ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31496—2015/ISO/IEC 27003:2010

信息技术　安全技术
信息安全管理体系实施指南

Information technology—Security techniques—
Information securitymanagement system implementation guidance

(ISO/IEC 27003:2010,IDT)

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术
信息安全管理体系实施指南
GB/T 31496—2015/ISO/IEC 27003:2010
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.5 字数 100 千字
2015年6月第一版 2015年6月第一次印刷
*
书号:155066·1-51118 定价 48.00元

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO/IEC 27003:2010《信息技术　安全技术　信息安全管理体系实施指南》。

本标准做了以下编辑性修改：

——在引言部分增加了有关信息安全管理体系标准族情况的介绍。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国电子技术标准化研究院、上海三零卫士信息安全有限公司、山东省计算中心、黑龙江省电子信息产品监督检验院、北京信息安全测评中心、中电长城网际系统应用有限公司。

本标准主要起草人：上官晓丽、许玉娜、董火民、闵京华、赵章界、周鸣乐、方舟、李刚。

引　言

信息安全管理体系标准族(Information Security Management System,简称 ISMS 标准族)是国际信息安全技术标准化组织(ISO/IEC JTC1 SC27)制定的信息安全管理体系系列国际标准。ISMS 标准族旨在帮助各种类型和规模的组织,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。ISMS 标准族包括的标准:a)定义了 ISMS 的要求及其认证机构的要求;b)提供了对整个"规划-实施-检查-处置"(PDCA)过程和要求的直接支持、详细指南和(或)解释;c)阐述了特定行业的 ISMS 指南;d)阐述了 ISMS 的一致性评估。

目前,ISMS 标准族由下列标准组成:

——GB/T 29246—2012/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

——GB/T 22080—2008/ISO/IEC 27001:2005　信息技术　安全技术　信息安全管理体系　要求

——GB/T 22081—2008/ISO/IEC 27002:2005　信息技术　安全技术　信息安全管理实用规则

——GB/T 31496—2015/ISO/IEC 27003:2010　信息技术　安全技术　信息安全管理体系实施指南

——GB/T 31497—2015/ISO/IEC 27004:2009　信息技术　安全技术　信息安全管理　测量

——GB/T 31722—2015/ISO/IEC 27005:2008　信息技术　安全技术　信息安全风险管理

——GB/T 25067—2010/ISO/IEC 27006:2007　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

——ISO/IEC 27007　信息技术　安全技术　信息安全管理体系审核指南

——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

——ISO/IEC 27013:2012　信息技术　安全技术　ISO/IEC 27001 和 ISO/IEC 20000-1 集成实施指南

——ISO/IEC 27014:2013　信息技术　安全技术　信息安全治理

——ISO/IEC TR 27015:2012　信息技术　安全技术　金融服务信息安全管理指南

本标准作为 ISMS 标准族之一,其目的是为组织按照 GB/T 22080—2008 制定信息安全管理体系(ISMS)的实施计划,提供实用指导。实际情况下,ISMS 的实施通常作为一个项目来执行。

本标准所描述的过程旨在为实施 GB/T 22080—2008 提供支持;第 4 章、第 5 章和第 7 章所包含的相关部分和文件可用于:

a)　准备启动组织的 ISMS 实施计划、定义该项目的组织结构,及获得管理者的批准;

b)　该 ISMS 项目的关键活动;

c)　实现 GB/T 22080—2008 要求的示例。

通过使用本标准,组织将能够制定信息安全管理的过程,并向利益相关方保证,信息资产的风险可持续保持在组织定义的可接受的信息安全边界内。

本标准不涉及运行活动和其他 ISMS 活动,但涉及了如何设计这些活动的概念,这些活动是在开始运行 ISMS 后所产生的。这些概念导致了最终的 ISMS 项目实施计划。ISMS 项目的组织特定部分的实际执行不在本标准范围内。

ISMS 项目的实施宜使用标准的项目管理方法学来执行(更多信息请参见 ISO 和 ISO/IEC 有关项目管理的标准)。

信息技术　安全技术
信息安全管理体系实施指南

1　范围

本标准依据 GB/T 22080—2008，关注设计和实施一个成功的信息安全管理体系(ISMS)所需要的关键方面。本标准描述了 ISMS 规范及其设计的过程，从开始到产生实施计划。本标准为实施 ISMS 描述了获得管理者批准的过程，为实施 ISMS 定义了一个项目(本标准称作 ISMS 项目)，并就如何规划该 ISMS 项目提供了相应的指导，产生最终的 ISMS 项目实施计划。

本标准可供实施一个 ISMS 的组织使用，适用于各种规模和类型的组织(例如，商业企业、政府机构、非赢利组织)。每个组织的复杂性和风险都是独特的，并且其特定的要求将驱动 ISMS 的实施。小型组织将发现，本标准中所提及的活动可适用于他们，并可进行简化。大型组织或复杂的组织可能会发现，为了有效地管理本标准中的活动，需要层次化的组织架构或管理体系。然而，无论是大型组织还是小型组织，都可应用本标准来规划相关的活动。

本标准提出了一些建议及其说明，但并没有规定任何要求。期望把本标准与 GB/T 22080—2008 和 GB/T 22081—2008 一起使用，但不期望修改和/或降低 GB/T 22080—2008 中所规定的要求，或修改和/或降低 GB/T 22081—2008 所提供的建议。因此，不宜声称符合这一标准。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 22080—2008　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2005，IDT)

GB/T 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009，IDT)

3　术语和定义

GB/T 29246—2012 和 GB/T 22080—2008 界定的以及下列术语和定义适用于本文件。

3.1

ISMS 项目　ISMS project

组织为实施一个 ISMS 所开展的结构化活动。

4　本标准的结构

4.1　章条的总结构

ISMS 的实施是一种重要活动，通常作为组织的一个项目来执行。本标准通过关注该项目的启动、

规划和定义，来说明 ISMS 的实施。规划该 ISMS 最终实施的过程包括 5 个阶段，每个阶段都用单独的一章来表达。所有各章具有相似的结构。这 5 个阶段是：

a) 获得管理者对启动 ISMS 项目的批准(第 5 章)；

b) 定义 ISMS 的范围、边界和 ISMS 的方针策略(第 6 章)；

c) 进行信息安全要求分析(第 7 章)；

d) 进行风险评估和规划风险处置(第 8 章)；

e) 设计 ISMS(第 9 章)。

参照有关标准，图 1 给出了规划该 ISMS 项目的 5 个阶段以及主要输出文档。

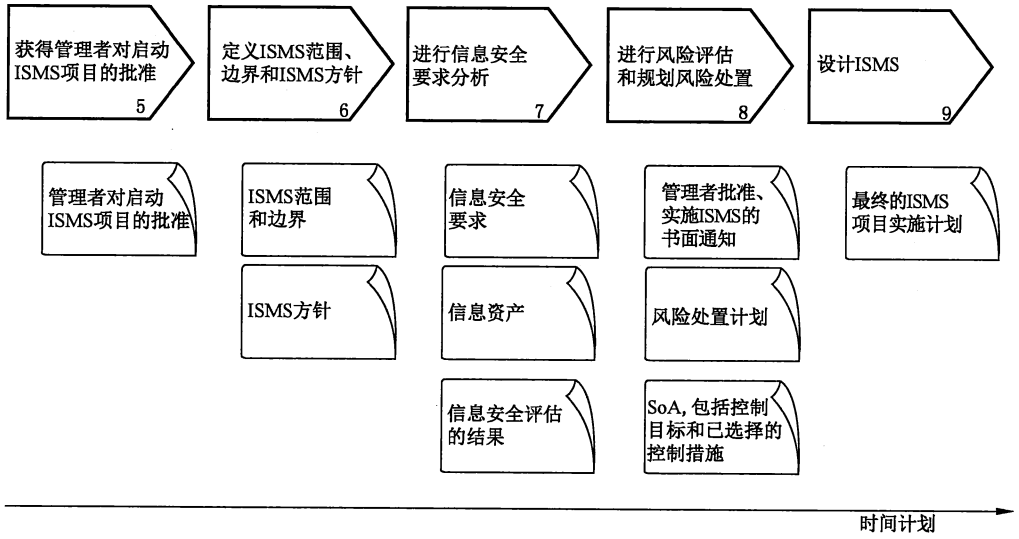


图 1 ISMS 项目的各个阶段

以下附录给出了进一步的信息：

附录 A：与 GB/T 22080—2008 相对照的活动概要。

附录 B：信息安全角色和责任。

附录 C：有关内部审核的规划信息。

附录 D：方针策略结构。

附录 E：有关监视和测量的规划信息。

4.2 每章的一般结构

每章包括：

a) 在每章开头的文本框中，陈述要达到的一个或多个目标；

b) 为达到该阶段目标所必要的一个或多个活动。

每一个活动都在子条款中描述。

每一条款中活动的描述结构如下：

活动

活动定义了为达到该阶段全部或部分目标，所必需满足的那些事宜。

输入

输入描述了起点，例如，存在的文档化决定，或描述在本标准中其他活动的输出。输入可能或者引自相关章节所陈述活动的完整输出，或者引自指该引用章节之后可能添加活动的特定信息。

指南

指南提供了使这一活动能够得以执行的详细信息。有些指南可能不适合所有情况，获得结果的其他方式也许更加适合。

输出

输出描述了活动完成后的结果或可交付项，例如一个文档。不论组织的规模或 ISMS 范围的大小，其活动完成后的结果或可交付项统称为输出。

其他信息

其他信息提供了可能有助于执行该活动的任何补充信息，例如，对其他标准的引用。

本标准描述的阶段和活动包括了基于相互依赖关系而建议的执行活动的顺序，这些相互依赖关系通过每个活动的“输入”和“输出”的描述来识别。然而，组织可按所需要的任何次序来选择活动，以便为 ISMS 的建立和实施做准备，这取决于很多不同的因素（例如，目前到位的管理体系的有效性、对信息安全重要性的理解和实施 ISMS 的原因）。

4.3 图表

定义一个组织的 ISMS 项目，通常以图的形式概要给出相应的活动及其输出。

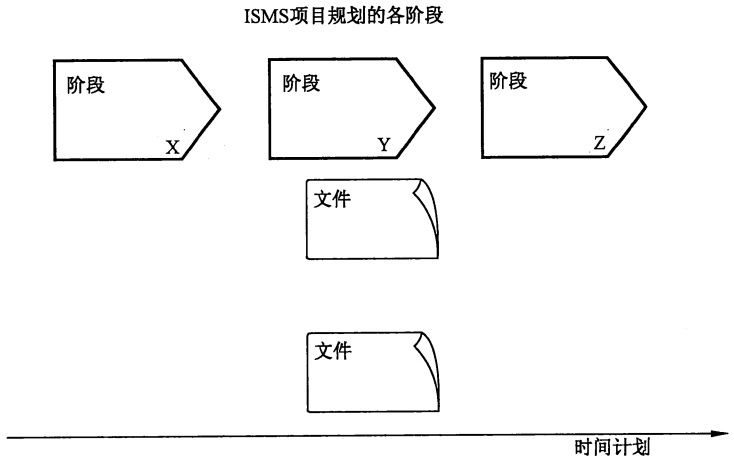
图 2 概要给出了每一阶段条款的示意图，示意图对每一阶段中所包含的活动进行了高度概括。

a）图示出一个 ISMS 项目的规划阶段，其中强调了特定章节中所解释的阶段及其关键的输出文件。

b）图（阶段的活动）包括 a）图中所强调的阶段包含的关键活动和每一个活动的主要输出文件。

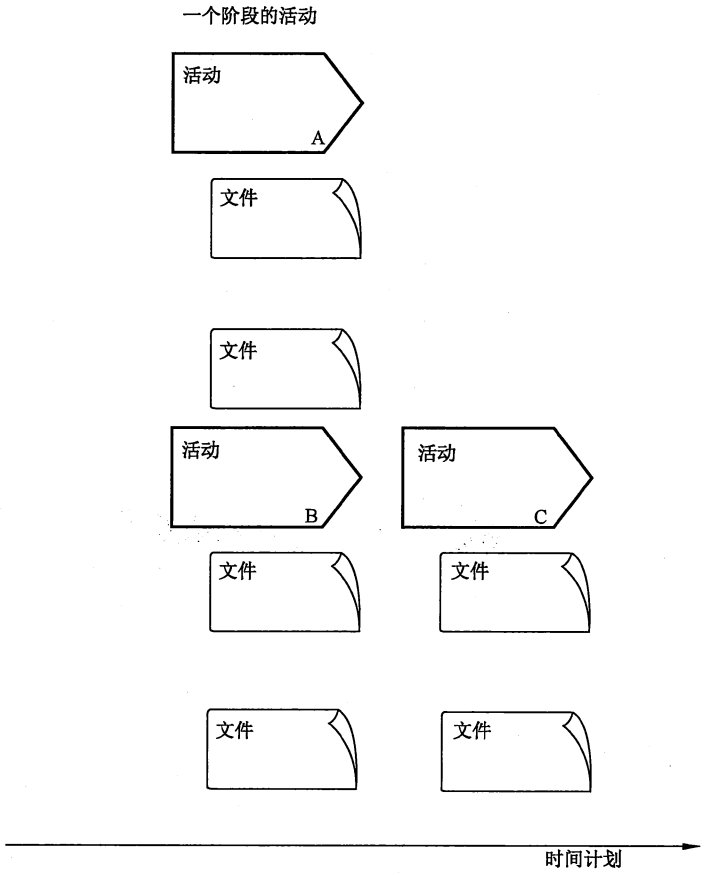
b）图中的时间段基于 a）图中的时间段。

活动 A 和活动 B 可能同时执行。活动 C 宜在活动 A 和活动 B 完成后开始。



a）

图 2 流程示意图图例



b)

图 2（续）

5 获得管理者对启动 ISMS 项目的批准

5.1 获得管理者对启动 ISMS 项目的批准的概要

当决定实施 ISMS 时，宜考虑若干因素。为了强调这些因素，管理者宜了解 ISMS 实施项目的业务案例并批准它。因此该阶段的目标是：

目标： 通过定义业务案例和项目计划来获得管理者对启动 ISMS 项目的批准。

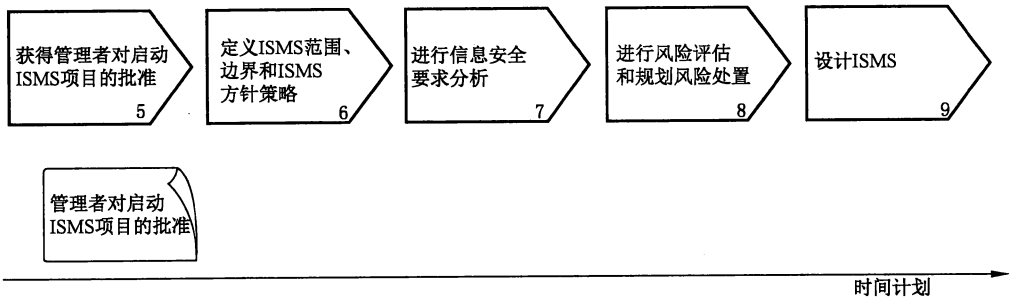
为了获得管理者的批准，组织宜创建业务案例。该业务案例除了包括实施 ISMS 的组织结构之外，还包括实施一个 ISMS 的优先级和目标。组织还宜创建初步的 ISMS 项目计划。

