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。

2.9

可用性 availability

根据授权实体的要求可访问和可使用的特性。

2.10

基本测度 base measure

用某个**属性**(2.4)及其量化方法定义的**测度**(2.47)。

[ISO/IEC 15939:2007,定义 2.3,做了修改:删除注 2]

注:基本测度在功能上独立于其他**测度**(2.47)。

2.11

能力 competence

应用知识和技能实现预期结果的才能。

2.12

保密性 confidentiality

信息对未授权的个人、实体或**过程**(2.61)不可用或不泄露的特性。

2.13

符合性 conformity

对**要求**(2.63)的满足。

注:术语"一致性"是被弃用的同义词。

2.14

后果 consequence

事态(2.25)影响**目标**(2.56)的结果。

[ISO Guide 73:2009,定义 3.6.1.3,做了修改]

注 1:一个**事态**(2.25)可能导致一系列后果。

注 2:一个后果可以是确定的或不确定的,在**信息安全**(2.33)的语境下通常是负面的。

注 3:后果可以被定性或定量地表示。

注 4:初始后果可能因连锁效应升级。

2.15

持续改进 continual improvement

为提高**性能**(2.59)的反复活动。

2.16

控制 control

改变**风险**(2.68)的措施。

[ISO Guide 73:2009,定义 3.8.1.1]

注 1:控制包括任何改变**风险**(2.68)的**过程**(2.61)、**策略**(2.60)、设备、实践或其他措施。

注 2:控制不一定总是达到预期或假定的风险改变效果。

2.17

控制目标 control objective

描述**控制**(2.16)的实施结果所要达到目标的声明。

2.18

纠正 correction

消除已查明的**不符合**(2.53)的措施。

2.19

整改措施 corrective action

消除**不符合**(2.53)成因以防再次发生的措施。

2.20

数据 data

基本测度(2.10)、**导出测度**(2.22)和(或)**指标**(2.30)所赋值的集合。

[ISO/IEC 15939:2007,定义 2.4,做了修改:增加注 1]

注:这个定义只适用于 ISO/IEC 27004 的语境。

2.21

决策准则 decision criteria

用于确定行动或进一步需要调查或者描述给定结果置信度的阈值、目标或模式。

[ISO/IEC 15939:2007,定义 2.7]

2.22

导出测度 derived measure

定义为两个或两个以上**基本测度**(2.10)值的函数的**测度**(2.10)。

[ISO/IEC 15939:2007,定义 2.8,做了修改:删除注 1]

2.23

文档化信息 documented information

组织(2.57)需要控制和维护的信息及其载体。

注 1:文档化信息可以采用任何格式,在任何载体中,出自任何来源。

注 2:文档化信息可能涉及

——**管理体系**(2.46),包括相关**过程**(2.61);

——为**组织**(2.57)运作所创建的信息(文档);

——结果实现的证据(记录)。

2.24

有效性 effectiveness

实现所计划活动和达成所计划结果的程度。

2.25

事态 event

一组特定情形的发生或改变。

[ISO Guide 73:2009,定义 3.5.1.3,做了修改:删除注 4]

注 1:一个事态可能是一个或多个发生,并可能有多种原因。

注 2:一个事态可能由一些未发生的事情组成。

注 3:一个事态可能有时被称为“事件”或“事故”。

2.26

执行管理者 executive management

为达成**组织**(2.57)意图,承担由组织**治理者**(2.29)委派的战略和策略实现责任的人或一组人。

注:执行管理者有时称为**最高管理者**(2.84),可以包括首席执行官、首席财务官、首席信息官和类似的角色。

2.27

外部语境 external context

组织(2.57)寻求实现其**目标**(2.56)的外部环境。

[ISO Guide 73:2009,定义 3.3.1.1]

注:外部语境可以包括如下方面:

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

——影响**组织**(2.57)**目标**(2.56)的关键驱动力和趋势;

——与外部**利益相关方**(2.82)的关系及其认知和价值观。

2.28

信息安全治理　governance of information security

指导和控制**组织**(2.57)**信息安全**(2.33)活动的体系。

2.29

治理者　governing body

对**组织**(2.57)的**性能**(2.59)和合规负有责任的人或一组人。

注：治理者在某些司法管辖区可以是董事会。

2.30

指标　indicator

针对定义的**信息需求**(2.31)，为**分析模型**(2.2)导出的**属性**(2.4)提供估算或评价的**测度**(2.47)。

2.31

信息需求　information need

对**目标**(2.56)、目的、风险和问题进行管理所必需的洞察。

[ISO/IEC 15939:2007，定义 2.12]

2.32

信息处理设施　information processing facilities

任何的信息处理系统、服务或基础设施，或者其安置的物理位置。

2.33

信息安全　information security

对信息的**保密性**(2.12)、**完整性**(2.40)和**可用性**(2.9)的保持。

注：另外，也可包括诸如**真实性**(2.8)、可核查性、**抗抵赖**(2.54)和**可靠性**(2.62)等其他特性。

2.34

信息安全持续性　information security continuity

确保**信息安全**(2.33)持续作用的**过程**(2.61)和规程。

2.35

信息安全事态　information security event

识别到的一种系统、服务或网络状态的发生，表明可能违反**信息安全**(2.33)**策略**(2.60)或**控制**(2.16)失效，或者一种可能与信息安全相关但还不为人知的情况。

2.36

信息安全事件　information security incident

单一或一系列不希望或意外的，极有可能损害业务运行和威胁**信息安全**(2.33)的**信息安全事态**(2.35)。

2.37

信息安全事件管理　information security incident management

发现、报告、评估、响应、处理和总结**信息安全事件**(2.36)的**过程**(2.61)。

2.38

信息共享社区　information sharing community

同意共享信息的**组织**(2.57)群体。

注：**组织**(2.57)可以是一个人。

2.39

信息系统　information system

应用、服务、信息技术资产或其他信息处理组件。

2.40

完整性 integrity

准确和完备的特性。

2.41

受益相关方 interested party

对于一项决策或活动，可能对其产生影响，或被其影响，或认为自己受到其影响的人或**组织**(2.57)。

2.42

内部语境 internal context

组织(2.57)寻求实现其目标的内部环境。

[ISO Guide 73:2009，定义 3.3.1.2]

注：内部语境可以包括如下方面：

——治理、组织结构、角色和职责；

——**策略**(2.60)、**目标**(2.56)和要实现它们的战略；

——在资源和知识方面的能力[如资本、时间、人员、**过程**(2.61)、系统和技术]；

——**信息系统**(2.39)、信息流和决策**过程**(2.61)(正式的和非正式的)；

——与内部**利益相关方**(2.82)的关系及其认知和价值观；

——**组织**(2.57)的文化；

——**组织**(2.57)采用的标准、指南和模型；

——契约关系的形式和程度。

2.43

信息安全管理体系项目 ISMS project

组织(2.57)为实施 ISMS 所开展的结构化活动。

2.44

风险程度 level of risk

以**后果**(2.14)和其**可能性**(2.45)的组合来表示的**风险**(2.68)大小。

[ISO Guide 73:2009，定义 3.6.1.8，做了修改：删除定义中的“或风险组合”]

2.45

可能性 likelihood

某事发生的概率。

[ISO Guide 73:2009，定义 3.6.1.1，做了修改：删除注 1 和注 2]

2.46

管理体系 management system

组织中相互关联或相互作用的要素集，用来建立**策略**(2.60)和**目标**(2.56)以及达到这些目标的**过程**(2.61)。

注 1：一个管理体系可能专注于单一学科或多个学科。

注 2：体系要素包括组织结构、角色和责任、规划、运行。

注 3：一个管理体系范围可能包括**组织**(2.57)的整体、**组织**(2.57)的特定且确定的功能、**组织**(2.57)的特定且确定的部门，或者跨一组**组织**(2.57)的一个或多个功能。

