

中华人民共和国国家标准

GB/T 20918—2007

信息技术 软件生存周期过程 风险管理

Information technology—Software life cycle processes—
Risk management

2007-04-30 发布

2007-07-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前言	Ⅲ
引言	Ⅳ
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 本标准的应用	4
5 软件生存周期中的风险管理	4
附录 A (资料性附录) 风险管理计划	11
附录 B (资料性附录) 避险措施请求	13
附录 C (资料性附录) 风险处理计划	14
参考文献	15

前 言

本标准的附录 A、附录 B 和附录 C 为资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位：中国电子技术标准化研究所。

本标准主要起草人：陈静、韩红强、王玮、杨根兴。

引 言

软件风险管理是进行有效决策并与软件组织交流结果的关键准则。风险管理的目的在于,在潜在的管理和技术上的问题出现以前对其加以标识,以便采取措施减少或排除这些问题出现的概率和/或影响。风险管理是一个关键工具,有助于持续地确定项目计划的可行性,改进对于那些影响软件生存周期活动和软件产品质量与性能的潜在问题所进行的查找和识别,改进对于软件项目的积极管理。

成功地实施本标准,可:

- 标识潜在问题;
- 了解这些风险的概率和后果;
- 确定所涉及风险的优先次序;
- 给出超出其风险阈值的每个潜在风险可供选择的处理建议;
- 对超出其阈值的风险选择合适的处理措施;
- 监督每项处理措施的有效性;
- 获取信息来改进风险管理策略;
- 定期评价并改进风险管理过程和规程。

本标准支持软件产品和服务的获取、供应、开发、运行和维护。本标准是为那些负责组织中定义、策划、实施或支持软件风险管理的人员而编写的。使用领域、软件项目或产品所在的软件生存周期的阶段和组织的具体特性将影响本标准在实践中的应用。

本标准定义了一个适用于所有与软件有关的工程和管理准则的持续的软件风险管理过程。风险管理过程由许多重复运行的活动和任务组成。该过程定义了风险管理过程的最小活动集、要求的和获取的风险管理信息及其在管理风险中的用法。本标准所定义的风险管理过程适用于在组织级或项目级使用,也适用于不同类型和规模的项目及处在不同生存周期阶段的项目,并支持不同共利益者的观点。由于个别组织和项目将对本标准进行剪裁以满足其具体情况和需要,因此,本标准不规定为实施风险管理的任何具体风险管理技术或相关组织结构的用法。本标准的用户可参考 IEC Std 60812:1985、IEC Std 61025:1990 或 IEC Guide 60300-3-9:1995 的指南来选择和使用不同的风险分析技术与方法。然而,本标准无保留地支持使用能使风险管理成为一个持续过程的工具和技术。鼓励项目中的所有相关人员以电子形式获取并交流与风险有关的信息。

本标准可单独使用,也可与 GB/T 8566 一起使用。

当单独使用本标准时,本标准提供了对应用于整个软件生存周期的软件风险管理过程的完整且自包含的描述。

当本标准与 GB/T 8566 一起使用时,本标准在 GB/T 8566—2007 所定义的软件生存周期过程集合中增加了一个管理风险的过程。这意味着本标准假定涉及风险处理的活动遵从 GB/T 8566 的管理惯例。因此,典型的风险处理将使用相同的管理措施。

本标准持这样的观点,软件风险管理是软件工程技术和管理过程的重要组成部分,它不能由一个单独的组织元素执行。如果出于某些原因,例如:由于软件项目的规模和性质、包含的风险的大小和数量,或者将不遵循 GB/T 8566,而要求由一个单独的组织元素来执行风险处理,则本标准仍适用。

为便于与 GB/T 8566 标准一起使用,本标准按 GB/T 8566 的术语和格式进行编写。

信息技术 软件生存周期过程 风险管理

1 范围

1.1 目的

本标准描述了软件获取、供应、开发、运作和维护过程中的风险管理过程。建议整个组织中的技术和管理人员都使用本标准。

本标准的目的是为软件供方、需方、开发者和管理者提供适合于管理广泛、多样的风险的一组过程要求。本标准不提供详细明确的风险管理技术,但致力于定义一个任何技术都可应用于其中的风险管理过程。

1.2 应用领域

本标准定义了一个贯穿于软件生存周期的风险管理过程。它适合由组织采用,用于所有适当的项目或单个项目。尽管本标准是为软件项目中的风险管理而编写的,但它也可用于系统级或组织级风险的管理。

本标准可以与 GB/T 8566 一起使用,也可以单独使用。

1.2.1 与 GB/T 8566 一起使用

GB/T 8566 描述了软件的获取、供应、开发、运作和维护的标准过程。该标准考虑到积极地管理风险是成功进行软件项目管理的关键因素。GB/T 8566 标准中多处提到风险和风险管理,但却没有给出风险管理的过程。本标准给出了这个过程。为了支持管理者、参与者和其他共利益者等各方的观点,在任何领域或生存周期阶段,本标准都可用于管理组织级风险或者项目级风险。

在由 GB/T 8566 所给出的生存周期过程框架中,风险管理是一个“组织的生存周期过程”。在一个组织级生存周期过程中,使用该过程的组织负责该过程中的活动和任务。因此,组织应确保过程存在并发挥作用。

当和 GB/T 8566 一起使用时,本标准假定 GB/T 8566 的其他管理和技术过程执行风险处理,并描述与这些过程的正确关系。

1.2.2 单独使用本标准

本标准可以不依赖于任何特定的软件生存周期过程标准而单独使用。当以这种方式使用时,将运用本标准风险处理的附加条款。

1.3 符合性

组织或项目在计划中列出并执行本标准第 5 章中描述的活动和任务中的所有要求(用“应”规定为必须执行的),就可以声称符合本标准。

在不依赖于 GB/T 8566 而使用本标准的那些实例中,有关风险处理的附加要求在 5.1.4.2 中给出。

1.4 免责声明

本标准建立了软件风险管理过程、活动和任务的最小要求集。实施这些要求,或根据本标准编写软件风险管理计划或软件避险措施请求,并不能确保与软件相关的风险或其他风险消失。符合本标准的任一团体并不能免除任何社会、道德、财务或法律的责任。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有

