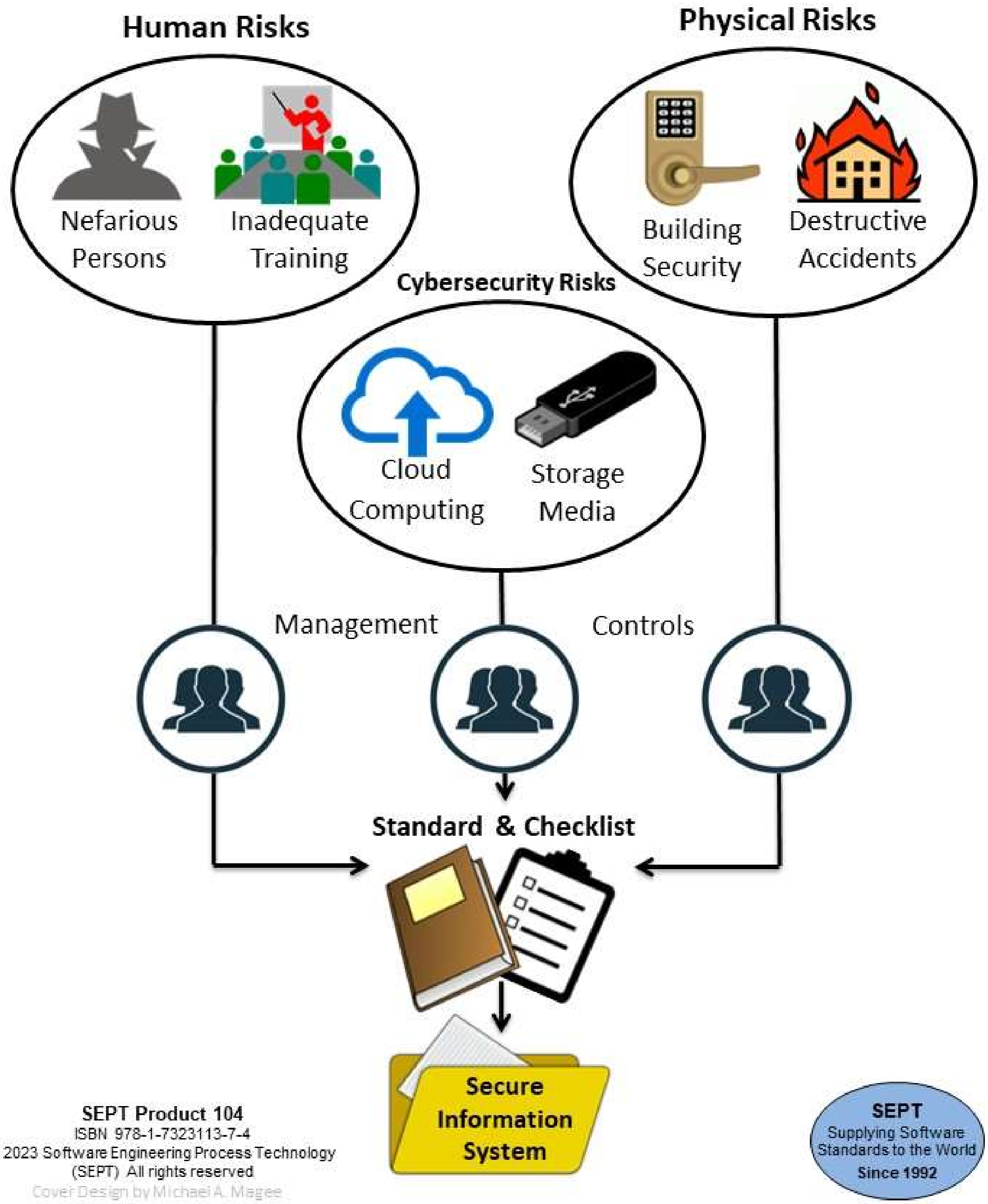
Checklist for Standard ISO/IEC 27001:2022

Information security, cybersecurity, and privacy protection – Information security management systems – Requirements



SEPT Product 104
ISBN 978-1-7323113-7-4

Cover Design by Michael A. Magee

SEPT
Supplying Software Standards to the World
Since 1992

Checklist for Standard ISO/IEC 27001:2022

Information Security, Cybersecurity And Privacy Protection - Information Security Management Systems - Requirements

