ISO 9000-3-97 质量管理和质量保证标准

ISO 9001:1994 在计算机软件开发、供应、安装和维护中的应用指南

下面列出有关软件 ISO9000-3-97 质量管理和质量保证标准，以便软件开发、管理人员了解、掌握相关的标准,为软件开发的质量保驾护航。

引言

本标准为计算机软件设计、开发、安装和维护等业务的供方应用 ISO 9001:1994 提供指导。供方业务可涉及以下内容:

a)作为同外部组织签订商务合同的部分;

b)作为市场部门可获得的产品;

c)为了支持供方的业务过程;

d)作为嵌入硬件产品中的软件。

本标准指出需要涉及的问题,而与供方采用的技术、生存周期模型、开发过程、活动顺序或组织结构无关。

当一个组织的活动范围包含非计算机软件开发领域时,该组织质量体系中计算机软件要素与其它方面之间的关系宜清楚地写在一个统一的质量体系文件中。

本标准为应用 ISO 9001:1994 提供指南,在引用 ISO 9001:1994 原文的地方加上方框,以便于辨别。

本标准自始至终用"应"(shall)表示双方或多方间有约束力的规定;用"愿意"(will)表示一方的目的声明或意图;用"最好"、"建议"或"宜"(should)表示在诸多可能性中的一种推荐;用"可以"(may)指明在本标准范围内允许的作法。

1. 范围

本标准为便于计算机软件开发、供应、安装和维护的组织采用国际标准 ISO 9001:1994 提供指南。本标准未增加或改变 ISO 9001 的要求。

本标准不打算用作质量体系注册/认证时的评估准则。

2. 引用标准

本标准引用下列标准的有关条款。本标准发布时,这些引用标准均为有效版本。所有的标准都将修订。因此,鼓励依据本标准达成协议的各方尽可能采用下列标准的最新版本。IEC 和 ISO 成员均持有现行有效的国际标准。

ISO 8402:1994 质量管理和质量保证术语

ISO 9001:1994 质量体系　设计、开发、生产、安装和服务的质量保证模式

3. 定义

本标准采用 ISO 8402 中的定义及下述定义。

3.1 产品 product

活动或过程的结果。

注 1:产品可以包括服务、硬件、流程性材料、软件或它们的组合。

注 2:产品可以是有形的(如组织或流程性材料),也可是无形的(如知识或概念),或是它们的组合。

注 3:本标准中"产品"这一术语,仅适用于期望提供的产品,而不是影响环境的非期望有"副产品",这不同于 ISO 8402 中的定义[ISO 9001]。

3.2 投标 tender

供方应邀作出提供满足合同要求产品的报盘[ISO 9001]。

3.3 合同 contract

供方和顾客之间以任何方式传递的、双方同意的要求[ISO 9001]。

3.4 基线 baseline

一个配置项在其生存周期的某一特定时间被正式标明、固定并经正式批准的版本。无论媒体是什么[ISO/IEC 12207]。

3.5 开发 development

软件生存周期过程,包括需求分析、设计、编码、集成、测试、安装和支持软件产品验收等活动。

3.6 生存周期模型 life cycle model

一个框架,它包含从定义需求开始到不能再使用为止的系统寿命期间与软件产品开发、运行和维护有关的过程、活动和任务[ISO/IEC 12207]。

3.7 阶段 phase

注:某一个阶段,并不意味着使用任一特定的生存周期模型。

3.8 回归测试 regression testing

为确认纠正缺陷所作的更改不致引起派生缺陷的测试。

3.9 复制 replication

将软件产品从一个媒体拷贝到另一媒体。

3.10 软件 software

见软件产品(3.11)。

注:本标准中的术语"软件"限定为计算机软件。

3.11 软件产品 software product

整套的计算机程序、规程。可能还有与其相关的文档和数据[ISO/IEC 12207]。

注:软件产品可以是指定用于交付的产品,另一产品的组成部分或在开发过程中使用的产品。

3.12 软件项 software item

软件产品的任何可标识部分。

4. 质量体系要求

4.1 管理职责

4.1.1 质量方针

负有执行职责的供方管理者,应规定质量方针,包括质量目标和对质量的承诺,并形成文件。质量方针应体现供方的组织目标以及顾客的期望和需要。供方应确保其各级人员都理解质量方针,并坚持贯彻执行。

4.1.2 组织

4.1.2.1 职责和权限

对从事与质量有关的管理、执行和验证工作的人员,特别是对需要独立行使权力开展以下工作的人员,应规定其职责、权限和相互关系,并形成文件:

a) 采取措施,防止出现与产品、过程和质量体系有关的不合格;

b) 确认和记录与产品、过程和质量体系有关的问题;

c) 通过规定的渠道,采取、推荐或提出解决办法;

d) 验证解决办法的实施效果;

e) 控制不合格品的进一步加工、交付或安装,直至缺陷或不满足要求的情况得到纠正。

4.1.2.2 资源

对管理、执行工作和验证活动(包括内部质量审核),供方应确定资源要求并提供充分的资源,包括委派经过培训的人员(见 4.18)。

4.1.2.3 管理者代表

负有执行职责的供方管理者,应在自己的管理层中指定一名成员为管理者代表,不论其在其他方面职责如何,应明确权限,以便:

a) 确保按照本标准要求建立、实施和保持质量体系;

b) 向供方管理者报告质量体系的运行情况,以供评审和作为质量体系改进的基础。

注:管理者代表的职责还可包括就供方质量体系有关事宜与外部各方的联络工作。

4.1.3 管理评审

负有执行职责的供方管理者,应按规定的时间间隔对质量体系进行评审,确保持续的适宜性和有效性,以满足本标准的要求和供方规定的质量方针和目标(见 4.1.1)。评审记录应予以保存(见 4.16)。

4.2 质量体系

4.2.1 总则

供方应建立质量体系,形成文件并加以保持,作为确保产品符合规定要求的一种手段。供方应编制覆盖本标准要求的质量手册。质量手册应包括或引用质量体系程序,并概述质量体系文件的结构。

注:ISO 10013 提供了质量手册的编制指南。

不需要有与软件有关的进一步指南。

4.2.2 质量体系程序

供方应:

a) 编制与本标准要求和供方规定的质量方针相一致的形成文件的程序;

b) 有效地实施质量体系及其形成文件的程序。

基于本标准的目的,作为质量体系一部分的质量体系程序,其范围和详细程度应取决于工作的复杂程度、所用的方法,以及开展这项活动涉及的人员所需的技能和培训。

注:形成文件的程序可以引用规定某项活动如何进行的作业指导书。

不需要有与软件有关的进一步指南。

4.2.3 质量策划

供方应对如何满足质量要求作出规定,并形成文件。质量策划应与供方质量体系的所有其他要求相一致,并形成适于供方操作的文件。为满足产品、项目或合同规定的要求,供方应适当考虑下述活动:

a) 编制质量计划;

b) 确定和配备必要的控制手段、过程、设备(包括检验和试验设备)、工艺装备、资源和技能,以达到所要求的质量;

c) 确保设计、生产过程、安装、服务、检验和试验程序和有关文件的相容性;

d) 必要时,更新质量控制、检验和试验技术,包括研制新的测试设备;

e) 确定所有测量要求,包括超出现有水平但在足够时限内能开发的测量能力;

f) 确定在产品形成适当阶段的合适的验证;

g) 对所有特性的要求,包括含有主观因素的特性和要求,明确接收标准;

h) 确定和准备质量记录(见 4.16)。

注:4.2.3a)提及的质量计划可以采取引用相应的形成文件的程序的方式,这些程序构成供方质量体系的一个部分。

当合适时,质量计划应规定下述项目:

a) 合适的地方,以可测量的术语表示的质量要求;

b) 用于软件开发的生存周期模型;

c) 规定起动和结束每一项目阶段的准则;

d) 明确需要执行的评审、测试以及其他验证和确认活动的类型;

e) 明确需要执行的配置管理规程;

f) 详细策划(包括进度安排、程序、资源和批准)和特定的质量活动职责和权限,比如

✧ 配置管理;

