DELEGATE NOTES

| **INFORMATION SECURITY**  **MANAGEMENT SYSTEM**  **REQUIREMENTS**  **ISO/IEC 27001:2022**  **Exemplar Global - IS**    26th December 2022  Confidential |
| --- |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 1 of 134

| **TRAINING PLAN** | | |
| --- | --- | --- |
| **DAY 1** | | |
| **TIME** | **DURATION** | **ACTIVITY** |
| 09.00- 09.45am | 45 mins | \* Introduction and Course Objectives  \* Overview -Annex SL - Common Text for ISO standards |
| 09.45 -10.30am | 45 mins | \* **Section 1:** Clause 3 ISMS Terms & Definitions  \* **Section 2:** Clause 4 External Context and Information security requirements and ISMS Legal compliance |
| 10.30 - 10.45am | 15 min | *Morning Tea* |
| 10.45 –11.30pm | 45 min | \* **Section 3:** Clause 5 Leadership and Management Commitment, Reviewing Scope of ISMS |
| 11.30 – 12.30pm | 1 hr | \* **Section 4:** Clause 6 Reviewing Risk Assessment methodology & Risk Register |
| 12.30 - 01.30pm | 1 hr | *Lunch* |
| 01.30 - 03.00pm | 1 hr 30 min | \* **Section 5:** Clause 8 Reviewing Risk Treatment Plan – Overview of Annex A and reviewing the Statement of Applicability (SOA). |
| 03.00-3.30pm | 15 min | *Afternoon Tea* |
| 03.30 - 4.15 pm | 45 min | \* **Section 6:** Clause 7 Reviewing Support Processes including HR \* **Section 7:** Clause 7 Reviewing ISMS Documented information requirements |
| 04.15- 05.00 pm | 45 min | \* **Section 8:** Clause 9 Reviewing ISMS implementation and effectiveness  \* **Section 9:** Clause 9 & 10 Reviewing ISMS Monitoring and Improvement |
| **DAY 2** | | |
| 09.00- 09.30 am 09.30- 10.30 am | 30 min  1 hr | \* Recap – Day 1  \* Reviewing controls in Annexure A - controls A.5 |
| 11.00 - 11.15am | 15 min | *Morning Tea* |
| 11.15 - 12.30pm | 1 hr 15 min | \* Reviewing controls in Annexure A - controls A.6 to A.7 |
| 12.30 - 01.30pm | 1 hr | *Lunch* |
| 01.30 - 02.30pm 02.30 - 03.15pm | 1 hr | \* Reviewing controls in Annexure A - controls A.8 |
| 03.15 - 03.30pm | 15 min | *Afternoon Tea* |
| 3.30 - 5.00 pm | 1 hr 30 min | \* **Candidate Assessment**  \* **Course Feedback** |

Please note that times may vary due to delegate numbers, time taken on individual days, etc.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 2 of 134

**TRAINING OBJECTIVES**

Upon successful completion of this course participants should be able to:

**UNDERSTAND**:

● the intent and the requirements of each clause and its relationship with organization’s operational information security requirements and legal compliance requirements;

● the documentation required and analyze the interrelationships among various ISMS documents; ● how ISMS planning, policy, objectives, and processes are implemented according to the ISO/IEC 27001:2022 standard and in relation to the context of the organization; and

● the process of addressing improvements in the organization’s ISMS and verify that identified improvements are effectively managed.

**REVIEW OF RISK ASSESSMENT**

● assess the effectiveness of an organization’s information security risk assessment (RA) methodologies;

● analyse the controls identified in the Statement of Applicability (SOA) and the controls of the ISO/IEC 27001:2022 Annex A as they apply to the treatment of risk;

● assess the organization’s operational control, information security RA and the implementation of the risk treatment (RT) plan;

● evaluate RA and RT results to ensure they are appropriately identified within the organization’s SOA; and

● assess an organization’s monitoring, measurement, analysis, and evaluation activities.

NOTE:

In this edition we used FIVE sources:

(1) ISO/IEC 27001:2022 ISMS requirements including Annexure A controls.

(2) ISO/IEC 27002:2022 Guidelines on implementation of Annexure A controls

(3) ISO/IEC 27007:2017 Guidelines on auditing and ISMS (covers clause 4 to clause 10) (4) ISO/IEC 27008:2019 Guidelines for the assessment of information security controls (Audit practice and type of evidence to look for when auditing each control in Annexure A of ISO/IEC 27001:2013. (5) ISO/IEC 27006:2015 Requirements for Certification Bodies providing ISMS certification (Type of test for each control in Annexure A of ISO/IEC 27001:2022.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 3 of 134

**Exemplar Global – IS: What are the requirements?**

**Source: www.exemplarglobal.org**

**Competency Unit: Exemplar Global-IS –Information Security Management Systems.**

Effective date: 21/Nov/2022

| 1: Information Security Management System in the context of  ISO/IEC 27001:2022 | 1.1 Understand the intent and the requirements of each clause of ISO/IEC 27001. |
| --- | --- |
| 1.2 Understand the documentation required by ISO/IEC 27001 and analyze the interrelationships among various ISMS documents. |
| 1.3 Understand how ISMS planning, policy, objectives and processes are implemented according to the ISO/IEC 27001 standard and in relation to the context of the organization. |
| 1.4 Understand the information security and specific organization terminologies, including the terms used in ISO/IEC 27001and ISO/IEC 27000. |
| 1.5 Evaluate the effectiveness of the entire ISMS, including monitoring and improvement activities. |
| 1.6 Understand the relationship between legal compliance and conformity to ISO/IEC 27001. |
| 2: ISMS and Information Security Requirements | 2.1 Understand the relationship between an organization’s operational information security requirements and the ISO/IEC 27001 standard. |
| 2.2 Assess the effectiveness of an organization’s information security risk assessment (RA) methodologies. |
| 2.3 Analyze how information security objectives, legal and regulatory requirements, and requirements from interested parties are incorporated into the RA methodologies. |
| 2.4 Evaluate RA and risk treatment (RT) results to ensure they are appropriately identified within the organization’s Statement of Applicability. |
| 2.5 Assess the organization’s operational control, information security RA and the implementation of the RT plan. |
| 2.6 Analyze the controls identified in the Statement of Applicability and the controls of Annex A as they apply to the treatment of risk. |
| 2.7 Assess an organization’s monitoring, measurement, analysis and evaluation activities. |
| 2.8 Understand the process of addressing improvements in the organization’s ISMS and verify that identified improvements are effectively managed. |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 4 of 134

**TABLE OF CONTENTS**

What Is Information Security? ..................................................................................................................................... 6 *What is Changing in ISO/IEC 27001:2022?*................................................................................................................ 8 *ISO/IEC 27001: 2022 Structure* ................................................................................................................................... 9 *ISO/IEC 27001:2022 Framework* .............................................................................................................................. 10

Changes in Annexure Controls from ISO/IEC 27001:2013................................................................................... 69 Comparison of ISO/IEC 27001:2013 and ISO/IEC 27001:2022 ANNEXURE CONTROLS.............................. 69 A.5 Organisational Controls................................................................................................................................... 70 A.6 People Controls ............................................................................................................................................... 91 A.7 Physical Controls............................................................................................................................................. 95 A.8 Technological Controls ................................................................................................................................. 104

HOW IS AN ISMS CERTIFICATION AUDIT CARRIED OUT?......................................................................... 127 Guidance for ISMS auditing practice....................................................................................................................... 128 ISO 27000 Family of Standards............................................................................................................................... 131 Annexure 4 – Mapping ISO/IEC 27001:2013 Annexure Controls to ISO/IEC 27001:2022 Annexure Controls 132

Table 1 : Risk Assessment Sample Template ............................................................................................................ 35 Table 2 : Sample Risk Register Template .................................................................................................................. 39 Table 3 : Sample SoA Template................................................................................................................................. 41 Table 4 : Sample Communication Chart .................................................................................................................... 51 Table 5: Categories of ISO/IEC 27001:2022 Annexure Controls.............................................................................. 69 Table 6 : Requirement for documented information ................................................................................................ 128 Table 7: ISO/IEC 27001:2013 Annexure Controls mapping to ISO/IEC 27001:2022............................................ 132

Figure 1: ISMS Processes and interactions between processes ................................................................................. 23 Figure 2 : Mapping of ISO/IEC 27001:2013 to ISO/IEC 2001:2022 ........................................................................ 69

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 5 of 134

| **What Is Information Security?**  − An organisation has many assets. Information is also an asset.  − Information drives business in today’s networked environment.  − Information includes, for example:  − Software: : Windows, Oracle  − Paper: : Contracts, Telephone list  − Supporting utilities: : VOIP, Telephone, Backup power supply − Hardware: : Server, Laptop, PDA  − People: : HR Manager, Network Engineer  − Information: : Voice message  − (Utilities themselves do not carry information. But they support other devices that carry information).  − Information can be static (e.g., stored on hard disk) or being transmitted (e.g., email) − Whatever form the information takes, it must always be protected.  − Physical and IT security alone are not sufficient. We need a management framework to improve information security.  − Types of protection:  − Confidentiality - based on ‘need to know’ and ‘need to do’ principle − Integrity - i.e., ‘accuracy’ and ‘completeness’  − Availability - making systems available to authorised users when they need it. |
| --- |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 6 of 134

| **What Is Information Security?**  − Having physical and technical security is the first step but is not enough. New threats occur every day. In addition, there are multiple regulatory requirements on security. − Identifying the information security requirements, and protecting the confidentiality, integrity & availability of business information is ‘vital’ for business survival. − Having too many controls may not be cost effective. Therefore an information security risk assessment followed by selection of appropriate controls strikes a balance between risks and controls to enable business growth.  − An information security management system (ISMS) based on ISO/IEC 27001:2022 includes:  − information security risk assessment;  − selection of appropriate controls to mitigate the risks to an acceptable level; and can use any of the following methods for continual improvement of security processes.  **Why Have an ISMS?**  **Benefits of Implementing an ISMS**  a) Compliance with multiple regulations are tracked  b) Security roles & responsibilities are defined  c) Essential supporting documentation is available  d) There is a defined balance between risk and control  e) The organization can remain competitive  f) Provides assurance to customers and partners that their information is protected.  **What Is Process Improvement?**  Any of the following models can be followed to improve the ISMS process.  − Plan-Do-Check-Act (PDCA) model  − CMMi - IDEAL  − Six Sigma - DMAIC – Define, Measure, Analyze, Improve, Control  − GMP – Good Manufacturing Practice  − GLP – Good Laboratory Practice  − GMP – Good Agricultural Practice  − Malcolm Baldridge Model of excellence  − EFQM Model of excellence |
| --- |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 7 of 134

***What is Changing in ISO/IEC 27001:2022?***

**ISO/IEC 27001:2013**

• **Information technology** —Security techniques —Information security management systems — Requirements

Is now changing to 

**ISO/IEC 27001:2022**

• Information security, **cybersecurity and privacy protection** — Information security management systems —Requirements

• The terms ‘Code of Practice’ and “Control objectives” have been removed.

• New standard includes control requirements for Cyber Security Protection & Privacy Protection • Basic Business Continuity controls reintroduced

• The text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022

The changes will make the standard more relevant and up to date to cope with the latest security threats and technologies

**Note: In this Delegates Manual, text from ISO/IEC 27001:2022 are shaded**

**Changes from ISO/IEC 27001:2013 are shaded**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 8 of 134

***ISO/IEC 27001: 2022 Structure***

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Context of the organization

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the information security management system 4.4 Information security management system

5 Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibilities and authorities

6 Planning

6.1 Actions to address risks and opportunities

6.2 Information security objectives and planning to achieve them

6.3 Planning of Changes

7 Support

7.1 Resources

7.2 Competence

7.3 Awareness

7.4 Communication

7.5 Documented information

8 Operation

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

10 Improvement

10.1 Continual improvement

10.2 Nonconformity and corrective action

Annex A (normative) Reference control objectives and controls

Bibliography

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 9 of 134

***ISO/IEC 27001:2022 Framework***

**Introduction**

The introduction to the Standard is having two sections namely General and Compatibility with other management system standards

**General**

Among the ISO 27000 family of nearly 50 standards, ISO/IEC 27001:2022 is the only standard that can be used for third party certification. The rest may be used as additional guidelines.

| *The ISO 27001 Standard is providing the requirements to establish, implement, maintain and continually improved ISMS. The implementation of ISMS is a strategic decision by the organisation and the business needs should drive the ISMS. It is often based on the security objectives, requirements, processes and the size and structure of the organization. As information security exists at all the process areas of the organisation, it is essential to consider integrating ISMS with all the processes of the organisation.* |
| --- |

The ISMS is based on the three basic security principles such as Confidentiality, Integrity and Availability. Based on the risk evaluation and risk treatment, the organisation and the other relevant internal and external stakeholders get an assurance that security is managed adequately.

**Compatibility with other management system standards**

ISO/IEC 27001:2022 Standard that uses the High Level Structure (also known as Annex SL / Guide 83). This follows the framework relating to clauses, sub-clause titles, text, common terms, and other definitions as required by ISO.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 10 of 134

| ***1 Scope***  *This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.* |
| --- |

**Plain English Explanation**

Note: The term ‘Scope of an ISMS’ is different and will be discussed later in this course.

Until now, a majority of ISMS implementations are seen in IT Departments. But the standard suits any department and any industry or type of organization. There are a few standards specific to an industry, for example, food, shipping, healthcare, financial institution, etc. This standard is not restricted to a specific industry or type of organisation. i.e., it is not IT specific although most of the ISMS implementations are seen in the IT areas.

| ***2 Normative Reference***  *In this Standard only one reference is given. i.e., ISO/IEC 27000:2012, ISMS Overview and vocabulary.* |
| --- |

**Plain English Explanation**

ISMS family of standards in the 27000 series are about 50. But in ISO/IEC 27001:2022 only one standard has been referred, i.e., ISO/IEC 27000:2018, ISMS Overview and vocabulary.

| ***3 Terms and definitions***  *This Standard does not have any definitions. But it has reference only to ISO/IEC 27000:2012* ISO and IEC maintain terminology databases for use in standardization at the following addresses: — ISO Online browsing platform: available at https://www.iso.org/obp  — IEC Electropedia: available at https://www.electropedia.org/ |
| --- |

**Plain English Explanation**

The Standard has now been revised to ISO/IEC 27000:2018.