SEPT Product 104

ISBN 978-1-7323113-7-4

Authors: **Andy Coster CQI (Ret.) and Stan Magee CCP (Ret.)**

Produced by Software Engineering Process Technology (SEPT)
1705 16th Lane NE Suite P203
Issaquah WA 98029
Tel. 425-391-2344
E-mail: stanmagee@smartwire.net
Web Site: www.12207.com

Change Page History

Date	Change	Reason
9 Feb 2017	First Version	To produce compatible pair with ISO/IEC 27002 checklist.
30 Jan 2023	Second version	This edition of the SEPT checklist incorporates changes in the Standard ISO/IEC 27001:2022.

Contents of the Checklist

This checklist is composed of 10 sections:

Checklist For Standard ISO/IEC 27001:2022 - Information Security, Cybersecurity And Privacy Protection - Information Security Management Systems - Requirements

SEPT Product 104

Introduction

Purpose of this checklist

This Software Engineering Process Technology (SEPT) checklist list gives an organization the confidence that it has all the artifacts required, recommended, or suggested (as identified by SEPT) by the ISO/IEC 27001:2022 standard. This checklist defines an artifact in terms of policies, procedures, plans, records, documents, audits, and reviews.

For 20 + years SEPT has produced checklists for organizations that require the highest proof that they have all the artefacts required to meet the requirements of a particular standard like ISO/IEC 27001:2022 (which has 371 identified artefacts).
An average SEPT checklist requires over 500 manhours to construct and verify that it is accurate, and no nuance of a standard has been overlooked. SEPT senior staff have many years' experience in developing world class software engineering process standards and checklists. Every step of a checklist in its construction has been verified.
This checklist will ensure that your organization will have the proof (artefacts) to demonstrate to any public body that the organization has met the requirements of ISO/IEC 27001:2022.

Overview of the base standard

ISO/IEC 27001:2022 provides requirements for organizational information security management system and information security management controls; taking into consideration the organization's information security risk environment(s).
It is designed to be used by organizations that intend to:

1. seek certification to ISO/IEC 27001:2022,
2. select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001:2022,
3. implement commonly accepted information security controls,
4. develop their own information security management system.

The requirements included in the ISO/IEC 27001:2022 standard are listed at a high level of detail, with an Annexed reference to ISO/IEC 27002:2022 as appropriate guidance to demonstrate compliance with ISO/IEC 27001:2022. If an organization is interested in testing their compliance with ISO/IEC 27001:2022 this checklist will provide an analysis of the detail in the ISO/IEC 27001 standard. However, if the organization is only interested in the guidance in ISO/IEC 27002:2022 this checklist provides a list of all items required in Annex A of ISO/IEC 27001 that are derived from the ISO/IEC 27002 guidelines. They are described in the Introduction to the checklist and in section 9.

How the SEPT checklist was developed and steps for using the checklist

The SEPT checklists state, in a clear and concise manner, what is required in the form of artefacts to satisfy the standard. These artifacts called out in this checklist, if properly constructed should satisfy any review body that the organization has satisfied the requirements of ISO/IEC 27001:2022.

The artefacts are constructed around a classification scheme of physical evidence comprised of policies, procedures, plans, records, documents, audits, and reviews. There must be an accompanying record of some type when an audit or review has been accomplished. This record would define the findings of the review or audit and any corrective action to be taken. For the sake of brevity this checklist does not call out a separate record for each review or audit. All procedures should be reviewed but the checklist does not call out a review for each procedure, unless the standard calls out the procedure review. In this checklist, “manuals, reports, scripts and specifications” are included in the document category. In the procedure category guidelines are included when the standard references another standard for physical evidence. The checklist does not call out the requirements of the referenced standard.

The SEPT Engineering Department have carefully reviewed the Standard “ISO/IEC 27001:2022 - Information security management systems – Requirements" and defined the physical evidence required based upon this classification scheme. Then the Engineering Department has conducted a second review of the complete list to ensure that the documents’ producers did not leave out a physical piece of evidence that a “reasonable person” would expect to find. It could certainly be argued that if the document did not call it out then it is not required; however, if the standard was used by an organization to improve its process, then it would make sense to recognize missing documents.

