ICS 35.040
L 80

中华人民共和国国家标准

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)

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

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、上海三零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。

引　言

信息安全管理体系标准族(Information Security Management System,简称 ISMS 标准族)是国际信息安全技术标准化组织(ISO/IEC JTC1 SC27)制定的信息安全管理体系系列国际标准。ISMS 标准族旨在帮助各种类型和规模的组织,开发和实施管理其信息资产安全的框架,并为保护组织信息(诸如,财务信息、知识产权、员工详细资料,或者受客户或第三方委托的信息)的 ISMS 的独立评估做准备。ISMS 标准族包括的标准:a)定义了 ISMS 的要求及其认证机构的要求;b)提供了对整个"规划-实施-检查-处置"(PDCA)过程和要求的直接支持、详细指南和(或)解释;c)阐述了特定行业的 ISMS 指南;d)阐述了 ISMS 的一致性评估。

目前,ISMS 标准族由下列标准组成:

——GB/T 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009)

——GB/T 22080—2008　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2005)

——GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则(ISO/IEC 27002:2005)

——GB/T 31496—2015　信息技术　安全技术　信息安全管理体系实施指南(ISO/IEC 27003:2010)

——GB/T 31497—2015　信息技术　安全技术　信息安全管理　测量(ISO/IEC 27004:2009)

——GB/T 31722—2015　信息技术　安全技术　信息安全风险管理(ISO/IEC 27005:2008)

——GB/T 25067—2010　信息技术　安全技术　信息安全管理体系审核认证机构的要求(ISO/IEC 27006:2007)

——ISO/IEC 27007:2011　信息技术　安全技术　信息安全管理体系审核指南

——ISO/IEC TR 27008:2011　信息技术　安全技术　信息安全控制措施审核员指南

——ISO/IEC 27010:2012　信息技术　安全技术　行业间及组织间通信的信息安全管理

——ISO/IEC 27011:2008　信息技术　安全技术　基于 ISO/IEC 27002 的电信行业组织的信息安全管理指南

——ISO/IEC 27013:2012　信息技术　安全技术　ISO/IEC 27001 和 ISO/IEC 20000-1 集成实施指南

——ISO/IEC 27014:2013　信息技术　安全技术　信息安全治理

——ISO/IEC TR 27015:2012　信息技术　安全技术　金融服务信息安全管理指南

本标准作为 ISMS 标准族之一,为组织内的信息安全风险管理提供指南,特别是支持按照 GB/T 22080 的 ISMS 要求。然而,本标准不提供信息安全风险管理的任何特定方法。由组织来确定其风险管理方法,这取决于诸如组织的 ISMS 范围、风险管理语境或所处行业。一些现有的方法可在本标准描述的框架下使用,以实现 ISMS 的要求。

本标准的相关方包括关心组织内信息安全风险的管理者和员工以及(在适当情况下)支持这种活动的外部方。

信息技术　安全技术
信息安全风险管理

1　范围

本标准为信息安全风险管理提供指南。

本标准支持 GB/T 22080 所规约的一般概念，旨在为基于风险管理方法来符合要求地实现信息安全提供帮助。

知晓 GB/T 22080 和 GB/T 22081 中所描述的概念、模型、过程和术语，对于完整地理解本标准是重要的。

本标准适用于各种类型的组织（例如，商务企业、政府机构、非盈利性组织），这些组织期望管理可能危及其信息安全的风险。

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 22080—2008　信息技术　安全技术　信息安全管理体系　要求（ISO/IEC 27001:2005，IDT）

GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则（ISO/IEC 27002:2005，IDT）

3　术语和定义

GB/T 22080—2008 和 GB/T 22081—2008 中界定的以及下列术语和定义适用于本文件。

3.1

影响　impact

对所达到业务目标的不利改变。

3.2

信息安全风险　information security risk

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

注：它以事态的可能性及其后果的组合来度量。

3.3

风险规避　risk avoidance

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]

3.4

风险沟通　risk communication

决策者和其他利益相关者之间关于风险的信息交换或共享。

[ISO/IEC Guide 73:2002]