An ISMS auditor is expected to understand these definitions as well as new terms in the IT Industry, for example, Cloud computing, iOT, cyber security, DevOps, Micro services programming, Offensive Security.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 11 of 134

A few definitions from ISO/IEC 27000:2018 are given below:

| Access control | means to ensure that access to assets is authorized and restricted based on business and security requirements. |
| --- | --- |
| Asset | anything that has value to the organization. |
| Control Objective | Statement describing what is to be achieved as a result of implementing controls. |
| Control | Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management or legal nature. |
| External context | External environment in which the organization seeks to achieve its objectives. Note: it can include:  ⎯ cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local  ⎯ key drivers and trends having impact on the objectives of the organization; and ⎯ relationships with, and perceptions and values of, external stakeholders. |
| Internal context | Internal environment in which the organization seeks to achieve its objectives. NOTE Internal context can include:  ⎯ governance, organisational structure, roles and accountabilities;  ⎯ policies, objectives, and the strategies that are in place to achieve them; ⎯ the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);  ⎯ information systems, information flows and decision-making processes (both formal and informal);  ⎯ relationships with, and perceptions and values of, internal stakeholders; ⎯ the organisation's culture;  ⎯ standards, guidelines and models adopted by the organisation; and ⎯ form and extent of contractual relationships. |
| Information  processing facilities | Any information processing system, service, infrastructure, or the physical locations housing them. |
| Information security | Preservation of confidentiality, integrity and availability of information. |
| Information security management system (ISMS) | Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. |
| Information system | Application, service, information technology asset, or any other information handling component. |
| ISMS project | structured activities undertaken by an organisation to implement an ISMS |
| Management system | framework of guidelines, policies, procedures, processes and associated resources aimed at ensuring an organisation meets its objectives |
| Statement of  Applicability (SOA) | documented statement describing the control objectives and controls that are relevant and applicable to the organization’s ISMS. |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 12 of 134

**4. Context of the organisation**

| ***ISO/IEC 27001:2022 - 4.1 Understanding the organization and its context***  *The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.*  *NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018.* |
| --- |

**Plan English Explanation.**

The organization requires to evaluate the relevant issues, both internal and external, that may have an impact while meeting the objective. By defining the relevant issues to its purpose, the organisations can set directional goal for establishing their framework. In addition, the internal and external issues that might affect the potential to meet the expected outcomes are understood.

This sets the stages as given below:

- Understanding the external context

- Understanding the internal context

- Understanding the purpose and intended outcome of the MANAGEMENT SYSTEM STANDARDS

- Analysing the factors to be considered to meet those objectives.

ISO 31000:2018 is the standard for Risk Management Guideline.

**Audit tool**

*Whom to meet:* Top Management and CISO

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on: a) the important issues that can affect, either positively or negatively, the ISMS; b) the organization;

c) the purpose of the organization;

d) the intended outcome of the ISMS.

Possible sources of the important issues can include:

a) environmental characteristics or conditions related to climate, pollution, resource availability, and biodiversity, and the effect these conditions can have on the organization’s ability to achieve its objectives;

b) the external cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive context, whether international, national, regional or local;

c) characteristics or conditions of the organization, such as organizational governance, information flows and decision-making processes;

— organizational policies, objectives, and the strategies that are in place to achieve them; — the organization's culture;

— standards, guidelines and models adopted by the organization;

— the life cycle of the organization’s products and services;

— information systems, processes, science and technology and underlying information security management.

d) trends of audits and risk assessment.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 13 of 134

Auditors should confirm that the organization:

a) Has a high-level (strategic) understanding of the important issues that can affect, either positively or negatively, the ISMS;

b) Knows the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 14 of 134

NOTE 1

The requirement in 4.3 is to “consider the external and internal issues referred to in 4.1”. The organization can take into consideration something that not necessarily appears in the output.

Auditors should also confirm that the intended outcomes include preservation of the confidentiality, integrity and availability of information by applying a risk management process and that risks are adequately managed.

Auditors should also verify that the issues include the important topics for the organization, problems for debate and discussion, or changing circumstances and also be verified that the knowledge gained is used to guide the organization’s efforts to plan, implement and operate the management system.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 15 of 134

| ***ISO/IEC 27001:2022 - 4.2 Understanding the needs and expectations of interested parties*** *The organization shall determine:*  *a) interested parties that are relevant to the information security management system; b) the relevant requirements of these interested parties;*  *c) which of these requirements will be addressed through the information security management system.*  *NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.* |
| --- |

**Plan English Explanation.**

Who are the “interested parties”?

In ISO terminology the term “interested parties” is the same as “stakeholder”. As mentioned in Annex A: **interested party** (preferred term) and **stakeholder** (admitted term)

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. The indicative list is given below:

**External**

- Legal authorities

- Clients / customers

- Contractors / suppliers

- Group Companies

- Public

**Internal**

- Internal organisational units

- Executive management

- Board of directors

- Employees

Regulations: At least one member in the audit team must have knowledge of local applicable legislation. For example: 1. Data Protection Act, UK; 2. ISM and PSM frameworks, Australia; 3. Government of India IT Act 2008, Rule No 11 of 11/April/2011; 4. HIPAA; 5. SOX

In order to design and build a management system, it is necessary to determine the relevant interested parties both internal and external and consider their requirements. At this stage more clear understanding is established in identifying the interested parties to the organisation that are appropriate to the ISMS. Once the interested parties are identified, their requirements are drawn. Usually the requirement of Legal, Business, and Finance etc in the Statement of Applicability are drawn from this understanding. The same can be used for doing the Risk Assessment.

**Audit tool**

*Whom to meet:* Top Management / CISO

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Organisation objective, Broad overview of processes, applicable legal requirements, Contracts, SLAs

NOTE 1

Audit evidence can be obtained through documented information or other information about: a) the interested parties;

b) the needs and expectations of relevant interested parties that are applicable to the ISMS and ISO/IEC 27001.

NOTE 2 Potential interested parties can include:

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 16 of 134

a) legal and regulatory authorities (local, regional, state/provincial, national or international); b) parent organizations;

c) customers;

d) trade and professional associations;

e) community groups;

f) non-governmental organizations;

g) suppliers;

h) neighbours;

i) members of the organization and others working on behalf of the organization; j) information security experts.

NOTE 3 Interested party requirements can include:

a) laws;

b) permits, licenses or other forms of authorization;

c) orders issued by regulatory agencies;

d) judgments of courts or administrative tribunals;

e) treaties, conventions and protocols;

f) relevant industry codes and standards;

g) contracts which have been entered into;

h) agreements with community groups or non-governmental organizations;

i) agreements with public authorities and customers;

j) organizational requirements;

k) voluntary principles or codes of practice;

l) voluntary labelling or environmental commitments;

m) obligations arising under contractual arrangements with the organization;

n) information and communication exchange

NOTE 4 Interested parties can have different interests, which can be wholly aligned, partially aligned or opposed to the organization’s business objectives. An example of where an interested party has interests that are opposed to the organization’s objectives is the hacker. The hacker requires the organization to have weak security. The organization should take account of this interested party requirement by having the complete opposite, i.e. strong security.

Auditors should be aware that the ISMS considers all internal and external risk sources. Therefore, the organization’s understanding of interested parties that are opposed to the organization and their requirements are highly relevant.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization has a high-level (e.g. strategic) understanding of the needs and expectations of relevant interested parties that are applicable to the ISMS and ISO/IEC 27001.

Auditors should verify that the organization has identified the interested party requirements that it decides to voluntarily adopt or enter into an agreement or contract, as well as the needs and expectations that are mandatory because they have been incorporated into laws, regulations, permits and licenses by governmental or court action. It is noted that not all interested party requirements are requirements of the organization and some are not applicable to the organization or relevant to the ISMS. Some interested party needs (e.g. those of a hacker) will be contrary to the purpose of the ISMS and the organization would be expected to ensure through appropriate information security controls that such needs and expectations are not satisfied.

Auditor should verify that the identified requirements should be addressed through ISMS.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 17 of 134

Auditors can also confirm that there are interested parties that perceive themselves to be affected by the ISMS and if there are so, they make it known to the organization.

Auditors can also verify that the organization uses the knowledge gained to guide its efforts to plan, implement and operate the management system.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 18 of 134

| ***ISO/IEC 27001:2022 - 4.3 Determining the scope of the information security management system*** *The organization shall determine the boundaries and applicability of the information security management system to establish its scope.*  *When determining this scope, the organization shall consider:*  *a) the external and internal issues referred to in 4.1;*  *b) the requirements referred to in 4.2; and*  *c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.*  *The scope shall be available as documented information.* |
| --- |

**Plan English Explanation.**

The organisation has to define the scope and boundaries for ISMS to meet internal and external requirements. The scope and boundaries determines the applicability of ISMS in terms of the - region,

- location i.e. physical address

- department / function,

- technology

- resources,

- contractors etc.,

Traditionally the scope of ISMS focuses on IT department. But ISMS is applicable to all the departments wherever information is processed either manually or electronically. The following are some of the sample scope statements. Providing information such as referencing to SOA with its version number and referencing to the ISO/IEC 27001:2022 standard will add clarity to the scope statement.

**Sample scope statements:**

**Sample 1**

Management of Information Security in providing application support, software development IT infrastructure management, data-centre management and helpdesk services to internal users. This is in accordance with the Statement of Applicability version 1.1 of 15th October, 2022.

**Sample 2**

Management of Information Security in providing internet banking to customers for its head office and branch locations. This is in accordance with the Statement of Applicability version 1.3 of 10th October, 2022.

**Sample 3**

Management of Information Security in hosting servers on behalf of customers using cloud computing technology. This is in accordance with the Statement of Applicability version 2.0 of 15th November, 2021.

**Audit tool**

*Whom to meet:* CISO / Management Representative

**Note down Issue date and version number of SOA in the Scope Document. This is the basis for issuing the certificate.**

| Also check if changes in the scope are approved in a MRM. Changes to Scope and SoA impact overall ISMS process and hence to be made known to the management.  Scope should include internally supported as well as externally supported services necessary for ISMS |
| --- |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 19 of 134

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information of: ● Scope diagram, Scope document, MOUs/SLAs/OLAs related to information security ● Type of assets at each location, Business areas excluded from Scope of ISMS and justification for their exclusion.

● the scope of an organization’s certification, if applicable;

● the Statement of Applicability.

NOTE 5 The scope of an organization’s certification is not necessarily the same as the scope of its ISMS. In general, the scope of certification will be confined to the ISMS organization.

*Note:* Management of an IT Data Centre or specific part of IT infrastructure can be the Scope of ISMS but not just the IT infrastructure.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization establishes the **physical, informational, legal and organizational** boundaries to which the ISMS is applied, at its own will and chooses to implement ISO/IEC 27001 within the entire organization or as a specific unit or particular function(s) within an organization.

Auditors should verify that the organization’s understanding of its context (4.1), the requirements of relevant interested parties (4.2) and interfaces and dependencies between activities performed by the organization and those that are performed by other organizations [4.3 c)], have been adequately considered when establishing the scope of the ISMS.

Auditors should further confirm that the organization’s information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the ISMS scope, to the extent applicable to the audit scope. Auditors should verify that there is at least one Statement of Applicability per scope and that all the controls determined in the risk management process are included in the Statement(s) of Applicability. These controls are the necessary controls referred to in ISO/IEC 27001:2022, 6.1.3 b) and are not necessarily ISO/IEC 27001:2022, Annex A controls. They may include sector-specific controls and controls that are designed by the organization or identified from any source.

Auditors should also confirm that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to be audited and are included in the organization’s information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations.

It should be verified that documentation of the scope is created and controlled in accordance with the requirements of documented information (7.5).

A report template used in CPG Certification Audit – Stage 1 is given below:

| **Audited Clauses** |
| --- |
| **4.3 Scope of ISMS**  Document Name: Version Number: Date: |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 20 of 134

| Scope is clear in terms of: | |
| --- | --- |
| Characteristics of business areas, example |  |
| Organisation, for example, legal entity is |  |
| Location, for example |  |
| External information security requirements |  |
| Internal information security requirements |  |
| Exclusion from scope of ISMS |  |
| Scope of ISMS is clear and justification for exclusion is acceptable.  Yes ☐ No☐ | |

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 21 of 134

| ***ISO/IEC 27001:2022 - 4.4 Information security management system***  *The organization shall establish, implement, maintain and continually improve an information security management system,* ***including the processes needed and their interactions****, in accordance with the requirements of this document.* |
| --- |

**Plain English Explanation**

There is no emphasis on the Plan, do, check and act cycle in the Standard. Therefore, the organisation can adopt any model of process improvement which is mentioned earlier.

The management system is required to be established, implemented, maintained and continually improved. In order to achieve these processes, policies, procedures and interaction amongst each other are developed.

Third Party Certification Stage 1 can start only after the organization has completed one cycle to establish, implement, maintain and continually improve an information security management system, for example, one PDCA cycle.

**Some of the ISMS processes** :

1. Interested Parties Analysis

2. Scope Definition

3. Setting Objectives

4. Communication

5. Risk Assessment

6. Metrics & Measures

7. Internal Audit

8. External Audit

9. MRM

10. Corrective Action

Each ISMS process interacts with various other ISMS processes as input / output relationship. **Interation between various ISMS processes is emphasised specifically in ISO/IEC 27001:2022.**

**Audit tool**

*Whom to meet:*

Management Representative

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on the processes required to be established in ISO/IEC 27001, which include:

a) processes for management system (ISO/IEC 27001:2022, 4.4);

b) operational planning and control processes, including outsourced processes (8.1); c) processes to address risks and opportunities when planning the ISMS, including the information security risk assessment processes (6.1.3 and/or 8.1.3);

d) processes to achieve information security objectives.

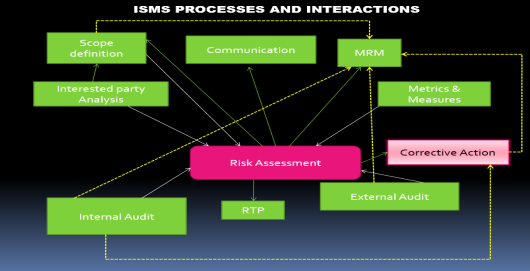
*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization creates the “necessary but sufficient” set of processes and controls that, together, form an effective management system in conformance to ISO/IEC 27001 and establishes the ISMS of the set of those interrelated or interacting elements.

**Auditors need to specifically look for evidence for interactions between various ISMS processes like Internal and External Audit findings have to be taken as inputs for Risk Assessment.**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 22 of 134

Auditors also should confirm that the organization, in its existing capacity, retains authority, accountability and autonomy, to decide how it will fulfil the ISMS requirements, including the level of detail and extent to which it will integrate the ISMS requirements into its business.

*Figure 1: ISMS Processes and interactions between processes*

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 23 of 134

**5. Leadership**

| ***ISO/IEC 27001:2022 - 5.1 Leadership and commitment***  *Top management shall demonstrate leadership and commitment with respect to the information security management system by:*  *a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;*  *b) ensuring the integration of the information security management system requirements into the organization’s processes;*  *c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements;*  *e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system;*  *g) promoting continual improvement; and*  *h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.*  NOTE *Reference to “business” in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization’s existence.* |
| --- |

**Plan English Explanation.**

The standard clearly mentions in the Introduction that the clauses are not placed in the order of their importance or imply the order of implementation, it clearly indicates that the leadership and commitment plays a significant role in implementation. And that may be one of the reasons to place this clause before the actual processes of implementation requirements are listed.