2.47

测度 measure

作为**测量**(2.48)结果赋值的变量。

[ISO/IEC 15939:2007，定义 2.15，做了修改]

注：术语“测度”是**基本测度**(2.10)、**导出测度**(2.22)和**指标**(2.30)的统称。

2.48

测量 measurement

确定一个值的**过程**(2.61)。

注：在**信息安全**(2.33)的语境下，确定一个值的**过程**(2.61)需要使用**测量方法**(2.50)、**测量函数**(2.49)、**分析模型**(2.2)和**决策准则**(2.21)，获得关于**信息安全**(2.33)**管理体系**(2.46)及其相关**控制**(2.16)**有效性**(2.24)的信息。

2.49

测量函数 measurement function

组合两个或两个以上**基本测度**(2.10)的算法或计算。

[ISO/IEC 15939:2007，定义 2.20]

2.50

测量方法 measurement method

用于按规定的**尺度**(2.80)量化**属性**(2.4)的通用逻辑操作序列。

[ISO/IEC 15939:2007，定义 2.22，做了修改：删除注 2]

注：测量方法的类型取决于**属性**(2.4)量化操作的性质。可区分为以下两种类型：

——主观的：包含人为判断的量化；

——客观的：基于数字规则的量化。

2.51

测量结果 measurement results

对**信息需要**(2.31)的一个或多个**指标**(2.30)及其相关解释。

2.52

监视 monitoring

确定系统、**过程**(2.61)或活动状态的行为。

注：为确定状态可能需要检查、监督或严密观察。

2.53

不符合 nonconformity

对**要求**(2.63)的不满足。

2.54

抗抵赖 non-repudiation

证明所声称**事态**(2.25)或行为的发生及其源头的能力。

2.55

对象 object

通过**测量**(2.48)其**属性**(2.4)来描述其特性的事项。

2.56

目标 objective

要实现的结果。

注 1：目标可以是战略性的、战术性的或操作性的。

注 2：目标可以涉及不同学科(诸如金融、健康与安全以及环境目标)，可以适用于不同层次[诸如战略、组织、项目、产品和**过程**(2.61)]。

注 3：目标可以以其他方式表示，例如，作为预期结果、意图、操作准则，作为**信息安全**(2.33)目标，或者使用具有类似含义的其他词(例如，目的或标靶)。

注 4：在**信息安全**(2.33)**管理体系**(2.46)的语境下，**组织**(2.57)制定与**信息安全**(2.33)**策略**(2.60)一致的**信息安全**(2.33)目标以实现特定结果。

2.57

组织 organization

具有自身的功能、责任、权威和关系来实现其**目标**(2.56)的人或一组人。

注：组织的概念包括但不限于个体经营者、公司、法人、商行、企业、机关、合伙关系、慈善机构或院校，或部分或其组合，不论注册与否，公共的还是私营的。

2.58

外包　outsource

做出由外部**组织**(2.57)执行部分的**组织**(2.57)功能或**过程**(2.61)的安排。

注：外部组织在**管理体系**(2.46)的范围之外，尽管外包的功能或**过程**(2.61)在范围之内。

2.59

性能　performance

可测量的结果。

注 1：性能可以涉及定量或定性的调查结果。

注 2：性能可以涉及活动、**过程**(2.61)、产品(包括服务)、系统或**组织**(2.57)的管理。

2.60

策略　policy

由**最高管理者**(2.84)正式表达的**组织**(2.57)的意图和方向。

2.61

过程　process

将输入转换成输出的相互关联或相关作用的活动集。

2.62

可靠性　reliability

与预期行为和结果一致的特性。

2.63

要求　requirement

明示的、默认的或强制性的需要或期望。

注 1："默认的"意指所考虑的需要或期望是不言而喻的，对于**组织**(2.57)或**受益相关方**(2.41)是惯例或常见做法。

注 2：指定要求是在例如**文档化信息**(2.23)中明示的。

2.64

残余风险　residual risk

风险处置(2.79)后余下的**风险**(2.68)。

注 1：残余风险可能包含未识别的**风险**(2.68)。

注 2：残余风险也可以被称为"保留风险"。

2.65

评审　review

针对实现所设立**目标**(2.54)的主题，为确定其适宜性、充分性和**有效性**(2.24)而采取的活动。

[ISO Guide 73:2009，定义 3.8.2.2，做了修改：删除注 1]

2.66

评审对象　review object

被评审的特定事项。

2.67

评审目标　review objective

描述**评审**(2.65)结果要达到什么的陈述。

2.68

风险　risk

对目标的不确定性影响。

[ISO Guide 73:2009，定义 1.1，做了修改]

注 1：影响是指与期望的偏离(正向的或反向的)。

注 2：不确定性是对**事态**(2.25)及其**结果**(2.14)或**可能性**(2.45)的相关信息、理解或知识缺乏的状态(即使是部分的)。

注 3：风险常被表征为潜在的**事态**(2.25)和**后果**(2.14)，或者它们的组合。

注 4：风险常被表示为**事态**(2.25)的**后果**(2.14)(包括情形的改变)和其发生**可能性**(2.45)的组合。

注 5：在**信息安全**(2.33)**管理体系**(2.46)的语境下，**信息安全**(2.33)风险可被表示为对**信息安全**(2.33)**目标**(2.56)的不确定性影响。

注 6：**信息安全**(2.33)风险与**威胁**(2.83)利用信息资产或信息资产组的**脆弱性**(2.89)对**组织**(2.57)造成危害的潜力相关。

2.69

风险接受　risk acceptance

接纳特定**风险**(2.68)的有根据的决定。

[ISO Guide 73:2009，定义 3.7.1.6]

注 1：可不经**风险处置**(2.79)或在**风险处置**(2.79)**过程**(2.61)中做出风险接受。

注 2：接受的**风险**(2.68)要受到**监视**(2.52)和**评审**(2.65)。

2.70

风险分析　risk analysis

理解**风险**(2.68)本质和确定**风险等级**(2.44)的**过程**(2.61)。

[ISO Guide 73:2009，定义 3.6.1]

注 1：风险分析提供**风险评价**(2.74)和**风险处置**(2.79)决策的基础。

注 2：风险分析包括风险估算。

2.71

风险评估　risk assessment

风险识别(2.75)、**风险分析**(2.70)和**风险评价**(2.74)的整个**过程**(2.61)。

[ISO Guide 73:2009，定义 3.4.1]

2.72

风险沟通与咨询　risk communication and consultation

组织(2.57)就**风险**(2.68)管理所进行的，提供、共享或获取信息以及与**利益相关方**(2.82)对话的持续和迭代**过程**(2.61)。

注 1：这些信息可能涉及到**风险**(2.68)的存在、性质、形式、**可能性**(2.45)、重要性、评价、可接受性和处置。

注 2：咨询是对问题进行决策或确定方向之前，在**组织**(2.57)和其**利益相关方**(2.82)之间进行知情沟通的双向**过程**(2.51)。

咨询是：

——通过影响力而不是权力来影响决策的**过程**(2.61)；

——决策的输入，而非联合决策。

2.73

风险准则　risk criteria

评价**风险**(2.68)重要性的参照条款。

[ISO Guide 73:2009，定义 3.3.1.3]

注 1：风险准则是基于组织的目标以及**外部语境**(2.27)和**内部语境**(2.42)。

注 2：风险准则可来自标准、法律、**策略**(2.60)和其他**要求**(2.63)。

2.74

风险评价　risk evaluation

将**风险分析**(2.70)的结果与**风险准则**(2.73)比较以确定**风险**(2.68)和(或)其大小是否可接受或可容忍的**过程**(2.61)。

[ISO Guide 73:2009,定义 3.7.1]

