



# 中华人民共和国国家标准

GB/T XXXXX—XXXX/ISO/IEC 27000:2009

---

## 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 27000:2009, IDT)

(报批稿)

XXXX – XX – XX 发布

XXXX – XX – XX 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 ..... IV

引言 ..... V

1 范围 ..... 1

2 术语和定义 ..... 1

3 信息安全管理體系 ..... 6

    3.1 介绍 ..... 6

    3.2 什么是 ISMS..... 7

        3.2.1 概述和原则 ..... 7

        3.2.2 信息 ..... 7

        3.2.3 信息安全 ..... 7

        3.2.4 管理 ..... 8

        3.2.5 管理体系 ..... 8

    3.3 过程方法 ..... 8

    3.4 ISMS 为什么重要..... 8

    3.5 建立、监视、保持和改进 ISMS..... 9

        3.5.1 概述 ..... 9

        3.5.2 识别信息安全要求 ..... 9

        3.5.3 评估信息安全风险 ..... 10

        3.5.4 选择和实施信息安全控制措施 ..... 10

        3.5.5 监视，保持和改进 ISMS 有效性 ..... 10

    3.6 ISMS 关键成功因素..... 10

    3.7 ISMS 标准族的益处..... 10

4 ISMS 标准族..... 11

    4.1 一般信息 ..... 11

    4.2 概述和术语标准 ..... 12

        4.2.1 ISO/IEC 27000（本标准） ..... 12

    4.3 要求标准 ..... 12

        4.3.1 ISO/IEC 27001 ..... 12

        4.3.2 ISO/IEC 27006 ..... 12

    4.4 一般指南标准 ..... 13

        4.4.1 ISO/IEC 27002 ..... 13

        4.4.2 ISO/IEC 27003 ..... 13

        4.4.3 ISO/IEC 27004 ..... 13

        4.4.4 ISO/IEC 27005 ..... 13

        4.4.5 ISO/IEC 27007 ..... 13

    4.5 行业特定指南标准 ..... 13

4.5.1 ISO/IEC 27011 ..... 13

4.5.2 ISO 27799 ..... 14

附录 A（资料性附录） 条款表达的措辞形式..... 15

附录 B（资料性附录） 术语分类..... 16

参考文献 ..... 18

## 前 言

本标准按照GB/T1.1-2009的规则起草。

本标准等同采用国际标准ISO/IEC 27000:2009《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提出并归口。

本标准起草单位：中国电子技术标准化研究所、上海二零卫士有限公司、北京信息安全测评中心。

本标准主要起草人：上官晓丽、许玉娜、闵京华、赵章界。

# 引言

## 0.1 概述

管理体系标准为建立和运行管理体系提供一个可遵循的模型。这个模型综合了该领域中专家已达成一致的、可代表国际技术发展水平的特征。ISO/IEC JTC1 SC27（国际信息安全技术标准化组织）设置了一个专家委员会专门开发信息安全管理国际标准，也称为信息安全管理（Information Security Management System，简称ISMS）标准族。

组织通过使用ISMS标准族，能够开发和实施管理其信息资产安全的框架，并为保护组织信息（诸如，财务信息、知识产权、员工详细资料，或者受客户或第三方委托的信息）的ISMS的独立评估做准备。

## 0.2 ISMS 标准族

ISMS标准族<sup>1</sup>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”这一通用标题下，ISMS标准族由下列标准组成：

- ISO/IEC 27000:2009(也即本标准) 信息技术 安全技术 信息安全管理 概述和词汇
- GB/T 22080-2008 信息技术 安全技术 信息安全管理 要求
- GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则
- ISO/IEC 27003:2010 信息技术 安全技术 信息安全管理实施指南
- ISO/IEC 27004:2009 信息技术 安全技术 信息安全管理测量
- ISO/IEC 27005:2008 信息技术 安全技术 信息安全风险管理
- GB/T 25067-2010 信息技术 安全技术 信息安全管理审核认证机构的要求
- ISO/IEC 27007 信息技术 安全技术 信息安全管理审核指南
- ISO/IEC 27011:2008 信息技术 安全技术 基于ISO/IEC 27002的电信行业组织的信息安全管理指南

注：通用标题“信息技术 安全技术”是指这些标准是由ISO/IEC JTC1 SC27制定的。

不在通用标题“信息技术 安全技术”之列，同时也属于ISMS标准族的标准如下所示：

- ISO 27799:2008 健康信息学 使用ISO/IEC 27002的健康信息安全管理

## 0.3 本标准的目的

本标准提供了信息安全管理概述，该体系形成了ISMS标准族的主题，并定义了相关术语。

注：附录A阐明了ISMS标准族在文字表达上如何区分要求和/或指南。

ISMS标准族包括的标准：

- a) 定义ISMS的要求及其认证机构的要求；
- b) 提供对整个“规划-实施-检查-处置”（PDCA）过程 and 要求的直接支持、详细指南和（或）解释；
- c) 阐述特定行业的ISMS指南；
- d) 阐述ISMS的一致性评估。

