1. 信息安全管理体系 ISO/IEC 27001

1.1. 管理体系及其产业链

管理体系是组织用来保证其完成任务，事件目标的过程集的框架。在 ISO 9000:2000 中，将其定义为建立方针和目标并实现这些目标的体系。

注:一个组织的管理体系可包括若干个不同的管理体系，如质量管理体系、财务管理体系或环境管理体系。

一个典型的管理体系框架如下图所示:

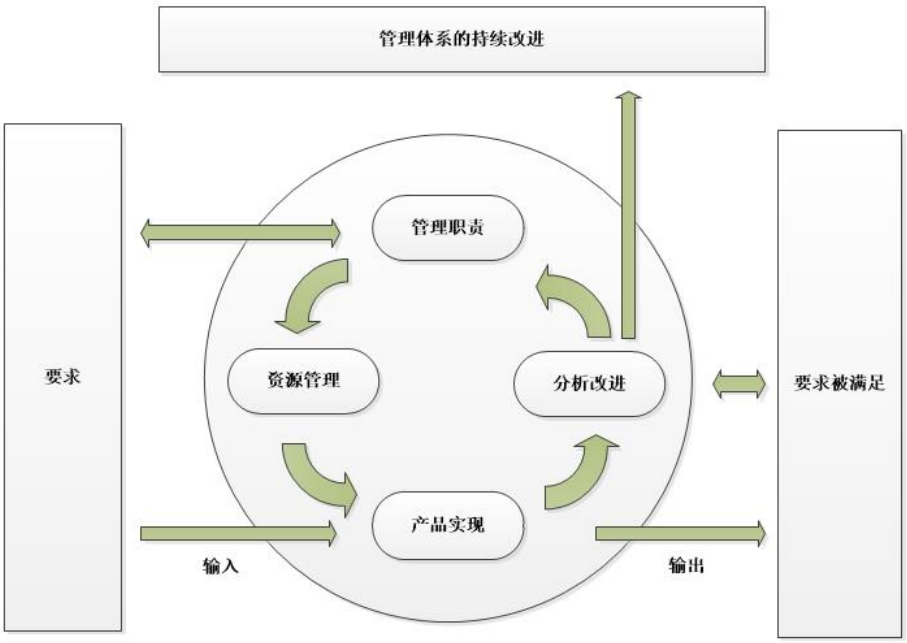


图 1-1

目前存在很多的管理体系，例如质量管理体、系环境管理体系、职业健康管理体系、信息安全管理体系等。质量管理体系是出现比较早发展比较成熟的管理体系，其他管理体系或多或少都借鉴了质量管理体系的经验。

管理体系形成的完整的产业链，如图 11 所示.

信息安全管理体系正如其名称所表述的含义，就是关于信息安全的管理体系。信息安全管理体系是整个管理体系的一部分。它是基于业务风险方法，来建立、实施、运行、监视、评审、保持和改进信息安全的。

ISMS 的概念已经跳出了传统的“为了安全信息而信息安全”的理解，它强调的是基于业务风险方法来组织信息安全活动，其本身只是整个管理体系的一部分。这就要求我们站在全局的观点看待信息安全问题。

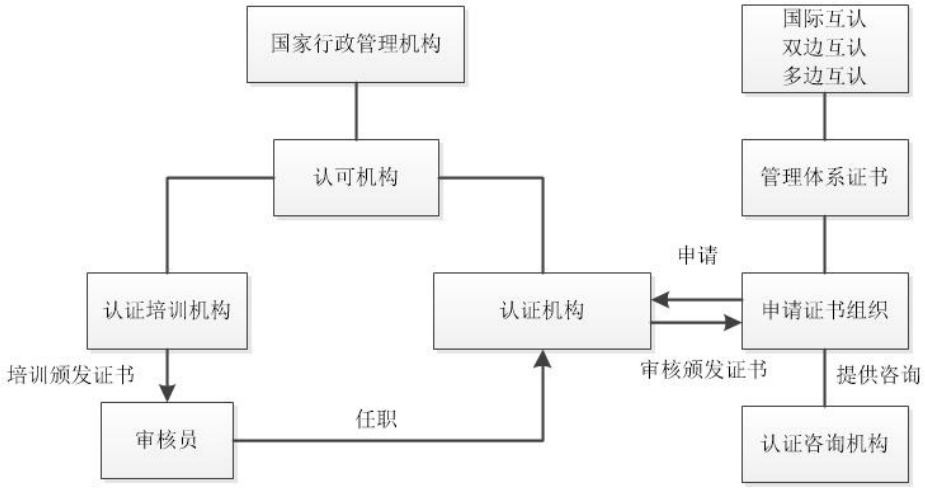


图 123123

1.2. ISO/IEC 27000 标准族

1.2.1. ISO/IEC 27001 发展历程

ISO27000 从诞生到现在只不过 20 年间的事情，但基本上可以看出一个标准 “源于生活，高于生活”的发展特点，也就是说，一个真正普遍适用并能被普遍接受的标准，必然是能体现相关领域最佳惯例并能为最佳惯例的推广起指导作用的。

BS7799 最初是由英国贸工部(DTI)立项的，是业界、政府和商业机构共同倡导的，旨在开发一套可供开发、实施和测量有效安全管理惯例并提供贸易伙伴间信任的通用框架。负责标准开发和管理工作的 BSI—DISC Committee BDD/2 是由来自贸易和工业部门的众多代表共同组成的，其成员在各自的领域都具有足够的影响力，包括金融业的英国保险协会、渣打会计协会、汇丰银行等，通信行业有大英电讯公司，还有像壳牌、联合利华、毕马威(KPMG)等这样的跨国机构。

1995 年，BS7799—1:1995《信息安全管理实施细则》首次出版(其前身是 1993 年发布的 PD0005)，它提供了一套综合性的、由信息安全最佳惯例构成的实施细则，目的是为确定各类信息系统通用控制提供唯一的参考基准。

在随后一段时间里，由于电子商务的发展，由此引发客户、供应商、贸易伙伴间对各自信息保护能力的信任问题，促使第三方认证成为一个急需。信息安全管理遵循一套最佳惯例，但怎样做的？执行程度如何？是否完备？这就需要有一个共同的尺度来进行衡量。

1998 年，BS7799—2:1998《信息安全管理体系规范》公布，这是对 BS7799—1 的有效补充，它规定了信息安全管理体系的要求和对信息安全控制的要求，是一个组织信息安全管理体系评估的基础，可以作为认证的依据。至此，BS7799 标准初步成型。

1999 年 4 月，BS7799 的两个部分被重新修订和扩展，形成了一个完整版的 BS7799:1999。新版本充分考虑了信息处理技术应用的最新发展，特别是在网络和通信领域。除了涵盖以前版本所有内容之外，新版本还补充了很多新的控制，包括电子商务、移动计算、远程工作等。

由于 BS7799 日益得到国际认同，使用的国家也越来越多，2000 年 12 月，国际标准化组织 ISO/IEC JTC 1/SC27 工作组认可 BS7799—1:1999，正式将其转化为国际标准，即所颁布

的 ISO/IEC 17799:2000《信息技术——信息安全管理实施细则》。作为一个全球通用的标准，ISO/IEC 17799 并不局限于 IT，也不依赖于专门的技术，它是由长期积累的一些最佳实践构成的，是市场驱动的结果。

2002 年，BSI 对 BS7799:2—1999 进行了重新修订，正式引入 PDCA 过程模型，以此作为建立、实施、持续改进信息安全管理体系的依据，同时，新版本的调整更显示了与 ISO9001:2000、ISO14001:1996 等其他管理标准以及经济合作与开发组织(OECD)基本原则的一致性，体现了管理体系融合的趋势。2004 年 9 月 5 日，BS7799—2:2002 正式发布，随即提交 ISO 并迈入“快速通道”。

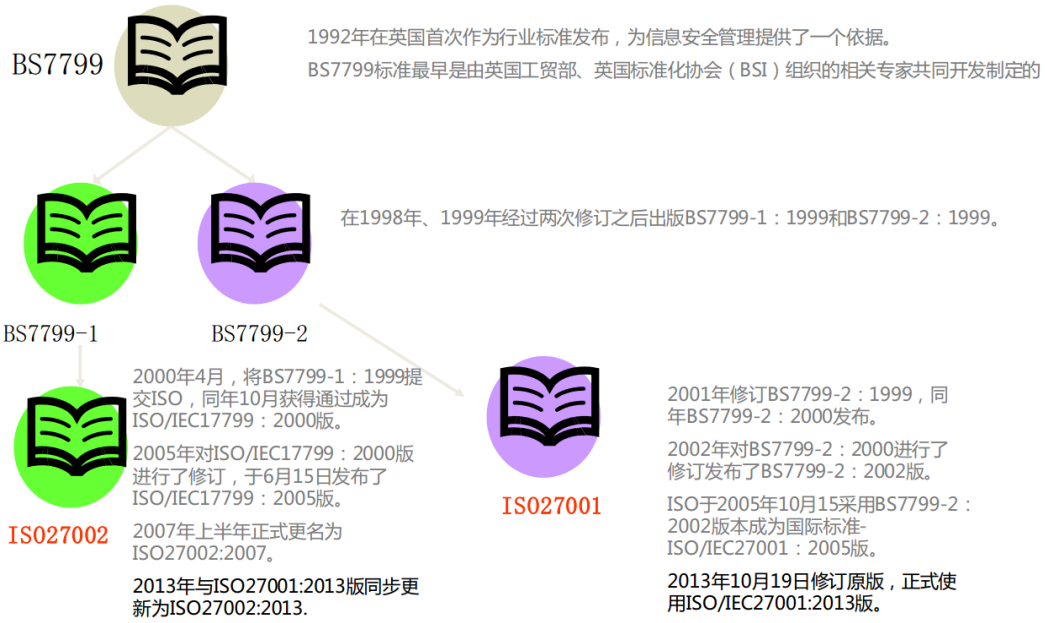
2005 年 6 月，ISO/IEC 17799:2000 经过改版，形成了新的 ISO/IEC 17799:2005，新版本较老版本无论是组织编排还是内容完整性上都有了很大增强和提升。紧接着，被期待已久的 BS7799—2:2002 也终于被 ISO 组织所采纳，于同年 10 月推出了 ISO/IEC 27001:2005。

2007 年 10 月，ISO/IEC 17799:2005 被正式纳入 ISO27000 体系，成为 ISO27002:2007。

2013 年 9 月，ISO/IEC 27001:2005 经过改版，形成了新的 ISO/IEC 27001:2013，新版本从原先 8 个章节扩展到 10 个章节，重建了 ISO 标准 PDCA 章节架构，并将旧版 11 个控制域扩展到 14 个，使结构更合理，表现更清晰。

作为认证标准，ISO27000 系列中最关键的还是 ISO27001，所以，人们更习惯以 ISO27001 来直接代表此系列信息安全管理标准。

图 5 所示为 ISO27000 系列标准的发展历程。



1.2.2. ISO/IEC 27000 标准族一览

ISO/IEC 27000 族标准是国际化组织专门为 ISMS 预留下来的一系列相关标准的总称具体如下:

序号	标准编号	标准名称	出版年份
1	ISO/IEC27000	信息技术-安全技术-信息安全管理体系-概述与术语	2009

序号	标准编号	标准名称	出版年份
2	ISO/IEC27001	信息技术-安全技术-信息安全管理体系-要求	2013
3	ISO/IEC27002	信息技术-安全技术-信息安全管理-实用规则	2013
4	ISO/IEC27003	信息技术-安全技术-信息安全管理体系-实施指南	2010
5	ISO/IEC27004	信息技术-安全技术-信息安全管理-度量	2009
6	ISO/IEC27005	信息技术-安全技术-信息安全风险管理	2011
7	ISO/IEC27006	信息技术-安全技术-信息安全管理体系-认证机构要求	2007
8	ISO/IEC27007	信息技术-安全技术-信息安全管理体系审核指南	2011
9	ISO/IEC27008	信息技术-安全技术-ISMS 控制措施的审核员指南	2011
10	ISO/IEC27010	信息技术-安全技术-部门间和组织间通信的信息安全管理	2012
11	ISO/IEC27011	信息技术-安全技术-通讯行业基于ISO/IEC27002 的信息安全管理指南	2008
12	ISO/IEC27013	信息技术-安全技术-ISO/IEC 27001 与ISO/IEC 20000-1 整合实施指南	2012
13	ISO/IEC27014	信息技术-安全技术-信息安全治理架构	2013
14	ISO/IEC27015	信息技术-安全技术-金融服务行业信息安全管理指南	2012
15	ISO/IEC27017	信息技术-安全技术-信息安全管理-基于ISO/IEC 27002 使用云计算服务信息安全控制措施指南	未发布
16	ISO/IEC27018	信息技术-安全技术-公共云计算服务数据保护控制措施实用规则	未发布
17	ISO/IEC27031	信息技术-安全技术-业务连续性信息通信技术准备指南	2011
18	ISO/IEC27032	信息技术-安全技术-网络安全技术指南	2012
19	ISO/IEC27033-1	信息技术-安全技术-网络安全-概述与概念	2009
20	ISO/IEC27033-2	信息技术-安全技术-网络安全-网络安全设计与实施指南	2012
21	ISO/IEC27033-3	信息技术-安全技术-网络安全-参考网络场景-威胁、设计技术与控制问题	2010
22	ISO/IEC27034-1	信息技术-安全技术-应用安全-应用安全概述与概念	2011
23	ISO/IEC27034-2	信息技术-安全技术-应用安全-组织规范框架	未发布

