INFOCUS-IT

Part-3

ISO 27001

Ver.2022

ISO27001:2022 lead Implementor Course

By Jagbir Singh | jagbir@infocus-it.com
MTech(CS) | LLB |CISA | ISO27001LA |ISO22301LA|CEH|CHFI

Clause -7 | Support

- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

Clause -7 | Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

Think of resource - Categorise them People , Process , technology & organization

ISO27001:2022

Clause -7 | Support

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

ISO27001:2022

Clause -7 | Support

Exercise-13	Resource and Competence matrix

Make a list of Resources required for ISMS and what qualification they need to possess They will be part of Information security working group

Competence Matrix

ISO27001:2022

Clause -7 | Support

7.3 Awareness

Persons doing work under the organization’s control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

Information security awareness ppt / Awareness Posters / Do’s and Don’t posters / Quiz and Mailers

INFOCUS-IT Provides phishing drill , cyber drill , cyber range , virtual machines for attach and defence trainings

ISO27001:2022

Clause -7 | Support

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

Communication plan , quick contact list , emergency list

Clause -7 | Support

ISO27001:2022

7.5 Documented information

7.5.1 General

The organization’s information security management system shall include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

Clause -7 | Support

ISO27001:2022

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

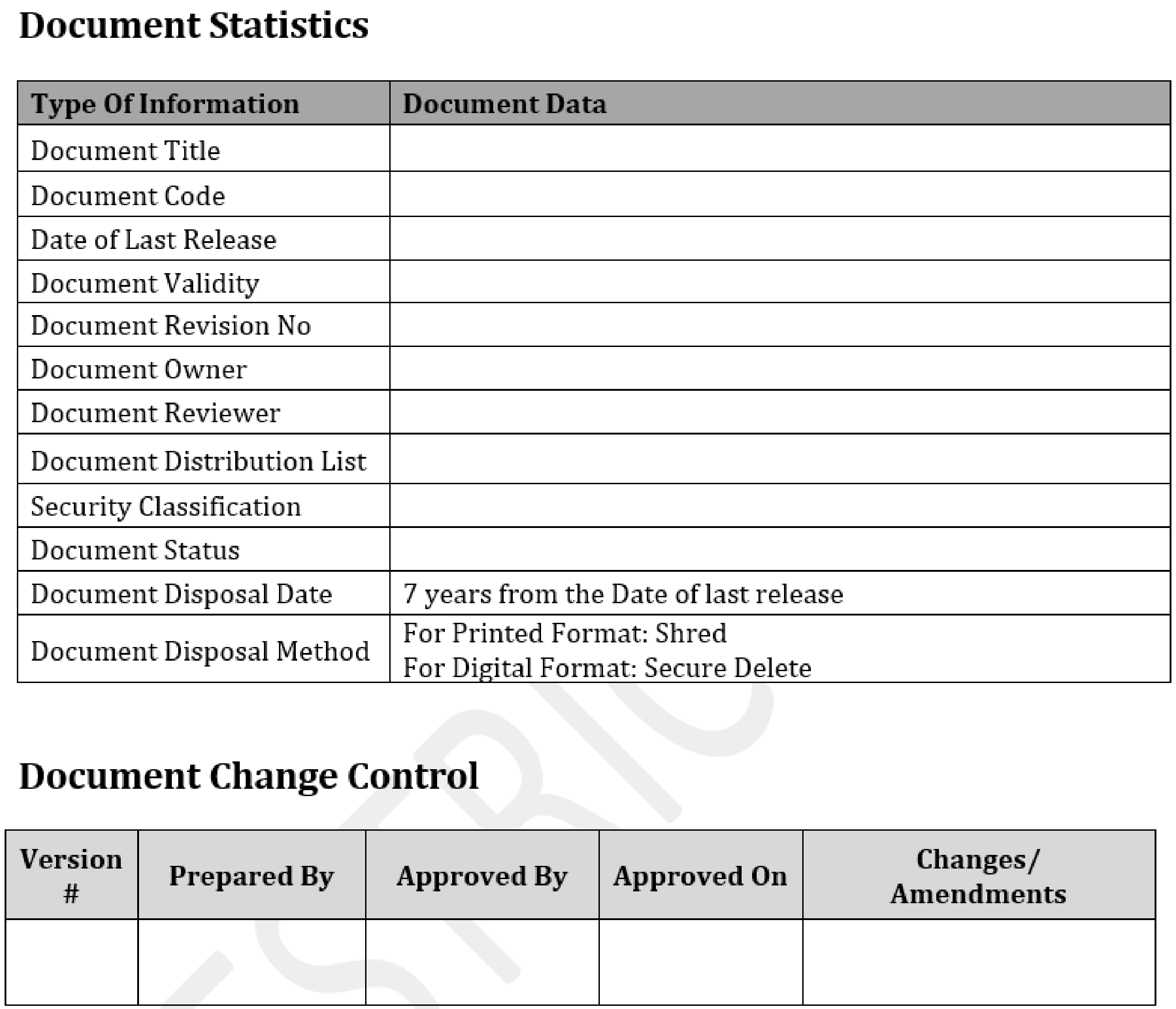
a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