本标准提供的术语和定义：

1) <sup>1</sup> 本节中列出的没有指明发布年的标准仍在开发中。

- 包含ISMS标准族中通用的术语和定义；
- 未包含ISMS标准族使用的所有术语和定义；
- 不限制ISMS标准族定义各自使用的术语。

相对于涉及ISO/IEC 27002中所有控制措施的标准而言，那些仅阐述ISO/IEC 27002中控制措施实施的标准，不包括在ISMS标准族内。





# 信息技术 安全技术 信息安全管理 概述和词汇

## 1 范围

本标准提供：

- a) ISMS标准族的概述；
- b) 信息安全管理（ISMS）的介绍；
- c) “规划-实施-检查-处置”（PDCA）过程的简要描述；
- d) ISMS标准族所用的术语和定义。

本标准适用于所有类型的组织（例如，商业企业、政府机构、非赢利组织）。

## 2 术语和定义

下列术语和定义适用于本文件。

注：定义或注中的术语如果在条款的其他地方被定义，则以黑体标出并在其后的圆括号中标明其条目号。这种黑体术语可以在定义中替换为其完整的定义。

示例：

**攻击**（2.4）被定义为“破坏、泄露、改变、损伤、偷窃或者未授权访问或未授权使用**资产**（2.3）的企图”；

**资产**被定义为“对组织有价值的任何东西”。

如果术语“**资产**”被其定义替换，则：

**攻击**的定义变为“破坏、泄露、改变、损伤、偷窃或者未授权访问或未授权使用对组织有价值的任何东西的企图”。

### 2.1

**访问控制** access control

基于业务要求和安全要求，确保授权和受限地访问**资产**（2.3）的手段。

### 2.2

**可核查性** accountability

实体的一种特性，表征对自己的动作和做出的决定负责。

### 2.3

**资产** asset

对组织有价值的任何东西。

注：有许多类型的资产，包括：

- (a) **信息资产**（2.18）；
- (b) 软件，如计算机程序；
- (c) 物理资产，如计算机；
- (d) 服务；

(e) 人员及其资格、技能和经验;

(f) 无形资产, 如名誉和形象。

## 2.4

### 攻击 attack

破坏、泄露、篡改、损伤、偷窃、未经授权访问或未经授权使用**资产** (2.3) 的企图。

## 2.5

### 鉴别 authentication

确保一个实体声称的特征是正确的保障措施。

## 2.6

### 真实性 authenticity

一个实体正是其所声称实体的特性。

## 2.7

### 可用性 availability

根据授权实体的要求可访问和使用的特性。

## 2.8

### 业务连续性 business continuity

确保持续的业务运作的**过程** (2.31) 和/或**规程** (2.30)。

## 2.9

### 保密性 confidentiality

信息不能被未授权的个人、实体或者**过程** (2.31) 利用或知悉的特性。

## 2.10

### 控制措施 control

管理**风险** (2.34) 的方法, 包括**方针** (2.28)、**规程** (2.30)、**指南** (2.16)、惯例或组织结构。它们可以是行政、技术、管理、法律等方面的。

注: 控制措施也用作防护措施或对策的同义词。

## 2.11

### 控制目标 control objective

描述实施**控制措施** (2.10) 的结果所要达到的目标的声明。

## 2.12

### 纠正措施 corrective action

消除已查明的不符合项或其他不期望情形的成因的措施。

[ISO 9000:2005]

## 2.13

### 有效性 effectiveness

实现计划活动和达到计划结果的程度。

[ISO 9000:2005]

## 2.14

**效率 efficiency**

所达到的结果和资源使用情况之间的关系。

## 2.15

**事态 event**

一组特别情况的发生。

[ISO/IEC Guide 73:2002]

## 2.16

**指南 guideline**

为达到目标而期望做什么的建议。

## 2.17

**影响 impact**

对已达到的业务目标水平的不利改变。

## 2.18

**信息资产 information asset**

对组织有价值的知识或数据。

## 2.19

**信息安全 information security**

保持信息的**保密性**（2.9）、**完整性**（2.25）和**可用性**（2.7）。

注：此外，诸如**真实性**（2.6）、**可核查性**（2.2）、**抗抵赖**（2.27）和**可靠性**（2.33）等其他特性也可被包括进来。

## 2.20

**信息安全事态 information security event**

已识别的一种系统、服务或网络状态的发生，指出可能违反**信息安全**（2.19）**方针**（2.28）或**控制措施**（2.10）失效，或者一种可能与安全相关但以前不为人知的情况。

## 2.21

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

一个或一系列意外或不期望的**信息安全事态**（4.20），它 / 它们极有可能损害业务运行并威胁**信息安全**（2.19）。

## 2.22

**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**（2.21）的**过程**（2.31）。

2.23

信息安全管理体系 (ISMS) information security management system (ISMS)