序号	标准编号	标准名称	出版年份
24	ISO/IEC27034-3	信息技术-安全技术-应用安全-应用安全管理流程	未发布
25	ISO/IEC27034-4	信息技术-安全技术-应用安全-应用安全验证	未发布
26	ISO/IEC27034-5	信息技术-安全技术-应用安全-协议和应用安全控制数据结构	未发布
27	ISO/IEC27034-6	信息技术-安全技术-应用安全-特定应用安全指南	未发布
28	ISO/IEC27035	信息技术-安全技术-信息安全事件管理	2011
29	ISO/IEC27036	信息技术-安全技术-供应关系信息安全(4 部分)	未发布
30	ISO/IEC27040	信息技术-安全技术-存储安全	未发布
31	ISO/IEC27044	信息技术-安全技术-安全信息与事态管理指南	未发布

1.2.3. 主要标准简介

1. ISO/IEC 27000

ISO/IEC 27000 信息安全管理体系—概述与术语提供了 ISMS 标准族中所涉及的通用术语及基本原则，是 ISMS 标准族中最基础的标准之一。ISMS 标准族中的每个标准都有“术语和定义”部分，但不同标准的术语间往往缺乏协调性，而 ISO/IEC 27000 则主要用于实现这种协调

2. ISO/IEC 27001

ISO/IEC 27001 信息安全管理体系—要求是建立信息安全管理体系(ISMS)的一套规范，其中详细说明了建立、实施和维护信息安全管理体系的要求，本标准将在第 3 章进行详细的解析。

3. ISO/IEC 27002

ISO/IEC 27002 信息安全管理—实用规则为在组织内启动、实施、保持和改进信息安全管理提供指南和通用的原则。该标准概述的目标提供了有关信息安全管理通常公认的目标的通用指南。其包含的实施规则可以认为是开发组织具体指南的起点。但该实施规则中的控制和指导并不全都是适用的，应当根据企业自身情况对控制措施进行扩充与裁减。

4. ISO/IEC 27003

ISO/IEC 27003 信息安全管理体系—实施指南为建立、实施、监视、评保持和改进符合 ISO/IEC 27001 的 ISMS 提供了实施指南和进一步的信息，使用者主要为组织内负责实施 ISMS 的人员。

5. ISO/IEC 27004

ISO/IEC 27004 信息安全管理测量主要为组织测量信息安全控制措施和 ISMS 过程的有效性提供指南。

该标准将测量分为有效性测量和过程测量两个类别，列出了多种测量方法，例如调查、问卷、观察、知识评估检查、二次执行、测试以及抽样等。

该标准定义了 ISMS 的测量过程:

1） 首先要实施 ISMS 的测量，应定义选择测量措施，同时确定测量对象和检验标准，形成测量计划；

2） 实施 ISMS 测量的过程中，应定义数据的收集、分析和报告程序并评审、批准提供资源以支持测量活动的开展；

3） 在 ISMS 的检查和处置阶段，也应对测量措施加以改进，这就要求首先定义测量过程的评价准则，对测量过程加以监控，并定期实施评审。

6. ISO/IEC 27005

ISO/IEC 27005 信息安全风险管理给出了信息安全风险管理的指南，其中描述的技术遵循 ISO/IEC 27001 中的通用概念、模型和过程。

该标准介绍了一般性的风险管理过程，并重点阐述了风险评估的几个重要环节，包括风险评估、风险处理、风险接受等。在标准的附录中，给出了资产、影响、脆弱性以及风险评估的方法，并列出了常见的威胁和脆弱性。最后还给出了根据不同通信系统以及不同安全问题和威胁选择控制措施的方法。

7. ISO/IEC 27006

ISO/IEC 27006 信息安全管理体系认证机构的要求认可的主要内容是对从事 ISMS 认证的机构提出了要求和规范，或者说它规定了一个机构“具备怎样的条件就可以从事 ISMS 认证业务”。

8. ISO/IEC 27007

ISO/IEC 27007 信息安全管理体系审核指南为有认证资格的组织按照 ISO/IEC 27001 和 ISO/IEC 27002 来审核待认证的企业的 ISMS。该标准主要参考 ISO/IEC 19001:2002 质量和环境管理体系审核指南。所有“管理体系”基本都是相通的，ISO/IEC 27007 强调了 ISMS 的特殊之处。

9. ISO/IEC 27008

ISO/IEC 27008 是关于技术类控制的审核部分，为审核员提供了控制措施的审核指南。

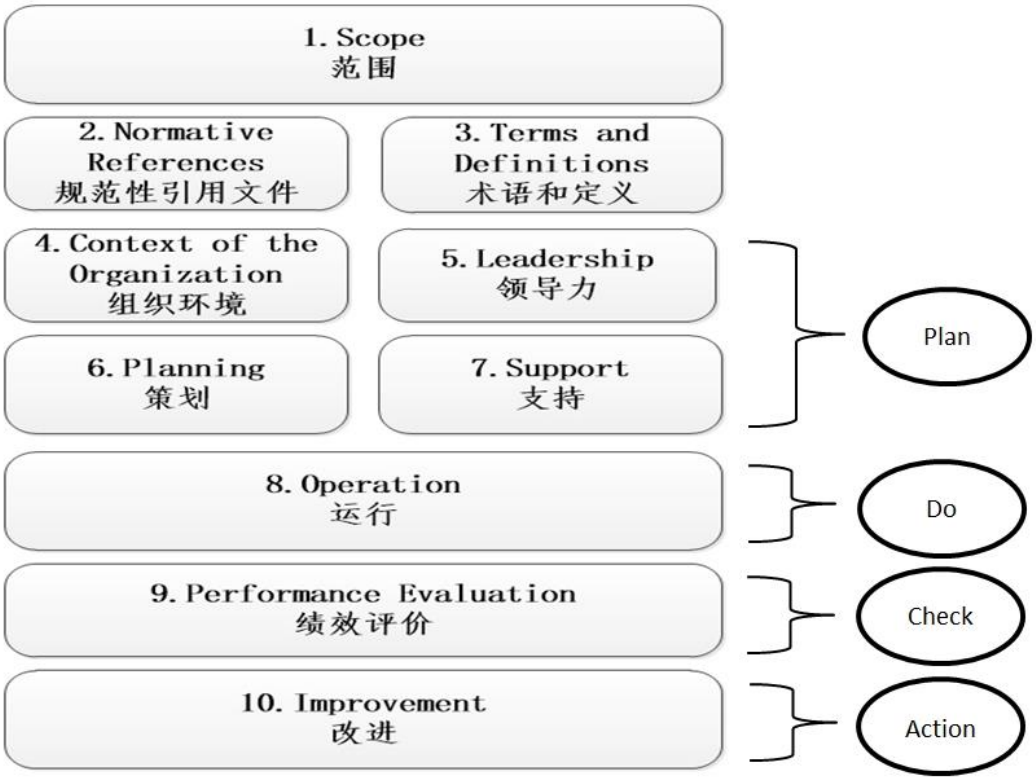
1.3. ISO/IEC 27001:2013 版概述

1.3.1. 标准的基本架构

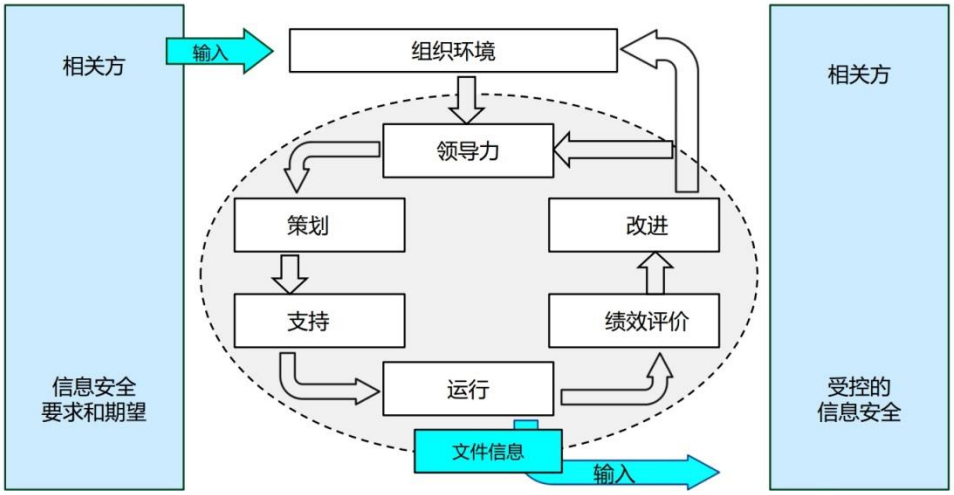
ISO/IEC 27001:2013 采用了 ISO Guide 83 的通用架构，该导则对管理体系标准在架构、格式、通用短语和定义方面进行了统一，同时也是 ISO 组织未来所有管理制度制定时的重要依据。此通用架构将确保今后编制或修订管理体系标准的持续性、整合性和简单化，这也将使标准更易读、易懂，有利于不同管理体系间进行接轨、整合。

第一个采用导则 83 的标准是 2013 年年 5 月发布的业务连续管理体系标准——ISO 22301:2012。预计已颁布的标准如 ISO9000/ ISO20000 未来的改版也将采用了 ISO Guide 83 的通用架构。

下图为 ISO Guide 83 的通用架构。



从目录结构上不难看出，标准不再对 PDCA 模型进行大段描述，而是将其思想方法融汇到标准的架构中。下图为 ISO/IEC 27001:2013 的基本架构。



1.3.2. 标准正文内容简介

该标准第 1-3 章主要阐明了该标准的适用范围、引用的文件及术语和定义。

第 4 章属于 Plan 阶段的一个组成部分。该章节介绍了建立适用于组织信息安全管理环境的必要要求，包括需求、要求与范围。涉及了解组织现状及背景、明确建立信息安全管理体系的目的、理解相关方的需求与期望、确定信息安全管理体系范围。

第 5 章属于 Plan 阶段的一个组成部分。该章节总结了最高管理层在信息安全管理体系中承担角色的具体要求，以及如何通过一份声明的策略来向组织传达领导层的期望。涉及了领导力和承诺、信息安全方针目标，以及角色、职责和承诺。

第 6 章属于 Plan 阶段的一个组成部分。该章节介绍了处理风险和机遇的行动，以及可实现的信息安全目标与实现计划。涉及了信息安全风险评估、风险所有者、信息安全风险处置、适用性声明、信息安全目标。

第 7 章属于 Plan 阶段的一个组成部分。该章节详细叙述了建立、实施、保持和改进一个有效的信息安全管理体系所需要的支持。包括:资源要求、参与人员的能力、意识、与利益相关方沟通、文档化信息。

第 8 章属于 Do 阶段的一个组成部分。该章节描述了组织信息安全体系实施中的必要过程，涉及运行计划及控制、信息安全风险评估、信息安全风险处置。

第 9 章属于 Check 阶段的一个组成部分。该章节总结了度量 ISMS 执行、ISMS 与国际标准及管理层期望的符合性、寻求管理层期望反馈的要求，涉及监控、度量、分析和评价，内部审核，管理评审。

