INFOCUS-IT

Part-4

ISO 27001

Ver.2022

ISO27001:2022 lead Implementor Course

By Jagbir Singh | jagbir@infocus-it.com

MTech(CS) | LLB |CISA | ISO27001LA |ISO22301LA|CEH|CHFI

ISO27001:2022

Clause -9 | Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

Clause -9 | Performance evaluation

ISO27001:2022

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

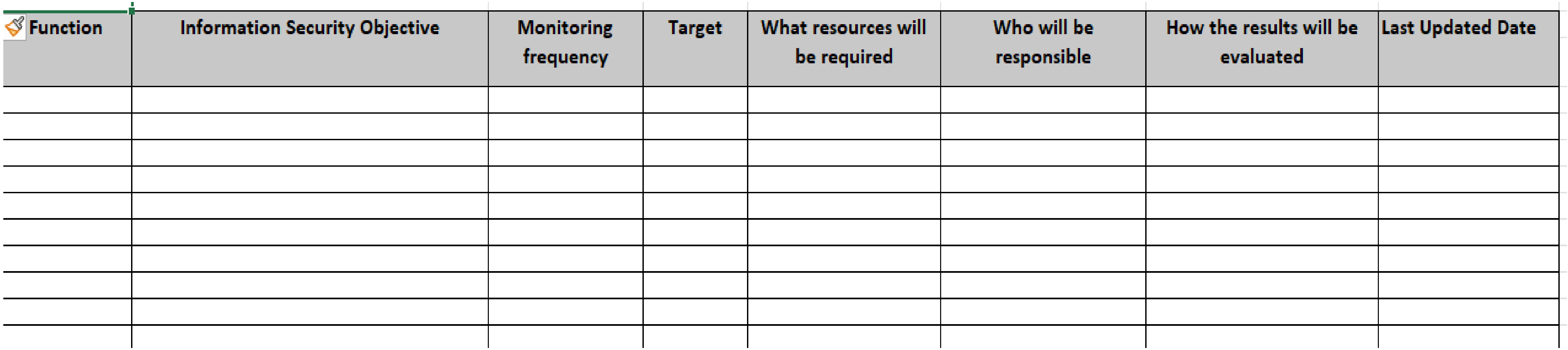
Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

Clause -9 | Performance evaluation

ISO27001:2022

9.1 Monitoring, measurement, analysis and evaluation



Function	Information Security Objective	Monitoring frequency	Target	What resources will be required	Who will be responsible	How the results will be evaluated	Last Updated Date

Clause -9 | Performance evaluation

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization’s own requirements for its information security management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

Clause -9 | Performance evaluation

9.2 Internal audit

9.2.1 General

Internal Audit Training – Who will do this , check the Roles and responsibilities