In ISO/IEC 27001:2022 many requirements are not specific about the type of artefact that would be needed to satisfy it. SEPT have therefore used the following codification rules:

1. If the requirement clearly asks for a Procedure, Plan, Document, Record (Documented information), Audit or Review we have made these "Required" items with no appended asterisks.

2. If the requirement is unclear about the type of artefact that would demonstrate compliance, then we have "Recommended" one and shown it with 2 asterisks (**) appended. An organization may decide not to follow this recommendation if they satisfy the requirement in a different and visible way.
3. If there is a suggestion to do something - "should" rather than "shall" we have "Suggested" an appropriate artefact and shown our suggestion with 1 asterisk (*) appended
4. Sometimes we will add additional "Suggested" artefacts as good practice. Again these are shown with 1 asterisk (*) appended.

If a document is called out more than one time, only the first reference is stipulated.

There are situations in which a procedure or document is not necessarily separate and could be contained within another document. For example, the "ISMS Risks and Opportunities Action Integration and Implementation Plan" could be a part of the "ISMS Risks and Opportunities Action Plan." The authors have called out these individual items separately to ensure that the organization does not overlook any facet of physical evidence. If the organization does not require a separate document, and an item can be a subset of another document or record, then this fact should be denoted in the detail section of the checklist for that item. This should be done in the form of a statement reflecting that the information for this document may be found in section XX of Document XYZ. If the organizational requirements do not call for this physical evidence for a particular project, this should also be denoted with a statement reflecting that this physical evidence is not required and why. The reasons for the evidence not being required should be clearly presented in this statement. Further details on this step are provided in the Detail Steps section of the introduction. The size of these documents could vary from paragraphs to volumes depending upon the size and complexity of the project or business requirements.

Clause 6.1.3 of ISO/IEC 27001:2022 requires that an organization determines all controls necessary to implement the information security risk treatment options based on the information security risk assessment results. A Statement of Applicability of controls based on those listed in Annex A of the standard is also required.
Control objectives and controls are listed in Annex A of ISO/IEC 27001:2022 based on the layout and artefacts needed to satisfy ISO/IEC 27002:2022, specifically related to controls. ISO/IEC 27002:2022 itself provides much more detail than ISO/IEC 27001:2022 about items needed to demonstrate best information security practices.
To satisfy Clause 6.1.3 of ISO/IEC 27001:2022 SEPT have included in Section 9 a sub set of items identified in the full ISO/IEC 27002:2022 Information security practices standard that are detailed in the related SEPT checklist (for ISO/IEC 27002:2022). These are listed by Clause of ISO/IEC 27002. For a fuller treatment of information security practice guidelines see ISO/IEC 27002:2022 and the related SEPT checklist for this standard. Mostly, buyers of the ISO/IEC 27001 checklist also buy the ISO/IEC 27002 checklist to complement the 27001 checklist to ensure that they have a full insight for defining or evaluating a Security Management System.

General Principles of the Checklist for ISO/IEC Standard 27001:2022

This checklist was prepared by analyzing each clause of this document for the key words that signify a:

- Policy
- Procedure (Including Guidelines)
- Plan
- Records
- Document (Including Manuals, Reports, Scripts and Specifications)
- Audit
- Review

This checklist specifies evidence that is unique. After reviewing the completed document, the second review was conducted from a common sense “reasonable person” approach. If a document or other piece of evidence appeared to be required, but was not called out in the document as required, then it is added with two asterisks as ”recommended”(**) or one asterisk as “suggested”(*) after its notation in the checklist. The information was transferred into checklist tables based on the type of product or evidence.

Beginning with those defined in Clause 4.0 (Context of the organization) of the standard there are 70 required artefacts, 85 recommended and 94 suggested artefacts included in the SEPT checklist in section 2, Additionally Section 9 introduces another 122 artefacts based on the companion Sept checklist for ISO/IEC 27002:2022 that need to be considered to satisfy Clause 6.1.3 of ISO/IEC 27001:2022. This makes a maximum of 371 artefacts to be considered of which 70 +up to 122 need consideration.

Using the Checklist

When a company is planning to use ISO/IEC 27001:2022 standard, the company should review the evidence checklist. If the company’s present process does not address an ISO/IEC 27001:2022 standard product, then the following question should be asked: “Is the evidence product required for the type of business conducted by the organization?” If, in the view of the organization, the evidence is not required, the rationale should be documented and inserted in the checklist and quality manual. This rationale should pass the “*reasonable person*” rule, as described above. If the evidence is required, plans should be prepared to address the missing item(s).

