ICS 35.030
CCS L80

# 中华人民共和国国家标准

GB/T 29246—XXXX/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）

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上。

（征求意见稿）

2022-07-01

XXXX－XX－XX 发布　　XXXX－XX－XX 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) 增加了“规范性引用文件”一章（见第2章）；
b) 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）；
c) 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）；
d) 在图1中增加了ISO/IEC 27021（见图1），删除了ISO/IEC 27015（见2017年版的图1）；
e) 增加了对ISO/IEC 27009（GB/T 38631）的描述（见5.3.3）；
f) 增加了对ISO/IEC 27021的描述（见5.4.10）；
g) 删除了对ISO/IEC 27015（已废止）的描述（见2017年版的4.5.3）；
h) 更新了信息安全管理体系标准族中一些标准的描述（见第5章，2017年版的第4章）；
i) 删除了2017年版的附录A和附录B。

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　概述和术语》。

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网络安全检测评估中心、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、公安第三研究所、深圳大学中国质量经济发展研究院、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。

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]

## 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标准族定义需使用的新术语。

## 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 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 19011:2011，3.14，有修改：删除注]

1 目前本文件名称中的“vocabulary”按照以往转标国家标准的通常译法译为“词汇”，但在 GB/T 1.1—2020 的表 1（文件名称中表示标准功能类型的词语及其英文译名）中建议将“术语”译为“vocabulary”，那么本文件名称中的“词汇”是否需要改为“术语”，值得商榷。

3.5

**鉴别 authentication**

为一个实体所声称特征的正确性而提供的确保措施。

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 base measure**

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 continual improvement**

为提高性能（3.52）而反复进行的活动。

3.14

**控制措施 control**

改变风险（3.61）的措施。

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

注 2：控制措施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 control objective**

描述控制措施（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（3.47）的措施。

3.17

**整改措施 corrective action**

消除不符合（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**

特定情况的发生或改变。

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 Guide 73:2009，3.5.1.3，有修改：删除注 4]

3.22

**外部语境 external context**

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内容：

——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。

[来源：ISO Guide 73:2009，3.3.1.1]

3.23

**信息安全治理 governance of information security**

指导和控制组织（3.50）信息安全（3.28）活动的体系。

3.24

**治理者 governing body**

对组织（3.50）的性能（3.52）和合规负有责任的个人或集体。

注：在某些司法管辖区，治理者可能是董事会。

3.25

**指标 indicator**

提供估算或评价的测度（3.42）。

3.26

**信息需要 information need**

对目标（3.49）、目的、风险和问题进行管理所需的了解。

[来源：ISO/IEC/IEEE 15939:2017，3.12]

3.27

**信息处理设施 information processing facilities**

任何信息处理系统、服务或基础设施，或者其安置的物理位置。

3.28

**信息安全 information security**

对信息的保密性（3.10）、完整性（3.36）和可用性（3.7）的保全。

注：另外，还可能包括其他特性，诸如真实性（3.6）、可问责性、抗抵赖性（3.48）和可靠性（3.55）。

3.29

**信息安全持续性 information security continuity**

保障信息安全（3.28）持续运行的过程（3.54）和规程。

3.30

**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（3.28）策略（3.53）或控制措施（3.14）失效，或者可能与信息安全相关的先前未知情况。

3.31

**信息安全事件 information security incident**

单个或一系列不希望或意外的、极有可能危及业务运营并威胁信息安全（3.28）的信息安全事态（3.30）。

3.32

**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（3.31）的一组过程（3.54）。

3.33

**信息安全管理体系（ISMS）专业人员** information security management system (ISMS) professional

建立、实施、维护和持续改进一个或多个信息安全管理体系过程（3.54）的人员。

3.34

**信息共享社区** information sharing community

同意共享信息的组织（3.50）群体。

注：组织（3.50）可能是个人。

3.35

**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的组合。

3.36

**完整性** integrity

准确和完备的性质。

3.37

**利益相关方** interested party; stakeholder

可能对一项决策或活动产生影响，或被其影响，或认为自己受到其影响的个人或组织（3.50）。

3.38

**内部语境** internal context

组织（3.50）寻求实现其目标的内部环境。

注：内部语境可能包括如下方面：

——治理、组织结构、角色和职责；

——策略（3.53）、目标（3.49）及其实现战略；

——在资源和知识（如资本、时间、人员、过程（3.54）、系统和技术）方面的能力；

——信息系统（3.35）、信息流和决策过程（3.54）（正式的和非正式的）；

——与内部利益相关方（3.37）的关系及其认知和价值观；

——组织（3.50）的文化；

——组织采用的标准、指南和模型；

——合同关系的形式和范围。

[来源：ISO Guide 73:2009，3.3.1.2]

3.39

**风险级别** level of risk

以后果（3.12）和其可能性（3.40）的组合来表示的风险（3.61）大小。

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

3.40

**可能性** likelihood

某事发生的机会。

[来源：ISO Guide 73:2009，3.6.1.1，有修改：删除注1和注2]

3.41

**管理体系 management system**

组织（3.50）中相互关联或相互作用，用来建立策略（3.53）和目标（3.49）以及实现这些目标过程（3.54）的元素集合。

注 1：管理体系可能专注于单一学科或多个学科。

注 2：体系元素包括组织的结构、角色和责任、规划和运行。

注 3：管理体系范围可能包括组织（3.50）的整体、组织的具体且确定的功能或部门，或者跨组织群的一项或多项功能。

3.42

**测度 measure**

作为测量（3.43）结果赋值的变量。

[来源：ISO/IEC/IEEE 15939:2017，3.15，有修改：删除注]

3.43

**测量 measurement**

确定一个值的过程（3.54）。

3.44

**测量函数 measurement function**

组合两个或两个以上基本测度（3.8）的算法或计算。

[来源：ISO/IEC/IEEE 15939:2017，3.20]