整个**管理体系** (2.26) 的一部分, 基于业务风险方法, 建立、实施、运行、监视、评审、保持和改进**信息安全** (2.19)。

2.24

信息安全风险 information security risk

**威胁** (2.45) 利用单个或一组**资产** (2.3) 的**脆弱性** (2.46) 并对组织造成损害的可能性。

2.25

完整性 integrity

保护**资产** (2.3) 的准确和完整的特性。

2.26

管理体系 management system

实现组织目标的**方针** (2.28)、**规程** (2.30)、**指南** (2.16) 和相关资源的框架。

2.27

抗抵赖 non-repudiation

证明所声称**事态** (2.15) 或行为的发生及其发起实体的能力, 以解决有关**事态** (2.15) 或行为发生与否以及**事态** (2.15) 中实体是否牵涉的争端。

2.28

方针 policy

管理者正式发布的总的宗旨和方向。

2.29

预防措施 preventive action

消除潜在不符合项或其他不期望的潜在情形的成因的措施。

[ISO 9000:2005]

2.30

规程 procedure

执行活动或**过程** (2.31) 的规定方式。

[ISO 9000:2005]

2.31

过程 process

将输入转换成输出的相互关联或相互作用的活动集。

[ISO 9000:2005]

2.32

记录 record

陈述所达到的结果或提供所执行活动的证据的文件。

[ISO 9000:2005]

## 2.33

**可靠性 reliability**

与预期行为和结果一致的特性。

## 2.34

**风险 risk**

**事态**（2.15）发生的可能性及其后果的组合。

[ISO/IEC Guide 73:2002]

## 2.35

**风险接受 risk acceptance**

接受**风险**（2.34）的决定。

[ISO/IEC Guide 73:2002]

## 2.36

**风险分析 risk analysis**

系统地使用信息以识别风险来源并估算**风险**（2.34）。

[ISO/IEC Guide 73:2002]

注：风险分析为**风险评价**（2.41）、**风险处置**（2.43）和**风险接受**（2.35）提供基础。

## 2.37

**风险评估 risk assessment**

**风险分析**（2.36）和**风险评价**（2.41）的整个过程（2.31）。

[ISO/IEC Guide 73:2002]

## 2.38

**风险沟通 risk communication**

决策者和其他利益相关者之间关于**风险**（2.34）的信息交换或共享。

[ISO/IEC Guide 73:2002]

## 2.39

**风险准则 risk criteria**

评估**风险**（2.34）重要程度的参照条款。

[ISO/IEC Guide 73:2002]

## 2.40

**风险估算 risk estimation**

为**风险**（2.34）发生的可能性及其后果赋值的活动。

[ISO/IEC Guide 73:2002]

## 2.41

风险评价 risk evaluation

将估算的**风险** (2.34) 与给定的**风险准则** (2.39) 加以比较以确定**风险** (2.34) 严重性的**过程** (2.31)。  
[ISO/IEC Guide 73:2002]

## 2.42

风险管理 risk management

指导和控制一个组织相关**风险** (2.34) 的协调活动。

[ISO/IEC Guide 73:2002]

注：风险管理一般包括**风险评估** (2.37)、**风险处置** (2.43)、**风险接受** (2.35)、**风险沟通** (2.38)、风险监视和风险评审。

## 2.43

风险处置 risk treatment

选择并且执行措施来更改**风险** (2.34) 的**过程** (2.31)。

[ISO/IEC Guide 73:2002]

## 2.44

适用性声明 statement of applicability

描述与组织的**信息安全管理**体系 (2.23) 相关的和适用的**控制目标** (2.11) 和**控制措施** (2.10) 的文件。

## 2.45

威胁 threat

可能导致对系统或组织的损害的不期望事件发生的潜在原因。

## 2.46

脆弱性 vulnerability

可能会被**威胁** (2.45) 所利用的**资产** (2.3) 或**控制措施** (2.10) 的弱点。

# 3 信息安全管理

## 3.1 介绍

所有类型和规模的组织：

- a) 收集、处理、存储和传输大量信息；
- b) 认识到信息以及相关过程、系统、网络和人实现组织目标的重要资产；
- c) 面临可能影响资产发挥作用的许多风险；
- d) 通过实施信息安全控制措施更改风险。

组织持有和处理的所有信息在使用中易受攻击、错误、自然灾害（例如，洪水或火灾）等威胁和内在脆弱性的影响。术语“信息安全”一般是建立在作为有价值资产的信息基础之上，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为已授权的需要者及时可用，可提高业务效率。

通过有效地定义、实现、保持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提高法律符合性及自身形象来说，必不可少。用以指导适当控制措施的实施和处理不可接受的信息安全风险的协调活动，通常被认为是信息安全管理要素。