注：风险评价辅助**风险处置**(2.79)的决策。

2.75

风险识别　risk identification

发现、识别和描述**风险**(2.61)的**过程**(2.61)。

[ISO Guide 73:2009,定义 3.5.1]

注 1：风险识别涉及风险源、**事态**(2.25)及其原因和潜在**后果**(2.14)的识别。

注 2：风险识别可能涉及历史数据、理论分析、知情者和专家的意见以及**利益相关方**(2.82)的需要。

2.76

风险管理　risk management

指导和控制**组织**(2.57)相关**风险**(2.57)的协调活动。

[ISO Guide 73:2009,定义 2.1]

2.77

风险管理过程　risk management process

管理**策略**(2.60)、规程和实践在沟通、咨询、语境建立以及识别、分析、评价、处置、监视和评审**风险**(2.68)活动上的系统性应用。

[ISO Guide 73:2009,定义 3.1,做了修改:增加注 1]

注：ISO/IEC 27005 使用术语“**过程**”(2.61)来描述全面风险管理。在**风险管理**(2.76)**过程**(2.61)中的要素被称为“活动”。

2.78

风险责任者　risk owner

具有责任和权威来管理**风险**(2.68)的人或实体。

[ISO Guide 73:2009,定义 3.5.1.5]

2.79

风险处置　risk treatment

改变**风险**(2.68)的**过程**(2.61)。

[ISO Guide 73:2009,定义 3.8.1,做了修改:将注 1 中的“决策”替换为“选择”]

注 1：风险处置可能涉及如下方面：

——通过决定不启动或不继续进行产生**风险**(2.68)的活动来规避**风险**(2.68)；

——承担或增加**风险**(2.68)以追求机会；

——消除**风险**(2.68)源；

——改变**可能性**(2.45)；

——改变**后果**(2.14)；

——与另外一方或多方共担**风险**(2.68)(包括合同和风险融资)；

——有根据地选择保留**风险**(2.68)。

注 2：处理负面**后果**(2.14)的风险处置有时被称为“风险缓解”“风险消除”“风险防范”和“风险降低”。

注 3：风险处置可能产生新的**风险**(2.68)或改变现有**风险**(2.68)。

2.80

尺度　scale

连续的或离散的值的有序集合,或者对应**属性**(2.4)的类集合。

[ISO/IEC 15939:2007,定义 2.35,做了修改]

注：尺度的类型取决于尺度上值之间关系的性质。通常定义如下四种尺度类型：

——名义的：**测量**(2.48)值是类别化的；

——顺序的：**测量**(2.48)值是序列化的；

——间距的：**测量**(2.48)值对应于**属性**(2.4)的等同量是等距离的；

——比率的：**测量**(2.48)值对应于**属性**(2.4)的等同量是等距离的，其中零值对应于属性的空。

这些只是尺度类型的示例。

2.81

安全实施标准　security implementation standard

规定授权的安全实现方式的文件。

2.82

利益相关方　stakeholder

对于一项决策或活动，可能对其产生影响，或被其影响，或认为自己受到其影响的人或**组织**(2.57)。

[ISO Guide 73:2009，定义 3.2.1.1，做了修改：删除注 1]

2.83

威胁　threat

可能对系统或**组织**(2.57)造成危害的不期望事件的潜在原由。

2.84

最高管理者　top management

最高层指导和控制**组织**(2.57)的人或一组人。

注 1：最高管理者具有在**组织**(2.57)内授权和提供资源的权力。

注 2：如果**管理体系**(2.46)的范围只涵盖**组织**(2.57)的一部分，则最高管理者就是指指导和控制**组织**(2.57)这部分的人或一组人。

2.85

可信信息通信实体　trusted information communication entity

支持在**信息共享社区**(2.38)内进行信息交换的自主**组织**(2.57)。

2.86

测量单位　unit of measurement

按惯例被定义和被采纳的特定量，用于其他同类量与其比较以表示它们相对于这个量的大小。

[ISO/IEC 15939:2007，定义 2.40，做了修改]

2.87

确认　validation

通过提供客观证据，证实满足特定预期使用或应用**要求**(2.63)的行为。

[ISO 9000:2015，定义 3.8.12，做了修改]

2.88

验证　verification

通过提供客观证据，证实满足规定**要求**(2.63)的行为。

[ISO 9000:2015，定义 3.8.4]

注：这也可被称为符合性测试。

2.89

脆弱性　vulnerability

可能被一个或多个**威胁**(2.83)利用的资产或**控制**(2.16)的弱点。

3　信息安全管理体系

3.1　概要

各种类型和规模的组织：

a)　收集、处理、存储和传输信息；

b) 认识到信息及其相关过程、系统、网络和人是实现组织目标的重要资产；

c) 面临可能影响资产运作的一系列风险；

d) 通过实施信息安全控制应对其感知的风险。

组织持有和处理的所有信息在使用中易受到攻击、过失、自然灾害(例如,洪水或火灾)等威胁以及内在脆弱性的影响。术语“信息安全”一般是建立在被认为有价值的信息资产的基础上,这些信息需要适当的保护,例如,防止可用性、保密性和完整性的丧失。使准确和完整的信息对已授权的需要者及时可用,可促进提升业务效率。

通过有效地定义、实现、维护和改进信息安全来保护信息资产,对于组织实现其目标并保持和增强其合法及形象,必不可少。指导适当控制的实施和处置不可接受的信息安全风险这些协调活动,通常被认为是信息安全管理的要素。

由于信息安全风险和控制的有效性随着环境的变化而改变,组织需要：

a) 监视和评价已实施的控制和规程的有效性；

b) 识别待处置的新出现的风险；

c) 视需要选择、实施和改进适当的控制。

为了关联和协调这类信息安全活动,每个组织需要建立其信息安全策略和目标,并通过使用管理体系有效地实现这些目标。

3.2 什么是 ISMS

3.2.1 概述和原则

信息安全管理体系(ISMS)由策略、规程、指南和相关资源及活动组成,由组织集中管理,目的在于保护其信息资产。ISMS 是建立、实施、运行、监视、评审、维护和改进组织信息安全来实现业务目标的系统方法。它是基于风险评估和组织的风险接受程度,为有效地处置和管理风险而设计。分析信息资产保护要求,并按要求应用适当的控制来切实保护这些信息资产,有助于 ISMS 的成功实施。下列基本原则也有助于 ISMS 的成功实施：

a) 意识到信息安全的需要；

b) 分配信息安全的责任；

c) 包含管理者的承诺和利益相关方的利益；

d) 提升社会价值；

e) 进行风险评估来确定适当的控制,以达到可接受的风险程度；

f) 将安全作为信息网络和系统的基本要素；

g) 主动防范和发现信息安全事件；

h) 确保信息安全管理方法的全面性；

i) 持续对信息安全进行再评估并在适当时进行修正。

3.2.2 信息

信息是一种资产,像其他重要的业务资产一样,对组织业务来说必不可少,因此需要得到适当保护。信息可以以多种形式存储,包括：数字形式(例如,存储在电子或光介质上的数据文件)、物质形式(例如,在纸上),以及以员工知识形式存在、未被表现的信息。信息可以采用各种手段进行传输,包括：信使、电子通信或口头交流。不管信息采用什么形式存在或什么手段传输,它总是需要适当的保护。

在许多组织中,信息依赖于信息和通信技术。这种技术往往是组织的基本要素,协助信息的创建、处理、存储、传输、保护和销毁。

3.2.3 信息安全

信息安全确保信息的保密性、可用性和完整性。信息安全包含应用和管理适当的控制，这些控制广泛地考虑到各种威胁，目标是确保业务的持续成功和连续性，并最大限度地减少信息安全事件的后果。