✧ 开发产品的验证和确认;

✧ 采购产品的验证和确认;

✧ 顾客提供的产品的验证;

✧ 不合格产品的控制以及纠正措施;

✧ 确保完成质量计划中所述的活动。

质量计划为质量体系应用于特定的项目、产品或合同提供剪裁方法。如合适,质量计划可以包括或引用通用的和/或项目/产品/合同的特定规程。

质量计划应根据开发进展情况更新,当某一阶段开始时,与该阶段有关的活动应完全确定。

质量计划应由在其执行中有关的所有组织加以评审和协商一致。

描述质量计划的文档可以是独立的文档(加质量计划标题),或作为另一文档的一部分,或由若干文档组成。

质量计划可以包括或引用单元测试、集成测试、系统测试和验收测试的计划,测试策划和测试环境的指南是检验和测试的一部分。

注:质量计划指南在 ISO 10005 中给出,配置管理指南在 ISO 10007 中给出。为得到更多的信息,参看 ISO/12207:1995 的 6.2 至 6.5 条。

4.3 合同评审

4.3.1 总则

供方应建立并保持合同评审和协调合同评审活动的形成文件的程序。

软件可以作为合同的一部分开发,作为市场上可获得的产品、作为硬件产品中嵌入的软件或作为供方业务过程的支撑软件而开发。合同评审适用于所有这些情况。

4.3.2 评审

在投标或接受合同或订单(对要求的说明)之前,供方应对标书、合同或订单进行评审,以确保:

a) 各项要求都有明确规定并形成文件;在以口头方式接到订单,而对要求没有书面说明的情况下,供方应确保订单的要求在其被接受之前得到同意;

b) 任何与投标不一致的合同或订单的要求已经得到解决;

c) 供方具有满足合同或订单的要求的能力。

在供方对软件标书、合同或订单评审期间,还可能涉及到下述有关事项。

a) 与顾客有关的事项:

- 采用的名词术语由有关各方协商一致;
- 顾客具有履行合同义务的能力和资源;
- 经过协商一致的顾客接受或拒收产品的准则;
- 顾客在提供资料和有关设施方面的职责;
- 在联合开发或分包工作中,顾客参与的程度;
- 为监督合同进展而进行联合评审的安排;
- 经过协商一致的在开发和/或维护期间处理顾客要求的更改的程序;
- 顾客强加的生存周期过程;
- 验收后发现的问题的处理,包括申诉、顾客的抱怨;
- 在任何保证期之后消除不合格部分的职责;
- 当供方要求时,向后续版本升级后顾客承担的义务。或者供方保存历史版本的义务;
- 推广应用和有关的用户培训。

b) 技术事项:

- 符合需求的可行性;
- 需采用的软件开发标准和规程;
- 明确需由顾客提供的设施、工具、软件项和资料,确定评估它们对使用的适合性的方法,并形成文档;
- 操作系统或硬件平台;
- 关于软件产品接口的控制协议;
- 复制和分发要求。

c) 管理方面:

- 明确可能的事故和风险,并评估它们对后续活动的影响;
- 供方与分包工作有关的职责;
- 进度、技术评审和交付物的安排;
- 安装、维护支持要求;
- 技术、人力和财力资源的及时可得性。

d) 法规、安全和保密事项:

- 按合同使用的信息可能会遇到知识产权、许可证协议、保密性和保护问题;
- 产品原版的保护,以及顾客访问或验证该原版的权力;
- 需由各方协商同意的向顾客透露信息的程度;
- 保证期限的确定;
- 与合同相关连的责任/处理。

注:为得到更多的信息,参看 ISO/IEC 12207:1995 的 5.2.1,5.2.6 和 6.4.2.1 条。

4.3.3 合同的修订

供方应确定如何进行合同修订,并正确传递到供方组织内的有关职能部门。

不需要有与软件有关的进一步指南。

注:为得到更多信息,参看 ISO/IEC12207 的 5.1.3.5 和 5.2.3.2 条。

4.3.4 记录

应保存合同评审的记录(见 4.16)。

注:供方应与顾客建立有关合同事宜的联络渠道和接口。

不需要有与软件有关的进一步指南。

4.4 设计控制

4.4.1 总则

供方应建立并保持产品设计控制和验证的形成文件的程序,以确保满足规定的要求。

本节提供需求分析、体系结构设计、详细设计和编码等开发活动的指南。这一切还包括开发策划指南。

软件开发项目应根据一个或多个生存周期模型进行组织。过程、活动和任务应根据采用的生存周期模型的性质加以计划并实施。采用的生存周期模型可以更新,应适合具体的项目要求。本实施大纲主张应用时与采用的生存周期模型无关,不主张指出特定的生存周期模型。

生存周期模型明确一套过程,并规定何时和如何引用这些过程。在本国际标准中所描述的过程的顺序并非以任何方式建议按此顺序完成这些任务。

开发过程就是将需求规范转换为软件产品。这种过程应以规定的方法步骤实施,以免引入错误。这种方法作为明确问题的唯一方法而降低了对验证和确认过程的依赖。因此,供方应建立和维持文件化的规程,以保证软件产品的设计和实现符合规定的要求,并按开发计划和/或质量计划进行。

下述设计活动的固有方面应加以考虑:

a) 设计方法:应系统地使用设计方法。应考虑这种方法对任务、产品或项目类型的适合性,以及所采用的方法与工具的兼容性。

b) 利用过去的经验:利用从过去的实践吸取的经验教训,供方通过应用从先前项目、度量分析和过去项目评审学到的经验,应避免同样的或类似的问题重复出现。

c) 后续过程:软件产品应尽可能设计得便于测试、安装、维护和使用。

d) 保密和安全:设计应特别考虑可测试性或便于确认。对于失效将给人员、性能或环境造成危险的产品,这种软件的设计应保证规定特定的设计要求,即规定所希望的免于发生潜在的失效状态,或对潜在的失效状态做出系统反应。

对于编码,最好规定并遵守:编程语言使用规则、一致的命名约定、编码和适当的注释规则。这类规则应形成文件并加以控制。

建议只有当所有已知缺陷的后果都能圆满解决时,或者进程中的风险已知时,才应开始进行设计活动。

供方可以使用工具、设备和技术,以便落实本标准中的质量体系指南。这些工具、设备和技术对于管理目的以及产品开发和/或服务可能是有效的。不管这些工具和技术是内部开发的或购买的,供方均应评价它们是否适合于使用目的。在产品实现中使用的工具,比如分析和设计工具、编译程序、汇编程序等应经批准,并在使用之前应按配置管理控制的适当级别配置。这种工具和技术的使用范围最好形成文件,并按规定的间隔复审它们的使用,确定是否需要改进它们和/或使它们升级。

在开始使用这种工具和技术时,或任何改进/升级之后,可能需要对人员进行培训。

4.4.2 设计和开发的策划

供方应对每项设计和开发活动编制计划。计划应阐明或列出应开展的活动,并规定实施这些活动的职责。设计和开发活动应委派给具备一定资格的人员去完成,并为其配备充分的资源。计划应随设计的进展加以修改。

对于软件产品,开发策划应确定软件产品的下述活动:需求分析、设计、编码、集成、测试、安装和接收支持。开发策划应以开发计划形式形成文件。

开发计划应加以评审和批准。开发计划可以有其他名称,比如"软件开发计划"或"软件项目计划"。

开发计划可以确定项目如何进行管理,要求的进度评审,向管理者、顾客和其他有关方报告的类型和频次。要考虑任何合同要求。

如合适,开发策划可包括下述内容:

a) 项目的定义,包括对其目的说明以及引用的顾客或供方的任何有关项目;

b) 作为一整体项目的输入和输出的定义;

c) 项目资源的组织,包括工作小组的组成、职责,分包商的使用以及需使用的物资资源;

d) 个人或小组之间的组织接口和技术接口,例如:

- 子项目小组;
- 分承包商;
- 用户;
- 顾客代表;
- 质量保证代表;

e) 标明或引用以下内容:

- 需完成的开发活动;
- 每一活动所要求的输入;
- 每一活动所要求的输出;
- 需完成的管理和支持过程;

f) 对伴随开发的可能风险、假设、相依性和问题的分析;

g) 进度安排标明:

- 项目的各个阶段;
- 需进行的工作(每项任务的输入、输出和定义);
- 相关的资源和时间要求;
- 相关的依存关系;
- 里程碑;

h) 明确下述内容:

- 标准、规则、惯例和约定;
- 开发用的工具和技术。包括对这类工具和技术的鉴定和配置控制;
- 配置管理惯例;
- 控制不合格品的方法;
- 用于支持开发的非交付软件的控制方法;
- 备份和恢复(包括应付偶然事故的计划)的规程;

- 归档、备份和恢复的程序,包括应急计划;
- 病毒防护的控制方法;

i) 标明有关计划(包括系统级计划),如:

- 质量计划;
- 风险管理计划;
- 配置管理计划;
- 集成计划;
- 测试计划;
- 安装计划;
- 移交计划;
- 培训计划;
- 维护计划;
- 重用计划。

开发计划和任何有关的这些计划可以是一份独立的文件,或作为另一文件的一部分,或者由若干文件组成。

注:为得到更多的信息,参看 ISO/IEC 12207:1995 的 5.2.4 条。

4.4.3 组织和技术接口

应规定参与设计过程的不同部门之间在组织上和技术上的接口,将必要的信息形成文件,予以传递并定期评审。

软件生产的每一部门的职责范围、在所有各方之间传递技术信息的方式,应在供方或分承包方的开发计划中清楚地确定。供方可以要求分承包方提交开发计划,以供评审。

在确定接口时,除了顾客和供方之外,应注意考虑到对设计、安装、维护和培训活动有要求的各方。他们可以包括分承包方、上级管理机关、相关开发项目和咨询服务人员。特别是,可能需要最终用户和所有中间运行职能部门的参与,以保证得到适当的能力和培训,达到承诺的服务水平。

按合同顾客可能有某些职责。特别需要关心的事包括需要顾客与供方合作以及时提供必要的信息,并解决相关事项。在有顾客代表的地方,顾客代表可以代表产品的最终使用者并执行管理,有权处理合同事项,包括但不限于下列事项:

a) 确定顾客对供方的要求;
b) 回答供方的询问;
c) 批准供方的建议;
d) 与供方达成协议;
e) 保证顾客的组织遵守与供方达成的协议;
f) 确定验收准则和规程;
g) 处理顾客提供的不适合使用的软件项、数据、设施和工具;
h) 确定顾客的职责。

相互协商一致时,供方和顾客的联合评审可以安排为定期的或项目发生重大事件时进行,联合评审视情况合适与否覆盖下述方面:

a) 供方的软件开发工作的进展;
b) 顾客同意承担的活动的进展;
c) 开发的产品是否符合顾客同意的需求规格说明;
d) 开发涉及系统最终用户的活动的进展,比如系统转换和培训;
e) 验证结果;
f) 验收测试结果。

注:为得到更多的信息,参看 ISO/IEC12207 的 6.6.2 条。

4.4.4 设计输入

供方应确定与产品有关的设计输入要求,包括适用的法令和法规要求,形成文件,并评审其是否适当。对不完善的、含糊的或矛盾的要求,应会同提出者一起解决。

设计输入应考虑合同评审活动的结果。

需求规格说明最好由顾客提供。然而,在相互协商一致时,供方也可提供需求规格说明。在这种情况下,如合适,供方应注意下列事项:

a) 建立文件化的程序来制订需求规格说明书,包括:

- 商定需求和授权更改的方法,特别是在反复制定需求的情况下;
- 如采用了原型或演示,对原型或演示的评价方法;
- 记录和审查双方讨论的结果;

b) 与顾客密切合作制订需求规格说明书,并且采取措施,例如提供术语定义、解释需求的背景等,力求避免误解;

c) 取得顾客对需求规格说明书的批准。

如合适,可采用交谈、调查、研究、提供原型、演示和分析等方法来制订需求规格说明书。

需求规格说明书可以以系统说明书形式提供并协商一致。在这种情况下,应有适当的程序以确保将系统要求正确地分配到硬件、软件以及适当的接口说明书中。

需求规格说明书在接受合同时可以不完全确定,在项目进行期间可继续制定。当需求规格说明书更改时,合同可以修订。对需求规格说明书的更改应加以控制。

需求应包括为满足用户同意的需要所必需的所有方面。需求规格说明书可能需要考虑运行环境。需求可以包括但不限于下述特性:功能性、可靠性、易用性、效率、可维护性和可移植性(见 ISO/IEC9126)。可以规定例如保密等子特性,还可规定安全性和法定义务。

如果软件产品需要与其他软件或硬件产品接口,在需求规格说明书中应尽可能规定这些接口,可以直接规定,也可以引用。

需要最好用产品验收时能够确认的形式表示。

注:为得到更多的信息,参看 ISO/IEC 12207:1995 的 5.3.2 至 5.3.4 条。

4.4.5 设计输出

设计输出应形成文件,并以能够对照设计输入要求进行验证和确认的形式来表达。

设计输出应:

a) 满足设计输入的要求;

b) 包含或引用验收准则;

c) 标出与产品安全和正常工作关系重大的设计特性(如操作、贮存、搬运、维修和处置的要求)。

设计输出文件在发放前应予以评审。

每项设计活动所要求的输出应根据所选择的方法确定并形成文档。这种文档应是正确的、完整的并符合要求。设计的输出可以包括:

- 概要设计说明书;
- 详细设计说明书;
- 源代码;
- 用户指南。

注:为得到更多的信息,参看 ISO/IEC12207:1995 的 5.3.5 至 5.3.7 条。

4.4.6 设计评审

在设计的适当阶段,应有计划地对设计结果进行正式的评审,并形成文件。每次设计评审的参加者应包括与被评审的设计阶段有关的所有职能部门的代表,需要时也应包括其他专家。这些评审记录应予以保存(见 4.16)。

供方应对所有软件开发项目制定计划并实施评审过程。与评审过程相关联的活动的形式和严格度应适

合于产品的复杂程序以及与软件产品规定的使用相关联的风险程度。供方应建立文件化的程序来处理在这些活动期间发现的产品缺陷和过程缺陷或不合格事项。

在设计评审时,最好考虑到设计活动的内要因素,例如,可行性、保密性、安全性、编程规则和可测试性。

评审结果以及为确保符合规定要求所需的进一步活动,当它们完成时应加以记录和核实。只有经验证的开发输出才应提交验收和后续使用。

开发期间的大多设计评审要加以计划安排,但也可能有一些未经安排的设计评审。

形成文件的设计评审程序应提及下述内容:

a) 评审什么,何时评审以及评审类型;

b) 在每种评审类型中应涉及什么功能组,如果需要召开评审会议,应由谁主持;

c) 必须产生什么记录,例如:会议记录、结果、问题、措施和措施状态。

在设计评审程序中,也可以阐明以下内容:

a) 为保证符合性对规则、惯例和约定的应用进行监督的方法,如同行评审、审查、代码审查;

b) 在进行评审之前必须做些什么,如制定目标、会议日程、需要的文档和评审人员的分工;

c) 评审期间要做些什么,包括需采用的技术和所有参加人员的守则;

d) 评审通过的准则;

e) 采用什么跟踪方法以确保评审中发现的问题得以解决。

合同中有规定时,供方应与顾客合作召开设计评审会议。双方应对评审结果协商一致。

建议只有当所有已知的缺陷都得到满意的解决,或者继续进行的风险已知时,才继续进行进一步的设计活动。

注:为得到更多的信息,参看 ISO/IEC12207:1995 的 5.3.4.2,5.3.5.6,5.3.6.7 和 6.6.3。

4.4.7 设计验证

在设计的适当阶段,应进行设计验证,以确保设计阶段的输出满足该设计阶段输入的要求。设计验证应予以记录(见 4.16)。

注:除实施设计评审(见 4.4.6)之外,设计验证还可包括以下活动:

✧ 变换方法进行计算;

✧ 可能时,将新设计与已证实的类似设计进行比较;

✧ 进行试验和证实;

✧ 对发放前的设计阶段文件进行评审。

建议在开发过程中,适当地进行设计验证。设计验证可由设计输出评审,包括原型和仿真的演示或测试组成。验证可对其他开发活动的输出进行。这些验证活动应根据质量计划或形成文件的程序予以计划和进行,以保证过程输出符合过程输入要求。

为保证符合设计阶段输入的要求而需要的验证结果和任何进一步措施应予以记录,并且当措施完成时进行核算。

只有经验证的开发输出才应提交验收和后续使用。建立对任何发现的问题都要充分论述并加以解决。

注:为得到更多的信息,参看 ISO/IEC12207:1995 的 5.3.4.2,5.3.5.6,5.3.5.7,5.3.7.5,5.3.9 和 6.4 条。

4.4.8 设计确认

应进行设计确认,以确保产品符合规定的使用者需要和/或要求。

注:

1. 设计确认在成功的设计验证(见 4.4.7)之后进行;

2. 确认通常在规定的操作条件下进行;

3. 确认通常针对最终产品进行,但产品完成前的各阶段也可能需要进行;

4. 如果有不同的预期用途,也可以进行多次确认。

在产品提交顾客验收之前,例如在最终检验和测试期间,供方应根据其规定的预期用途确认产品。

在软件开发中,为了确保满足规定的要求,确认结果以及需进一步采用的措施应加以记录,并且当措施完

成时加以核查。这一点非常重要。只有经确认的产品才应提交验收或后续使用。

注:为了得到更多信息,参见 ISO/IEC12207:1995 的 5.3.1 和 6.5 条。

4.4.9 设计更改

所有的设计更改和修改的实施之前都应由授权人员加以确定,形成文件,并评审和批准。

供方应建立和维持控制任何设计更改的实施的程序,这种更改可能在产品开发生存周期的任何时期发生。建立这种程序为了:

a) 将更改形成文档并证实它是合理的;

b) 评价更改的后果;

c) 批准或不批准更改;

d) 实施并验证更改。

在软件开发环境中,设计更改的控制通常在配置管理规定中说明。

注:为了得到更多信息,参见 ISO 12207:1995 的 5.5.2,5.5.3 和 6.2.3 条。

4.5 文件和资料控制

4.5.1 总则

供方应建立并保持形成文件的程序,以控制与本标准要求有关的所有文件和资料,包括适当范围的外来文件,如标准和顾客提供的图样。

注:文件和资料可以呈任何媒体形式,如硬拷贝或电子媒体。

配置管理程序可以用来实施文档和数据控制。在建立的控制所有文档和数据的程序中,供方应确定那些需服从控制程序的文档的数据,包括外部来源的文档和数据,例如标准和顾客提供的数据。

文档和数据控制程序应用于有关的文档和数据,包括下述种类:

a) 合同规定的文档,包括需求规格说明书;

b) 用于描述软件生存周期内的质量体系的形式文件的程序;

c) 描述供方活动的策划和进展,以及供方与顾客相互配合的计划文档;

d) 描述一具体软件产品的或与特定软件产品相关联的产品文件和数据。

注:为了得到更多信息,参见 ISO/IEC12207:1995 的 6.1 条。

4.5.2 文件和资料的批准和发布

文件和资料在发布前应由授权人员审批其适用性。应制定并可随时得到识别文件的现行修订状态的控制清单或相当的文件控制程序,以防止使用失效和/或作废的文件。

这种控制应确保:

a) 在对质量体系有效运行起重要作用的各个场所,都能得到相应文件的有效版本;

b) 从所有发放或使用场所及时撤出失效和/或作废的文件,或以其他方式确保防止误用;

c) 为法律和/或积累知识的目的所保留的任何已作废的文件,都应进行适当标识。

在使用电子手段实现文档控制的地方,对其适当的批准、存取、发放、媒体和归档规程应予以特别注意。

4.5.3 文件和资料的更改

除非有专门指定,文件和资料的更改应由该文件的原审批部门/组织进行审批。若指定其他部门/组织审批时,该部门/组织应获得审批所需依据的有关背景资料。

可行时,应在文件或相应附件上标明更改的性质。

不需要有与软件有关的进一步指南。

4.6 采购

4.6.1 总则

供方应建立并保持形成文件的程序,以确保所采购的产品(见 3.1)符合规定要求。

在开发、供应、安装和维护软件产品过程中,采购的产品可包括:

- 市售现成软件;
- 分承包方开发的软件;

- 计算机和通信硬件;
- 帮助软件开发的工具;
- 合同制工作人员;
- 维护和顾客支持服务;
- 培训课程和教材。

注:为了得到更多信息,参看 ISO/IEC12207:1995 的 5.1 条。

4.6.2 分承包方的评价

供方应:

a) 根据满足分合同要求(包括质量体系和特定的质量保证要求)的能力评价和选择分 承包方;

b) 明确供方对分承包方实行控制的方式和程度,这种方式和程度取决于产品的类别以及分承包的产品对成品质量的影响,还取决于已证实的分承包方能力和业绩的质量审核报告和/或质量记录;

c) 建立并保存合格分承包方的质量记录(见 4.16)。

不需要有与软件有关的进一步指南。

4.6.3 采购资料

采购文件应清楚地说明订购产品的资料,可包括:

a) 类别、形式、等级或其他准确标识方法;

b) 规范、图样、过程要求、检验规程及其他有关技术资料(包括产品、程序、过程设备和人员的认可或鉴定要求)的名称或其他明确标识和适用版本;

c) 适用的质量体系标准的名称、编号和版本。

供方应在采购文件发放前对规定的要求是否适当进行审批。

用于软件开发的采购文档最好包括清楚地说明订购产品的数据,可包括:

a) 订购产品的准确标识,如产品名称和/或产品编号;

b) 需求规格说明,或它的等同文档(或当需求规格说明在订购时尚未完全确定,就规定确定需求规格说明的规程);

c) 采用的标准(例如通信协议、体系结构规范);

d) 规程和/或工作需求说明;

e) 开发环境;

f) 对人员的要求。

关于合同评审的考虑也可用于分合同。

4.6.4 采购产品的验证

4.6.4.1 供方在分承包方货源处的验证

当供方提出在分承包方货源处对采购产品进行验证时,供方应在采购文件中规定验证的安排以及产品放行的方式。

不需要有与软件有关的进一步指南。

4.6.4.2 顾客对分承包方产品的验证

当合同规定时,供方的顾客或其代表应有权在分承包方处和供方处对分承包的产品是否符合规定要求进行验证。供方不能把该验证用作分承包方对质量进行了有效控制的证据。

顾客的验证既不能免除供方提供可接收产品的责任,也不能排除其后顾客的拒收。

不需要有与软件有关的进一步指南。

4.7 顾客提供产品的控制

供方对顾客提供的产品(用于供应品或有关活动)应建立并保持验证、贮存和维护的形成文件的控制程序。如有丢失、损坏或不适用的情况,应予以记录并向顾客报告(见 4.16)。