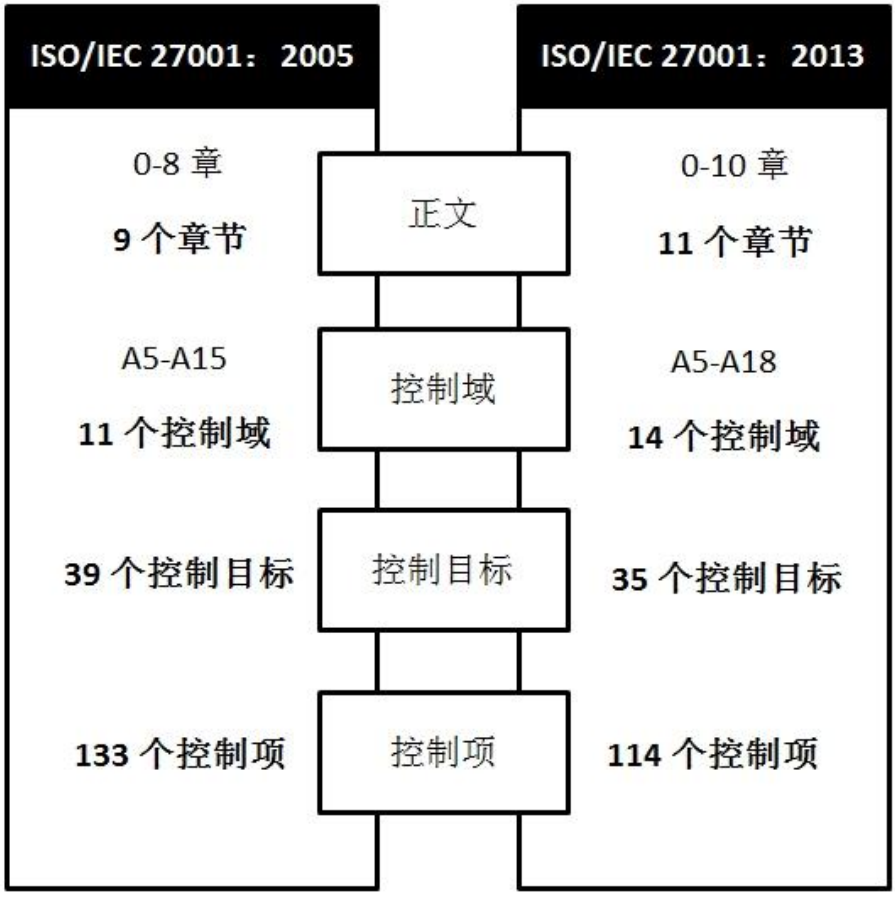
第 10 章属于 Action 阶段的一个组成部分。该章节描述了组织应通过纠正行动来识别和改进不符合项，涉及不符合项不纠正措施、持续改进。

1.4. ISO/IEC 27001:2013 版变化

1.4.1. 整体变化

ISO27001:2013 版对标准架构进行了大幅修改，以适应未来管理体系标准中使用的新的架构，简化与其他管理体系的整合。标准新版删除了旧版中重复、不适用的内容，结构上更清晰，内容上更精炼，逻辑上更严谨，并且在管理要求的定义上变得更具弹性，给予组织更灵活的实施空间。

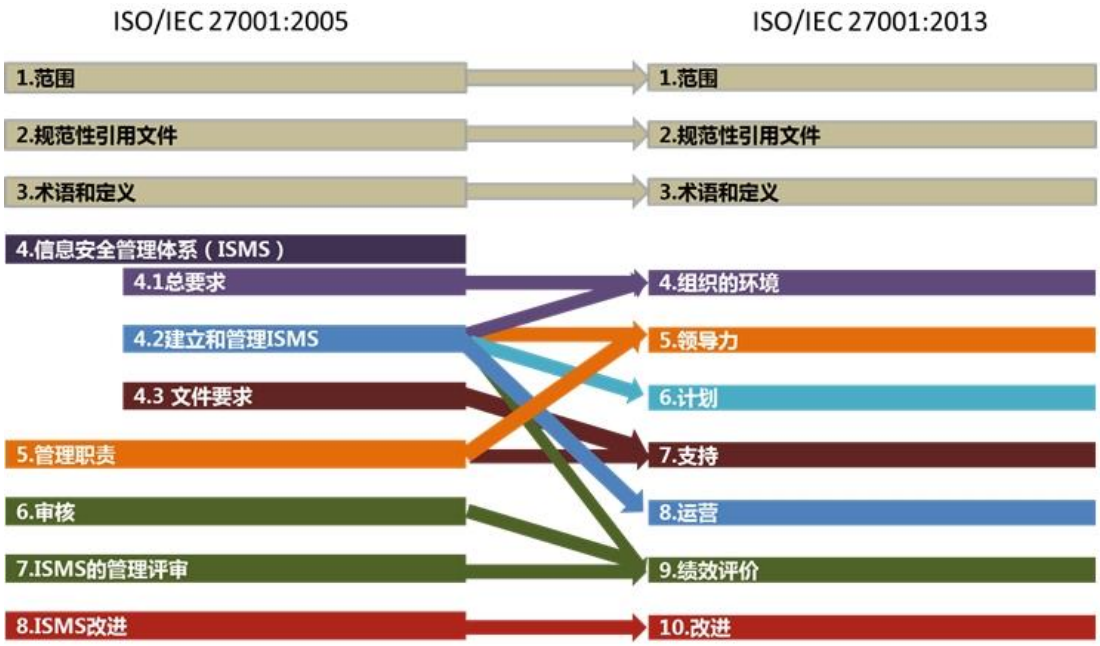
2005 版原本有 11 个控制域、133 个控制项，2013 标准调整为 14 个控制域、114 个控制项。控制项变化:增加了 11 个控制项、删除了 20 个控制项、合并移动减少 10 个控制项，总计减少了 19 个控制项。



1.4.2. 正文部分的变化

1.4.2.1. 正文部分架构的变化

ISO27001:2013 版对正文的架构进行了调整，采用了 ISO Guide 83 的通用架构，采用此架构的好处在于可将各标准的要求，以统一的架构进行描述。Annex SL 架构考虑了管理体系间的兼容性，有利于不同管理体系间进行接轨、整合。变化的调整详见下图。



1.4.2.2. PDCA 的融合

在 ISO27001:2005 版中，标准在正文部分中对 PDCA 模型进行了大幅描述，在 ISO27001:2013 版中，标准删除了对 PDCA 的描述内容，取而代之的是正文 10.2 中的一句“持续改进”。但从标准编写的目录结构上看，2013 版正文内容调整为策划—支持—运行—绩效评价—改进，架构上其实已经融入了 PDCA 思想。如图——。

1.4.2.3. 风险评估的变化

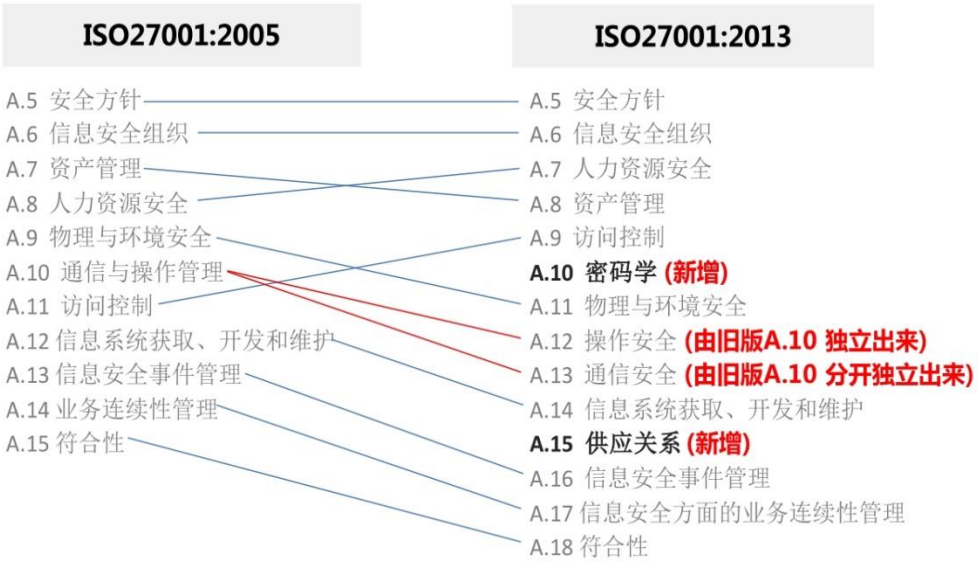
新版简化了对风险识别、风险分析的要求的描述，不再强调对资产责任人、威胁、脆弱性等进行识别，这意味着组织可选用的风险评估的方法可以更加宽泛和灵活。组织可以根据自身的情况，选用简化的风险评估方法，或继续使用现行的方法。

1.4.3. 附录 A 内容变化

1.4.3.1. 附录 A 变化变化概述

在控制域结构上，ISO27001:2013 版将密码学和供应关系列成两个单独的控制域，并将旧版的通信与操作管理拆分为操作安全和通信安全两个控制域，详见下图。

在控制措施的设置上，ISO27001:2013 保留了多数老的控制项，但对旧版中相近或类似的项进行了整合，删除了部分过时的或太过于具体的控制措施，并针对这几年信息技术的发展，将移动设备管理列入了控制项。



1.4.3.2. 新增的控制措施

ISO/IEC 27001:2013 较 2005 版新增了 11 个控制措施，新增的控制措施如下:

注:由于对应国标暂未出台，尚无官方的中文翻译，以下译文仅作参考。

1) A.6.1.5 Information security in project management 项目管理中的信息安全

【描述】

Information security shall be addressed in project management, regardless of the type of the project.

【参考译文】

实施任何项目应考虑信息安全的相关要求。

【说明】

该控制项加强了对项目中的安全管理。

2) A.12.6.2 Restrictions on software installation 限制软件安装

【描述】

Rules governing the installation of software by users shall be established and implemented.

【参考译文】

应建立和实施用户软件安装的规则。

【说明】

该控制项意在加强对版权和技术漏洞的控制。

3) A.14.2.1 Secure development policy 安全的开发策略

【描述】

Rules for the development of software and systems shall be established and applied to developments within the organization.

【参考译文】

应建立组织内部的软件和系统的开发准则。

【说明】

该控制项加强了信息系统生命周期中的安全开发策略。

4) A.14.2.5 Secure system engineering principles 安全系统工程原则

【描述】

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development efforts.

【参考译文】

应建立、记录、维护和应用安全系统工程原则，并应用于任何信息系统工程。

【说明】

该控制项加强了信息系统生命周期中的程序与流程。

5) A.14.2.6 Secure development environment 开发环境安全

【描述】

Organizations shall establish and appropriately protect secure development environment for system development and integration efforts that cover the entire system development lifecycle.

【参考译文】

在整个系统开发生命周期的系统开发和集成工作中，应建立并适当保护开发环境的安全。

【说明】

该控制项加强了信息系统生命周期中的开发环境安全。

6) A.14.2.8 System security testing 系统安全测试

【描述】

Testing of security functionality shall be carried out during development.

【参考译文】

在开发过程中，应进行安全性测试。

【说明】

该控制项加强了信息系统生命周期中的系统安全性。

7) A.15.1.1 Information security policy for supplier relationships 供应商关系的信息安全策略

【描述】

Information security requirements for mitigating the risks associated with supplier access to organization’s assets shall be documented.

【参考译文】

为降低供应商使用组织资产所带来的风险，应与供应商签署包含安全要求的协议。

【说明】

此项控制措施加强了对供应商的管理要求。

8) A.15.1.3 Information and communication technology supply chain 信息和通信技术的供应链

【描述】

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

【参考译文】

供应商协议应包括信息、通信技术服务和铲平供应链的相关信息安全要求。

【说明】

此项控制措施提出了供应链的概念，加强了对供应链中断的风险控制。

9) A.16.1.4 Assessment and decision on information security events 评估和决策信息安全事件

【描述】

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

【参考译文】

应评估信息安全事态，以决定是否将其认定为信息安全事件。

【说明】

信息安全事件处理中增加了评估程序。

10) A.16.1.5 Response to information security incidents 信息安全事件的响应

【描述】

Information security incidents shall be responded to in accordance with the documented procedures.