List of internal auditors

Name	Dept/Function	Designation

Clause -9 | Performance evaluation

9.2 Internal audit

Audit Criteria

1. ISMS Standard (ISO27001:2022)
2. Interested Party Requirements
3. ISMS Documents
4. Legal Requirements

ISO27001:2022

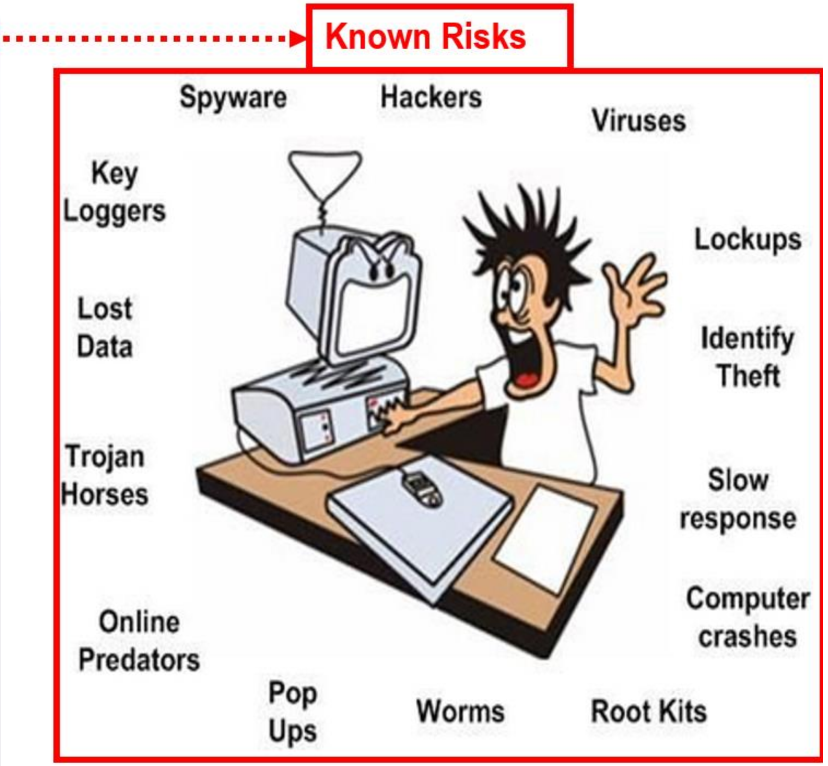
Clause -9 | Performance evaluation

9.2 Internal audit

Auditors to check Organization’s knowledge on Information Security

- Known risks are those that have been identified and analyzed
- Unknown risks cannot be managed, may be addressed by contingency plan

Known Risks
Un-Known Risks



Clause -9 | Performance evaluation

ISO27001:2022

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

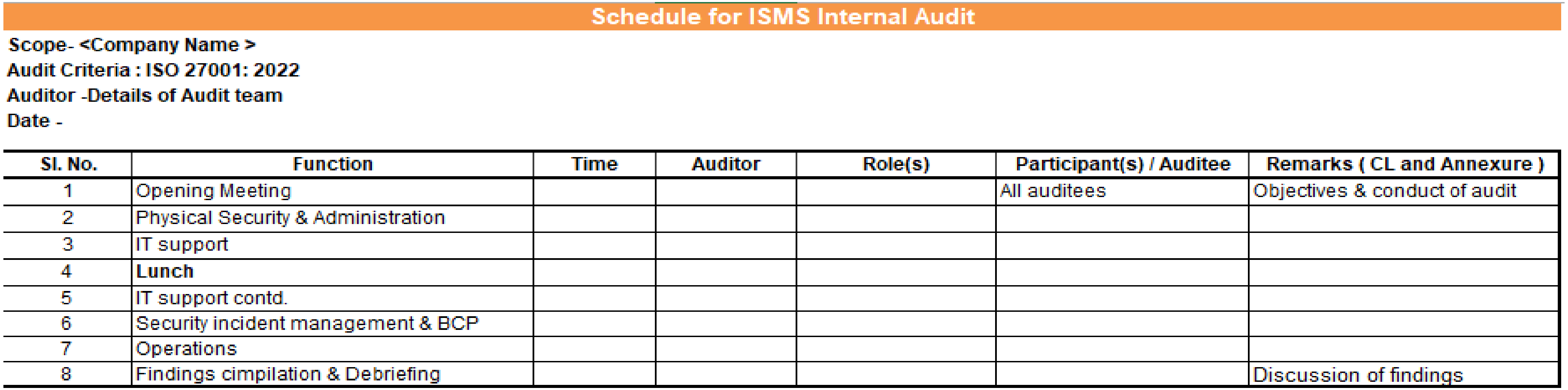
Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

Clause -9 | Performance evaluation

ISO27001:2022

9.2.2 Internal audit programme

Internal Audit Plan



Schedule for ISMS Internal Audit

Scope- <Company Name >
Audit Criteria : ISO 27001: 2022
Auditor -Details of Audit team
Date -