的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 8566 信息技术 软件生存周期过程(GB/T 8566—2007, ISO/IEC 12207:1995、ISO/IEC 12207/Amd.1:2002、ISO/IEC 12207/Amd.2:2004, IDT)

GB/T 18492—2001 信息技术 系统和软件完整性级别(idt ISO/IEC 15026:1998)

3 术语和定义

下列术语和定义适用于本标准。

3.1

后果 consequence

事件的结果。

注1:一个事件可能有多个后果。

注2:后果可能是正面的,也可能是负面的,然而,安全方面的后果总是负面的。

注3:后果可以定量或定性地表示。

3.2

事件 event

一组特定情形的出现。

注1:事件可能是确定的,也可能是不确定的。

注2:事件可能是单个出现,也可能是一系列出现。

注3:事件发生的概率可在一段时间内进行估计。

3.3

相关方 interested party

对一个组织的业绩或成就感兴趣的个人或团体。例如:顾客、所有者、组织内的人员、供方、银行家、合作伙伴和社团。

注:团体可包括一个组织、组织的一部分或多个组织。

3.4

概率 probability

事件可能发生的程度。

注1:ISO 3534-1:1993中的1.1给出了概率的数学定义:随机事件的概率是0~1之间的一个实数,它与很长时间内事件发生的相对频率有关,或与事件可能发生的置信度有关。对于高置信度的事件,其概率接近于1。

注2:描述风险时可以使用频率,而不使用概率。

注3:可用类别或等级来选择概率的置信度,如:稀少、不一定、中等、很可能、几乎一定,或者难以置信、不太可能、可能性极小、偶然、很可能、频繁的。

3.5

项目风险概要 project risk profile

项目当前的和历史上的与风险相关的信息;在一个项目中,所有单个风险概要的摘要或汇集。

注:项目风险概要信息包括风险管理环境,按年代顺序排列的风险记录及它们的单个风险概要、优先次序、风险相关的测度、处理状态、应急计划和避险措施请求。项目风险概要包括所有单个风险的风险概要的集合,还包含当前的和历史上的风险状态。见风险概要和风险状态。

3.6

风险 risk

事件的概率及其后果的组合。

注1:术语“风险”通常仅用于至少存在负面后果可能性的情形。

注2:在某些情况下,风险从偏离期望的结果或可能的事件中产生。

注3：见 ISO/IEC 指南 51 中与安全有关的议题。

3.7

风险接受 risk acceptance

接受风险的决定。

注：风险接受取决于风险准则。

3.8

避险措施请求 risk action request

对于所确定的超过阈值的一个或多个风险而建议的处理可选方案和支持信息。

3.9

风险类别 risk category

对风险源类型的描述(例如,技术、法律、组织、安全、经济、工程、费用和进度)。

3.10

风险准则 risk criteria

评估风险重要性所引用的条款。

注：风险准则包括相关代价和利益、法律和法定需求、社会经济和环境方面、共利益者关系、优先权及其他评估输入。

3.11

风险预估 risk exposure

风险给个人、项目或组织造成的潜在损失；风险出现概率及其出现后果大小的函数。

注：风险预估通常定义为概率和后果大小的乘积，即，预期值。本标准采用包括风险预估的定性表示的更广义的观点。

3.12

风险管理计划 risk management plan

对一个组织或项目内执行风险管理过程的要素和资源如何实施的描述。

3.13

风险管理过程 risk management process

在整个产品或服务的生存周期中，系统地标识、分析、处理和监督风险的一个持续的过程。

3.14

风险管理体系 risk management system

在组织的管理体系中涉及管理风险的要素的集合。

注1：管理体系要素可包括战略策划、决策和处理风险的其他过程。

注2：风险管理体系中反映组织文化。

3.15

风险概要 risk profile

一个风险的当前的和历史上的风险状态信息按年代顺序排列的记录。

3.16

风险状态 risk state

与单个风险有关的项目风险信息。

注：涉及单个风险的信息可包括当前描述、起因、概率、后果、估计范围、估计置信度、处理、阈值及风险达到其阈值时间的估计。

3.17

风险阈值 risk threshold

引发一些共利益者采取措施的条件。

注：基于不同的风险准则，可以为每个风险、风险类别和风险组合定义不同的风险阈值。

3.18

风险处理 risk treatment

选择并实施缓解风险的措施的过程。

注1：术语“风险处理”有时用于表示一些风险处理措施。

注2：风险处理措施包括避免、缓解、转移或接受风险。

3.19

(风险)源 source

具有潜在后果的项或活动。

注：在安全的环境中，源是一个危险(引用 ISO/IEC 指南 51:1999)。

3.20

共利益者 stakeholder

对风险产生影响、受风险影响或感到自己受风险影响的任何个人、团体或组织。

注1：决策人员也是共利益者。

注2：术语“共利益者”包括有关当事人，但比其含义更广(当事人在 ISO 9000:2000 中定义)。

4 本标准的应用

为便于和 GB/T 8566 一起使用，本标准用与 GB/T 8566 的过程描述相同的约定编写。这里讨论的风险管理生存周期过程可分为一系列活动，每个活动的需求又规定为一系列任务。二级条(×.×)表示过程，三级条(×.×.×)表示活动，四级条(×.×.×.×)表示任务。

在 GB/T 8566 所给出的软件生存周期过程框架中，风险管理是一个“组织级生存周期过程”。在一个组织级生存周期过程中，使用该过程的组织负责该过程中的活动和任务。组织应确保过程存在并发挥作用。