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改变，组织需：

- a) 监视和评价已实施的控制措施和规程的有效性；
- b) 识别需要处理的新出现的风险；
- c) 视需要，选择、实施和改进适当的控制措施。

为了关联和协调这种信息安全活动，每个组织需要建立信息安全方针和目标，并通过使用管理体系来有效地达到这些目标。

## 3.2 什么是 ISMS

### 3.2.1 概述和原则

ISMS提供了一个建立、实施、运行、监视、评审、保持和改进保护信息资产的模型，以实现组织的业务目标，该目标是基于风险评估和组织为有效处置和管理风险而设定的风险可接受级别来确定的。分析信息资产的保护要求并按照要求应用适当的控制措施确保这些信息资产得到保护，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) 得到管理承诺和反映利益相关者的利益；
- d) 提升社会价值观；
- e) 进行风险评估，用以确定适当的控制措施来达到可接受的风险级别；
- f) 将安全作为一个基本要素纳入信息网络和系统；
- g) 主动预防和发现信息安全事件；
- h) 确保有一个整体的信息安全管理方法；
- i) 持续地对信息安全进行再评估和适时进行修正。

### 3.2.2 信息

信息是一种资产，像其他重要的业务资产一样，对组织业务来说是必不可少的，因此需要得到适当的保护。信息可以以许多形式存储，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的未被表示的信息。信息可采用各种不同手段进行传输，包括：信使、电子通讯或口头交谈。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。

组织的信息依赖信息和通信技术。这种技术是任何组织中的基本元素，并有助于创建、处理、存储、传输、保护和销毁信息。随着全球业务环境互联程度的不断扩大，由此现在的信息面临着各种各样大量的威胁和脆弱性，因此保护信息的需求就随之增多。

### 3.2.3 信息安全

信息安全主要包括保密性、可用性和完整性。信息安全以确保业务成功和持续性以及将影响最小化为目标，涉及到应用和管理防范各种威胁的适当安全措施。

信息安全是通过实施一套适用的控制措施来实现的，包括方针政策、过程、规程、组织结构、软件和硬件；这套控制措施通过所选用的风险管理过程来选择并使用ISMS来管理，以保护已识别的信息资产。

这些控制措施需要得到详细说明、实施、监视、评审和必要时的改进，以确保满足组织的特定安全和业务目标。相关的信息安全控制措施宜与组织的业务过程充分整合。

### 3.2.4 管理

管理包括一些活动：指导、控制和不断改进在适当结构中的组织。这样的管理活动包括有关组织、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的一个人，到大规模组织中许多个体所组成的管理层次体系。

就ISMS而言，管理包括通过保护组织的信息资产来实现业务目标所必需的监督和决策。信息安全管理是通过制定和使用为所有与组织相关的人员所应用的、贯穿于整个组织的信息安全方针、标准、规程和指南来表达。

### 3.2.5 管理体系

管理体系使用资源框架来达到组织的目标。管理体系包括组织结构、方针策略、规划活动、责任、实践、规程、过程和资源。

就信息安全而言，管理体系可以使组织：

- a) 满足客户和其它利益相关者的安全要求；
- b) 改进组织的计划和活动；
- c) 符合组织的信息安全目标；
- d) 遵从法律法规、规章和行业要求；
- e) 采取有组织的方式管理信息资产，以便于持续改进和调整以适应当前的组织目标 and 环境。

## 3.3 过程方法

为使组织有效运作，需要识别和管理众多活动。任何使用资源的活动需要予以管理，以便能够用一组相互关联或相互作用的活动来完成从输入到输出的转换——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，通常这个转换是在计划和受控的条件下完成的。组织内过程的系统化应用，连同这些过程的识别和相互作用及其管理，可称作“过程方法”。

ISMS标准族中所呈现的ISMS过程方法基于ISO管理体系标准中所采用的运行原则，通常称为“规划—实施—检查—处置”（PDCA）过程。

- a) 规划——确定目标并制定计划（分析组织的情况，确定整体目标和设定具体目标，并制定实现这些目标的计划）；
- b) 实施——实施计划（完成计划要做的事情）；
- c) 检查——测量结果（测量/监视达到计划目标的程度）；
- d) 处置——纠正和改进活动（总结教训以改进活动进而达到更好的结果）。

## 3.4 ISMS 为什么重要

作为组织ISMS的一部分，与组织信息资产相关的风险需要受到关注。实现信息安全需要对风险进行管理，包括与组织内部或组织使用的所有形式的信息相关的，来自物理、人员和技术上威胁的风险。

采用ISMS宜是一个组织的战略决策，并应按照组织的需要进行充分整合、调整和更新。

组织ISMS的设计和实施受到组织的需要与目标、安全要求、所采用的业务过程和规模与结构的影响。ISMS的设计和运行需要反映组织的所有利益相关者（包括顾客、供应商、业务伙伴、股东和其它相关第三方）的利益和信息安全要求。

在相互连接的世界中，信息及其相关过程、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着来自各个方面的安全威胁，包括计算机辅助欺诈、间谍活动、故意破坏、火灾和洪水。由恶意



代码、计算机黑客和拒绝服务攻击引起的对信息系统和网络的损害已经变得更加普遍、更有野心和日益复杂。

ISMS对于公共和专用两部分业务都是重要的。在任何行业中，ISMS支持电子商务，并且对于风险管理活动是必不可少的。公共和专用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，含有信息资产的移动存储设备的分散可削弱传统控制措施的有效性。当组织采用了ISMS标准族后，可以向业务伙伴和其它相关方证明其应用一致的和互认的信息安全原则的能力。