Sl. No.	Function	Time	Auditor	Role(s)	Participant(s) / Auditee	Remarks (CL and Annexure)
1	Opening Meeting				All auditees	Objectives & conduct of audit
2	Physical Security & Administration					
3	IT support					
4	**Lunch**					
5	IT support contd.					
6	Security incident management & BCP					
7	Operations					
8	Findings cimpilation & Debriefing					Discussion of findings

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

Clause -9 | Performance evaluation

ISO27001:2022

9.2.2 Internal audit programme Internal Audit Plan

Exercise-18	**Define Internal Audit Schedule**
Exercise-19	**Internal Audit training**
Exercise-19	**Internal Audit Process**

ISO27001:2022

Clause -9 | Performance evaluation

9.3 Management review

9.3.1 General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

Exercise-20 **Management Review Process**

Clause -9 | Performance evaluation

ISO27001:2022

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;
2) monitoring and measurement results;
3) audit results;
4) fulfilment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

ISO27001:2022

Clause -9 | Performance evaluation

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

Exercise-21 Corrective action process Management Review Process

ISO27001:2022

Clause -10 | Improvement

10.1 Continual improvement

10.2 Nonconformity and corrective action

ISO27001:2022

Clause -10 | Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

Clause -10 | Improvement

ISO27001:2022

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
   1) take action to control and correct it;
   2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1) reviewing the nonconformity;
   2) determining the causes of the nonconformity; and
   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system,

if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of:

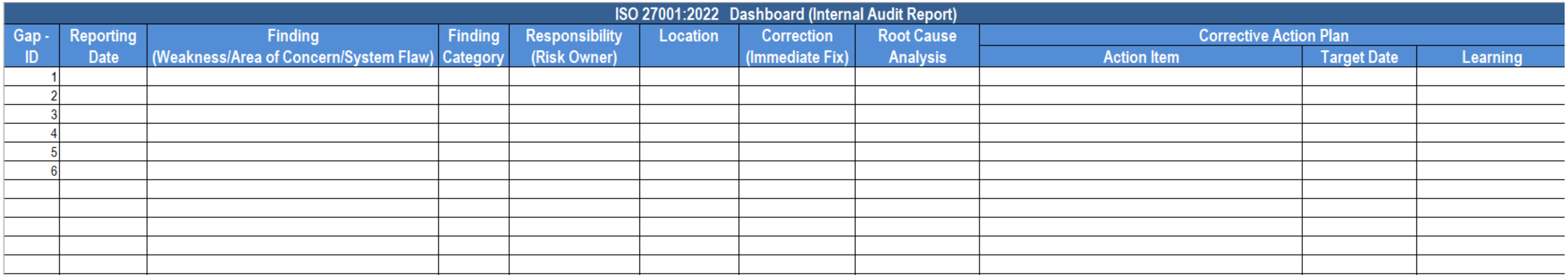
f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.

Clause -10 | Improvement

ISO27001:2022

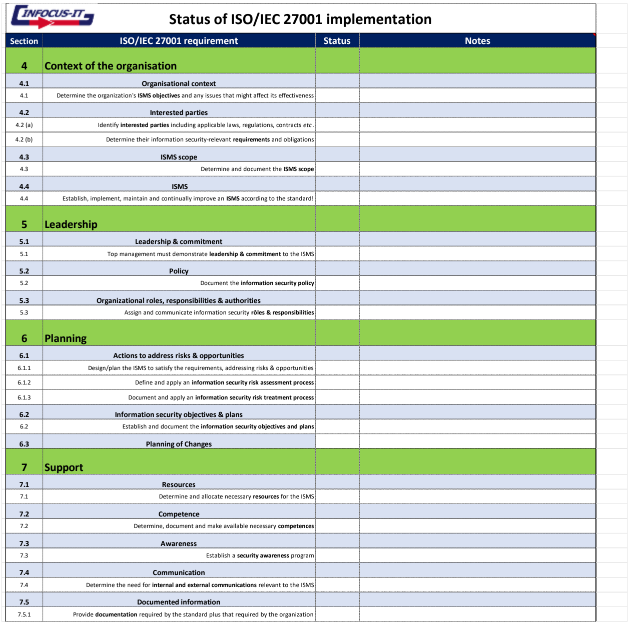
10.2 Nonconformity and corrective action