供方的验证不能免除顾客提供可接收产品的责任。

顾客可能要求供方取得由顾客提供的包括数据在内的产品,并将其纳入供方产品中,例如:

a) 软件产品,包括顾客提供的市售软件产品;

b) 开发工具;

c) 开发环境,包括网络服务;

d) 测试数据和运行数据;

e) 接口规格说明或其他规格说明;

f) 硬件;

g) 顾客专有信息,包括规格说明。

在任何与待交付的产品有关的维护协议中,最好在合同中说明这类软件产品所需的许可证和支持。

应确定已接收并已集成的顾客提供的软件项的更新方法,供方可以应用与采购产品相同的验证活动来验证顾客提供的产品。

注:为得到更多信息,参看 ISO/IEC12207:1995 的 6.1 条。

4.8 产品标识和可追溯性

必要时,供方应建立并保持形成文件的程序,在接收和生产、交付及安装的各阶段以适当的方式标识产品。

在规定有可追溯性要求的场合,供方应建立并保持形成文件的程序,对每个或每批产品都应有唯一标识,这种标识应加以记录(见 4.16)。

供方最好建立并保持程序,用以标识从规格说明到开发、复制与交付的所有阶段的软件项。如果合同要求,这些程序也可适用于产品交付之后。

该程序最好跟踪产品整个生存周期的软件项或软件产品的部件。根据合同和市场需求的不同,跟踪范围可以有所不同,从可将某一变更要求加于特定发行物到记录产品的每一变更的目标和用法。

在软件中,可以实现的标识和可追溯性的一种方法就是配置管理。配置管理是一种管理学科,对配置项(包括软件项)的开发和生存周期的支持,给予技术和管理指导。这种学科还适用于有关的文档编制和硬件。配置管理的使用取决于项目规模和复杂性以及风险水平。

配置管理的一个目标是编制文档,并对产品现有的配置和达到其要求的状态提供足够的可视性。另一目标是项目的每个工作人员在项目的生存周期中的任何时刻都能采用正确的和准确的信息。

配置管理系统可以提供下述能力:

a) 唯一地标识每一软件项的版本;

b) 标识共同构成一完整产品的特定版本的每一软件项的版本;

c) 标识正在开发的和已交付或安装的软件产品的构成状态;

d) 控制由两个或多个独立工作的人员同时对一给定软件项的更新;

e) 按要求在一个或多个位置对复杂产品的更新进行协调;

f) 标识并跟踪所有的措施和更改,这些措施和更改是在从开始直到放行期间,由于更改请求或问题引起的。

供方应按下述内容标识配置:

a) 产品结构和配置项的选择;

b) 文档编制和计算机文档;

c) 命名惯例;

d) 配置基线的建立。

可能由配置管理系统管理的产品包括:

a) 与合同、过程、计划和产品有关的文档和数据;

b) 源代码、目标代码和可执行代码;

c) 相关产品,包括:

——软件工具;

——包括库在内的可重复用软件;

——外购软件;

——顾客提供的软件。

供方最好建立程序,以保证每一软件项的下述内容都能标识:

a) 文档;

b) 所有有关的开发工具;

c) 与其他软件项的接口与硬件的接口;

d) 硬件环境与软件环境。

供方应建立和维持配置管理状态的记述和报告规程,以记录、管理和报告软件项的状态,更改要求的状态和已批准的更改实施状态。

供方最好建立并实施一个包含以下内容的配置管理计划:

a) 负责配置管理的组织以及每一个管理组织的职责;

b) 需要进行的配置管理活动;

c) 所使用的配置管理工具、技术及方法;

d) 将软件项置于配置控制之下的时机。

注:为得到更多配置管理信息,参见 ISO 10007 和 ISO/IEC12207:1995 的 6.1 和 6.2 条。

4.9 过程控制

供方应确定并策划直接影响质量的生产、安装和服务过程,确保这些过程在受控状态下进行。受控状态包括:

a) 如果没有形成文件的程序就不能保证质量时,则对生产、安装和服务的方法制定形成文件的程序;

b) 使用合适的生产、安装和服务设备并安排适宜的工作环境;

c) 符合有关标准/法规、质量计划和/或形成文件的程序;

d) 对适宜的过程参数和产品特性进行监视和控制;

e) 需要时,对过程和设备进行认可;

f) 以最清楚实用的方式(如文字标准、样件或图示)规定技艺评定准则;

g) 对设备进行适当的维护,以保持过程能力。

当过程的结果不能通过其后产品的检验和试验完全验证时,如加工缺陷仅在使用后才能暴露出来,这些过程应由具备资格的操作者完成和/或要求进行连续的过程参数监视和控制,以确保满足规定要求。

对过程运行[包括有关设备和操作人员(见 4.18)]的任何鉴定要求都应加以规定。

注:这些要求预先鉴定过程能力的过程,通常被称为是"特殊过程"。必要时,应保存经鉴定合格的过程、设备和人员的记录(4.16)。

正如在 ISO 9001 的"设计控制"要素的指南所规定的,软件开发项目最好根据将需求转化为软件产品的一系列过程加以组织。当"过程控制"要素应用于软件开发时,也适用于软件项或软件产品的复制、交付和安装。

当合同要求时,供方最好考虑下述事项建立和执行复制规程,以确保复制正确地进行

a) 原件和复制件的标识,包括格式、变型和版本;

b) 待交付的每一软件项复制件的数目;

c) 适用时,包括原件和备份件的保护在内的故障恢复计划;

d) 供方提供复制件和阅读原件的能力的责任期限;

e) 每一软件项的媒体类型及相应的标签;

f) 防止可能发生的软件病毒的检查;

g) 需要的诸如手册和用户指南等文档的规定,包括标识和包装;

h) 涉及的并已协商同意的版权和许可证事宜;

i) 为确保再现性,对影响复制的环境的控制。

为了软件产品的放行,供方和顾客应就初始版本发行和后续版本发行的程序协商一致

并形成文件。

建议对于软件的发行要建立一条基线,以记录所完成测试和已查明的缺陷的解决措施。对于有安全和/或保密要求的软件,可以进行定量分析以预计系统的可靠性。

建议这些程序包括下述内容:

a) 根据频度和/或对顾客操作的影响以及在任何时候及时实施更改的能力,对软件版本发行类型(或级别)进行描述;

b) 向顾客通告目前或计划的未来更改的方法;

c) 确认实施的更改将不引起其他问题的方法,这种方法最好包括确定为每一发行版本实施的回归测试的水平;

d) 确定一些基本规则,以判明何处可以插入局部的临时的修改,或者判明在何时发行软件产品的完整的更新的复制件;

e) 要求记录说明哪些更改已经实现和对于多处加工的复合产品及位置是在何处作了更改。

当安装软件产品是合同要求时,供方和顾客应就它们各自的作用、职责和义务协商一致,这种协议应形成文件。在准备安装中,应考虑下列各点:

a) 是否需要在合同要求的每一次安装确认;

b) 安装规程;

c) 对每一个已完成的安装的批准程序;

d) 进度安排;

e) 访问顾客设施的办法(例如保密标记、口令、护送);

f) 对熟练人员的可得性;

g) 顾客系统和设备的可利用性以及访问这些设施的办法;

h) 标明顾客在现场需提供什么;

i) 使用新设施的培训。

注:为得到更多信息,参看 ISO/IEC12207:1995 的 5.3.12 和 6.3.3 条。

4.10 检验和试验

4.10.1 总则

供方应建立并保持进行检验和试验活动的形成文件程序,以便验证产品是否满足规定要求。所要求的检验和试验及所建立的记录应在质量计划或形成文件的程序中详细规定。

可能需要在从单独的软件项到完整的软件产品的若干级别上进行测试。有若干不同的测试方法、测试范围,对测试环境的控制程序、测试输入和测试输出可以随测试方法、产品复杂性和风险大小而变化。软件测试还要在软件集成期间进行。在"设计评审"中描述的技术也可能与"检验和试验"活动相关。