本标准支持软件产品和服务的获取、供应、开发、运作和维护。应用本标准不需特殊的软件生存周期过程模型。

软件风险管理在与组织的风险管理过程一起使用时最有效。本标准的过程、活动和任务应与组织的其他风险管理的惯例和系统融为一体。如果组织没有风险管理过程，本标准也可作为建立组织风险管理过程的指南。

此外，虽然本标准的应用集中于软件风险，但该过程也应与组织的问题管理方法相结合并协调一致，例如，在必须实施应急计划的情况下，风险处理活动应以与其他项目管理活动相同的方式进行管理。

5 软件生存周期中的风险管理

5.0 风险管理目的

风险管理的目的在于持续地标识并缓解风险。成功实施风险管理的结果为：

- a) 确定了风险管理的执行范围；
- b) 定义并实施了适当的风险管理策略；
- c) 在策略中标识了风险，并在项目执行期间随其进展标识风险；
- d) 分析风险，确定了使用有关资源来监督这些风险的优先次序；
- e) 定义、应用并评估了风险测试，以便确定风险状态的变更和监督活动的进展；
- f) 采取了适当的措施来减缓或避免风险的影响。

5.1 风险管理过程

在整个产品或服务的生存周期中，风险管理过程是一个持续地系统地处理风险的过程。

该过程包括下列活动：

- a) 策划并实施风险管理；

- b) 管理项目风险概要；
- c) 执行风险分析；
- d) 执行风险监督；
- e) 执行风险处理；
- f) 评价风险管理过程。

风险管理过程如图 1 所示。注意，假定执行风险处理是全部技术和管理过程的一部分。

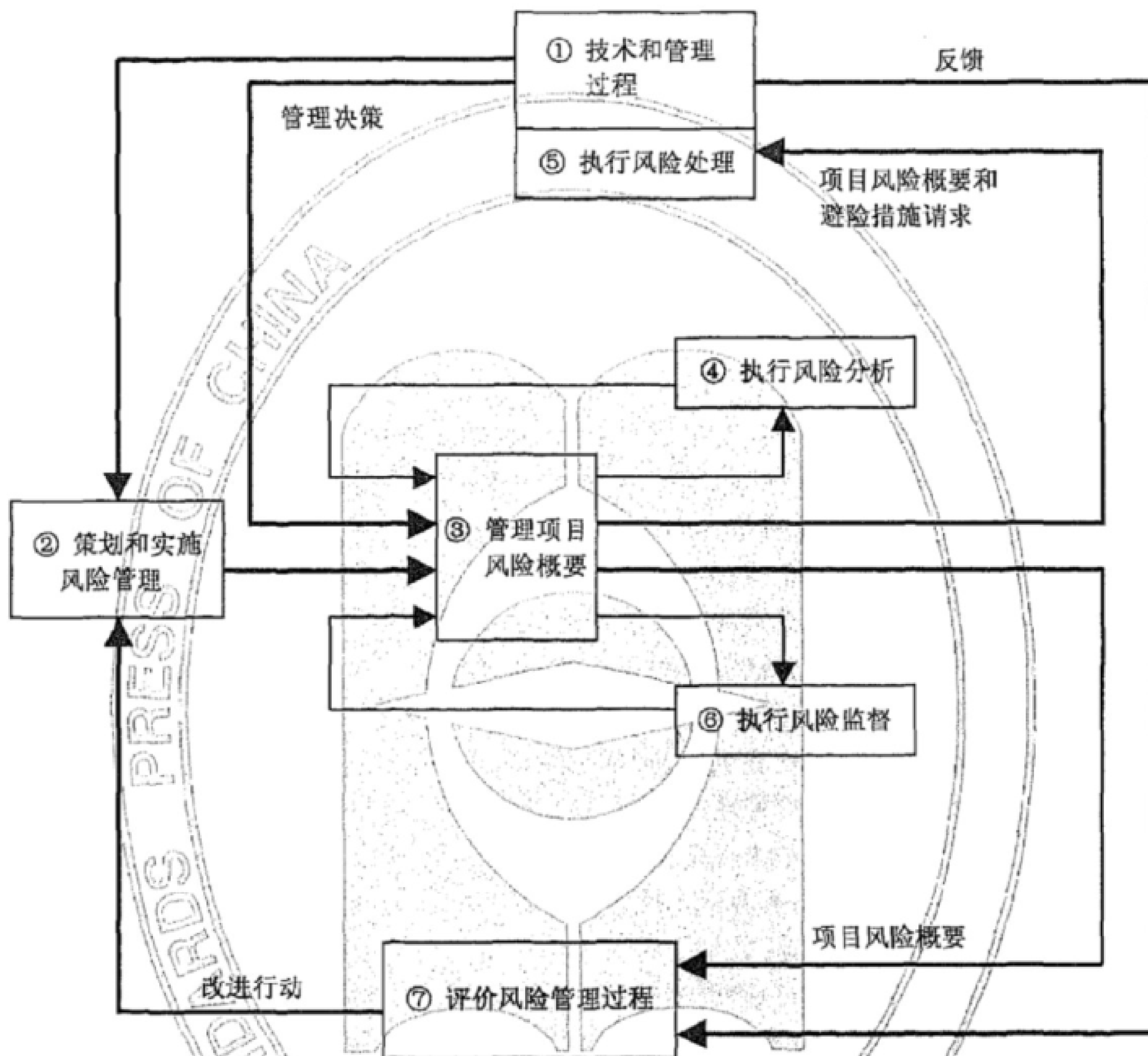


图 1 风险管理过程模型

下面论述中的数字表示图 1 中相应的方框。

涉及共利益者的管理和技术过程定义了风险管理过程必须支持的信息需求（即：共利益者需要做出涉及风险的决定的信息）①。将这些信息需求传递给“策划和实施风险管理”和“管理项目风险概要”活动。在“策划和实施风险管理”活动②中，定义了将执行的风险管理的总的方针政策、要使用的规程及要应用的专门技术等。