3.45

**测量方法 measurement method**

用于按规定的尺度量化属性的，一般描述的操作规程。

注：测量方法的类型取决于属性量化操作的性质。能区分为以下两种类型：

——主观的：涉及人为判断的量化；

——客观的：基于数字规则的量化。

[来源：ISO/IEC/IEEE 15939:2017，3.21，有修改：删除注 2]

3.46

**监视 monitoring**

确定系统、过程（3.54）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。

3.47

**不符合 nonconformity**

对要求（3.56）的不满足。

3.48

**抗抵赖性 non-repudiation**

证明所声称事态（3.21）或行动的发生及其起源实体的能力。

3.49

**目标 objective**

要实现的结果。

注 1：目标可能是战略性的、战术性的或操作性的。

注 2：目标可能涉及不同学科（诸如金融、健康与安全以及环境目标），可能适用于不同层次（诸如战略、组织、项目、产品和过程（3.54））。

注 3：目标可能以其他方式表示，例如，作为预期结果、意图、操作准则，作为信息安全（3.28）目标，或者使用具有类似含义的其他词语（例如，目的或靶标）。

注 4：在信息安全（3.28）管理体系（3.41）的语境下，组织（3.50）制定与信息安全策略（3.53）一致的信息安全目标，以实现特定结果。

3.50

**组织 organization**

具有自身的职责、权威和关系以实现其目标（3.49）的个人或集体。

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，或者其部分或其组合，无论注册与否，是公共的还是私营的。

3.51

**外包 outsource**

做出由外部组织（3.50）执行组织的部分功能或过程（3.54）的安排。

注：外部组织（3.50）不在管理体系（3.41）的范围，尽管外包的功能或过程（3.54）在范围之内。

3.52

**性能 performance**

一种可测量的属性。

注 1：性能可能与定量或定性的调查发现相关。

注 2：性能可能与活动、过程（3.54）、产品（包括服务）、系统或组织（3.50）的管理相关。

3.53

**策略 policy**

由其最高管理层（3.75）正式表达的组织（3.50）的意图和方向。

注：总策略一般称为方针，包括总策略的策略集可称为方针策略。

3.54

**过程 process**

将输入转化为输出的相互关联或相关作用的活动集合。

3.55

**可靠性 reliability**

与预期行为和结果一致的性质。

3.56

**要求 requirement**

明示的、通常隐含的或强制性的需要或期望。

注 1：“通常隐含的”意指所考虑的需要或期望是不言而喻的，对于组织（3.50）或利益相关方（3.37）是惯例或常见做法。

注 2：规定的要求是明示的，例如在文档化信息（3.19）中明示。

3.57

**残余风险 residual risk**

风险处置（3.72）后余下的风险（3.61）。

注 1：残余风险可能包含未识别的风险（3.61）。

注 2：残余风险也可称为“保留风险”。

3.58

**评审 review**

为确定主题事项的适宜性、充分性和有效性（3.20）以实现既定目标而采取的活动。

[来源：ISO Guide 73:2009，3.8.2.2，有修改：删除注]

3.59

**评审对象 review object**

被评审的特定事项。

3.60

**评审目标 review objective**

描述所要达到的评审（3.58）结果的声明。

3.61

**风险 risk**

对目标（3.49）的不确定性影响。

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（3.21）及其后果（3.12）或可能性（3.40）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”（3.21）和“后果”（3.12），或者它们的组合。

注 4：风险常被表示为事态（3.21）（包括境况改变）的后果（3.12）和其发生“可能性”（3.40）的组合。

注 5：在信息安全（3.28）管理体系（3.41）的语境下，信息安全风险能被表示为对信息安全目标（3.49）的不确定性影响。

注 6：信息安全（3.28）风险与威胁（3.74）利用信息资产或信息资产组的脆弱性（3.77）对组织（3.50）造成伤害的潜力相关。

3.62

**风险接受 risk acceptance**

承担特定风险（3.61）的知情决定。

注 1：风险接受可能是在不经风险处置（3.72）或风险处置过程（3.54）中做出。

注 2：接受的风险（3.61）处于监视（3.46）和评审（3.58）中。

[来源：ISO Guide 73:2009，3.7.1.6]

3.63

**风险分析 risk analysis**

理解风险（3.61）本质和确定风险级别（3.39）的过程（3.54）。

注 1：风险分析为风险评价（3.67）和风险处置（3.72）决策提供基础。

注 2：风险分析包括风险估算。

[来源：ISO Guide 73:2009，3.6.1]

3.64

**风险评估** risk assessment

风险识别（3.68）、风险分析（3.63）和风险评价（3.67）的全过程（3.54）。

[来源：ISO Guide 73:2009，3.4.1]

3.65

**风险沟通与咨询** risk communication and consultation

组织（3.50）就风险（3.61）管理所进行的，提供、共享或获取信息以及与利益相关方（3.37）对话的持续和迭代过程（3.54）。

注1：这些信息可能涉及风险（3.61）的存在、性质、形式、可能性（3.40）、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（3.50）和其利益相关方（3.37）之间进行知情沟通的双向过程（3.54）。咨询是指：

——通过影响力而不是权力来影响决策的过程（3.54）；

——决策的输入，而非联合做出决策。

3.66

**风险准则** risk criteria

评价风险（3.61）重要性的基准。

注1：风险准则是基于组织的目标以及外部语境（3.22）和内部语境（3.38）。

注2：风险准则能根据标准、法律、策略（3.53）和其他要求（3.56）得出。

[来源：ISO Guide 73:2009，3.3.1.3]

3.67

**风险评价** risk evaluation

将风险分析（3.63）的结果与风险准则（3.66）比较，以确定风险（3.61）和/或其大小是否可接受或可容忍的过程（3.54）。

注：风险评价有助于风险处置（3.72）的决策。

[来源：ISO Guide 73:2009，3.7.1]

