acceptable use of assets	Yes	Information Security			CO	BP	RRA	Implemented
	8.1.4	Return of assets	Yes	HR			CO	BP	RRA	Implemented
	8.2	**Information classification**								
	8.2.1	Classification of information	Yes	Information Security		LR	CO	BP	RRA	Implemented
	8.2.2	Labeling of information	Yes	Information Security			CO	BP	RRA	Implemented
	8.2.3	Handling of assets	Yes	Information Security			CO	BP	RRA	Implemented

	8.3	**Media handling**								
	8.3.1	Management of removable media	Yes	Information Security			CO	BP	RRA	Implemented
	8.3.2	Disposal of media	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	8.3.3	Physical media transfer	Yes	Information Security			CO	BP	RRA	Implemented
9 Access control	**9.1**	**Business requirements of access control**								
	9.1.1	Access control policy	Yes	Information Security			CO	BP	RRA	Implemented
	9.1.2	Access to networks and network services	Yes	Information Security			CO	BP	RRA	Implemented
	9.2	**User access management**								
	9.2.1	User registration and de-registration	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	9.2.2	User access provisioning	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	9.2.3	Management of privileged access rights	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	9.2.4	Management of secret authentication information of users	Yes	Operations (handled by supplier relationship ID 64)			CO	BP	RRA	Implemented
	9.2.5	Review of user access rights	Yes	Information Security			CO	BP	RRA	Implemented
	9.2.6	Removal or adjustment of access rights	Yes	HR			CO	BP	RRA	Implemented
	9.3	**User responsibilities**								
	9.3.1	Use of secret authentication information	Yes	Information Security			CO	BP	RRA	Implemented
	9.4	**System and application access control**								
	9.4.1	Information access restriction	Yes	Information Security			CO	BP	RRA	Implemented
	9.4.2	Secure log-on procedures	Yes	Information Security			CO	BP	RRA	Implemented
	9.4.3	Password management system	Yes	Operations: (handled by supplier relationship ID 64)			CO	BP	RRA	Implemented
	9.4.4	Use of privileged utility programs	Yes	Operations			CO	BP	RRA	Implemented
	9.4.5	Access control to program source code	Yes	Information Security			CO	BP	RRA	Implemented
10 Cryptography	**10.1**	**Cryptographic controls**								
	10.1.1	Policy on the use of cryptographic controls	Yes	Information Security			CO	BP	RRA	Implemented
	10.1.2	Key management	Yes	Information Security			CO	BR	RRA	Implemented
11 Physical and environmental security	**11.1**	**Secure areas**								

	11.1.1	Physical security perimeter	Yes	Information Security			CO	BP	RRA	Implemented
	11.1.2	Physical entry controls	Yes	Information Security (handled by supplier relationship)			CO	BP	RRA	Implemented
	11.1.3	Securing office, room and facilities	Yes	Information Security (handled by supplier relationship)			CO	BP	RRA	Implemented
	11.1.4	Protecting against external end environmental threats	Yes	Operations (handled by supplier relationship ID 69)			CO	BP	RRA	Implemented
	11.1.5	Working in secure areas	Yes	Information Security			CO	BP	RRA	Implemented
	11.1.6	Delivery and loading areas	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	11.2	**Equipment**								
	11.2.1	Equipment siting and protection	Yes	Information Security			CO	BP	RRA	Implemented
	11.2.2	Supporting utilities	Yes	Operations (handled by supplier relationship ID 69)			CO	BP	RRA	Implemented
	11.2.3	Cabling security	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	11.2.4	Equipment maintenance	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	11.2.5	Removal of assets	Yes	Information Security			CO	BP	RRA	Implemented
	11.2.6	Security of equipment and assets off-premises	Yes	Information Security			CO	BP	RRA	Implemented
	11.2.7	Secure disposal or re-use of equipment	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	11.2.8	Unattended user equipment	Yes	Information Security			CO	BP	RRA	Implemented
	11.2.9	Clear desk and clear screen policy	Yes	Information Security			CO	BP	RRA	Implemented
12 Operations security	**12.1**	**Operational procedures and responsibilities**								
	12.1.1	Documented operating procedures	Yes	Operations			CO	BP	RRA	Implemented
	12.1.2	Change management	Yes	Product Development			CO	BP	RRA	Implemented
	12.1.3	Capacity management	Yes	Operations (handled by supplier relationship ID 80)			CO	BP	RRA	Implemented
	12.1.4	Separation of development, testing and operational environments	Yes	Operations Operations (handled by supplier relationship ID 120)			CO	BP	RRA	Implemented
	12.2	**Protection from malware**								

	12.2.1	Controls against malware	Yes	Operations (handled by supplier relationship ID 82)			CO	BP	RRA	Implemented
	12.3	**Backup**								
	12.3.1	Information backup	Yes	Operations (handled by supplier relationship ID 83)			CO	BP	RRA	Implemented
	12.4	**Logging and monitoring**								
	12.4.1	Event logging	Yes	Operations Product Development Operations (handled by supplier relationship)			CO	BR	RRA	Implemented
	12.4.2	Protection of log information	Yes	Operations Product Development Operations (handled by supplier relationship)			CO	BR	RRA	Implemented
	12.4.3	Administrator and operator logs	Yes	Operations Product Development Operations (handled by supplier relationship)			CO	BR	RRA	Implemented
	12.4.4	Clock synchronisation	Yes	Operations (handled by supplier relationship ID 121)			CO	BP	RRA	Implemented
	12.5	**Control of operational software**								
	12.5.1	Installation of software on operational systems	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	12.6	**Technical vulnerability management**								
	12.6.1	Management of technical vulnerabilities	Yes	Operations Operations (handled by supplier relationship ID 91)			CO	BP	RRA	Implemented
	12.6.2	Restrictions on software installation	Yes	Operations (handled by supplier relationship)			CO	BP	RRA	Implemented
	12.7	**Information systems audit considerations**								
	12.7.1	Information systems audit controls	Yes	Operations			CO	BP	RRA	Implemented
13 Communications security	**13.1**	**Network security management**								
	13.1.1	Network controls	Yes	Operations (handled by supplier relationship ID 95)			CO	BP	RRA	Implemented
	13.1.2	Security of network services	Yes	Operations (handled by supplier relationship ID 95)			CO	BP	RRA	Implemented
	13.1.3	Segregation in networks	Yes	Operations (handled by supplier relationship ID 95)			CO	BP	RRA	Implemented
	13.2	**Information transfer**								
	13.2.1	Information transfer policies and procedures	Yes	Information Security			CO	BP	RRA	Implemented