在“管理项目风险概要”活动③中，收集当前的和历史的风险管理环境及风险状态信息。项目风险概要包括所有单个风险概要（即：关于单个风险的当前的和历史的风险信息）的汇总，及所有的风险状态。

“执行风险分析”活动④识别风险，确定其可能性及结果，确定其风险预估，并为已确定的将超出风险阈值的风险准备避险措施请求的处理建议。在整个“执行风险分析”活动中，持续地更新和维护项目风险概要信息。

将处理建议与其他风险状态及其处理状态一起送至管理部门⑤进行评审。对发现的任何不可接受

的风险,管理部门决定执行什么风险处理,为要求处理的风险制定风险处理计划,使这些计划与其他管理计划和其他正在进行的活动相协调。

在“执行风险监督”活动⑥期间,持续地对所有风险进行监督,直到不再需要监督为止。此外,要寻找新的风险和新的风险源。

要求定期评价风险管理过程,以确保其有效性。在“评价风险管理过程”活动⑦中,为改进过程或改进组织的或项目的能力以管理风险,收集用户的和其他的反馈信息。在“策划和实施风险管理”活动②中,实施作为评价结果规定的改进。

在整个产品生存周期中,持续地应用软件风险管理过程。不过,一旦风险管理过程开始,风险管理过程的活动和任务就以迭代的方式与单个风险交互作用。例如,在执行风险分析活动④中,在评价任务本身时,由于获取的风险方面的知识的增加,使得在执行风险评价期间,风险可能被重新估计好几次。风险管理过程不是“瀑布”过程。

5.1.1 策划并实施风险管理

“策划和实施风险管理”活动的目的在于建立一个软件风险管理过程。只要建立了组织风险管理过程,相应的软件风险管理过程就宜与之相匹配。本活动应确定执行风险管理的人员,定义所要使用的特殊风险管理过程,分配实施过程所需的资源,并定义如何在共利益者间沟通和协调风险及其处理。

本活动宜在项目的开始就执行。活动中所产生的信息应记录在类似附录 A 的风险管理计划中。

注: IEEE Std 1058:1998 要求,在软件项目管理计划中应有风险管理计划的文档集。

本活动包含 5.1.1.1~5.1.1.5 中所列的任务。

5.1.1.1 确定风险管理方针

应明确定义描述风险管理的风险管理方针。在这些方针下,风险管理得以执行。这些方针应支持收集共利益者所需的风险相关信息。这些方针宜涉及:

- a) 管理和人员如何实施、监管并支持风险管理;
- b) 如何获取并维护共利益者正在进行的风险管理承诺;
- c) 如何协调共利益者间的风险管理过程;
- d) 如何完成风险管理过程中的人员定位和培训;
- e) 共利益者如何、多长时间沟通并评审风险信息,例如项目风险概要;
- f) 如何使资源可用于处理风险。

只要可行,政策宜与现有的组织风险管理政策相结合。可以引用定义上述政策的已形成文档的组织风险管理政策,但是项目的特征要形成文档。

5.1.1.2 确定风险管理过程

要实施的风险管理过程的描述应形成文档并予以公布。实施风险管理过程的规程描述宜包括:

- a) 对风险进行重新分析和监督的频率;
- b) 要求的风险分析类型(定量和/或定性);
- c) 用于估计风险概率和后果的标度和说明,以其测量不确定性;
- d) 使用的风险阈值类型;
- e) 用于追踪和监督风险状态的测度类型;
- f) 风险处理的优先顺序如何;
- g) 风险管理过程支持的共利益者的看法;
- h) 需考虑的风险源和风险种类。

在这个任务中,宜选择与项目情况匹配的风险管理过程、特殊规程和技术。

注: IEC 60300-3-9:1995 指南提供了选择和使用常用的风险分析技术的指南。IEC Std 61508-7:2000 提供了与测度有关的有用材料和与软件安全性有关的技术。

只要可行,风险管理过程宜与现有的组织风险管理过程密切结合。可以引用定义了前面所列内容

的已形成文档的组织风险管理过程,但是项目的特征要形成文档。

5.1.1.3 确定职责

应明确地标识负责执行风险管理的部门及其角色和职责。在组织单位内,应指定部门负责风险管理过程。

5.1.1.4 分配资源

应给予负责部门足够的资源来执行风险管理过程。

5.1.1.5 确定风险管理过程评价

应给出有关评价和改进风险管理过程的过程描述,以及获取什么样的信息以总结经验教训。任何运用本过程之前获得的经验教训都宜加入到本过程的实现中。

5.1.2 管理项目风险概要

“管理项目风险概要”活动的目的在于产生一个随着风险处理而展开的历史的和当前协调的风险呈现视图,使风险能充分、简洁地与相关的共利益者沟通。它包括风险管理环境、当前风险状态及风险历史。

在整个软件生存周期内应对项目风险概要进行维护。

本活动包含 5.1.2.1~5.1.2.4 所列的任务。

5.1.2.1 定义风险管理环境

应定义风险管理过程环境,并形成文档。

风险管理环境的定义应包括避险措施请求支持的一个或多个共利益者观点的描述,以及要对其进行管理的一个或多个风险种类。对于特别重要的软件安全保密性、安全性或其他种类的软件风险可分别进行说明。

注:可将 IEEE Std 1228:1994、IEC Std 60300 系列标准、IEC Std 61508 系列标准和本标准一起用于说明与软件安全性有关的风险。

风险管理环境的定义也应包括下列技术和管理上的描述:

- a) 目标(例如,项目成功所必须满足的关键技术、政治或经济性能准则是什么?);
- b) 假定(例如,除项目控制之外还应考虑的?);
- c) 约束条件(例如,对项目进行了什么限制?)。

