ICS 35.080
L 77

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
中国国家标准化管理委员会　发布

目　　次

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