ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 29246—2023/ISO/IEC 27000:2018
代替 GB/T 29246—2017

# 信息安全技术　信息安全管理体系　概述和词汇

**Information security technology—Information security management systems—Overview and vocabulary**

（ISO/IEC 27000:2018,Information technology—Security techniques—Information security management systems—Overview and vocabulary,IDT）

2023-12-28 发布　　2024-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 29246—2017《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—2017相比,除结构调整和编辑性改动外,主要技术变化如下:

a) 删除了术语“分析模型”“属性”“数据”“决策准则”“执行管理者”“信息安全管理体系(ISMS)专业人员”“信息安全管理体系项目”“测量结果”“对象”“尺度”“测量单位”“确认”“验证”(见2017年版的第3章);

b) 合并了定义相同的术语“受益相关方”(见2017年版的2.41)和“利益相关方”(见2017年版的2.82)为“利益相关方”(见3.37);

c) 增加了对ISO/IEC 27009的说明(见5.3.3);

d) 增加了对ISO/IEC 27021的说明(见5.4.10);

e) 更新了对信息安全管理体系标准族中一些标准的说明(见第5章,2017年版的第4章)。

本文件等同采用ISO/IEC 27000:2018《信息技术　安全技术　信息安全管理体系　概述和词汇》。

本文做了下列最小限度的编辑性改动:

——为与现有标准协调,将标准名称改为《信息安全技术　信息安全管理体系　概述和词汇》。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位: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、杭州安恒信息技术股份有限公司、中国软件评测中心、中国信息通信研究院、北京赛西认证有限责任公司、中通服咨询设计研究院有限公司、国家计算机网络应急技术处理协调中心、深信服科技股份有限公司、启明星辰信息技术集团股份有限公司、长扬科技(北京)有限公司、公安部第三研究所、深圳大学、北京百度网讯科技有限公司、北京时代新威信息技术有限公司、中国长江三峡集团有限公司。

本文件主要起草人:闵京华、王惠莅、范博、周亚超、左冉、李松恬、李汪蔚、赵丽华、高丽芬、王文磊、刘晨、朱宇泽、赵华、王宁、刘伟丽、王海棠、郭建领、潘文博、唐进、王秉政。

本文件及其所代替文件的历次版本发布情况为:

——2012年首次发布为GB/T 29246—2012;

——2017年第一次修订;

——本次为第二次修订。

# 信息安全技术　信息安全管理体系
# 概述和词汇

## 1　范围

本文件给出了信息安全管理体系(ISMS)概述,界定了ISMS标准族中常用的术语和定义。

本文件适用于所有类型和规模的组织(例如,商业企业、政府机构、非营利组织)。

本文件中提供的术语和定义:

——包含ISMS标准族中的通用术语和定义;

——不包含ISMS标准族中应用的所有术语和定义;

——不限制ISMS标准族定义新的使用术语。

## 2　规范性引用文件

本文件没有规范性引用文件。

## 3　术语和定义

3.1

**访问控制　access control**

确保对资产访问是基于业务和安全要求(3.56)进行授权和限制的手段。

3.2

**攻击　attack**

企图破坏、泄露、篡改、禁用、窃取或者未经授权访问或未经授权使用资产的行为。

3.3

**审核　audit**

为获取审核证据并对其进行客观评价,以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程(3.54)。

注1:审核可能是内部审核(第一方)或外部审核(第二方或第三方),也可能是联合审核(结合两个或更多管理体系)。

注2:内部审核由组织(3.50)自己或由外部方代表进行。

注3:ISO 19011:2018中定义了“审核证据”和“审核准则”。

3.4

**审核范围　audit scope**

审核(3.3)的程度和边界。

[来源:ISO 19011:2018,3.5,有修改:删除注]

3.5

**鉴别　authentication**

确保实体所声称其特征是正确的一种措施。