在某些情况下,确认、现场测试和验收测试可以是同一活动。

供方最好根据质量计划或形成文件的程序,为单元测试、集成测试、系统测试和验收测试建立测试计划,编成文件并予以评审。如合适,包括:

a) 测试目的;

b) 必须测试的配置;

c) 需进行的测试类型,例如功能测试、边界测试、性能测试、可用性测试;

d) 测试顺序、测试条件、测试过程、测试数据和预期结果;

e) 测试实施的作用域,用测试覆盖率和极限量表示;

f) 测试与测试目的的相关性及测试与操作使用的相关性;

g) 特殊事项,例如保密性和安全性;

h) 测试环境、测试工具和测试软件,包括任何相关的鉴定和控制;

i) 最终用户文档的检验;

j) 所需人员和相关的培训要求,包括培训资料;

k) 软件开发人员和软件测试人员间的独立程度;

l) 测试规格说明和测试实施的职责;

m) 判断测试完成的准则;

n) 记录结果的方法;

o) 分析及认可测试结果的规程;

p) 处理测试实施期间发现问题的规程,包括暂停准则和恢复要求;

q) 回归测试的必要性以及执行程度;

r) 测试的再现性。

注:为了得到更多信息,参看 ISO/IEC 12207:1995 的 5.1.5,5.3.5.5,5.3.6.5,5. 3.6.6,5.3.7,5.3.11 和 5.3.13 条。

4.10.2 进货检验和试验

4.10.2.1 供方应确保未经检验或未经验证合格的产品不投入使用或加工(4.10.2.3 中规定的情况除外)。应按质量计划和/或形成文件的程序验证是否符合规定要求。

4.10.2.2 确定进货检验的数量和性质时,应考虑在分承包方处所进行的控制程度和所提供的合格证据。

4.10.2.3 如因生产急需来不及验证而放行时,应对该产品作出明确标识,并作好记录(见 4.16),以便一旦发现不符合规定要求时,能立即追回和更换。

供方可能要求取得第三方提供的包括数据在内的软件产品,并纳入供方软件产品中。建议供方建立和保持形成文件的程序,以便根据合同要求进行这种产品的(接收)验证。

对于顾客提供的产品,供方也可进行与采购的产品相同的验证活动。

4.10.3 过程检验和试验供方应:

a) 按质量计划和/或形成文件的程序的要求,检验和试验产品;

b) 所要求检验和试验完成或必需的报告收到和验证前,不得将产品放行。除非有可靠追回程序(见 4.10.2.3)才可例外放行,但仍应遵循 4.10.3a)规定。

可参看 4.10.1 条的内容。

4.10.4 最终检验和试验

供方应按照质量计划和/或形成文件的程序进行全部的最终检验和试验,以提供符合规定要求的证据。

质量计划和/或最终检验和试验的形成文件的程序,应要求所有规定的检验和试验(包括进货检验和过程检验)均已完成,且结果满足规定要求。

只有在质量计划和/或形成文件的程序中规定的各项活动已经圆满完成且有关数据和文件齐备并得到认可后,产品才能发出。

在提交产品供顾客验收之前,建议供方根据合同中的规定,在与应用环境类似的条件下,根据规定的预定用途,确认产品的运行正确性。确认环境和实际应用环境的任何差别,以及与这种差别相关联的风险,应尽可能在生存周期早期阶段予以查明和判断,并记录。

在确认过程中,只要合适,在发放配置基线以前,可以根据对评审、检验和测试记录的核查,进行配置审核或评价,以确保软件产品是否符合其合同或规定的要求。

当考虑测试环境时,建议注意下述事项:

a) 待测试的特性;

b) 需对测试环境,包括测试工具施加的控制;

c) 环境对测试的任何限制。

当要求在目标环境中测试时,建议考虑下述事项:

a) 供方和顾客在进行测试和评价测试中的特定职责;

b) (测试后)用户环境的恢复。

当供方准备好交付已确认的产品时,可以要求验收测试支持。顾客应根据事先商定的准则和合同中规定的方式,判断产品是否可被接受。验收测试最好由顾客进行,也可由供方或第三方代表顾客进行。供方应按

合同中的规定,在验收活动中与顾客合作。

当合同要求验收测试由供方进行时,可以认可最终检测和测试以及确认活动与验收测试活动相关。有时确认测试、现场测试与验收测试可以是同一活动。

在进行验收活动之前,供方应协助顾客明确下述事项:

a) 时间安排;

b) 评价规程,包括验收准则;

c) 软件/硬件环境,包括对它们的控制;

d) 要求的人力资源和相关的培训。

在实施验收规程期间发现问题的处理方法以及对它们的处置,最好由供方和顾客协商一致,并应形成文件。

4.10.5 检验和试验记录

供方应建立并保存表明产品已经检验和/或试验的记录。这些记录应清楚地表明产品是否已按所有规定的验收标准通过了检验和/试验。当产品未能通过某种检验和/或试验时,应执行不合格品控制程序(见 4.13)。

记录应标明负责合格产品放行的授权检验者(见 4.16)。

建议供方保证测试结果按有关规格说明书中的规定进行记录。

4.11 检验、测量和试验设备的控制

4.11.1 总则

供方对其用以证实产品符合规定要求的检验、测量和试验设备(包括试验软件)应建立并保持控制、校准和维修的形成文件的程序。检验、测量和试验设备使用时,应确保其测量不确定度已知,并与要求的测量能力一致。

如果试验软件或比较标准(如试验硬件)用作检验手段时,使用前,应加以校验,以证明其能用于验证生产、安装和服务过程中产品的可接收性,并按规定周期加以复检。供方应规定复检的内容和周期,并保存记录作为控制的证据(见 4.16)。

在检验、测量和试验设备的技术资料按要求可以提供的场合,当顾客或其代表要求时,供方应提供这些资料,以证实检验、测量和试验设备的功能是适宜的。

注:在本标准中,术语"测量设备"包括测量装置。

供方使用工具、设备和技术进行测试,来验证软件产品是否符合规定的要求,当批准它们时,供方应考虑工具对软件产品的影响。此外,这些工具在使用之前最好置于配置管理之下。

测试工具和技术的使用范围最好形成文件,对它们的使用情况按规定的间隔复查,以确定是否需要改进和/或使它们升级。

注:为了得到更多信息,参看 ISO/IEC12207:1995 的 7.2 条。

4.11.2 控制程序

供方应:

a) 确认测量任务及所要求的准确度,选择适用的具有所需准确度和精密度的检验、测量和试验设备;

b) 确认影响产品质量的所有检验、测量和试验设备,按规定的周期或使用前对照与国际或国家承认的有关基准,有已知有效关系的鉴定合格的设备进行校准和调整,当不存在上述基准时,用于校准的依据应形成文件;

c) 规定校准检验、测量和试验设备的过程,其内容包括设备型号、唯一性标识、地点、校验周期、校验方法、验收准则,以及发现问题时应采取的措施;

d) 检验、测量和试验设备应带有表明其校准状态合适的标志或经批准的识别记录;

e) 保存检验、测量和试验设备的校准记录(见 4.16);

f) 发现检验、测量和试验设备偏离校准状态时,应评定已检验和测试结果的有效性,并形成文件;

g) 确保校准、检验、测量和试验有适宜的环境条件;

h) 确保检验、测量和试验设备在搬运、防护和贮存期间,其准确度和适用性保持完好

i) 防止检验、测量和试验设备(包括试验硬件和软件),因调整不当而使校准失效。

注:ISO10012 所提供的测量设备的计量确认体系可以用作指南。

校准是一种不直接适用于软件的验证技术。然而,它可以适用于测试和确认软件的硬件和工具。结果是,上述方框中 b)到 g)项不适用于软件本身,但在测试软件时可用于测试环境。

4.12 检验和试验状态

产品的检验和试验状态应以适当的方式加以标识,标明产品经检验和试验后合格与否。在产品生产、安装和服务整个过程中,应按质量计划和/或形成文件的程序中的要求,保护好检验和试验状态的标识,以确保只有通过了规定的检验和试验的[或授权让步放行的(见 4.13.2)]产品才能发出、使用或安装。

供方最好有标识产品组件的开发阶段和测试状态的方法。例如:未经测试的;已经测试但有错的;已成功地测试或批准放行至进一步开发活动的。构造的产生或软件项在开发、测试和工作环境之间的流动可用来表明此状态。检验和测试记录也可用来标识检验和试验状态。