也宜包括可能影响风险分析或风险处理(例如,项目是否能公开地沟通与风险相关的信息,或是否有原因禁止)的任何其他相关信息。

5.1.2.2 确定风险阈值

定义风险接受条件的风险阈值应在每个风险的风险状态中定义并形成文档。风险阈值是无需共利益者明确评审便可接受的受测风险准则的最大级别。应为单个风险或风险组合定义风险阈值。也应给作为一个整体的项目定义风险阈值。宜依照 GB/T 18492—2001 的规定,从系统完整性级别推导出软件的风险阈值。也可根据成本、进度、技术和其他相关后果或预估值定义风险阈值。

表明某个风险何时可能超过其风险阈值的测度应在其风险状态中定义并形成文档。

注:IEEE Std 1012:1998 描述了在策划验证和确认活动时如何使用完整性级别。GB/T 18492—2001 论述了软件完整性级别的用法。IEC 61508-5:1998 提供了确定安全性完整性级别的方法。

5.1.2.3 确定并维护项目风险概要

应确定并维护项目风险概要。项目风险概要包括全部的项目风险信息、所有单个风险的风险概要的汇集,也包括当前的和历史的的风险状态。项目风险概要至少应包括:

- a) 风险管理环境;
- b) 按时间顺序排列的每个风险状态的记录,包括它们的概率、后果和风险阈值;
- c) 根据共利益者提供的风险准则而定的每个风险的优先次序;
- d) 避险措施请求及其处理状态。

概要宜包括每个风险的详细描述、其原因、所用的估计标度、用于评价状态的与风险相关的测度、应急计划,以及在风险状态中获得的其他与风险相关的信息。

当单个风险的状态例如其描述、预估或处理有一些变更,风险管理环境出现变更,或标识了一个新风险时,应对项目风险概要进行更新。宜以电子形式获取信息,以便于获取、沟通和评估。

5.1.2.4 沟通风险状态

应根据共利益者的要求,定期与其沟通项目风险概要或相关的风险概要(例如,单个风险或风险组合)。宜尽可能广泛地使所有共利益者利用风险状态信息。

5.1.3 执行风险分析

“执行风险分析”活动的目的在于:

- a) 标识产生风险的诱发事件、危险、威胁或情况;
- b) 估计发生概率、每个风险的后果及预期的时刻;
- c) 根据适当的阈值,评价每个风险或已定义的风险组合,产生处理超出阈值的风险的可选方案,并根据优先顺序做出处理建议。

在整个软件生存周期中应持续地执行风险分析。

本活动包含 5.1.3.1~5.1.3.3 所列的任务。

5.1.3.1 风险标识

应以风险管理环境中的类别来标识风险。还应标识风险管理环境中的变更,例如,由于假设中的变更而导致的附加风险。

宜使用不同的方法来标识风险,包括使用风险调查问卷、分类法、头脑风暴法、情景分析、吸取教训、原型法或其他所知的获取方法。可重复的标识过程可用于帮助吸取教训。只要可能,宜标识会产生风险的各种事件、危险、威胁或情况,从而有助于将来的风险处理。未标识的风险是隐含地接受。

使用风险类别宜保持一致,以有效地与共利益者沟通。可把相关的风险合并,从而易于分析、监督和处。宜把软件异常、软件测度报告和其他指标作为风险源进行连续地评审。

注: IEEE Std 1044:1993 规定了异常分类的可用信息。IEEE Std 982.1:1998 规定了与可靠性相关的软件测度的可用信息。

5.1.3.2 风险估计

应估计每个已标识风险的发生概率和后果。

可定量估计,也可定性估计。共利益者宜定义哪些风险将使用定性标度进行评价,哪些风险将使用定量标度进行评价。

使用估计风险概率和后果的标度应保持一致。宜在风险管理计划中描述所用的标度中固有的描述不确定性和测量不确定性。风险估计中的置信等级宜在其风险状态中获得。

5.1.3.3 风险评价

应依据风险阈值对每个风险进行评价。风险宜单独评价、综合评价、以及与系统和企业风险的相互影响一起评价。宜依据项目风险阈值评价风险,以确保风险组合在低于其单个阈值时,不会把项目作为一个整体置于不可接受的风险状态。可用不同的技术来评价风险,如决策树、场景策划、博弈论、概率分析和线性规划法。

应确定风险的优先顺序——由共利益者确定排序准则。当预计风险要成为问题时,优先权可以以风险预估、与风险相关的测度或某些其他一致的准则为基础。

为了降低或消除风险,宜考虑论述风险的不同的可选的处理方案。对于超出其风险阈值的每个风险,应在如附录 B 中给出的避险措施请求中定义建议的处理策略,如消除风险、降低其出现的概率或后果的严重性,或接受风险并形成文档。宜为所有超出其阈值的风险制定应急计划。也应定义表明可选的处理方案的有效性的测度。应将风险、其建议的处理和风险处理有效性的测度与共利益者沟通,由其批准、拒绝或修改。

注：IEEE Std 982.1:1988 提供了可能在定义与风险相关的测度方面有帮助的信息。IEC 指南 60300-3-9:1985、IEC Std 60812:1985 和 IEC Std 61025:1990 提供了支持风险评价的有用的技术。

5.1.4 执行风险处理

“执行风险处理”活动的目的是：

- a) 确定风险对共利益者来说是否是可接受的，如果不可接受；
- b) 启动行动将风险降低到可接受的等级。

风险处理包括减少风险预估行动的选择、策划、监督和控制。

共利益者应对超出其风险阈值的每个风险的处理进行评价。必要时，应持续地进行风险处理。

本活动包含 5.1.4.1~5.1.4.2 所列的任务。

5.1.4.1 选择风险处理

在避险措施请求中应向共利益者提供建议的风险处理的可选方案。只要在避险措施请求中建议风险处理可选方案，共利益者就应做出评价，以确定风险是否是可接受的。如果共利益者决定宜采取行动以使风险可接受，就应实施，由必要的资源支持、监督并与其他项目活动协调风险处理可选方案。