信息安全是通过实施一套适用的控制来实现，这套控制通过所采用的风险管理过程选出，并使用ISMS来管理，包括策略、过程、规程、组织结构、软件和硬件，用以保护已识别的信息资产。这些控制需要得到详细说明、实施、监视、评审和必要时的改进，以确保满足组织的特定信息安全和业务目标。相关信息安全控制宜与组织业务过程无缝集成。

3.2.4 管理

管理包含在适当的结构中指导、控制和持续改进组织的活动。管理活动包括组织、处理、指导、监督和控制资源的行为、方式或实践。管理结构从小规模组织中的一个人扩展到大规模组织中由许多人组成的管理层次结构。

就ISMS而言，管理包含通过保护组织的信息资产来实现业务目标所必要的监督和决策。信息安全的管理通过信息安全策略、规程和指南的制定与采用来表达，然后应用到整个组织中所有与组织相关的个人。

3.2.5 管理体系

管理体系采用一种资源框架来实现组织的目标。管理体系包括组织结构、策略、规划、责任、实践、规程、过程和资源。

就信息安全而言，管理体系使组织：

a) 满足客户和其他利益相关方的信息安全要求；
b) 改进组织的计划和活动；
c) 满足组织的信息安全目标；
d) 遵从法律法规、规章制度和行业规定；
e) 以有组织的方式管理信息资产，来促进持续改进和调整当前的组织目标。

3.3 过程方法

组织需要识别和管理众多活动来有效果和有效率地运作。任何使用资源的活动都需要被管理，以便能够使用一组相互关联或相互作用的活动完成输入到输出的转换，这也被称为过程。一个过程的输出可以直接形成另一个过程的输入，通常这个转换是在计划和受控的条件下完成。过程系统在组织中的应用，连同这些过程的识别和交互及其管理，可被称为“过程方法”。

3.4 为什么ISMS重要

与组织的信息资产相关的风险需要加以解决。实现信息安全需要管理风险，包括与组织内部或组织使用的所有形式的信息相关，来自物理、人类和技术相关威胁的风险。

采用ISMS宜是一个组织的战略决策，并且有必要根据组织的需要进行无缝集成、规模调整和更新。

设计和实施组织的ISMS受组织的需要和目标、安全要求、采用的业务过程以及组织的规模和结构影响。设计和运行ISMS需要反映组织的利益相关方(包括客户、供应商、业务伙伴、股东和其他相关第三方)的利益和信息安全要求。

在相互连接的世界中，信息和相关的过程、系统和网络组成关键业务资产。组织及其信息系统和网络面临来源广泛的安全威胁，包括计算机辅助欺诈、间谍活动、蓄意破坏、火灾和洪水。由恶意代码、计

算机黑客和拒绝服务攻击造成的信息系统和网络的损害已变得更加普遍、更有野心和日益复杂。

ISMS 对于公共和私营部门业务都是重要的。在任何行业,ISMS 是使电子商务成为可能,是风险管理活动所必需的。公共和私营网络的互联以及信息资产的共享增加了信息访问控制和处理的难度。另外,含有信息资产的移动存储设备的分布能够消弱传统控制的有效性。当组织采用了 ISMS 标准族,便可以向业务伙伴和其他受益相关方证明其运用一致的和互认的信息安全原则的能力。

在信息系统的设计和开发中,信息安全有时并没被考虑到的。而且,信息安全常被认为是技术解决方案。然而,能够通过技术手段实现的信息安全是有限的,并且若没有 ISMS 语境下适当的管理和规程支持,可能是无效的。将安全集成到已经功能完备的信息系统中可能是困难和昂贵的。ISMS 包含识别哪些控制已经就位,并且要求仔细规划和注意细节。举例来说,访问控制,可能是技术的(逻辑的)、物理的、行政的(管理的)或某种组合,提供一种手段来确保对信息资产的访问是基于业务和信息安全要求得到授权和受限制的。

成功采用 ISMS 对于保护信息资产是重要的,它使组织能够:

a) 更好地保障其信息资产得到持续的充分保护免受威胁;

b) 保持一个结构化和全面的框架,来识别和评估信息安全风险,选择和应用适用的控制,并测量和改进其有效性;

c) 持续改进其控制环境;

d) 有效地实现法律法规的合规性。

3.5 建立、监视、保持和改进 ISMS

3.5.1 概述

组织在建立、监视、保持和改进其 ISMS 时,需要采取如下步骤:

a) 识别信息资产及其相关的信息安全要求(见 3.5.2);

b) 评估信息安全风险(见 3.5.3)和处置信息安全风险(见 3.5.4);

c) 选择和实施相关控制来管理不可接受的风险(见 3.5.5);

d) 监视、保持和改进组织信息资产相关控制的有效性(见 3.5.6)。

为确保 ISMS 持续有效地保护组织的信息资产,有必要不断重复步骤 a)~d)来识别风险的变化,或者组织战略或业务目标的变化。

3.5.2 识别信息安全要求

在组织的整体战略和业务目标及其规模和地理分布的范围内,信息安全要求可以通过了解如下方面来识别:

a) 已识别的信息资产及其价值;

b) 信息处理、存储和通信的业务需求;

c) 法律法规、规章制度和合同要求。

对组织信息资产的相关风险进行的系统化评估将包含分析信息资产面临的威胁、信息资产存在的脆弱性、威胁实现的可能性,以及任何信息安全事件对信息资产的潜在影响。相关控制的支出宜与感知的风险成为现实时所造成的业务影响相称。

3.5.3 评估信息安全风险

管理信息安全需要一种适合的风险评估和风险处置方法,该方法可能包括成本和效益的估算、法律要求、利益相关方的关切和其他适合的输入和变量。

风险评估宜识别、量化并依据风险接受准则和组织目标排序风险。评估结果宜指导和确定适当的

管理行动及其优先级，以管理信息安全风险和实施所选择的控制来抵御这些风险。

风险评估宜包括估算风险大小（风险分析）的系统性方法和将估算的风险与风险准则比较来确定风险重要性（风险评价）的过程。

风险评估宜定期以及当发生重大变化时进行，以便应对信息安全要求和风险状况的变化，例如，资产、威胁、脆弱性、影响、风险评价等方面的变化。这些风险评估宜以系统化方式进行，从而能够产生可比较和可重现的结果。

信息安全风险评估为了有效宜有一个明确界定的范围，还宜包括与其他区域风险评估的关系（如果合适）。

ISO/IEC 27005 提供信息安全风险管理指南，包括对风险评估、风险处置、风险接受、风险报告、风险监视和风险评审的建议，还包括风险评估方法的示例。

3.5.4 处置信息安全风险

在考虑风险处置前，组织宜确定决定风险是否可接受的准则。如果评估结果是，例如，风险低或处置成本不符合成本效益，风险可能也会被接受。这样的决定宜被记录。

对于经过风险评估后识别的每个风险，需要做出风险处置决定。可能的风险处置选项包括如下：

a) 采用适当的控制来降低风险；

b) 在明显满足组织策略和风险接受准则的条件下，有意并客观地接受风险；

c) 通过不允许导致风险发生的行动来规避风险；

d) 与其他方共担相关风险，例如，保险公司或供应商。

对于那些已决定采用适当控制来处置的风险，宜选择和实施相应控制。

3.5.5 选择和实施控制

一旦识别了信息安全要求，明确和评估了所识别信息资产的信息安全风险（见 3.5.3），并做出了信息安全风险处置的决定，则选择和实施风险降低的控制。

控制宜确保将风险降低至可接受程度，并考虑到以下方面：

a) 国家法律法规的要求和约束；

b) 组织目标；

c) 运行要求和约束；

d) 风险降低的相关实施和运行成本，保持与组织要求和约束相称；

e) 监视、评价和改进信息安全控制的效果和效率，以支持组织的目标；

f) 控制的实施和运行投入与信息安全事件可能导致的损失之间平衡的需要。

ISO/IEC 27002 中规范的控制是公认的适用于多数组织的最佳实践，并易于裁剪来适应各种规模和复杂度的组织。ISMS 标准族中的其他标准为选择和应用 ISO/IEC 27002 控制来建立信息安全管理体系提供指南。