ISO 27001:2022 Dashboard (Internal Audit Report)

Gap - ID	Reporting Date	Finding (Weakness/Area of Concern/System Flaw)	Finding Category	Responsibility (Risk Owner)	Location	Correction (Immediate Fix)	Root Cause Analysis	Corrective Action Plan		
								Action Item	Target Date	Learning
1										
2										
3										
4										
5										
6										

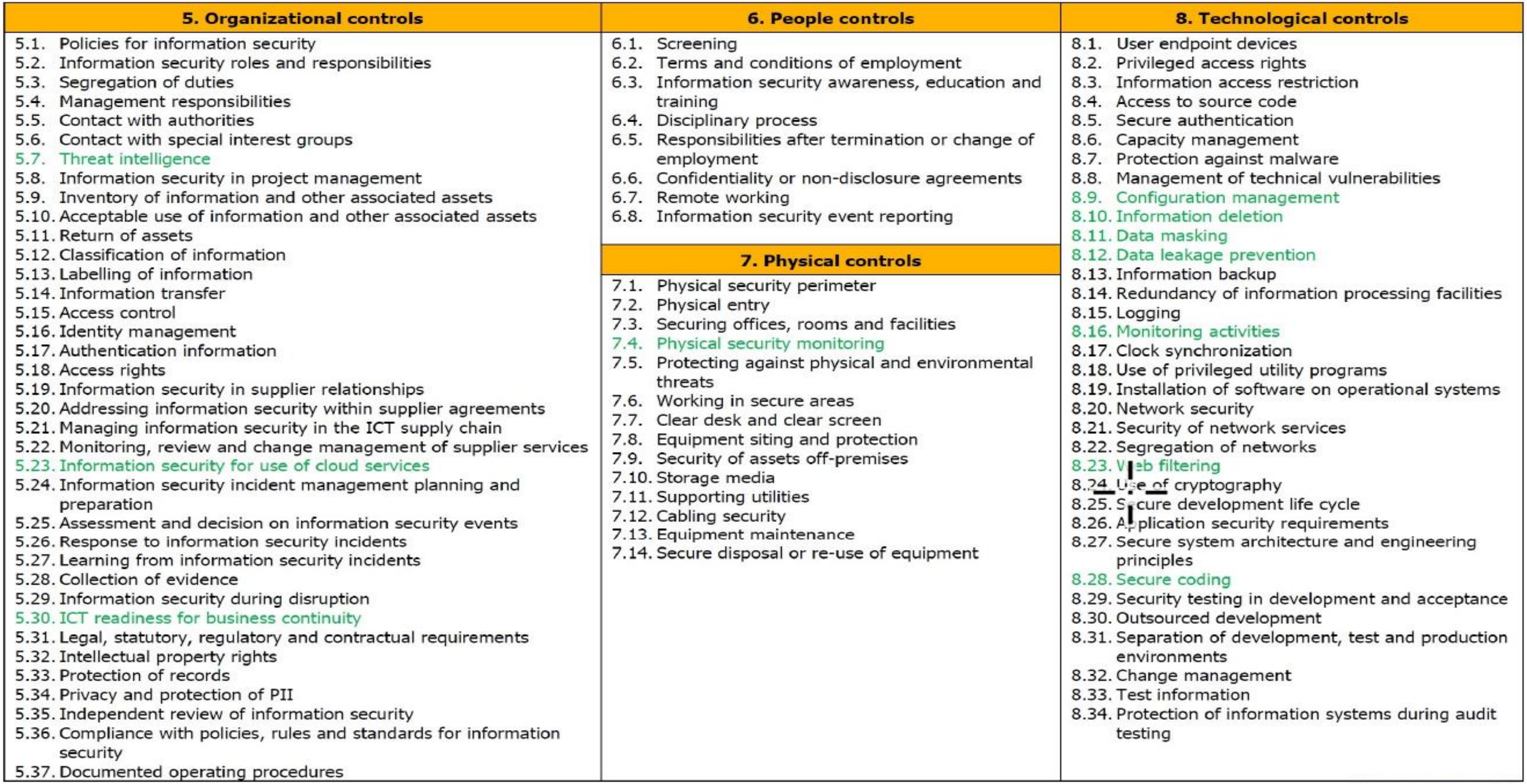
CHECKLIST FOR COMPLETE IMPLEMENTATION – ISO27001:2022