在设计和开发信息系统时，并不是总能考虑到信息安全考虑。而且，信息安全经常被认为是一种技术解决方案。然而，通过技术手段实现的安全是有限的，并且在没有ISMS的适当管理和规程的支持下，可能是无效的。事后将安全集成到信息系统中可能是麻烦且昂贵的。ISMS包括识别哪些控制措施已经就位，且要求仔细规划和关注细节。举例来说，访问控制措施，可能是技术的（逻辑的）、物理的、行政的（管理的）或其组合，提供一种手段以确保对信息资产的访问是基于业务和安全要求进行授权和限制的。

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以防范信息安全风险；
- b) 保持一个结构化的和整体的框架，来识别和评估信息安全风险、选择和应用适用的控制措施、测量和改进控制措施的有效性；
- c) 持续改进其控制环境；
- d) 有效地达到法律法规的符合性。

### 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，需要采取下列步骤：

- a) 识别信息资产及其相关的安全要求（见3.5.2）；
- b) 评估信息安全风险（见3.5.3）；
- c) 选择和实施相关控制措施以管理不可接受的风险（见3.5.4）；
- d) 监视、保持和改进与组织信息资产相关的安全控制措施的有效性（见3.5.5）。

为确保在持续发展的基础上，ISMS有效地保护组织的信息资产，有必要不断地重复执行步骤a)～d)，以识别风险的变化，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之内，信息安全要求可通过了解下列方面进行识别：

- a) 已识别的信息资产及其价值；
- b) 信息处理和存储的业务需求；
- c) 法律法规、规章和合同要求。

对组织信息资产相关风险所进行的系统化评估将包括分析：信息资产面临的威胁；信息资产的脆弱性及其威胁发生的可能性；以及任何信息安全事件对信息资产的潜在影响。相关安全控制措施的支出费用宜与认识到的风险发生时对业务的影响相适合。

#### 3.5.3 评估信息安全风险

信息安全风险管理，需要一种合适的风险评估和风险处置方法，该方法可以包括成本和效益的估算、法律要求、社会、经济以及环境，并涉及利益相关者的关注，优先排序，有时还涉及其它输入和变量。

信息安全风险评估的结果，有助于指导和确定以下两方面做出合适的管理处置决策，一是有关信息安全风险管理措施和优先顺序的决策，二是为了防止这些风险，有关实现相关安全控制的决策。ISO/IEC 27005 提供了信息安全风险管理指南，包括有关风险评估、风险处置、风险接受、风险沟通、风险监视和风险评审等方面的建议。

### 3.5.4 选择和实施信息安全控制措施

一旦识别了信息安全要求并确定和评估了所识别信息资产的信息安全风险(包括作出的信息安全风险处置决定)，需要选择并实施适当的控制措施，以确保信息安全风险降低到组织可接受的级别。控制措施可以选自ISO/IEC 27002，也可以选自其他相关的控制措施集，或者适当时可以设计新的控制措施以满足特定的需要。安全控制措施的选择依据安全要求并考虑到信息安全风险接受的准则、风险处置选项和组织所应用的一般风险管理方法。控制措施的选择和实施可以写入适用性声明文件中，以有助于符合性要求。

ISO/IEC 27002中规定的控制措施是公认的适用于大多数组织的最佳实践，并易于裁剪以适应于各种规模和复杂度的组织。ISMS标准族中的其他标准为管理体系（ISO/IEC 27001）选择和应用ISO/IEC 27002中的信息安全控制措施提供指南。

### 3.5.5 监视，保持和改进 ISMS 有效性

组织需要通过对照其方针和目标，监视和评估ISMS的执行情况，并将结果报告给管理层以供评审，来保持和改进ISMS。这种ISMS评审允许将受监视领域（包括信息安全控制措施的监视）的记录，作为纠正、预防和改进措施的确认、验证和可追溯的证据。

### 3.6 ISMS 关键成功因素

很多因素对于一个组织成功实施ISMS以满足其业务目标都是关键的。关键成功因素示例包括：

- a) 信息安全方针、目标和与目标保持一致的活动；
- b) 与组织文化一致的设计、实施、监视、保持和改进信息安全的方法和框架；
- c) 来自所有管理层，尤其是最高管理者的可见的支持和承诺；
- d) 通过应用信息安全风险管理（见 ISO/IEC 27005）所达到的对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，以使所有员工和其他相关方知悉在信息安全方针、标准等中所阐明的他们的信息安全职责，并激发他们做出相应的行动；
- f) 有效的信息安全事件管理过程；
- g) 有效的业务连续性管理方法；
- h) 用于评价信息安全管理执行情况和改进反馈建议的测量系统。

ISMS将增加组织始终具备保护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的益处主要来自于信息安全风险的降低（即减少信息安全事件发生的可能性和（或）由其造成的影响）。特别地，采用ISMS标准族可获得的益处包括：