信息安全控制宜在系统和项目要求的规范与设计阶段就加以考虑。否则，可能导致额外成本和低效解决方案，最坏情况下，可能无法实现足够的安全。控制可以选自 ISO/IEC 27002 或其他控制集，或者设计新的控制来满足组织的特定需要。需要承认，一些控制可能不适用于每个信息系统或环境，可能不适用于所有组织。

有时需要时间来实施所选择的一组控制，但在这期间的风险程度可能不可长期承受。风险准则宜涵盖在实施控制期间风险的短期承受性。在分步实施控制时，宜告知受益相关方不同时间点上估算或预计的风险程度。

宜记住没有一套控制能够实现完全的信息安全。宜实施额外的管理行动来监视、评价和改进信息安全控制的效果和效率以支持组织目标。

宜在适用性声明中记录控制的选择和实施来辅助合规要求。

3.5.6 监视、保持和改进 ISMS 有效性

组织需要通过对照组织的策略和目标监视和评估执行情况，并将结果报告给管理者进行评审，来保持和改进 ISMS。这种 ISMS 评审将检查 ISMS 是否包含了适合处置 ISMS 范围内风险的控制。此外，基于所监视区域的记录，提供对纠正、预防和改进措施进行确认和追溯的证据。

3.5.7 持续改进

ISMS 持续改进的目标是增加对保持信息保密性、可用性和完整性目标实现的可能性。持续改进的关注点是寻求改进的机会，没有现有管理活动已经足够好或已尽力而为的假设。

改进措施包括如下：

a) 分析和评价现有状况来识别改进的地方；

b) 建立改进的目标；

c) 寻找实现目标的可能解决方案；

d) 评价这些解决方案并做出决策；

e) 实施所选择的解决方案；

f) 测量、验证、分析和评价改进结果，以确定目标已被满足；

g) 正式确认改进带来的变化。

必要时，对结果进行评审结果，以确定进一步的改进机会。如此，改进就是一个持续活动，即经常地重复行动。

3.6 ISMS 关键成功因素

很多因素对于一个组织成功实施 ISMS 来满足其业务目标都是关键的。关键成功因素的例子包括：

a) 信息安全策略、目标和与目标一致的活动；

b) 与组织文化一致的，信息安全设计、实施、监视、保持和改进的方法与框架；

c) 来自所有管理层级，特别是最高管理者的可见支持和承诺；

d) 对应用信息安全风险管理(见 ISO/IEC 27005)实现信息资产保护的理解；

e) 有效的信息安全意识、培训和教育计划，以使所有员工和其他相关方知悉在信息安全策略、标准等当中他们的信息安全义务，并激励他们做出相应的行动；

f) 有效的信息安全事件管理过程；

g) 有效的业务持续性管理方法；

h) 评价信息安全管理性能的测量系统和反馈的改进建议。

ISMS 将增加组织持续实现其信息资产所需关键成功因素的可能性。

3.7 ISMS 标准族的益处

实施 ISMS 的益处主要体现在信息安全风险的降低[即降低信息安全事件发生的可能性和(或)造成的影响]。特别是，通过采用 ISMS 标准族为组织实现持续成功带来如下益处：

a) 一个结构化框架来支持规范、实施、运行和保持一个全面的、经济有效的、创造价值的、集成和一致的 ISMS 这一过程，以满足组织跨不同运行和场所的需要。

b) 在企业风险管理和治理的语境下，协助管理者以负责任的方式始终如一地管理和运用其信息安全管理方法，包括对业务和系统责任者进行整体信息安全管理的教育和培训。

c) 以非定型的方式推广全球公认的良好信息安全实践，给组织一定的自由度来采纳和改进适合

其特定环境的相关控制，并在面临内部和外部变化的情况下保持这些控制。

d) 为信息安全提供共同语言和概念基础，使得在业务伙伴中利用合规的 ISMS 建立信心更为容易，尤其是当他们需要由一个认可的认证机构进行 ISO/IEC 27001 认证时。