这一阶段所执行的工作将使组织能够了解 ISMS 的相关事宜，并使组织能够阐明 ISMS 项目所需要的组织内信息安全角色和责任。

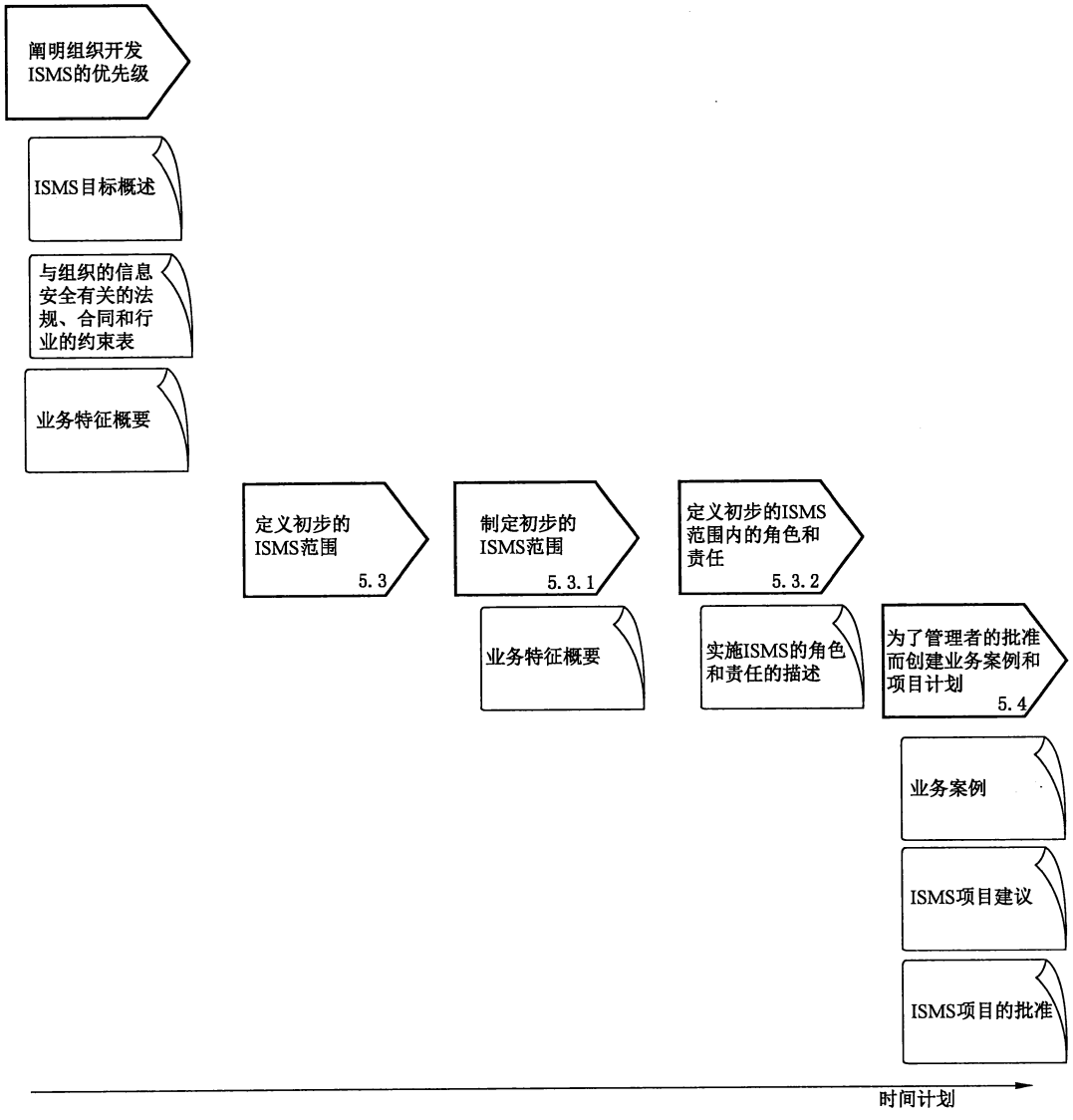
这一阶段的预期输出是，就 ISMS 的实施以及执行本标准所描述的活动，获得管理者的初步批准和承诺。本章的可交付项包括业务案例和一个具有关键里程碑的 ISMS 项目计划草案。

图 3 示出获得管理者对启动 ISMS 项目的批准过程。

第 5 章的输出（对计划和实施一个 ISMS 的文档化管理承诺）和第 7 章的输出（信息安全状况的概述文档），它们并不是 GB/T 22080—2008 的要求。但是，建议这些活动的输出作为本标准所描述的其他活动的输入。



a)



b)

图 3　获得管理者对启动 ISMS 项目的批准的概览

5.2　阐明组织开发 ISMS 的优先级

活动

在考虑组织的信息安全优先级和要求时，宜将实施 ISMS 的目的一并考虑。

输入

a) 组织的战略目标；

b) 现有管理体系概要；

c) 可用于组织的法律法规、规章和合同上的信息安全要求清单。

指南

启动 ISMS 项目，通常需要管理者的批准。因此，宜执行的第一个活动是收集那些对组织可显示 ISMS 价值的相关信息。组织宜阐明需要 ISMS 的原因，并决定 ISMS 实施的目标，启动 ISMS 项目。

实施 ISMS 的目标可通过回答以下问题来决定：

a) 风险管理——ISMS 如何产生更好地管理信息安全风险？

b) 效率——ISMS 如何能改进信息安全的管理？

c) 业务优势——ISMS 如何能为组织创造竞争优势？

为回答上述问题，尽可能通过以下因素来阐明组织的安全优先级和要求：

a) 关键的业务域和组织域：

1) 关键业务域和关键组织域是什么？

2) 组织哪些域提供该业务以及关注什么？

3) 有什么第三方关系及其协议？

4) 是否有外包服务？

b) 敏感信息或有价值的信息：

1) 什么信息对组织是至关重要的？

2) 如果某些信息被泄露给未授权方，可能产生什么后果（例如，失去竞争优势、损害品牌或名誉、引起法律诉讼等）？

c) 对信息安全测量有要求的相关法律：

1) 什么法律适用于组织的风险处置或信息安全？

2) 组织是否是必须对外进行财务报告的公众性全球性组织的一部分？

d) 与信息安全有关的合同协议或组织协议：

1) 对数据存储的要求（包括保留期限）是什么？

2) 是否有任何与隐私或质量有关的合同要求（例如，服务级别协议——SLA）？

e) 规定特定信息安全控制措施的行业要求：

1) 有哪些行业特定的要求适用于组织？

f) 威胁环境：

1) 需要什么类型的保护，及需要应对哪些威胁？

2) 需要保护的信息的特定类别是什么？

3) 需要保护的信息活动的特定类型是什么？

g) 竞争动力：

1) 对信息安全的最小化市场要求是什么？

2) 哪些另外的信息安全控制措施可为组织提供竞争优势？

h) 业务持续性要求：

1) 关键业务过程是什么？

2) 对每个关键业务过程而言，组织能够容忍其中断的时间是多长？

通过回答上述问题，可以确定初步的 ISMS 范围。并且这对创建要得到管理者批准的业务案例和实施 ISMS 的计划是需要的。详细的 ISMS 范围将在 ISMS 项目期间予以定义。

GB/T 22080—2008 4.2.1 a)中所提及的要求，从业务、组织、位置、资产和技术等方面特点，概要描述了范围。以上所产生的信息支持 ISMS 范围的确定。

在做出 ISMS 范围的初步决定时，宜考虑一些主题，具体包括：

a) 组织管理者对建立信息安全管理的指示及外部对组织的强制性义务是什么？

b) 建议的范围内系统的责任是否由不止一个管理团队(例如，不同的分支机构或不同的部门)承担？

c) ISMS 相关文档在整个组织如何流通(例如，通过纸质文件或者通过公司内联网)？

d) 当前的管理体系是否能支持组织的需求？是否得到充分运行、良好维护且如预期般发挥作用？

管理者目标可作为确定 ISMS 初步范围的输入，举例如下：

a) 促进业务持续性和灾难恢复；

b) 提高事件恢复的能力；

c) 解决法律/合同的符合性/义务；

d) 使能够获得其他 ISO/IEC 标准的认证；

e) 使组织能够发展和占据优势地位；

f) 降低安全控制措施的成本；

g) 保护具有战略价值的资产；

h) 建立一个健康的、有效的内部控制环境；

i) 向利益相关方保证信息资产获得适当保护。

输出

本活动的可交付项是：

a) 概述 ISMS 的目标、信息安全优先级和组织要求的文档；

b) 与组织的信息安全相关的法律法规、规章、合同和行业的要求清单；

c) 业务、组织、位置、资产和技术等方面的概要特征。

其他信息

ISO/IEC 9001:2008，ISO/IEC 14001:2004，ISO/IEC 20000-1:2005。

5.3 定义初步的 ISMS 范围

5.3.1 制定初步的 ISMS 范围

活动

为实现 ISMS 的目标，宜定义初步的 ISMS 范围。

输入

5.2(阐明组织开发 ISMS 的优先级)活动的输出。

指南

为了执行 ISMS 实施项目，宜定义组织实施 ISMS 的结构。现在宜定义初步的 ISMS 范围，以便给管理者提供实施决策指南，以及支持进一步的活动。

初步的 ISMS 范围对于创建业务案例和建议的项目计划以获得管理者的批准而言，是必需的。

本阶段的输出是一份定义初步 ISMS 范围的文档，内容包括：

a) 组织的管理者对信息安全管理的指示概述，以及外部施加于组织的义务；

b) ISMS 范围内的区域如何与其他管理体系交互的描述；

c) 信息安全管理的业务目标清单(见 5.2)；

d) ISMS 将被应用的关键业务过程、系统、信息资产、组织结构和地理位置的清单；

e) 现有管理体系、规章、符合性和组织目标之间的关系；

f) 业务、组织、位置、资产和技术等方面的特点。

宜识别现有管理体系与被提议的 ISMS 的过程间的共同要素和运行差异。

输出

可交付项是一份描述初步的 ISMS 范围的文档。

其他信息

无其他特定信息。

注：宜特别注意的是，不论组织内已有的管理体系如何，都要满足 GB/T 22080—2008 关于 ISMS 范围的认证特定文件的要求。

5.3.2 定义初步的 ISMS 范围内的角色和责任

活动

宜定义初步的 ISMS 范围的全部角色和责任。

输入

a) 5.3.1(制定初步的 ISMS 范围)活动的输出；

b) 将从 ISMS 项目结果获益的利益相关方清单。

指南

为了执行 ISMS 项目，宜确定组织在该项目中的角色。因为每个组织中处理信息安全的人数不同，所以一般来说，每个组织的角色通常也不同。信息安全的组织结构和资源随着组织的规模、类型和组织结构的变化而变化。例如，在小型组织中，若干角色可由同一个人担任。然而，管理者宜明确识别负责整个信息安全管理的角色(典型的是首席信息安全官、信息安全管理者或类似的)。宜基于工作岗位所需要的技能来分配员工的角色和责任。这对于确保任务被有效地和有力地完成至关重要。

在定义信息安全管理角色时，最重要的考虑事项是：

a) 该任务的总体责任由管理者承担；

b) 指定一个人(通常是首席信息安全官)来促进和协调信息安全过程；

c) 每个员工对其最初任务与维护工作场所和组织中的信息安全负有同等责任。

管理信息安全的角色宜一起工作；这可通过诸如信息安全论坛或类似机构来促进。

在制定、实施、运行和维护 ISMS 的所有阶段，宜与适当的业务专家进行协作。

已确定范围内(诸如风险管理)各部门代表是潜在的 ISMS 实施组成员。为快速、有效地使用资源，该组宜保持最小的实际规模。这些区域不仅有 ISMS 范围所直接包含的部门，还有间接包含的部门，诸如法律部门、风险管理部门和行政管理部门。

输出

可交付项是一个描述角色和责任的文档或表格，带有对于成功实施 ISMS 所需要的名称和组织。

其他信息

附录 B 提供了组织成功实施 ISMS 所需要的角色和责任的详细情况。

5.4 为了管理者的批准而创建业务案例和项目计划

活动

宜通过创建业务案例和 ISMS 项目建议，来获得管理者对 ISMS 实施项目所需资源的批准和承诺。

输入

a) 5.2(阐明组织开发 ISMS 的优先级)活动的输出；

b) 5.3(定义初步的 ISMS 范围)活动的输出——已形成的文档：初步的

1) ISMS 范围；

2) 相关的角色和责任。

指南

关于业务案例和初始 ISMS 项目计划的信息宜包括已估算的时间计划、资源，以及本标准第 6 章～第 9 章所述的主要活动所需要的里程碑。

业务案例和初始的 ISMS 项目计划不仅是该项目的基础，而且也确保管理者对 ISMS 实施所需资源的承诺和批准。已实施的 ISMS 支持业务目标的方式，促进了组织过程的有效性，提高了业务效率。

实施 ISMS 的业务案例宜包括与组织目标有联系的简短声明，并涵盖以下主题：

a) 目的和特定目标；

b) 组织的利益；

c) 初步的 ISMS 范围，包括受影响的业务过程；

d) 实现 ISMS 目标的关键过程 & 因素；

e) 高层级项目概要；

f) 初始的实施计划；

g) 已定义的角色和责任；

h) 需要的资源(包括技术和人员两方面)；

i) 实施考虑事项，包括现有的信息安全；

j) 带有关键里程碑的时间计划；

k) 预期的成本；

l) 关键的成功因素；

m) 组织利益的量化。

项目计划宜包括第 6 章～第 9 章所述的各个阶段的相关活动。

影响 ISMS 或受 ISMS 影响的个人宜进行识别，并允许其有充分的时间对 ISMS 业务案例和 ISMS 项目建议进行评审和提出意见。业务案例和 ISMS 项目建议宜在得到输入后按需更新。一旦获得足够的支持，宜将业务案例和 ISMS 项目建议呈送管理者以获得其批准。

管理者宜批准业务案例和初始的项目计划，以实现整个组织的承诺并开始执行 ISMS 项目。

从管理者承诺实施 ISMS 便可获得的期望利益是：

a) 由于知悉相关法律法规、规章、合用义务和信息安全标准，并加以实施，从而避免了不遵从的负债和处罚；

b) 信息安全多个过程的有效使用；

c) 通过信息安全风险的更好管理，提高了稳定性和信心；

d) 关键业务信息的识别和保护。

输出

本活动的可交付项是：

a) 一份管理者批准的以分配的资源执行 ISMS 项目的文档；

b) 一份业务案例文档；

c) 初始的 ISMS 项目建议，具有执行风险评估、实施、内部审核和管理评审等里程碑。

其他信息

GB/T 22080—2008 中支持 ISMS 业务案例的关键成功因素的例子。

6 定义 ISMS 范围、边界和 ISMS 方针策略

6.1 定义 ISMS 范围、边界和 ISMS 方针策略的概述

管理者对实施 ISMS 的批准是基于初步的 ISMS 范围、ISMS 业务案例和初始的项目计划。ISMS 的范围和边界的详细定义、ISMS 方针策略的定义及管理者的认可与支持，是成功实施 ISMS 的关键因素。图 4 给出了定义 ISMS 范围、边界和 ISMS 方针策略的概述。

因此，本阶段的目标是：

目标： 定义详细的 ISMS 范围和边界、制定 ISMS 方针策略，并获得管理者的赞同。 见 GB/T 22080—2008 的 4.2.1 a)和 4.2.1 b)

为了实现“定义详细的 ISMS 范围和边界”的目标，有必要进行以下活动：

a) 定义组织的范围和边界；

b) 定义信息通信技术(ICT)的范围和边界；

c) 定义物理范围和边界；

d) 确定 GB/T 22080—2008 的 4.2.1 a)和 4.2.1 b)中所规约的范围和边界内业务、组织、位置、资产和技术方面的特征，并确定在定义这些范围和边界过程中的方针策略；

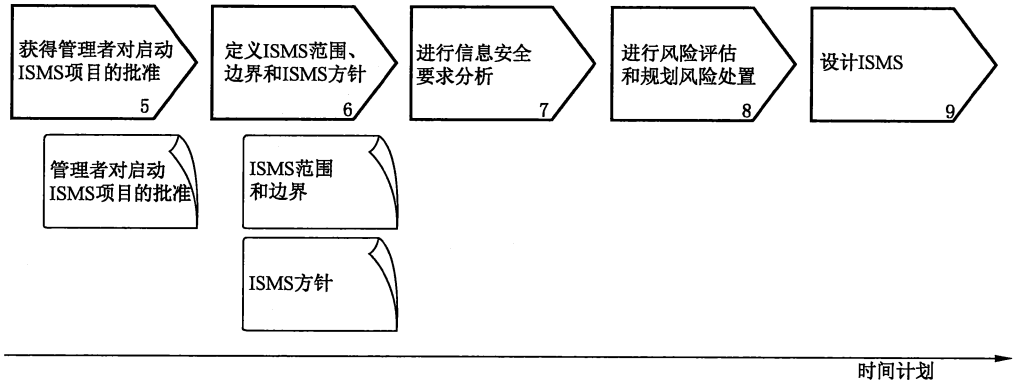
e) 集成这些基础性的范围和边界，以获得 ISMS 的范围和边界。

为了完成 ISMS 方针策略的定义并获得管理者的认可，必须进行一个活动。

为了在组织中构建一个有效的管理体系，宜通过考虑组织的关键信息资产来确定详细的 ISMS 范围。为了标识信息资产和评估可行的安全机制，使有共同的术语和系统化方法是非常重要的。这使得在所有实施阶段中容易沟通，培养一致的理解。确保关键的组织域被包含在该范围之内，也是很重要的。