【参考译文】

应按照文件化的程序响应信息安全事件。

【说明】

强调安全事件响应的规范性、程序化。

11) A.17.2.1 Availability of information processing facilities 信息处理设施的可用性

【描述】

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

【参考译文】

信息处理设施应具备足够的冗余以满足可用性要求。

【说明】

加强可用性管理，完善原 BCM 管理的生命周期。

1.4.3.3. 删除的控制措施

ISO/IEC 27001:2013 较 2005 版删减了 20 项控制措施，删减的控制措施如下:

编号	控制措施	删除原因
A.6.1.1	信息安全的管理承诺	在新版正文管理层承诺中已包含其内容
A.6.1.2	信息安全协调	新版正文中已包含其内容
A.6.1.4	信息处理设施的授权过程	已在新版 A.8.1.3 资产的合理使用中涵盖
A.6.2.1	与外部各方相关风险的识别	在新版正文风险评估与处理中已涵盖
A.6.2.2	处理与客户有关的安全问题	在新版正文风险评估与处理中已涵盖

编号	控制措施	删除原因
A.10.7.4	系统文件安全	系统文件也属于信息资产，相关要求已包含在其他控制项中
A.10.8.5	业务信息系统	相关要求已包含在其他控制项中
A.11.4.2	外部连接的用户鉴别	要求太过具体，已在新版 A.9 中涵盖
A.11.4.3	网络上的设备标识	要求太过具体，已在新版 A.13.1.3 中涵盖
A.11.4.4	远程诊断和配置端口的保护	要求太过具体，已在新版 A.13.1.3 中涵盖
A.11.4.6	网络连接控制	要求太过具体，已在新版 A.13.1.3 中涵盖
A.11.4.7	网络路由控制	要求太过具体，已在新版 A.13.1.3 中涵盖
A.11.6.2	敏感系统隔离	部分要求已在新版 A.13.1.3 网络隔离中涵盖，其他相关要求由物理安全等体现
A.12.2.1	输入数据确认	要求太过具体，已在新版 A.14.2.5 安全系统工程原则中涵盖
A.12.2.2	内部处理的控制	要求太过具体，已在新版 A.14.2.5 安全系统工程原则中涵盖
A.12.2.3	消息完整性	要求太过具体，已在新版 A.14.2.5 安全系统工程原则中涵盖
A.12.2.4	输出数据确认	要求太过具体，已在新版 A.14.2.5 安全系统工程原则中涵盖
A.12.5.4	信息泄露	相关要求已包含在其他控制项中
A.15.1.5	防止滥用信息处理设施	相关要求已包含在其他控制项中
A.15.3.2	信息系统审计工具的保护	审计工具作为软件资产的一种，已受访问控制及其他措施的管控

1.4.3.4. 合并的控制措施

ISO/IEC 27001:2005	ISO/IEC 27001:2013	合并原因
A.6.1.3 信息安全职责的分配 A.8.1.1 角色和职责	A.6.1.1 信息安全的角色和职责	两者存在冗余
A.11.2.1 用户的注册 A.11.5.2 用户的标识和鉴别	A.9.2.1 用户的注册和注消	两者存在冗余
A.11.5.1 安全登陆规程 A.11.5.5 会话超时 A.11.5.6 联机时间的限定	A.9.4.2 安全登陆程序	要求太过具体，进行提炼合并
A.10.4.1 恶意代码控制 A.10.4.2 控制移动代码	A.12.2.1 控制恶意软件	两者存在冗余
A.10.10.1 审计记录 A.10.10.2 监视系统的使用 A.10.10.5 日志信息的保护	A.12.4.1 事件日志	三者存在冗余
A.10.10.3 管理员和操作员日志 A.10.10.4 故障日志	A.12.4.3 管理员和操作者日志	两者存在冗余

ISO/IEC 27001:2005	ISO/IEC 27001:2013	合并原因
A.10.9.1 电子商务 A.10.9.3 公共可用信息	A.14.1.2 公共网络应用服务的安全	两者存在冗余，电子商务也是公共网络应用服务的一种
A.14.1.1 在业务连续性管理过程中包含信息安全 A.14.1.3 制定和实施包含信息安全的业务连续性计划 A.14.1.4 测试、维护和再评估业务连续性计划	A.17.1.2 实施信息安全的连续性	三者存在冗余

2. ISO/IEC 27001:2013 版标准解析

2.1. 概述

ISO/IEC 27001:2013 由引言、正文及附录三个部分组成。

1. 引言部分

ISO/IEC 27001:2013 的引言包括两部分:0.1 总则和 0.2 与其他管理体系的兼容性。

0.1 总则描述了制定 ISO/IEC 27001:2013 的用途、信息安全管理体系的组成及应用对象。

0.2 与其他管理体系的兼容性则解释该标准采用标准化 ISO Annex SL 通用架构，对于与其他管理体系兼容的的好处。

2. 正文部分

ISO/IEC 27001:2013 的正文分为 10 章，分别为:

1) 范围；
2) 引用标准；
3) 术语与定义；
4) 组织环境；
5) 领导力；
6) 策划；
7) 支持；
8) 实施；
9) 绩效评价；
10) 改进。

3. 附录部分

ISO/IEC 27001:2013 的附录命名为附录 A，附录 A 为规范性附录，列出了实施 ISMS 的控制目标和控制措施，与正文部分内容一样，在附录 A 中选择控制目标和控制措施是规定的 ISMS 过程的一部分。

2.2. 引言

2.2.1. 总则

【参考译文/原文】

本国际标准为组织建立、实施、维护和持续改进信息安全管理体系(ISMS)提出相关要求。采用 ISMS 是组织的一项战略决策。组织 ISMS 的设计和实施受组织的战略决策、组织需求、目标、安全需求以及工作流程和组织规模等因素的影响。上述因素会随着时间不断发生变化。

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

信息安全管理体系通过实施风险管理过程来保护组织信息的保密性、完整性和可用性，对风险进行充分的管理并为相关方带来信心。

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

信息安全管理体系是组织整体管理架构和管理流程的组成部分。组织在进行流程、信息系统、控制措施设计过程中均应考虑信息安全。

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

本国际标准可以用于内部或外部机构用于对组织的信息安全管理能力进行评估以确认其是否满足组织自身的信息安全需求。

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

本标准附录中列举的控制措施的先后顺序不代表其重要程度或实施的先后顺序要求。列表编号顺序只做参考用途。

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 描述了信息安全管理体系的综述和术语，参考了信息安全管理体系标准族(包括 ISO/IEC 27003W, ISO/IEC 27004[3]和 ISO/IEC 27005[4])的相关名词解释和定义 。	ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

【内容解析】

本标准给出了信息安全管理体系的基本要求，为信息安全管理体系的建立、实施、运行和保持改进提供了有效的参考。采用信息安全管理体系应是组织的一项战略决策。

信息安全管理的本质是风险管理，组织可以通过信息安全管理体系的建设来保护组织信息的保密性、完整性、可用性，并对相关风险进行有效的管控。信息安全管理体系应建立在组织的管理架构和管理流程之上，脱离了组织的经营宗旨和经营环境谈信息安全是没有意义的。

信息安全的建设是一个系统工程，它需求对信息的各个处理环节进行统一的综合考虑、规划和构架，并要时时兼顾组织内外环境的不断变化，任何环节上的缺陷都会对企业信息安全构成威胁。在这里我们可以引用管理学上的木桶原理加以说明。木桶原理指的是:一个木桶由许多块木板组成，如果组成木桶的这些木板长短不一，那么木桶的最大容量不取决于长的木板，而取决于最短的那块木板。这个原理同样适用信息安全。一个组织的信息安全水平将由与信息安全有关的所有环节中最薄弱的环节决定。信息从产生到销毁的生命周期过程中包括了产生、收集、加工、交换、存储、检索、存档、销毁等多个事件，表现形式和载体会发生各种变化，这些环节中的任何一个都可能影响整体信息安全水平。要实现信息安全目标，一个组织必须使构成安全防范体系这只“木桶”的所有木板都要达到一定的长度。

2.2.2. 与其他管理体系的兼容性

【参考译文/原文】

本国际标准采用了标准化的 ISO Annex SL 通用架构，采用此架构的好处在于将各标准的要求以统一的架构进行描述。保持了与其他管理体系的兼容性，有利于不同管理体系进行接轨和整合。	This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

【内容解析】

为满足持续业务运营的要求，组织可能将管理体系方法论用于多个领域的管理，包括以产品和服务质量满足要求为核心目的的质量管理体系、以污染物的产生和排放满足环境管理要求为核心的环境管理体系，以及以信息资产的安全满足要求为核心的信息安全管理体系。

越来越多的组织会选择其中几个甚至全部在组织内应用，显然，让各个体系自行其是是

不现实的。因此，管理体系的整合已经成为大势所趋。

ISO/IEC 27001:2013 采用了 ISO Annex SL 通用架构，该架构对标准的结构、格式、通用短与和定义方面进行了统一。这将确保今后编制或修订管理体系标准的持续性和易整合性。

以融合管理体系要求的方式设计信息安全管理体系的另一个好处，可以使实施和维护管理体系所需的资源得到最有效率的适用，从而在一定程度上减少因运行不同管理体系造成的机构重叠和管理官僚化，也可减少业务过程中的执行人员不得不分别理解不同管理体系要求带来的混乱。

2.3. 范围

【参考译文/原文】

本国际标准规定了在组织内部建立、实施、维护和持续改进信息安全管理体系的要求。本国际标准还包括了组织进行评估和处置信息安全风险的要求。在本国际标准中规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织宣布符合本国际标准，对于 4 到 10 章节的任何条款的删减是不可接受的。	This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

【内容解析】

本条款中申明了标准是通用的，适用于各种类型的组织。

本标准所提出的架构是高度概括和通用的，并不针对具体的行业，因此标准指出，4 到 10 章的内容不能删减。也就是说，采用 ISMS 的组织只能删减附录 A 的内容，即建立整个管理框架的方法是不能删减的，能删减的只是具体的控制措施。

对于附录 A 的删减原则是:

1. 满足组织风险接受的准则；
2. 满足法律法规要求；
3. 删减必须是合理的，且能够证明；
4. 必须提供证据，证明相关责任人员可以接受相关风险。

需要注意的是:ISO/IEC 27001:2013 对需要采用标准的组织而言，是最基本的要求。组织所建立的 ISMS 可超出标准的要求，但不能低于标准的所有要求，删减要满足规定的前提。

2.4. 规范性引用文件

【参考译文/原文】

下面是本标准的规范性引	用文件。凡注明日期的引用文件，仅该引用的版本适用。没

有注明日期的引用文件，则引用文件的最新版本(包括任何修订后的版本)适用。 The following documents, in whole or in part, are ISO/IEC 27000，信息技术-安全技术-信息安全管理体系概述和术语	normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies.For undated references, the latest edition of the referenced document (including any amendments) applies. ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

【内容解析】

本条款明确了该标准引用的标准是 ISO/IEC 27000，

需要注意的是，凡注明日期的引用文件，仅该引用的版本适用。

2.5.术语和定义

【参考译文/原文】

ISO/IEC 27000 中的术语与定义适用于本标准。	For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

注:以下术语和定义均来自 27000,保留了原先顺序。

2.5.1. 访问控制 access control

确保在业务和安全要求的基础上对**资产**(4.5.3)的访问被授权和限制

【内容解析】

访问控制是按照用户身份及其所归属的某项定义组来限制用户对资产的访问，或限制其对资产的的使用。访问控制通常用于系统控制、物理控制等多个领域。

2.5.2. 可核查性 accountability

对一个实体的行为和决定负责

【内容解析】

此处可核查性通常含有可问责的含义，如标准 A.9.3 中对认证信息的保护负责。

2.5.3. 资产 asset

任何对组织有价值的东西

【内容解析】

1.对于资产的定义比较含糊，或者说比较宽泛。任何有价值的东西都以资产来论述，组织的东西就分为两类:资产和垃圾。就“资产”和“**信息资产**”(4.5.18)来说，后者显然是前者的子集。资产可以分为以下几种:

a） 信息，例如:文档和数据等；

b） 软件，例如:电脑程序等；

c） 硬件，例如:存储设备、网络设备等；

d） 服务，例如:IT 服务等

e） 人力资源，包:括人的资格、经验、能力等；

f） 无形资产:例如声誉和形象等。

2.根据资产拥有者的情况，资产拥有者可以是组织，也可以是个人。

2.5.4. 攻击 attack

试图摧毁、暴露、涂改、禁用、窃取或非法访问未经授权使用的**资产**(4.5.3)

【内容解析】

任何对资产的未授权访问或使用都视为攻击。

2.5.5. 认证 authentication

确保对某个实体特征描述正确性的证据

【内容解析】

认证是确认用户为实体的授权者的过程，认证可以基于以下一个或多个因素:

1.根据你所知道的信息来证明你的身份 (what you know，你知道什么)；假设某些信息只有你本人知道，如暗号、密码等，通过询问这个信息就可以确认你的身份；

2.根据你所拥有的东西来证明你的身份 (what you have，你有什么)；假设某一件东西只有你本人拥有，如 IC 卡、 USB Key 、单位数字证书等，通过出示这个东西也可以确认你的身份；