e) 增加利益相关方对组织的信任。

f) 满足社会的需要和期望。

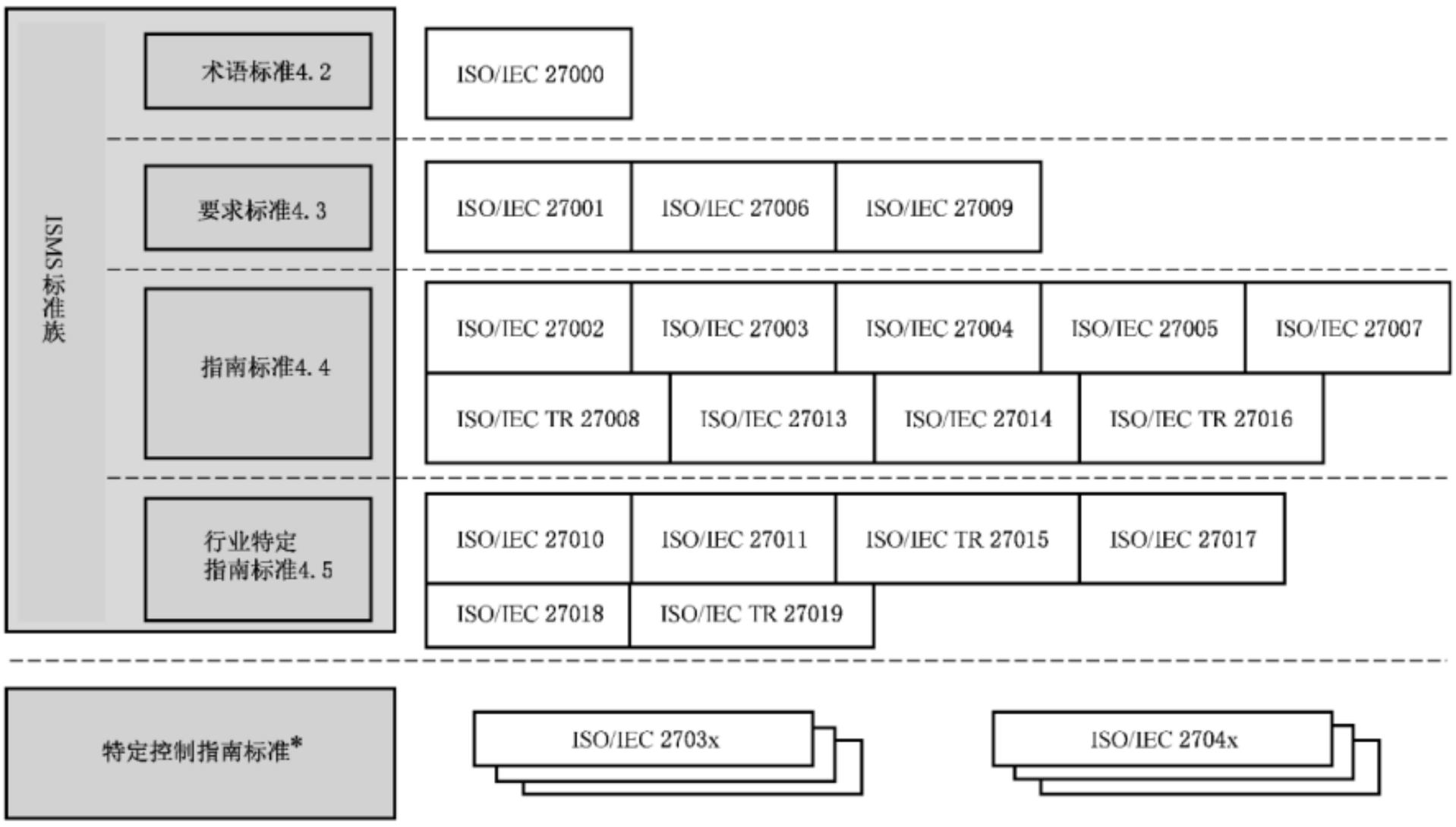
g) 更有效、经济的信息安全投资管理。

4 信息安全管理体系标准族

4.1 一般信息

信息安全管理体系(ISMS)标准族由一系列已发布的或制定中的相互关联的标准组成，并包含许多重要的结构组件。这些组件着重于对 ISMS 要求(ISO/IEC 27001)、对进行 ISO/IEC 27001 符合性认证的认证机构的要求(ISO/IEC 27006)和对行业特定 ISMS 实施的附加要求框架(ISO/IEC 27009)进行描述的规范性标准。其他标准提供 ISMS 实施的各方面指南，包括通用过程以及行业特定指南。

ISMS 标准族中各标准之间的关系如图 1 所示。



* 本标准范围之外。

图 1 ISMS 标准族关系

ISMS 标准族的每一个标准按照其在 ISMS 标准族中的类型(或角色)和编号分别在下面描述。相应的条款为：

a) 给出概述和术语的标准(见 4.2)；

b) 规范要求的标准(见 4.3)；

c) 给出一般指南的标准(见 4.4)；

d) 给出行业特定指南的标准(见 4.5)。

4.2 给出概述和术语的标准

4.2.1 ISO/IEC 27000

信息技术 安全技术 信息安全管理体系 概述和词汇

范围:该标准为组织和个人提供:

a) ISMS 标准族的概述;

b) 信息安全管理体系的介绍;

c) ISMS 标准族中使用的术语和定义。

目的:该标准描述信息安全管理体系的基础,形成 ISMS 标准族的主题,并定义相关术语。

4.3 规范要求的标准

4.3.1 ISO/IEC 27001

信息技术 安全技术 信息安全管理体系 要求

范围:该标准规范在组织整体业务风险的语境下建立、实施、运行、监视、评审、保持和改进正式信息安全管理体系(ISMS)的要求。它规范可被用来定制以满足单个组织或其部门需要的信息安全控制的实现要求。该标准可被用于所有类型、规模和性质的组织。

目的:ISO/IEC 27001 为 ISMS 的开发和运行提供规范性要求,包括一套控制和降低信息资产相关风险的控制。组织通过运行 ISMS 寻求对其信息资产的保护。组织可以对其运行的 ISMS 的符合性进行审核和认证。作为 ISMS 过程的一部分,应从 ISO/IEC 27001 附录 A 中选择对所识别要求适合的控制目标和控制。ISO/IEC 27001 附录 A.1 中列出的控制目标和控制是直接来自 ISO/IEC 27002 第 5 章~第 18 章并与其一致。

4.3.2 ISO/IEC 27006

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

范围:该标准在 ISO/IEC 17021 所含要求的基础上,为依据 ISO/IEC 27001 提供审核和 ISMS 认证的机构,规范要求并提供指南。它主要为依据 ISO/IEC 27001 提供 ISMS 认证的认证机构的认可提供支持。

目的:ISO/IEC 27006 是对 ISO/IEC 17021 的补充,提供对认证组织进行认可的要求,以此许可这些组织一贯地提供对 ISO/IEC 27001 要求的符合性认证。

4.4 给出一般指南的标准

4.4.1 ISO/IEC 27002

信息技术 安全技术 信息安全控制实践指南

范围:该标准提供一套被广泛接受的控制目标和最佳实践的控制,为选择和实施实现信息安全的控制提供指南。

目的:ISO/IEC 27002 提供关于信息安全控制实施的指南。特别是第 5 章~第 18 章为支持 ISO/IEC 27001 中所规范的控制提供最佳实践方面的具体实施建议和指南。

4.4.2 ISO/IEC 27003

信息技术 安全技术 信息安全管理体系实施指南

范围:该标准为依据 ISO/IEC 27001 建立、实施、运行、监视、评审、保持和改进 ISMS 提供实用的实施指南和进一步信息。

目的:ISO/IEC 27003 为依据 ISO/IEC 27001 成功实施 ISMS 提供面向过程的方法。

4.4.3 ISO/IEC 27004

信息技术 安全技术 信息安全管理 测量

范围:该标准为了对 ISO/IEC 27001 所规范的,用于实施和管理信息安全的,ISMS、控制目标和控制的有效性进行评估,提供测量的开发和使用指南及建议。

目的:ISO/IEC 27004 提供一种测量框架,以便能够依据 ISO/IEC 27001 对 ISMS 的有效性进行测量。

4.4.4 ISO/IEC 27005

信息技术 安全技术 信息安全风险管理

范围:该标准为信息安全风险管理提供指南。该标准给出的方法支持 ISO/IEC 27001 中所规范的一般概念。

目的:ISO/IEC 27005 为实施面向过程的风险管理方法提供指南,有助于圆满实施和兑现 ISO/IEC 27001 中的信息安全风险管理要求。

4.4.5 ISO/IEC 27007

信息技术 安全技术 信息安全管理体系审核指南

范围:该标准在适用于一般管理体系的 ISO 19011 指南的基础上,为 ISMS 审核实施以及信息安全管理体系审核员能力提供指南。

目的:ISO/IEC 27007 为需要依据 ISO/IEC 27001 中所规范的要求,进行 ISMS 内部或外部审核或者管理 ISMS 审核方案的组织提供指南。

4.4.6 ISO/IEC TR 27008

信息技术 安全技术 信息安全控制措施审核员指南

范围:该指导性技术文件为评审控制措施的实施和运行符合组织建立的信息安全标准提供指南,包括信息系统控制措施的技术符合性检查。

目的:该指导性技术文件重点在于评审信息安全控制措施,包括对照组织建立的信息安全实施标准检查技术符合性。它不是为分别在 ISO/IEC 27004、ISO/IEC 27005 或 ISO/IEC 27007 中规范的测量、风险评估或 ISMS 审核,提供任何具体的符合性检查指南。该指导性技术文件不用于管理体系审核。

4.4.7 ISO/IEC 27013

信息技术 安全技术 ISO/IEC 27001 和 ISO/IEC 20000-1 综合实施指南

范围:该标准为组织进行如下任何一种 ISO/IEC 27001 和 ISO/IEC 20000-1 的综合实施提供指南:

a) 在已经实施了 ISO/IEC 20000-1 的情况下实施 ISO/IEC 27001,或者反之;

b) 同时实施 ISO/IEC 27001 和 ISO/IEC 20000-1;

c) 集成现有的 ISO/IEC 27001 和 ISO/IEC 20000-1 管理体系。

该标准专门聚焦在综合实施 ISO/IEC 27001 中所规范的信息安全管理系统(ISMS)和 ISO/IEC 20000-1 中所规范的服务管理体系(SMS)。

目的:为组织提供对 ISO/IEC 27001 和 ISO/IEC 20000-1 的特征和异同的更好理解,有助于规划同时符合两个标准的综合管理体系。

4.4.8 ISO/IEC 27014

信息技术 安全技术 信息安全治理

范围:该标准就信息安全治理的原则和过程提供指南,组织依此可以评价、指导和监视信息安全管理。

目的:信息安全已成为组织的一个关键问题。不仅法律法规要求日益增加,而且组织的信息安全措

施失效会直接影响其声誉。因此,治理者越来越需要承担起治理责任中的信息安全监督职责,来确保组织目标的实现。

4.4.9 ISO/IEC TR 27016

信息技术 安全技术 信息安全管理 组织经济学

范围:该指导性技术文件提供一种方法学,以使组织能够更好地从经济上理解如何准确估价其所识别的信息资产,评价这些信息资产面临的潜在风险,认识对这些信息资产进行保护控制的价值,并确定用于保护这些信息资产的资源最佳配置程度。