即使风险超出其风险阈值，共利益者也可能接受风险，例如：如果处理成本太高、时间安排不适当、或处理资源缺乏。在这种情况下，应认为该风险具有高优先权并应持续地监督该风险，以决定任何未来的风险处理行动是否是必要的。

共利益者还可能要求在避险措施请求中提供更多的供其做出风险处理决定的信息，或他们可能建议一些其他的处理方法。如果共利益者建议的处理可选方案不在避险措施请求之内，则避险措施请求应转到“执行风险分析”活动分析建议的处理可选方案。然后，避险措施请求应再提交给共利益者进行再评价。

5.1.4.2 风险处理策划和实现

当本条与 GB/T 8566 一起使用时，执行 5.1.4.2.1 的规定；否则，执行 5.1.4.2.2 的规定。

5.1.4.2.1 依赖 GB/T 8566 的风险处理

本条适用于和 GB/T 8566 一起使用本标准的所有用户。

只要选择风险处理，就应接受与 GB/T 8566 中管理过程的执行和控制活动一致的管理活动。

5.1.4.2.2 不依赖 GB/T 8566 的风险处理

本条适用于不依赖于 GB/T 8566 而使用本标准的所有用户。

在接受了风险处理可选方案时，共利益者应规定如附录 C 中描述的详细的处理计划。应确定将如何执行本计划、提供资源并监督进展和成果。应指定参与者对每个风险处理的职责。

应执行风险处理计划，并与现有项目计划及其管理过程和活动相结合。

共利益者宜定义失败的风险处理事件中的应急措施。对于某些认为可接受的风险，应急措施可能是必要的。

5.1.5 执行风险监督

“执行风险监督”活动的目的是：

- a) 评审并更新单个的风险状态和风险管理环境；
- b) 评估风险处理的有效性；
- c) 寻找新的风险和来源。

本活动包含 5.1.5.1~5.1.5.3 所列的任务。

5.1.5.1 监督风险

应利用测度持续地监督所有风险在其状态中的变更，并记录在项目风险概要中。也应监督风险管理环境的变更，并记录在项目风险概要中。应根据共利益者提供的准则（例如：风险预估、时间安排），按监督优先权顺序排列风险。宜频繁地监督高优先级风险。应对状态已变更的风险进行风险评价。发现状态变更后，宜立即进行评价。

5.1.5.2 监督风险处理

应执行并监督测度以评价风险处理的有效性。宜快速地识别无效处理的原因并采取补救措施。宜由共利益者提出准则,以确定何时不再需要就处理有效性而监督风险。

5.1.5.3 寻找新的风险

应在整个软件生存周期中持续地监督项目,以发现新的风险和风险源。在风险分析之后,应与共利益者沟通新的风险和风险源。

5.1.6 评价风险管理过程

“评价风险管理过程”活动的目的是向共利益者提供关于下列问题的反馈:

- a) 风险管理过程的质量;
- b) 应改进的风险管理规程、过程或政策的一些方面;
- c) 标识修改组织风险管理规程、过程或政策的时机,以更好地降低或消除系统性风险。

本活动包含 5.1.6.1~5.1.6.3 所列的任务。

5.1.6.1 收集风险管理信息

应在整个软件项目生存周期过程中收集有关已标识的风险、其风险源、风险成因、风险处理和所选处理的结果的信息,以改进风险管理过程,总结经验教训。收集的信息对于改进组织风险管理规程、过程或政策可能是有帮助的。可以以电子形式收集信息以易于收集、传达并评估信息。

5.1.6.2 评估并改进风险管理过程

应定期地评审风险管理过程的有效性和效率。应标识改进项目或组织风险管理体系和过程的时机。适当时,宜改进过程、更新组织风险管理体系、政策和过程(如果有),并更新项目风险管理计划。共利益者应确定评审周期。

5.1.6.3 总结经验教训

共利益者和其他参与者应定期地评审有关已识别的风险、风险处理和处理的的结果的信息,以识别系统性的项目和组织的风险。可以收集单个项目的经验教训,以帮助标识系统性风险。共利益者应确定评审周期。

附 录 A
(资料性附录)
风险管理计划

A.1 目的

风险管理计划的目的是要定义在项目进行期间怎样实现和支持风险管理活动。风险管理计划是策划过程的一个关键输出,并且可作为实现软件风险管理的机制。风险管理计划将满足 GB/T 8566 要求在项目管理计划中包括风险管理信息的意图。

A.2 风险管理计划

风险管理过程宜产生包括下面大纲所示章条的风险管理计划。如果在计划的章条中没有大纲中有关章和所要求的段落的信息,管理计划宜在该章或段落标题下含有“本章不适用于本计划”和省略该章的适当理由的说明段落。如果需要,可以增加补充信息。有些风险管理计划的内容可能在其他文档中出现。如果这样,则宜在管理计划的主要内容中引用这些文档。

风险管理计划大纲如下所示:

- 1 概述
 - 1.1 发布日期和状态
 - 1.2 发布组织
 - 1.3 批准人
 - 1.4 更新
- 2 范围
[定义项目风险的范围和限制。]
- 3 引用文件
- 4 术语
- 5 风险管理概述
[描述有关该项目或组织状况的风险管理的细节。]
- 6 风险管理政策
[描述将要执行的风险管理所依据的指南。]
- 7 风险管理过程概述
- 8 风险管理职责
[定义执行风险管理的参与者的职责。]
- 9 风险管理组织
[定义在组织单位内风险管理的职能或指定组织的职责。]
- 10 风险管理定位和培训
- 11 风险管理费用和进度安排
- 12 风险管理过程描述
[如果有一个正被用于该项目或状态的组织风险管理过程,则引用它。如果过程的调整是适当的,则描述所做的调整。描述实现风险管理过程的规程。如果没有组织的过程,则描述将要用于该项目或状态的风险管理过程和规程。]