Detail Steps

An organization should compare the proposed output of their organization against the checklist. In doing this, they will find one of five conditions that exist for each item listed in the checklist. The following five conditions and the actions required by these conditions are listed in the table below.

Condition	Action Required
1. The title of the documented evidence specified by the checklist (document, plan, etc.) *agrees* with the title of the evidence being planned by the organization.	Record in checklist that the organization is compliant.
2. The title of the documented evidence specified by the checklist (document, etc.) *disagrees* with the title of the evidence planned by the organization but the content is the same.	Record in the checklist the evidence title the organization uses and record that the organization is compliant, and the evidence is the same although the title is different.
3. The title of the documented evidence specified by the checklist (document, etc.) is *combined* with another piece of evidence.	Record in the checklist the title of the evidence (document, etc.) in which this information is contained.
4. The title of the documented evidence specified by the checklist (document, etc.) *is not planned* by the organization because it is not required.	Record in the checklist that the evidence is not required and the rationale for this decision.
5. The title of the documented evidence called out by the checklis*t* (document, etc.*) is not planned* by the organization and *should be* planned by it.	Record in the checklist when this evidence will be planned and reference a plan for accomplishing the task.

Product Support
All reasonable questions concerning this checklist, or its use will be addressed by SEPT free of charge for 60 days from time of purchase, up to a maximum of 4 hours consultation time.

Guarantees and Liability
Software Engineering Process Technology (SEPT) makes no guarantees implied or stated with respect to this checklist, and it is provided on an "*as is*" basis. SEPT will have no liability for any indirect, incidental, special or consequential damages or any loss of revenue or profits arising under, or with respect to the use of this document.

Section 2
ISO/IEC 27001:2022 Evidence Products Checklist by Clause

ISO/IEC 27001:2022 Clause Number and Name	**Policies** and Procedures	Plans	Records	Documents	**Audits** and Reviews
4 Context of the organization					
4.1 Understanding the Organization and its context	• Information Security Management System (ISMS) External and Internal Issues Determination Plan Procedure* • ISMS External and Internal Issues Determination Document Procedure*	• Information Security Management System (ISMS) External and Internal Issues Determination Plan*		• ISMS External and Internal Issues Determination Document*	• Information Security Management System (ISMS) External and Internal Issues Determination Plan Review* • ISMS External and Internal Issues Determination Document Review*

Section 2
ISO/IEC 27001:2022 Evidence Products Checklist by Clause

ISO/IEC 27001:2022 Clause Number and Name	**Policies** and Procedures	Plans	Records	Documents	**Audits** and Reviews
4.2 Understanding the needs and expectations of interested parties	• ISMS Interested Parties Determination Procedure** • ISMS Interested Parties Requirements Document Plan Procedure* • ISMS Interested Parties Requirements Document Procedure* • ISMS Legal and Regulatory Requirements and Contractual Obligations Document Procedure* • ISMS Requirements for Implementation Plan Procedure*	• ISMS Interested Parties Requirements Document Plan* • ISMS Requirements for Implementation Plan**		• ISMS Interested Parties Requirements Document** • ISMS Legal and Regulatory Requirements and Contractual Obligations Document**	• ISMS Interested Parties Requirements Document Plan Review* • ISMS Interested Parties Requirements Document Review* • ISMS Legal and Regulatory Requirements and Contractual Obligations Document Review* • ISMS Requirements for Implementation Plan Review*

Section 2
ISO/IEC 27001:2022 Evidence Products Checklist by Clause

ISO/IEC 27001:2022 Clause Number and Name	**Policies** and Procedures	Plans	Records	Documents	**Audits** and Reviews
4.3 Determining the scope of the information security management system	• ISMS Boundaries and Applicability Determination Procedure** • ISMS Improvement Plan Procedure • ISMS Scope Document Procedure*	• ISMS Improvement Plan**		• ISMS Scope Document	• ISMS Scope Document Review* • ISMS Improvement Plan Review*
4.4 Information security Management system	• ISMS Processes and Process Interaction Procedure • Organization Establishment and Implementation of ISMS Procedures • Organization Maintenance and Continual Improvement of the ISMS Procedures				
5 Leadership					