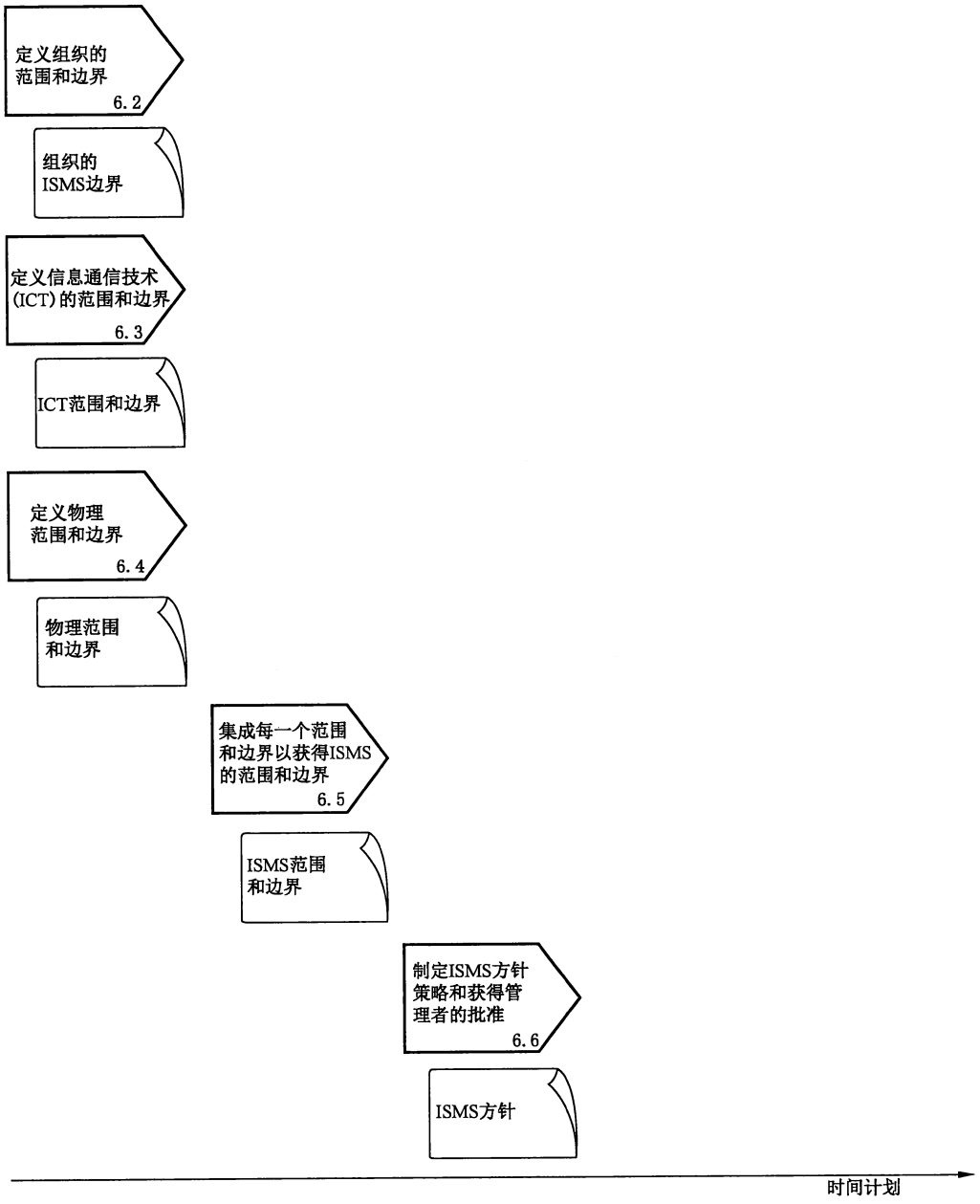
可以把整个组织定义为 ISMS 的范围，或者把组织的一部分，诸如一个部门或一个边界清楚的组织元素，定义为 ISMS 的范围。例如，在为顾客提供“服务”的情况下，ISMS 的范围可以是某种服务，或者是跨越职能的管理体系(整个部门或部门的一部分)。对于认证而言，不管现有的管理体系在组织内情况如何，均宜满足 GB/T 22080—2008 的要求。

定义组织的范围和边界、ICT 范围和边界(6.3)以及物理范围和边界(6.4)，并不总是按一定顺序来完成之。然而，在定义其他范围和边界时，可参照已经获得的范围和边界。



a)

图 4 定义 ISMS 范围、边界和 ISMS 方针策略的概述



b)

图 4 （续）

6.2 定义组织的范围和边界

活动

宜定义组织的范围和边界。

输入

a) 5.3(定义初步的 ISMS 范围)活动的输出——文档化的初步的 ISMS 范围，它涉及：

1) 现有的管理体系、规章、符合性和组织目标之间的关系；

2) 业务、组织、位置、资产和技术等方面的特征。

b) 5.2(阐明组织开发 ISMS 的优先级)活动的输出——管理者有关实施 ISMS 并开始该项目的

批准文件，其中包含所分配的必需资源。

指南

实施 ISMS 的工作量取决于其应用范围的大小。这也影响到与维护 ISMS 范围内各客体（诸如过程、物理位置、IT 系统和人员）的信息安全有关的所有活动，包括实施和维护控制措施、管理运行和诸如识别信息资产和评估风险等任务。如果管理者决定把组织的某些部分从 ISMS 的范围中排除出去，那么宜把这样做的理由写成文件。

在定义 ISMS 的范围时，重要的是对于那些未包含于定义中的人，可以把 ISMS 边界解释得非常清楚。

一些与信息安全有关的控制措施，可能已经作为其他管理体系的结果而存在。在规划 ISMS 时，宜考虑这些控制措施，但不必指出当前的 ISMS 范围的边界。

一个定义组织边界的方法是，标识那些相互不重叠的责任域，以便易于赋予组织内的可核查性。

直接与信息资产相关的责任或直接与 ISMS 范围内所包括的业务过程相关的责任，宜选作为处于 ISMS 控制下的组织的一部分。当定义组织的边界时，宜考虑以下因素：

a) ISMS 管理论坛宜由 ISMS 范围所直接涉及的管理人员组成；

b) ISMS 的管理成员，宜是最终负责所有受影响的责任域的人员（即，他们的角色通常由其所跨越的控制措施和责任指定的）；

c) 在负责管理 ISMS 的角色不是高层管理者的情况下，高层发起人基本代表对信息安全的利益，并在组织的最高层起到 ISMS 倡导者的作用；

d) 范围和边界需要予以定义，以确保考虑了风险评估中所有相关的资产，确保强调了可能发生于这些边界上的风险。

基于这一途径，所分析的组织边界宜标识受 ISMS 影响的所有人员，他们宜包含在 ISMS 范围内。人员的标识，可能依赖于所选择途径，可能关联到过程和功能。如果该范围内的某些过程外包给第三方，那么这些依赖就宜清楚地写入相应的文档之中。在 ISMS 实施项目中，这样的依赖以后还要做进一步分析。

输出

本活动的可交付项是：

a) 组织的 ISMS 边界的描述，包括被排除在 ISMS 范围之外组织任何部分的正当理由；

b) 在 ISMS 范围内那些组织各部分的功能和结构；

c) 在该范围内交换的信息和通过边界交换的信息的标识；

d) 在该范围之内和范围之外的信息资产的组织过程和责任；

e) 有关做出层次化决策的过程，及其在 ISMS 内的结构。

其他信息

没有其他特定信息。

6.3 定义信息通信技术（ICT）的范围和边界

活动

宜定义 ISMS 所覆盖的信息通信技术（ICT）元素和其他技术项的范围和边界。

输入

a) 5.3（定义初步的 ISMS 范围）活动的输出——初步的 ISMS 范围的文件；

b) 6.2（定义组织的范围和边界）活动的输出。

指南

ICT 范围和边界的定义可通过一种信息系统的途径来获得(而不是基于 IT 技术)。一旦管理者决定把信息系统的业务过程归入 ISMS 范围,那么还宜考虑所有相关的 ICT 元素。这包括存储、处理或传输关键信息、资产的组织的所有部分,或者包括范围内对这些组织部分是至关重要的其他元素。信息系统可能跨越组织边界或国家边界。在这种情况下,宜考虑以下事宜:

a) 社会与文化的环境;

b) 适用于组织的法律法规、规章和合同的要求;

c) 关键责任的可核查性;

d) 技术约束(例如,可用的带宽和服务的可用性等)。

通过以上考虑,ICT 边界宜包括以下事宜的描述(在适用时):

a) 组织负责管理的通信基础设施,其中包括采用各种不同的技术(例如无线网络、有线网络或数据/语音网络);

b) 组织使用和控制的组织边界内的软件;

c) 网络、应用或生产系统所需要的 ICT 硬件;

d) 有关 ICT 硬件、网络和软件的角色和责任。

如果上述任何一个或多个事宜不由组织控制,那么就宜建立第三方依赖关系的文档,见 6.2 的指南。

输出

本活动的可交付项是:

a) 在范围内交换的信息和跨越边界交换的信息;

b) ISMS 的 ICT 边界,包括对任何被排除在 ISMS 范围之外、但在组织管理之下的 ICT,给出正当性理由;

c) 信息系统和电子通讯网络,描述什么系统在范围内,并描述对这些系统的角色和责任。对范围之外的系统宜给出简要概述。

其他信息

没有其他特定信息。

6.4 定义物理范围和边界

活动

宜定义由 ISMS 所覆盖的物理范围和边界。

输入

a) 5.3 (定义初步的 ISMS 范围)活动的输出——ISMS 初始范围文件;

b) 6.2 (定义组织的范围和边界)活动的输出;

c) 6.3 (定义信息通信技术(ICT)的范围和边界)活动的输出。

指南

物理范围和边界的定义,包括标识组织(宜属于 ISMS 的各部门)内的建筑物、位置或设施。对于跨越物理边缘的信息系统的处理,这就更复杂一些,因为这样的系统需要:

a) 远程设施;

b) 与客户信息系统的接口以及与第三方服务商所提供服务的接口;

c) 适用的适当接口和服务水准。

基于上述考虑,物理边界宜包括以下描述(在适用时):

a) 描述功能或过程，其中考虑了它们的物理位置以及组织控制它们的范围；

b) 基于 ICT 边界的覆盖范围，描述用于储存/容纳 ICT 硬件或范围内数据的特殊设施。

如果上述描述的任何事物不受组织控制，那么就宜形成第三方依赖关系文档。见 6.2 的“指南”。

输出

本活动的可交付项是：

a) ISMS 物理边界的描述，包括对排除在 ISMS 范围之外的组织管理之下、又被排除在物理边界之外的任何过程和功能以及设备，给出正当性理由；

b) 与该范围有关的组织及其地理特征的描述。

其他信息

没有其他特定信息。

6.5 集成每一个范围和边界以获得 ISMS 的范围和边界

活动

宜通过集成每一个范围和边界来获得 ISMS 的范围和边界。

输入

a) 5.3(定义初步的 ISMS 范围)活动的输出——初步的 ISMS 范围的文件；

b) 6.2 (定义组织的范围和边界)活动的输出；

c) 6.3(定义信息通信技术(ICT)的范围和边界)活动的输出；

d) 6.4(定义物理范围和边界)活动的输出。

指南

可以采用很多方式来描述 ISMS 的范围并证明其正当性。例如，可以选择诸如数据中心或办公室的物理位置，并列出一些关键过程；其中每一个关键过程均涉及一些之外的域，而该数据中心就可使这些之外的域成为范围之内的域。这样的关键过程，例如就可以移动访问一个中心信息系统。

输出

本活动的可交付项是描述 ISMS 范围和边界的文件，包含以下信息：

a) 组织的关键特征(其功能、结构、服务、资产以及每项资产责任的范围和边界)；

b) 范围内的组织过程；

c) 范围内设备和网络的配置；

d) 范围内信息资产的初步清单；

e) 范围内 ICT 资产(例如服务器)清单；

f) 范围内各场所位置图，该图指出 ISMS 的物理边界；

g) ISMS 范围内的角色和责任的描述及其它们之间的关系和组织结构；

h) 任何被排除在 ISMS 范围之外的东西的详细说明及其正当理由。

其他信息

没有其他特定信息。

6.6 制定 ISMS 方针策略和获得管理者的批准

活动

宜制定 ISMS 方针策略并获得管理者的批准。

输入

a) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界

的文件；

b) 5.2(阐明组织开发 ISMS 的优先级)活动的输出——实施 ISMS 的目标的文件；

c) 5.4(为了管理者的批准而创建业务案例和项目计划)活动的输出——以下事宜的文件：

1) 组织的要求和信息安全优先级；

2) 初始的 ISMS 实施项目计划，里面有里程碑，诸如执行风险评估、实施、内部审核和管理评审。

指南

在定义 ISMS 方针策略时，宜考虑以下方面：

a) 基于组织的要求和信息安全优先级，建立 ISMS 目标；

b) 为达到 ISMS 目标，建立一般性的关注和动作指南；

c) 考虑组织的信息安全要求、法律法规或规章，以及合同义务；

d) 组织内风险管理语境；

e) 建立评价风险(见 GB/T 31722—2015)和定义风险评估结构的准则；

f) 阐明高层管理者对 ISMS 的责任；

g) 获得管理者的批准。

输出

可交付项是描述经管理者批准的 ISMS 方针策略的文件。该文件宜在 ISMS 项目后期的一个阶段重新予以证实，因此它依赖于风险评估的输出。

其他信息

GB/T 31722—2015 所提供的关于评价风险的准则的附加信息。

7 进行信息安全要求分析

7.1 进行信息安全要求分析的概述

对组织当前状况进行分析是重要的，因为在实施 ISMS 时，需要考虑现有的要求和信息资产。基于效率和实践性原因，本阶段所描述的活动大体上可与第 6 章描述的活动同时进行。图 5 给出了信息安全要求阶段的概览信息。

目标： 定义要通过 ISMS 来支持的有关要求，标识信息资产，并获得范围内当前信息安全的状况。 见 GB/T 22080—2008:4.2.1 c) 1) 部分，4.2.1 d)，4.2.1 e)

通过信息安全分析所收集的信息，宜：

a) 为管理者提供一个起点(即正确的基本数据)；

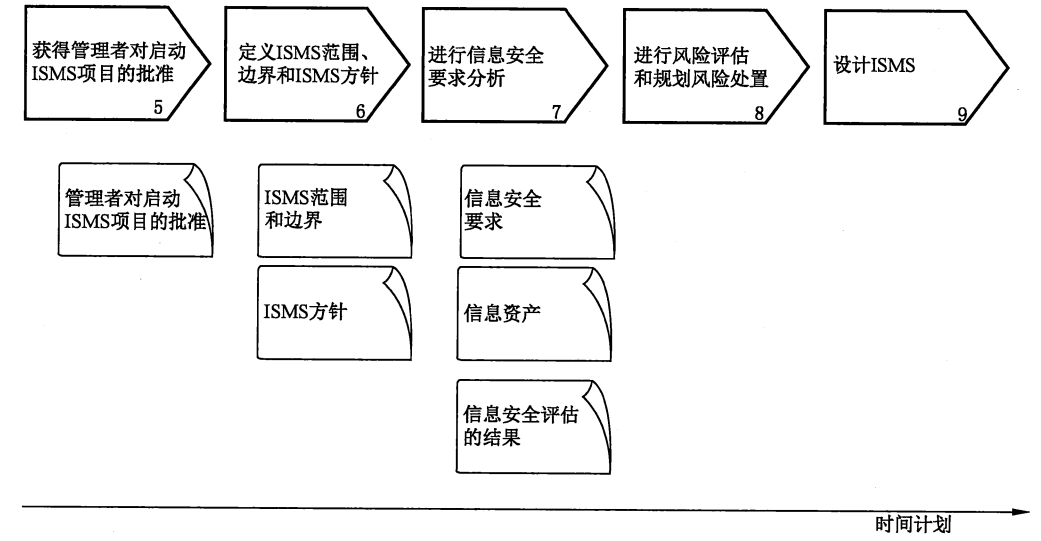
b) 标识实施 ISMS 的条件并形成文件；

c) 提供一份清晰并已很好理解的组织设施；

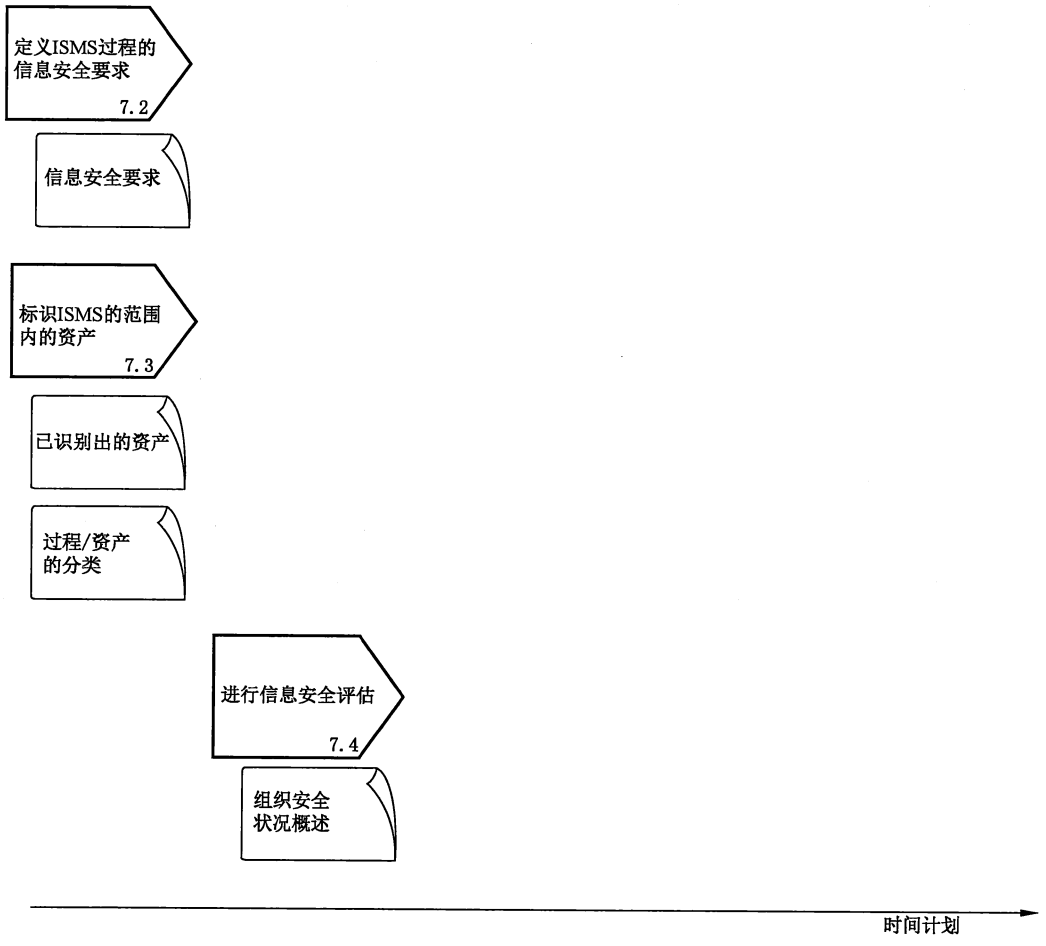
d) 考虑组织的特殊情况和状态；

e) 标识所期望的信息保护水平；

f) 在所提议的实施范围内，确定企业部分或企业全部所需的信息编辑。



a)



b)

