ICS 35.040
L 80

中华人民共和国国家标准

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

Information technology—Security techniques—Information security management systems—Overview and vocabulary

(ISO/IEC 27000:2009,IDT)

2012-12-31 发布　　2013-06-01 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。

本标准使用翻译法等同采用 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》。

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所、上海三零卫士有限公司、北京信息安全测评中心。

本标准主要起草人:上官晓丽、许玉娜、闵京华、赵章界。

引　言

0.1　概述

管理体系标准为建立和运行管理体系提供一个可遵循的模型。这个模型综合了该领域中专家已达成一致的、可代表国际技术发展水平的特征。ISO/IEC JTC1 SC27(国际信息安全技术标准化组织)设置了一个专家委员会专门开发信息安全管理体系国际标准,也称为信息安全管理体系(Information Security Management System,简称 ISMS)标准族。

组织通过使用 ISMS 标准族,能够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。

0.2　ISMS 标准族

ISMS 标准族[1)]旨在帮助所有类型和规模的组织实施和运行 ISMS。在《信息技术　安全技术》这一通用标题下,ISMS 标准族由下列标准组成:

——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

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

——ISO/IEC 27004:2009　信息技术　安全技术　信息安全管理测量

——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

注:通用标题《信息技术　安全技术》是指这些标准是由 ISO/IEC JTC1 SC27 制定的。

不在通用标题“信息技术　安全技术”之列,同时也属于 ISMS 标准族的标准如下所示:

——ISO 27799:2008　健康信息学　使用 ISO/IEC 27002 的健康信息安全管理

0.3　本标准的目的

本标准提供了信息安全管理体系的概述,该体系形成了 ISMS 标准族的主题,并定义了相关术语。

注:附录 A 阐明了 ISMS 标准族在文字表达上如何区分要求和/或指南。

ISMS 标准族包括的标准:

a)　定义 ISMS 的要求及其认证机构的要求;

b)　提供对整个“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)　阐述特定行业的 ISMS 指南;

d)　阐述 ISMS 的一致性评估。

本标准提供的术语和定义:

---

1)　本节中列出的没有指明发布年的标准仍在开发中。

——包含 ISMS 标准族中通用的术语和定义；

——未包含 ISMS 标准族使用的所有术语和定义；

——不限制 ISMS 标准族定义各自使用的术语。

相对于涉及 ISO/IEC 27002 中所有控制措施的标准而言，那些仅阐述 ISO/IEC 27002 中控制措施实施的标准，不包括在 ISMS 标准族内。

信息技术　安全技术
信息安全管理体系　概述和词汇

1　范围

本标准提供：

a)　ISMS 标准族的概述；

b)　信息安全管理体系(ISMS)的介绍；

c)　“规划—实施—检查—处置”(PDCA)过程的简要描述；

d)　ISMS 标准族所用的术语和定义。

本标准适用于所有类型的组织(例如，商业企业、政府机构、非赢利组织)。

2　术语和定义

下列术语和定义适用于本文件。

注：定义或注中的术语如果在条款的其他地方被定义，则以黑体标出并在其后的圆括号中标明其条目号。这种黑体术语可以在定义中替换为其完整的定义。

示例：

攻击(2.4)被定义为“破坏、泄露、篡改、损伤、偷窃、未授权访问或未授权使用**资产**(2.3)的企图”；

资产被定义为“对组织有价值的任何东西”。

如果术语“**资产**”被其定义替换，则：

攻击的定义变为“破坏、泄露、篡改、损伤、偷窃、未授权访问或未授权使用对组织有价值的任何东西的企图”。

2.1

访问控制　access control

基于业务要求和安全要求，确保授权和受限地访问**资产**(2.3)的手段。

2.2

可核查性　accountability

实体的一种特性，表征对自己的动作和做出的决定负责。

2.3

资产　asset

对组织有价值的任何东西。

注：有许多类型的资产，包括：

a)　**信息资产**(2.18)；

b)　软件，如计算机程序；

c)　物理资产，如计算机；

d)　服务；

e)　人员及其资格、技能和经验；

f)　无形资产，如名誉和形象。

2.4

攻击　attack

破坏、泄露、篡改、损伤、偷窃、未授权访问或未授权使用**资产**(2.3)的企图。