Immediately after the opening meeting we have a brief meeting with the top management to confirm their commitment and support to ISMS.

***Note:*** This audit is a difficult one for beginners. We suggest that the beginners observe a few top management interviews conducted by experience auditors before doing such interviews independently. Always start your conversation with generic topics such as business trend, market share etc. that are related to the business. Then you can continue with open ended questions about ISMS. For example, you may avoid asking questions such as “When did you attend the last Management Review Meeting?”, because they attend so many management meetings and may not remember the operational details. About writing audit notes, we suggest you write your audit notes after the interview is finished and not during the interview.

**Audit tool**

*Whom to meet:* Top Management

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on: a) the information security policy [ISO/IEC 27001:2022, 5.1 a)];

b) the information security objectives [5.1 a)];

c) the organization’s processes;

d) results of management reviews [5.1 c), e) and g)];

e) evaluation of resource need;

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 24 of 134

f) communication of the importance of effective information security management and of conforming to the information security management system requirements.

Evidence can also be obtained through interviews with top management. The results of the management reviews can also provide audit evidence with sub clauses other than 5.1 c), e) and g).

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm visible support, involvement and commitment of the organization’s top management which is important to the successful implementation of ISO/IEC 27001 is evident.

Auditors should also verify that:

a) top management delegated tasks are identified;

b) top management remains accountable for the satisfactory completion of activities assigned to the organization;

c) top management ensures that the information security policy and objectives are established and they are aligned with the strategic direction of the overall organization;

d) top management communicates the importance of effective information security management and of conforming to the ISMS requirements;

e) top management ensures that the ISMS achieves its intended outcome(s) by supporting the implementation of all information security management processes and in particular, through requesting and reviewing reports on the status and effectiveness of the ISMS [see 5.3 b)];

f) top management directs and supports people in the organization directly involved with information security and the ISMS;

g) top management ensures the integration of the ISMS requirements into the organization’s processes; h) top management ensures the availability of resources for having an effective ISMS; i) top management assesses resource needs during management reviews and set objectives for continual improvement and for monitoring effectiveness of planned activities;

j) top management creates a culture and environment that encourages people to work actively towards implementing the requirements of the ISMS and seeking to achieve the information security objectives.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 25 of 134

**5.2 Policy**

| ***ISO/IEC 27001:2022 - Top management shall establish an information security policy that:*** *a) is appropriate to the purpose of the organization;*  *b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;*  *c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.*  *The information security policy shall:*  *e) be available as documented information;*  *f) be communicated within the organization; and*  *g) be available to interested parties, as appropriate.* |
| --- |

**Plan English Explanation**

This is normally a 1-page statement. The policy that is established should be appropriate for the purpose and not too generic, i.e., if it is bank, it must suit a bank. It should Support the development of an ISMS with a management framework, resourcing and a policy framework. It must include a commitment to satisfy applicable legal and regulatory requirements related to MANAGEMENT SYSTEM STANDARDS

and emphasise continual improvement of ISMS.

The ISMS policy is a documented information, communicated and should be made available to the interested parties. A few organisations also have the practice of issuing an extract of the ISMS Policy and displaying that at critical locations so that it is communicated to all employees and contractor.

Also, cross check with Annexure A.5.1 – Policies for information security. Requirements of clause 5.2 and Control A 5.1 may be met with a single implementation by approving the one-page statement and about 5 to 10 pages of security policies, for example, password, email, back up, etc.

**Audit tool**

*Whom to meet:* Management Representative

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on: a) information security policy (5.1);

b) information security objectives [5.2 b) and 6.2]

*Note:* If the organization is also audited by external auditors, they may insist on a ‘statement of assertion’, for example, each employee has acknowledged that he/she has read and understood the contents of the ISMS policy. This related to understanding and meeting requirements of external parties.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that:

a) the information security policy specifies the high-level organizational commitments as required by ISO/IEC 27001, taking into account the organization’s purpose;

b) the information security policy is either used to frame or build the information security objectives which the organization sets for itself, or are stated explicitly as part of the information security policy; c) documented information of the information security policy is created and controlled in accordance with the requirements of documented information (7.5);

d) the information security policy is communicated internally, in accordance with the requirements of the communication clause (7.4);

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 26 of 134

e) the information security policy also is made available to other interested parties as appropriate.

With the information security policy containing a commitment to satisfy applicable requirements, in particular, relevant laws and regulations, the ISMS should not be considered out of conformance

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 27 of 134

**5.3 Organization roles, responsibilities and authorities**

| ***ISO/IEC 27001:2022 - 5.3 Organizational roles, responsibilities and authorities*** *Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.*  *Top management shall assign the responsibility and authority for:*  *a) ensuring that the information security management system conforms to the requirements of this International Standard; and*  *b) reporting on the performance of the information security management system to top management.*  NOTE *Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.* |
| --- |

**Plan English Explanation**

The term ‘Management Representative’ is not used in the standard. There could be more than one level of ISMS champions managing ISMS within the organization. Also, earlier versions of the standard had a requirement that the Management Representative’ had to be from the organization, i.e., this role could not be outsourced. These requirements were rigid.

Another reasons could be that the title CISO, Chief Information Security Officer, may not be found in every organisation. The organization may be using other titles, for example, Chief Risk Officer, Security Administrator, Manager – GRC, or any other designation/title.

**Audit tool**

*Whom to meet:* Management Representative / CISO

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Considering ISO/IEC 27001:2022, 7.5.1 b), audit evidence can be obtained through documented information or other information on:

a) the organizational roles;

b) the job description of persons doing work under its control that can have impact on the organization’s information security performance;

c) the implementation of internal audit programme and the audit results;

d) the ISMS scope and structure of the organization.

e) Email from CXO nominating the Management Representative and other team members.

In addition, there can be further audit evidence obtained through documented information or other information on the results of management reviews.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm through review of documented information and/or interview that: a) responsibilities and authorities for the implementation of the ISMS requirements are assigned to relevant roles within the organization;

b) top management is accountable for these responsibilities and authorities being assigned and communicated to the respective persons performing those roles;

c) the responsibilities and authorities are communicated in accordance with the requirements of the communication clause (7.4);

d) demonstration of conformance to the requirements of ISO/IEC 27001 is conducted in accordance with the requirements of the internal audit (9.2);

e) performance reporting is conducted in accordance with the requirements of management review (9.3).

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 28 of 134

Auditors should verify that responsible individuals have sufficient access to top management to keep management informed of the status and performance of the ISMS.

NOTE 6 The role of ensuring that the management system conforms to the requirements of ISO/IEC 27001 can be assigned to an individual, shared by several individuals or assigned to a team. **Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 29 of 134

**Definitions related to Risk**

**Level of risk** magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

**Likelihood** chance of something happening risk analysis.

**Risk** effect of uncertainty on objectives.

Note: effect could be either positive or negative.

**Risk identification** Process of finding, recognizing and describing risks

Note1 Risk identification involves the identification of risk sources, events, their causes & their potential consequences.

Note2 Risk identification can involve historical data, theoretical analysis, informed & expert opinions, & stakeholders’ needs.

**Risk analysis** Process to comprehend the nature of risk and to determine the level of risk.

**Risk evaluation** process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Note: This process assists in the decision about risk treatment.

**Risk assessment** overall process of risk identification, risk analysis and risk evaluation

**Risk treatment** process to modify risk

NOTE 1: risk treatment can involve:

1. avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

2. taking or increasing risk in order to pursue an opportunity;

3. removing the risk source;

4. changing the likelihood;

5. changing the consequences;

6. sharing the risk with another party or parties (including contracts and risk financing); and

2. retaining the risk by informed choice.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.

**Residual risk** the risk remaining after risk treatment

**Risk acceptance** decision to accept a risk

e.g., risk is within the acceptance criteria or Top Management accepts the risk even if it is above the risk acceptance criteria.

**Risk management** coordinated activities to direct and control an organization with regard to risk i.e. Risk Management = Risk Assessment (i.e., Risk Analysis + Risk Evaluation) + Risk Treatment + Risk Monitoring + Risk Review

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 30 of 134

**6. Planning**

| ***ISO/IEC 27001:2022 - 6.1 Actions to address risks and opportunities***  ***6.1.1 General***  *When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:*  *a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and*  *c) achieve continual improvement.*  *The organization shall plan:*  *d) actions to address these risks and opportunities; and*  *e) how to*  *1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.* |
| --- |

**Plain English Explanation**

This clause addresses the planning requirement of risks and opportunities. It requires developing assurance methods to prevent, reduce the undesired effects. This clause emphasizes the proactive approach that is required to be carried as a prevention solution. It is always preferred that correction and corrective action are taken after the risk has been assessed.

The planning will focus on

- How the organization plans to prevent, or reduce, undesired effects?

- How the organization ensures that it can achieve its intended outcomes and continual improvement? - What will be done to address this

- Who will do and when it will be done.

**RISK ASSESSMENT**

- Any Risk Assessment method can be used.

- Define a comparable and repeatable process of risk assessment.

- The process is repeatable if the same person does risk assessment over a period of time and comparable if several person use the same method and arrive at similar conclusions about the information security risk level, type of threats, list of controls from Annexure, etc.

- The ISMS Auditor should look for several indicators of comparable and repeatable process: ● list of threats based on nature of service/asset

● a standard method of measuring ‘likelihood’ of threats, for example 1 to 5,

● a defined list of information security risks,

● a defined method of assessing the risk level, for example 1 to 5,

● list of controls from Annexure A related to specific information security risks

- List all services/projects/department and related information assets within the scope of ISMS and their risk owners.

- Conduct risk assessment and select controls to reduce the risk to a predefined acceptable level. - Review the risk register. Confirm that minutes are available for discussion with Risk Owners and selection of controls.

- Review a higher percentage of Very High/High value risks and a lower percentage of risk of low or negligible value.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 31 of 134

**Audit tool**

*Whom to meet:* Risk Owners

***Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):***

Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS [ISO/IEC 27001:2022, 6.1.1, 6.3, 7.5.1 b) and 8.1)];

b) the information security risk assessment process (6.1.2);

c) the results of the information security risk assessments (8.2);

d) the information security risk treatment process (6.1.3);

e) the results of the information security risk treatment (8.3);

f) the results of monitoring and measurements (9.1);

g) the internal audit programme(s) and the results of the internal audit (9.2);

h) the results of management reviews (9.3);

i) context of the organization (4);

j) Information Security Objectives (6.2).

***Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):***

Auditors should confirm that the planning:

a) is being performed at a level appropriate to establishing the ISMS;

b) includes the consideration of the issues relevant to the organization’s context identified in (4.1) and the organization’s applicable requirements identified in (4.3) in order to address any negative or positive consequence related to ISO/IEC 27001:2022, 6.1.1 a) to c);

c) has anticipated potential scenarios and consequences and as such being preventive in addressing undesired effects before they occur.

d) addresses the intended outcomes [6.1.1 a)] determined by the organization that include preserving the confidentiality, integrity and availability of information by applying a risk management process;

e) includes determining how to incorporate the actions deemed necessary or beneficial into the ISMS, either through objective setting (6.2), planning of changes (6.3), operational control (8.1) or other specific clauses of ISO/IEC 27001, e.g., resource provisions (7.1), competence (7.2), information security risk assessment (8.2), information security risk treatment (8.3);

f) includes determining the mechanism for evaluating the effectiveness of action taken is also planned, and can include monitoring, measurement techniques (9.1), internal audit (9.2) or management review(9.3).

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 32 of 134

| ***Risk Assessment - Other requirements in ISO/IEC 27001:2022***  ***6.1.2) Information security risk assessment***  *The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include:*  *1) the risk acceptance criteria; and*  *2) criteria for performing information security risk assessments;*  *b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;*  *c) identifies the information security risks:*  *1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and*  *2) identify the risk owners;*  *d) analyses the information security risks:*  *1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;*  *2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;*  *e) evaluates the information security risks:*  *1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analysed risks for risk treatment.*  *The organization shall retain documented information about the information security risk assessment process.* |
| --- |

***Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):***

Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS [ISO/IEC 27001:2022, 6.1.1, 7.5.1 b) and 8.1)];

b) the information security risk assessment process (6.1.2) and the results of information security risk assessment (8.2).

***Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):***

Auditors should confirm that an information security risk assessment:

a) identifies the security information risks associated with the ISMS;

b) consists of risk identification, risk analysis, and risk evaluation processes.

**Audit practice guide - Risk criteria [ISO/IEC 27001:2022, 6.1.2 a)]**

Auditors should confirm that the organization has established and maintains the risk acceptance criteria and the criteria for performing information security risk assessments.

Although the organization is at liberty to consider whatever factors it deems relevant in establishing its risk criteria including risk acceptance criteria and the criteria for performing information security risk assessments, auditors should assess that the organization established its risk criteria including risk acceptance criteria and its criteria for performing information security risk assessments based on informed decision.

It is reasonable to expect that the organization’s risk criteria are included in the documented information regarding the risk assessment process. If not, the organization should be able to explain to the auditors what they are. At the very least, they should include the organizations’ risk acceptance criteria and the criteria for performing risk assessments.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 33 of 134

NOTE 7 ISO/IEC 27001:2022, 8.2 requires organizations to perform information security risk assessments at planned intervals or when significant changes are proposed or occur. Risk assessment can be performed on all the ISMS or on parts of it (this last case can show when significant changes have impacts on parts of ISMS and then a new partial risk assessment is required).

**Delegate Notes - Sample Audit Questions:**

**Consistency, validity and comparability of results [ISO/IEC 27001:2022, 6.1.2b]**

Auditors should confirm that the results of risk assessments by the information security risk assessment process are consistent, valid and comparable. This confirmation can be performed by: — asking the organization why its own risk assessment results are consistent, valid and comparable; — sampling the documented information concerning results of information security risk assessment.

For assessing consistency and reproducibility, auditors can verify if:

— similar risks in similar contexts have been similarly assessed;

— risks differently assessed have a rationale for such difference;

— the overall assessment results are unequivocally understandable.

For assessing comparability, auditors can verify:

— how the same risk has been evaluated in previous risk assessment and if it is understandable if it has changed;

— if it is unequivocally understandable if a risk is higher or lower than others.