注:为了得到更多信息,参看 ISO/IEC12207:1995 的 6.2 条。

4.13 不合格品的控制

4.13.1 总则

供方应建立并保持不合格品控制的形成文件的程序,以防止不合格品的非预期使用或安装。应控制不合格品的标识、记录、评价、隔离(可行时)和处置,并通知有关职能部门。

在软件开发中,不合格项的隔离可通过将编制出的软件项从生产环境或测试环境转入隔离环境来实现。如果是嵌入式软件,可能有必要将包含不合格软件的不合格项(硬件)也隔离出来。

供方应规定在哪些点需要控制和记录不合格产品。当软件项在开发或维护过程中暴露出缺陷时,对这类缺陷的调查和解决应加以控制并记录。

可以调用配置管理过程来实现部分或全部要求。

注:为了得到更多信息,参看 ISO/IEC12207:1995 的 6.2 和 6.8 条。

4.13.2 不合格品的评审和处置

应规定对不合格品进行评审的职责和处置的权限。

应按照形成文件的程序评审不合格品,评审后可能:

a) 进行返工,以达到规定要求;

b) 经返修或不经返修作为让步接收;

c) 降级改作它用;

d) 拒收或报废。

合同要求时,供方若要使用或返修不符合规定要求的产品(见 4.13.2b)应向顾客或其代表提出让步申请。同意后,应记录不合格和返修情况,以说明不合格品的实际状况(见 4.16)。

返修和/或返工后的产品应按质量计划和/或形成文件的程序重新检验。

在不合格品的处置中,应注意下述情况:

a) 任何暴露的问题及对软件其他部分可能的影响应记录并通知负责人员,以便跟踪问题直至解决;

b) 受修改影响的区域应加以识别并重新测试;确定重新测试范围的方法应在形成文件的规程中规定;

c) 不合格产品的等级。

对软件来说,为满足规定要求的修订或返工产生新的软件版本。在软件开发过程中,可通过以下方法来处理不合格品:

a) 对其返修或返工(即修复缺陷)以满足要求;

b) 通过协商确定是否接受修改;

c) 在对要求进行修改后,视为合格产品;

d) 拒绝接受。

4.14 纠正和预防措施

4.14.1 总则

供方应建立并保持实施纠正和预防措施的形成文件的程序。

为消除实际或潜在不合格原因所采取的任何纠正或预防措施,应与问题的重要性及所承受的风险程序相适应。

供方应执行和记录由纠正或预防措施所引起的形成文件的程序的任何更改。

当修改措施直接影响到软件产品时,可以调用配置管理过程进行控制。更改了软件生存周期过程的修改措施,最好经由管理机构评审,并且借助文件及数据控制程序来实施。

注:为了得到更多的信息,参看 ISO/IEC12207:1995 的 6.2、6.8 和 7.3 条。

4.14.2 纠正措施

纠正措施的程序应包括:

a) 有效地处理顾客的意见和产品不合格报告;

b) 调查与产品、过程和质量体系有关的不合格产生的原因,并记录调查结果(见 4.16);

c) 确定消除不合格原因所需的纠正措施;

d) 实施控制,以确保纠正措施的执行及其有效性。

不需要有与软件有关的进一步指南。

4.14.3 预防措施

预防措施的程序应包括:

a) 利用适当的信息来源,如影响产品质量的过程和作业、让步、审核结果、质量记录、服务报告和顾客意见,以发现、分析并消除不合格的潜在原因;

b) 对任何要求预防措施的问题确定所需的处理步骤;

c) 采取预防措施并实施控制,以确保有效性;

d) 确保将所采取措施的有关信息提交给管理评审(见 4.1.3)。

预防措施需借鉴对不合格产品产生原因的分析。那些旨在阻止软件的某些度量指标向不利方向改变的措施也可认为是预防措施。

4.15 搬运、贮存、包装、防护和交付

4.15.1 总则

供方应建立并保持产品的搬运、贮存、包装、防护和交付的形成文件的程序。

不需要有与软件有关的进一步指南。

注:为了得到更多的信息,参看 ISO/IEC12207:1995 的 5.2.7.1,5.3.13.2 和 6.2.6 条。

4.15.2 搬运

供方应提供防止产品损坏或变质的搬运方法。

软件的损坏意味着其内容的改变,受病毒感染的软件被认为是受损坏软件。

软件的内容本身不会变质,但存储信息的媒体可能受到损坏,建议供方采取适当的预防措施。

防止要交付的软件产品受病毒侵害,在"复制指南"中已作了描述。

4.15.3 贮存

供方应使用指定的贮存场地或库房,以防止产品在使用或交付前受到损坏或变质。应规定授权接收和发放的管理方法。

按适宜的时间间隔检查库存品状况,以便及时发现变质情况。

应建立一个系统,以便:

a) 存贮软件项;

b) 控制对软件项的访问;

c) 按已建立的基本资料维护产品的各种版本。

为保护产品的完整性,并为更改控制提供基础,软件项必须装载在下述环境中:

a) 保护它们免于未授权的更改或损坏;

b) 允许对软件母版及其拷贝进行受控检索。

应考虑计算机媒体的贮藏,特别是电磁和静电环境。

4.15.4 包装

供方应对装箱、包装和标志过程(包括所用材料)进行必要的控制,以确保符合规定要求。

为交付规定的适用于软件产品的包装要求,已作为复制指南的一部分进行了描述。在采用电子存贮的情况下,关于这一条可能没有实际活动。在包装时,可以对软件进行压缩和/或加密。

4.15.5 防护

当产品受供方控制时,供方应采用适当的防护和隔离措施。

应建立一个软件防护体系:

a) 软件的定期备份;

b) 保证及时将软件复制到可替换的媒体上;

c) 将软件媒体存储在受保护的环境中;

d) 软件媒体存入于备用环境中以保证受损后的恢复。

4.15.6 交付

在最终检验和试验后,供方应采取保护产品质量的措施。合同要求时,这种保护应延续到交付的目的地。

软件的交付可以是存放软件的媒体或是借助于电子传送。

在采用电子传送的情况下,需要注意保护软件免受病毒侵害。

为验证交付软件产品的复制件的正确性和完整性,应建立和维护形成文件化的规程。这些规程应提供适当的预防措施,以保护软件产品免于在交付期间损坏。此外,应有形成文件的规程用来证实已进行适当程度的软件病毒检查,并已采取适当措施来保护产品的完整性。

4.16 质量记录的控制

供方应建立并保持质量记录的标识、收集、编目、查阅、归档、贮存、保管和处理的形成文件的程序。

质量记录应予保存,以证明符合规定的要求和质量体系有效运行。来自分承包方的质量记录也应成为这些资料的组成部分。

所有的质量记录应清晰,保管方式应便于存取和检索,保管设施应提供适宜的环境,以防止损坏、变质和丢失。应规定并记录质量记录的保存期。合同要求时,在商定期内质量记录可提供给顾客或其代表评价时查阅。

注:记录可以呈任何媒体形式,如硬拷贝或电子媒体。

质量记录示例有:

✧ 测试结果;

✧ 问题报告;

✧ 更改请求;

✧ 带注释的文档;

✧ 评审记录;

✧ 会议记录;

✧ 审核报告。

当记录保存在电子媒体中时,考虑保存时间和记录的可访问性时应考虑到电子图像的退化速率,以及为访问记录所需的设备和软件的可用性。

注:为了得到更多信息,参看 ISO/IEC12207:1995 的 6.1.6.2 条。

4.17 内部质量审核

供方应建立并保持用于策划和实施内部质量审核的形成文件的程序,以验证质量活动和有关结果是否符合计划的安排,并确定质量体系的有效性。

内部质量审核应根据所审核的活动的实际情况和重要性来安排日程计划,并由与所审核的活动无直接责任的人员进行。

应记录质量审核结果(见 4.16),并提请受审核区域的责任人员注意。对审核时发现的问题,负责该区域的

管理人员应及时采取纠正措施。

在跟踪审核活动中,应验证和记录所采取纠正措施的实际情况及其有效性(见 4.16)。

注:内部质量审核的结果是管理评审活动(见 4.1.3)输入的一部分。

注:ISO10011 给出了质量体系审核的指南。

当供方开展多个项目的开发时,审核计划应确定项目的选择。应考虑逐步地覆盖供方的整个质量体系。这可通过在生存周期的不同阶段审核若干项目来实现。当某个单个项目正在消耗组织的大多数资源时,该项目的审核可以随其进展安排多次。当拟议中的项目更改其时间安排时,对内部审核计划安排应加以评审,或者更改审核的时间,或者考虑其他的项目。

