

EVIDENCE PRODUCT CHECKLIST
For Standard ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management*
(Revision 1 to incorporate Technical Corrigendum 1)



ISBN 0-9770309-5-4



Standard



Checklist



Security

SEPT Product 44

Produced by Software Engineering Process Technology (SEPT)
2726 NW Pine Cone Drive
Issaquah, WA, 98027
Tel. 425-391-2344

E-mail: Stanmag33@smartwfr.net
Web Site: www.12207.com

© 2008, Software Engineering Process Technology (SEPT) All rights reserved.

Evidence Product Checklist
for Standard ISO/IEC 27002:2005
Information technology – Security
techniques -- Code of practice for
information security management
(Revision 1 to incorporate Technical Corrigendum 1)

ISBN 0-9770309-5-4

SEPT Product 44

**Evidence Product Checklist
for Standard ISO/IEC 27002:2005
*Information technology – Security
techniques -- Code of practice for
information security management***

(Revision 1 to incorporate Technical Corrigendum 1)

ISBN 0-9770309-5-4

Authors: Maynard Hanscom CISSP, George Jackelen PMP and Stan Magee CCP

SEPT Product 44

Produced by Software Engineering Process Technology (SEPT)

2725 NW Pine Cone Drive

Issaquah, WA. 98027

Tel. 425-391-2344

E-mail: stanmagee@smartwire.net

Web Site: www.12207.com

© 2006. Software Engineering Process Technology (SEPT) All rights reserved.

Change Page History

Date	Change	Reason
1/3/2008	Incorporate Technical Corrigendum 1	Number change, throughout the document 17799 has been replaced with 27002.

Sample

ISO/IEC 27002:2005 — Security techniques -- Code of practice for information security management

Evidence Product Checklist

Introduction

The process of defining what is necessary for compliance with a standard such as “ISO/IEC 27002:2005 for security management of information and related assets is often confusing and laborious because the directions contained in the standards are unclear or ambiguous. To aid in determining what is actually “recommended” by the document in the way of physical evidence of compliance, the experts at SEPT have produced this checklist. This checklist is 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 policies, procedures and records should be reviewed but the checklist does not call out a review for each item unless the standard calls out the review. In this checklist “manuals, reports, scripts and specifications” are included in the document category.

The Authors have carefully reviewed the document “ISO/IEC 27002:2005 Information technology – Security techniques -- Code of practice for information security management” and defined the physical evidence recommended based upon this classification scheme. SEPT 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 recommended; however if the document 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 in the document, and they are designated by an asterisk (*) throughout this checklist. These items are classified as suggested. 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 or procedure. For example, the “Equipment Siting and Protection Procedure” could be a part of the “Equipment Security Procedure”. 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 recommended and why. The reasons for the evidence not being recommended 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.

“ISO/IEC 27002:2005 Information technology – Security techniques -- Code of practice for information security management” Checklist

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

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

This checklist specifies evidence that is unique and industry best practices. 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 recommended, but was not called out in the document, 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. Recommended items do not have an asterisk (*) after its notation in the checklist.

Using the Checklist

When a company is planning to use the “ISO/IEC 27002:2005 Information technology – Security techniques -- Code of practice for information security management”, the company should review the evidence checklist. If the company’s present process does not address an ISO/IEC 27002:2005 product, then this question should be asked: Is the evidence product recommended for the type of business of the company? If in the view of the company the evidence is not recommended, the rationale should be documented and inserted in the checklist and quality control manual. This rationale should pass “*the reasonable person rule.*” If the evidence is recommended, 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 (Procedure, Plan, Records, Document (Including Manuals, Reports, Scripts and Specifications), Audit and Review) <i>agrees</i> with the title of the evidence being planned by the organization.	Record in the 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 titles of the evidence (document, etc) in which this information is contained.
4 The title of the documented evidence specified by the checklist (document, etc) <i>is 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 called out by the checklist (document, etc) <i>is not planned</i> by the organization and <i>should be planned</i> by it.	Record in the checklist when this evidence will be planned and reference a plan for accomplishing the task.

Components of the Checklist

This checklist is composed of 9 sections:

- Section 1. Introduction
- Section 2. Composites of all recommended and suggested “ISO/IEC 27002:2005 Information technology – Security techniques -- Code of practice for information security management” evidence products.
- Sections 3-8. Individual checklists for each evidence type.
- Section 9. “About the Authors”

Product Support

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

Warranties and Liability

Software Engineering Process Technology (SEPT) makes no warranties 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.

