ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29246—2017/ISO/IEC 27000:2016
代替 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

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

（ISO/IEC 27000:2016,IDT）

2017-12-29 发布　　2018-07-01 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。

本标准代替 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》，与 GB/T 29246—2012 相比主要技术变化如下：

——ISMS 标准族的组成标准由 10 项增加至 19 项(见 0.2 和 4.1～4.5，2012 年版的 0.2 和 4.1～4.5)；

——术语和定义由 46 条增加至 89 条(见 2.1～2.89，2012 年版的 2.1～2.46)；

——将附录“术语分类”改为“术语和术语归属”(见附录 B，2012 年版的附录 B)。

本标准使用翻译法等同采用 ISO/IEC 27000:2016《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：中电长城网际系统应用有限公司、中国电子技术标准化研究院、中国信息安全研究院有限公司。

本标准主要起草人：闵京华、上官晓丽、许玉娜、王惠莅、罗锋盈、左晓栋、周亚超、马洪军、廖飞鸣、黄凯峰、马文荷。

本标准所代替的历次版本发布情况为：

——GB/T 29246—2012。

引　言

0.1　概述

管理体系标准提供一个在建立和运行管理体系时可遵循的模型。专门为信息安全开发的管理体系标准称为信息安全管理体系(Information Security Management System,简称 ISMS)标准族。

通过使用 ISMS 标准族,组织能够开发和实施管理其信息资产安全的框架,包括财务信息、知识产权和员工详细资料,或者受客户或第三方委托的信息。这些标准还可用于对组织应用 ISMS 保护其信息做独立评估准备。

0.2　信息安全管理体系标准族

信息安全管理体系(ISMS)标准族(见第 4 章)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》通用标题下,ISMS 标准族由下列标准组成(按标准号排序):

——ISO/IEC 27000　信息安全管理体系　概述和词汇(Information security management systems—Overview and vocabulary)

——ISO/IEC 27001　信息安全管理体系　要求(Information security management systems—Requirements)

——ISO/IEC 27002　信息安全控制实践指南(Code of practice for information security controls)

——ISO/IEC 27003　信息安全管理体系实施指南(Information security management system implementation guidance)

——ISO/IEC 27004　信息安全管理　测量(Information security management—Measurement)

——ISO/IEC 27005　信息安全风险管理(Information security risk management)

——ISO/IEC 27006　信息安全管理体系审核认证机构的要求(Requirements for bodies providing audit and certification of information security management systems)

——ISO/IEC 27007　信息安全管理体系审核指南(Guidelines for information security management systems auditing)

——ISO/IEC TR 27008　信息安全控制措施审核员指南(Guidelines for auditors on information security controls)

——ISO/IEC 27009　ISO/IEC 27001 的行业特定应用　要求(Sector-specific application of ISO/IEC 27001—Requirements)

——ISO/IEC 27010　行业间和组织间通信的信息安全管理(Information security management for inter-sector and inter-organizational communications)

——ISO/IEC 27011　基于 ISO/IEC 27002 的电信组织信息安全管理指南(Information security management guidelines for telecommunications organizations based on ISO/IEC 27002)

——ISO/IEC 27013　ISO/IEC 27001 和 ISO/IEC 20000-1 综合实施指南(Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1)

——ISO/IEC 27014　信息安全治理(Governance of information security)

——ISO/IEC TR 27015　金融服务信息安全管理指南(Information security management guidelines for financial services)

——ISO/IEC TR 27016　信息安全管理　组织经济学(Information security management—Or-

ganizational economics)

——ISO/IEC 27017　基于 ISO/IEC 27002 的云服务信息安全控制实践指南(Code of practice for information security controls based on ISO/IEC 27002 for cloud services)

——ISO/IEC 27018　可识别个人信息(PII)处理者在公有云中保护 PII 的实践指南(Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)

——ISO/IEC 27019　基于 ISO/IEC 27002 的能源供给行业过程控制系统信息安全管理指南(Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry)

注：通用标题《信息技术　安全技术》是指这些标准是由 ISO/IEC 的信息技术委员会(JTC 1)下属的安全技术分委员会(SC 27)制定的。

不在通用标题《信息技术　安全技术》之下，但也属于 ISMS 标准族的标准如下：

——ISO 27799　健康信息学　使用 ISO/IEC 27002 的健康信息安全管理(Health informatics—Information security management in health using ISO/IEC 27002)

0.3　本标准的目的

本标准提供信息安全管理体系概述，并定义相关术语。

注：附录 A 阐明在 ISMS 标准族中表达要求和(或)指南的措辞形式。

ISMS 标准族包括的标准：

a)　定义 ISMS 及其认证机构的要求；

b)　为建立、实施、维护和改进 ISMS 的整个过程提供直接支持、详细指南和(或)解释；

c)　提出行业特定的 ISMS 指南；

d)　提出 ISMS 的符合性评估。

本标准提供的术语和定义：

——包含 ISMS 标准族中的通用术语和定义；

——不包含 ISMS 标准族中的所有术语和定义；

——不限制 ISMS 标准族定义所需的新术语。

信息技术　安全技术
信息安全管理体系　概述和词汇

1　范围

本标准概述了信息安全管理体系(ISMS),提供了ISMS标准族中常用的术语及其定义。本标准适用于所有类型和规模的组织(例如,商业企业、政府机构、非盈利组织)。

2　术语和定义

下列术语和定义适用于本文件。

2.1

访问控制　access control

确保对资产的访问是基于业务和安全**要求**(2.63)进行授权和限制的手段。

2.2

分析模型　analytical model

将一个或多个**基本测度**(2.10)和(或)**导出测度**(2.22)关联到**决策准则**(2.21)的算法或计算。

2.3

攻击　attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

2.4

属性　attribute

可由人工或自动化手段定量或定性辨别的**对象**(2.55)特性或特征。

[ISO/IEC 15939:2007,定义2.2,做了修改:将原定义中的"实体"替换为"对象"]

2.5

审核　audit

获取审核证据并客观地对其评价以确定满足审核准则程度的,系统的、独立的和文档化的**过程**(2.61)。

注1:审核可以是内部审核(第一方)或外部审核(第二方或第三方),可以是结合审核(结合两个或两个以上学科)。

注2:"审核证据"和"审核准则"在ISO 19011中被定义。

2.6

审核范围　audit scope

审核(2.5)的程度和边界。

[ISO 19011:2011,定义3.14,做了修改:删除注1]

2.7

鉴别　authentication

为一个实体声称的特征是正确的而提供的保障措施。

2.8

真实性　authenticity

一个实体是其所声称实体的这种特性。