图 5　进行信息安全要求阶段的概览

7.2 定义 ISMS 过程的信息安全要求

活动

宜分析和定义 ISMS 过程的详细信息安全要求。

输入

a) 5.2(阐明组织开发 ISMS 的优先级)活动的输出——其文件：
   1) 概述 ISMS 的目标、信息安全优先级和组织的要求；
   2) 与组织的信息安全有关的规章、合同和行业的约束表。
b) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界；
c) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略。

指南

第一步要求收集 ISMS 的所有支持性信息。对于每一个组织过程和专家任务，均需要根据信息的关键性(即所要求的保护程度)做出一个决定。很多内部条件都可能影响信息安全，因此宜确定这些内部条件。在这一阶段的初期，详细描述信息技术并不是重要的。为了分析一个组织过程及其关联的 ICT 应用和系统，对所需信息应有一个基本概括。

组织过程的分析提供了信息安全事件对组织活动影响的陈述。在很多情况下，组织过程分析充分依赖组织过程的基本描述。如果过程、功能、位置、信息系统和通信网络尚未作为 ISMS 范围的一部分，那么它们就需要加以标识并形成文档。

为了获得 ISMS 的详细信息安全要求，宜强调以下工作：

a) 初步标识重要的信息资产及其当前的信息安全保护；
b) 标识组织的愿景，并确定所标识的愿景对未来信息处理要求的影响；
c) 分析信息处理、系统应用、通信网络、活动场所和 IT 资源等的当前形式；
d) 标识所有的基本要求(例如，法律法规和规章的要求、合同义务、组织要求、行业标准、客户和供应商协议和保险条件等)；
e) 标识信息安全了解的程度，并由此针对每一个运行和管理单位，导出相应的培训和教育要求。

输出

本活动的可交付项是：

a) 主要过程、功能、位置、信息系统和通信网络的标识；
b) 组织的信息资产；
c) 关键过程/资产的分类；
d) 由组织的法律法规、规章和合同的要求而导出的信息安全要求；
e) 作为安全要求的结果而加以强调的众所周知的脆弱性清单。

其他信息

没有其他特定信息。

7.3 标识 ISMS 范围内的资产

活动

宜标识 ISMS 所支持的资产。

输入

a) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界；
b) 6.6(制定 ISMS 方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略；

c) 7.2(定义 ISMS 过程的信息安全要求)活动的输出。

指南

为了标识 ISMS 范围内的资产,宜标识并列出以下信息:

a) 过程的唯一名称;

b) 过程描述及其所关联的活动(创建、存储、传输和删除);

c) 过程对组织的至关重要性(关键的、重要的和支持性的);

d) 过程责任人(组织部门);

e) 提供输入的过程以及这一过程的输出;

f) 支持过程的 IT 应用;

g) 信息分类(保密性、完整性、可用性、访问控制、不可否认性,和/或对组织有用的其他重要特性,例如,信息可能保存的时间)。

输出

本活动的可交付项是:

a) 在 ISMS 范围内组织的主要过程中所标识的信息资产;

b) 关键过程和信息资产的信息安全分类。

其他信息

没有其他特定信息。

7.4 进行信息安全评估

活动

宜通过组织期望的目标与组织当前信息安全状况的比较,来执行信息安全评估。

输入

a) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界;

b) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略;

c) 7.2(定义 ISMS 过程的信息安全要求)活动的输出;

d) 7.3(标识 ISMS 范围内的资产)活动的输出。

指南

信息安全评估是标识现有的信息安全水平(即组织当前处理信息保护的规程)的活动。信息安全评估的基本目的是,以策略和指南形式,为管理体系提供所需要的支持性描述信息。当然,必须确保已标识的缺陷能够通过一个具有优先级的纠正措施计划予以并行处理。所有相关方均宜熟悉组织分析的结果、标准文档,并要访问适当的管理人员。

信息安全评估通过使用以下信息:

a) 基于关键过程来研究的背景事实;

b) 信息资产分类;

c) 组织的信息安全要求。

分析了组织的当前状况,并确定了信息安全的当前状态,建立了脆弱性文件。

信息安全评估的结果以及组织目标,常常是激发未来信息安全工作的一个重要部分。信息安全评估宜由相对独立于组织的内部资源或外部资源来执行。

信息安全评估的参与者宜包括很了解当前环境、条件,并了解信息安全相关事物的个体。宜挑选这些个体来代表组织的方方面面,包括:

a) 在岗管理人员(例如,组织单位的领导);

b) 过程责任人(即,代表重要的组织域);

c) 对当前环境、条件和信息安全具有很强知识的其他人员。例如，业务过程用户、运行管理职能部门和法律部门的人员。

对于一个成功的信息安全评估而言，采取以下措施是重要的：

a) 标识和列出相关的组织标准(例如，GB/T 22080—2008)；

b) 标识已知的控制要求，这些控制要求一般出现在策略、法律法规和规章的要求、合同义务、过去审核的发现或过去执行的风险评估的发现中；

c) 使用上述这些作为基准文档，以便针对组织信息安全水平，做出当前要求的粗略估算。

宜考虑把所做出的优先级和组织分析结合一起，构成安全预防和检查(控制措施)的基础。

进行信息安全评估的途径如下：

a) 选择涉及信息安全要求的重要组织业务过程和过程步骤；

b) 创建一个涵盖组织主要过程的综合流程图，包含基础设施(逻辑的和技术的)，如果这在组织分析期间尚未给出或执行的话；

c) 与适当的关键人员讨论并分析与信息安全要求有关的组织当前状况。例如哪些过程是关键的，它们当前起怎样的作用？(其结果随后用于以后的风险评估)

d) 通过将现有的控制措施与先前所标识出的控制要求进行比较，确定现有控制措施的缺陷；

e) 完善当前状况，并形成相应文档。

输出

本活动的可交付项是：

概述评估出的组织安全状况以及评价出的脆弱性的一个文档。

其他信息

本阶段进行的信息安全评估仅交付有关组织信息安全状况和脆弱性的初步信息，因为有关信息安全方针策略和标准的完整信息将在以后阶段开发(见第9章)，且尚未进行风险评估。

8 进行风险评估和规划风险处置

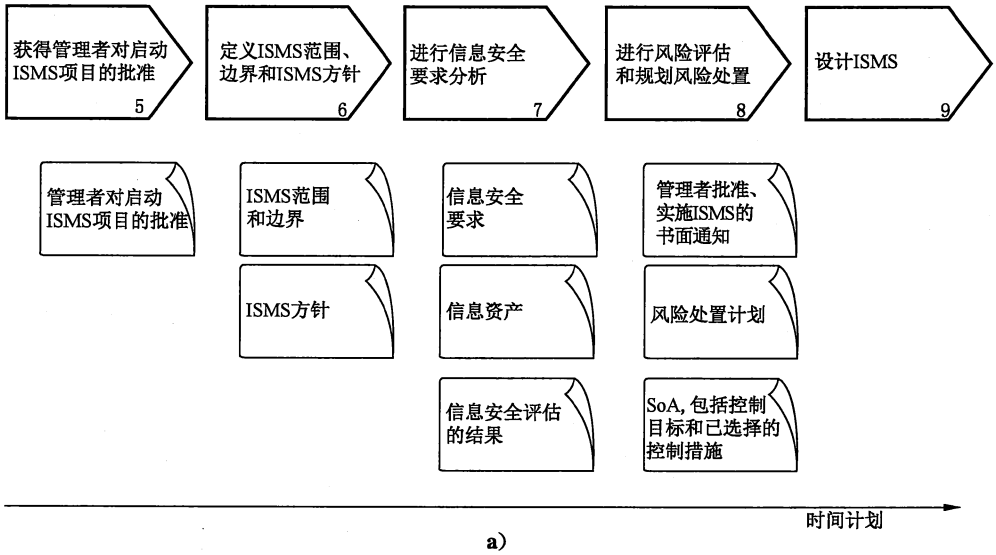
8.1 进行风险评估和规划风险处置的概述

ISMS的实施宜关注相关的信息安全风险。风险的标识、评价和有计划的处理，以及控制目标和控制措施的选择，都是ISMS实施的重要步骤，宜在本阶段予以处理。图6给出了风险评估阶段的概览信息。

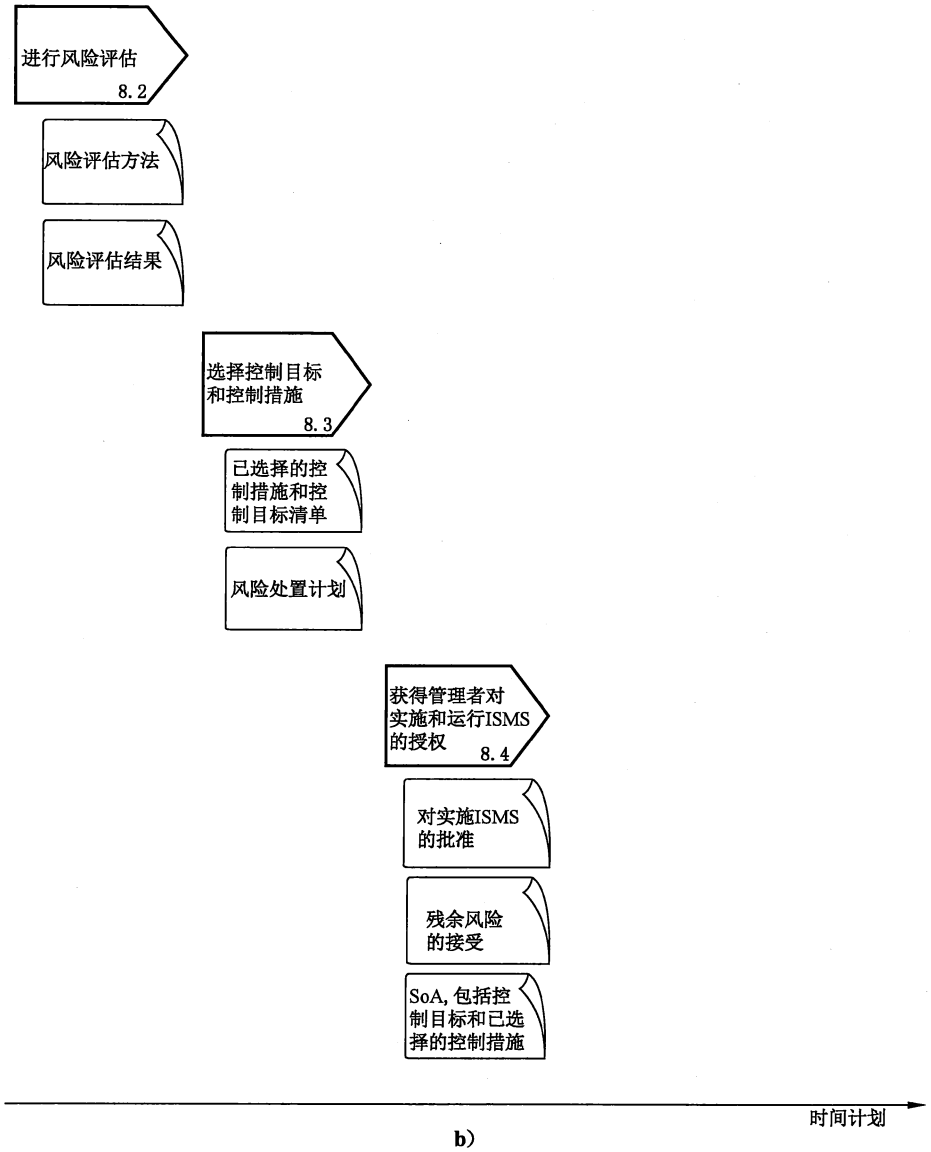
GB/T 31722—2015提供专门的信息安全风险管理指南，其内容宜在整个第8章中予以参照。

进行风险评估的前提是，管理者已承诺实施ISMS，已定义了ISMS的范围和ISMS的方针策略，已了解信息资产；而进行风险处置规划的前提是，已得到信息安全评估的结果。

目标： 定义风险评估方法，标识、分析和评价信息安全风险，以便选择风险处置措施以及选择控制目标和控制措施。 见GB/T 22080—2008:4.2.1 c)～4.2.1 j)



a)



b)

图 6　风险评估阶段的概览

8.2 进行风险评估

活动

宜执行风险评估。

输入

a) 第7章(进行信息安全要求分析)活动的输出——关于以下事宜的信息：
   1) 信息安全状况概述；
   2) 已识别出的信息资产。
b) 第6章(定义ISMS范围、边界和ISMS的方针策略)活动的输出——关于以下事宜的文件：
   1) ISMS的范围；
   2) ISMS的方针策略。
c) GB/T 31722—2015。

指南

在ISMS范围所支持的业务语境内，安全风险评估的好与坏(绩效)主要是看是否符合GB/T 22080—2008，并成功地实施了ISMS。风险评估宜：

a) 标识威胁及其来源；
b) 标识现有的和要计划的控制措施；
c) 标识可为威胁利用而造成对资产或组织损害的脆弱性；
d) 标识资产损失保密性、完整性、可用性、不可否认性以及资产损失其他信息安全要求所产生的后果；
e) 评估可能来自预期的或实际的信息安全事件所产生的业务影响；
f) 评估安全事件场景的可能性；
g) 估算风险的级别；
h) 按风险评价准则和风险接受准则，比较风险的级别。

参与风险评估的人员，宜包括那些具有很好组织目标的知识，并很了解安全的人员(例如，对组织目标的当前威胁具有良好洞察力)。宜挑选能广泛代表组织方方面面的人员。参见附录B。

组织可以采用项目特定标准、公司特定标准或行业特定标准的风险评估方法。

输出

本活动的可交付项是：

a) 风险评估方法的描述；
b) 风险评估结果。

其他信息

附录B——有关角色和责任的信息。

注：安全事件场景是对一个威胁的描述，其中该威胁在信息安全事件中利用了某种脆弱性或一组脆弱性。GB/T 22080—2008把安全事件场景的出现描述为“安全故障”。(见GB/T 22080—2008)

8.3 选择控制目标和控制措施

活动

宜标识风险处置的可选措施，并宜按已标识的风险处置可选措施来标识要选择的适当控制措施。

输入

a) 8.2(进行风险评估)活动的输出——风险评估结果；
b) GB/T 31722—2015；

c) GB/T 22081—2008。

指南

重要的是规约风险与已选择的处置风险可选措施之间的关系(例如,风险处置计划),因为这将提供风险处置的一个概要。可能的风险处置可选措施在所见的 GB/T 22081—2008 的 4.2.1 f)中列出。

GB/T 22081—2008 的附录 A 可为风险处置用来选择控制目标和控制措施。如果在该附录 A 中没有适用的控制目标或控制措施,就宜规约附加的控制目标和控制措施并使用之。重要的是,要按风险处置计划的要求,演示证明所选择的控制措施将如何缓解风险。

GB/T 22081—2008 附录 A 所给出的数据并不意味着是完备无缺的。可标识特定于部门的控制措施,以支持业务及 ISMS 的特殊需求。

在风险降低的情况下,管理每一个风险与已选择的控制目标和控制措施之间的关系,有利于设计 ISMS 的实施。它可加到描述风险与所选择的风险处置可选措施之间关系的列表中。

为了便于审核,组织宜编制一个控制措施表,其中列出已选择的、并适用于组织 ISMS 的控制措施。通过提供现有控制措施概述,这对改进诸如外包等业务关系具有一些额外的好处。

重要的是,要意识到概述的控制措施极有可能包含一些敏感信息。因此,当做出可用于内部和外部人员的控制措施概述时,宜适当注意这一情况。实际上,考虑把所生成的信息作为在定义资产期间创建 ISMS 的一部分,这可能是合适的。

输出

本活动的可交付项是:

a) 已选择的控制措施和控制目标的清单;

b) 具有以下内容的风险处置计划:

1) 风险与已选择的风险处置可选措施之间的关系描述;