3.根据独一无二的身体特征来证明你的身份 (who you are，你是谁)，比如指纹、面貌等。

2.5.6. 真实性 authenticity

验证一个实体是其所声称的所得结果中的一种属性

【内容解析】

此处真实性一般指认证信息的真实性、可靠性。

2.5.7. 可用性 availability

根据授权实体的要求可访问或可利用的特性

【内容解析】

可用性的目的是让所有合法用户能够使用到已授权的信息和功能。可用性通常用百分率表示，公式为:{(规定服务时间-因意外中断服务时间)/规定服务时间}X100%。例如:99.9%。

其与保密性和完整性并成为信息安全 CIA 三要素。

2.5.8. 业务连续性 business continuity

确保业务持续运行的**程序**(4.5.30)或**过程**(4.5.31)

【内容解析】

业务连续性是指企业有应对风险、自动调整和快速反应的能力，以保证企业业务的连续运转。为企业重要应用和流程提供业务连续性应该包括以下三个方面。

1.高可用性(High availability)。它是指提供在本地故障情况下，能继续访问应用的能力。无论这个故障是业务流程、物理设施，还是 IT 软硬件故障。

2.连续操作(Continuous operations)。 它是指当所有设备无故障时保持业务连续运行的能力。用户不需要仅仅因为正常的备份或维护而需要停止应用的能力。

3.灾难恢复(Disaster Recovery)。它是指当灾难破坏生产中心时，在不同的地点恢复数据的能力。

同时，上述三个部分不是相互孤立的，是相互关联，而且有交叉的。

2.5.9. 保密性 confidentiality

信息不能被未授权的个人、实体或者**过程**(4.5.31)利用或知悉的特性

【内容解析】

保密性强调信息只为授权用户使用的特征。保密性是在可靠性和可用性的基础之上，保障信息安全的重要手段。常用的保密技术：

1)物理保密:利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露。

2)防窃听:使对手侦察、接收不到有用的信息。

3)防辐射:防止有用的信息以各种途径辐射出去。

4:信息加密:在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息也会因为没密钥而无法读懂有效信息。

2.5.10. 控制措施 control

在行政、技术、管理和法律的管理**风险**(4.5.34)的方法，包括**方针**(4.5.28)，**程序**(4.5.30)，**指南**(4.5.16)，实践或组织结构

【内容解析】

控制是指控制主体按照给定的条件和目标，对控制客体施加影响的过程和行为。控制也常视为保护和对策的同义词。

2.5.11. 控制目标 control objective

声明中描述的**控制措施**(4.5.10)所要实现的目标

【内容解析】

控制目标在附录 A 中得以体现，ISO/IEC 27001:2013 中有 35 个控制目标。

2.5.12. 纠正措施 corrective action [ISO 9000:2005]

为消除已发现的不符合或其他不期望情况的原因所采取的措施

【内容解析】

纠正措施和**预防措施**(4.5.29)的区别在于：采取纠正措施是为了防止再发生，而采取预防措施是为了防止发生。

2.5.13. 有效性 effectiveness

完成策划的活动并得到策划的结果的程度

【内容解析】

在信息安全管理体系中，有效性通常指信息安全目标达成的程度，通过信息安全管理体系有效性测量准确的衡量 ISMS 的绩效，而且还能够为管理层对信息安全管理的资源投入提供数据依据。

2.5.14. 效率 efficiency

得到的结果与所使用的资源之间的关系

2.5.15. 事态 event

特定情况的发生

【内容解析】

1. 事态可能是确定的，也可能是不确定的。
2. 事态可能是单一的，也可能是系列的。

3. 对于给定时间内事态发生的概率可以估算出来。

2.5.16. 指南 guideline

为达成制定控制目标所给出的建议

【内容解析】

指南阐明应该做什么河怎么做以达到策略中所制定的控制目标。

2.5.17. 影响 impact

对实现业务目标产生的不利变化

2.5.18. 信息资产 information asset

对组织有价值的知识或数据

【内容解析】

一般信息资产按其形式的不同分为五大类：数据资产、实物资产、软件资产、人员资产和服务资产

2.5.19. 信息安全 information security

保持信息的**保密性**(4.5.9)，**完整性**(4.5.25)，**可用性**(4.5.7)；另外也可以包括诸如**真实性**(4.5.6)，**可核查性**(4.5.2)，**不可否认性**(4.5.27)和**可靠性**(4.5.33)等

【内容解析】

关于信息安全的详细解释参见本教材第一章。

2.5.20. 信息安全事态 information security event

信息安全事态是指系统、服务或网络的一种可识别的状态的发生，他可能是对**信息安全**(4.5.19)**方针**(4.5.28)的违反或**控制措施**(4.5.10)的失败，或是和安全关联的一个先前未知的状态

【内容解析】

1. 有害或意外的信息安全事态是引发信息安全事件的源头。
2. 信息安全事态发生后可能造成信息安全事件，也可能未造成信息安全事件。
3. 信息安全事态可能由一个原因导致，也可能由多个原因导致。

2.5.21. 信息安全事件 information security incident

一个信息安全事件由单个的或者一系列的有害或意外信息安全事态(4.5.20)组成，它们具有损害业务运作和威胁信息安(4.5.19)的极大的可能性

【内容解析】

1. 一个或多个有害的或者意外信息安全事态是导致信息安全事件的源头。
2. 事件发生后，根据事件的影响程度，可分为一般事件和重大事件。根据信息安全事件的影响程度，对信息安全事件做出最恰当和最有效的响应。
3. 尽管信息安全事态可能是意外或违故意违反信息安全控制措施的企图的结果，但在多数情况下，信息安全事态本身并不意味着破坏信息安全的企图真正获得了成功，因此也并不一定会对保密性、完整性和/或可用性产生影响。也就是说，并非所有信息安全事态都会被归类为信息安全事件。

2.5.22. 信息安全事件管理 information security incident management

从**信息安全事件**(4.5.21)中检测、报告、评估、响应、处理和学习的**过程**(4.5.31)

【内容解析】

关于信息安全事件管理的标准，详见 ISO/IEC 27035。

2.5.23. 信息安全管理体系 information security management system

整个管理体系(4.5.26)的一部分。它是基于业务风险方法来建立、实施、运行、监视、评审、保持和改进信息安全(4.5.19)的。

【内容解析】

1. 信息安全管理体系是组织管理体系的一个组成部分。其目的是为了保护组织的信息安全。
2. 信息安全管理体系应基于整体业务活动风险。
3. 信息安全管理体系与其他管理体系一样，采用过程方法，PDCA 模型。支持与管理标准一致的、协调的实施和运行。

2.5.24. 信息安全风险 information security risk

威胁(4.5.45)利用一项或多项**资产**(4.5.3)的**脆弱性**(4.5.46)，并由此对组织造成损害或破坏的可能性

【内容解析】

在信息安全领域，风险就是指信息资产遭受损坏并给企业带来负面影响的潜在可能性。

2.5.25. 完整性 integrity

保护**资产**(4.5.3)准确和完整的特性

【内容解析】

完整性指的是防止未授权的更改和篡改。包含非授权的增加、减少或破坏。例如：在原有代码中非授权加入代码，或者在原有代码中非授权裁剪或非授权修改了一部分代码，均视为破坏完整性的行为。

2.5.26. 管理体系 management system

实现组织控制目标的方针(4.5.28)、程序(4.5.30)、指南(4.5.16)和相关资源的框架

【内容解析】

1. 管理体系包括组织结构、方针策略、规划活动、指责、实践、程序、过程和资源。
2. 一个组织的管理体系可以包括若干个不同的管理体系，如质量管理体系、财务管理体系、信息安全管理体系等。

2.5.27. 不可否认性 non-repudiation

证明声称的事件的发生和发起实体的特性

【内容解析】

不可否认性是通过对授权主体的控制，实现对保密性、完整性和可用性的有效补充，主要强调对授权用户行为进行监督和审查。

2.5.28. 方针 policy

由组织最高管理者正式发布的关于信息安全方面的全部宗旨和方向。

【内容解析】

1. 方针应由管理者制定，最高管理者批准、发布并传达给所有员工和外部相关方。

2. 方针必须体现管理者的意图。
3. 方针不应该经常变化，组织应按计划的时间间隔或当重大变化发生时进行方针的评审。

2.5.29. 预防措施 preventive action [ISO 9000:2005]

为消除潜在的不符合或其他潜在不期望情况的原因所采取的措施

【内容解析】

1. 一个潜在的不符合可以有若干的原因。
2. **纠正措施**(4.5.12)和预防措施的区别在于：采取预防措施是为了防止发生，而采取纠正措施是为了防止再发生。

2.5.30. 程序 procedure [ISO 9000:2005]

为进行某项活动或过程(4.5.31)所规定的途径

【内容解析】

1. 程序可以形成文件，也可以不形成文件。
2. 当程序形成文件时，通常称为“书面程序”或“形成文件的程序”。含有程序的文件可称为“程序文件”。

2.5.31. 过程 process [ISO 9000:2005]

将输入转化为输出的互相关联或互相作用的一组活动

【内容解析】

一个过程的输入通常是其他过程的输出。

2.5.32. 记录 record [ISO 9000:2005]

阐明所取得的结果或提供所完成活动的证据的文件

【内容解析】

记录可用于文件的可追溯性活动，并为验证、预防措施、纠正措施提供证据。

2.5.33. 可靠性 reliability

与事先规划的行为或结果一致的特性

【内容解析】

信息的可靠性指当信息没有重要错误或偏向，并且能够如实反映其拟反映或该反映的情况供使用者作依据。

2.5.34. 风险 risk [ISO/IEC Guide 73:2002]

某一**事件**(4.5.15)发生的概率和其后果的组合

【内容解析】

1. 风险有两个重要的方面：事件的概率和事件的结果，或者说是事件发生的可能程度和事件发生后的最终后果。
2. 风险在不同的应用领域，可能有不同的计算方法，但是概率和结果是其考虑的主要因素。

2.5.35. 风险接受 risk acceptance [ISO/IEC Guide 73:2002]

接受风险(4.5.34)的决定

【内容解析】

组织确定风险程度可接受的决定。在明显满足组织方针策略和接受风险的准则的条件下，有意识地、客观地接受风险。

2.5.36. 风险分析 risk analysis [ISO/IEC Guide 73:2002]

系统地使用信息来识别风险来源和估计风险

【内容解析】

1. 风险识别的目的是决定什么发生可能会造成潜在损失，并深入了解损失可能如何、何地、为什么发生。
2. 风险识别包括：威胁识别、脆弱性识别、后果识别和现有控制措施的识别。
   a) 威胁识别：威胁有可能损害资产，诸如信息、过程、系统甚至组织。威胁的来源可能是自然的或认为的，可能是意外的或是故意的。也可能来自组织内部或外部。所以对整体并按类型(如未授权行为，物理损害，技术故障)识别威胁意味着没有威胁被忽视，包括突发的威胁。
   b) 脆弱性识别：脆弱性本身不会产生危害，只有被某个威胁利用时才会产生危害。没有相应威胁的脆弱性可能不需要实施控制措施，但是应关注和监视其变化。
   c) 后果识别：后果可能是丧失有效性、不利运行条件、业务损失、声誉破坏等。资产受到损害后，后果可能是面临性的，也可能是永久的。
   d) 现有控制措施识别：为避免不必要的工作或成本，如：重复的控制措施。此外，识别现有的控制措施时，进行检查以确保控制措施
3. 在考虑丧失资产的保密性、完整性和可用性所造成的后果的情况下，评估安全失效可能造成对组织的影响。
4. 根据主要的威胁和脆弱性、对资产的影响以及当前实施的控制措施，评估安全失效发生的现实可能性。

2.5.37. 风险评估 risk assessment

风险分析(4.5.36)和**风险评价**(4.5.41)的整个**过程**(4.5.31)

【内容解析】

1. 对信息和信息处理设施的威胁、脆弱性和影响及三者发生的可能性的评估
2. 风险评估也就是确认安全风险及其大小的过程，即利用适当的风险评估工具，包括定性和定量的方法，确定资产风险等级和有限控制顺序。
3. 风险评估确定了信息资产的价值，对存在(或可能存在的)适用的威胁和脆弱性进行识别，考虑现有的控制措施及其对已识别风险的影响，确定潜在的后果。
4. 对确定的风险根据紧急度和影响度进行优先级排序，并按照确定的风险准则划分等级。

2.5.38. 风险沟通 risk communication [ISO/IEC Guide 73:2002]