	13.2.2	Agreements on information transfer	Yes	Information Security Legal			CO	BP	RRA	Implemented
	13.2.3	Electronic messaging	Yes	Information Security		LR	CO	BP	RRA	Implemented
	13.2.4	Confidentiality or non-disclosure agreements	Yes	HR Legal			CO	BP	RRA	Implemented
14 System acquisition, development and maintenance	**14.1**	**Security requirements of information systems**								
	14.1.1	Information security requirements analysis and specification	Yes	Legal		LR	CO	BP	RRA	Implemented
	14.1.2	Securing applications services on public networks	Yes	Legal		LR	CO	BP	RRA	Implemented
	14.1.3	Protecting application services transactions	Yes	Legal		LR	CO	BP	RRA	Implemented
	14.2	**Security in development and support processes**								
	14.2.1	Secure development policy	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.2	System change control procedures	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.3	Technical review of applications after operating platform changes	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.4	Restrictions on changes to software packages	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.5	Secure system engineering principles	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.6	Secure development environment	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.7	Outsourced development	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.8	System security testing	Yes	Product Development			CO	BP	RRA	Implemented
	14.2.9	System acceptance testing	Yes	Product Development			CO	BP	RRA	Implemented
	14.3	**Test data**								
	14.3.1	Protection of test data	Yes	Product Development			CO	BP	RRA	Implemented
15 Supplier relationships	**15.1**	**Information security in supplier relationships**								
	15.1.1	Information security policy for supplier relationships	Yes	Legal Information Security		LR	CO	BR	RRA	Implemented

	15.1.2	Addressing security within supplier agreements	Yes	Legal Information Security		LR	CO	BR	RRA	Implemented
	15.1.3	Information and communication technology supply chain	Yes	Legal Information Security			CO	BR	RRA	Implemented
	15.2	**Supplier service delivery management**								
	15.2.1	Monitoring and review of supplier services	Yes	Operations Information Security		LR	CO	BP	RRA	Implemented
	15.2.2	Managing changes to supplier services	Yes	Operations Legal			CO	BP	RRA	Implemented
16 Information security incident management	**16.1**	**Management of information security incidents and improvements**								
	16.1.1	Responsibilities and procedures	Yes	Information Security (Data Protection Manager ved privacy breach)		LR	CO	BP	RRA	Implemented
	16.1.2	Reporting information security events	Yes	Information Security Data Protection Manager ved privacy breach)		LR	CO	BP	RRA	Implemented
	16.1.3	Reporting information security weaknesses	Yes	Information Security			CO	BP	RRA	Implemented
	16.1.4	Assessment of and decision on information security events	Yes	Information Security			CO	BP	RRA	Implemented
	16.1.5	Response to information security incidents	Yes	Information Security			CO	BP	RRA	Implemented
	16.1.6	Learning from information security incidents	Yes	Information Security			CO	BP	RRA	Implemented
	16.1.7	Collection of evidence	Yes	Legal			CO	BP	RRA	Implemented
17 Information security aspects of business continuity management	**17.1**	**Information security continuity**								
	17.1.1	Planning information security continuity	Yes	Operations Information Security			CO	BR	RRA	Implemented
	17.1.2	Implementing information security continuity	Yes	Operations			CO	BR	RRA	Implemented
	17.1.3	Verify, review and evaluate information security continuity	Yes	Operations			CO	BR	RRA	Implemented
	17.2	**Redundancies**								
	17.2.1	Availability of information processing facilities	Yes	Operations (handled by supplier relationship)			CO	BR	RRA	Implemented
18 Compliance	**18.1**	**Compliance with legal and contractual requirements**								

18.1.1	Identification of applicable legislation and contractual requirements	Yes	Legal		LR	CO	BP	RRA	Implemented
18.1.2	Intellectual property rights	Yes	HR Operations Legal			CO	BP	RRA	Implemented
18.1.3	Protection of records	Yes	Information Security		LR	CO	BP	RRA	Implemented
18.1.4	Privacy and protection of personally identifiable information	Yes	Legal		LR	CO	BP	RRA	Implemented
18.1.5	Regulation of cryptographic controls	Yes	Legal			CO		RRA	Implemented
18.2	**Information security reviews**								
18.2.1	Independent review of information security	Yes	Information Security			CO	BP	RRA	Implemented
18.2.2	Compliance with security policies and standards	Yes	Information Security			CO	BP	RRA	Implemented
18.2.3	Technical compliance review	Yes	Operations			CO	BP	RRA	Implemented

*Selected Controls and Reasons for controls selection:

- LR: Legal requirements
- CO: Contractual obligations
- BR/BP: Business requirements /adopted best practices
- RRA: Results of risk assessment,TSE: to some extent