Supplier Assessment Checklist

A Checklist For
Assessing Software Supplier Compliance
With
ISO/IEC 90003:2014

Author: Andy Coster, CCP

ISBN 978-0-9859732-3-0

SEPT Product 84
Produced by Software Engineering Process Technology (SEPT)
1705 16th Lane NE, Suite P203
Issaquah WA 98029

E-mail: Stanmagee@smartwire.net
Web Site: www.12207.com

A Checklist For
Assessing Software Supplier Compliance
With ISO/IEC 90003:2014

ISBN 978-0-9859732-3-0

Author: Andy Coster, CCP

Produced by
Software Engineering Process Technology
(SEPT)
1705 16th Lane NE
Suite P203
Issaquah WA 98029
Tel. 425-391-2344, Fax 425-557-9419
E-mail: StanMagee@SMARTWIRE.NET
Web Site: www.12207.com

Checklist for Assessing Software Vendors for Compliance with ISO/IEC 90003:2014 Software engineering: Guidelines for the application of ISO 9001:2008 to computer software

Section 1

Background

Many companies have asked SEPT- **"Do you have a checklist to use with our software suppliers to determine if they meet the requirements of Standard ISO/IEC 90003:2014"**? These companies stated they wanted a checklist that contained only **basic requirements** and no suggested artifacts. After determining our customer's needs SEPT has developed this checklist to meet that requirement. SEPT also produces a checklist for internal use within an organization to determine compliance with ISO/IEC 90003:2014. These two checklists are designed to be used as companion documents:

1. The Evidence Product checklist – to be used internally within an organization
2. The Supplier Assessment checklist to be used for supplier qualification and in supplier audits and reviews.

Introduction

The purpose of this document (Checklist) is to assist a company to determine if their "software" supplier(s) meet the requirements of Standard ISO/IEC 90003:2014 Software engineering: Guidelines for the application of ISO 9001:2008 to computer software. This document is designed to be used to:

- determine if a potential supplier has in place the key software process (artifacts), or
- qualify a supplier as approved for use, or
- provide a checklist for audit or review of a supplier.

The steps we used to develop this document are very similar to the ones used to produce the base line evidence product document.

The process of defining what is necessary for compliance with a quality management process standard such as "ISO/IEC 90003:2014" is often confusing and laborious because the directions contained in the standards are unclear or ambiguous. 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. All our 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. In these checklists, "manuals, reports, scripts and specifications" are included in the document category. When the subject standard references another standard for physical evidence, the checklist does not call out the full requirements of the referenced standard, only the expected physical evidence that should be available.

The author has carefully reviewed the document “ISO/IEC 90003:2014 Software Engineering: Guidelines for the application of ISO 9001:2008 to computer software " and defined the physical evidence required based upon this classification scheme. If a document is called out more than one time, only the first reference is stipulated. Additionally, there are many references to ISO/IEC 12207 in ISO/IEC 90003:2014 so ISO/IEC 12207 required items have been included and are denoted by a (#).
There are occasional situations in which a procedure or document is not necessarily separate and could be contained within another document. For example, the "Design and Development Verification Procedure" could be a part of the "Design and Development Procedure". The author has 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 vendor organizational requirements do not call for this physical evidence for a particular item, 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 assigned to the vendor.

General principles of this requirements checklist.
This checklist was prepared by analyzing each clause of this document for the key words that signify a policy, procedure, plan, record, document, audit, or review.

Artifact	Number required by 90003	Number required by 12207
Policy	1	0
Procedure	8	36
Plan	2	40
Record	24	60
Document (Including Manuals, Reports, Scripts and Specifications)	15	31
Audit	1	8
Review	21	38

This checklist specifies evidence that is unique. The information was transferred into checklist tables, based on the type of artifact. **Note:** All documents cited in ISO/IEC 12207 and required are denoted with a (# - ISO/IEC 12207 item): If the document is required by ISO/IEC 90003 it is under lined. An item can be underlined and have a # if required by both standards. These notations are listed in the footnotes for each section.

