ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33132—2016

信息安全技术　信息安全风险处理实施指南

Information security technology—Guide of implementation for information security risk treatment

2016-10-13 发布　　2017-05-01 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 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　风险处理实施概述 …… 2
4.1　风险处理基本原则 …… 2
4.2　风险处理的方式 …… 2
4.3　风险处理的角色和职责 …… 3
4.4　风险处理的基本流程 …… 3
5　风险处理准备 …… 5
5.1　制定风险处理计划 …… 5
5.2　获得管理层批准 …… 6
6　风险处理实施 …… 6
6.1　风险处理方案制定 …… 6
6.2　风险处理方案实施 …… 8
7　风险处理效果评价 …… 8
7.1　概述 …… 8
7.2　评价原则 …… 8
7.3　评价方法 …… 9
7.4　评价方案 …… 9
7.5　评价实施 …… 9
7.6　持续改进 …… 10
附录A（资料性附录）　风险处理实践示例 …… 11
A.1　背景 …… 11
A.2　风险处理准备 …… 12
A.3　风险处理实施 …… 14
A.4　风险处理评价 …… 21
参考文献 …… 23

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、北京信息安全测评中心、中国民航大学、东软集团股份有限公司、北京数字认证股份有限公司、西安交大捷普网络科技有限公司。

本标准主要起草人:吴亚非、禄凯、陈永刚、赵章界、马勇、席斐、陈青民、何建锋。

引　言

信息安全风险管理是信息安全保障工作中的一项重要基础性工作，其核心思想是对管理对象面临的信息安全风险进行管控。信息安全风险管理工作贯穿于信息系统生命周期（规划、设计、实施、运行维护和废弃）的全过程，主要工作过程包括风险评估和风险处理两个基本步骤。风险评估是对风险管理对象所面临的风险进行识别、分析和评价的过程。风险处理是依据风险评估的结果，选择和实施安全措施的过程。

为指导各类组织规范性地开展信息安全风险处理，在GB/T 20984—2007《信息安全技术　信息安全风险评估规范》、GB/Z 24364—2009《信息安全技术　信息安全风险管理指南》和GB/T 31509—2015《信息安全技术　信息安全风险评估实施指南》的基础上，本标准针对风险评估工作中反映出来的各类信息安全风险，从风险处理工作的组织、管理、流程、评价等方面给出了相关描述，用于指导组织形成客观、规范的风险处理方案，促进风险管理工作的完善。

信息安全技术　信息安全风险处理实施指南

1　范围

本标准给出了信息安全风险处理的基本概念、处理原则、处理方式、处理流程以及处理结束后的效果评价等管理过程和方法，并对处理过程中的角色和职责进行了定义。

本标准适用于指导信息系统运营使用单位和信息安全服务机构实施信息安全风险处理活动。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20984—2007　信息安全技术　信息安全风险评估规范

GB/Z 24364—2009　信息安全技术　信息安全风险管理指南

3　术语和定义

GB/T 20984—2007、GB/Z 24364—2009 界定的以及下列术语和定义适用于本文件。

3.1

风险处理　risk treatment

选择并且执行措施来更改风险的过程。

[ISO/IEC Guide 73:2002]。

注：在本标准中，术语“控制措施”被用作“措施”的同义词。

3.2

风险规避　risk elimination

不卷入风险处境的决定或撤离风险处境的行动。

[ISO/IEC Guide 73:2002]。

3.3

风险转移　risk mitigation

与另一方对风险带来的损失或收益的共享。

[ISO/IEC Guide 73:2002]。

注：在信息安全风险的语境下，对于风险转移仅考虑负面结果(损失)。

3.4

风险降低　risk reduction

为降低风险的可能性和(或)负面结果所采取的行动。

[ISO/IEC Guide 73:2002]。

3.5

风险接受　risk retention

对来自特定风险的损失或收益的接受。