- a) 支持规定、实施、运行和保持一个全面的、成本有效的、集成的、与 ISMS 紧密符合的过程，，以满足组织跨不同业务和场所的需要；
- b) 在整体风险管理和治理的背景下，帮助管理者构造其面向信息安全管理的方法，包括对业务和系统所有者进行关于信息安全整体管理的教育和培训；
- c) 以非限定的方式促进全球认可的良好的信息安全实践，给予组织一定自由度，以方便其采用和改进适合其特定环境的相关控制措施，并在面临内部和外部变化的情况下保持控制措施；

- d) 为信息安全提供共同语言和概念基础，使得利用符合规范的 ISMS 在业务伙伴中建立信心更为容易，尤其是当他们需要有一个经认可的认证机构进行 ISO/IEC27001 认证时。

4 ISMS 标准族

4.1 一般信息

ISMS标准族由一系列相互关联的标准组成，包括已经发布的或正在制定中的，并包含许多重要的结构化部分。这些部分关注描述ISMS要求（ISO/IEC 27001）和那些进行ISO/IEC 27001符合性认证的认证机构的要求（ISO/IEC 27006）的规范性标准。其他标准提供ISMS实施的各方面指南，包括一般过程、控制措施的相关指南以及行业特定的指南。ISMS标准族中各标准<sup>2</sup>之间的关系如图1所示。

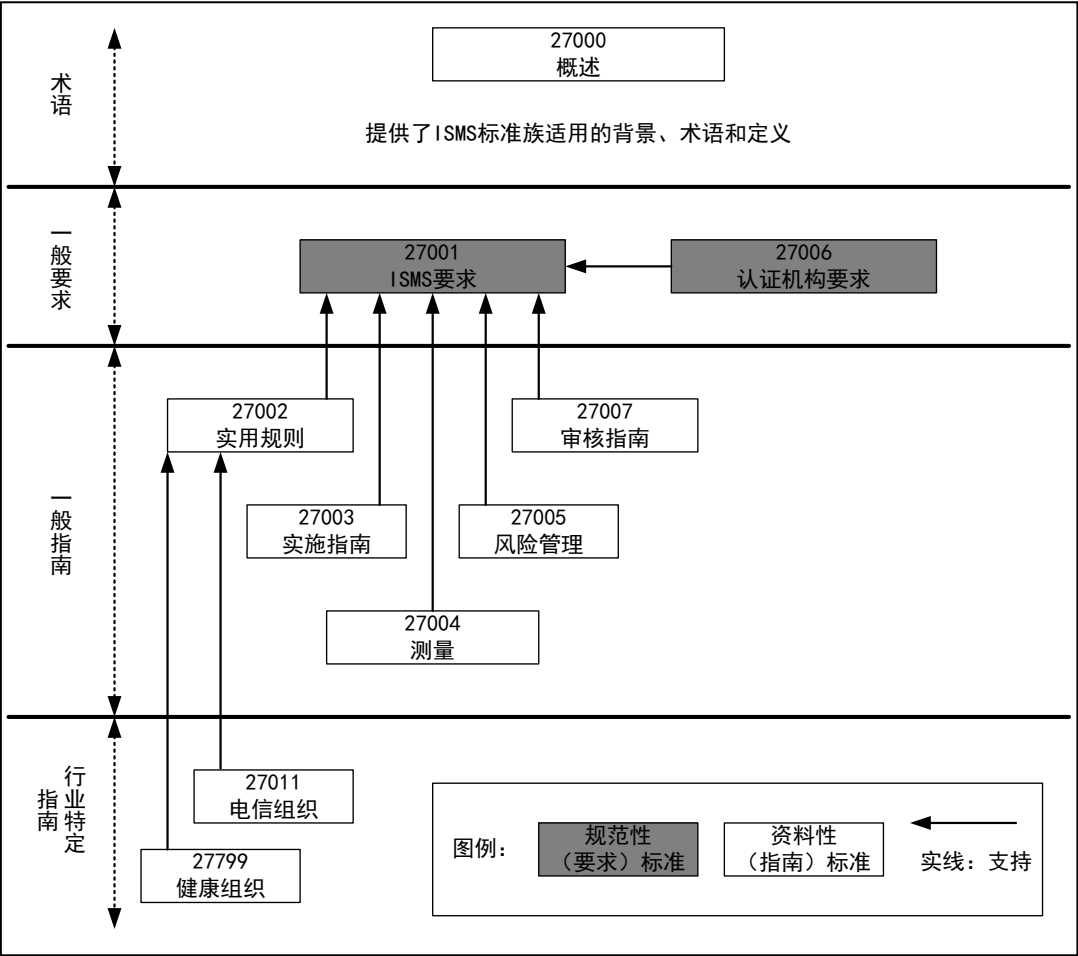


图1 ISMS 标准族关系

为整个PDCA过程和ISO/IEC 27001（见4.3.1）中所规范的要求提供直接支持、详细指南和/或解释的标准有：ISO/IEC 27000（见4.2.1）、ISO/IEC 27002（见4.4.1）、ISO/IEC 27003（见4.4.2）、ISO/IEC 27004（见4.4.3）、ISO/IEC 27005（见4.4.4）和ISO/IEC 27007（见4.4.5）。