Status of ISO/IEC 27001 implementation

Section	ISO/IEC 27001 requirement	Status	Notes
4	**Context of the organisation**		
4.1	**Organisational context**		
4.1	Determine the organization's **ISMS objectives** and any issues that might affect its effectiveness		
4.2	**Interested parties**		
4.2 (a)	Identify **interested parties** including applicable laws, regulations, contracts *etc*.		
4.2 (b)	Determine their information security-relevant **requirements** and obligations		
4.3	**ISMS scope**		
4.3	Determine and document the **ISMS scope**		
4.4	**ISMS**		
4.4	Establish, implement, maintain and continually improve an **ISMS** according to the standard!		
5	**Leadership**		
5.1	**Leadership & commitment**		
5.1	Top management must demonstrate **leadership & commitment** to the ISMS		
5.2	**Policy**		
5.2	Document the **information security policy**		
5.3	**Organizational roles, responsibilities & authorities**		
5.3	Assign and communicate information security **rôles & responsibilities**		
6	**Planning**		
6.1	**Actions to address risks & opportunities**		
6.1.1	Design/plan the ISMS to satisfy the requirements, addressing risks & opportunities		
6.1.2	Define and apply an **information security risk assessment process**		
6.1.3	Document and apply an **information security risk treatment process**		
6.2	**Information security objectives & plans**		
6.2	Establish and document the **information security objectives and plans**		
6.3	**Planning of Changes**		
7	**Support**		
7.1	**Resources**		
7.1	Determine and allocate necessary **resources** for the ISMS		
7.2	**Competence**		
7.2	Determine, document and make available necessary **competences**		
7.3	**Awareness**		
7.3	Establish a **security awareness** program		
7.4	**Communication**		
7.4	Determine the need for **internal and external communications** relevant to the ISMS		
7.5	**Documented information**		
7.5.1	Provide **documentation** required by the standard plus that required by the organization		

Exercise A – Start here



5. Organizational controls

5.1. Policies for information security
5.2. Information security roles and responsibilities
5.3. Segregation of duties
5.4. Management responsibilities
5.5. Contact with authorities
5.6. Contact with special interest groups
5.7. Threat intelligence
5.8. Information security in project management
5.9. Inventory of information and other associated assets
5.10. Acceptable use of information and other associated assets
5.11. Return of assets
5.12. Classification of information
5.13. Labelling of information
5.14. Information transfer
5.15. Access control
5.16. Identity management
5.17. Authentication information
5.18. Access rights
5.19. Information security in supplier relationships
5.20. Addressing information security within supplier agreements
5.21. Managing information security in the ICT supply chain
5.22. Monitoring, review and change management of supplier services
5.23. Information security for use of cloud services
5.24. Information security incident management planning and preparation
5.25. Assessment and decision on information security events
5.26. Response to information security incidents
5.27. Learning from information security incidents
5.28. Collection of evidence
5.29. Information security during disruption
5.30. ICT readiness for business continuity
5.31. Legal, statutory, regulatory and contractual requirements
5.32. Intellectual property rights
5.33. Protection of records
5.34. Privacy and protection of PII
5.35. Independent review of information security
5.36. Compliance with policies, rules and standards for information security
5.37. Documented operating procedures

6. People controls

6.1. Screening
6.2. Terms and conditions of employment
6.3. Information security awareness, education and training
6.4. Disciplinary process
6.5. Responsibilities after termination or change of employment
6.6. Confidentiality or non-disclosure agreements
6.7. Remote working
6.8. Information security event reporting