目的:该指导性技术文件在组织所处的更广泛社会环境的语境下,在组织信息资产的保护中叠加经济视角,并通过模型和例子提供如何应用信息安全组织经济学的指南,是对 ISMS 标准族的补充。

4.5 给出行业特定指南的标准

4.5.1 ISO/IEC 27010

信息技术 安全技术 行业间和组织间通信的信息安全管理

范围:该标准在 ISMS 标准族已有指南的基础上,为在信息共享社区中实施信息安全管理提供指南,特别是为在组织间和行业间启动、实施、保持和改进信息安全另外提供控制和指南。

目的:该标准适用于所有形式的敏感信息交换与共享,不论公共的还是私人的、国内的还是国际的、同行业或市场的还是行业间的。特别是,它可适用于与组织或国家关键基础设施的供给、维护和保护相关的信息交换与共享。

4.5.2 ISO/IEC 27011

信息技术 安全技术 基于 ISO/IEC 27002 的电信组织信息安全管理指南

范围:该标准为支持在电信组织中实施信息安全控制提供指南。

目的:ISO/IEC 27011 能使电信组织满足保密性、完整性、可用性和任何其他相关安全属性的信息安全管理基线要求。

4.5.3 ISO/IEC TR 27015

信息技术 安全技术 金融服务信息安全管理指南

范围:该指导性技术文件在 ISMS 标准族已有指南的基础上,为在提供金融服务的组织中启动、实施、保持和改进信息安全提供指南。

目的:该指导性技术文件是对 ISO/IEC 27001 和 ISO/IEC 27002 的专业补充,为提供金融服务的组织所用,以提供如下方面的支持:

a) 启动、实施、保持和改进基于 ISO/IEC 27001 的信息安全管理体系。

b) 设计和实施 ISO/IEC 27002 或该标准中定义的控制。

4.5.4 ISO/IEC 27017

信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实践指南

范围:ISO/IEC 27017 通过提供如下指南给出适用于云服务供给和使用的信息安全控制指南:

——ISO/IEC 27002 中规范的相关控制的额外实施指南;

——与云服务特别相关的额外控制及其实施指南。

目的:该标准为云服务提供者和云服务客户提供控制和实施指南。

4.5.5 ISO/IEC 27018

信息技术　安全技术　可识别个人信息(PII)处理者在公有云中保护 PII 的实践指南

范围:ISO/IEC 27018 按照 ISO/IEC 29100 中公有云计算环境下的隐私保护原则,为保护可识别个人信息(PII)建立被广泛接受的控制目标和控制,并提供措施的实施指南。

目的:该标准适用于通过与其他组织签约的云计算提供信息处理服务,作为 PII 处理者的组织,不论公共企业还是私营企业、政府机构还是非营利组织。该标准中的指南可能与作为 PII 控制者的组织也有关,但 PII 控制者可能受制于额外的,不适用于 PII 处理者的且不在该标准范围内的,保护 PII 的法律法规、规章制度和义务。

4.5.6 ISO/IEC TR 27019

信息技术　安全技术　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

范围:ISO/IEC TR 27019 就能源供给行业过程控制系统中实施的信息安全控制提供指南。能源供给行业的过程控制系统,与支持过程的控制相结合,对电力、燃气和供热的产生、传输、存储和分配进行控制和监视。特别是包括如下系统、应用和组件:

——全面信息技术(IT)支持的集中式和分布式过程控制、监视和自动化技术以及用于其运行的 IT 系统,诸如编程和参数化设备;

——数字控制器和自动化组件,诸如控制和现场设备或可编程逻辑控制器(PLC),包括数字传感器和执行器元件;

——过程控制领域中用到的所有进一步的 IT 系统支持,例如对补充的数据可视化任务的支持,对控制、监控、数据归档和文档化的支持;

——过程控制领域中用到的全部通信技术,例如,网络、遥测、远程控制应用和远程控制技术;

——数字计量和测量装置,例如,对能量消耗、产生和释放的测量;

——数字保护和安全系统,例如,继电保护或安全 PLC;

——未来智能电网环境下的分布式组件;

——上述系统中安装的所有软件、固件和应用。

目的:在 ISO/IEC 27002 所规范的安全目标和措施的基础上,该指导性技术文件为能源供给行业和能源供应商使用的系统提供满足其进一步特定要求的信息安全控制的指南。

4.5.7 ISO 27799

健康信息学　使用 ISO/IEC 27002 的健康信息安全管理

范围:该标准为支持信息安全管理在健康组织中实施提供指南。

目的:ISO 27799 基于 ISO/IEC 27002,除了那些满足 ISO/IEC 27001 附录 A 要求的指南外,为健康组织提供其行业独特的指南。

附 录 A
（资料性附录）
条款表达的措辞形式

ISMS 标准族的每个标准文件本身没有对任何人施加遵从的义务。但是，这种义务可以通过，例如，法律或合同被施加。为了能够声明符合一个标准文件，用户需要能够识别要满足的要求。用户还需要能够将这些要求与其他可选的建议进行区分。

下表阐明 ISMS 标准族文件如何在措辞上区分要求和建议。

该表是基于《ISO/IEC 导则　第 2 部分：国际标准结构和起草规则》(2011 版)的附录 H。

表明	解释
要求	助动词“应”和“不应”表明要严格遵循的要求，以符合标准文件，且不允许偏离
建议	助动词“宜”和“不宜”表明在许多可能性中建议一个特别适合的，但不提及或不排除其他的，也就是说，某种做法是优选的但不是必需的，或者反过来讲，某种做法是不提倡的但不是禁止的
允许	助动词“可”和“不必”表明在标准文件的限制范围内某做法是许可的
可能	助动词“能”和“不能”表明某事发生的可能

附 录 B
（资料性附录）
术语和术语归属

B.1 术语归属

ISMS 标准族的术语归属者是指最初定义该术语的标准。术语归属者还要负责对定义进行维护，即提供、评审、更新和删除。

注 1：ISO/IEC 27000 本身不定义任何术语。

注 2：ISO/IEC 27001 和 ISO/IEC 27006 作为规范性标准(即包含要求)总是始终作为各自术语的归属者。

B.2 ISMS 标准族中使用的术语

B.2.1 ISO/IEC 27001

审核 audit	2.5	测量 measurement	2.48
可用性 availability	2.9	监视 monitoring	2.52
能力 competence	2.11	不符合 nonconformity	2.53
保密性 confidentiality	2.12	目标 objective	2.56
符合性 conformity	2.13	组织 organization	2.57
持续改进 continual improvement	2.15	外包(动词) outsource (verb)	2.58
控制 control	2.16	性能 performance	2.59
纠正 correction	2.18	策略 policy	2.60
整改措施 corrective action	2.19	过程 process	2.61
文档化信息 documented information	2.23	要求 requirement	2.63
有效性 effectiveness	2.24	评审 review	2.65
信息安全 information security	2.33	风险 risk	2.68
完整性 integrity	2.40	风险责任者 risk owner	2.78
受益相关方 interested party	2.41	最高管理者 top management	2.84
管理体系 management system	2.46		