2) 风险与已选择的控制目标和控制措施之间的关系描述(特别是在风险降低的情况下)。

其他信息

GB/T 22081—2008。

8.4 获得管理者对实施和运行 ISMS 的授权

活动

宜获得管理者对实施 ISMS 的批准,并形成残余风险接受文件。

输入

a) 5.4(为了管理者的批准而创建业务案例和项目计划)活动的输出——管理者对 ISMS 项目的初始批准;

b) 第 6 章(定义 ISMS 的范围、边界和 ISMS 的方针策略)活动的输出——以下事宜的声明文件:

1) ISMS 的方针策略和目标;

2) ISMS 的范围。

c) 8.2(进行风险评估)活动的输出——以下事宜的文件:

1) 风险评估方法的描述;

2) 风险评估结果。

d) 8.3(选择控制目标和控制措施)活动的输出——风险处置计划。

指南

为了获得管理者的批准,宜按本条的输入,为管理者的评估和决定准备相应文档。

适用性声明(SoA)的准备宜归入信息安全管理工作。所规约的控制措施之详细程度,宜满足支持

组织管理者批准 ISMS 所需要的要求。

有关接受残余风险的决定以及有关实际运行 ISMS 所获授权的决定，宜获得高层管理者的批准。这些决定宜基于风险评估，并基于实施 ISMS 的结果可能产生风险的机遇之评估（比较不实施 ISMS 而产生的风险）。

输出

本活动的可交付项是：

a) 管理者批准实施 ISMS 的书面通知；

b) 管理者接受的残余风险；

c) 适用性声明，包括控制目标和已选择的控制措施。

其他信息

没有其他特定信息。

9 设计 ISMS

9.1 设计 ISMS 的概述

现在，宜开发一个 ISMS 项目的详细设计，为它的实施规划相应的活动。图 7 给出了设计 ISMS 阶段的概览信息。最终 ISMS 项目计划在有关特定组织的细节方面上是独特的，这依赖于以前活动的结果，同时也依赖于本节中所描述的设计阶段特定活动的结果。

特定的最终 ISMS 实施计划是本章的输出。基于这个计划，ISMS 实施项目可以在组织内发布，作为 PDCA 循环（如在 GB/T 22080—2008 中描述）的第一个“DO”阶段。

设计 ISMS 的前提是，管理者已对实施 ISMS 做了承诺，定义于 ISMS 的范围和 ISMS 的方针策略之中。信息资产以及信息安全评估的结果是可用的。另外，描述风险的风险处置计划、风险处置可选措施以及已标识选择的控制目标和控制措施均是可用的。

这里所描述的 ISMS 设计，关注 ISMS 的内部结构和要求。宜注意的是，在某些情况下，ISMS 的设计可能对业务过程的设计具有直接或间接的影响。同样宜注意，通常需要把一些 ISMS 组件集成到以前存在的管理和基础设施协议之中。

目标： 通过以下事宜来完成最终的 ISMS 实施计划：基于已选择的风险处置可选措施，设计组织的信息安全以及相关记录和文档的要求；设计那些集成 ICT 安全条款、物理过程和组织过程的安全控制；设计 ISMS 特定的要求。 见 GB/T 22080—2008 的 4.2.2 a)～e)，h)

在设计 ISMS 时，宜考虑以下事宜：

a) 组织安全——涵盖行政管理方面的信息安全，包括风险处置的组织运行责任。组织安全宜形成一个活动集，该活动集为处理和改善与组织需求和风险有关的信息安全，产生相应的方针策略、目标、过程和规程。

b) ICT 安全——涵盖那些为风险降低特别有关的 ICT 运行责任方面的信息安全。ICT 安全为了达到组织方面以及控制措施技术实施方面的要求集，以为降低风险；

c) 物理安全——涵盖与物理环境（诸如建筑物及其用于降低风险的基础设施）的处理特别相关的责任方面的信息安全。物理安全要达到组织和控制措施技术实施方面的要求集，以降低风险；

d) ISMS 特定事项——涵盖除了上述三个方面之外的、GB/T 22080—2008 规定的 ISMS 其他不同方面的特定要求。其关注点是，为达到一个可运行的 ISMS 而要进行的一些确定的活动，这

些活动是：

1） 监视；

2） 测量；

3） 内部的 ISMS 审核；

4） 培训和意识；

5） 安全事件管理；

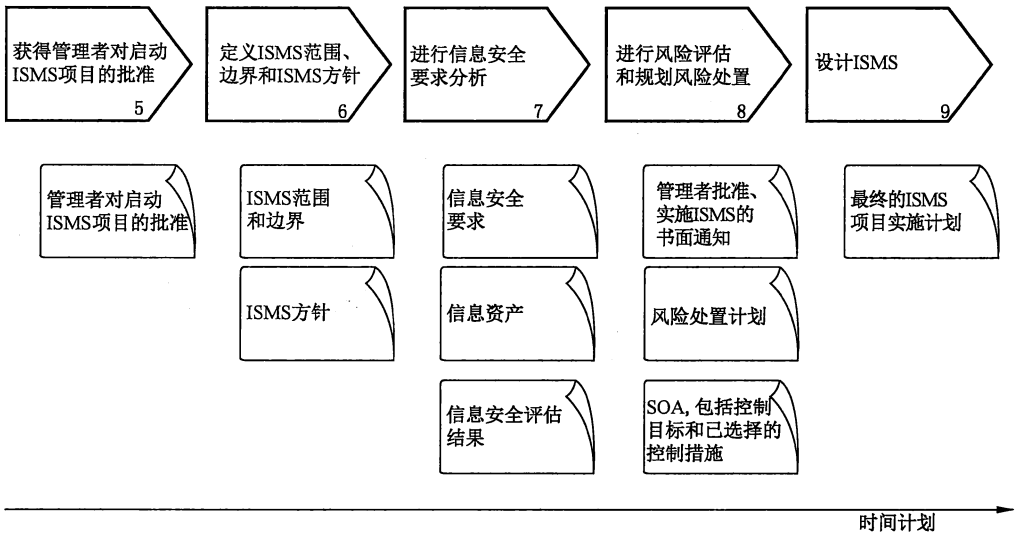
6） 管理评审；

7） ISMS 改进，包括纠正措施和预防措施。

ISMS 项目的开发及其相关已规划控制措施实施的设计，宜涉及并使用有关员工技能和经验，其中这些员工或属于 ISMS 范围内相关组织部门，或具有 ISMS 相关管理责任。ISMS 的一些特定方面，要求与管理者进行必要的对话。

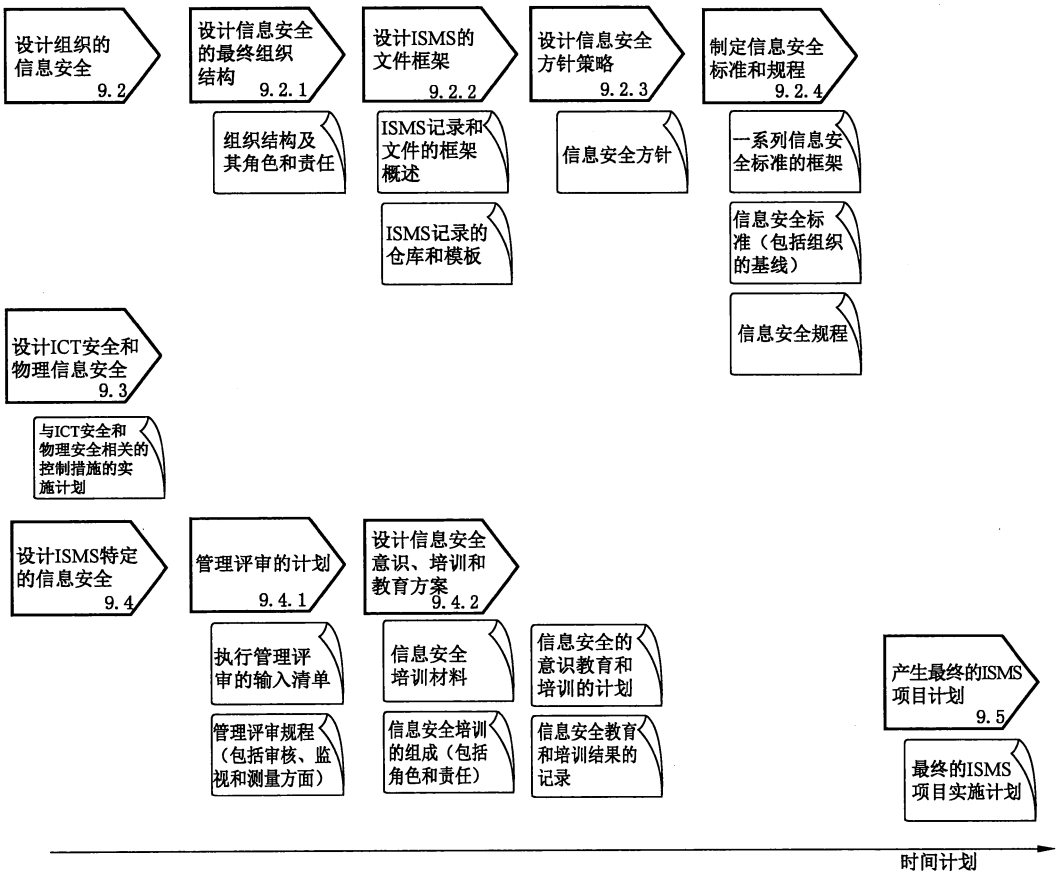
为了设计为风险处置所选择的控制措施，至关重要的是，设计 ICT 安全以及物理安全环境和组织安全环境。ICT 安全不仅涉及信息系统和网络，还涉及运行要求。物理安全涉及访问控制、不可否认性、信息资产的物理保护和存储或保管什么等所有方面，也涉及本身保护手段的安全控制措施。

在 8.3 所描述的活动中所选择的控制措施，宜按照一种特定的结构化和详细的实施计划予以实现，作为 ISMS 项目计划一部分的。ISMS 实施计划的这一特定部分，宜强调为实现控制目标如何处理每一个风险。如果所选择的这些控制措施是合适的、有效的，那么 ISMS 实施计划的这一特定部分就是必要的。信息安全管理团队负责拟定实施计划的这一特定部分，接着使这一部分成为最终 ISMS 项目计划的组成部分。



a)

图 7 设计 ISMS 阶段的概览



b)（续）

图 7（续）

9.2 设计组织的信息安全

9.2.1 设计信息安全的最终组织结构

活动

有关信息安全的组织功能、角色和责任，宜紧密结合风险处置。

输入

a) 5.3.2(定义初步的 ISMS 范围的角色和责任)活动的输出——角色和责任表；

b) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界；

c) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略；

d) 7.2(定义 ISMS 过程的信息安全要求)活动的输出；

e) 7.3(标识 ISMS 范围内的资产)活动的输出；

f) 7.4(进行信息安全评估)活动的输出；

g) 8.2(进行风险评估)活动的输出——风险评估结果；

h) 8.3(选择控制目标和控制措施)活动的输出；

i) GB/T 22081—2008。

指南

为了内部运行 ISMS，宜适当依赖并集成已有的各个方面，寻求构建相应组织结构和组织过程的设

计。同样地，要把 ISMS 集成到更宽泛的已有管理结构(例如内部审核)之中，就宜考虑 ISMS 的设计过程。

为 ISMS 所设计的组织结构，宜反映 ISMS 实施和运行的活动，并强调活动实施方法，例如监视和记录方法，作为 ISMS 运行的一部分。

因此，ISMS 运行结构宜基于规划的 ISMS 实施，通过考虑以下事宜来设计：

a) ISMS 实施的每一个角色，是否对 ISMS 的运行是必需的？

b) 所定义的角色，是否不同于 ISMS 实施的其他角色？

c) 宜为 ISMS 实施，增加什么角色？

例如，对于 ISMS 运行，可增加的角色有：

a) 负责每一个部门信息安全运行的人员；

b) 负责每一个部门 ISMS 测量的人员。

考虑附录 B 中概述的要点，可有助于通过修改 ISMS 实施的结构和角色来决定 ISMS 运行的结构和角色。

输出

本活动的可交付项是一个文件，这个文件概述以下内容：

组织结构及其角色和责任。

其他信息

附录 B——角色和责任的信息。

附录 C——规划审核的信息。

9.2.2 设计 ISMS 的文件框架

活动

为了控制 ISMS 中的记录和文档，宜标识相应的要求并给出一个框架，该框架能满足对 ISMS 记录和文件加以控制的要求。

输入

a) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界；

b) ISMS 的范围和边界的定义；

c) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略；

d) 8.4(获得管理者对实施和运行 ISMS 的授权)活动的输出；

e) 9.2.1(设计信息安全的最终组织结构)活动的输出；

f) GB/T 22081—2008。

指南

设计 ISMS 记录，包括以下活动：

a) 开发一个框架，该框架描述 ISMS 的建档原则、ISMS 文件结构、所涉及的角色、数据格式，以及向管理者报告的途径；

b) 设计文件要求；

c) 设计记录要求。

ISMS 文件宜包括管理者决定的记录；确保相关措施可追踪到管理者的决定和策略，并且所记录的结果是可再现的。

有关 ISMS 的建档，宜提供证据，证明所选择控制措施是基于风险评估和风险处置的结果，并且这些过程随同 ISMS 的方针策略和目标一起予以实施。

文件的基本特性是结果和规程的再现。就所选择的控制措施而言，规程的建立和文件化，宜参照文

件实际部分的人员责任。

ISMS 文件宜包括引用的 GB/T 22080—2008 的 4.3.1 中规定的文件。

ISMS 文件必须予以管理，并对需要人员是可用的。这包括：

a) 建立 ISMS 文件管理的行政管理规程；

b) 文件发布前得到正式批准；

c) 确保文件的更改和现行修订状态得到识别；

d) 把文件作为组织的信息资产进行保护和控制。

重要的是在使用时可获得相关版本的适用文件，确保文件保持清晰、易于识别，并依照其适用的类别的规程进行传输、存储和最终销毁。

此外，确保外来文件得到识别，文件的分发得到控制，防止作废文件的无意识使用，以及如果作废文件因任何目的而保留时，对其进行适当的跟踪。

记录宜作为组织的 ISMS 符合 GB/T 22080—2008 和展示运行效果的证据，而加以创建、保持和控制。

也需要为整个 PDCA 阶段的实施状况，保持一些记录；并为信息安全事件和一般性事件，为教育、培训、技能、经历与资格、内部 ISMS 审核、纠正措施与预防措施等保持一些记录。

为了控制这些记录，宜执行以下任务：

a) 为数据标识、保存、保护、查找和废弃，建立所需要的控制文档，并建立数据保存期限的文档；

b) 定义在运行管理过程中宜记录的事项和范围；

c) 当相关法律或法规规约了任何一个保存期，那么就该宜按这样的法律要求，设定保存期。

输出

本活动的可交付项是：

a) 概述 ISMS 记录和文件控制的要求的文件；

b) 所要求的 ISMS 记录的仓库和模板。

其他信息

没有其他特定信息。

9.2.3 设计信息安全方针策略

活动

对于 ISMS 的运行，宜建立有关信息安全目标的决策管理者和行政管理者战略定位的文件。

输入

a) 5.2(阐明组织开发 ISMS 的优先级)活动的输出——概述的目标和要求清单；

b) 5.4(为了管理者的批准而创建业务案例和项目计划)活动的输出——管理者对 ISMS 项目的初始批准；

c) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界；

d) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略；

e) 7.2(定义 ISMS 过程的信息安全要求)活动的输出；

f) 7.3(标识 ISMS 范围内的资产)活动的输出；

g) 7.4(进行信息安全评估)活动的输出；

h) 8.2(进行风险评估)活动的输出——8.3(选择控制目标和控制措施)活动的风险评估输出的结果；

i) 9.2.1(设计信息安全的最终组织结构)活动的输出；

j) 9.2.2(设计 ISMS 文件的框架)活动的输出；

k) 见 GB/T 22081—2008 的 5.1.1。

指南

信息安全方针策略记录了组织的战略定位，以及整个组织相关的信息安全目标。

该方针策略是基于信息和知识而拟定的。管理者在以前进行分析中所标识的事宜是非常重要的，宜把它们作为证据，并在方针策略中予以强调，以便提供组织的动机和动力。要重点指出，如果不遵守该方针策略将会发生什么。还宜强调影响组织解决问题的法律和法规。

可以参照参考文献、互联网以及行业协会等，给出一些信息安全方针策略的例子。可以依据年度报告、其他方针策略文件或管理者支持的其他文件，配置并联想一些安全方针策略。

关于一个方针策略的实际篇幅，可能存在一些不同的说明和要求。方针策略宜简明扼要的给出，以使有关人员能理解该方针策略的意图。此外，方针策略宜充分地凸现需要什么目标，以便强调相关的一组规章和组织目标。