供方内部审核员应考虑使项目质量计划与组织质量体系相协调。

注:为了得到更多信息,参看 ISO/IEC12207:1995 的 6.7,6.8 和 7.3.2 条。

4.18 培训

供方应建立并保持形成文件的程序,明确培训需求并对所有从事对质量有影响的工作人员都进行培训。对从事特殊工作的人员应按所要求的教育、培训和/或经历进行资格考核。应保存适当的培训记录(见 4.16)。

在确定培训要求时,应考虑软件产品开发和管理中需使用的专用工具、技术、方法和计算机资源。还可要求包括与软件有关的专门领域的技能和知识的培训。资格鉴定和培训要求应形成文档。

注:为了得到更多的信息,参看 ISO/IEC 12207:1995 的 7.4 条。

4.19 服务

在规定有服务要求的情况下,供方应建立并保持对服务的实施、验证和报告形成文件程序,以使服务满足规定要求。

在本标准中所提及的服务是与软件项目有关的服务:维护和顾客支持。顾客支持在 ISO 9000-2 中描述。

软件产品的维护活动通常划分为以下几类:

a) 问题解决:此类维护包括对引起运行问题的软件进行检查和分析,并纠正潜在的软件缺陷。解决问题时,临时修补可减少停机时间,并在此后完成永久性改进。

b) 接口修改:当对受软件控制的硬件系统或组件进行增补或更改时,可能需要修改接口。

c) 功能扩展或性能改进。

对于接口修改和功能扩展来说,根据工作量,应采用更改控制规程的方法,或应起动新的与原项目不同的开发项目,这样就会涉及本标准的全部内容。因此,本条中所述的维护活动只限于解决问题(通常称为纠正性维护)。

当顾客要求在初始交付和安装之后对软件产品维护时,应在合同中作出规定。为进行维护活动并证明这种活动符合规定的维护要求,供方应建立并维持形成文档的规程。维护活动也可以是对开发环境、工具和文档的维护。

需维护的项目以及维护的时间周期应在合同中规定。这种项目的示例如下:

a) 规程;

b) 数据及数据结构;

c) 规格说明;

d) 顾客和/或用户文档;

e) 供方的使用文档;

f) 测试计划。

所有维护活动应按照供主和顾客事先确定和协商一致的维护计划和/或规程实施和管理。计划应尽可能包括下述内容:

a) 维护范围;

b) 产品初始状态的标识;

c) 支持组织;

d) 维护活动;

e) 维护记录和报告;

f) 配置管理活动;

g) 建议的进度安排。

尽可能记录并保存维护活动。维护报告的提交规则应由供方和顾客建立并协商一致。

对于正在进行维护的每一软件产品,维护记录应尽可能包括下述项目:

a) 已收到的问题报告以及各自的目前状况;

b) 负责答复协助请求或实施适当纠正措施的组织;

c) 纠正措施的优先次序;

d) 纠正措施的结果;

e) 失效发生和维护活动的统计数据。

维护活动的记录可以用于软件产品的评价和加固以及质量体系本身的改进。

注:为了得到更多的信息,参看 ISO/IEC 12207:1995 的 5.4.4,5.5 和 6.8 条。

4.20 统计技术

4.20.1 *确定需求*

对确定、控制和验证过程能力以及产品特性所需的统计技术,供方应明确其需求。

4.20.2 *程序*

供方应建立并保持形成文件的程序,以实施 4.20.1 中确定的统计技术,并控制其应用。

统计技术可用来分析过程能力和产品特性的度量,目的是产生可用于评价产品质量和过程能力的数据。当资料数据定量地表示时,可用来评价是否符合质量要求。

可应用统计技术的产品特性示例有:

✧ 可测试性;

✧ 易用性;

✧ 可靠性;

✧ 可维护性;

✧ 有效性。

可应用统计技术的软件过程能力特性示例有:

✧ 程成熟度;

✧ 过程输出中的缺陷类型和数目;

✧ 缺陷清除效率;

✧ 重大的能力下降。

"量度"这一术语指可度量的特性。

量度应符合下述原则:

a) 量度应得出过程或产品的量值;

b) 量度已明确定义;

c) 理解与软件产品质量或开发过程质量有关的量度含义;

d) 可能影响量度的方面(比如更改设计和开发技术)已明确;

e) 理解指示质量改进的量度变化方向。

和所采用的量度方法无关,重要的事情是知晓其水平并将其用于控制和改进,而不是采用哪种特殊的量度方法。

不同的过程量度可能适合于同一供应方生产的不同的软件产品。

注:可以在 ISO/IEC9126 中找到更多的指导。

附录 A 参考文献(标准件)

(1) ISO9000-2:1997 "质量管理和质量保证标准"——第二部分:ISO9001、ISO9002、ISO9003 应用通用指南

(2) ISO10005:1995"质量管理"——质量计划指南
(3) ISO10006:"质量管理"——项目管理质量指南
(4) ISO10007:1995 "质量管理"——配置管理指南
(5) ISO10011——1:1991 "质量体系审核指南"——第一部分:审核
(6) ISO10011——2:1991 "质量体系审核指南"——第二部分:质量体系审核员资格确认准则
(7) ISO10011——3:1991 "质量体系审核指南"——第三部分:审核程序管理
(8) ISO10012——1:1992 "测量设备质量保证要求"——第一部分:测量设备的计量确认体系
(9) ISO10013:1995 "质量手册编制指南"
(10) ISO/IEC 9126:1991 信息技术——软件产品评价,质量特性及其使用指南
(11) ISO/IEC 12207:1995 信息技术——软件生存周期过程
注:其中(3)待发布。
附录 B ISO9000——3 与 ISO/IEC12207 的对照索引表
本对照表:
• 指出了 ISO/IEC12207 与 ISO9001 相符的有助于质量体系建立的一些条目;
• 集中了本标准各节中的"注";
•并未完整地描述 ISO/IEC12207 如何覆盖 ISO9001 的要求,以及反之,ISO9001 如何覆盖 ISO/IEC12207 的要求。

ISO9000——3 ISO/IEC12207

表 1

ISO9000——3 ISO／IEC12207

4.1.2	7.2,6.3.1.6
4.1.3	7.4
4.2.3	6.2,6.3,6.4,6.5
4.3.2	5.2.1,5.2.6,6.4.2.1
4.3.3	5.1.3.5,5.2.3.2
4.4.2	5.2.4
4.4.3	5.2.6.1,6.6.2
4.4.4	5.3.2.5,3.3,5.3.4
4.4.5	5.3.5,5.3.6,5.3.7
4.4.6	5.3.4.2,5.3.5.6,5.3.6.7,6.6.3
4.4.7	5.3.4.2,5.3.5.6,5.3.5.7,5.3.7.5,5.3.9,6.4
4.4.8	5.3.1,6.5
4.4.9	5.5.2,5.5.3,6.2.3
4.5.1	6.1
4.6.1	5.1
4.7	6.1
4.8	6.1,6.2
4.9	5.3.12,6.3.3
4.10.1	5.1.5,5.3.5.5,5.3.6.5,5.3.6.6,5.3.7,5.3.8,5.3.9,5.3.10,5.3.11,5.3.13
4.11.1	7.2
4.12	6.2
4.13.1	6.2,6.8
4.14.1	6.2,6.8,7.3
4.15.1	5.2.7.1,5.3.13.2,6.2.6
4.16	6.1.6.2
4.17	6.7,6.8,7.3.2
4.18	7.4
4.19	5.4.4,5.5,6.8