决策者和其他利益相关者之间交换或分享关于**风险**(4.5.34)的信息

【内容解析】

这些风险的信息可能是风险的存在情况、自然特性、形态、概率、严重程度、可接受程度、处理措施及风险的其他方面。

2.5.39. 风险准则 risk criteria [ISO/IEC Guide 73:2002]

评价**风险**(4.5.34)严重性的依据

【内容解析】

风险准则包括相关的成本及收益、法律法规相关要求，社会经济及环境因素，利益相关者的态度，优先次序和在评估过程中的其他要素。

2.5.40. 风险估计 risk estimation [ISO/IEC Guide 73:2002]

对**风险**(4.5.34)的概率及后果进行赋值的过程

【内容解析】

风险估计可以考虑成本、收益、利益相关者的利害关系，以及其他各种用于风险评价的因素。

2.5.41. 风险评价 risk evaluation [ISO/IEC Guide 73:2002]

将估计后的**风险**(4.5.34)与给定的**风险准则**(4.5.39)对比，来决定风险严重性的**过程**(4.5.31)

【内容解析】

风险评价是综合考虑信息安全事件的影响和发生可能性而得出的风险的级别。确定风险是否可接受，通常将风险分为：不可接受风险、有条件可接受风险(需要关注)，可接受风险。

在需要时，根据建立的风险准则进行处理。

2.5.42. 风险管理 risk management [ISO/IEC Guide 73:2002]

指导和控制某一组织与**风险**(4.5.34)相关问题的协调

【内容解析】

1. 风险管理师以可以接受的方式识别、控制、降低或规避和转移可能影响信息系统的安全风险过。程。
2. 风险管理一般包括风险评估、风险处理、风险接受和风险沟通。
3. 通过风险评估来分析和评价风险。
4. 通过制定信息安全方针，采用适当的控制目标和控制方式对风险进行控制和降低。
5. 风险管理的目的是使风险被降低、规避、转移或降至一个可能接受的水平。

2.5.43. 风险处理 risk treatment [ISO/IEC Guide 73:2002]

选择及实施**风险**(4.5.34)应对措施的过程

【内容解析】

风险处理的有效性取决于风险评估结果。风险处理有可能不能立即达到一个可接受水平的残余风险，在这种情况下可能需要进行风险评估迭代，接下来做进一步的风险处置。

风险处置的四种方式：

1) 风险降低：为降低风险发生的可能性或不利后果所采取的行动。例如：采取纠正、消除、预防、影响最小化、威慑、检测、恢复、监视和意识培训等措施。
2) 风险规避：对新技术或不能控制风险的活动，不采用该活动的方式。例如：避免采用新技术等。
3) 风险转移：与另一方共享由风险带来的损失或收益。对于信息安全风险而言，风险转移不仅考虑不利的后果(损失)。例如：保险、供应商等。
4) 风险保留：也成“风险接受”，组织确定风险程度可接受的决定。在明显满足组织方针策略和接受风险的准则的条件下，有意识、客观地接受风险。

2.5.44. 适用性声明 statement of applicability risk treatment

描述与组织的信息安全管理体系相关的和适用的控制目标和控制措施的文档

【内容解析】

1. 适用性声明提供了一份关于风险处置决定的综述。证明不会因疏忽而遗漏控制措施。
2. 适用性声明包含当前实施的控制目标和控制措施。
3. 适用性声明是一个包含组织所选择的控制目标和控制措施的文件，以及选择的理由。如果对标准附录 A 中任何控制目标和控制措施的删减，应在适用性声明中说明删减的合理性。

2.5.45. 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

【内容解析】

详见第二章。

2.5.46. 脆弱性 vulnerability

可能会被一个或多个威胁所利用的资产或一组资产的弱点

【内容解析】

详见第二章。

2.6. 组织环境

2.6.1. 理解组织环境

【参考译文/原文】

组织应确定与其总体目标相关的内部和外部环境因素，相关因素将影响其实现信息安全管理体系的预期成果。 **注:**确定这些相关因素可参考 ISO 31000:2009 [5] 5.3 “环境的建立”。	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. **NOTE:** Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

【内容解析】

外部环境包括如下几个方面，但并不局限于此：

- 文化、政治、法律、规章、金融、技术、经济、自然环境以及竞争环境，无论是国际、国内、区域或地方；
- 影响组织目标的主要驱动因素和发展趋势；
- 外部利益相关者的观点和价值观。

内部环境包括如下几个方面，但并不局限于此：

- 资源与知识的理解能力（如：资本、时间、人力、流程、系统和技术）；
- 信息系统、信息流动以及决策过程（包括正式和非正式的）；
- 内部利益相关者；
- 政策，为实现的目标及战略；
- 观念、价值观、文化；
- 组织通过的标准以及参考模型；

- 结构（如：治理、角色、责任）。

2.6.2. 理解相关方的需求和期望

【参考译文/原文】

组织应确定： a) 与信息安全管理体系有关的相关方； b) 相关方的信息安全需求 。 注 ： 相关方的要求包括法律法规要求和合同规定的义务。	The organization shall determine: a) interested parties that are relevant to the information security management system; and b) the requirements of these interested parties relevant to information security. NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

【内容解析】

组织识别出相关方的需求和期望是非常重要的，相关方的需求和期望有两个主要来源：

a) **组织内部相关需求与期望。**包括但不限于：
   - 治理、组织结构、作用和责任；
   - 方针、目标，为实现方针和目标制定的战略；
   - 基于资源和知识理解的能力（如：资金、时间、人员、过程、系统和技术）；
   - 与内部利益相关方的关系，内部利益相关者的观点和价值观；
   - 组织的文化；
   - 信息系统、信息流和决策过程；
   - 组织所采用的标准、指南和模式；
   - 合同关系的形式与范围。
   - 支持组织运行的信息处理、加工、存储、沟通和存档的原则、目标和业务要求的特定集合。

b) **组织外部相关需求和期望。** 外部相关方（如贸易伙伴、承包方和服务提供者等）以组织所处的整体环境为基础，包括法律和监管要求、利益相关者的诉求和与具体风险管理过程相关的其他方面的信息等，包括但不限于：
   - 国际、国内、地区及当地的政治、经济、文化、法律、法规、技术、金融以及自然环境和竞争环境；
   - 影响组织目标实现的外部关键因素及其历史和变化趋势；
   - 外部利益相关者及其诉求、价值观、风险承受度；外部利益相关者与组织的关系等。

实施控制措施所用资源需要根据缺乏这些控制措施时由安全问题导致的业务损害加以平衡。

风险评估的结果将帮助指导和确定适当的管理措施、管理信息安全风险以及实现所选择的用以防范这些风险的控制措施的优先级。

2.6.3. 明确信息安全管理体系的范围

【参考译文/原文】

组织应明确信息安全管理体系的边界和适用性，以确定其范围。 确定范围时，组织应考虑： a) 与在4.1章节中有关的内部、外部问题； b) 与在 4.2 章节中提及的需求； c) 组织自身活动和与其他组织开展活动的接口和依赖关系； 范围的相关内容应形成文档。	The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1; b) the requirements referred to in 4.2; and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information.

【内容解析】

ISMS 范围应包括：

- 为内部或外部客户提供的(也是需要保护的)服务、信息系统、资产等。
- 实际的物理场所和对象信息(地理位置、部门等)。

2.6.4. 信息安全管理体系

【参考译文/原文】

组织应按照本国际标准要求建立、实施、维护和持续改进信息安全管理体系。	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

【内容解析】

本标准给出了信息安全管理体系的基本要求，为信息安全管理体系的建立、实施、维护和持续改进提供了一个有用的模型。本标准提出的信息安全管理体系要求框架，可以作为组织内部和外部信息安全管理一致性评估的依据，也就是说本标准可以作为第一方审核、第二方审核和第三方审核的依据。

2.7. 领导力

2.7.1. 领导和承诺

【参考译文/原文】

管理者应通过以下行动证明其实施了与信息安全管理体系有关的领导工作与承诺： a) 确保建立与组织战略目标一致的信息安全方针和信息安全目标； b) 确保信息安全管理体系要求集成到组织的管理流程； c) 确保提供信息安全管理体系需要的各项资源； d) 传达信息安全管理的重要性及信息安全管理体系要求； e) 确保信息安全管理体系实现其预期目标； f) 指导和支持信息安全团队； g) 促使持续改进； h) 支持其他相关的管理者在其职责范围内履行管理职责。	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b) ensuring the integration of the information security management system requirements into the organization's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

【内容解析】

建立、实施、保持和持续改进信息安全管理体系，应是组织出于业务运营的需要作出的一项战略决策。因此建立、实施、保持和持续改进信息安全管理体系首先需要管理者作出承诺。标准本条款提出了管理者应做出的承诺，并且这种承诺应是可评价的。

此条文中的“管理者”指在确定的信息安全管理体系范围内的信息安全事项具有决策权的执行最高管理者，根据组织的具体管理模式不同，该“管理者”可以是一个人，也可以是一组人。

建立、实施、维护和持续改进 ISMS 必定需要一定的投入，管理者必须确保这些资源的获得。

2.7.2. 方针

【参考译文/原文】

管理者应建立的信息安全方针： a) 应适合组织的目标； b) 应包括信息安全目标(见6.2)或者提供建立信息安全目标的框架； c) 应包括承诺满足信息安全的相关要求； d) 应包括承诺持续改进信息安全管理体系。 信息安全管理方针应： e) 形成文档； f) 在组织内部充分沟通； g) 需要时对外部相关方可	用。 Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information; f) be communicated within the organization; and g) be available to interested parties, as appropriate.

【内容解析】

方针(policy)文件是 ISMS 的基础，即实施某项活动的指导原则和行动路线，它是一个组织在其整体业务范围框架下开展某项活动的总的指导原则和行动路线,这个文件如同法律体系中的宪法一样。我们无法从其中找到具体的安全要求或安全策略，但是这个文件是所有体系文件和技术措施的根本。

ISMS 方针一般由组织的管理者批准和发布，以体现管理着对信息安全的领导和承诺。

制定方针的目的可以归纳为以下三个方面：

1) 为组织提供信息安全关注的焦点，指明方向，确定目标。
2) 用简洁通俗的方法阐述组织最重要的信息安全问题，确保 ISMS 被充分理解和贯彻实施。
3) 统领整个 ISMS，是所有的其他文件和措施的基础。

2.7.3. 组织角色、职责和权力

【参考译文/原文】

管理者应确保信息安全管理角色和权力得到分配和沟通。	管理者应对以下职责和权力进行分派： a) 确保组织建立的信息安全管理体系符合本国际标准要求；

b) 向高层汇报信息安全管理体系的执行情况。 注： 管理者也应被赋予相应的职责和权力，向组织内部汇报信息安全管理体系的执行情况。 Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	Top management shall assign the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this International Standard; and b) reporting on the performance of the information security management system to top management. NOTE Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

【内容解析】

信息安全活动离不开人员的参与，要执行信息安全活动，人员必须被赋予相应的职责和权限，即建立信息安全岗位和指责。管理者履行其承诺的方式，主要在于指派和批准信息安全的相关角色及其职责和权限，为相应信息安全管理活动的展开提供资源支持。

2.8. 计划

2.8.1. 处置风险和机遇

2.8.1.1. 总则

【参考译文/原文】

当进行信息安全管理体系规划时，组织应参考 4.1 中的问题和 4.2 中的需求，来决定需要被处置的风险和机遇： a) 确保信息安全管理体系可以实现其预期目标； b) 避免或减少不良影响； c) 实现持续改进。 组织应规划： d) 处置风险和机遇的行动； e) 如何 1) 将实施行动整合到信息安全管理体系流程中； 2) 评价行动的有效性。	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.