信息安全方针策略的篇幅和结构，宜支持下一阶段（引入信息安全管理体系过程）中所使用的文件（参见附录 D——方针策略结构的信息）。

对于大型和复杂的组织（例如，拥有大量不同的运行域），可能有必要拟定一个总方针策略和一些运作上经改编的基础性方针策略。

关于信息安全方针策略内容的指南见 GB/T 22081—2008 的 5.1.1。

所提议的方针策略（带版本号和日期）宜在组织内由运行管理人员进行反复核对和建立。运作管理人员逐条批准管理小组或相关小组内所建立的方针策略，接之以对读者可访问和可理解的方式，在组织内有关人员之间进行沟通。

输出

本活动的可交付项是信息安全方针策略文件。

其他信息

附录 B——角色和责任的信息。

附录 D——方针策略结构的信息。

9.2.4 制定信息安全标准和规程

活动

宜制定强调整个组织或者强调组织特定部分的信息安全标准和规程。

输入

a) 6.5（集成每一个范围和边界以获得 ISMS 的范围和边界）活动的输出——ISMS 的范围和边界；

b) 6.6（制定 ISMS 的方针策略和获得管理者的批准）活动的输出——ISMS 的方针策略；

c) 8.2（进行风险评估）活动的输出；

d) 8.3（选择控制目标和控制措施）活动的输出；

e) 8.4（获得管理者对实施和运行 ISMS 的授权）活动的输出——适用性声明，包括控制目标和已选择的控制措施；

f) 9.2.1（设计信息安全的最终组织结构）活动的输出；

g) 9.2.2（设计 ISMS 文件的框架）活动的输出；

h) 9.2.3（设计信息安全方针策略）活动的输出；

i) GB/T 22081—2008。

指南

为了给组织的信息安全工作提供一个基础，宜为那些需要知道的人员提供一些可用的信息安全标准和一组适用的法律法规和规章的要求。

由ISMS范围所覆盖的组织的各个不同部分的代表，宜参与制定标准和规程的过程。这些参与宜有权威机构，并是组织的代表。例如，可包括以下角色：

a) 信息安全管理人员；

b) 物理安全的代表；

c) 信息系统责任人；

d) 战略域和运行域的过程责任人。

建议成立一个规模尽可能小的编辑组，选择一些指定的专家临时加入到该编辑组。每一个代表宜积极地与各自的组织域保持联系，以便得到无缝的运行支持。这有助于以后在运行层面上有关规程和例程内容的细化工作。

这样，安全标准和规程就宜作为设计详细的技术规程或操作规程的基础予以使用。

编制信息安全标准和规程的一种有用的途径是，基于风险评估结果，考虑GB/T 22080—2008和GB/T 22081—2008的实现指导中那些真正可用的每一条款，并精确地描述宜如何应用之。

宜对现有的信息安全标准和规程的评价加以评审。例如，它们是否可以加以细化并开发之？或者它们是否需要被完全取代？

宜向范围内的每一个人员，提供相关的最新文档。信息安全标准和规程宜适用于整个组织，或使它们可清楚地表明所涉及的角色、系统和域。宜及时产生第一版本。

宜在早期阶段，定义信息安全标准和规程的修订和评审过程。因此，方针策略变更信息宜如何发布，宜拟定一个战略。

输出

a) 本活动的可交付项是一个结构化、详细的实施计划，该计划是有关组织安全的控制，并作为最终ISMS项目计划一部分，包括该信息安全标准集的一个文档化框架；

b) 涵盖组织基线的信息安全标准；

c) 实现信息安全标准的信息安全规程。

其他信息

附录D——方针策略结构的信息。

9.3 设计ICT安全和物理信息安全

活动

宜为ICT和物理安全环境设计相应的控制措施。

输入

a) 6.5(集成每一个范围和边界以获得ISMS的范围和边界)活动的输出——ISMS的范围和边界；

b) 6.6(制定ISMS的方针策略和获得管理者的批准)活动的输出——ISMS的方针策略；

c) 7.2(定义ISMS过程的信息安全要求)活动的输出；

d) 7.3(标识ISMS范围内的资产)活动的输出；

e) 7.4(进行信息安全评估)活动的输出；

f) 8.3(选择控制目标和控制措施)活动的输出；

g) 8.4(获得管理者对实施和运行ISMS的授权)活动的输出——适用性声明，包括控制目标和已选择的控制措施；

h) GB/T 22081—2008。

指南

在本活动中，宜为每一个控制措施建立如下文档，它们宜作为ISMS项目计划的一部分：

a) 负责实施一个控制措施的责任人姓名；

b) 要实施的那个控制措施的优先级；

c) 实施控制措施的任务或活动；

d) 实施完该控制措施的时间陈述；

e) 控制措施一旦完成，宜向谁报告；

f) 实施资源(人力、资源要求、空间要求、费用)。

最初，宜进行 ICT 安全和物理安全的概念设计。其中宜考虑以下事宜：

有关初始实施过程的责任，一般包括：

a) 控制目标的规格说明，其中要描述所期望的规划状态；

b) 资源的分配(工作量、财力资源)；

c) 实施该控制措施的实际终结时间；

d) 要与 ICT 安全、物理安全和组织安全进行集成的可选措施。

在概念设计之后，宜像系统开发一样进行 ICT 安全和物理安全的实际设计，以便达到和实现组织的最佳实践。其中宜考虑以下事宜：

有关实际实现过程的责任，包括：

a) 为工作运行的操作层面上，针对各 ICT 域、物理域和组织域，设计所选择的每一个控制措施；

b) 按所达成一致的设计，实例化每一个控制措施；

c) 为促进安全意识的控制及其培训课程，供给相应的规程和信息；

d) 在工作场所上，供给该控制措施的援助和实施。

ICT 安全和物理信息安全的设计，依赖于 ICT、物理、或组织方面控制措施的类型；清晰地切分实施过程的初始部分和最后部分，可能并不总是适当或必需的。

控制措施的实施常常需要组织内若干个不同角色之间的合作。因此，例如往往需要承担系统责任的人员来购置、安装和维护技术设施。而其他角色可能更适合于设计用来治理系统使用的规程，并形成相应的文档。

信息安全宜被集成到组织范围内的规程和过程之中。如果对该组织的一部分或对第三方，证明实施这一集成是困难的，那么相关方就宜立即就此进行沟通，以便能达成一个一致的解决方案。这一类型问题的解决，包括修改规程和过程，重新分配角色和责任，并调整技术规程。

以下方面是实施 ISMS 控制措施的结果：

a) 实施计划，其中规约了控制措施的实施细节，例如进度，实施小组的结构等；

b) 实施结果的记录和文档。

输出

本活动的可交付项是，针对与 ICT 安全和物理安全有关的控制措施，给出一个结构化、详细的实施计划，作为 ISMS 项目计划一部分的，其中对每一个控制，包括：

a) 详细的描述；

b) 设计和实施的责任；

c) 期望的时间；

d) 涉及的任务；

e) 要求的资源；

f) 责任关系(报告途径)。

其他信息

没有其他特定信息。

9.4 设计 ISMS 特定的信息安全

9.4.1 管理评审的计划

活动

宜制定一个计划，以确保管理者参与 ISMS 运行和持续改进的评审，并给出相应的承诺。

输入

a) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界；

b) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略；

c) 8.4(获得管理者对实施和运行 ISMS 的授权)活动的输出——适用性声明，包括控制目标和已选择的控制措施；

d) 9.2.3(设计信息安全方针策略)活动的输出；

e) GB/T 31497—2015。

指南

宜在 ISMS 规格说明和业务案例开发的最早阶段，开始进行 ISMS 活动的管理评审，并持续不断地进行 ISMS 运行的定期评审。这种紧密的参与，为确认 ISMS 是否符合业务需求，并为维护对 ISMS 的业务承诺，提供了一种手段。

管理评审的规划包括确定宜在何时和如何进行管理评审。关于管理评审的前提的详细信息，在 GB/T 22080—2008 的 7.2 中给出。

为了规划评审，必须对涉及的角色进行评估。角色的选择宜寻求管理者的批准，并且宜尽可能早地通知这些角色。建议给管理者提供有关评审过程的必要性及目的的充分数据。(关于角色和责任的更多信息参见附录 B。)

管理评审宜基于 ISMS 测量的结果和在 ISMS 运行期间收集的其他信息。这些信息被 ISMS 的管理活动使用，以决定 ISMS 的成熟程度和有效性。ISMS 测量所需要的输入和输出见 GB/T 22080—2008，关于 ISMS 测量的更多信息可以从附录 E 和 GB/T 31497—2015 中获得。

也宜注意到，管理评审宜包括对风险评估的方法和结果的评审。管理评审宜按计划的时间间隔进行，考虑到环境中的所有变化，诸如组织和技术的变化。

宜规划内部的 ISMS 审核，以便一旦实施了 ISMS，就能够定期评价它。内部 ISMS 审核的结果是 ISMS 管理评审的重要输入。因此，在执行管理评审之前，宜规划内部的 ISMS 审核。内部的 ISMS 审核宜包括的视角，包括控制目标、控制措施以及 ISMS 的过程和规程，看它们是否得到有效的实施和维护，并符合：

a) GB/T 22080—2008 的要求；

b) 相关法律法规和规章；

c) 已识别的信息安全要求。

(关于规划审核的更多信息见附录 C。)

管理评审的前提条件是基于实施和运行 ISMS 所收集的信息。提供给管理评审组的信息可包括以下内容：

a) 最近一个运行期间的安全事件报告；

b) 控制措施有效性的验证和已识别的不符合性；

c) 其他常规检查的结果(如果该项检查揭示出不符合方针策略的话，其结果就要更加详细)；

d) ISMS 的改进建议。

监视的计划宜形成监视结果的文件，监视结果宜记录之并向管理者报告，(关于监视的更多信息见

附录 E)。

输出

本活动输出的可交付项是一个文件,该文件概述了管理评审所需的计划,涉及的内容包括:

a) 执行 ISMS 管理评审所需的输入;

b) 涵盖审核、监视和测量方面的管理评审规程。

其他信息

附录 B——信息安全的角色和责任。

附录 C——内部审核的信息。

附录 E——建立监视和测量的信息。

9.4.2 设计信息安全意识、培训和教育方案

活动

宜制定信息安全意识以及培训和教育方案。

输入

a) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界;

b) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略;

c) 7.2(定义 ISMS 过程的信息安全要求)活动的输出——特别是组织对信息安全培训和教育的要求;

d) 8.4(获得管理者对实施和运行 ISMS 的授权)活动的输出——适用性声明,包括控制目标和已选择的控制措施;

e) 8.3(选择控制目标和控制措施)活动的输出——风险处置计划;

f) 9.2.3(设计信息安全方针策略)活动的输出;

g) 9.2.4(制定信息安全标准和规程)活动的输出;

h) 组织的普通教育和培训方案的概述。

指南

管理者负责对具有明确角色的所有人员进行教育和培训,以确保他们有能力执行所需要的操作。在理想情况下,所进行的教育和培训的内容,宜帮助所有人员了解他们所执行的信息安全活动,并理解这些活动的含义和重要性,以及他们如何为达到 ISMS 的目标做出自己的贡献。

重要的一点是,要确保 ISMS 范围内的每一个员工都接受必要的安全培训和/或教育。在大型组织中,一整套单一的培训教材通常是不够的,因为它包含仅与特定类型工作有关的大量数据,因此是庞大的、复杂的和难以使用的。在这些情况下,合适的做法是,分别为广泛的每类角色,诸如办公室工作人员、IT 职员或驾驶员,按他们各自的需求,定制设计多套不同的培训教材。

信息安全意识培训和教育方案宜确保安全培训和教育的记录得以产生。这些记录宜定期评审,以确保所有人员都接受过其所需要的培训。宜有一个角色对这一过程负责。

信息安全培训教材宜与组织使用的其他培训教材,特别是给 IT 系统用户提供的培训课程,相互配合而设计。理想上,信息安全相关方面的培训宜集成到 IT 用户的每门课程中。

为适合于目标受众,信息安全培训教材宜至少包含以下知识点:

a) 有关信息安全的风险和威胁;

b) 信息安全的基本术语;

c) 安全事件的清晰定义:关于可如何标识安全事件、宜如何处理和报告安全事件的指南;

d) 组织的信息安全方针策略、标准和规程;

e) 组织内与信息安全有关的责任和汇报渠道;

f) 如何辅助信息安全改进的指南；

g) 信息安全事件和报告的指南；

h) 从何处获得更多信息。

宜确定一个信息安全培训组，该组可包括以下任务：

a) 创建和管理培训记录；

b) 创建和管理培训教材；

c) 承担培训。

可把这些任务分配给现有的培训人员。但为了确保这些任务被有效地和准确地提交给现有的职员，可能需要对他们进行信息安全概念方面的基础培训。

信息安全意识、培训和教育方案宜包括一个规程，以确保培训教材得以定期评审和更新。宜明确指定一个角色，具体负责评审和更新培训教材。

输出

本活动的可交付项是：

a) 信息安全意识、教育与培训教材；

b) 信息安全意识教育与培训的形成，包括角色和责任；

c) 信息安全意识、教育与培训的计划；

d) 展示员工的信息安全意识、教育与培训的结果的实际记录。

其他信息

没有其他特定信息。

9.5 产生最终的 ISMS 项目计划

活动

宜最终产生 ISMS 项目计划，包括为实施已选择的控制措施所需要的活动。

输入

a) 6.5(集成每一个范围和边界以获得 ISMS 的范围和边界)活动的输出——ISMS 的范围和边界；

b) 6.6(制定 ISMS 的方针策略和获得管理者的批准)活动的输出——ISMS 的方针策略；

c) 9.2(设计组织的信息安全)活动的输出；

d) 9.3(设计 ICT 安全和物理信息安全)活动的输出；

e) 9.4(设计 ISMS 特定的信息安全)活动的输出；

f) GB/T 22081—2008。

指南

实施已选择的控制措施所需要的活动以及执行 ISMS 的相关其他活动，宜正式编入一个详细的实施计划中，作为最终的 ISMS 项目的一部分。还可以通过描述一些建议的实施工具和方法，支持这一详细的实施计划。当 ISMS 项目涉及组织内很多不同的角色时，重要的是要把这些活动清晰地指派给有关责任方，要在项目初期且在整个组织内交流这一计划。

当然，对于所有项目最主要的是，负责该项目的人员确保为该项目分配了足够的资源。

输出

本活动的可交付项是一个最终的 ISMS 项目实施计划。

其他信息

没有其他特定信息。

附 录 A
（资料性附录）
检查表的描述

目的：

a） 提供建立和实施 ISMS 所需活动的检查表（见表 A.1）；

b） 支持 ISMS 实施进展的监视；

c） 把相关 ISMS 实施活动映射到对应的 GB/T 22080—2008 的要求。

表 A.1 检查表

本标准的实施阶段	步骤编号	本标准对照的活动	步骤的先决条件	输出文档	与 GB/T 22080—2008 的对照
5 获得管理者对实施 ISMS 的批准	1	收集公司的业务目标	无	公司业务目标清单	无对应条款
	2	获得对现有管理体系的理解	无	现有管理体系的描述	无对应条款
	3	5.2 定义 ISMS 的目标、信息安全需求和业务要求	1,2	ISMS 的目标、信息安全需求和业务要求的概要	无对应条款
	4	收集适用于公司的相关规章、符合性和行业标准	无	适用于公司的规章、符合性和行业标准的概要	无对应条款
	5	5.3 定义初步的 ISMS 范围	3,4	ISMS 初步范围的描述(5.3.1)	无对应条款
				ISMS 角色和责任的定义(5.3.2)	无对应条款
	6	5.4 为了管理者的批准而创建业务案例和项目计划	5	业务案例和建议的项目计划	无对应条款
	7	5.4 为了管理者的批准而创建业务案例和项目计划	6	管理者对启动实施 ISMS 项目的批准和承诺	无对应条款
6 定义 ISMS 的范围和 ISMS 的方针策略	8	6.2 定义组织边界	7	• 组织边界的描述 • 组织的功能和结构 • 通过边界的信息交换 • 范围之内和范围之外的信息资产的业务过程和责任	4.2.1 a)（部分）
	9	6.3 定义信息通信技术(ICT)边界	7	• ICT 边界的描述 • 范围之内和范围之外的信息系统和电信网络的描述	4.2.1 a)（部分）
	10	6.4 定义物理边界	7	• ISMS 物理边界的描述 • 范围之内和范围之外的组织及其地理特征的描述	4.2.1 a)（部分）

