

Sample Pages of

SUPPLIER ASSESSMENT CHECKLIST
For Standard ISO/IEC 90003:2004
*Software engineering: Guidelines for the
application of ISO 9001:2000 to computer
software*

ISBN 0-9770309-1-1

Sample Pages of

SUPPLIER ASSESSMENT CHECKLIST
For Standard ISO/IEC 90003:2004
*Software engineering: Guidelines for the
application of ISO 9001:2000 to computer
software*

ISBN 0-9770309-1-1
Author: Andy Coster, CCP

Produced by
Software Engineering Process Technology
(SEPT)
2725 NW Pine Cone Drive
Issaquah, WA. 98027
Tel. 425-391-2344
E-mail: Stanmagee@COMPUSERVE.COM
Web Site: www.12207.com

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

Standard ISO/IEC 90003:2004 – Supplier Assessment Checklist

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 90003:2004**”? These vendors 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 90003:2004. 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 90003:2004 *Software engineering: Guidelines for the application of ISO 9001:2000 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 90003:2004” 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 90003:2004 Software Engineering: Guidelines for the application of ISO 9001:2000 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 90003:2004 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 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.

General Principles of the Standard ISO/IEC 90003:2004 Software engineering – Guidelines for the application of ISO 9001:2000 to computer software - 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 this document
Policy	1*
Procedure	39*
Plan	36
Record	58
Document (Including Manuals, Reports, Scripts and Specifications)	41
Audit	7
Review	47

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 are denoted with a (# - ISO/IEC 12207 item): This notation is listed in the footnotes for each section. The asterisk (*) is used to differentiate between ISO/IEC 90003 and ISO/IEC 12207 requirements for Policies and Procedures, those that are mandatory for ISO/IEC 90003 are coded M in sections 3 and 4. In practice this relates to 1 policy and 6 procedures. The remaining policies and procedures are those required by ISO/IEC 12207 from a compliance viewpoint.

Using the Supplier Checklist

When a company is planning to use "ISO/IEC 90003:2004" (and by implication ISO 9001:2000) 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 90003:2004 or ISO/IEC 12207 (or ISO 9001:2000) 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”?

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) <i>agrees</i> with the title of the evidence being planned by the organization.	Record in checklist that the organization is compliant.