On the next page, we have given a simple risk assessment methodology that ensures consistency, validity and comparability of results.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 34 of 134

**Risk Assessment Process - sample**

*Table 1 : Risk Assessment Sample Template*

**Determining Likelihood**

| **Level** | **Rating** | **Qualitative Characteristic** |
| --- | --- | --- |
| **5** | Almost certain | Is expected to occur in most circumstances. Could occur within ‘days to weeks’ |
| **4** | Likely | Will probably occur in most circumstances. Could occur within ‘weeks to months’ |
| **3** | Possible | Could occur ‘within a year or so’ |
| **2** | Unlikely | Could occur but not expected. Could occur ‘after several years’ |
| **1** | Rare | Occurs only in exceptional circumstances. A ‘100 year event’ or greater |

**Determining Impact**

| **Level** | **Rating** | **Qualitative Characteristic** |
| --- | --- | --- |
| **5** | Extreme | Would have a serious impact on the political, legal and/or commercial credibility of the Department. |
| **4** | High | Would have an immediate impact on operations and would require significant effort to restore normal operations. |
| **3** | Medium | Would have a short-terms impact on operations, however damage should be able to be contained without significant after-effects. |
| **2** | Low | May affect a number of personnel, however it would not be expected to impact significantly on their normal activities and would be able to be contained without major disruption to the affected area. |
| **1** | Negligible | Would marginally affect the ability of a single employee to perform normal operational activities. |

**Determining Risk**

| **Likelihood** | **Impact** | | | | |
| --- | --- | --- | --- | --- | --- |
| **1.**  **Negligible** | **2.**  **Low** | **3.**  **Medium** | **4.**  **High** | **5.**  **Extreme** |
| 5 (almost certain) | M | M | H | H | H |
| 4 (likely) | M | M | M | H | H |
| 3 (possible) | L | M | M | M | H |
| 2 (unlikely) | L | L | M | M | H |
| 1 (rare) | L | L | L | M | H |
| **Risk Legend:**  H High risk; detailed research and management planning required at senior levels.  M Moderate risk; management responsibility must be specified.  L Low risk; manage through routine procedures. | | | | | |

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 35 of 134

**Audit practice guide** *-* **Risk identification [ISO/IEC 27001:2022, 6.1.2c)]**

Auditors should confirm that the organization has identified the information security risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS.

NOTE 8 ISO/IEC 27001 does not require the identification of risks by the identification of assets, threats and vulnerabilities. Other methods of risk identification are acceptable, such as identifying risks through a consideration of events and consequences.

It is reasonable to expect to find a description of the organization’s risk identification process in its documented information concerning the risk assessment process (see below). Factors that the organization can have considered (but need not) in formulating its approach to risk identification can include: a) how risks are found, recognized and described;

b) the sources of risk to be considered.

Further factors that the organization can have considered (but need not) are:

a) how risks can create, enhance, prevent, degrade, accelerate or delay the achievement of the organization’s information security objectives; the risks associated with not pursuing an opportunity; b) risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident;

c) examination of the knock-on effects of particular consequences, including cascade and cumulative effects;

d) consideration of a wide range of consequences, even if the risk source or cause may not be evident; e) consideration of possible causes and scenarios that show what consequences can f) consideration of all significant causes and consequences;

g) how a comprehensive list of risks can be generated.

NOTE 9 A discovery that large numbers of necessary controls have been inadvertently omitted can be indicative of a weak risk identification process.

It should be confirmed on sampling, that all important information within the scope of ISMS is included in the risk assessment.

Auditors should verify that there are risks identified in the documented information regarding the risk assessment results that are associated with the loss of confidentiality, integrity and availability of information within scope of the ISMS. The organization’s information security objectives can assist the auditors to identify information security risks. Auditors should also confirm that:

a) for each risk, the risk owner(s) have been identified;

b) each risk owner has the accountability and authority to manage their identified risk(s). c) Risk and Risk Treatment Plan communicated to the Risk Owners and acknowledged by the Risk Owners

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 36 of 134

**Audit practice guide – Risk analysis [ISO/IEC 27001:2022, 6.1.3d]**

Auditors should confirm that:

a) the organization comprehends the nature of identified risk and determines the level of the risk, as risk analysis in the information security risk assessment process;

b) the risk analysis provides an input to risk evaluation and to decisions on how risks need to be treated and on the most appropriate risk treatment, strategies and methods.

Auditors should also confirm that the organization has assessed the potential consequences and likelihoods associated with the risks that it identified in conformance to ISO/IEC 27001:2022, 6.1.2 c) and has thereby determined the levels of risk.

It is reasonable to expect to find a description of the organization’s approach to risk analysis in the documented information concerning the risk assessment process and the results will be in the documented information regarding the risk assessment results (see below). Auditors should refer to risk management policies, strategies, methods of the organization.

Risk analysis can be:

a) undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis and the information, data and resources available;

b) qualitative, semi-quantitative or quantitative or a combination of these, depending on the circumstances. **Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 37 of 134

**Audit practice guide – Risk evaluation [ISO/IEC 27001:2022, 6.1.3e]**

Auditors should confirm that the organization has compared the results of its risk analysis with the information security risk acceptance criteria to determine the acceptability of the identified risks.

Auditors should also confirm that results of the risk assessment(s) reveal as evidence that the risk acceptance criteria have been properly applied and that identified and analysed risks have been prioritized for treatment.

In more details, auditors should review that the risk evaluation:

a) assists in making decisions, based on the outcomes of risk analysis, about how risks need treatment and the priority for treatment implementation;

b) involves comparing the level of risk found during the analysis process with the information security risk criteria established when the context was considered.

Auditors should also assess that the decisions:

a) take account of the wider context of the risk;

b) consider the requirements of relevant interested parties, including legal, regulatory and other requirements.

**Delegate Notes - Sample Audit Questions:**

**Documented information [ISO/IEC 27001:2022, 6.1.2 and 8.2]**

Auditors should confirm that documented information regarding the risk assessment process exists.

It would be reasonable to expect that the documented information about the information security risk assessment process will contain:

a) a definition of the risk criteria including the risk acceptance criteria and the criteria for performing information security risk assessments;

b) rationale for the consistency, validity and comparability of results;

c) a description of the risk identification process (including the identification of risk owners); d) a description of the process for analysing the information security risks (including the assessment of potential consequences, realistic likelihood and resultant level of risk);

e) a description of the process for comparing the results with the risk criteria and the prioritization of risks for risk treatment.

NOTE 10 The above-mentioned items each correspond to an ISO/IEC 27001 requirement, which is why it is reasonable for information about them to be found in the documented information regarding the risk assessment process.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 38 of 134

| ***6.1.3 Information security risk treatment***  *The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results;*  *b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;*  *NOTE 1 Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;*  *NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked. NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.*  *d) produce a Statement of Applicability that contains:*  *— the necessary controls (see 6.1.3 b) and c));*  — justification for their inclusion;  — whether the necessary controls are implemented or not; and  — the justification for excluding any of the Annex A controls.  e) formulate an information security risk treatment plan; and  f) obtain risk owners’ approval of the information security risk treatment plan and acceptance of the residual information security risks.  The organization shall retain documented information about the information security risk treatment process.  *NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000* |
| --- |

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS;

b) the information security risk treatment process;

c) the results of information security risk treatment;

d) the Statement of Applicability.

Here is a sample Risk Register:

*Table 2 : Sample Risk Register Template*

| **Service/**  **Project/**  **Department** | **Related**  **Assets** | **Related**  **asset** | **Asset**  **Owner** | **Business**  **Value** | **Threat** | **Existing Control** | **Annexure A**  **Control**  **Reference** |
| --- | --- | --- | --- | --- | --- | --- | --- |

| **Impact** | **Impact**  **value** | **Likelihood**  **Value (based on existing**  **control)** | **Existing**  **Risk**  **Value** | **Risk**  **Strategy**  **(see notes on next page)** | **New**  **Control**  **selected** | **Annexure A Control**  **reference** | **Reduced**  **Impact**  **Value** | **Reduced**  **Likelihood Value** | **Reduced**  **Risk**  **Value** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Management Decision Yes / NO** | **If No, Justification for exclusion.** | **If Yes, Target Date** | **Responsible Person** |
| --- | --- | --- | --- |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 39 of 134

**Information Security Risk Treatment [ISO/IEC 27001:2022, 6.1.3]**

*Audit evidence:*

Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS;

b) the information security risk treatment process;

c) the results of information security risk treatment;

d) the Statement of Applicability.

*Audit practice guide:*

Auditors should confirm that the organization modifies information security risks as an information security risk treatment process.

Auditors also should review that the information security risk treatment involves: a) selecting one or more options for modifying information security risks, and implementing those options, which provide or modify the controls;

b) a cyclical process of assessing the effectiveness of that treatment.

**Select appropriate information security risk treatment options [ISO/IEC27001:2022, 6.1.3 a)]** Auditors should confirm that the documented information concerning the risk treatment process contains a description of the method that the organization uses for selecting appropriate information security risk treatment options. Auditors should also confirm that this description corresponds to what the organization actually performs.

Note that ISO/IEC 27000:2016, 2.79, Note 1 enumerates seven risk treatment options and there is a note referencing ISO 31000 in ISO/IEC 27001:2022, 6.1.3 from which they are derived.

Auditors should verify the consistency between the risk criteria and the risk treatment plan. The organization should be able to explain the decisions that it has made regarding risk treatment options even if they are not documented.

Auditors should review the organization's selected risk treatment options. Auditors should also review the appropriateness of the selected risk treatment options.

Auditors should verify whether recent changes (e.g., new IT systems or business processes) have been suitably incorporated in the risk assessment and the risk treatment decisions.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

**Determine all necessary controls [ISO/IEC 27001:2022, 6.1.3 b)].**

Auditors should confirm that the documented information concerning the risk treatment process contains a description of the method that the organization uses for determining necessary information security controls. Auditors should also confirm that this description corresponds to what the organization actually does.

It is a requirement [ISO/IEC 27001:2022, 6.1.3 d)] that the Statement of Applicability contains the necessary controls. The necessary controls do not need to be ISO/ IEC 27001, Annex A controls. They may be sector-specific controls (as defined in the sector specific standards, such as ISO/IEC 27011, ISO/IEC 27017). They may also be “custom controls”, as organizations can design their own or identified from any source [see ISO/IEC 27001:2022, 6.1.3 b)]. All controls determined to implement the risk treatment options should be included in the Statement of Applicability. Moreover, any custom controls should be explicitly defined as both in requirement and implementation.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 40 of 134

**Compare with Annex A [ISO/IEC 27001:2022, 6.1.3 c)]**

Conformance with this requirement is evidenced through review of the Statement of Applicability as described below.

**Produce a Statement of Applicability [ISO/IEC 27001:2022, 6.1.3 d)]**

Here is a sample SOA:

*Table 3 : Sample SoA Template*

| **Control**  **Ref** | **Control** | **Implem ented**  **( Y/N )** | **Justification** | **Justification for selection** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **RA** | **Lega**  **l** | **Contra**  **ct** | **Best**  **Practic**  **e** |
| A.5.1 | Policies for  information security | Y | Based on Risk  assessment | Y | - | Y | - |
| A.5.5 | Contact with  authorities | Y | Processing card  information | - | - | - | Y |
| A.5.8 | Information security in project management | N | No projects are  handled in the  organisation | - | - | - | Y |
| A.5.12 | Classification of  information | Y | Risk assessment | Y | - | Y | - |
| A.8.24 | Use of cryptography | Y | Risk assessment and regulatory  requirement | Y | Y | Y | - |
| A.8.24 | Segregation of  networks | Y | Risk assessment and contract | Y | - | Y | - |
| A.5.21 | Managing information security in the  information and  communication  technology (ICT)  supply chain | N | Only one vendor and no supply chain exist in the  organisation | Y | - | - | - |
| A.6.8 | Information security event reporting | Y | Risk assessment | - | - | - | Y |
| A.5.33 | Protection of records | Y | Risk assessment | Y | Y | Y | Y |

- Annexure A is the starting point for IS controls. There are 93 controls. Depending on the nature of threat and vulnerability, select appropriate control objective/s and related controls.

- It is not necessary to select all the controls listed in Annexure A under a specific control objective category. Only 1 or 2 under a control objective may be selected.

| **Statement Of Applicability (SoA) should include the following** | |
| --- | --- |
|  | 1. Should include all the Controls  2. For each of the control, If APPLICABLE or NOT APPLICABLE  3. For each of the APPLICABLE control, if IMPLEMENTED or NOT IMPLEMENTED 4. JUSTIFICATION FOR INCLUSION if APPLICABLE (Can be based on Legal Requirement, Contractual Requirement, Risk Requirement or Best Practice Requirement)  5. JUSTIFICATION FOR EXCLUSION if NOT APPLICABLE |

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 41 of 134

SoA could have other information such as How Implemented, optionally.

**Note down Issue date and version number of the SOA. This is the basis for issuing the certificate.**

| Also check if changes in SoA are approved in a MRM. Changes to Scope and SoA impact overall ISMS process and hence to be made known to the management. |
| --- |

Review the risk register and the SOA. From the risk register, take a few sample controls (both currently implemented and selected for implementation and also controls not selected) and confirm that these controls are correctly stated in the SOA. Then do the reverse.

***Remember: 6.1.3.c***

*c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;*

**SOA is just an extract from the risk register.** SOA should not be prepared before the risk register is ready, i.e., SOA should not be the outcome of a preliminary ‘gap analysis’. It has to be derived from the Risk Register.

***Note:*** Auditors should be familiar with risks that are relevant to the organisation. Also the consequences of a security event and the associated likelihood of occurrence should be understood. They should understand methods to avoid, eliminate, minimise or mitigate the risk needs to. They also need to focus on the positive aspect - opportunities for the business and how to optimize them. The risks and opportunities identified will lead to policies and objectives. Auditors should be able to identify and follow a clear path from issues and requirements through risks and opportunities, policies and objectives.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should verify that the Statement of Applicability contains:

a) the necessary controls as determined by the process of applying ISO/IEC 27001:2022, 6.1.3 b) and c);

b) the justification for their inclusion (e.g., by reference to the risk treatment options where it is used); c) whether the necessary controls are implemented or not;

d) a justification for all excluded Annex A controls (e.g.:

1) the control applies in the context of an activity that the organization does not engage in; 2) the organization uses a custom control that obviates the need for an Annex A control; 3) the organization uses a custom control that serves the same purpose as the Annex A control (see ISO/IEC 27003 for further information);

e) relevant sector-specific controls, which will either be designated as necessary controls or treated in the same way as excluded Annex A controls.

Auditors should therefore confirm the consistency between the controls necessary to realize selected risk treatment options and the Statement of Applicability.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

**Formulate a risk treatment plan [ISO/IEC 27001:2022, 6.1.3 e)]**

Auditors should confirm that the documented information concerning the risk treatment process contains a description of the method that the organization uses for producing

Auditors should also confirm that the risk treatment plan is formulated from the outputs of ISO/IEC 27001:2022, 6.1.3 a) to c).