3.68

**风险识别** risk identification

发现、识别和描述风险（3.61）的过程（3.54）。

注1：风险识别涉及风险源、事态（3.21）及其原因和潜在后果（3.12）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（3.37）的需要。

[来源：ISO Guide 73:2009，3.5.1]

3.69

**风险管理** risk management

指导和控制组织（3.50）相关风险（3.61）的协调活动。

[来源：ISO Guide 73:2009，2.1]

3.70

**风险管理过程** risk management process

管理策略（3.53）、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（3.61）活动上的系统性应用。

注：GB/T 31722 使用术语“过程”（3.54）来描述全面风险管理。风险管理（3.69）过程中的元素称为“活动”。

[来源：ISO Guide 73:2009，3.1，有修改：增加注]

3.71

**风险责任者 risk owner**

具有责任和权力来管理风险（3.61）的个人或实体。

[来源：ISO Guide 73:2009，3.5.1.5]

3.72

**风险处置 risk treatment**

改变风险（3.61）的过程（3.54）。

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引发风险（3.61）的活动来规避风险；

——承担或增加风险（3.61）以追求机会；

——消除风险源；

——改变可能性（3.40）；

——改变后果（3.12）；

——与另外一方或多方共担风险（包括合同和风险融资）；

——有根据地选择保留风险。

注2：处理负面后果（3.12）的风险处置有时称为“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（3.61）或改变现有风险。

[来源：ISO Guide 73:2009，3.8.1，有修改：将注1中的“决定”替换为“选择”]

3.73

**安全实施标准 security implementation standard**

规定授权的安全实现方式的文件。

3.74

**威胁 threat**

可能对系统或组织（3.50）造成伤害的不希望事件的潜在因素。

3.75

**最高管理层 top management**

在最高级别上指导和控制组织（3.50）的个人或集体。

注1：最高管理层有权在组织（3.50）内授权和提供资源。

注2：如果管理体系（3.41）的范围仅涵盖组织（3.50）的一部分，则最高管理层就是指指导和控制组织这一部分的个人或集体。

注3：最高管理层有时称为执行管理层，可能包括首席执行官、首席财务官、首席信息官和类似角色。

3.76

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

支持信息共享社区（3.34）内信息交换的自主组织（3.50）。

3.77

**脆弱性 vulnerability**

能被一个或多个威胁（3.74）利用的资产或控制措施（3.14）的弱点。

# 4 信息安全管理体系（ISMS）

## 4.1 概要

各种类型和规模组织的主要任务：

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、网络和人员是实现组织目标的重要资产；

c) 面临一系列可能影响资产运作的风险；

d) 通过实施信息安全控制措施解决其感知的风险暴露。

组织持有和处理的所有信息在其使用中都会受到攻击、错误、自然灾害（例如，洪水或火灾）等威胁，并存在固有的脆弱性。术语“信息安全”通常基于将信息视为一种资产，其价值需要适当保护，例如，防止丧失保密性、完整性和可用性。使已授权的需要者能及时获得准确、完整的信息，有助于促进提升业务效率。

通过有效地阐明、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法律合规性和形象至关重要。这些指导实施适当控制措施和处置不可接受的信息安全风险的协调活动通常被称为信息安全管理的元素。

由于信息安全风险和控制措施的有效性随着环境的变化而变化，组织需要：

e) 监视和评价已实施的控制措施和规程的有效性；

f) 识别待处置的新风险；

g) 根据需要选择、实施和改进适当的控制措施。

为了相互关联和协调此类信息安全活动，每个组织都需要制定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。

## 4.2 ISMS 的概念

### 4.2.1 概述和原则

信息安全管理体系（ISMS）由策略、规程、指南以及相关资源和活动组成，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的。分析信息资产保护的需求，并根据需要应用适当的控制措施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) 认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措施，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元素；

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酌情进行修改。

### 4.2.2 信息

信息是一种资产，与其他重要的业务资产一样，对组织的业务至关重要，因此需要得到适当的保护。信息可以以多种形式存储，包括：数字形式（如存储在电子或光媒体上的数据文件）、物质形式（如纸

质），以及以员工知识形式表示的未呈现信息。信息可能通过各种方式进行传输，包括：快递、电子或口头通信。无论信息采用何种形式，或以何种形式传输，它总是需要适当的保护。

在许多组织中，信息依赖于信息通信技术。这项技术通常是组织的一个基本元素，有助于促进信息的创建、处理、存储、传输、保护和销毁。

### 4.2.3 信息安全

信息安全确保信息的保密性、可用性和完整性。信息安全涉及应用和管理适当的控制措施，包括考虑到各种威胁，以确保业务的持续成功和持续性，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措施来实现的，这套控制措施通过选定的风险管理过程进行选择，并使用ISMS进行管理，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。必要时，需要规定、实施、监视、评审和改进这些控制措施，以确保满足组织的特定信息安全和业务目标。相关的信息安全控制措施也是期望与组织业务过程无缝集成。

### 4.2.4 管理

管理涉及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。管理结构从小型组织中的一个人扩展到大型组织中由许多人组成的管理层级。

就ISMS而言，管理涉及到通过保护组织的信息资产来实现业务目标所需的监督和决策。信息安全管理通过制定和使用信息安全策略、规程和指南来表达，然后由与组织相关的所有个人在整个组织中应用这些策略、规程和指南。

### 4.2.5 管理体系

管理体系使用资源框架来实现组织的目标。管理体系包括组织架构、策略、规划活动、责任、实践、规程、过程和资源。

在信息安全方面，管理体系使组织能够：

a) 满足客户和其他利益相关方的信息安全需求；
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。

## 4.3 过程方法

组织需要识别和管理许多活动，以便既有效果又有效率地运作。需要管理任何使用资源的活动，以便能够使用一组相互关联或相互作用的活动将输入转换为输出，这也称为过程。一个过程的输出可直接形成另一个过程的输入，通常这种转换是在计划和受控的条件下进行的。组织内过程系统的应用，以及这些过程的识别、交互及其管理，可称为“过程方法”。

