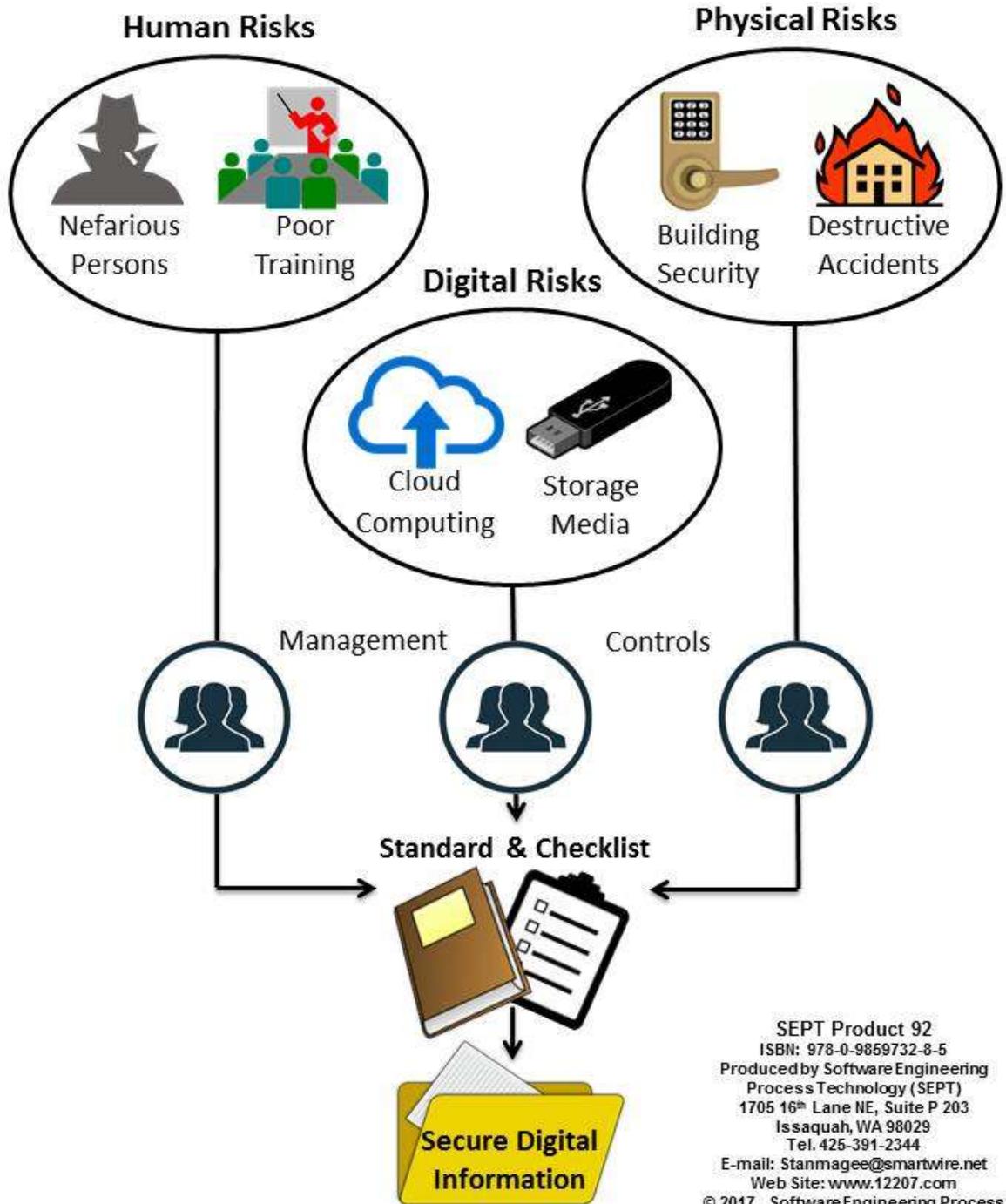


Checklist for Standard ISO/IEC 27001:2013 Information Security Requirements



Cover Design by Michael A. Magee

SEPT Product 92
ISBN: 978-0-9859732-8-5
Produced by Software Engineering
Process Technology (SEPT)
1705 16th Lane NE, Suite P 203
Issaquah, WA 98029
Tel. 425-391-2344
E-mail: Stanmagee@smartwire.net
Web Site: www.12207.com
© 2017. Software Engineering Process
Technology (SEPT) All rights reserved.

