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/T29246—2017

信息安全技术　信息安全管理体系　概述和词汇

Information securitytechnology—Information security managementsystems—Overview and vocabulary

(ISO/IEC 27000:2018,Information technology—Securitytechniques—Information security managementsystems—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/TC260)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、李柲恬、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　accesscontrol

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 auditscope

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。

3.6

真实性 authenticity

一个实体是其所声称实体的性质。

3.7

可用性 availability

可由经授权实体按需访问和使用的性质。

3.8

基本测度 basemeasure

用某一属性及其量化方法定义的测度(3.42)。

注：基本测度在功能上独立于其他测度。

[来源：ISO/IEC/IEEE 15939:2017,3.3,有修改：删除注 2]

3.9

胜任力 competence

运用知识和技能实现预期结果的能力。

3.10

保密性 confidentiality

信息对未经授权的个人、实体或过程(3.54)不可用或不泄露的性质。

3.11

符合性 conformity

对要求(3.56)的满足。

3.12

后果 consequence

事态(3.21)影响目标(3.49)的结果。

注 1：一个事态(3.21)可能导致一系列后果。

注 2：一个后果可能是确定的或不确定的，在信息安全(3.28)的语境下通常是负面的。

注 3：后果可能定性或定量表示。

注 4：初始后果可能通过连锁效应升级。

[来源：ISO Guide 73:2009,3.6.1.3,有修改：更改注 2]

3.13

持续改进 continualimprovement

为提高性能(3.52)而反复进行的活动。

3.14

控制 control

改变风险(3.61)的措施。

注 1: 控制包括任何改变风险(3.61)的过程(3.54)、策略(3.53)、装置、实践或其他措施。

注 2: 控制可能并不总是发挥出预期或假定的改变效果。

[来源 :ISO Guide 73:2009,3.8.1.1,有修改 :更改注 2]

3.15

控制目标 controlobjective

描述控制(3.14)的实施结果所要达到目标的声明。

3.16

纠正 correction

消除已查明不符合性(3.47)的措施。

3.17

整改措施 correctiveaction

消除不符合性(3.47)根源以防再次发生的措施。

3.18

导出测度 derived measure

定义为两个或两个以上基本测度(3.8)值的函数的测度(3.42)。

[来源:ISO/IEC/IEEE 15939:2017,3.8,有修改:删除注]

3.19

文档化信息 documented information

组织(3.50)需要控制和维护的信息及其媒体。

注 1: 文档化信息可能采用任何格式,存于任何媒体中和出 自任何来源。

注 2: 文档化信息可能涉及

— 管理体系(3.41),包括相关过程(3.54);
— 为组织(3.50)运营而创建的信息(文档);
— 取得结果的证据(记录)。

3.20

有效性 effectiveness

实现所计划活动和达成所计划结果的程度。

3.21

事态 event

一组特殊情况的发生或改变。

注 1: 一个事态可能是一次或多次发生,并可能有多种原因。

注 2: 一个事态可能由未发生的事情组成。

注 3: 一个事态有时可能称为“事件”或“事故”。

[来源:ISO Guide73:2009,3.5.1.3,有修改:删除注 4]

3.22

外部语境 externalcontext

组织(3.50)寻求实现其目标(3.49)的外部环境。

注:外部语境可能包括如下方面:

— 文化、社会、政治、法律、监管、金融、技术、经济、自然和竞争环境,无论是国际的、国家的、地区的还是地方的;

— 影响组织(3.50) 目标(3.49)的关键驱动力和趋势;

— 与外部利益相关方(3.37)的关系及其认知和价值观 。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
https://d.book118.com/037201053036006136