【内容解析】

风险将影响组织目标的实现，这些目标可能关系到组织中从战略决策到运营的各种活动，包括各个过程和具体项目，表现在领导、战略、经营、财务、环境、社会、声誉等各个方面。即追求成功时，机遇和危险并存，通过有效的管理，可以趋利避害。

对信息安全进行管理，并不意味着将所有的资产置于绝对安全的保护措施。因为“绝对安全”的成本是巨大的。因此，在风险控制措施的选择时，应当考虑组织的内外部环境因素以及相关方的需求和期望。一般来说，风险处置可考虑：风险降低、风险转移、风险规避和风险接受。

2.8.1.2. 信息安全风险评估

【参考译文/原文】

组织应定义和实施信息安全风险评估流程，从而： a) 建立和维护信息安全风险标准，包括： 1) 风险接受标准； 2) 实施信息安全风险评估的标准； b) 确保信息安全风险评	估活动产生一致性，产生有效的和可比较的结果； c) 识别信息安全风险： 1) 在信息安全管理体系范围内，通过信息安全风险评估流程，识别由于信息的机密性、完整性和可用性的丧失带来的风险； 2) 识别风险的属主； d) 分析信息安全风险： 1) 评估在 6.1.2 c)1)中识别的风险产生的潜在后果；

2) 评估在 6.1.2 c)1)中识别的风险转化为事件的可能性；
3) 确定风险的等级；
e) 评价信息安全风险：
1) 将风险分析结果与在 6.1.2 a)中所定义的风险标准进行比较；
2) 根据风险等级确定风险处置的优先级。
组织应保留有关信息安全风险评估的过程文档。

The organization shall define and apply an information security risk assessment process that:
a) establishes and maintains information security risk criteria that include:
1) the risk acceptance criteria; and
2) criteria for performing information security risk assessments;
b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;
c) identifies the information security risks:
1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
2) identify the risk owners;
d) analyses the information security risks:
1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;
2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and
3) determine the levels of risk;
e) evaluates the information security risks:
1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
2) prioritize the analysed risks for risk treatment.
The organization shall retain documented information about the information security risk assessment process.

【内容解析】

在进行风险评估之前，最重要的就是确定风险评估方法，风险评估方法应满足 ISMS 的要求、已识别的业务信息安全和法律法规的要求。

标准中对风险评估方法提出了细致的要求，即：产生有效的和可比较的结果。有效意味着风险评估方法的过程和结果都是正确、科学的。可比较意味着，根据结果，可以判断风险大小。可比较不一定是可以从结果判断绝对的大小，也可能是判断相对的大小。

组织可以根据自身的情况，选用适合自身的风险评估方法，当前风险评估可参照的标准有 ISO31000，GB/T20984，ISO27005 等。

在新版标准中，新增了“风险的属主”这一概念，资产所有者未必是风险属主，风险属主可以是资产的管理者、该风险管控的负责人（如部门领导）、或组织领导者等。

一般而言，风险评估的结果是一个风险的 Rank，即一个相对的等级列表，其中的值没有很实际的意义，这个值在整体中的位置可能（类似于排名）更有价值。这种结果必须是可比较和可再现的。

2.8.1.4. 信息安全风险处置

【参考译文/原文】

组织应定义和实施信息安全风险处置过程：

a) 依据风险评估的结论，选择适当的信息安全风险处置方式；

b) 确定信息安全风险处置选用的各项控制措施；

注： 组织可以根据标准要求来设计控制措施，也可以根据其他方面因素和来源设计控制措施。

c) 比较以上 6.1.3 b)中的和附录 A 的控制措施，确保未遗漏有效的控制措施；

注 1：附录 A 包括完整的控制目标和控制措施的清单，使用本标准的用户可以直接使用附录 A 内容，并确保没有遗漏必要的控制措施。

注 2：控制措施隐含在选择的控制目标中。附录 A 中未涉及的控制对象和控制措施内容应给予补充和增加。

d) 制定具备必要控制措施(见 6.1.3 b)和 c))的适用性声明 SOA，来判断包含项是否被有效纳入实施范围，判断排除内容是否从附录 A 的控制措施被有效排除；

e) 制定信息安全风险处置计划；

f) 得到风险属主对信息安全风险处置计划和残余风险接受的审核。

组织应保留信息安全风险处置的过程文档。

注：本标准中的信息安全风险评估和处置流程与 ISO 31000[5]中的原则和通用指南保持一致。

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.

NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000[5]

【内容解析】

无论风险评估方法多么先进，没有相应的风处置理过程，都是一纸空文。识别、分析并评价风险的目的还是为了风险处置。

在选择控制措施的时候，应把握以下要点：

1. 考虑风险接受的准则，即这些控制措施应将风险降低至可接受的程度；
2. 满足法律法规和合同要求；
3. 可以参照附录 A，这样可以让选择比较全面，不至于遗漏重要的可接受的程度；
4. 附录 A 不一定是全部，可以在此基础上添加额外的控制目标和控制措施。

“适用性声明”是说明控制目标和控制措施的文件，这个文件也是 ISMS 认证所需要的工作文件之一。对实施哪些控制目标、措施、不实施哪些控制目标、措施应记入“适用性声明”中，但不宜记录太细，以避免过多披露控制措施的细节。

2.8.2. 信息安全目标的计划和实现

【参考译文/原文】

组织应建立不同职能及层级的信息安全目标。	The organization shall establish information security objectives at relevant functions and levels.
信息安全目标应：	The information security objectives shall:
a) 与信息安全方针一致；	a) be consistent with the information security policy;
b) 可度量(如果可操作)；	b) be measurable (if practicable);
c) 考虑适用的信息安全要求,以及风险评估和风险处置结果；	c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
d) 得到沟通；	d) be communicated; and
e) 及时更新。	e) be updated as appropriate.
组织应将信息安全目标以文档化形式保留。	The organization shall retain documented information on the information security objectives.
在规划如何实现信息安全目标时，组织应明确：	When planning how to achieve its information security objectives, the organization shall determine:
f) 要做什么；	f) what will be done;
g) 需要什么资源；	g) what resources will be required;
h) 谁来负责；	h) who will be responsible;
i) 什么时候完成 ；	i) when it will be completed; and
j) 如何评价结果。	j) how the results will be evaluated

【内容解析】

信息安全目标的设定应以风险评估和风险处置的结果为基础，并应对其对信息安全目标进行审核。

信息安全目标应是可测量的，测量标准可以从：息安全管理体系运行、员工信息安全行为、意识管理、日常安全管理、业务连续性管理几个方面来考虑。

2.9. 支持

2.9.1. 资源

【参考译文/原文】

组织应确定并提供建立、实施、维护和持续改进信息安全管理体系所需的资源。	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

【内容解析】

建立、实施、维护和持续改进 ISMS 的每个过程都离不开资源，因此组织要及时确定资源的需求，并在需要时提供。

资源包括：人员、基础设施、工作环境等

组织必须根据自身特点和信息安全现状确定所需资源，必要时可借助外部资源。

组织利用所需的资源，应确保信息安全程序支持业务需求，因为业务是组织的根本关注点，信息安全程序必须为业务目标服务。另外，组织要能够通过所需资源识别并满足法律法规要求，以及合同中的安全义务。

资源的需求并不是一成不变的，它会随着组织业务的发展、安全技术的发展等发生变化，所以在必要的时候要对其进行评审，并适当相应评审结果，以满足变化的需要。例如当组织的业务规模变大时，所需资源也随之变大，当出现新的网络攻击技术时，组织需要更改原有的硬件或软件来应对新的攻击。

2.9.2. 能力

【参考译文/原文】

组织应： a) 确定员工为完成其本职工作所所需的安全技能； b) 确保员工具备完成工作所需的教育、培训和经验； c) 采取合适的措施确保员工具备相应的技能并对技能进行考核； d) 保留适当的文档信息作为证据。 注：适当的措施可能包括，例如：提供培训、指导或重新分派现有员工，或雇用具备相关技能的人士。 The organization shall:	a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence. NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

【内容解析】

组织应通过培训或其他方法提高 ISMS 相关人员的能力，增强员工的信息安全以使，满

足信息安全工作的要求。

针对分配有 ISMS 指责的人员，组织要确保其具备执行所有任务的能力。

应对从事这些工作的人员实施必要的能力培训或用其他方式满足岗位的能力要求，例如通过应用有能力的人员。

应对所有与 ISMS 活动有关的人员的培训及所采取的其他措施进行有效性评价，评价方式可以是面试、鄙视或实际的操作测试等，也可以通过观察员工的能力变化、工作效果及效率的变化来评价是否达到了培训计划或其他措施所策划的目标。

应保留与 ISMS 活动有关的人员的教育、培训、技能、经历和资格的适当的记录，例如学历或学位证书、信息安全相关培训的合格证书、工作的经历证明文件等。

2.9.3. 意识

【参考译文/原文】

组织的员工应了解： a) 信息安全方针； b) 个人对于实现信息安全管理的重要性，提高组织信息安全绩效的收益； c) 不符合信息安全管理体系要求所造成的影响。	the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.

Persons doing work under

【内容解析】

组织应加强员工信息安全以使的教育，使所有相关人员都意识到所从事的信息安全活动的适当性和重要性，并能积极地从自身做起，为达到 ISMS 的目标做出贡献。

2.9.4. 沟通

【参考译文/原文】

组织应明确与信息安全管理体系相关的内、外部沟通需求，包括： a) 沟通什么； b) 何时沟通； c) 和谁沟通； d) 谁应该沟通； e) 哪种沟通过程有效。	The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.

【内容解析】

沟通贯穿着建立、实施、维护和持续改进 ISMS 的各个过程。沟通活动可以按多种维度进行分类。需要考虑的维度包括（但不限于）：

1. 组织内部和外部（客户、供应商、外部利益相关方等）；
2. 正式（报告、会议记录、简报）和非正式（电子邮件、备忘录、即兴讨论）；
3. 垂直（上下级之间）和水平（同级之间）；

4. 官方（新闻通讯、年报）和非官方（私下的沟通）。

2.9.5. 文档要求

2.9.5.1. 综述

【参考译文/原文】

组织的信息安全管理体系应包括： a) 符合本国际标准的文件； b) 组织所明确的，表明信息安全管理体系有效性的必要的记录文档。 注：不同组织的信息安全管理体系的文档的复杂度根据以下情况有所不同： 1)组织的规模、活动类型、过程、产品和服务； 2)过程的复杂程度及其相互作用。 3)人员能力	The organization's information security management system shall include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system. NOTE The extent of documented information for an information security management system can differ from one organization to another due to: 1) the size of organization and its type of activities, processes, products and services; 2) the complexity of processes and their interactions; and 3) the competence of persons.

【内容解析】

文件化是 ISMS 重要特征之一。

文件是 ISMS 运行的依据。文件是实现管理意愿的一种有效途径。另外，文件还可以提供适宜的培训、实现重复性和追溯性、提供客观证据、评价信息安全管理体系的有效性和持续适宜性等。

文件可以是程序文档、规范文档、记录文档、报告文档等，而文件媒体包括纸张、磁盘、磁带或其他电子媒体等。

2.9.5.2. 创建和更新

【参考译文/原文】

组织应明确何时创建和更新文档信息是适合的： a)识别和描述(例如：标题、日期、作者和版本号)； b)格式(例如：语言、软件版本和图形)与介质(例如：纸质、电子)； c)适宜性和充分性经过评审。	When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number); b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c) review and approval for suitability and adequacy.

【内容解析】

组织应编制形成文件的程序，对文件的创建、评审、批准、发放、使用、更新和处理等

活动做出相应的规定。正式的文件应该标有文件名、编号、编制人、审批人、批准人和发布日期等。

2.9.5.3. 文档控制

【参考译文/原文】

信息安全管理体系和本国际标准要求的文档信息应予以控制以确保：	Documented information required by the information security management system and by this International Standard shall be controlled to ensure:
a) 在需要的时间和场合可用；	a) it is available and suitable for use, where and when it is needed; and
b)文档得到充分保护(例如：防止泄密、不当使用或丧失完整性)。	b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).
为做好文件控制，组织应明确以下文档控制活动的恰当执行：	For the control of documented information, the organization shall address the following activities,as applicable:
c)分发、访问、收回和使用；	c) distribution, access, retrieval and use;
d)得到良好存储和保管，确保清晰易读；	d) storage and preservation, including the preservation of legibility;
e)变更控制(例如：版本控制)；	e) control of changes (e.g. version control); and
f)归档和处置。	f) retention and disposition.
明确组织进行信息安全管理体系规划和运行所必需的外部文档，并进行适当的标识和控制。	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.
注：访问意味着允许查看文档信息，或经许可和授权对文档进行查看和修改。	NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

【内容解析】

所有信息安全管理体系的文档信息应作为信息资产予以管理，以确保这些文档的完整性和可用性，以及必要的保密性。对于体系运行的记录应真实、完整。

文档保存的期限，决定于组织和相关方要追溯记录的时间期限。一般情况下，文档的保存期限应不低于文档对应对象的自然生命周期。

外部文档是指来自组织外部的文档，例如法律法规、技术标准、规范、来自供应商或客户的图样、投标书等。对外部文档应识别并跟踪，及时更新，确保获得和使用有效的外部文档，防止误用。

文档信息可以以各种形式存在，例如纸质文档、网页发布或电子文档等都可以。

2.9.6. 运行计划和控制

【参考译文/原文】

组织应计划、实施和控制相关过程以满足信息安全要求所需的过程。包括实施在 6.1 中决定采取的行动，按计划实现在 6.2 中所明确的信息安全目标。 组织应保留必要的过程文档信息，以表明相关过程已按照计划执行。 组织应控制计划更改，并审核计划变更的影响，如有必要采取措施减少不利影响。 组织应确保外包过程受控。	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.