Auditors should confirm further that the information provided in the treatment plan includes or links to: a) the risk(s) that the plan addresses;

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 42 of 134

b) necessary control(s);

c) how the necessary controls are expected to modify the risk so that the risk acceptance criteria are met;

d) the risk owners;

NOTE 11 The risk owners are responsible for approving the risk treatment plan and accepting the residual risk.

e) selected risk treatment option(s);

f) the implementation status of necessary controls;

g) the reasons for selection of treatment options, including expected benefits to be gained; h) proposed actions including responsible individuals, timeframes and schedule; i) resource requirements including contingencies;

j) performance measures and constraints;

k) reporting and monitoring.

Auditors should review that the risk treatment plan takes into consideration the objective setting and management processes of the organization and is discussed with relevant interested parties.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

**Obtain risk owner approval [ISO/IEC 27001:2022, 6.1.3f)]**

Auditors should confirm that the organization

a) identifies appropriate risk owners;

b) documents the residual risks;

c) obtains the risk owners’ approval for the information security risk treatment plan and acceptance of the residual risks.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

**Documented information**

Auditors should confirm that documented information regarding the risk treatment process exists. It would be reasonable to expect that the documented information about the information security risk treatment process will contain descriptions of:

a) the method for selecting appropriate information security risk treatment options; b) the method for determining necessary controls;

c) how ISO/IEC 27001:2022, Annex A is used to determine that necessary controls have not been inadvertently overlooked;

d) how the SOA is produced;

e) how the risk treatment plan is produced;

f) how risk owners’ approval is obtained.

NOTE 12 There is no particular requirement for the content or format of an organization’s risk treatments plan

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 43 of 134

| ***ISO/IEC 27001:2022 - 6.2 Information security objectives and planning to achieve them*** *The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:*  *a) be consistent with the information security policy;*  *b) be measurable (if practicable);*  *c) take into account applicable information security requirements, and results from risk assessment and risk treatment;*  *d) be communicated;*  *e) be monitored;*  *f) be updated as appropriate;*  *g) be available as documented information.*  *The organization shall retain documented information on the information security objectives.*  *When planning how to achieve its information security objectives, the organization shall determine: h) what will be done;*  *i) what resources will be required;*  *j) who will be responsible;*  *k) when it will be completed; and*  *l) how the results will be evaluated.* |
| --- |

**Plain English Explanation**

- The requirements for the planning objectives are narrated in greater detail. The planning objectives are to be consistent with the ISMS policy, measurable (if practicable), consider applicable requirements, monitored, communicated, and updated as appropriate. They have to be established at relevant functions and levels.

- Developing measuring technique and constantly evaluating the effectiveness can demonstrate that the management system is continually improving.

- Other Management Systems Standards, for example, ISO 45001:2018 uses the terms ‘objectives’ and ‘programmes’ to achieve those objectives. This is conceptually similar to ‘selection of controls’ and a ‘risk treatment plan’ but a higher level of MANAGEMENT SYSTEM STANDARDS objectives.

- To achieve specific objectives, we need to have a ‘programme’, i.e., a series of projects to implement the overall MANAGEMENT SYSTEM STANDARDS within which ‘selection of controls’ and ‘risk treatment’ will be specific projects.

***If we have an overall ISMS project plan based on specific goals for the ISMS project, that would satisfy the requirements of this clause.***

**Audit tool**

*Whom to meet:* Top Management

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on information security objectives and plans to achieve them.

Risk Assessment Document, Risk treatment plan, Metrics document, Responsibility matrix, KPIs, KRAs

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

It is noted that there are linkages from information security objectives and planning to achieve them (ISO/IEC 27001:2022, 6.2) to leadership and commitment (5.1) and policy (5.2).

Auditors should confirm that:

a) information security objectives are established at relevant functions and levels of the organization;

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 44 of 134

b) information security objectives are specified in a way that allows determination of their fulfilment to be made;

c) objectives are measurable, if applicable (there can be situations when it may not be feasible to measure an information security objective);

d) the status and progress on information security objectives and plans to achieve them are periodically verified in accordance with the requirements of monitoring, measurement, analysis and evaluation (9.1) and updated as appropriate, consistent with the requirements of continual improvement (10.2);

e) information security objectives and plans to achieve them are communicated in accordance with the requirements of the communication (7.4);

f) documented information of the objectives is created and controlled in accordance with the requirements of documented information (7.5).

Auditors should also verify that:

a) the actions required to achieve the information security objectives (i.e., “what”) and the associated timeframe (i.e., “when”) are determined;

b) the assignment of responsibility for doing it (i.e., “who”) is established in accordance with the requirements of organization roles, responsibilities and authorities (5.3);

c) applicable information security requirements, and results from risk assessment and risk treatment are taken into account in the objectives and planning to achieve them;

d) any need for budgets, specialized skills, technology or infrastructure, for example, to achieve the objectives are determined and provided in accordance with the requirements of resources (7.1); e) a mechanism for evaluating the overall results of what was accomplished is determined in accordance with the requirements of monitoring, measurement, analysis

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 45 of 134

**NEW**

| ***ISO/IEC 27001:2022 - 6.3 Planning of changes***  When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner. |
| --- |

**Plain English Explanation**

⎯ Changes to ISMS like transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 should be planned and managed.

⎯ The change includes review of ISMS for changes in Internal and External Context like new business line, mergers, etc. Changes can also align with A.8.32 Change Management.

**Audit tool**

*Whom to meet:* Top Management / CISO

*Audit Evidence:*

Audit evidence can be obtained through documented information as evidence of changes in ISMS are handled in a planned manner and not ad-hoc.

E.g., MRMs, Change Requests, Project Plan

Auditors should confirm that:

a) Changes to ISMS shall be incorporated in all the projects involving changes to internal and external stakeholder’s requirements such as New Regulations, Changes in products / services, Forward as well as Backward Integration, Mergers, etc.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 46 of 134

**6. Support**

| ***ISO/IEC 27001:2022 - 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.* |
| --- |

**Audit tool**

*Whom to meet:* HR Manager, Facilities Manager, IT Manager, Purchase Manager

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on the resources that organisation needs to:

a) establish and implement the ISMS (including its operations and controls);

b) maintain and continually improve the ISMS.

For example, Personnel records, Facilities maintenance records, IT procurement of IT Security hardware and software.

Resources can include:

a) people;

b) specialized skills or knowledge;

c) organizational infrastructure (e.g. buildings, communication lines, etc.);

d) technology;

e) information, other assets associated with information and information processing facilities; f) money (e.g. cash, liquid securities and credit lines)

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization anticipates, determines and allocates the resources needed for establishing and implementing the ISMS (including its operations and controls), as well as those needed for its maintenance and continual improvement.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 47 of 134

| ***ISO/IEC 27001:2022 - 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.*  *NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.* |
| --- |

**Plain English Explanation**

Technical training for relevant areas is required for those managing security, i.e., ISMS Project Team, Incident Management Team, ISMS Internal Audit Team, etc.

For example:

● Training in ISO/IEC 27001

● Firewall administration

● On Boarding of staff

● Network Vulnerability management

● Monitoring Data Centre environment

● Risk assessment

Copies of professional certifications in security, if any, should be maintained on the personnel files.

**Audit tool**

*Whom to meet:* Management Representative

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on relevant: a) organizational roles, responsibilities and authorities;

b) job descriptions;

c) required competence;

d) previous employment references

e) Employee’s training certificate

f) records of education;

g) training programmes, courses and educational activities;

h) records of actions taken to acquire and retain the necessary competence;

i) evaluation of their effectiveness.

ISO/IEC 27001:2022, 7.2 broadens the scope of competence to persons who are not members of the organization. The requirement specifies that they are “doing work under the control of the organization”. Examples can include subcontractors and volunteer workers.

Audit evidence requested from a third party should be restricted to the evidence of the functions and activities performed for the ISMS organisation.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization:

a) determines:

1) the persons doing work under its control that affects its information security performance;

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 48 of 134

2) the knowledge and skills for the persons to achieve intended results;

3) the ability of the persons to apply the knowledge and skills to achieve intended results; b) ensures that these persons have the ability on the basis of appropriate education, training, or experience; c) where applicable, takes actions to acquire the necessary ability and evaluate the effectiveness of actions taken.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 49 of 134

| ***ISO/IEC 27001:2022 - 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.* |
| --- |

**Plain English Explanation**

Awareness training is required for all employees. If all the employees are aware of ISMS, the level of compliance will be much higher. If they understand why they have to follow the policies and how they are to be followed, the security posture of organisation will certainly show an upward trend.

**Audit tool**

*Whom to meet:* Management Representative. HR / Training Manager.

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on: a) information security policy;

b) Information security objectives;

c) information security performance;

d) nonconformity and corrective action;

e) organizational roles, responsibilities and authorities;

f) job descriptions;

g) awareness programmes and training material, where applicable.

h) Training attendance sheets and training feedback form.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that persons doing work under the organization’s control are aware of: a) the information security policy;

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

c) the implications of not conforming with the ISMS requirements.

Auditors should interview an appropriate number of persons as sampling to confirm that they are aware of this information.

Awareness of the policy should not be taken to mean that it needs to be memorized; rather, persons should be aware of the key policy commitments, and their role in achieving them.

Auditors can find information security awareness evidence also in awareness and training initiatives not dedicated to information security. These activities can be closely related to the communication activities by top management [ISO 27001:2022, 5.1 d) and 7.4].

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 50 of 134

| ***ISO/IEC 27001:2022 - 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.* |
| --- |

**Plain English Explanation**

Communication is an important element for any Management System Standard. Other standards, for example, ISO 45001:2018 have detailed requirements for communication. Now these are of part of the requirements for all Management System standards.

Communication chart – example:

*Table 4 : Sample Communication Chart*

| **What**  VPN usage | **When** | **To whom** | **How** |
| --- | --- | --- | --- |
| Monthly | customer | IT Manager via email |
| ISMS Policy | Annually | All employees | HR-Training section via  Classroom |
| SLA terms | Quarterly | Suppliers | Purchase Manager via Face-to face Meeting |

**Audit tool**

*Whom to meet:* Management Representative.

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on a) information security policy;

b) organizational roles, responsibilities and authorities;

c) the information security risk assessment process;

d) the information security risk treatment process;

e) information security objectives;

f) information that the processes have been carried out as planned;

g) the results of the information security risk assessments;

h) the results of the information security risk treatment;

i) performance of the ISMS;

j) results of audits;

k) results of management reviews.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization's communication needs are identified, implemented and maintained effectively along the communication requirements of ISO/IEC 27001.

Examples of evidence can include:

a) answers being documented in the minutes of a meeting, or

b) a formal communications plan, documented procedures and results, or

c) interviews with people assigned to defined roles in order to demonstrate that they know, for communication relevant to their roles, on what, when, whom to communicate, who have authorities for such communication and how it is the processes by which communication is affected.

Such evidence can be supplemented by:

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 51 of 134

a) information of communication on the following:

1) importance of effective information security management and of conforming to the information security management system requirements;

2) policy;

3) responsibilities and authorities;

4) performance of the ISMS;

5) objectives;

6) contribution to the effectiveness of the ISMS, including the benefits of improved performance; 7) implications of not conforming with the ISMS requirements;

8) results of audits;

b) a formal communications plan, documented procedures and results.

Auditors should verify that the organization has determined its needs for communication related to the ISMS. For example, these can include transparency, appropriateness, credibility, responsiveness, clarity and protection. Communication can be verbal or written, one-way or two-way, internal or external.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 52 of 134

**7.5 Documented information**

| ***ISO/IEC 27001:2022 - 7.5 Documented information***  ***7.5.1 General***  *The organization’s information security management system shall include:*  *a) documented information required by this International Standard; and*  *b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.*  *NOTE The extent of documented information for an information security management system can differ from one organization to another due to:*  *1) the size of organization and its type of activities, processes, products and services; 2) the complexity of processes and their interactions; and*  *3) the competence of persons.* |
| --- |

**Plain English Explanation**

So far, all MANAGEMENT SYSTEM STANDARDS had two terms ‘documents’ and ‘records. Now they are called ‘documented information.’. **The phrase “documented information as evidence of ...” implies the former term “record”.**

● Approve documents before you distribute them.

● Have a suitable naming convention. Specify the current revision status of your documents. ● Review and re-approve documents whenever you update them.

● Provide the correct/relevant version of documents at points of use.

● Monitor documents that come from external sources. Know how you will ensure you have the latest issue.

● Prevent the accidental use of obsolete documents.

● Preserve the usability of your Information Security documents.

● Clarify identification, storage, protection, retrieval, retention time and disposition. ● Ensure you do not throw your records away too early; they can be used to prove your organisation was duly diligent in a court of law! Know what laws can be used in product litigation and the statute of limitations pertinent to each law.

● Define the retention period, for example, 7 years for emails.

● Also, define on-line retention period and off-line retention period.

**Audit tool**

*Whom to meet:* All process owners and employees

*Audit Evidence 7.5.1 (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information created, controlled and/or maintained in an ISMS, including:

a) scope of the management system;

b) policy;

c) objectives;

d) evidence of competence;

e) information of external origin necessary for the planning and operation of the management system; f) information security risk assessment process;

g) information security risk treatment process;

h) Statement of Applicability;

i) information necessary to have confidence that the processes and determined controls have been carried out as planned;

j) results of information security risk assessment;

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 53 of 134

k) results of information security risk treatment;

l) monitoring, measurement, analysis and evaluation results;

m) internal audit programme and evidence of its implementation;

n) internal audit results;

o) management review results;

p) nature of nonconformities and actions taken;

q) corrective action results.

Documented information, originally created for the purposes other than the fulfilment of the requirements of ISO/IEC27001, can be used.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization’s ISMS includes:

a) documented information required by ISO/IEC 27001;

b) documented information determined by the organization as being necessary for the effectiveness of the ISMS.

Auditors should confirm that the organization determines what documented information it needs beyond that which is explicitly required by ISO/IEC 27001 for the effectiveness of its ISMS. The factors it should take into account are listed in the row of audit evidence.

The term “documented information” refers to information that ISO/IEC 27001 determines is necessary to control and maintain in any format or media (see 7.5.3).

The auditor should confirm that documented information is created and controlled in accordance with the requirements of 7.5.2 and 7.5.3.

**Delegate Notes - Sample Audit Questions:**

| ***ISO/IEC 27001:2022 - 7.5 Documented information***  ***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.* |
| --- |

*Audit Evidence 7.5.2 (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on: a) common attributes which allow clear and unique identification;

b) format and media used;

c) date of last review or update;

d) history of changes;

e) identity of reviewer and approver

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that when creating and updating documented information, the organization ensures 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); c) review and approval for suitability and adequacy documented information.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 54 of 134

NOTE 13 The identification, format and media used for documented information are the choice of the organization implementing ISO/IEC 27001; it need not be in the form of a textual format or a paper manual.