7. Physical controls

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

8. Technological controls

8.1. User endpoint devices
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
8.6. Capacity management
8.7. Protection against malware
8.8. Management of technical vulnerabilities
8.9. Configuration management
8.10. Information deletion
8.11. Data masking
8.12. Data leakage prevention
8.13. Information backup
8.14. Redundancy of information processing facilities
8.15. Logging
8.16. Monitoring activities
8.17. Clock synchronization
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
8.20. Network security
8.21. Security of network services
8.22. Segregation of networks
8.23. Web filtering
8.24. Use of cryptography
8.25. Secure development life cycle
8.26. Application security requirements
8.27. Secure system architecture and engineering principles
8.28. Secure coding
8.29. Security testing in development and acceptance
8.30. Outsourced development
8.31. Separation of development, test and production environments
8.32. Change management
8.33. Test information
8.34. Protection of information systems during audit testing

*New control, 2022

Activities Home – Task

Exercise-0	Your Objective from this course & Exercise
Exercise-1	Terms & Definitions pertaining to ISO27001
Exercise-2	Auditing Information Security Principles
Exercise-3	External and Internal Issues – list down the external and internal issues consider you company as case study for ISO27001 implementation.
Exercise-4	List down interested parties
Exercise-5	Write Scope statement
Exercise-6	Write your Information security policy
Exercise-7	Draw Organization chart as per your company structure (only to cover information security team & concerned team)
Exercise-8	Define Roles and responsibilities as per the organization chart in exercise -7
Exercise-9	Risk Assessment and Risk Assessment methodology. Asset base V/s Issue base Risk assessment
Exercise-10	Make a list of information asset (Inventory)
Exercise-11	Make a list of Risk / Issues as per your organization
Exercise-12	List down information security objectives of your organization
Exercise-13	Resource and Competence matrix
Exercise-14	Resource and Competence matrix
Exercise-15	Policy / process doc for Document control
Exercise-16	Define communication Plan /policy
Exercise-17	Risk treatment plan
Exercise-18	Define Internal Audit Schedule
Exercise-19	Internal Audit training
Exercise-20	Internal Audit Process
Exercise-21	Management Review Process
Exercise-22	Corrective action process Management Review Process
Exercise-23	Prepare Your own checklist - for Implemention & Audit
Exercise-24	Internal Audit template
Exercise-25	Non Confirmity Exercise
Exercise-26	NC – Template
Exercise-27	Final Audit Report - Template

ISO27001:2022

1.Introduction – describes what information security is and why an organization should manage risks.
2.Scope – covers high-level requirements for an ISMS to apply to all types or organizations.
3.Normative References – explains the relationship between ISO 27000 and 27001 standards.
4.Terms and Definitions – covers the complex terminology that is used within the standard.
5.Context of the Organization – explains what stakeholders should be involved in the creation and maintenance of the ISMS.
6.Leadership – describes how leaders within the organization should commit to ISMS policies and procedures.
7.Planning – covers an outline of how risk management should be planned across the organization.
8.Support – describes how to raise awareness about information security and assign responsibilities.
9.Operation – covers how risks should be managed and how documentation should be performed to meet audit standards.
10.Performance Evaluation – provides guidelines on how to monitor and measure the performance of the ISMS.
11.Improvement – explains how the ISMS should be continually updated and improved, especially following audits.
12.Reference Control Objectives and Controls – provides an annex detailing the individual elements of an audit.

Quick Links

Course Presented by

Jagbir Singh

INFOCUS IT CONSULTING PVT ltd.

Course link

https://infocus-it.com/iso-27001-2022-lead-implementer-course/

YouTube Channel

INFOCUSIT

Telegram group – ISO27001_2022 | support@infocus-it.com

If you like this course please write your comments on our YouTube channel , LinkedIn and tag me And don’t forgot to like , Subscribe our channel .