2) <sup>2</sup> 国际标准 ISO/IEC 27007 正在制定中。

ISO/IEC 27006(见4.3.2)阐述对提供ISMS认证的机构的要求。ISO/IEC 27011(见4.5.1)和ISO 27799(见4.5.2)阐述ISMS的行业特定指南。<sup>3</sup>

ISMS标准族与许多其他ISO和ISO/IEC标准保持着关系,按如下分类做进一步描述:

- a) 描述概述和术语的标准(见4.2);
- b) 规范要求的标准(见4.3);
- c) 描述一般指南的标准(见4.4);
- d) 描述行业特定指南的标准(见4.5)。

## 4.2 概述和术语标准

### 4.2.1 ISO/IEC 27000(本标准)

*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 (ISMS) 的介绍;
- c) “规划-实施-检查-处置”(PDCA)过程的简要描述;
- d) 整个ISMS标准族中使用的术语和定义。

目的:ISO/IEC 27000描述信息安全管理体 系 (ISMS标准族的主题)的基础,并定义相关术语。

## 4.3 要求标准

### 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:该标准规定了在组织整体业务风险的背景下建立、实施、运行、监视、评审、保持和改进正式的信息安全管理体 系 (ISMS)的要求。它规定了适合于单个组织或其部门需要的安全控制措施的实施要求。该标准适用于所有类型的组织(例如,商业企业、政府机构、非赢利组织)。

目的:ISO/IEC 27001提供开发和运行ISMS的规范性要求,包括一套控制和减轻风险的控制措施,这些风险与组织力求通过运行其ISMS保护的信息资产相关。运行ISMS的组织可以对其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中恰当地选择控制目标和控制措施,以覆盖已识别的要求。表A.1(ISO/IEC 27001)中列出的控制目标和控制措施是直接来自ISO/IEC 27002第5章至第15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中规定要求的基础上,为依据ISO/IEC 27001提供审核和ISMS认证的机构规定要求并提供指导。它主要为依照ISO/IEC 27001实施ISMS认证的认证机构的认可提供支持。

目的:ISO/IEC 27006补充ISO/IEC 17021以提供认证机构被认可的要求,从而许可这些组织提供与ISO/IEC 27001中所阐明要求一致的符合性认证。

## 4.4 一般指南标准

### 4.4.1 ISO/IEC 27002

---

3) <sup>3</sup> ISO/IEC 27008、ISO/IEC 27009 和 ISO/IEC 27010 保留给那些在本标准发布之时还没有被定义的、与 ISMS 标准族有关的将来标准。

*信息技术 — 安全技术 — 信息安全管理实用规则*

范围：该标准提供一套普遍接受的控制目标和最佳实践控制措施，用于指导选择和实施控制措施以实现信息安全。

目的：ISO/IEC 27002提供关于信息安全控制措施实施的指南。特别是第5章至第15章在支持ISO/IEC 27001的A.5至A.15中所规定的控制措施的最佳实践方面提供特定的实施建议和指南。

**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：该标准为依照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更多信息。

目的：ISO/IEC 27003为依照ISO/IEC 27001成功实施ISMS提供一种面向过程的方法。

**4.4.3 ISO/IEC 27004***信息技术 — 安全技术 — 信息安全管理 测量*

范围：该标准为评估ISO/IEC 27001中规定的用于实施和管理信息安全的ISMS、控制目标和控制措施的有效性，针对相关测量的开发和使用提供指南和建议。

目的：ISO/IEC 27004提供了一个测量框架，允许ISMS按ISO/IEC 27001进行测量，实现有效性评估。

**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。该标准中描述的方法支持ISO/IEC 27001中所规定的一般概念。

目的：ISO/IEC 27005为实施面向过程的风险管理方法提供指南，以帮助满意地实施和完成ISO/IEC 27001中给出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ISO/IEC 19011中可用于一般管理体系指南的基础上，提供实施ISMS审核指南和信息安全管理体系审核员能力的指南。

目的：ISO/IEC 27007为需要对照ISO/IEC 27001中所规定的要求，进行ISMS内部或外部审核或者ISMS审核方案管理的组织，提供指南。

**4.5 行业特定指南标准****4.5.1 ISO/IEC 27011***信息技术 — 安全技术 — 基于ISO/IEC 27002的电信行业组织的信息安全管理指南*

范围：该标准为支持电信行业组织的信息安全管理（ISM）的实施提供指南。

目的：ISO/IEC 27011根据电信行业特点对ISO/IEC 27002进行了调整和补充，为电信行业组织提供信息安全管理指南，以实现ISO/IEC 27001附录A的要求。