Auditors should take the opportunity to carry out these audit tasks whenever documented information within scope of the ISMS is presented to the audit. They do not need to be performed each and every time Just a sufficient number to confirm conformity to ISO/IEC 27001:2022, 7.5.2.

**Delegate Notes - Sample Audit Questions:**

| ***ISO/IEC 27001:2022 - 7.5 Documented information***  ***7.5.3 Control of documented information***  *Documented information required by the information security management system and by this International Standard 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).* |
| --- |

*Audit Evidence 7.5.3 (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on the following activities:

a) distribution, access, retrieval and use;

b) storage and preservation, including the preservation of legibility;

c) control of changes (e.g., version control);

d) retention and disposition;

e) structure and configuration of documented information library.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that documented information required by the ISMS and by ISO/IEC 27001 is controlled to ensure that:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity).

The auditor should confirm that the organization addresses the following activities, as applicable: a) distribution, access, retrieval and use;

b) storage and preservation, including the preservation of legibility (in digital or other formats or hand-written);

c) control of changes (e.g., version control);

d) retention and disposition.

Auditors should take the opportunity to carry out these audit tasks whenever documented information within the scope of the ISMS is presented to the audit. They do not have to be performed each and every time, just a sufficient number to confirm conformity to ISO/IEC 27001:2022, 7.5.3.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 55 of 134

**8. Operation**

| ***ISO/IEC 27001:2022 - 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.* |
| --- |

**Plan English Explanation.**

| **All ISMS processes such as Risk Assessment, Internal Audit, MRM, Communication, etc (Refer control 4.4) should have an established criterion. What could be criteria? Criteria could be** | |
| --- | --- |
|  | • Regularity – Processes are repeated on regular basis  • Accountability – Every process should have an identified owner  • Value Generating – Delivers direct value to the management  • End-to-End – Each process is monitored and tracked end-to-end |

Most of the ISO Management System Standards have unique requirements only in clause 8. The other clauses 4,5,6,7,9 and 10 are almost the same for all the ISO Management System Standards. But ISMS standard ISO/IEC 27001 is unique. Requirements specific to ISMS have been grouped as Annexure A.

**In the latest BCMS standard ISO 22301:2019**, the committee has clarified that ‘risk assessment’ as stated in clause 6.0 is for ‘Risk to BCMS management system’ and ‘risk assessment’ as stated in clause 8 is for risks to business operations. In ISMS, this separation is not transparent except for the term ‘Operation’ as header for clause 8. Clause 6.1 refers to risks to ISMS but includes a requirement as shown below:

| ***Clause 6.1.2 c (1):***  *apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and* |
| --- |

Therefore clause 6 includes requirements for ISMS risk as well as business operational risk. In our opinion, clause 8.2 is a repetition of clause 6.1.2 Risk assessment and clause 8.3 is a repetition of clause 6.1.3 – Risk Treatment.

**NOTE: ISMS is one of the rare ISO standards where an Annexure is a part of the requirements. Usually, annexures are for information only.**

**Audit tool**

*Whom to meet:* Management Representative, Process owners

*Audit Evidence 8.1 (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 56 of 134

Audit evidence can be obtained through documented information or other information which is: a) needed for the organization to have confidence that the operational control processes have been carried out as planned is created and controlled (ISO/ IEC 27001:2022, 8.1);

b) determined by the organization as being necessary for the effectiveness of the ISMS [ISO/IEC 27001:2022, 7.5.1 b)];

c) on planning for the ISMS (ISO/IEC 27001:2022, 6.1.1);

d) on information security objectives (ISO/IEC 27001:2022, 6.2).

For example: Information security risk assessment procedure, Risk Treatment plan, SOA

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization plans, implements and controls the processes needed to meet information security requirements within the organization’s operations to make sure that the requirements of ISO/IEC 27001 are fulfilled and the priority risks and opportunities are being addressed.

Auditors should confirm that the operational control includes the methods and information security controls implemented to make sure business operations, activities or equipment conform to specified conditions, performance standards or regulatory compliance limits, and thereby effectively achieve the intended outcome of the ISMS. These controls establish technical requirements necessary to achieve the desired optimal functionality for business processes, such as technical specifications or operating parameters or a prescribed methodology.

Reviewing should be performed for the situations which the operational control and information security controls are required for, related to business processes where absence of the operational control and information security controls could lead to deviations from the policy and objectives or poses unacceptable risk. These situations can be related to business operations, activities or processes, production, installation or servicing, maintenance or contractors, suppliers or vendors. The degree of control exercised will vary depending on many factors, including the functions performed, their importance or complexity, the potential consequences of deviation or variability or the technical competency involved versus what is available.

Auditors should thereby verify that the organization:

a) implements the actions determined in “actions to address risks and opportunities” (ISO/IEC 27001:2022, 6.1);

b) implements the plans to achieve information security objectives determined in Information security objectives and planning to achieve them (ISO/IEC 27001:2022, 6.2);

c) creates and controls documentation needed to have confidence that the operational control processes and information security controls have been carried out as planned in accordance with the requirements of documented information (ISO/IEC 27001:2022, 7.5);

d) controls planned changes and reviews the consequences of unintended changes, to prevent or otherwise minimize the chance technical requirements are not fulfilled or new risks are introduced (ISO/IEC 27001:2022, 6.3);

e) objectives, guidelines or procedures that address the implementation of process f) takes actions necessary to address any resultant undesired effect(s) when operational controls fail; g) ensures that outsourced processes are determined and controlled, i.e., applies the control of

operations under considerations such that the degree of control can be limited to partial control or influence and be not intended to change any legal relationship with the external entity performing the outsourced process.

**Delegate Notes - Sample Audit Questions**

***ISO/IEC 27001:2022 - 8.2 Information security risk assessment***

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 57 of 134

*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.*

**Plain English Explanation (copied from clause 6.1 above for immediate reference)**

**RISK ASSESSMENT**

- Any Risk Assessment method can be used.

- Define a comparable and repeatable process of risk assessment.

- The process is repeatable if the same person does risk assessment over a period of time and comparable if several people use the same method and arrive at similar conclusions about the information security risk level, type of threats, list of controls from Annexure, etc.

- The ISMS Auditor should look for several indicators of comparable and repeatable process: ● list of threats based on nature of service/asset

● a standard method of measuring ‘likelihood’ of threats, for example 1 to 5,

● a defined list of information security risks,

● a defined method of assessing the risk level, for example 1 to 5,

● list of controls from Annexure A related to specific information security risks - List all services/projects/department and related information assets within the scope of ISMS and their risk owners.

- Conduct risk assessment and select controls to reduce the risk to a predefined acceptable level. - Review the risk register. Confirm that minutes are available for discussion with Risk Owners and selection of controls.

- Review a higher percentage of Very High/High value risks and a lower percentage of risk of low or negligible value.

*Audit Evidence 8.2 (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS (ISO/IEC 27001:2022, 6.1.1);

b) the information security risk assessment process (ISO/IEC 27001:2022, 6.1.2); c) the results of information security risk assessment (ISO/IEC 27001:2022, 8.2); d) the Statement of Applicability;

e) the risk treatment plans.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the information security risk assessment process defined and applied in (ISO/IEC 27001:2022, 6.1) is implemented and integrated into the organizational operations and be performed at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in ISO/ IEC 27001:2022, 6.1.2 a).

Auditors should assess that:

a) the planned intervals at which the risk assessment is performed are appropriate to the ISMS; b) when any significant changes of the ISMS (or its context) or information security incidents have occurred, the organization determines which of these changes or incidents require an additional information security risk assessment and how these assessments are triggered.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 58 of 134

| ***ISO/IEC 27001:2022 - 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.* |
| --- |

**(Please also see 6.1.3 above)**

*Audit Evidence 8.3 (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS;

b) the information security risk treatment process;

c) the risk treatment plans;

d) the results of information security risk treatment;

e) the Statement of Applicability.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the information security risk treatment process defined and applied in "Planning the ISMS" and “Planning of Changes” (ISO/IEC 27001:20222, 6.1 and 6.3) is implemented and integrated into the organizational operations and be performed after each iteration of the information security risk assessment process (ISO/IEC 27001:2022, 8.2) or when the implementation of (parts of) the risk treatment has failed.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 59 of 134

**9. Performance evaluation**

| ***ISO/IEC 27001:2022 - 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.* |
| --- |

**Plain English Explanation**

Many of these following devices such as Anti-malware, Firewalls, Intrusion Detection/Prevention, Web Filtering, Anti-SPAM, Patch Management, Application Security Scanners, Databases, Network Access Control, Operating Systems, Data Leakage Protection, Configuration Hardening, Secure Web Gateways, Web Application Firewalls and Mobile Data Protection can be monitored, and the results can be measured. Various logs collected from these sources can be analysed and evaluated. If an organisation is using the log analysis software, it may be possible to co-relate various events.

**Audit tool**

*Whom to meet:*

Network team, application development team, backup team, IT infra team,

Process Owners

- Monitor ISMS metrics

Other Managers:

- Conduct internal ISMS audits

Senior Management:

- Conduct management reviews

- Review risk assessments at least once a year or when there is major change

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information on the results of monitoring, measurement, analysis and evaluation (see ISO/ IEC 27001:2022, 9.1).

Evidence can also be obtained through documented information or other information about: a) information security objectives at relevant functions and levels;

b) planning how to achieve the information security objectives;

c) the status of and extent to which the information security objectives are fulfilled;

d) reporting on the performance of the ISMS to top management [see ISO/ IEC 27001:2022, 5.3 b)]; e) planned changes that could affect the current ISMS [see ISO/ IEC 27001:2022, 6.3];

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

g) the methods for monitoring, measurement, analysis and evaluation;

h) internal audit programme(s) and the audit results;

i) management review(s) and the management reviews' results;

j) information security events reports (see ISO/IEC 27001:2022, A.6.8);

k) Information security incident management planning and preparation (see ISO/IEC 27001:2022, A.5.24).

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization has:

a) evaluated the information security performance and effectiveness of its ISMS;

b) has thereby determined:

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 60 of 134

1) what to be monitored and measured (qualitatively and quantitatively), including information security processes and controls;

2) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

3) when the monitoring and measuring is to be performed;

4) who performs monitoring and measurement;

5) when the results from monitoring and measurement are to be analysed and evaluated; 6) who conducts analysis and evaluation of these results;

7) how the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 worked out.

Auditors should review the information security performance using documented information as evidence such as plans, reports on the performance of the ISMS to top management, the results of management review, internal audit reports and information security event, weakness incident reports.

Auditors should assess the extent to which nonconformities, processing errors, information security breaches and other incidents are predicted, detected, reported and addressed. Auditors should determine whether and how the organization evaluates the effectiveness of the actions to address the risks and opportunities to ensure that the information security controls identified in the risk treatment, are effectively implemented and be in operation.

Auditors should also assess the evaluation of information security performance for being used to drive continual improvements of the ISMS.

Auditors should also confirm that changes to be considered (ISO/IEC 27001:2022, 6.3, 8.1 and 8.2) as of the results are reflected in the processes for risk assessment and risk treatment processes. In addition, auditors should confirm that the documented information related to the actions to address risk and opportunities have been updated.

Auditors should review that the information of characteristics that are monitored or measured, analysed and evaluated is necessary and sufficient enough to judge the extent to which the ISMS planned activities are realized and its planned results are achieved.

Auditors should confirm that the information gained through monitoring or measurement, analysis and evaluation is presented to top management in accordance with the requirements of management review (ISO/IEC 27001:2022, 9.3.2 and 9.3.3).

NOTE 14 If an organization follows the guidance given in ISO/IEC 27004, in addition to “information need”, it can use the terms “performance measure” and “effectiveness measure”.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 61 of 134

| ***ISO/IEC 27001:2022 - 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.*  **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.* |
| --- |

**Plain English Explanation**

● Develop an internal audit procedure.

● Set up an internal audit program and train internal auditor.

(Note: A Security calendar may include internal audit program, external audit program, security monitoring program, etc.)

● Ensure that audits are conducted by independent persons.

● Perform regular internal audits (see 9.2.2).

● Report problems discovered during audits (see 9.2.2).

● **Conduct a Follow up** audit to verify that implemented solutions have solved the problems (see 9.2.2). ● Records of the audits and their results shall be maintained (see 4.3.3).

● The management responsible for the area being audited shall ensure that any necessary corrections and corrective actions (see 9.2.2)

Remember – It is the auditee’s (process owners) responsibility to develop a solution, not the auditors. Be helpful and contribute to the problem solving if asked. If the auditor’s attitude is helpful they will be asked to help solve the problems found).

**Audit tool**

*Whom to meet:* Management Representative, ISMS Implementation team

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information about: a) an internal audit programme(s);

b) internal audit plans;

c) internal audit results;

d) competence of internal auditors;

e) results of management reviews.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization plans, implements and maintains an internal audit programme for the purpose of providing information on whether the ISMS conforms to both ISO/IEC 27001 requirements and any additional ISMS related requirements the organization self imposes and that the ISMS is being effectively implemented and maintained as planned.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 62 of 134

Auditors should verify that the internal audit programme is such that:

a) internal audits are planned and scheduled based on the importance of the processes audited and the results of previous audits;

b) the approach for planning and conducting internal audits is established;

c) roles and responsibilities within the audit programme are assigned by taking into account the integrity and independence of the internal audit process;

d) the audit objectives, audit criteria and audit scope are established for each audit planned; e) it is designed to provide information to confirm that the ISMS conforms to:

1) the requirements of ISO/IEC 27001;

2) the organization’s own requirements;

f) it is designed to provide information to confirm that the ISMS is effectively implemented and maintained. An example of an audit criterion is a reference (e.g., policies, procedures and requirements) against which relevant and verifiable records, statements of fact or other information will be compared.

Audit scopes can include descriptions of the physical locations, organizational units, activities and processes, as well as the time period covered for the audits concerned.

Auditors should confirm that the internal audit programme and the audits are planned and implemented and maintained by internal personnel or be managed by external persons acting on the organization’s behalf. In either case, auditors should confirm that the selection of persons responsible for managing the internal audit programme and the auditors who conduct the internal audits meet competence (see ISO/ IEC 27001:2022, 7.2 and 9.2) requirements and guidelines (see ISO/IEC 27007:2022, 7.2).

Auditors should confirm that the results of internal audits are reported to the management responsible for the functions/unit audited and any other individuals deemed appropriate in accordance with the requirements of communication (ISO/ IEC 27001:2022, 7.4). Auditors should confirm that the information, including trends, on internal audit results is reviewed in accordance with the requirements of management review (see ISO/IEC 27001:2022, 9.3).