Checklist for Standard ISO/IEC 27001:2013 - Information Security Requirements SEPT Product 92

ISBN 978-0-9859732-8-5

Authors: **Andy Coster CQI 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

© 2017. Software Engineering Process Technology (SEPT) All rights reserved.

Change Page History

Date	Change	Reason
9 Feb 2017	First Version	To produce compatible pair with ISO/IEC 27002 checklist.

Sample

Checklist for Standard ISO/IEC 27001:2013 - Information Security Requirements SEPT Product 92

Purpose of this checklist

This SEPT checklist list, if used properly, will give an organization the confidence that it has all the documentation required by the ISO/IEC 27001:2013 standard.

This checklist is a tool to ease the pain in becoming certified to ISO/IEC 27001:2013 by clearly defining the artefacts required, whether your organization is upgrading to the new version or addressing certification to ISO/IEC 27001:2013 for the first time.

Components of the Checklist

This checklist is composed of 10 sections:

- Section 1. Introduction
- Section 2. Composites of all required and suggested “ISO/IEC 27001:2013” artefacts.
- Sections 3-8. Individual checklists for each evidence type.
- Section 9. Additional controls that may be required for an organization (by ISO/IEC 27001:2013 Annex A)
- Section 10. “About the Author(s)”

Overview of the base standard

ISO/IEC 27001:2013 provides requirements for organizational information security standards and information security management practices including the selection, implementation, and management of controls; taking into consideration the organization's information security risk environment(s).

It is designed to be used by organizations that intend to:

1. select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
2. implement commonly accepted information security controls;
3. develop their own information security management practices

The requirements included in the ISO/IEC 27001:2013 standard are listed at a high level of detail, with an Annexed reference to ISO 27002:2013 as appropriate guidance to demonstrate compliance with ISO/IEC 27001:2013. If an Organization is interested in testing their compliance with ISO/IEC 27001:2013 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 27002:2013 this checklist provides a list of all items suggested in Annex A of ISO/IEC 27001 that are derived from the ISO/IEC 27002 guidelines. They are addressed in detail in the Introduction to the checklist and in section 9.

Introduction to the SEPT checklist for implementing this standard

For 20 + years Software Engineering Process Technology (SEPT) has produced checklists for standards that address software issues. This is a checklist for a software related standard in the IT industry that will aid an organization's compliance with an international information security code of practice.

The task of getting information security under control is daunting. The last thing an organization wants in its security management operation is to call in a Notified Body for certification and to find out that the organization is lacking the correct records or documents for the auditor to examine.

The first step that an organization has in meeting the guidance of an information security management standard such as Standard ISO/IEC 27001:2013 is to determine what is required and what is suggested. Often these systems and technical standards are confusing and laborious because the directions contained in the standards are unclear to a lay person. In order to reduce this fog surrounding these types of standards SEPT has been producing checklists for standards since 1994. The checklists lift this fog around a standard and state what is required and suggested by the standard in a clear and concise manner. To aid in determining what is actually "required" by the document in the way of physical evidence of compliance, the experts at SEPT have produced this checklist. The SEPT checklists 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 authors have carefully reviewed the Standard "ISO/IEC 27001:2013 Information technology – Security techniques – Requirements" and defined the physical evidence required based upon this classification scheme. SEPT's 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. Therefore, there are documents specified in this checklist that are implied by the standard, though not specifically called out by it, and they are designated by an asterisk (*) throughout this checklist. If a document is called out more than one time, only the first reference is stipulated.