Clause -7 | Support

7.5.2 Creating and updating



Document Statistics

Type Of Information	Document Data
Document Title	
Document Code	
Date of Last Release	
Document Validity	
Document Revision No	
Document Owner	
Document Reviewer	
Document Distribution List	
Security Classification	
Document Status	
Document Disposal Date	7 years from the Date of last release
Document Disposal Method	For Printed Format: Shred For Digital Format: Secure Delete

Document Change Control

Version #	Prepared By	Approved By	Approved On	Changes/ Amendments

Clause -7 | Support

ISO27001:2022

7.5.3 Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

Control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) retention and disposition.

ISO27001:2022

Clause -7 | Support

7.5.3 Control of documented information

Exercise-15 : Policy / process doc for Document control

Exercise-16 : Define communication Plan /policy

Clause -8 | Operation

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

Clause -8 | Operation

ISO27001:2022

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:
— establishing criteria for the processes;
— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

ISO27001:2022

Clause -8 | Operation

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

* Progress Tracker

ISO27001:2022

Clause -8 | Operation

8.3 Information security risk treatment

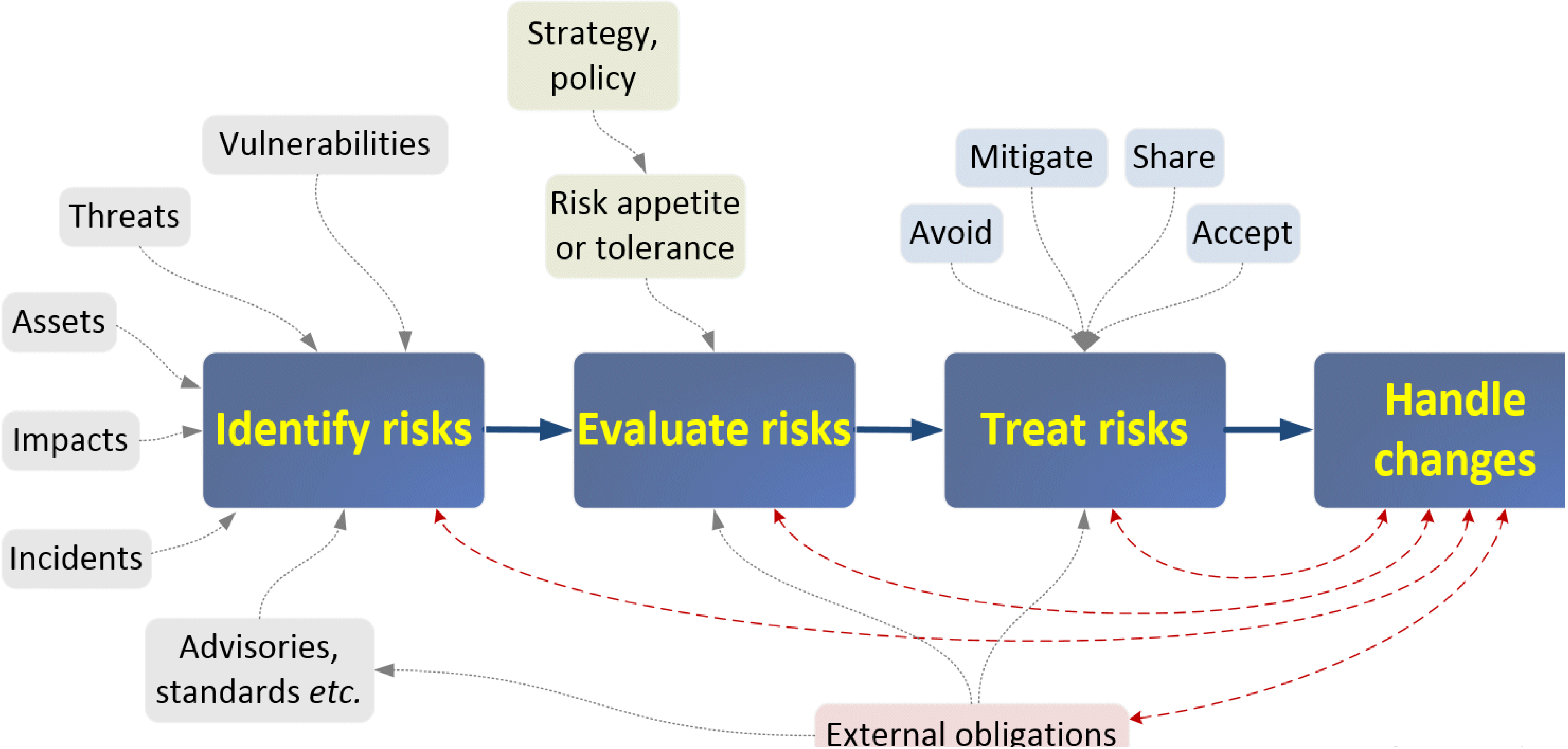
The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