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 63 of 134

| ***ISO/IEC 27001:2022 - 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.*  **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;*  *c) feedback on the information security performance, including trends in:*  *- nonconformities and corrective actions;*  *- monitoring and measurement results;*  *- audit results; and*  *- fulfilment of information security objectives;*  *d) feedback from interested parties;*  *e) results of risk assessment and status of risk treatment plan;*  *f) opportunities for continual improvement.*  **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.* |
| --- |

**Plain English Explanation**

There are many business meetings where issues related to information security are discussed. For example, monthly dashboard review meetings, weekly operational review meetings, daily stand up meetings, etc. One question we always come across is: can we not consider one of these meetings as a ‘Management Review meeting’? The answer is NO.

Another question frequently asked is: Should it be a face-to-face meeting always? The answer is NO. Management Representatives and BCMS champions should report on the status of BCMS to Top Management. In a small organization, this may just one of the daily meetings that the Manager in charge of BCMS has with the CXO. Or it can be an audit/video conference call.

Top management should chair the Management Review Meeting (MRM). For small organizations, one MRM per year is enough. It should be a meeting 'dedicated to ISMS ISO/IEC 27001’ and should strictly adopt the agenda as required in clause 9.3 of ISO/IEC 27001:2022. If it is difficult to organize a separate meeting for ISMS, then one of the normal monthly meetings may be extended as an MRM. But agenda as required in clause 9.3 of ISO/IEC 27001:2022. should be adopted for such a meeting.

**Audit tool**

*Whom to meet:* Management Representative

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information about: a) conducting the reviews at planned intervals;

b) the status of actions from previous management reviews;

c) changes in external and internal issues that are relevant to the ISMS;

d) feedback on the information security performance, including trends in nonconformities and corrective actions, monitoring and measurement results, audit results and fulfilment of information security objectives; e) feedback from interested parties;

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

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 64 of 134

g) opportunities for continual improvement.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that top management has conducted management reviews in accordance with a planned schedule of reviews, reviewing the information to be covered and providing the expected outputs.

Auditors should assess through auditing that the top management be personally engaged in this review, carrying out this mechanism to drive changes to the ISMS and direct continual improvement priorities, particularly in relation to the changing issues in the organization’s context, deviations from intended results or favourable conditions that offer an advantage with beneficial outcome. Auditors should verify that the management review includes consideration of all the items b) to g) listed in the audit evidence of A.6.3.

Auditors should also confirm that the outputs of the management review include decisions related to continual improvement opportunities and any needs for changes to the ISMS.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 65 of 134

**10. Improvement**

| **ISO/IEC 27001:2022 - 10.1 Continual improvement**  The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system. |
| --- |

**Plain English Explanation**

**Suitability**

- Changing Information security policy according to the developing needs

- Reviewing and modifying Information security objectives

**Effectiveness**

- Take actions on Audit results

- Analysis of monitored events

- Ensure corrective actions are taken effectively and on time

**Adequacy**

- Management review

- Detect potential nonconformities.

- Reviewing the effectiveness of your corrective actions.

**Audit tool**

*Whom to meet:* Management Representative

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information about: a) the nature of nonconformities and any subsequent actions taken, including reporting of corrective actions; b) the results of any corrective action;

c) monitoring and measurement results;

d) audit programme(s) and the audit results;

e) the results of management review;

f) the requirements of interested parties relevant to information security;

g) assessment & decision on information security event and incidents (see ISO/IEC 27001:2022, A.5.25).

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that the organization conducts its recurring activity to enhance measurable results of the suitability, adequacy and effectiveness of the ISMS.

Auditors should review and verify that the continual improvement involves making changes to the design and implementation of the ISMS in order to improve the organization’s ability to achieve conformity with the requirements of the ISMS and meet its objectives and policy commitments.

Auditors should confirm through auditing that the organization:

a) develops a implementation to achieve this improvement, including, but not limited to: 1) taking actions to address risks and opportunities (see ISO/IEC 27001:2022, 6.1);

2) establishing objectives (see ISO/IEC 27001:2022, 6.2);

3) upgrading operational controls (see ISO/IEC 27001:2022, 8.1), taking into consideration new technologies, methods or information;

4) analysing and evaluating performance (see ISO/IEC 27001:2022, 9.1);

b) conducts internal audits (see ISO/IEC 27001:2022, 9.2);

c) conducts management reviews (see ISO/IEC 27001:2022, 9.3);

d) detects non-conformity(ies) and implements corrective action(s) (see ISO/ IEC 27001:2022, 10.2); e) periodically evaluates and reviews its ISMS in accordance with the requirements of monitoring, measurement, analysis and evaluation (ISO/IEC 27001:2022, 9.1) and internal audit (ISO/IEC 27001:2022, 9.2) and management review (ISO/IEC 27001:2022, 9.3) to identify opportunities for improvement and plans appropriate actions to be taken in accordance with actions to address risks and opportunities (ISO/ IEC

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 66 of 134

27001:2022, 6.1), objectives and planning to achieve them (ISO/IEC 27001:2022, 6.2), planning of changes (ISO/IEC 27001:2022, 6.3) and operational planning and controls (ISO/IEC 27001:2022, 8.1).

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 67 of 134

| **ISO/IEC 27001:2022 - 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.* |
| --- |

**Plain English Explanation**

The word preventive action has been removed from this section. However, the corrective action is given more prominence. It is emphasised that the action taken are eliminate the root cause for the non-conformity, so that it does not recur elsewhere.

**Audit tool**

*Whom to meet:* Management Representative

*Which documented information to review:*

Information Security policy, Internal audit reports, corrective actions

*Audit Evidence (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Audit evidence can be obtained through documented information or other information about: a) the nature of the nonconformities and any subsequent actions taken;

b) the results of any corrective action;

c) monitoring and measurement results;

d) audit programme(s) and the audit results;

e) the results of management review;

f) the requirements of interested parties relevant to information security;

g) the changes to the ISMS brought by corrective actions.

*Audit practice guide (Ref: ISO/IEC 27007:2017 Annexure A Table A2):*

Auditors should confirm that

a) the organization responds by finding nonconformity and requiring corrective action when ISO/IEC 27001 and ISMS (including operational) requirements are not satisfied;

b) the nonconformity and corrective action includes taking action to correct the situation, examine the cause and determine if other occurrences exist or potentially exist elsewhere so that action can be taken to prevent recurrence;

c) the organization’s response covers evaluation of the action taken to confirm that the intended result was achieved, and evaluation of the ISMS to determine if changes are warranted to avoid future occurrences of similar nonconformities;

d) documentation of the nonconformity, corrective action and the results is created and controlled in accordance with the requirements of documented information (see ISO/IEC 27001:2022, 7.5). **Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 68 of 134

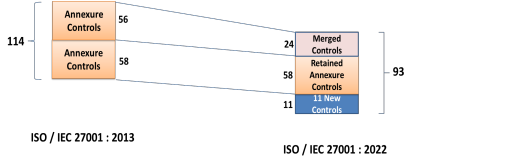
***ANNEXURE CONTROLS***

**Changes in Annexure Controls from ISO/IEC 27001:2013**

• The control sets are now organized into four (4) categories or themes as opposed to fourteen (14) control domains. The 4 categories include Organizational, People, Physical, and Technological. • The total control count has been reduced—there are 21 less controls in the 2022 version; leading to a total of 93 controls.

• There was a concentrated effort to avoid control redundancy. 24 controls in the 2022 version included merged controls from the 2013 version.

• There are now 11 new controls to update the standard to the current information security and cyber security landscape.

• Objectives for controls have been removed from ISO/IEC 27001:2022 standards. **Comparison of ISO/IEC 27001:2013 and ISO/IEC 27001:2022 ANNEXURE CONTROLS ***Figure 2 : Mapping of ISO/IEC 27001:2013 to ISO/IEC 2001:2022*

**All 93 Annexure Controls have now been categorized under 4 categories as below:**

*Table 5: Categories of ISO/IEC 27001:2022 Annexure Controls*

| **Control Area (i.e., Domain)** | **No of Controls** |
| --- | --- |
| A.5 Organizational controls | 37 |
| A.6 People controls | 8 |
| A.7 Physical controls | 14 |
| A.8 Technological controls | 34 |
|  | **93** |

Note:

1. In Risk Treatment, you select either one or more of controls.

a. Control Reference stated in ISO/IEC 27001:2022. ISMS Auditor can find this in the risk register and the Statement of Applicability.

b. PLAIN ENGLISH EXPLANATION is based on ISO/IEC 27002:2022 – Guidelines on ISMS controls - and is written in a user-friendly style.

**Delegate Notes - Sample Audit Questions:**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 69 of 134

**A.5 Organisational Controls**

| ***Control Ref A.5.1 Policies for information security***  ***Control:*** *Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.*  ***ISO/IEC 27001:2013 Ref: A.5.1.1 & A.5.1.2*** |
| --- |

**PLAIN ENGLISH EXPLANATION**

Set of policies covering APPLICABLE ISMS controls shall be documented, approved by management, published and communicated to necessary stakeholders as per defined Information classification and the policies shall be reviewed and updated as and when necessary ie when a significant change occurs to ISMS processes requiring a change in the policy(ies), based on a defined frequency if there are no changes.

**Ref: ISO/IEC 27002:2022**

At a lower level, the information security policy should be supported by topic-specific policies as needed, to further mandate the implementation of information security controls. Topic-specific policies are typically structured to address the needs of certain target groups within an organization or to cover certain security areas. Topic-specific policies should be aligned with and complementary to the information security policy of the organization.

Examples of such topics include:

a) access control;

b) physical and environmental security;

c) asset management;

d) information transfer;

e) secure configuration and handling of user endpoint devices;

f) networking security;

g) information security incident management;

h) backup;

i) cryptography and key management;

j) information classification and handling;

k) management of technical vulnerabilities;

l) secure development.

The responsibility for the development, review and approval of the topic-specific policies should be allocated to relevant personnel based on their appropriate level of authority and technical competency. The review should include assessing opportunities for improvement of the organization’s information security policy and topic-specific policies and managing information security in response to changes to:

a) the organization’s business strategy;

b) the organization’s technical environment;

c) regulations, statutes, legislation and contracts;

d) information security risks;

e) the current and projected information security threat environment;

f) lessons learned from information security events and incidents.

The review of information security policy and topic-specific policies should take the results of management reviews and audits into account. Review and update of other related policies should be considered when one policy is changed to maintain consistency.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 70 of 134

The organization can determine the formats

and names of these policy documents that meet the organization’s needs. In some organizations, the information security policy and topic-specific policies can be in a single document. The organization can name these topic-specific policies as standards, directives, policies or others.

**SAMPLE AUDIT QUESTIONS**

1. Who has reviewed the Information Security policy?

2. What were the changes made in the policies during the last review?

3. When was the last review conducted?

4. Where is the approval of the information security policy?

5. Why does the review not include business owners?

6. How do you address changed business requirement in the policy?

7. Show me the changes made in the polices based on the changes to the business processes?

| ***Control Ref A.5.2 Information security roles and responsibilities***  ***Control:*** *Information security roles and responsibilities shall be defined and allocated according to the organization needs.*  ***ISO/IEC 27001:2013 Ref: A.6.1.1*** |
| --- |

**PLAIN ENGLISH EXPLANATION**

ISMS implementation is a shared responsibility. The purpose of this set of controls is to ‘use existing resources’ of an organization and adopt a ‘committee’ or a ‘team’ approach. Responsibilities for various processes of ISMS such as Risk Assessment, Internal Audit, MRM, Metrics & Measures, Incident Management are defined and communicated to respective individuals

SAMPLE AUDIT QUESTIONS

1. Check if the above-mentioned roles & responsibilities have been defined (how documented) and evidence of communication

2. Are employees aware who handles ISMS responsibilities?

3. Is there an organization structure where ISMS responsibilities are identified?

| ***Control Ref A.5.3 Segregation of duties***  ***Control:*** *Conflicting duties and conflicting areas of responsibility shall be segregated.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.6.1.2***

**PLAIN ENGLISH EXPLANATION**

Responsibilities should be segregated such that no individual gets complete control. Software development and IT operations should be done by different groups. In small organizations, where segregation is not possible, this may be compensated by a supervisory review. The purpose of this control is to reduce the risk of accidental or deliberate misuse of access to information.

| ***Control Ref A.5.4 Management responsibilities***  ***Control:*** *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.* ***ISO/IEC 27001:2013 Ref: A.7.2.1*** |
| --- |

**PLAIN ENGLISH EXPLANATION**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 71 of 134

Examples of responsibilities includes briefing on:

a) information security roles and responsibilities

b) defining information security goals for the year (Key Result Areas)

c) need to comply with information security policy

d) need to report information security incidents

e) need to maintain technical skills and attend continuing professional education (CPE) meetings

| ***Control Ref A.5.5 Contact with authorities***  ***Control:*** *The organization shall establish and maintain contact with relevant authorities.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.6.1.3***

**PLAIN ENGLISH EXPLANATION**

e.g., Fire Station, utilities, emergency services, electricity suppliers and health and safety, telecommunication providers, water suppliers and regulatory authorities.

Small security incidents are managed within an organization. But security incidents that have a large impact need to be reported to law enforcement, (e.g., police), regulatory bodies (e.g., CERT-In), supervisory authorities (e.g., Head Office if the incident occurs at a branch).

| ***Control Ref A.5.6 Contact with special interest groups***  ***Control:*** *The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.6.1.4***

**PLAIN ENGLISH EXPLANATION**

Organization shall establish contact with professional groups in the field of Information Security & Compliance. There are also opportunities to network with other information security professionals at monthly professional education meetings, other Seminars/Conferences of professional associations such as ISACA, Computer Society, CERT, DSCI, etc.

| ***Control Ref A.5.7 Threat intelligence (NEW)*** |
| --- |

***Control:*** *Information relating to information security threats shall be collected and analysed to produce threat intelligence.*

**PLAIN ENGLISH EXPLANATION**

Information about existing or emerging threats should be collected and analysed in order to a facilitate informed actions to prevent the threats from causing harm to the organization and reduce the impact of such threats. Process for actioning threat advisories (such as CERT) and threat feeds (such as SIEM).

Smaller companies probably do not need any new technology related to this control; rather, they will have to figure out how to extract the threat information from their existing systems. If they do not have one already, larger companies will need to acquire a system that will alert them to new threats (as well as to vulnerabilities and incidents). Companies of any size will have to use threat information to harden their systems.

**Ref: ISO/IEC 27002:2022**

Threat intelligence should be:

a) relevant (i.e. related to the protection of the organization);

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 72 of 134

b) insightful (i.e. providing the organization with an accurate and detailed understanding of the threat landscape);

c) contextual, to provide situational awareness (i.e. adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organizations); d) actionable (i.e. the organization can act on information quickly and effectively).

Threat intelligence activities should include:

a) establishing objectives for threat intelligence production;

b) identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence; c) collecting information from selected sources, which can be internal and external; d) processing information collected to prepare it for analysis (e.g. by translating, formatting or corroborating information);

e) analysing information to understand how it relates and is meaningful to the organization; f) communicating and sharing it to relevant individuals in a format that can be understood.