B.2.2 ISO/IEC 27002

访问控制 access control	2.1	信息安全事态 information security event	2.35
攻击 attack	2.3	信息安全事件 information security incident	2.36
鉴别 authentication	2.7	信息安全事件管理 information security incident management	2.37
真实性 authenticity	2.8	信息系统 information system	2.39
控制目标 control objective	2.17	抗抵赖 non-repudiation	2.54
信息处理设施 information processing facilities	2.32	可靠性 reliability	2.62

信息安全持续性　information security continuity　2.34

B.2.3　ISO/IEC 27003

ISMS 项目　ISMS project　2.43

B.2.4　ISO/IEC 27004

分析模型　analytical model　2.2
属性　attribute　2.4
基本测度　base measure　2.10
数据　data　2.20
决策准则　decision criteria　2.21
导出测度　derived measure　2.22
指标　indicator　2.30
信息需求　information need　2.31
测度　measure　2.47
测量函数　measurement function　2.49
测量方法　measurement method　2.50
测量结果　measurement results　2.51
对象　object　2.55
尺度　scale　2.80
测量单位　unit of measurement　2.86
确认　validation　2.87
验证　verification　2.88

B.2.5　ISO/IEC 27005

后果　consequence　2.14
事态　event　2.25
外部语境　external context　2.27
内部语境　internal context　2.42
风险程度　level of risk　2.44
可能性　likelihood　2.45
残余风险　residual risk　2.64
风险接受　risk acceptance　2.69
风险分析　risk analysis　2.70
风险评估　risk assessment　2.71
风险沟通与咨询　risk communication and consultation　2.72
风险准则　risk criteria　2.73
风险评价　risk evaluation　2.74
风险识别　risk identification　2.75
风险管理　risk management　2.76
风险管理过程　risk management process　2.77
风险处置　risk treatment　2.79
威胁　threat　2.83
脆弱性　vulnerability　2.89

B.2.6　ISO/IEC 27006

认证文件标志　certification documents mark

B.2.7　ISO/IEC 27007

审核范围　audit scope　2.6

B.2.8　ISO/IEC TR 27008

评审对象　review object　2.66
评审目标　review objective　2.67
安全实现标准　security implementation standard　2.81

B.2.9 ISO/IEC 27010

信息共享社区 information sharing community 2.38

可信信息通信实体 trusted information communication entity 2.85

B.2.10 ISO/IEC 27011

搭配 collocation
通信中心 communication centre
基本通信 essential communications
通信保密 non-disclosure of communications
个人信息 personal information
优先呼叫 priority call
电信应用 telecommunications applications
电信业务 telecommunications business
电信设备间 telecommunications equipment room
电信设施 telecommunications facilities
电信组织 telecommunications organizations
电信记录 telecommunication records
电信服务 telecommunications services
电信客户 telecommunications service customer
电信用户 telecommunications service user
终端设施 terminal facilities
用户 user

B.2.11 ISO/IEC 27014

执行管理者 executive management 2.26

信息安全治理 governance of information security 2.28

治理者 governing body 2.29

利益相关方 stakeholder 2.82

B.2.12 ISO/IEC TR 27015

金融服务 financial services

B.2.13 ISO/IEC TR 27016

年预期损失 annualized loss expectancy,ALE
直接价值 direct value
经济比较 economic comparison
经济因素 economic factor
经济合理性 economic justification
经济增加值 economic value added
经济学 economics
预期值 expected value
扩充值 extended value
间接价值 indirect value
信息安全经济学 information security economics
信息安全管理 information security management, ISM
损失 loss
市场价值 market value
净现值 net present value
非经济效益 non economic benefit
现值 present value
机会成本 opportunity cost
机会价值 opportunity value
法规要求 regulatory requirements
投资回报 return on investment
社会价值 societal value
价值 value
风险值 value-at-risk

B.2.14 ISO/IEC TR 27017

能力 capability
数据受侵 data breach
安全的多租户 secure multi-tenancy
虚拟机 virtual machine

B.2.15 ISO/IEC TR 27018

数据受侵 data breach
可识别个人信息 personally identifiable information,PII
PII 控制者 PII controller
PPI 主体 PII principal
PII 处理者 PII processor
PII 处理 processing of PII
共有云提供者 public cloud service provider

B.2.16 ISO/IEC TR 27019

停电 blackout
计算机安全应急响应组 Computer Emergency Response Team,CERT
关键基础设施 critical infrastructure
调试 debugging
分布 distribution
能源设备装置 energy equipment installation
能源供给 energy supply
能源供应者 energy utility
人机接口 human-machine interface,HMI
维护 maintenance
可编程逻辑控制器 PLC
过程控制系统 process control system
安全性 safety
安全系统 safety systems
智能电网 smart grid
适用性声明 statement of applicability,SOA
传输系统 transmission system

参 考 文 献

[1] ISO/IEC 17021 合格评定 管理体系审核认证机构的要求(Conformity assessment—Requirements for bodies providing audit and certification of management systems)(GB/T 27021—2007,IDT)

[2] ISO 9000:2015 Quality management systems—Fundamentals and vocabulary

[3] ISO 19011:2011 管理体系审核指南(Guidelines for auditing management systems)(GB/T 19011—2013,IDT)

[4] ISO/IEC 27001 信息技术 安全技术 信息安全管理体系 要求(Information technology—Security techniques—Information security management systems—Requirements)(GB/T 22080—2016,IDT)

[5] ISO/IEC 27002 信息技术 安全技术 信息安全控制实践指南(Information technology—Security techniques—Code of practice for information security controls)(GB/T 22081—2016,IDT)

[6] ISO/IEC 27003 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 security management system implementation guidance)(GB/T 31496—2015,IDT)

[7] ISO/IEC 27004 信息技术 安全技术 信息安全管理 测量(Information technology—Security techniques—Information security management—Measurement)(GB/T 31497—2015,IDT)

[8] ISO/IEC 27005 信息技术 安全技术 信息安全风险管理(Information technology—Security techniques—Information security risk management)(GB/T 31722—2015,IDT)

[9] ISO/IEC 27006 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(Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems)(GB/T 25067—2016,IDT)

[10] ISO/IEC 27007 Information technology—Security techniques—Guidelines for information security management systems auditing

[11] ISO/IEC TR 27008 信息技术 安全技术 信息安全控制措施审核员指南(Information technology—Security techniques—Guidelines for auditors on information security controls)(GB/Z 32916—2016,IDT)

[12] ISO/IEC 27009 Information technology—Security techniques—Sector-specific application of ISO/IEC 27001—Requirements

[13] ISO/IEC 27010 信息技术 安全技术 行业间和组织间通信的信息安全管理(Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications)(GB/T 32920—2016,IDT)

[14] ISO/IEC 27011 Information technology—Security techniques—Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

[15] ISO/IEC 27013 Information technology—Security techniques—Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[16] ISO/IEC 27014 信息技术 安全技术 信息安全治理(Information technology—Security techniques—Governance of information security)(GB/T 32923—2016,IDT)

[17] ISO/IEC TR 27015 Information technology—Security techniques—Information security management guidelines for financial services

[18] ISO/IEC TR 27016 Information technology—Security techniques—Information security management—Organizational economics

[19] ISO/IEC 27017 Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[20] ISO/IEC 27018 Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[21] ISO/IEC 27019 Information technology—Security techniques—Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

[22] ISO 27799 Health informatics—Information security management in health using ISO/IEC 27002

[23] ISO Guide 73:2009 Risk management—Vocabulary

[24] ISO/IEC 15939:2007 Systems and software engineering—Measurement process

[25] ISO/IEC 20000-1:2011 Information technology—Service management—Part 1:Service management system requirements

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　概述和词汇
GB/T 29246—2017/ISO/IEC 27000:2016
*
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.spc.org.cn
服务热线:400-168-0010
2017年12月第一版
*
书号:155066·1-59262

GB/T 29246-2017