Statement of Applicability (SOA)

SOA along wioth scope define the boundary for an organisations' ISMS.

It defines the following:

- Applicable and the not applicable requirements
- Justification for inclusion and exclusion
- Currently implemented or not

Additional Coral references

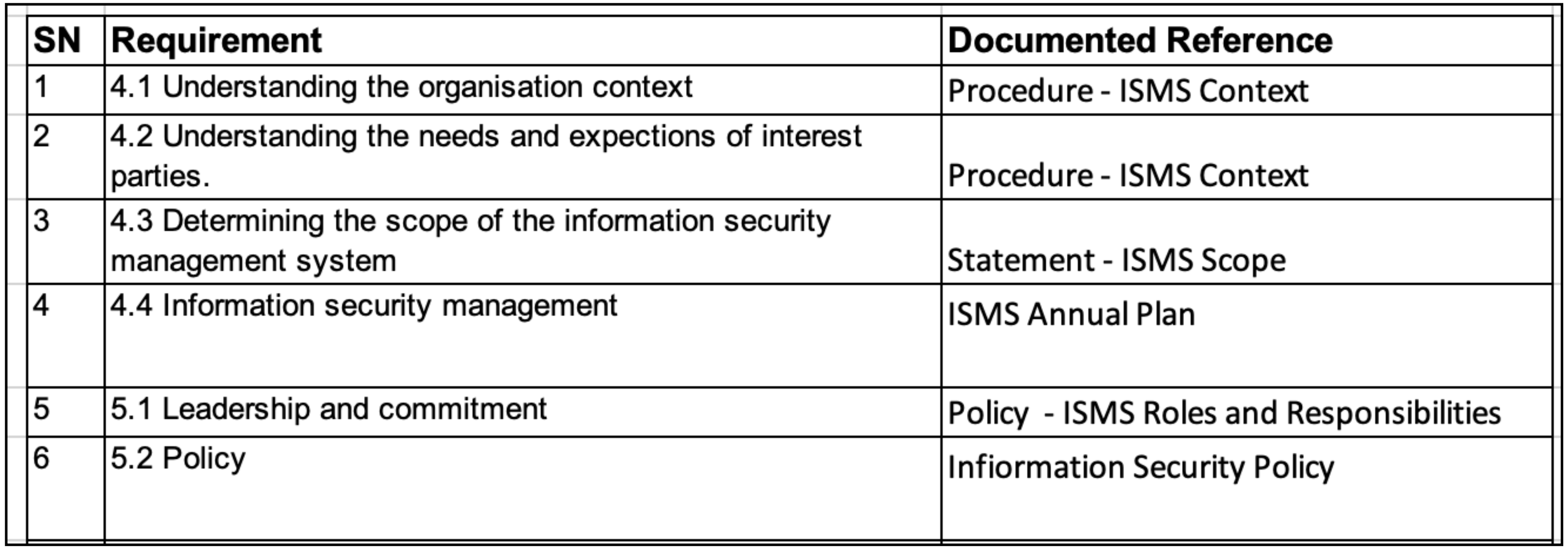
- policy/procedure references – enables easy audit references for implementer and auditor
- Risk owner – role or function responsible for the specific requirement

ISO 27001:22 reference:

6.1.3 Information security risk treatment
d) produce a Statement of Applicability (SOA)

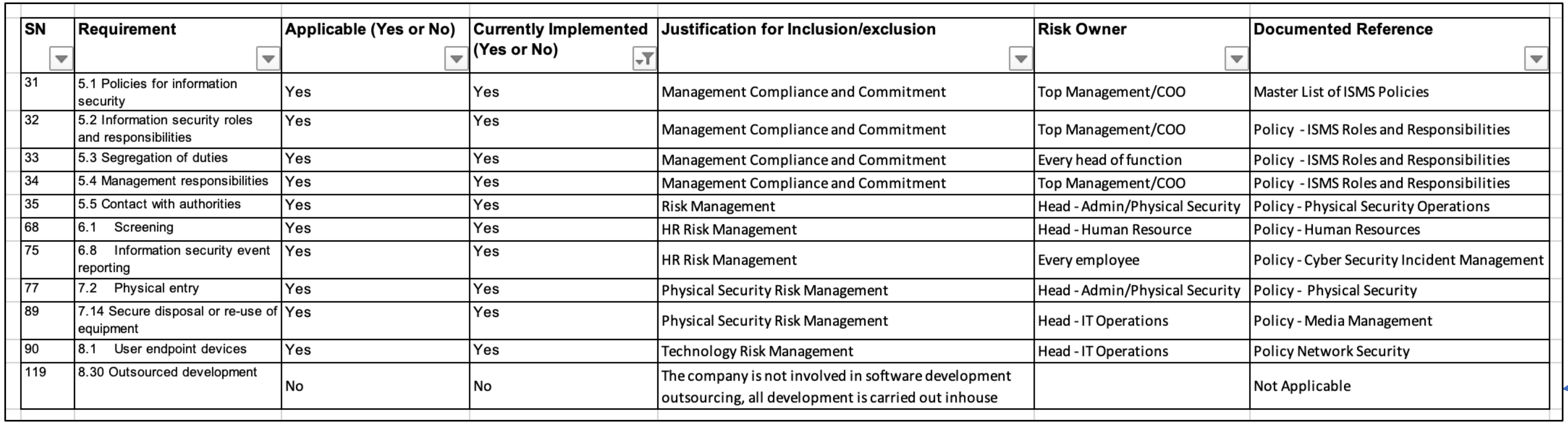
Additional Note: SOA has many other usages such as in distributing controls and setting accountability in the organisation, as well as documenting contextual risk assessment.

Management System Clauses



SN	Requirement	Documented Reference
1	4.1 Understanding the organisation context	Procedure - ISMS Context
2	4.2 Understanding the needs and expections of interest parties.	Procedure - ISMS Context
3	4.3 Determining the scope of the information security management system	Statement - ISMS Scope
4	4.4 Information security management	ISMS Annual Plan
5	5.1 Leadership and commitment	Policy - ISMS Roles and Responsibilities
6	5.2 Policy	Inficormation Security Policy

Annexure Controls



SN	Requirement	Applicable (Yes or No)	Currently Implemented (Yes or No)	Justification for Inclusion/exclusion	Risk Owner	Documented Reference
31	5.1 Policies for information security	Yes	Yes	Management Compliance and Commitment	Top Management/COO	Master List of ISMS Policies
32	5.2 Information security roles and responsibilities	Yes	Yes	Management Compliance and Commitment	Top Management/COO	Policy - ISMS Roles and Responsibilities
33	5.3 Segregation of duties	Yes	Yes	Management Compliance and Commitment	Every head of function	Policy - ISMS Roles and Responsibilities
34	5.4 Management responsibilities	Yes	Yes	Management Compliance and Commitment	Top Management/COO	Policy - ISMS Roles and Responsibilities
35	5.5 Contact with authorities	Yes	Yes	Risk Management	Head - Admin/Physical Security	Policy - Physical Security Operations
68	6.1 Screening	Yes	Yes	HR Risk Management	Head - Human Resource	Policy - Human Resources
75	6.8 Information security event reporting	Yes	Yes	HR Risk Management	Every employee	Policy - Cyber Security Incident Management
77	7.2 Physical entry	Yes	Yes	Physical Security Risk Management	Head - Admin/Physical Security	Policy - Physical Security
89	7.14 Secure disposal or re-use of equipment	Yes	Yes	Physical Security Risk Management	Head - IT Operations	Policy - Media Management
90	8.1 User endpoint devices	Yes	Yes	Technology Risk Management	Head - IT Operations	Policy Network Security
119	8.30 Outsourced development	No	No	The company is not involved in software development outsourcing, all development is carried out inhouse		Not Applicable

Example of a not applicable control with justification for exclusion

Questions?

Write to us roadmap@coralesecure.com

Interested in a demo of all the policy documents and templates?

Kindly book a slot using calendly.com/probcy