【内容解析】

组织应针对信息安全目标制定可执行的计划，并对计划的实施进行控制。

当计划发生变更时，组织应对变更造成的影响进行评估。

2.9.7. 信息安全风险评估

【参考译文/原文】

组织应按照计划，或者在重大改变提出或发生时进行信息安全风险评估，并考虑 6.1.2a)制订的标准。 组织应将信息安全风险评估的结果作为文档信息保留。	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.

【内容解析】

组织应按照固定的时间间隔对风险评估方法有效性、残余风险和可接受风险级别的适宜性进行评审。当组织结构、技术、业务目标和过程、面临的威胁、控制措施的有效性和外部环境等因素发生变化时，也应考虑启动一次风险评估。

2.9.8. 信息安全风险处置

【参考译文/原文】

组织应执行风险处置计划。 组织应将信息安全风险处置的结果作为文档信息保留。	The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.

【内容解析】

在风险处置计划中，最好要包括：

1. 为处理风险所选择的管理措施；
2. 实施所需要的资源；
3. 管理者应承担的职责；
4. 计划的优先级或时间安排；

以上 4 条属于管理者责任。

下面 3 条属于计划的具体实施所涉及的方面：

1. 实施计划所需要的资金安排；
2. 实施计划所涉及的角色；
3. 实施计划所需要的职责分配。

风险处置计划是针对风险评估的结果制定的实施计划。实施所选择的控制措施的过程，可以仍未是风险处置计划具体实现的过程。

风险处置计划属于 ISMS 规定的必须文件之一。

2.10. 绩效评价

2.10.1. 监视、测量、分析和评价

【参考译文/原文】

组织应评价信息安全管理体系的绩效。 组织应明确： a) 包括信息安全过程和控制措施在内，应监控和测量什么； b) 适用的监视、测量、分析和评价方法，以确保结果有效； 注：选用的方法应能产生可比较的和可重现的结果。 c) 何时实施监视和测量； d) 谁负责监视和测量； e) 何时分析和评价监视和测量的结果； f) 谁应分析和评价这些结果。 组织应保留适当的文档信息作为监视和测量已开展的证据。	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; NOTE The methods selected should produce comparable and reproducible results to be considered valid. c) when the monitoring and measuring shall be performed; d) who shall monitor and measure; e) when the results from monitoring and measurement shall be analysed and evaluated; and f) who shall analyse and evaluate these results. The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

【内容解析】

控制措施的有效性必须能够进行测量，以使管理者和员工确定控制措施达到计划的控制目标的程度，测量控制措施的有效性的方法及如何进行测量要预先确定。

使用的控制措施有效性测量方法与风险评估方法一样，要确保能够产生可比较和可再现的结果，测量程序可文件话，作为 ISMS 体系文件之一。

一般来说，监视和测量可分为管理性监视测量和技术性监视测量。

对系统实施技术性监视和测量，一种情况为了实时监测系统资源的使用情况是否在安全阀值内，以及是否有安全违规情况发生和能否对这些安全违规进行有效的拦截。另一方面，这些系统中的设备硬件的耗损情况虽不需进行实时监测，但也需要根据硬件的寿命顶起进行检查，以便于及时排出因设备故障而导致的系统功能不可用，进而影响信息的完整性和可用性。

管理性的监视和测量则是针对各种信息安全管理规程执行情况的常规检查，通常使用以管理规程的要求为依据的检查表方法。例如：内部管理体系审核，以高层管理者为主导的管理评审等。

组织应对监视和测量的结果设定分析方法和评价指标。

2.10.2. 内部审核

【参考译文/原文】

组织应定期进行内部审核以表明信息安全管理体系是否： a) 符合 1) 满足组织自身的信息安全管理要求； 2) 本国际标准的要求； b) 有效的执行和保持。 组织应： c) 规划、建立、执行和保持审核程序，包括频率、方法、责任、计划要求和报告。审核程 序应考虑组织所关注的重要过程和之前的审核结果； d) 定义审核准则和审核范围； e) 选择审核员并进行审核，确保审核过程的客观和公正； f) 确保审核结果报告给相关管理层； g) 组织应保留内部审核的过程文档作为证据。	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard; b) is effectively implemented and maintained. The organization shall: c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods,responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits; d) define the audit criteria and scope for each audit; e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; f) ensure that the results of the audits are reported to relevant management; and g) retain documented information as evidence of the audit programme(s) and the audit results.

【内容解析】

内部审核的目的是评价组织的信息安全管理体系的符合性、适宜性和有效性，是检查组织的信息安全体系是否符合法律法规、本标准、组织的信息安全管理体系要求，以及管理体系的运行是否有效、是否可实现组织的信息安全管理方针和目标的有效手段。

和外审不同，内部审核用于内部目的，由组织自己进行，因此，应该更偏重于解决问题，

也应该更加细致地组织进行。

针对一定时间框架内（例如 12 个月内）制定的审核方案，对管理体系审核的频次、每一次审核的范围、每一次审核的准则和审核方法做出具体规定。内部审核周期一般不超过一年。

内部审核人员必须具备适宜的能力。审核人员的能力包括对审核准则的熟悉和理解以及对审核方法的熟练掌握。为确保审核的公正性，审核人员的选择应考虑其与受审核区域相关活动无利害关系和无利益冲突，在具体的审核日程计划中，不应安排审核员审核自己的工作。

组织应该安排适宜的人员对审核员发现的不符合采取纠正措施，并跟踪验证，确认已到达了消除原因以防止不符合再发生的效果。审核的全过程应形成文件、保持记录。

2.10.3. 管理评审

【参考译文/原文】

管理者应定期评审组织的信息安全管理体系，以确保其持续的适宜性、充分性和有效性。 管理评审应关注： a) 以往管理评审后所采取措施的状态； b) 内、外部信息安全管理体系相关环境的变化； c) 安全控制措施执行的反馈情况，包括如下趋势： 1) 不符合情况和改正措施 2) 监控和测量的结果； 3) 审核结果； 4) 信息安全目标实现情况； d) 相关方的反馈； e) 风险评估的结果和风险处置计划的状态； f) 持续改进的时机。 管理评审的输出应包括持续改进的时机和安全管理体系所需变更的决定。 组织应保留文档信息作为管理评审结果的证据。	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of: a) the status of actions from previous management reviews; b)changes in external and internal issues that are relevant to the information security management system; c) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives; d) feedback from interested parties; e) results of risk assessment and status of risk treatment plan; and f) opportunities for continual improvement. The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.

【内容解析】

管理评审是由管理者主导的监视测量活动，目的是对组织的信息安全方针和目标的适宜性、充分性和有效性进行评价。

管理评审的时间间隔一般为 12 个月，特殊性况下，也可以实施专项评审。一般以会议方式进行。

所有向管理评审会议提供输入信息的各职能区域负责人，应在其报告中包含标准中评审输入的内容。

管理评审会议在所有输入的信息进行评审后，应就评审输出内容作出决定。管理评审的

输出结果以及任何决定应及时传递到相应负责人员，以便及时按照管理评审决定的要求制定具体的措施计划和实施改进。

组织要根据监视程序和评审活动的结果，对 ISMS 过程中涉及的安全计划进行更新，以保持这些安全计划的适宜性，使之持续适于组织的安全要求。

在监视和评审过程中要随时记录可能影响 ISMS 的有效性或施行的行动和事件，这些记录是 ISO/IEC 27001 中明确提出的要求，可以为保持和改进 ISMS 提供信息。

2.11. 改进

2.11.1. 不符合项和纠正措施

【参考译文/原文】

当不符合情况项时，组织应：

a) 对不符合情况采取措施，如：

1) 采取措施，以控制和改正它；

2) 处置影响；

b) 明确必要的控制措施，以消除不符合情况产生的原因，确保它不会再发生或在其他地方发生，通过：

1) 评审不符合项；

2) 明确不符合项产生的原因；

3) 明确是否存在或可能发生类似的不符合项；

c) 采取必要的措施；

d) 评审已采取的改正措施的有效性；

e) 必要时改进信息安全管理体系。

纠正措施应与所发生的不符合的影响程度相适应。

组织应保留以下文档信息作为证据：

f) 不符合情况的性质和所采取的后续行动；

g) 纠正措施的结果。

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it; and

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

f) the nature of the nonconformities and any subsequent actions taken, and

g) the results of any corrective action.

【内容解析】

纠正措施主要针对不符合项，也可能是针对建立阶段的活动或实施和运行阶段的活动而采取的。不符合项是指没有或缺乏执行与维护一个 ISMS 的需求；根据可用的客观证据，提出了对 ISMS 完成该组织信息安全方针和目标的能力的重大怀疑。当发现不符合项时，必须对其采取措施，以符合 ISMS 的要求。

纠正措施应与不符合项的严重程度以及 ISMS 满足规定需求能力的风险相适应。

完全消除孤立的不符合项是绝不可能的，而且，孤立的事件事实上可能是某种安全事故的表现，如果不能妥善处理，可能对整个组织都有影响。因此，在识别和执行任何纠正措施时，应不仅仅考虑孤立的事件本身。除了识别直接的纠正措施外，更重要的是要有长远的眼光，确保所采取的措施不仅解决考虑到的问题，而且预防或减少类似事件再次发生的可能性。

执行纠正措施是改进阶段的重要内容，但必须注意一下两方面：

（1）维护 ISMS 文件内部的一致性；不发生会使组织产生不可接受的风险的变更的影响。

（2）在制定纠正措施时，可参照其他组织或组织以前的安全经验，少走弯路，以便迅速、高效地制定有效的措施。

2.11.2. 持续改进

【参考译文/原文】

组织应不断完善信息安全管理体系的适宜性、充分性和有效性。	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

【内容解析】

持续改进是指增强满足要求的能力的循环活动，ISMS 持续改进的目的是利用各种数据和信息，不断提高 ISMS 的有效性。持续改进可以是渐进性的改进，也可以是突破性的改进。对于渐进性改进来说，组织内人员是提供信息的最佳来源，参与人员应当被授予相应的权限，并应当得到与改进有关的技术支持和必须的资源。

改进阶段必须保证改进达到了预期目标，这需要对纠正措施进行跟踪和反馈，并对措施结果的有效性进行评审，通过评审结果来判定改进是否达到了预期目标。

2.12. 附录 A

2.12.1. A.5 信息安全方针

A.5.1 信息安全管理指引

目标：提供符合有关法律法规和业务需求的信息安全管理指引和支持。

A.5.1.1 信息安全方针

应定义信息安全方针，信息安全方针文件应经过管理层批准，并向所有员工和相关方发布和沟通。

A.5.1.2

信息安全方针的评审

应定期或在发生重大的变化时评审方针文件，确保方针的持续性、稳定性、充分性和有效性。

A.7.2.2

“人”是企业整个信息安全体系的最关键因素。无论多么精良的设备，多么严谨的系统

与体系。如果员工的信息安全意识不足，在他们工作形成习惯之后，认为无关紧要的东西，无意“泄露”出去之后，将会给企业带来不可估量的损失。培养企业信息安全意识文化，树立员工信息安全责任心，这才是解决企业信息安全的关键之匙。

为了让所有承担 ISMS 相关任务的人员能够恪尽职守，组织必须确保：

1. 确定承担信息安全工作的人员需要何种技能；
2. 给予相关人员适当的培训，必要时，需要为特定任务招聘有经验的人；
3. 评估培训效果；
4. 维护一个教育和培训程序，对每个职员的能力、经验和资历进行登记。

组织必须确保相关人员能够意识到其所进行的信息安全活动的重要性，并且清楚各自在符合 ISMS 目标过程中参与的方式。

为此，开发一个培训和意识程序是非常重要的。通过有计划有步骤地实施意识培训，让每一个职员都能理解并遵守信息安全最佳实践，这比购买最高端产品采用最精尖技术来得更有效更经济。

组织在实施一个信息安全意识程序时，有几个关键因素需要考虑：

1. 努力使这种意识能够融入到组织整体的环境和文化当中；
2. 确保高级管理者承诺并支持；
3. 理解职员对于安全的重要性；
4. 找到内部沟通渠道；
5. 充分利用现有资源；
6. 建立策略、程序、表格和相关的检查表单；
7. 识别程序的最终结果；
8. 确保能够交付到人。