## 4.4 ISMS的重要性

需要解决与组织信息资产相关的风险。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的物理、人为和技术威胁带来的风险。

采用ISMS是期望其成为组织的一项战略决策，并且该决策有必要根据组织的需要进行无缝集成、扩展和更新。

组织ISMS的设计和实施受组织的需要和目标、安全需求、采用的业务过程以及组织的规模和结构的影响。ISMS的设计和运行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）的利益和信息安全需求。

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。恶意代码、计算机黑客和拒绝服务攻击对信息系统和网络造成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很重要。在任何行业中，ISMS都使电子商务成为可能，对风险管理活动至关重要。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。此外，包含信息资产的移动存储设备的分布可能削弱传统控制措施的有效性。当组织采用了ISMS标准族，便可向业务伙伴和其他受益相关方证明其运用一致且互认的信息安全原则的能力。

在信息系统的设计和开发中，信息安全并不总是被考虑到的。而且，信息安全常被认为是技术解决方案。然而，能通过技术手段实现的信息安全是有限的，若没有ISMS的适当管理和规程支持，信息安全可能是无效的。将安全性集成到功能完备的信息系统中可能是困难和昂贵的。ISMS涉及确认哪些控制措施到位，需要仔细规划并注意细节。例如，可能是技术（逻辑）、物理、行政（管理）或组合的访问控制提供了一种手段，以确保根据业务和信息安全需求授权和限制对信息资产的访问。

ISMS的成功采用对于保护信息资产非常重要，它使组织能够：

a) 更好地确保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措施，并测量和改进其有效性；
c) 持续改进其控制环境；
d) 有效地遵从法律法规。

### 4.5 建立、监视、保持和改进 ISMS

#### 4.5.1 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需求（见4.5.2）；
b) 评估信息安全风险（见4.5.3）和处置信息安全风险（见4.5.4）；
c) 选择并实施相关控制措施，以管理不可接受的风险（见4.5.5）；
d) 监视、保持和改进组织信息资产相关控制措施的有效性（见4.5.6）。

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）至 d），以识别风险或组织战略或业务目标的变化。

#### 4.5.2 识别信息安全需求

在组织的总体战略和业务目标、规模和地理分布的范围内，可通过了解如下方面来识别信息安全需求：

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要；
c) 法律法规、规章制度和合同要求。

对与组织信息资产相关的风险进行有条不紊的评估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。期望相关控制措施的支出与感知到的风险成为现实所造成的业务影响相称。

### 4.5.3 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，该方法可包括对成本和收益、法律要求、利益相关方的关切以及其他适合的输入和变量的判断。

风险评估宜根据风险接受准则和与组织相关的目标来识别、量化并按重要性排列风险。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，并实施为防范这些风险而选择的控制措施。

风险评估宜包括：

——系统性估算风险大小的方法（风险分析）；

——将估算的风险与风险准则比较，以确定风险重要性的过程（风险评价）。

宜定期进行风险评估，以应对信息安全需求和风险状况的变化，例如，资产、威胁、脆弱性、影响、风险评价以及发生重大变化时的变化。这些风险评估宜以能够产生可比较和可重现结果的有条不紊的方法进行。

信息安全风险评估宜具有明确界定的范围以保障其有效性，还宜包括与其他区域风险评估的关系（如果适用）。

ISO/IEC 27005（GB/T 31722）提供信息安全风险管理指南，包括关于风险评估、风险处置、风险接受、风险报告、风险监视和风险评审的建议。风险评估方法的例子也包括在内。

### 4.5.4 处置信息安全风险

在考虑风险处置之前，组织宜确定风险是否可接受的准则。例如，如果评估风险较低或处置成本对组织不具有成本效益，则可接受风险。此类决定宜予以记录。

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策。风险处置的可能选项包括：

a) 采用适当的控制措施来降低风险；

b) 明知而客观地接受风险，前提是这些风险明确地满足组织的风险接受策略和准则；

c) 通过不允许可能导致风险发生的行为来规避风险；

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措施来处置的风险，宜选择和实施这些控制措施。

### 4.5.5 选择和实施控制措施

一旦识别了信息安全需求（见4.5.2），确定和评估了所识别信息资产的信息安全风险（见4.5.3），并做出了处置信息安全风险的决定，则选择和实施风险降低的控制措施。

控制措施宜确保将风险降低至可接受的程度,同时考虑到以下因素：

a) 国家和国际法律法规的要求和约束；

b) 组织目标；

c) 运行要求和约束；

d) 风险降低相关的实施和运行成本，并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措施的效果和效率以支持组织目的的目标。控制措施的选择和实施宜记录在适用性声明中，以协助合规要求；

f) 控制措施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（GB/T 22081）中规范的控制措施是公认的适用于大多数组织的最佳实践，并易于调整以适应各种规模和复杂性的组织。ISMS标准族中的其他标准为选择和应用ISMS的ISO/IEC 27002（GB/T 22081）控制措施提供了指导。

宜在系统和项目需求规范和设计阶段考虑信息安全控制措施。如果不这样做，可能会导致额外的成本和低效的解决方案，并且在最坏的情况下，无法实现足够的安全性。控制措施可从ISO/IEC 27002（GB/T

22081）或其他控制措施集中选择。或者，可设计新的控制措施，以满足组织的特定需要。有必要认识到，某些控制措施可能不适用于每个信息系统或环境，也不适用于所有组织。

有时，实施所选择的一组控制措施需要时间，在此期间，风险程度可能高于长期所能容忍的程度。风险准则宜涵盖控制措施实施期间短期风险的可承受性。随着控制措施的逐步实施，宜将在不同时间点估算或预计的风险程度告知利益相关方。

宜记住，没有一套控制措施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措施的效果和效率，以支持组织目的。