表 A.1（续）

本标准的实施阶段	步骤编号	本标准对照的活动	步骤的先决条件	输出文档	与 GB/T 22080—2008 的对照
6 定义 ISMS 的范围和 ISMS 的方针策略	11	6.5 最终确定 ISMS 的边界	8，9，10	一个描述 ISMS 范围和边界的文件	4.2.1 a)
	12	6.6 制定 ISMS 方针策略	11	管理者批准的 ISMS 方针策略	4.2.1 b)
7 进行组织分析	13	7.2 定义支持 ISMS 的信息安全要求	12	• 主要过程、功能、位置、信息系统和通信网络的清单	无对应条款
				组织在保密性、可用性和完整性方面的要求	无对应条款
				组织在法律法规、规章、合同和业务的信息安全要求方面的要求	4.2.1 c) 1) 部分
				组织已知的脆弱性清单	4.2.1 d) 3)
	14	7.3 标识 ISMS 范围内的资产	13	组织的主要过程的描述	无对应条款
				标识组织的主要过程的信息资产	4.2.1 d) 1)
				关键过程/资产类别	无对应条款
	15	7.4 进行信息安全评估	14	• 记录组织实际的信息安全状况，并进行评价，包括现有的信息安全控制措施，形成文件 • 记录已评估和评价的组织缺陷，并形成文件	4.2.1 e) 2)部分
8 进行风险评估和选择风险处置可选措施	16	8.2 进行风险评估	15	• 风险评估的范围 • 已获批准的、与组织的战略风险管理环境保持一致的风险评估方法 • 风险接受准则	4.2.1 c) 1)
	17	8.3 选择控制目标和控制措施	16	高层风险评估文件	4.2.1 e) 3) 部分
				识别更多的深度风险评估的需求	无对应条款
				深度风险评估文件	4.2.1 e) 3) 部分
				综合的风险评估结果	无对应条款
	18	8.4 获得管理者对实施 ISMS 的批准	17	风险和已识别的风险处置可选措施	4.2.1 f)
				已选择的风险降低控制目标和控制措施	4.2.1 g)

表 A.1（续）

本标准的实施阶段	步骤编号	本标准对照的活动	步骤的先决条件	输出文档	与 GB/T 22080—2008 的对照
8 进行风险评估和选择风险处置可选措施	19	管理者对残余风险的批准	18	管理者对所提议的残余风险的批准文件（宜是 8.4 的输出）	4.2.1 h)
	20	管理者对实施和运行 ISMS 的授权	19	管理者对实施和运行 ISMS 的授权书（宜是 8.4 的输出）	4.2.1 i)
	21	准备适用性声明	18	适用性声明	4.2.1 j)
9 设计 ISMS	22	9.2 设计组织的信息安全	20	组织结构及其信息安全相关的角色和责任	5.1 c)
				• ISMS 相关文件的识别 • ISMS 记录的模板及其使用和存储说明书	4.3
				信息安全方针策略文件	5.1.1
				信息安全方针策略和规程基线（必要时，制定特定的方针策略、规程等的合适的计划）	
	23	9.3 设计 ICT 和物理安全	20,21	用于为 ICT 和物理信息安全所选的安全控制措施的实施过程的实施项目计划	4.2.2 c) 部分
	24	9.4 设计 ISMS 特定的信息安全	22,23	描述报告和管理评审过程的规程	7.1
	25			• 审核、监视和测量的描述	4.2.3 a) 部分； 4.2.3 b)部分； 第 6 章
	26			• 培训和意识方案	5.2.2
	27	9.5 产生最终的 ISMS 项目计划	25	管理者批准的实施过程的实施项目计划	无对应条款
	28	最终的 ISMS 项目计划	28	一个 ISMS 的组织特定的实施项目计划，涵盖了组织的、ICT 和物理信息安全以及 ISMS 特定要求的活动的有计划的执行，为按照本标准中包含的活动的结果来实施 ISMS	无对应条款

附 录 B
（资料性附录）
信息安全的角色和责任

本附录就组织内信息安全相关的角色和责任，提供了更多的指导。首先，从组织实施 ISMS 的视角给出了角色。然后以表格的形式总结了这些信息，并提供了有关角色和责任的一般示例。

B.1 信息安全委员会的角色

信息安全委员会宜负有组织 ISMS 的领导角色。信息安全委员会宜负责处理组织的信息资产，并宜充分理解信息安全，以指导、监视和完成必要的任务。

下面是信息安全委员会这一角色的示例：

a) 完成风险管理、制定 ISMS 文件计划、负责决定这些文件的内容，并取得管理者的认可；
b) 规划新设备的采购和/或决定组织已拥有设备的再使用；
c) 处理可能产生的任何问题；
d) 考虑实施和测量 ISMS 之后所提出的那些改进；
e) 给出 ISMS(在实施项目期间及在运行期间)的战略方向；
f) 担任高级管理者、实施项目团队以及信息安全人员之间的联络者。

B.2 信息安全规划团队的角色

该项目团队负责 ISMS，在规划该项目时，宜得到其成员的帮助，因为他们对 ISMS 范围内的重要信息资产有广泛的了解，并具有足够的知识来考虑如何处理这种信息。例如，当决定如何处理信息资产时，ISMS 范围内的各个部门之间，可能有不同的意见，因此，可能需要调整该计划的正面与负面的影响。该项目团队需要充当跨部门边界的冲突调解者的角色。为了做到这一点，其成员需要具有经验丰富的沟通技能和调解能力，以及高层次的安全知识。

B.3 专家和外部顾问

组织在建立 ISMS 之前，宜选择完成上述职责的成员(如有可能，每个成员具有一个唯一的角色)。然而，成员必须具有信息安全领域广泛的知识和经验，诸如“IT”、“行政管理决策”和“了解该组织”。组织内负责指定运行的人员，可能最了解该指定领域。组织内的许多专业人员是某些特定领域的专家，在 ISMS 中应咨询他们，因为 ISMS 与这些特定领域相关。在这种专业技术与满足组织目标所需要的广泛知识之间需要进行平衡，这也是很重要的。外部顾问能根据其对组织的宏观观点和其他类似场合的经验，给出建议，即使他们通常不必具有关于组织特定的和运行的情况等详细信息的深度了解。上述示例所使用的词语，诸如“信息安全委员会”和“信息安全规划组”，并不重要。但是宜理解每一个机构的职能。理想情况下，宜有内部结构来协调组织的信息安全，与每一个技术部门紧密地沟通和合作。

B.4 信息资产责任人

宜为每一个组织过程和专门的应用指定一个人；这个人担当所谓的“信息资产责任人”，负责与该特定的组织过程内数据处理有关的所有信息安全问题。例如，联系人或过程责任人，负责委派任务和处理

被分配到该组织过程内的信息。

在风险分担、风险规避和风险保留的情况下，宜从组织的安全方面采取必要的措施。如果已经做出了转移风险的决定，那么宜通过合同、保险协议和组织结构（诸如合伙企业和合资企业），来采取适当的措施。

图 B.1 展示了一个建立 ISMS 的组织结构示例。后面给出的组织的主要角色和责任都基于此示例。

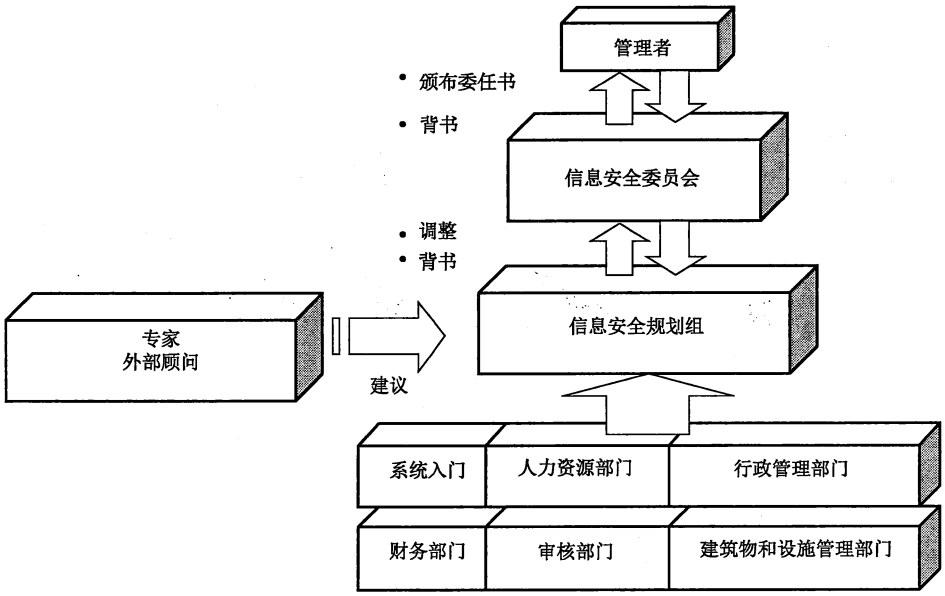


图 B.1 建立 ISMS 的组织结构例子

与组织互动

所有相关方宜评审并熟悉当前组织资产的保护要求。组织分析的参与者宜包括那些对组织及其运作环境非常了解的人员。这些人员宜被选择，以代表组织范围的广泛参与，他们包括：

a) 高级管理者（例如 首席运营官 COO 和首席财务官 CFO）；
b) 信息安全委员会的成员；
c) 信息安全规划团队的成员；
d) 生产线管理人员（例如，组织某部门的领导）；
e) 过程责任人（即代表重要的运行区域）；
f) 专家和外部顾问。

信息安全相关的一般角色和责任的示例

信息安全是影响整个组织的一个广泛的领域。因此，清晰定义安全责任是成功实施 ISMS 的根本。由于安全相关的角色和责任会发生变化，因此，理解各种不同角色是理解本标准后面所述的某些活动的基础。表 B.1 概述了安全相关的角色和责任。宜注意到，这些角色是一般性的，对于每个单独 ISMS 实施而言，需要进行特定的描述。

表 B.1　信息安全角色和责任的示例清单

角色	责任的简要描述
高级管理者(例如首席运营官 COO、首席执行官 CEO、首席安全官 CSO 和首席财务官 CFO)	负责愿景、战略决策和协调活动,以指导和控制组织
生产线管理人员	对组织的功能负有最高责任
首席信息安全官	全面负责和治理信息安全,以确保信息资产得到正确处理
信息安全委员会(包括成员)	处理信息资产,在组织的 ISMS 中具有领导角色
信息安全规划团队(包括团队成员)	负责 ISMS 建立期间的运作。规划团队跨部门工作,解决各种冲突,直到 ISMS 被建成
利益相关方	在其他信息安全角色的描述中,这里的利益相关方主要被定义为正常运作之外的人员/机构,诸如董事会、责任人(如果组织属于一个集团或是政府组织,是指组织责任人,和/或直接责任人,诸如私人组织的利益相关方)。其他利益相关方的例子可以是有关联的公司、客户、供应商或更公开的组织,诸如政府财政控制机构或相关的证券交易所,如果组织被列入的话
系统管理员	系统管理员负责 IT 系统
IT 经理	所有 IT 资源的管理者(例如,IT 部门管理者)
物理安全员	负责物理安全(例如建筑物等)的人员,通常称作“设施经理”
风险管理者	负责组织的风险管理框架(包括风险评价、风险处置和风险监视)的人员
法律顾问	很多信息安全风险都有法律方面的问题,法律顾问负责考虑这些问题
人力资源管理者	负责整个员工的人员
档案管理员	所有组织都有包含关键信息的档案。这些信息需要长期保存。信息可能存放在多种介质上,宜有专人对这种存储介质的安全负责
个人数据管理员	如果国家法律有要求,那么可能要有一个人负责联系数据检查委员会或类似的官方组织来监管个人诚信和隐私保护问题
系统开发者	如果组织开发自己的信息系统,那么就应有人对这种开发负责
专家/行家	当 ISMS 涉及其在特定领域的使用时,宜就 ISMS 事宜的意图咨询负责组织中某些运行工作的专家和行家
外部顾问	外部顾问能根据其对组织的宏观观点和行业经验,给出建议。然而,顾问可能对组织和组织的运作了解不多
员工/用户	每一个员工都对维持其工作场所和环境中的信息安全负有同等责任
审核员	审核员负责评估和评价 ISMS
培训师	培训师实施培训和意识方案
局部 IT 或 IS 的负责人	在一个大型组织内,常常有局部组织的人负责局部的 IT 事宜,可能还有信息安全
拥护者(有影响力的人员)	拥护者本身不是一个承担责任的角色,但在大型组织中,实施阶段中有人对 ISMS 的实施有深刻的了解且在实施的理解和真正的原因上能够给予支持,可能有很大帮助。他们可正面地影响组织的观点,也可称作“大使”

附 录 C
（资料性附录）
有关内部审核的信息

本附录提供了支持审核的规划的附加指南。

ISMS 的实施情况的评价宜采用定期的时间间隔，通过内部审核和独立审核的方式来进行。这还可以达到核对和评价日常实践中总结的经验的目的。为了实施 ISMS，审核的方式必须加以规划。

在 ISMS 审核中，审核的结果宜基于证据而决定。因此，在 ISMS 运行期间，宜分配适当长的时间去收集合适的证据。

ISMS 内部审核宜定期加以实施和执行，以评价 ISMS 的控制目标、控制措施、过程和规程是否符合 GB/T 22080—2008 以及相关法律法规和规章的要求，是否符合已识别的信息安全要求，并得到有效地实施和保持。

然而，对于小公司来讲，挑选 ISMS 内部审核员可能是困难的。如果没有足够的资源来完成这些需要经验丰富的内部成员或员工才能执行的审核，宜委托外部专家负责执行审核活动。当组织使用外部审核员时，宜考虑以下事项：外部审核员是否熟悉 ISMS 内部审核；然而，外部审核员可能对组织的内部环境不够了解。这些关于组织环境的信息宜由内部员工来提供。另外，在考虑组织环境的情况下，内部审核员可以执行详细的审核，但他们可能没有足够知识来执行 ISMS 审核。组织宜认识到内部审核员和外部审核员执行 ISMS 内部审核时的特征及可能的缺陷。

已实施的控制措施的有效性和效率（见 GB/T 31497—2015），宜在内部审核的范围内加以检查。

重要的是，参与安全目标的规划与设计的人员不能执行审核，因为找到自己的错误对他们来讲是困难的。因此，管理者宜挑选 ISMS 内部审核范围以外的组织部门或个人作为审核员。这些审核员宜拟定 ISMS 内部审核计划、加以实施、做出报告，并进行跟踪，以获得管理者的承诺。为了避免内部员工掩饰自己工作的情形出现，根据组织的规模来聘请外部审核员可能是有用的。

在 ISMS 内部审核中，宜检查 ISMS 是否得到有效地运行、保持以及按预期执行。在拟定审核方案时，审核员宜考虑到受审核的管理目标、控制措施、过程和规程的状态及重要性，以及以前审核的结果。

在执行审核时，审核的准则、适用范围、频度和方法宜被文件化。

当选择审核员时，宜确保审核过程的客观性和公正性。当执行审核所涉及的过程时，审核员需要具有以下能力：

a） 规划和执行审核；

b） 报告审核结果；

c） 提出纠正措施和预防措施等。

此外，组织必须在规程文件中定义审核员的责任和审核所涉及的过程。

负责被审核过程的管理人员，宜确保不符合项及其产生的原因没有延误地、得到恰当解决。然而，这并不意味着不符合项必须立刻得以纠正。此外，所执行的纠正措施宜包括对已采取措施的验证和验证结果的报告。

从治理的角度来看，ISMS 内部审核可作为组织中其他内部审核的一部分来执行，或与之合作执行。在执行审核时，建议参考 GB/T 25067—2010。

附 录 D
（资料性附录）
方针策略的结构

本附录提供了包括信息安全方针策略在内的方针策略结构的附加指南。

通常，方针是管理者正式表达的总意图和方向的声明（见 GB/T 29246—2012 和 GB/T 22081—2008）。方针的内容指导该方针主题相关的措施和决策。一个组织可以有许多方针；每个活动领域一个方针，这个方针对组织来讲是重要的。某些方针是相互独立的，而其他一些方针则有层次关系。在安全领域中，方针策略通常是按层级进行组织的。典型地，组织的安全方针是最高层次的方针。它由许多更加具体的方针策略（包括信息安全方针和信息安全管理体系方针）来支撑。信息安全方针可被许多涉及信息安全特定主题的更加具体的方针策略支持。关于这些方针策略已在 GB/T 22081—2008 中讨论过，例如，信息安全方针被访问控制、桌面清空与屏幕清空、网络服务的使用和密码控制的使用等相关方针策略支持。在某些情况下，增加其他层面的方针策略也是可能的。这种安排如图 D.1 所示。

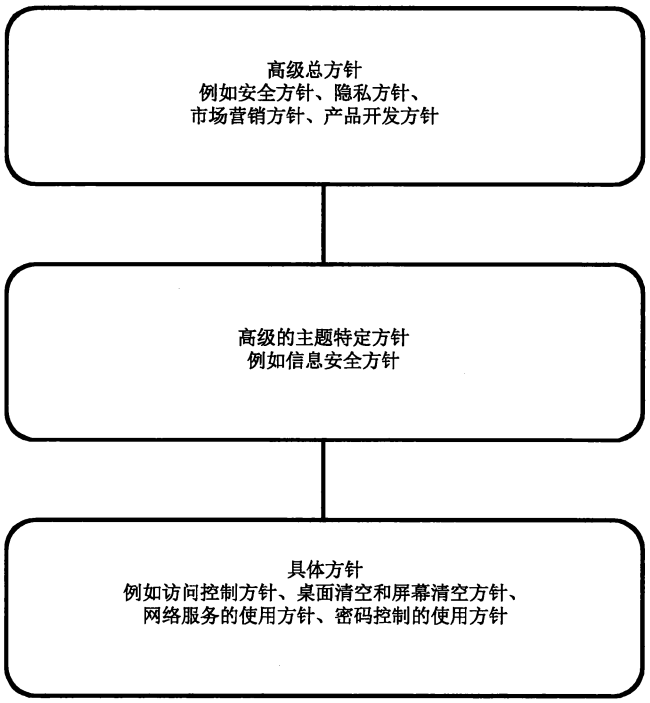


图 D.1 方针策略的层次

GB/T 22080—2008 要求组织具有 ISMS 方针和信息安全方针。然而，它没有规定这些方针策略之间的任何特定关系。对于 ISMS 方针的要求见 GB/T 22080—2008 的 4.2.1。对于信息安全方针的指南见 GB/T 22081—2008 的 5.1.1。这两类方针策略可作为同级方针策略来制定。ISMS 方针可从属于信息安全方针，或者信息安全方针可从属于 ISMS 方针。