**Tools & Technologies:**

1. Subscription to threat feeds including CERT-In. Analyse and action based on threat feeds 2. SIEM (Security Incident and Event Management)

| ***Control Ref A.5.8 Information security in project management***  ***Control:*** *Information security shall be integrated into project management.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.6.1.5 & A.14.1.1**

**PLAIN ENGLISH EXPLANATION**

Information security implications should be addressed and reviewed regularly in all the projects. Responsibilities for information security should be defined and allocated to specified roles defined in the project management methods.

**Ref: ISO/IEC 27002:2022**

Information security should be integrated into project management to ensure information security risks are addressed as part of the project management.

The project management in use should require that:

a) information security risks are assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle;

b) information security requirements [e.g. application security requirements (A.8.26), requirements for complying with intellectual property rights (A.5.32), etc.] are addressed in the early stages of projects;

c) information security risks associated with the execution of projects, such as security of internal and external communication aspects are considered and treated throughout the project life cycle; d) progress on information security risk treatment is reviewed and effectiveness of the treatment is evaluated and tested.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 73 of 134

| ***Control Ref A.5.9 Inventory of information and other associated assets***  ***Control:*** *An inventory of information and other associated assets, including owners, shall be developed and maintained.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.8.1.1 & A.8.1.2***

**PLAIN ENGLISH EXPLANATION**

Inventory of assets within the scope of ISMS.

Only 'baseline security controls' for assets outside the scope but owned by the organization. Assets may be listed as a group for each service or project or department.

The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ‘owner’ does not mean that the person actually has property rights to the asset. Owners of each information asset is different from the custodian of the asset

‘Owner’ is normally a single person. In exceptional cases of a shared asset, Information Security committee or a group of persons may be the ‘owner’ of an asset. Owner approves the ‘risk level’ and controls selected for protecting that asset.

| ***Control Ref A.5.10 Acceptable use of information and other associated assets***  ***Control:*** *Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.8.1.3 & A.8.2.3***

**PLAIN ENGLISH EXPLANATION**

Personnel and external party users using or having access to the organization’s information and other associated assets should be made aware of the information security requirements for protecting and handling the organization’s information and other associated assets. They should be responsible for their use of any information processing facilities.

**Ref: ISO/IEC 27002:2022**

Acceptable Use Policy should state

a) expected and unacceptable behaviours of individuals from an information security perspective. b) permitted and prohibited use of information and other associated assets.

c) monitoring activities being performed by the organization.

The following acceptable use procedure should be considered:

a) access restrictions supporting the protection requirements for each level of classification. b) maintenance of a record of the authorized users of information and other associated assets. c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information.

d) storage of assets associated with information in accordance with manufacturers’ specifications (see A.7.8).

e) clear marking of all copies of storage media (electronic or physical) for the attention of the authorized recipient (see A.7.10).

f) authorization of disposal of information and other associated assets and supported deletion method(s) (see A.8.10).

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 74 of 134

| ***Control Ref A.5.11 Return of assets***  ***Control:*** *Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.8.1.4***

**PLAIN ENGLISH EXPLANATION**

The change or termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted by the organization. In cases where personnel and other interested parties purchase the organization’s equipment or use their own personal equipment, procedures should be followed to ensure that all relevant information is traced and transferred to the organization and securely deleted from the equipment. Should be inline with A.6.5 and A.7.14. e.g. access card, laptops

**Ref: ISO/IEC 27002:2022**

The organization should clearly identify and document all information and other associated assets to be returned. Process should be evident of tracking and ensuring return of assets. Applicable where information assets are involved in a contractual agreement. List of information assets could include a) user endpoint devices;

b) portable storage devices;

c) specialist equipment;

d) authentication hardware (e.g. mechanical keys, physical tokens and smartcards) for information systems, sites and physical archives;

e) physical copies of information.

| ***Control Ref A.5.12 Classification of information***  ***Control:*** *Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.8.2.1***

**PLAIN ENGLISH EXPLANATION**

Classification is done to identify the level of sensitive data that is stored, either in a system or as a physical asset. – e.g., Confidential, Public, Internal Use.

**ISO/IEC 27002:2022**

An example of an information confidentiality classification scheme could be based on four levels as follows:

a) disclosure causes no harm;

b) disclosure causes minor reputational damage or minor operational impact;

c) disclosure has a significant short-term impact on operations or business objectives; a) disclosure has a serious impact on long term business objectives or puts the survival of the organization at risk.

| ***Control Ref A.5.13 Labelling of information***  ***Control:*** *An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.* |
| --- |

***ISO/IEC 27001:2013 Ref: A.8.2.2***

**PLAIN ENGLISH EXPLANATION**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 75 of 134

Labelling should reflect the classification scheme established.

The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information, to reduce workloads.

**ISO/IEC 27002:2022**

Examples of labelling techniques include:

a) physical labels;

b) headers and footers;

c) metadata;

d) watermarking;

e) rubber-stamps.

| ***Control Ref A.5.14 Information transfer***  ***Control:*** *Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.13.2.1 & A.13.2.2 & A.13.2.3**

**PLAIN ENGLISH EXPLANATION**

Policies and procedures should be defined on controls to be put in place before information could be transferred to third parties. NDA should be signed with third parties before transferring information to third parties. Security in file transfer, email and any other electronic messaging such as chat applications used should be defined

| ***Control Ref A.5.15 Access control***  ***Control:*** *Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.9.1.1 & A.9.1.2**

**PLAIN ENGLISH EXPLANATION**

Owners of information and other associated assets should determine information security and business requirements related to access control. A topic-specific policy on access control should be defined which takes account of requirements (like asset access, privileged access, management of access rights, etc.) and should be communicated to all relevant interested parties.

**Ref: ISO/IEC 27002:2022**

The following should be taken into account when defining and implementing access control rules: a) consistency between the access rights and information classification;

b) consistency between the access rights and the physical perimeter security needs and requirements; c) considering all types of available connections in distributed environments so entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use;

d) considering how elements or factors relevant to dynamic access control can be reflected.

Two of the most frequently used principles are:

a) need-to-know: an entity is only granted access to the information which that entity requires in order to perform its tasks (different tasks or roles mean different need-to-know information and hence different access profiles);

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 76 of 134

b) need-to-use: an entity is only assigned access to information technology infrastructure where a clear need is present.

| ***Control Ref A.5.16 Identity management***  ***Control:*** *The full life cycle of identities shall be managed.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.9.2.1**

**PLAIN ENGLISH EXPLANATION**

Organisation should allocate unique identification of individuals. This includes systems used to access the organization’s information and other associated assets and to enable appropriate assignment of access rights (see A.5.18).

**Ref: ISO/IEC 27002:2022**

The processes used in the context of identity management should ensure that:

a) for identities assigned to persons, a specific identity is only linked to a single person to be able to hold the person accountable for actions performed with this specific identity;

b) identities assigned to multiple persons (e.g. shared identities) are only permitted where they are necessary for business or operational reasons and are subject to dedicated approval and documentation;

c) identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight;

d) identities are disabled or removed in a timely fashion if they are no longer required (e.g. if their associated entities are deleted or no longer used, or if the person linked to an identity has left the organization or changed the role);

e) in a specific domain, a single identity is mapped to a single entity, [i.e. mapping of multiple identities to the same entity within the same context (duplicate identities) is avoided]; f) records of all significant events concerning the use and management of user identities and of authentication information are kept.

| ***Control Ref A.5.17 Authentication information***  ***Control:*** *Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.9.2.4, A.9.3.1 & A.9.4.3**

**PLAIN ENGLISH EXPLANATION**

Authentication information such as passwords, PINs, OTPs, and other forms of secret authentication information are configured and implemented for all personnel

Passwords are a commonly used type of secret authentication information and are a common means of verifying a user’s identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes

**Ref: ISO/IEC 27002:2022**

When passwords are used as authentication information, the password management system should: a) allow users to select and change their own passwords and include a confirmation procedure to address input errors;

b) enforce strong passwords according to good practice recommendations;

c) force users to change their passwords at first login;

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 77 of 134

d) enforce password changes as necessary, for example after a security incident, or upon termination or change of employment when a user has known passwords for identities that remain active (e.g. shared identities);

e) prevent re-use of previous passwords;

e) prevent the use of commonly-used passwords and compromised usernames, password combinations from hacked systems;

f) not to display passwords on the screen when being entered;

g) store and transmit passwords in protected form.

| ***Control Ref A.5.18 Access rights***  ***Control:*** *Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.9.2.2, A.9.2.5 & A.9.2.6**

**PLAIN ENGLISH EXPLANATION**

• Logical access (IDs and Passwords) to applications and AD should be based on approval and documented process. Changes to access should be communicated through appropriate channels and should be granted as per business requirement (like emails).

• Logical access (IDs and Passwords) to be reviewed and confirmed if they are as per current requirement and action taken if discrepancy identified. This should be done on a predefined frequency. Individuals managing logical access (IDs and Passwords) should take a report of the current status and reconcile and verify the same with the process owners.

• Logical access (IDs and Passwords) to applications and AD should be removed when not required such as termination, change of responsibility internally.

• Verify that the level of access granted is in accordance with the topic-specific policies on access control (see 5.15) and is consistent with other information security requirements such as segregation of duties (see 5.3);

| ***Control Ref A.5.19 Information security in supplier relationships***  ***Control:*** *Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.15.1.1**

**PLAIN ENGLISH EXPLANATION**

The organization should identify and implement processes and procedures to address security risks associated with the use of products and services provided by suppliers. This should also apply to the organization’s use of resources of cloud service providers.

**Ref: ISO/IEC 27002:2022**

These processes and procedures should include those to be implemented by the organization, as well as those the organization requires the supplier to implement for the commencement of use of a supplier’s products or services or for the termination of use of a supplier’s products and services, such as:

a) identifying and documenting the types of suppliers (e.g. ICT services, logistics, utilities, financial services, ICT infrastructure components) which can affect the confidentiality, integrity and availability of the organization's information;

b) establishing how to evaluate and select suppliers according to the sensitivity of information, products and services (e.g. with market analysis, customer references, review of documents, onsite assessments, certifications);

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 78 of 134

c) evaluating and selecting supplier’s products or services that have adequate information security controls and reviewing them; in particular, accuracy and completeness of controls implemented by the supplier that ensure integrity of the supplier’s information and information processing and hence the organization’s information security;

d) defining the organization’s information, ICT services and the physical infrastructure that suppliers can access, monitor, control or use;

e) defining the types of ICT infrastructure components and services provided by suppliers which can affect the confidentiality, integrity and availability of the organization's information; f) assessing and managing the information security risks associated with:

1) the suppliers’ use of the organization’s information and other associated assets, including risks originating from potential malicious supplier personnel;

2) malfunctioning or vulnerabilities of the products (including software components and subcomponents used in these products) or services provided by the suppliers;

g) monitoring compliance with established information security requirements for each type of supplier and type of access, including third-party review and product validation;

h) mitigating non-compliance of a supplier, whether this was detected through monitoring or by other means;

i) handling incidents and contingencies associated with supplier products and services including responsibilities of both the organization and suppliers;

j) resilience and, if necessary, recovery and contingency measures to ensure the availability of the supplier’s information and information processing and hence the availability of the organization’s information;

k) awareness and training for the organization’s personnel interacting with supplier personnel regarding appropriate rules of engagement, topic-specific policies, processes and procedures and behaviour based on the type of supplier and the level of supplier access to the organization’s systems and information;

l) managing the necessary transfer of information, other associated assets and anything else that needs to be changed and ensuring that information security is maintained throughout the transfer period; m) requirements to ensure a secure termination of the supplier relationship, including: 1) de-provisioning of access rights;

2) information handling;

3) determining ownership of intellectual property developed during the engagement; 4) information portability in case of change of supplier or insourcing;

5) records management;

6) return of assets;

7) secure disposal of information and other associated assets;

8) ongoing confidentiality requirements;

n) level of personnel security and physical security expected from supplier's personnel and facilities.

| ***Control Ref A.5.20 Addressing information security within supplier agreements Control:*** *Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.* |
| --- |

***ISO/IEC 27001:2013 Ref:* A.15.1.2**

**PLAIN ENGLISH EXPLANATION**

Supplier agreements should be established and documented to ensure that there is clear understanding between the organization and the supplier regarding both parties’ obligations to fulfil relevant information security requirements. To simply put it. 3rd party NDAs should be evident.

**Ref: ISO/IEC 27002:2022**

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 79 of 134

The following terms can be considered for inclusion in the agreements to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information.

b) classification of information according to the organization’s classification scheme (see A.5.10, A.5.12, A.5.13).

c) mapping between the organization’s own classification scheme and the classification scheme of the supplier.

d) legal, statutory, regulatory and contractual requirements, including data protection, handling of personally identifiable information (PII), intellectual property rights and copyright and a description of how it will be ensured that they are met;

e) obligation of each contractual party to implement an agreed set of controls, including access control, performance review, monitoring, reporting, and auditing, and the supplier’s obligations to comply with the organization’s information security requirements.

f) rules of acceptable use of information and other associated assets, including unacceptable use if necessary.

g) procedures or conditions for authorization and removal of the authorization for the use of the organization’s information and other associated assets by supplier personnel (e.g., through an explicit list of supplier personnel authorized to use the organization’s information and other associated assets);

h) information security requirements regarding the supplier’s ICT infrastructure; in particular, minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization’s business needs and risk criteria.

i) indemnities and remediation for failure of contractor to meet requirements.

j) incident management requirements and procedures (especially notification and collaboration during incident remediation).

k) training and awareness requirements for specific procedures and information security requirements (e.g., for incident response, authorization procedures).

l) relevant provisions for sub-contracting, including the controls that need to be implemented, such as agreement on the use of sub-suppliers (e.g., requiring to have them under the same obligations of the supplier, requiring to have a list of sub-suppliers and notification before any change). m) relevant contacts, including a contact person for information security issues.

n) any screening requirements, where legally permissible, for the supplier’s personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern.

o) the evidence and assurance mechanisms of third-party attestations for relevant information security requirements related to the supplier processes and an independent report on effectiveness of controls.

p) right to audit the supplier processes and controls related to the agreement.

q) supplier’s obligation to periodically deliver a report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report.

r) defect resolution and conflict resolution processes.

s) providing backup aligned with the organization’s needs (in terms of frequency and type and storage location).

t) ensuring the availability of an alternate facility (i.e., disaster recovery site) not subject to the same threats as the primary facility and considerations for fall back controls (alternate controls) in the event primary controls fail.

u) having a change management process that ensures advance notification to the organization and the possibility for the organization of not accepting changes.

v) physical security controls commensurate with the information classification.

CPG - Exemplar Global IS Iss 3 Rev 0 Nov 2022 Page 80 of 134