ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31496—2015/ISO/IEC 27003:2010

信息技术　安全技术
信息安全管理体系实施指南

Information technology—Security techniques—
Information securitymanagement system implementation guidance

(ISO/IEC 27003:2010,IDT)

2015-05-15 发布　　2016-01-01 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

中 华 人 民 共 和 国
国 家 标 准
信息技术　安全技术
信息安全管理体系实施指南
GB/T 31496—2015/ISO/IEC 27003:2010
*
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.gb168.cn
服务热线:400-168-0010
010-68522006
2015年6月第一版
*
书号:155066·1-51118

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO/IEC 27003:2010《信息技术　安全技术　信息安全管理体系实施指南》。

本标准做了以下编辑性修改：

——在引言部分增加了有关信息安全管理体系标准族情况的介绍。

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：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、山东省计算中心、黑龙江省电子信息产品监督检验院、北京信息安全测评中心、中电长城网际系统应用有限公司。

本标准主要起草人：上官晓丽、许玉娜、董火民、闵京华、赵章界、周鸣乐、方舟、李刚。

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/ISO/IEC 27000:2009　信息技术　安全技术　信息安全管理体系　概述和词汇

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

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

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

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

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

——GB/T 25067—2010/ISO/IEC 27006:2007　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 27007　信息技术　安全技术　信息安全管理体系审核指南

——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,其目的是为组织按照 GB/T 22080—2008 制定信息安全管理体系(ISMS)的实施计划,提供实用指导。实际情况下,ISMS 的实施通常作为一个项目来执行。

本标准所描述的过程旨在为实施 GB/T 22080—2008 提供支持;第 4 章、第 5 章和第 7 章所包含的相关部分和文件可用于:

a)　准备启动组织的 ISMS 实施计划、定义该项目的组织结构,及获得管理者的批准;

b)　该 ISMS 项目的关键活动;

c)　实现 GB/T 22080—2008 要求的示例。

通过使用本标准,组织将能够制定信息安全管理的过程,并向利益相关方保证,信息资产的风险可持续保持在组织定义的可接受的信息安全边界内。

本标准不涉及运行活动和其他 ISMS 活动,但涉及了如何设计这些活动的概念,这些活动是在开始运行 ISMS 后所产生的。这些概念导致了最终的 ISMS 项目实施计划。ISMS 项目的组织特定部分的实际执行不在本标准范围内。

ISMS 项目的实施宜使用标准的项目管理方法学来执行(更多信息请参见 ISO 和 ISO/IEC 有关项目管理的标准)。

信息技术　安全技术
信息安全管理体系实施指南

1　范围

本标准依据 GB/T 22080—2008,关注设计和实施一个成功的信息安全管理体系(ISMS)所需要的关键方面。本标准描述了 ISMS 规范及其设计的过程,从开始到产生实施计划。本标准为实施 ISMS 描述了获得管理者批准的过程,为实施 ISMS 定义了一个项目(本标准称作 ISMS 项目),并就如何规划该 ISMS 项目提供了相应的指导,产生最终的 ISMS 项目实施计划。

本标准可供实施一个 ISMS 的组织使用,适用于各种规模和类型的组织(例如,商业企业、政府机构、非赢利组织)。每个组织的复杂性和风险都是独特的,并且其特定的要求将驱动 ISMS 的实施。小型组织将发现,本标准中所提及的活动可适用于他们,并可进行简化。大型组织或复杂的组织可能会发现,为了有效地管理本标准中的活动,需要层次化的组织架构或管理体系。然而,无论是大型组织还是小型组织,都可应用本标准来规划相关的活动。

本标准提出了一些建议及其说明,但并没有规定任何要求。期望把本标准与 GB/T 22080—2008 和 GB/T 22081—2008 一起使用,但不期望修改和/或降低 GB/T 22080—2008 中所规定的要求,或修改和/或降低 GB/T 22081—2008 所提供的建议。因此,不宜声称符合这一标准。

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 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,IDT)

3　术语和定义

GB/T 29246—2012 和 GB/T 22080—2008 界定的以及下列术语和定义适用于本文件。

3.1

ISMS 项目　ISMS project

组织为实施一个 ISMS 所开展的结构化活动。

4　本标准的结构

4.1　章条的总结构

ISMS 的实施是一种重要活动,通常作为组织的一个项目来执行。本标准通过关注该项目的启动、