



中华人民共和国国家标准

GB/T 31722—2015/ISO/IEC 27005:2008

GB/T 31722—2015/ISO/IEC 27005:2008

信息技术 安全技术 信息安全风险管理

Information technology—Security techniques—
Information security risk management

(ISO/IEC 27005:2008, IDT)

中华人民共和国
国家标准
信息技术 安全技术
信息安全风险管理

GB/T 31722—2015/ISO/IEC 27005:2008

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

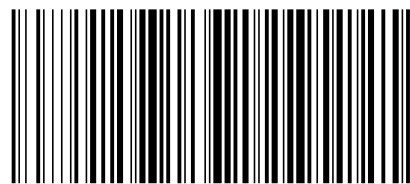
*

开本 880×1230 1/16 印张 3 字数 84 千字
2015年6月第一版 2015年6月第一次印刷

*

书号: 155066·1-51115 定价 42.00 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)68510107



GB/T 31722-2015

2015-06-02 发布

2016-02-01 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 本标准结构	2
5 背景	3
6 信息安全风险管理过程概述	3
7 语境建立	5
8 信息安全风险评估	7
9 信息安全风险处置	13
10 信息安全风险接受	16
11 信息安全风险沟通	16
12 信息安全风险监视和评审	17
附录 A (资料性附录) 确定信息安全风险管理过程的范围和边界	19
附录 B (资料性附录) 资产识别和估价以及影响评估	22
附录 C (资料性附录) 典型威胁示例	28
附录 D (资料性附录) 脆弱性和脆弱性评估方法	31
附录 E (资料性附录) 信息安全评估方法	35
附录 F (资料性附录) 风险降低的约束	40
参考文献	42

参 考 文 献

- [1] ISO/IEC Guide 73:2002, Risk management—Vocabulary—Guidelines for use in standards (风险 词汇 在标准中的使用指南)
- [2] ISO/IEC 16085:2006, Systems and software engineering—Life cycle processes—Risk management(系统和软件工程 生存周期过程 风险管理)
- [3] AS/NZS 4360:2004, Risk Management(风险管理)
- [4] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook(计算机安全介绍: NIST 手册)
- [5] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology(信息技术系统的风险管理指南, 美国国家标准与技术研究所建议)
-

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。

本标准使用翻译法等同采用 ISO/IEC 27005:2008《信息技术 安全技术 信息安全风险管理》(英文版)。

本标准做了以下修改：

——对引言做了一些编辑性修改。

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:中国电子技术标准化研究院、上海二零卫士信息安全有限公司、中电长城网际系统应用有限公司、山东省计算中心、北京信息安全测评中心。

本标准主要起草人:许玉娜、闵京华、上官晓丽、董火民、赵章界、李刚、周鸣乐。