12.1 风险管理背景

12.2 风险分析

12.3 风险监督

12.4 风险处理

[描述将怎样处理风险。如果有处理偏离或问题的标准的管理过程,则引用该过程。如果风险因具体的环境而要求单独的风险处理活动,则描述该活动。]

13 风险管理过程评价

[描述该项目或组织将怎样收集和利用测度信息,帮助项目和/或组织改进风险管理过程。]

13.1 获取风险信息

13.2 评估风险管理过程

13.3 产生经验教训

14 风险沟通

[描述怎样在共利益者间协调和沟通风险管理信息,如什么样的风险需要向哪个管理层报告。]

14.1 过程文档集和报告

14.2 与共利益者协调风险管理

14.3 与有关当事人协调风险管理

15 风险管理计划变更规程和历史记录



附录 B
(资料性附录)
避险措施请求

B.1 目的

避险措施请求的目的是提供一种获取风险信息并将其与共利益者沟通的机制。风险管理过程要求为超出其风险阈值的风险创建避险措施请求。

B.2 避险措施请求

风险管理过程宜产生包括下面大纲所示信息的避险措施请求。如果在计划的章条中没有大纲中有关章和所要求的段落的信息,措施请求宜在该章或段落标题下含有“本章不适用于本计划”和省略该章的适当理由的说明段落。如果需要,可以增加补充章条。部分避险措施请求的内容可能在其他文档中出现。如果这样,则宜在措施请求的主要内容中引用这些文档。

避险措施请求大纲如下所示:

- | | |
|---|--|
| <ol style="list-style-type: none"> 1 启动日期 2 范围 3 主题 4 请求发起人 5 风险管理过程环境 [本章可以只描述一次,然后,若无变更,则在随后的行动请求中引用它。] <li style="padding-left: 20px;">5.1 过程范围 <li style="padding-left: 20px;">5.2 共利益者观点 <li style="padding-left: 20px;">5.3 风险类别 <li style="padding-left: 20px;">5.4 风险阈值 <li style="padding-left: 20px;">5.5 项目目标 <li style="padding-left: 20px;">5.6 项目假设 <li style="padding-left: 20px;">5.7 项目约束 6 风险 [根据用户的选择,本章可以包括一个或多个风险。当上述所有信息适用于整个风险集合时,一个行动请求可能就够了。但在信息改变时,每个请求都可能包括该风险或共享公共信息的风。 <li style="padding-left: 20px;">6.1 风险描述 <li style="padding-left: 20px;">6.2 风险概率 <li style="padding-left: 20px;">6.3 风险后果 <li style="padding-left: 20px;">6.4 预期的风险时间 7 风险处理可选方案 <li style="padding-left: 20px;">7.1 可选方案描述 <li style="padding-left: 20px;">7.2 推荐的可选方案 <li style="padding-left: 20px;">7.3 理由 8 避险措施请求部署 [宜对每一个请求就其是否被接受、拒绝或修改加以评注,并解释所做的决定的理由。] | |
|---|--|

附 录 C
(资料性附录)
风险处理计划

C.1 目的

风险处理计划的目的是要定义怎样处理发现的不可接受的风险。风险处理计划作为实施避险措施请求中规定的选择的建议可选方案的机制。

C.2 风险处理计划

选择了避险措施请求中描述的推荐的处理可选方案后,宜制定包括下面大纲中所示章条的风险处理计划。有些处理计划的信息可能在避险措施请求中出现。如果是这样,则宜在相关章条的处理计划的主要内容中引用这些避险措施请求。如果没有大纲中有关章的信息,处理计划宜在该章或段落标题下含有“本章不适用于本计划”和省略该章的适当理由的说明段落。如果需要,补充信息可以加到计划中。

为了减小为每个单个风险制定一个单独的风险处理计划的必要性,可以对涉及共享相关特征的各风险,规定风险处理计划。

风险处理计划大纲如下所示:

1 概述

1.1 发布日期和状态

1.2 发布组织

1.3 批准人

1.5 更新

2 范围

3 引用文件

4 术语

5 计划的风险处理活动和任务

[描述为发现的、将是不可接受的风险或风险组合所选的风险处理的细节。描述所有可能在实施处理中发现的困难。]

6 处理进度安排

7 处理资源及其分配

8 职责和权力

[描述谁负责确保将要执行的处理及其权力。]

9 处理控制测度

[定义将用于评价风险处理有效性的测度。]

10 处理费用

11 有关参与者间的接口

[描述共利益者间或与项目主计划的协调,这些协调是要正确执行处理所必须的。]

12 环境/基础设施

[描述所有环境的或基础设施的需求或影响,例如:处理可能有的安全或保密影响。]