Clause -8 | Operation

ISO27001:2022

8.3 Information security risk treatment



ISO27001:2022

Clause -8 | Operation

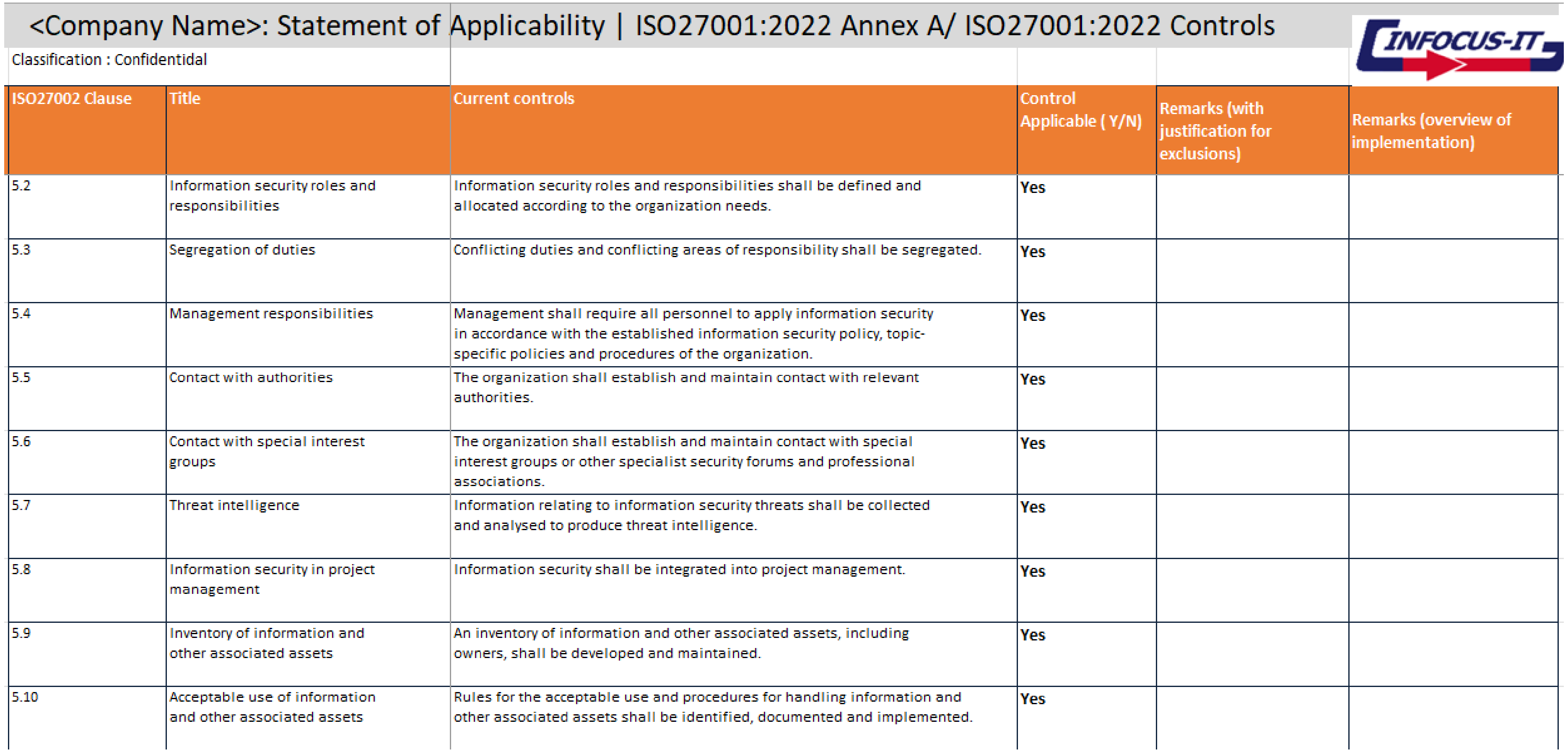
8.3 Information security risk treatment

Exercise-17 : Prepare Risk Treatment Plan

ISO27001:2022

Clause -8 | Operation

Statement of Applicability (SOA)



<Company Name>: Statement of Applicability | ISO27001:2022 Annex A/ ISO27001:2022 Controls

INFOCUS-IT

Classification : Confidentidal

ISO27002 Clause	Title	Current controls	Control Applicable (Y/N)	Remarks (with justification for exclusions)	Remarks (overview of implementation)
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes		
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes		
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes		
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes		
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes		
5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes		
5.8	Information security in project management	Information security shall be integrated into project management.	Yes		
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes		
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes		

ISO27001:2022

Clause -8 | Operation

Statement of Applicability (SOA)

Exercise-17 A – SOA