控制措施的选择和实施宜记录在适用性声明中，以协助合规要求。

### 4.5.6 监视、保持和改进 ISMS 有效性

组织需要根据其策略和目标监视和评估ISMS的执行情况，并将结果报告给管理层审查，从而保持和改进ISMS。这种ISMS审查检查ISMS是否包括适用于处置ISMS范围内风险的特定控制措施。此外，根据所监视区域的记录，提供对纠正、预防和改进措施进行验证和追溯的证据。

### 4.5.7 持续改进

ISMS持续改进的目的是提高实现信息保密性、可用性和完整性目标的可能性。持续改进的重点是寻找改进的机会，而不是假设现有的管理活动已经足够好或已尽其可能。

改进措施包括：

a) 分析和评价现状，以识别改进的地方；
b) 制定改进的目标；
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选择；
e) 实施选定的解决方案；
f) 测量、验证、分析和评价实施结果，以确定目标已实现；
g) 正式确认改进。

必要时，对结果进行评审，以确定进一步的改进机会。因此，改进是一个持续活动，即经常重复行动。客户和其他利益相关方的反馈、信息安全管理体系的审核和评审也可用于识别改进机会。

## 4.6 ISMS 关键成功因素

许多因素对于ISMS的成功实施至关重要，以使组织能够实现其业务目标。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) 设计、实施、监视、保持和改进符合组织文化的信息安全的方法与框架；
c) 各级管理层，特别是最高管理层的明显支持和承诺；
d) 对应用信息安全风险管理（见ISO/IEC 27005（GB/T 31722））实现的信息资产保护要求的理解；
e) 有效的信息安全意识、培训和教育计划，告知所有员工和其他相关方信息安全策略、标准等中规定的信息安全义务，并激励他们采取相应的行动；
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) 用于评价信息安全管理绩效和反馈改进建议的度量系统。

ISMS提高了组织持续实现其信息资产所需关键成功因素的可能性。

### 4.7 ISMS 标准族的益处

实施ISMS的益处主要来自降低信息安全风险（即降低信息安全事件发生的可能性和/或造成的影响）。具体而言，通过采用ISMS标准族，组织实现可持续成功的益处包括：

a) 以结构化框架支持规范、实施、运行和保持一个综合全面、成本有效、创造价值、一体化和一致的ISMS，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，协助管理层以负责任的方式持续管理和运用其信息安全管理方法，包括就信息安全的整体管理对业务和系统所有者进行教育和培训；
c) 以非指定的方式促进全球公认的良好信息安全实践，使组织有自由采纳和改进适合其具体环境的相关控制措施，并在面对内部和外部变化时保持这些控制措施；
d) 提供信息安全的共同语言和概念基础，使其更容易信任具有符合ISMS的业务伙伴，特别是如果他们需要由一个被认可的认证机构根据ISO/IEC 27001（GB/T 22080）进行认证；
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) 对信息安全投资进行更有效的经济管理。