There are occasional 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 27001:2013 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 27001:2013 based on the layout and artefacts needed to satisfy ISO/IEC 27002:2013, specifically related to controls. ISO/IEC 27002:2013 itself provides much more detail than ISO/IEC 27001:2013 about items needed to demonstrate best information security practices. To satisfy Clause 6.1.3 of ISO/IEC 27001:2013 SEPT have included in Section 9 a subset of items identified in the full ISO/IEC 27002:2013 Information security practices standard that are detailed in the related SEPT checklist (for ISO/IEC 27002:2013). These are listed by Clause of ISO/IEC 27002. For a fuller treatment of information security practice guidelines see ISO/IEC 27002:2013 and the related SEPT checklist for this standard.

General Principles of the Checklist for ISO/IEC Standard 27001:2013

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 an asterisk (*) 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 45 required artefacts and 189 suggested artefacts included in the SEPT checklist in section 2, Additionally Section 9 introduces another 145 artefacts based on the companion Sept checklist for ISO/IEC 27002:2013 that need to be considered to satisfy Clause 6.1.3 of ISO/IEC 27001:2013.

Using the Checklist

When a company is planning to use ISO/IEC 27001:2013 standard, the company should review the evidence checklist. If the company’s present process does not address an ISO/IEC 27001:2013 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.) <i>agrees</i> 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.) <i>disagrees</i> 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 <i>combined</i> 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 <i>not planned</i> 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	Record in the checklist when this

called out by the checklist (document, etc.) <i>is not planned</i> by the organization and <i>should be</i> planned by it.	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 27001:2013 Evidence Products Checklist by Clause

ISO /IEC 27001:2013 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	<ul style="list-style-type: none"> • Information Security Management System (ISMS) External and Internal Issues Determination Plan Procedure* • ISMS External and Internal Issues Determination Document Procedure* 	<ul style="list-style-type: none"> • Information Security Management System (ISMS) External and Internal Issues Determination Plan* 		<ul style="list-style-type: none"> • ISMS External and Internal Issues Determination Document* 	<ul style="list-style-type: none"> • Information Security Management System (ISMS) External and Internal Issues Determination Plan Review* • ISMS External and Internal Issues Determination Document Review*

Section 2
ISO/IEC 27001:2013 Evidence Products Checklist by Clause

ISO /IEC 27001:2013 Clause Number and Name	Policies and Procedures	Plans	Records	Documents	Audits and Reviews
4.2 Understanding the needs and expectations of interested parties	<ul style="list-style-type: none"> • 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* 	<ul style="list-style-type: none"> • ISMS Interested Parties Requirements Document Plan* 		<ul style="list-style-type: none"> • ISMS Interested Parties Requirements Document* • ISMS Legal and Regulatory Requirements and Contractual Obligations Document* 	<ul style="list-style-type: none"> • ISMS Interested Parties Requirements Document Plan Review* • ISMS Interested Parties Requirements Document Review* • ISMS Legal and Regulatory Requirements and Contractual Obligations Document Review*

Section 2
ISO/IEC 27001:2013 Evidence Products Checklist by Clause

ISO /IEC 27001:2013 Clause Number and Name	Policies and Procedures	Plans	Records	Documents	Audits and Reviews
4.3 Determining the scope of the information security management system	<ul style="list-style-type: none"> • ISMS Boundaries and Applicability Determination Procedure • ISMS Improvement Plan Procedure • ISMS Scope Document Procedure* 			<ul style="list-style-type: none"> • ISMS Scope Document 	<ul style="list-style-type: none"> • ISMS Scope Document Review*
4.4 Information security Management system	<ul style="list-style-type: none"> • Organization Establishment and Implementation of ISMS Procedures • Organization Maintenance and Continual Improvement of the ISMS Procedures 				
5 Leadership					