13 风险处理计划变更规程和历史记录

参 考 文 献

- [1] IEEE 100, The authoritative dictionary of the IEEE standards terms, Seventh Edition.
- [2] IEEE Std 982.1:1988, IEEE standard dictionary of measures to produce reliable software.
- [3] IEEE Std 982.2:1998, IEEE guide for the use of IEEE standard dictionary of measures to produce reliable software.
- [4] IEEE Std 1012:1998, IEEE standard for software verification and validation plans.
- [5] IEEE Std 1228:1994, IEEE standard for software safety plans.
- [6] IEEE Std 1044:1993, IEEE standard classification for software anomalies.
- [7] IEEE Std 1058:1998, IEEE standard for software project management plans—Content map to IEEE/EIA 12207.1.
- [8] IEEE/EIA 12207.1:1997, IEEE/EIA guide—industry implementation of international standard ISO/IEC 12207:1995, Standard for information technology—Software life cycle processes—Life cycle data.
- [9] IEEE/EIA 12207.2:1997, IEEE/EIA guide—industry implementation of international standard ISO/IEC 12207:1995, standard for information technology—Software life cycle processes—Implementation considerations.
- [10] ISO/IEC GUIDE 73:2002, Guide on risk management—Vocabulary—Guidelines for use in standards.
- [11] IEC 60300-1:1993, Dependability management—Part 1: Dependability programme management.
- [12] IEC 60300-2:1995, Dependability management—Part 2: Dependability programme elements and tasks.
- [13] IEC 60300-3-9:1995, Dependability management—Part 3: Application guide—Section 9: Risk analysis of technological systems.
- [14] IEC 60812:1985 Analysis techniques for system reliability—Procedures for failure mode and effects analysis(FEMA).
- [15] IEC 61025:1990 Fault tree analysis(FTA).
- [16] IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1: General requirements.
- [17] IEC 61508-2:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.
- [18] IEC 61508-3:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements.
- [19] IEC 61508-4:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 4: Definitions and abbreviations.
- [20] IEC 61508-5:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 5: Examples of methods for the determination of safety integrity levels.
- [21] IEC 61508-6:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.

- [22] IEC 61508-7:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 7: Overview of techniques and measures.
 - [23] ISO/IEC Guide 51:1999 Safety aspects—Guidelines for their inclusion in standards
 - [24] ISO 9000:2000 Quality management systems—Fundamentals and vocabulary.
-

中 华 人 民 共 和 国
国 家 标 准
信 息 技 术 软 件 生 存 周 期 过 程
风 险 管 理

GB/T 20918—2007

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

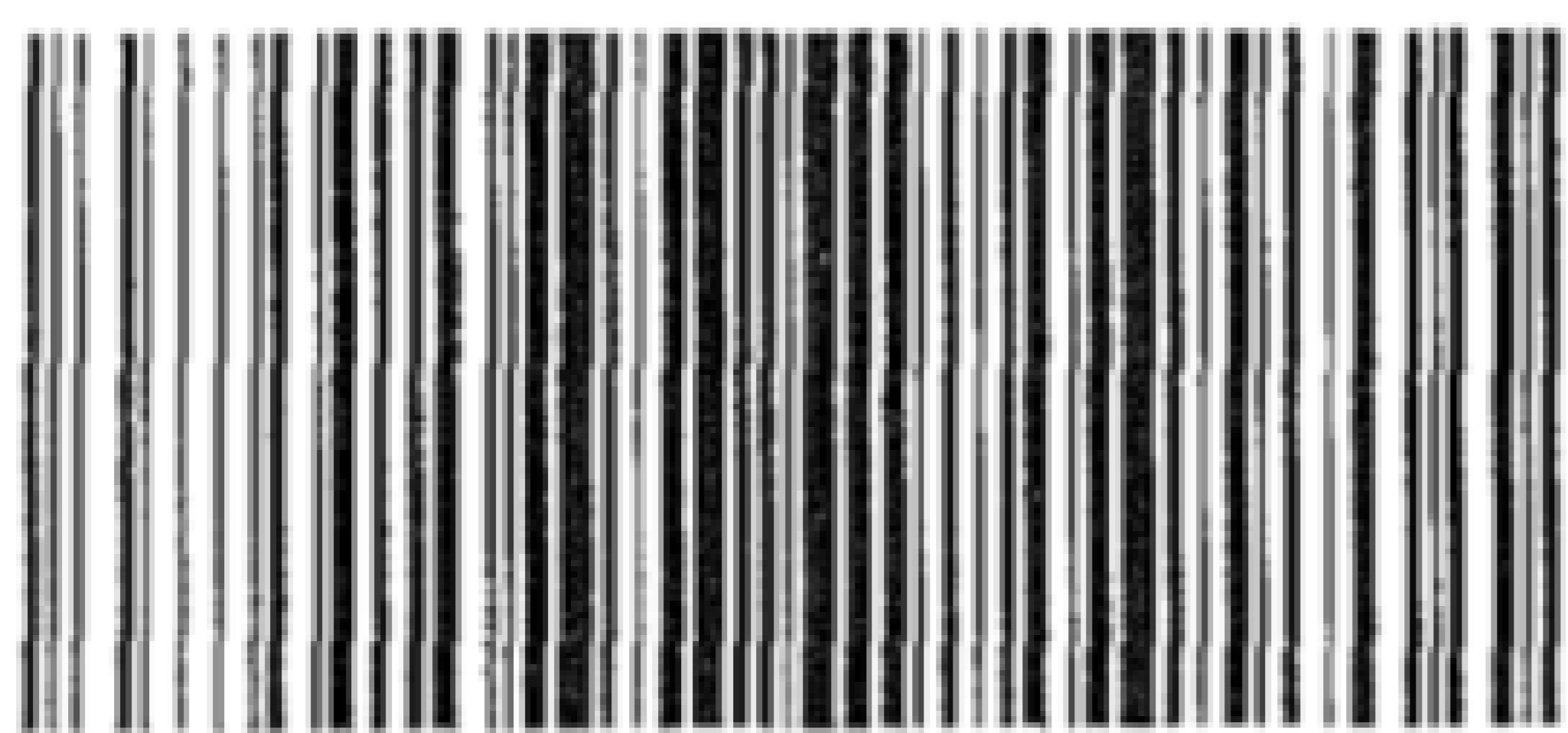
开本 880×1230 1/16 印张 1.5 字数 34 千字
2007年7月第一版 2007年7月第一次印刷

*

书号: 155066·1-29686 定价 20.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究

举报电话:(010)68533533



GB/T 20918—2007

www.bzxz.net

免费标准下载网