## 5 信息安全管理体系标准族

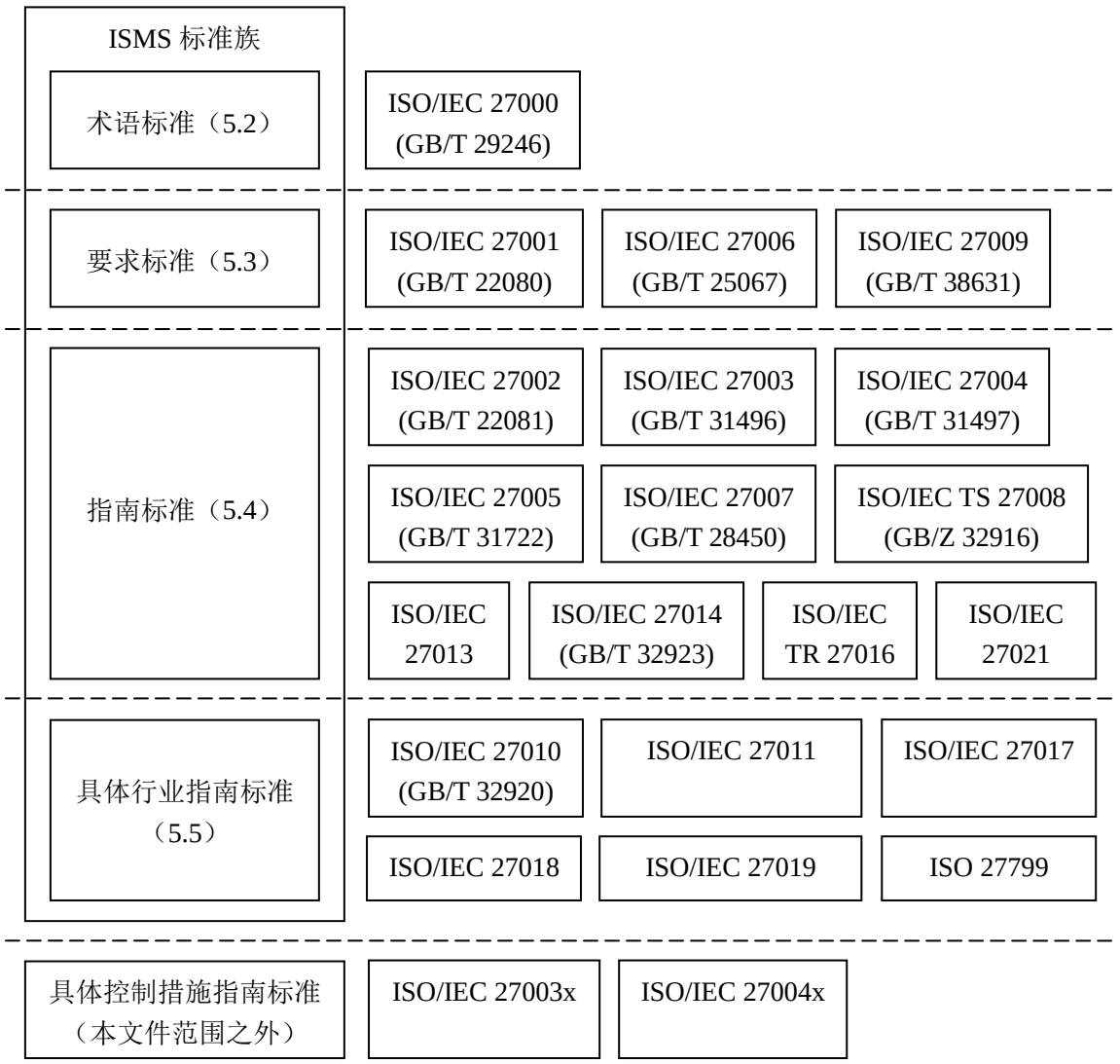
### 5.1 一般信息

信息安全管理体系（ISMS）标准族由已发布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。这些组件的重点是规定如下要求的标准：

——ISMS的要求（ISO/IEC 27001（GB/T 22080））；
——对进行ISO/IEC 27001（GB/T 22080）符合性认证的认证机构的要求（ISO/IEC 27006（GB/T 25067））；
——对具体行业ISMS实施的附加要求框架（ISO/IEC 27009（GB/T 38631））。

其他文件为ISMS实施的各个方面提供指导，包括通用过程以及具体行业指导。

ISMS标准族中各标准之间的关系如图1所示。




注：对于已转国家标准的国际标准编号，加括号标出对应的国家标准编号，具体发布年号详见参考文献。

**图1 ISMS 标准族关系**

以下对ISMS标准族的每个标准按其在ISMS标准族中的类型（或角色）及其编号进行说明。

### 5.2 概述和术语标准：ISO/IEC 27000（GB/T 29246（本文件））

*信息技术　安全技术　信息安全管理体系　概述和术语(信息安全技术　信息安全管理体系　概述和术语)*

**范围**：该文件为组织和个人提供了：

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**：该文件描述信息安全管理体系的基础，构成ISMS标准族的主题，并定义相关术语。

## 5.3 要求标准

### 5.3.1 ISO/IEC 27001（GB/T 22080）

*信息技术　安全技术　信息安全管理体系　要求*

**范围：**该文件规定了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。它规定了实施信息安全控制措施的要求，这些控制措施是根据单个组织或其组成部分的需要定制的。该文件可供所有类型、规模和性质的组织使用。

**目的：**ISO/IEC 27001（GB/T 22080）为ISMS的开发和运行提供规范性要求，包括一套控制措施，用于控制和降低与组织试图通过运行其ISMS来保护的信息资产相关的风险。组织可对其运行的ISMS的合规性进行审核和认证。作为ISMS过程的一部分，应从ISO/IEC 27001:2013（GB/T 22080—2016）附录A中选择适合的控制目标和控制措施，以涵盖明确的要求。ISO/IEC 27001:2013（GB/T 22080—2016）表A.1中列出的控制目标和控制措施直接源自ISO/IEC 27002:2013（GB/T 22081—2016）第5章至第18章，并与其一致。

### 5.3.2 ISO/IEC 27006（GB/T 25067）

*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：**除了ISO/IEC 17021中包含的要求外，该文件还为根据ISO/IEC 27001（GB/T 22080）提供审核和ISMS认证的机构规定了要求，并提供了指南。其主要目的是为根据ISO/IEC 27001（GB/T 22080）提供ISMS认证的认证机构的认可提供支持。

该文件中包含的要求需要由提供ISMS认证的任何机构在胜任力和可靠性方面进行证明，该文件中包含的指南为提供ISMS认证的任何机构提供这些要求的附加解释。

**目的：**ISO/IEC 27006（GB/T 25067）对ISO/IEC 17021补充认证机构的认可要求，从而允许这些机构按照ISO/IEC 27001（GB/T 22080）中规定的要求提供一致的合规认证。

### 5.3.3 ISO/IEC 27009（GB/T 38631）

*信息技术　安全技术　ISO/IEC 27001具体行业应用　要求（信息技术　安全技术　GB/T 22080具体行业应用　要求）*

**范围：**该文件规定了在任何具体行业（领域、应用领域或市场领域）使用ISO/IEC 27001的要求，并解释如何包括ISO/IEC 27001（GB/T 22080）中的附加要求，如何细化任何ISO/IEC 27001要求，以及如何包括ISO/IEC 27001:2013:2013（GB/T 22080—2016）附录A中的控制措施或控制措施集。