Using the Supplier Checklist

When a company is planning to use "ISO/IEC 90003:2014" (and by implication ISO 9001:2008) standard as a Supplier assessment tool, the company should either:

1. Send the checklist (to the vendor for completion and return (or post on an extranet site)
2. Take the checklist for completion on site as part of a supplier assessment or audit

If the Supplier's present process does not address an ISO/IEC 90003:2014 or ISO/IEC 12207, standard product, then this question should be asked: Is the evidence product required for the type of business of the supplier? If in the view of the supplier 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*." If the evidence is required, plans should be prepared to address the missing item(s). This checklist can be used to test a supplier's software processes from both a certification viewpoint (ISO/IEC 90003) and implementation of good practice (ISO/IEC 12207). However, it is unlikely that any organization will be fully compliant, so a user of the checklist should apply a pragmatic view of the results. After considering other commercial factors such as cost, experience, and supplier reputation, the organization must still ask the following question: "With this amount of non-compliance, should the company still do business with this supplier"? This is a question of the risk a company is prepared to take.

Detail Steps

A supplier 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.

Components of the Checklist
This checklist is composed of 4 sections:

- Section 1. Background and Introduction
- Section 2. Supplier summary information
- Section 3. Supplier Assessment checklist for all evidence types by clause.
- Section 4. "About the Author"

Rights to Make Multi Copies of This Document by the Purchaser or by Other Parties Who Have a Business Relationship with the Purchaser of the Document.
This document was designed to be used by companies with their suppliers who produce software or products with software. In this regard, the purchaser of this document may make as many copies as required to use within their organization and up to 3 copies to give to other companies who are suppliers or potential suppliers. However the suppliers may not make additional copies of the original document. All copies released outside an organization must be clearly stamped "Property of XYZ company duplication of the original document is not allowed". After a document has been filled out by a supplier additional copies may be made. This Product is also available in Microsoft Word format. Please see the SEPT web site www.12207.com for more details.

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

Section 2
Suppler Information

The following information records basic information concerning the supplier - Section 3 records the findings. Add additional items to suit your organizational needs.

Type of Assessment:	**Qualification** □	**Review** □	**Audit** □	**Other** □
Supplier Details				
Company Name				
Address				
E Mail address				
Telephone				
Fax				
Website				
Product Range Summary				
ISO 9001 Certification Body (if relevant)				
Date of Certificate				
Scope of Certification				
Date of (Last) Assessment				
Completed by				
Title/Role				
Email address				
Additional Data				

Section 3
ISO/IEC 90003 Supplier Assessment—Compliance Check List

Note: Section 3 items are in order of Policy, Plan, Record, Document, Audit, Reviews

ISO/IEC 90003:2014 Clause Number and Name		Item	Supplier Compliance	Not Required/ Rationale	Comments
4	**Quality management system**				
4.1	General requirements	• Software Life Cycle Model Document Procedure#			
		• Quality Management System Document			
		• Quality Management System Processes Used Document			
		• Software Development, Operation and Maintenance Processes Used Document#			
		• Software Life Cycle Model Document#			
		• Quality Management System Document Review			

Section 3
ISO/IEC 90003 Supplier Assessment—Compliance Check List

Note: Section 3 items are in order of Policy, Plan, Record, Document, Audit, Reviews

ISO/IEC 90003:2014 Clause Number and Name		Item	Supplier Compliance	Not Required/ Rationale	Comments
4.1	General requirements (cont.1)	• Quality Management System Processes Used Document Review			
4.2	Documentation requirements				
4.2.1	General	• Documentation Procedure#			
		• **Quality Policy**			
		• Tools, Techniques, Technologies and Methods Used Document Procedure#			
		• Documentation Plan#			
		• Process Planning, Operation and Control Records			
		• Quality Management System Records (All)#			
		• Quality Manual Document			

Section 3

ISO/IEC 90003 Supplier Assessment—Compliance Check List

Note: Section 3 items are in order of Policy, Plan, Record, Document, Audit, Reviews

ISO/IEC 90003:2014 Clause Number and Name		Item	Supplier Compliance	Not Required/ Rationale	Comments
4.2.1	General (cont.1)	• Quality Objective Document			
		• Tools, Techniques, Technologies and Methods Used Document#			
		• Quality Manual Document Review			
		• Quality Objective Document Review			
		• Quality Policy Review			
4.2.2	Quality manual	• Process Interaction Description Document			
		• Process Interaction Description Document Review			
4.2.3	Control of documents	• Document Control Procedure			