**4.5.2 ISO 27799***健康信息学 — 使用ISO/IEC 27002的健康信息安全管理*

范围：该标准为支持在健康组织中实施信息安全管理（ISM）提供指南。

目的：ISO/IEC 27799根据健康组织特点对ISO/IEC 27002进行了调整和补充，为健康组织提供信息安全管理指南，以实现ISO/IEC 27001附录A的要求。

附 录 A  
(资料性附录)  
条款表达的措辞形式

ISMS 标准族的每个标准本身没有对任何人施加遵从的义务。但是，这种义务可以被施加，例如通过法律或合同。为了能够声明符合某一个标准，用户需要能够识别必需被满足的要求。用户还需要能够将这些要求与可选择的其它建议进行区分。

下表阐明了 ISMS 标准族的标准在文字表达上如何区分要求和/或建议。

类别	解释
要求	术语“应”和“不应”表明要求，要严格遵从以符合标准且不允许偏离。
建议	术语“宜”和“不宜”表明在几种可能中建议特别适合的一种但没有提到或排除其它的可能，或者某种做法是首选的但不是必然要求的，或者（从反面说）某种可能性或做法是不赞成的但不是禁止的。
许可	术语“可”和“不必”表明在标准的限制中做法是许可的。
可能性	术语“能”和“不能”表明某件事情发生的可能性。

附 录 B  
(资料性附录)  
术语分类

B.1 信息安全相关的术语

- 2.2 可核查性 accountability
- 2.5 鉴别 authentication
- 2.6 真实性 authenticity
- 2.7 可用性 availability
- 2.9 保密性 confidentiality
- 2.19 信息安全 information security
- 2.25 完整性 integrity
- 2.27 抗抵赖 non-repudiation
- 2.33 可靠性 reliability

B.2 管理相关的术语

- 2.8 业务连续性 business continuity
- 2.12 纠正措施 corrective action
- 2.13 有效性 effectiveness
- 2.14 效率 efficiency
- 2.16 指南 guideline
- 2.23 信息安全管理体系 (ISMS) information security management system (ISMS)
- 2.26 管理体系 management system
- 2.28 方针 policy
- 2.29 预防措施 preventive action
- 2.31 过程 process

B.3 信息安全风险相关的术语

- 2.1 访问控制 access control
- 2.3 资产 asset
- 2.4 攻击 attack
- 2.10 控制措施 control
- 2.11 控制目标 control objective
- 2.15 事态 event
- 2.17 影响 impact
- 2.18 信息资产 information asset
- 2.20 信息安全事态 information security event
- 2.21 信息安全事件 information security incident
- 2.22 信息安全事件管理 information security incident management
- 2.24 信息安全风险 information security risk
- 2.34 风险 risk



- 2.35 风险接受 risk acceptance
- 2.36 风险分析 risk analysis
- 2.37 风险评估 risk assessment
- 2.38 风险沟通 risk communication
- 2.39 风险准则 risk criteria
- 2.40 风险估算 risk estimation
- 2.41 风险评价 risk evaluation
- 2.42 风险管理 risk management
- 2.43 风险处置 risk treatment
- 2.45 威胁 threat
- 2.46 脆弱性 vulnerability

#### B.4 与文件化有关的术语

- 2.30 规程 procedure
- 2.32 记录 record
- 2.44 适用性声明 statement of applicability

## 参 考 文 献

- [1] ISO/IEC 17021:2006, Conformity assessment — Requirements for bodies providing audit and certification of management systems (合格评定 — 管理体系审核认证机构的要求)
- [2] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary (质量管理体系 — 基础和词汇)
- [3] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing (质量和/或环境管理体系审核指南)
- [4] ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements (信息技术 — 安全技术 — 信息安全管理要求)
- [5] ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management (信息技术 — 安全技术 — 信息安全管理实用规则)
- [6] ISO/IEC 27003:2010, Information technology — Security techniques — Information security management system implementation guidance (信息技术 — 安全技术 — 信息安全管理实施指南)
- [7] ISO/IEC 27004:2009, Information technology — Security techniques — Information security management measurement (信息技术 — 安全技术 — 信息安全管理测量)
- [8] ISO/IEC 27005:2008, Information technology — Security techniques — Information security risk management (信息技术 — 安全技术 — 信息安全风险管理)
- [9] ISO/IEC 27006:2007, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems (信息技术 — 安全技术 — 信息安全管理审核认证机构的要求)
- [10] ISO/IEC 27007<sup>4</sup>, Information technology — Security techniques — Guidelines for information security management systems auditing (信息技术 — 安全技术 — 信息安全管理审核指南)
- [11] ISO/IEC 27011:2008, Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (信息技术 — 安全技术 — 基于 ISO/IEC 27002 的电信行业组织的信息安全管理指南)
- [12] ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002 (健康信息学 — 使用 ISO/IEC 27002 的健康信息安全管理)
- [13] ISO/IEC Guide 73:2002, Risk Management — Vocabulary — Guidelines for use in Standards (风险管理 — 词汇 — 标准中使用指南)

---

4) <sup>4</sup> 待发布。