Sample

Section 2
ISO/IEC 27002:2005 Evidence Products Checklist By Clause

ISO/IEC 27002:2005 Clause Number and Name	Policies and Procedures	Plans	Records	Documents	Audits and Reviews
4.0 Risk assessment and treatment					
4.1 Assessing security risks	<ul style="list-style-type: none"> • Risk Assessment Results Document Procedure* 			<ul style="list-style-type: none"> • Risk Assessment Results Document 	<ul style="list-style-type: none"> • Risk Assessment Results Document Review*
4.2 Treating security risks					
5.0 Security policy					
5.1 Information security policy					
5.1.1 Information security policy document	<ul style="list-style-type: none"> • Information Security Document Procedure* • Information Security Policy • Information Security Policy Document Procedure* • Information Security Policy Procedure* 			<ul style="list-style-type: none"> • Information Security Document • Information Security Policy Document 	<ul style="list-style-type: none"> • Information Security Document Review • Information Security Policy Document Review • Information Security Policy Review
5.1.2 Review of the information security policy					

Section 2
ISO/IEC 27002:2005 Evidence Products Checklist By Clause

ISO/IEC 27002:2005 Clause Number and Name	Policies and Procedures	Plans	Records	Documents	Audits and Reviews
6.0 Organization of information security					
6.1 Internal Organization	<ul style="list-style-type: none"> Information Security Infrastructure Document Procedure* 		<ul style="list-style-type: none"> Information Security Specialist Adviser Records 	<ul style="list-style-type: none"> Information Security Infrastructure Document* 	<ul style="list-style-type: none"> Information Security Infrastructure Document Review*
6.1.1 Management commitment to informational security	<ul style="list-style-type: none"> Information Security Goals Document Procedure* Security Awareness Plan Procedure* User Security Training Procedure* 	<ul style="list-style-type: none"> Security Awareness Plan 		<ul style="list-style-type: none"> Information Security Goals Document 	<ul style="list-style-type: none"> Information Security Goals Document Review* Security Awareness Plan Review User Security Training Procedure Review*
6.1.2 Information security co-ordination					

Section 2
ISO/IEC 27002:2005 Evidence Products Checklist By Clause

ISO/IEC 27002:2005 Clause Number and Name	Policies and Procedures	Plans	Records	Documents	Audits and Reviews
6.1.3 Allocation of information security responsibilities	<ul style="list-style-type: none"> • Asset Responsibility Document Procedure* • Authorization Level Procedure • Authorization Process for Implementing Information Security Processing Procedure • Information Security Responsibility Document Procedure* • Security Roles and Responsibilities of Information Asset Owners Document Procedure* 		<ul style="list-style-type: none"> • Authorization Level Records 	<ul style="list-style-type: none"> • Asset Responsibility Document* • Information Security Responsibility Document • Security Roles and Responsibilities of Information Asset Owners Document • System Asset Document • System Security Process Document 	<ul style="list-style-type: none"> • Asset Responsibility Document Review* • Information Security Responsibility Document Review* • Security Roles and Responsibilities of Information Asset Owners Document Review* • System Asset Document Review* • System Security Process Document Review*

Section 2
ISO/IEC 27002:2005 Evidence Products Checklist By Clause

ISO/IEC 27002:2005 Clause Number and Name	Policies and Procedures	Plans	Records	Documents	Audits and Reviews
6.1.3 Allocation of information security responsibilities (Cont. 1)	<ul style="list-style-type: none"> • System Asset Document Procedure* • System Security Process Document Procedure* 				
6.1.4 Authorization process for information processing facilities	<ul style="list-style-type: none"> • New Information Processing Facilities Authorization Procedures • Use of (Personnel or Privately) Owned Information Processing Facilities and or Equipment Procedure 				

Section 2
ISO/IEC 27002:2005 Evidence Products Checklist By Clause

ISO/IEC 27002:2005 Clause Number and Name	Policies and Procedures	Plans	Records	Documents	Audits and Reviews
6.1.5 Confidentiality agreements	<ul style="list-style-type: none"> • Confidentiality/Non-Disclosure Agreement Document Procedure* • Confidentiality/Non-Disclosure Agreement Procedure 		<ul style="list-style-type: none"> • Confidentiality/Non-Disclosure Agreement Records* 	<ul style="list-style-type: none"> • Confidentiality/Non-Disclosure Agreement Document 	<ul style="list-style-type: none"> • Confidentiality/Non-Disclosure Agreement Document Review • Confidentiality/Non-Disclosure Agreement Procedure Review • Confidentiality/Non-Disclosure Agreement Review
6.1.6 Contact with authorities	<ul style="list-style-type: none"> • Contact With Authorities Procedure 		<ul style="list-style-type: none"> • Information Security Contact With Authorities Records 		
6.1.7 Contact with special interest groups	<ul style="list-style-type: none"> • Contact With Special Interest Groups Procedure* • Information Sharing Agreements Document Procedure* 			<ul style="list-style-type: none"> • Information Sharing Agreements Document 	<ul style="list-style-type: none"> • Information Sharing Agreements Document Review*