**目的：**ISO/IEC 27009（GB/T 38631）确保附加或改进的要求不与ISO/IEC 27001（GB/T 22080）中的要求冲突。

## 5.4 一般指南标准

### 5.4.1 ISO/IEC 27002（GB/T 22081）

*信息安全、网络空间安全和隐私保护　信息安全控制措施（信息技术　安全技术　信息安全控制实践指南）*

**范围：**该文件提供了一套通用信息安全控制措施的参考集，包括实施指南。

**目的：**该文件旨在供以下组织使用：

a)　在基于ISO/IEC 27001（GB/T 22080）的信息安全管理系统（ISMS）的语境下；

b) 基于国际公认的最佳实践实施信息安全控制措施；
c) 制定特定于组织的信息安全管理指南。

5.4.2 ISO/IEC 27003（GB/T 31496）

*信息技术 安全技术 信息安全管理体系 指南(信息技术 安全技术 信息安全管理体系实施指南)*

**范围：**该文件提供了ISO/IEC 27001:2013（GB/T 22080—2016）的解释和指南。

**目的：**ISO/IEC 27003（GB/T 31496）为根据ISO/IEC 27001（GB/T 22080）成功实施ISMS提供背景。

5.4.3 ISO/IEC 27004（GB/T 31497）

*信息技术 安全技术 信息安全管理 监视、测量、分析和评价(信息技术 安全技术 信息安全管理 测量)*

**范围：**该文件提供了旨在帮助组织评价信息安全性能和ISMS有效性的指南，以满足ISO/IEC 27001:2013（GB/T 22080—2016）中9.1的要求。它解决：

a) 信息安全性能的监视和测量；
b) 信息安全管理体系（ISMS）有效性的监视和测量，包括其过程和控制措施；
c) 监视和测量结果的分析和评价。

**目的：**ISO/IEC 27004（GB/T 3149）提供一个能根据ISO/IEC 27001（GB/T 22080）对ISMS有效性进行测量的框架。

5.4.4 ISO/IEC 27005（GB/T 31722）

*信息技术 安全技术 信息安全风险管理*

**范围：**该文件提供了信息安全风险管理指南。该文件中描述的方法支持ISO/IEC 27001(GB/T 22080)中规范的一般概念。

**目的：**ISO/IEC 27005（GB/T 31722）提供关于实施面向过程的风险管理方法的指南，以帮助圆满实施和满足ISO/IEC 27001（GB/T 22080）的信息安全风险管理要求。

5.4.5 ISO/IEC 27007（GB/T 28450）

*信息安全、网络空间安全和隐私保护 信息安全管理体系审核指南*

**范围：**除了ISO 19011中包含的适用于一般管理体系的指南外，该文件还提供了关于进行ISMS审核的指南，以及关于信息安全管理体系审核员胜任力的指南。

**目的：**ISO/IEC 27007（GB/T 28450）为需要根据ISO/IEC 27001（GB/T 22080）规定的要求对ISMS进行内部或外部审核或管理ISMS审核方案的组织提供指导。

5.4.6 ISO/IEC TS 27008（GB/Z 32916）

*信息技术 安全技术 信息安全控制措施评估指南(信息技术 安全技术 信息安全控制措施审核员指南)*

**范围：**该文件为评审和评估信息安全控制措施的实施和运行提供了指南，包括信息系统控制措施的技术评估，与组织制定的信息安全要求的符合性，包括符合基于组织制定的信息安全要求的评估准则的技术合规性。

**目的：**该文件指导如何评审和评估信息安全控制措施，这些控制措施是通过ISO/IEC 27001（GB/T 22080）规范的信息安全管理体系来管理的

5.4.7 ISO/IEC 27013

*信息安全、网络空间安全和隐私保护　ISO/IEC 27001和ISO/IEC 20000-1综合实施指南*

**范围：**该文件为打算以如下其中一种方式综合实施ISO/IEC 27001和ISO/IEC 20000-1提供了指南：

a) 当ISO/IEC 20000-1已经实施时，实施ISO/IEC 27001，或者相反；

b) 同时实施ISO/IEC 27001和ISO/IEC 20000-1；

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

该文件专门关注综合实施ISO/IEC 27001中规范的信息安全管理体系（ISMS）和ISO/IEC 20000-1中规范的服务管理体系（SMS）。

**目的：**为组织更好地理解ISO/IEC 27001和ISO/IEC 20000-1的特征和异同提供帮助，有助于规划同时符合这两个标准的综合管理体系。

5.4.8 ISO/IEC 27014（GB/T 32923）

*信息安全、网络空间安全和隐私保护　信息安全治理*

**范围：**该文件提供了关于信息安全治理的概念、目标和过程的指南，组织依此能在其内部对信息安全相关的过程进行评价、指导、监督和沟通。

**目的：**信息安全已成为组织的关键问题。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也会直接影响其声誉。因此，作为其治理责任的一部分，越来越多地要求治理层对信息安全进行监督，以确保组织目标的实现。

5.4.9 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：**该文件提供了一种方法学，使组织能够更好地从经济上理解如何更准确地对其所识别的信息资产以及这些信息资产面临的潜在风险和为此采取的信息保护控制措施进行价值评估，并确定用于保护这些信息资产的最佳资源配置水平。

**目的：**该文件是对ISMS标准族的补充，在组织运营所处的更广泛社会环境中，从经济学的角度对组织的信息资产进行保护，并提供如何通过模型和示例应用信息安全组织经济学的指南。

5.4.10 ISO/IEC 27021

*信息技术　安全技术　信息安全管理体系专业人员胜任力要求*

**范围：**该文件规定了领导或参与建立、实施、保持和持续改进一个或多个符合ISO/IEC 27001:2013的信息安全管理体系过程的ISMS专业人员的胜任力要求。

**目的：**该文件旨在供以下人员使用：

a) 希望证明其作为信息安全管理体系（ISMS）专业人员的胜任力，或希望了解并完成该领域工作所需的胜任力，以及希望扩大其知识面的个人。

b) 寻找潜在ISMS专业候选人的组织，以确定ISMS相关职位所需的胜任力；

c) 为需要一个知识体系（BOK）作为考试来源，来开发ISMS专业人员认证的机构；

d) 教育和培训组织，如大学和职业机构，使其教学大纲和课程符合ISMS专业人员的胜任力要求。

## 5.5 具体行业指南标准

### 5.5.1 ISO/IEC 27010（GB/T 32920）

*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：**除了ISMS标准族中给出的指南外，该文件还提供了在信息共享社区中实施信息安全管理的指南。

该文件提供了与发起、实施、保持和改进组织间和行业间通信中的信息安全相关的控制措施和指导。

**目的：**该文件适用于敏感信息的所有形式的交换与共享，不论是公共的还是私人的、国家的还是国际的、同一行业或市场的还是行业间的。特别是，它可适用于与提供、保持和保护组织或国家关键基础设施相关的信息交换与共享。

### 5.5.2 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控制措施实践指南*

**范围：**该文件提供了支持电信组织实施信息安全控制措施的指南。

**目的：**ISO/IEC 27011使电信组织能够满足保密性、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。

### 5.5.3 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措施实践指南*

**范围：**ISO/IEC 27017通过如下指导提供了适用于云服务供给和使用的信息安全控制措施指南：

——ISO/IEC 27002中规范的相关控制措施的附加实施指导；

——具体与云服务相关的附加控制措施及其实施指导。

**目的：**该文件为云服务提供者和云服务客户提供控制措施和实施指导。

### 5.5.4 ISO/IEC 27018

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

**范围：**ISO/IEC 27018根据ISO/IEC 29100中针对公有云计算环境的隐私保护原则，为实施保护个人可识别信息（PII）的措施制定了公认的控制目标、控制措施和指南。

**目的：**该文件适用于作为PII处理者，通过签约的云计算向其他组织提供信息处理服务的组织，包括公共和私人企业、政府机构和非营利组织。该文件中的指南也可能与作为PII控制者的组织相关。但是，PII控制者可能受其他PII保护法律法规、规章制度和义务的约束，不适用于PII处理者，该文件不包括这些内容。

### 5.5.5 ISO/IEC 27019

*信息技术　安全技术　能源公用事业行业信息安全控制措施*

**范围：**该文件提供了基于ISO/IEC 27002:2013，适用于能源公用事业行业使用的过程控制系统的指南，用于控制和监测电力、燃气、石油和热能的生产或发电、传输、储存和分配，以及相关支持过程的控制。尤其包括以下内容：

——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信息系统，如编程和参数化设备；
——数字控制器和自动化组件，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组件；
——过程控制领域中使用的所有其他辅助信息系统支持，例如，用于辅助数据可视化任务用于控制、监视、数据归档、历史日志、报告和文档；
——用于过程控制领域的通信技术，例如，网络、遥测、远程控制应用和远程控制技术；
——高级计量基础设施（AMI）组件，例如，智能电表；
——测量装置，例如，排放值测量装置；
——数字保护和安全系统，例如，继电保护、安全PLC、紧急调节器装置；
——能源管理系统，例如，分布式能源（DER）、私人家庭、住宅建筑或工业客户装置中的充电基础设施；
——智能电网环境的分布式组件，例如，在能源网、私人家庭、住宅建筑或工业客户装置中；
——安装在上述系统上的所有软件、固件和应用程序，例如，DMS（配电管理系统）应用程序或OMS（停电管理系统）；
——容纳上述设备和系统的任何场所；
——上述系统的远程维护系统。

该文件不适用于核设施的过程控制领域。IEC 62645涵盖了该领域。

该文件还包括使ISO/IEC 27001:2013中所述的风险评估和处置过程适应该文件中提供的能源公用事业行业特定指南的要求。

**目的：**除了ISO/IEC 27002中给出的安全目标和措施外，该文件还为能源公用事业和能源提供者使用的系统提供了关于信息安全控制措施的指南，进一步满足特殊要求。

### 5.5.6 ISO 27799

*健康信息学　使用ISO/IEC 27002的健康信息安全管理*

**范围：**该文件给出了组织信息安全标准和信息安全管理实践的指南，包括控制措施的选择、实施和管理，同时考虑到组织的信息安全风险环境。

该文件为ISO/IEC 27002中描述的控制措施提供了实施指导，并在必要时对其进行了补充，以便能有效地用于管理健康信息安全。

**目的：**ISO 27799为健康组织提供了适用于其行业的ISO/IEC 27002指南，是对满足ISO/IEC 27001:2013附录A要求而提供的指南的补充。

# 参 考 文 献

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

[2] ISO/IEC/IEEE 15939:2017, Systems and software engineering — Measurement process

[3] ISO/IEC 17021, Conformity assessment — Requirements for bodies providing audit and certification of management systems

[4] ISO 19011:2011, Guidelines for auditing management systems

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

[6] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements (GB/T 22080—2016, ISO/IEC 27001:2013, IDT)

[7] ISO/IEC 27002, Information security, cybersecurity and privacy protection — Information security controls (GB/T 22081—2016, ISO/IEC 27002:2013, IDT)

[8] ISO/IEC 27003, Information technology — Security techniques — Information security management — Guidance (GB/T 31496—2015, ISO/IEC 27003:2010, IDT)

[9] ISO/IEC 27004, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (GB/T 31497—2015, ISO/IEC 27004:2004, IDT)

[10] ISO/IEC 27005, Information technology — Security techniques — Information security risk management (GB/T 31722—2015, ISO/IEC 27005:2008, IDT)

[11] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems(GB/T 25067—2020, ISO/IEC 27006:2015, IDT)

[12] ISO/IEC 27007, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (GB/T 28450—2020, ISO/IEC 27007:2017, IDT)

[13] ISO/IEC TS 27008, Information technology — Security techniques — Guidelines for the assessment of information security controls (GB/Z 32916—2016, ISO/IEC TR 27008:2011, IDT)

[14] ISO/IEC 27009, Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements (GB/T 38631—2020, ISO/IEC 27009:2016, MOD)

[15] ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications(GB/T 32920—2016,ISO/IEC 27010:2012, IDT)

[16] ISO/IEC 27011, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

[17] ISO/IEC 27013, Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[18] ISO/IEC 27014, Information security, cybersecurity and privacy protection — Governance of information security (GB/T 32923—2016, ISO/IEC 27014:2013, IDT)

[19] ISO/IEC TR 27016, Information technology — Security techniques — Information

security management — Organizational economics

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

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

[22] ISO/IEC 27019, Information technology — Security techniques — Information security controls for the energy utility industry

[23] ISO/IEC 27021, Information technology — Security techniques — Competence requirements for information security management systems professionals

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

[25] ISO Guide 73:2009, Risk management — Vocabulary

[26] IEC 62645, Nuclear power plants — Instrumentation, control and electrical power systems — Cybersecurity requirements

# 索　　引

## 汉语拼音索引

G



H



J



K



L



M



N



P



S

W



X



Y



Z

# 英文对应术语索引

L



M



N



O



P



R