方针策略的内容根据组织运行环境而定。特别是，当在方针框架内制定任何方针时，宜考虑以下事项。

a） 组织的目的和目标；

b） 为达到其目标所采用的战略；

c） 组织所采用的结构和过程；

d) 与方针主题相关的目的和目标；

e) 与较高级方针策略有关的要求。

这些事项如图 D.2 所示。

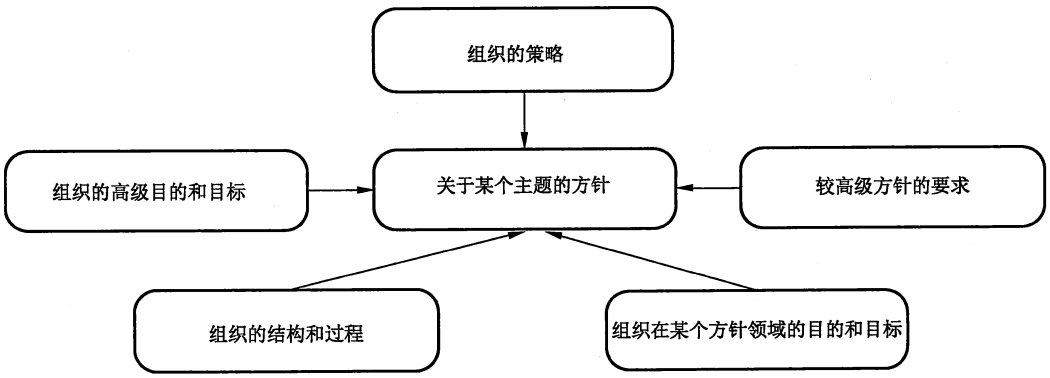


图 D.2 制定方针策略的输入

方针策略可具有以下结构：

1. 方针策略概要——一两句内容的综述。（有时可合并到引言中）
2. 引言——该方针策略主题的简要说明。
3. 范围——描述该方针策略所影响的组织部门或活动。如果有相关的方针策略，则列出该方针策略所支持的其他方针策略。
4. 目标——描述该方针策略的意图。
5. 原则——描述关于实现目标的行动和决策的规则。在某些情况下，原则可用于识别与该方针策略的主题相关的关键过程，以及运行这些过程的规则。
6. 责任——描述满足该方针策略要求的行动负责人。在某些情况下，责任可包括组织安排的描述以及担任指定角色的人员的责任。
7. 关键结果——描述目标得以实现时的业务结果。
8. 相关方针策略——描述与实现目标相关的其他方针策略，通常通过提供关于特定主题的附加详细信息的方式来实现。

注：方针策略的内容可用多种方式进行组织。例如，强调规则和责任的组织，可简化对目标的描述，并采用专门描述责任的原则。

下面是一个信息安全方针的示例，展现了其结构和示例内容。

信息安全方针（示例）

方针概要

信息宜始终加以保护，而不管其以什么形式存在和如何进行共享、沟通或存储。

引言

信息能以多种形式存在。它能打印或写在纸上、以电子方式存储、用邮寄或电子手段传送、呈现在胶片上或用语言表述。

信息安全是保护信息免受各种威胁的损害，以确保业务持续性、业务风险最小化，以及投资回报和业务机遇最大化。

范围

本方针支持组织的总安全方针。

本方针适用于组织的所有部门。

信息安全目标

1) 要理解战略层面和运行层面的信息安全风险，并将其处理到组织可接受的程度；
2) 要保护客户信息、产品开发和市场计划的保密性；
3) 要保存账目记录的完整性；
4) 公共 Web 服务和内部网络要满足特定的可用标准。

信息安全原则

1) 组织鼓励风险承担和容忍那些在保守管理的组织中可能不被容忍的风险，假设该信息风险可被理解、监视并在必要时进行处置。风险评估及处置的方法细节见 ISMS 方针；
2) 所有员工都要知悉与其岗位角色相关的信息安全，并对其负责；
3) 要制定资助运行及项目管理过程中的信息安全控制措施的相关规定；
4) 在整个信息系统管理中，要考虑到与滥用信息系统相关的欺骗的可能性；
5) 信息安全状态报告要可用；
6) 信息安全风险要加以监视，并当发生变化以致产生不可接受的风险时，采取适当的措施；
7) ISMS 方针策略中要包括风险分类和风险接受的准则；
8) 不允许可能使组织违背法律法规和规章的情形出现。

责任

1) 高级管理组负责确保信息安全在整个组织中得到充分强调；
2) 每一个高级管理者负责确保在其控制下工作的人员依照组织的标准对信息进行保护；
3) 首席安全官建议高级管理组，为组织的员工提供专家支持，并确保信息安全现状报告可用；
4) 每一个员工都具有信息安全责任，这是其工作的一部分内容。

关键结果

1) 信息安全事件不会导致严重的和意外的代价，或服务和业务活动的严重中断；
2) 欺骗带来的损失是可知的，并在可接受的范围内；
3) 客户对产品或服务的接受不会受到信息安全问题的负面影响。

相关方针策略

以下具体的方针策略就信息安全的特定方面，提供了原则和指导：

1) 信息安全管理体系(ISMS)方针；
2) 访问控制方针策略；
3) 桌面清空和屏幕清空方针策略；
4) 未授权软件的方针策略；
5) 关于从(或通过)外部网络获得软件文件的方针策略；
6) 关于移动代码的方针策略；
7) 备份方针策略；
8) 关于组织之间信息交换的方针策略；
9) 关于电子通信设施的可接受使用的方针策略；
10) 记录保存方针策略；
11) 关于网络服务的使用方针策略；
12) 关于移动计算和通信的方针策略；
13) 远程工作方针策略；
14) 关于密码控制的使用方针策略；
15) 符合性方针策略；
16) 软件许可方针策略；
17) 软件处置方针策略；

18） 数据保护和隐私方针策略。

所有这些方针策略支持：

a） 风险识别，通过提供控制措施基线的方式，可用于识别系统设计和实施上的差距；

b） 风险处置，通过支持对已识别的脆弱性和威胁的处置选项的识别的方式。

风险识别和风险处置都是在方针策略的“原则”部分所定义的过程中。详情参见“ISMS 方针策略”。

附 录 E
（资料性附录）
监视和测量

本附录就支持监视和测量的规划和设计，提供了另外的指导。

建立监视和测量的信息

ISMS 特定要求的设计包括支持管理评审的 ISMS 安全监视和测量方案。

监视的设计

图 E.1 展示了监视过程的流程。

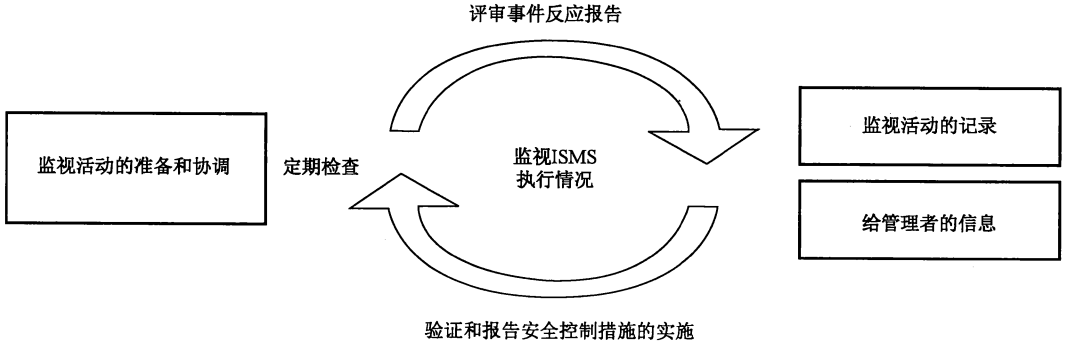


图 E.1 监视过程的流程

准备和协调：识别需要监视的相关资产

宜注意到，监视是一个持续的过程。因此设计时，宜考虑监视过程的建立及设计实际的监视需求和活动。作为设计的一部分，这些活动需要进行协调。

基于先前由所定义的范围和资产建立的信息，结合风险分析和控制措施选择的结果，可以定义监视的目标。这些目标宜包括：

a) 发现什么；

b) 什么时候；

c) 针对什么。

在实际中，先前已建立的组织活动/过程及相关联的资产是监视的基本范围（上述的“针对什么”）。为了设计监视，需要从信息安全的角度来进行选择，以涵盖重要的资产。为了找出在资产和相关联的组织活动/过程方面宜监视的内容，还宜考虑风险处置和控制措施的选择。（这将建立“发现什么”和“什么时候”。）

由于监视可能涉及法律方面的问题，因此检查监视的设计使其不涉及任何法律问题是最基本的。

为确保监视真实有效，对所有监视活动进行协调并进行最终设计是重要的。

监视活动

为了保持信息安全水平，已被适当识别的信息安全控制措施宜获得正确地应用；安全事件宜被发现并及时做出反应，宜定期对信息安全管理体系的执行情况进行监视。宜进行定期检查，以了解是否所有的控制措施都按信息安全的规划得到应用，并按计划予以实施。这宜包括检查技术控制措施（例如，有关配置）和组织控制措施（例如，过程、规程和操作）是否符合要求。检查宜主要针对修补中的缺陷。如果检查要获得接受，那么重要的是其动机要得到与检查目标相关的所有人员的认可。重要的是，在检查期间要与参与者讨论问题的可能解决方案，并预备适当的修补措施。

宜仔细地准备检查，以确保尽可能有效地达到目标，同时，尽可能少地中断日常工作。一般的检查

宜预先与管理者进行协调。设计活动可能以三种不同的基本形式进行总结：

a) 事件报告；

b) 控制措施功能的验证或不符合性；

c) 其他定期检查。

进而，活动的结果宜根据如何做记录和向管理层提交信息，进行设计。宜编制正式的文件，来描述设计和所涵盖的原则活动及其目的，以及不同的责任。

对监视结果的要求

其结果是：

a) 达到所要求的详细程度的监视活动记录；

作为监视活动的结果，宜提供一个管理报告。管理者为了完成其管理和监督职责而要求的所有信息，都宜以所要求的详细程度记录在管理报告中。

b) 需要迅速行动时，为管理者决策而提交的信息。

管理报告宜总是以一个具有清晰的优先顺序的推荐的措施列表来结束，该列表中包含了对每个措施的预期实施成本的实际评估。这就确保能适时地从管理者处获得所需要的决定。

建立信息安全测量方案

设计信息安全测量方案的概述

测量过程宜无缝地集成到项目或组织的 ISMS 周期中，并用于实现安全相关过程和项目或组织内结果的持续改进。这称作信息安全测量方案(GB/T 31497—2015)。方案的设计需要从 ISMS 周期的视角进行观察。下图描述了测量过程如何适配于 ISMS 周期。

下面的功能是管理体系所需要的，以确保满足所要求的事宜和期望，诸如，架构必要的 PDCA；测量输出及其有效性的确认；为过程的管理者提供测量结果的反馈。

为了适当地安排正确的测量，先前产生的信息是重要的，特别是：

a) ISMS 方针，包括范围和边界；

b) 风险评估结果；

c) 控制措施的选择；

d) 控制目标；

e) 特定的信息安全目标；

f) 指定的过程和资源及其分类。

管理者宜建立和保持对全部测量过程的承诺。在实施测量的过程中，管理者宜：

a) 接受测量要求；详情见 GB/T 31497—2015；

b) 关注信息需求，详情见 GB/T 31497—2015；

c) 通过下列方面，取得员工承诺：

1) 组织宜通过某些措施证明其承诺，例如，组织的测量方针策略、责任和义务的分配、培训、预算和其他资源的分配；

2) 宜指派负责测量方案的人员或组织部门；

3) 该指派的人员或组织部门负责在整个组织内沟通 ISMS 测量的重要性和结果，以确保测量得到接受和使用，并宜获得管理者的支持；

4) 确保 ISMS 测量数据得以收集、分析以及向 CIO 和其他利益相关方报告；

5) 教育计划生产线的管理者关于使用方针策略、资源分配和预算决策的 ISMS 测量结果。

信息安全测量的方案及其设计宜包括以下角色：

a) 高级管理者；

b) 安全产品的使用者；

c) 信息系统负责人；

d) 信息安全负责人。

信息安全测量方案的制定是为了得到 ISMS、控制目标和控制措施的有效性的指标。该方案在 GB/T 31497—2015 中描述。

“规划(P)阶段”的适当测量结果宜得到执行,以完成这些目标。

适当的信息安全测量方案可以不同,这取决于组织结构的:

a) 规模;

b) 复杂性;

c) 信息安全的总体风险概况/需求。

通常,一个组织越大、越复杂,需要的测量方案就越大。但是总体风险的水平也影响了测量方案的范围。如果信息安全问题的影响是严重的,那么一个相对小的组织,与没有面临同样影响的大型组织相比,可能需要一个更全面的测量方案才能覆盖风险。测量方案的范围可以根据需要涵盖的控制措施的选择和风险分析的结果,来进行评价。

信息安全测量方案的设计

信息安全测量方案的负责人宜考虑以下事项:

a) 范围;

b) 测量方法;

c) 测量的执行;

d) 测量周期;

e) 报告。

测量方案的范围宜涵盖 ISMS 的范围、控制目标和控制措施。特别是,ISMS 测量的目标和边界宜根据业务、组织、位置、资产和技术等方面的特征,来加以确定,并且包括对任何 ISMS 范围删减的详细说明和正当性理由。这可以是单个的安全控制措施、一个过程、一个系统、一个功能区域、整个企业、单一场所或多场所的组织。

当选择了单一测量方法时,GB/T 31497—2015 的“信息安全测量过程”规定了起点是测量的对象。为了建立测量方案,宜识别这些对象。这些对象可以是过程或资源(详情见 GB/T 31497—2015)。在定义方案时,ISMS 范围所定义的对象通常被分解成易于查找的、宜被测量的实际对象。这个定义过程可以用下面的示例来说明:组织是整体对象(组织过程 A/或 IT 系统 X 是该整体对象的一部分,而其本身也构成一个对象)。为了观察保护信息的有效性,影响信息安全的该过程内的众多对象(人员、规则、网络、应用和设施等)通常是测量对象。

在实施一个信息安全测量方案时,宜仔细考虑到测量对象可能服务于 ISMS 范围内的许多组织过程,因此可能对 ISMS 和控制目标的有效性有较大的影响。通常,这些对象,诸如安全组织和相关联过程,计算机大厅和信息安全相关的合作人员等,宜在方案的范围内优先考虑。

测量时间间隔可能变动,但是为了配合管理评审、持续的改进过程和 ISMS 期望,在特定的时间间隔内执行或总结测量是最好的。方案的设计宜陈述这一点。

宜按照 GB/T 31497—2015 设计测量结果报告,以确保沟通。

信息安全测量方案的设计宜以一个符合规程的文件结束。这个文件宜得到管理者的批准。这个文件宜包括以下内容:

a) 信息安全测量方案的责任;

b) 沟通的责任;

c) 测量的范围;

d) 如何执行(使用的基本方法、外部和内部执行等);

e) 宜何时执行;

f) 如何报告。

如果组织开发其自己的测量要点，那么这些要点必须作为设计阶段的一部分被文件化（详情见GB/T 31497—2015）。这个文件可以非常全面，并可不必由管理者签署，因为细节可能在实施时发生变化。

ISMS 有效性的测量

在设置宜被实施的信息安全测量方案的范围时，要注意对象不要太多。如果对象太多，那么可将方案划分成不同的部分。这些部分的范围可看作独立的测量以便比较，但其主要目的是：将这些测量组合起来，就可提供一个评价 ISMS 有效性的指标。这些子范围通常是一个具有清晰边界定义的组织部门。在这些子范围内，作为对象的许多组织过程和测量的众多对象，组合在一起，就可形成一个信息安全测量方案的适当范围。这也可看作一系列具有两个以上过程/对象构造的 ISMS 活动。因此，整个 ISMS 的有效性可根据这些具有两个以上过程/对象的测量结果，进行测量。图 E.2 给出了一个示例：两方面有效性的测量：ISMS 的 PDCA 过程和组织内过程的示例。

由于目标是测量 ISMS 的有效性，因此对控制目标和控制措施进行测量是重要的。足够数量的控制措施是一方面，另一方面则是这些控制措施对于评价 ISMS 的有效性来讲是充分的。（可能还有限制信息安全测量方案范围的其他理由，这在 GB/T 31497—2015 中提到）。

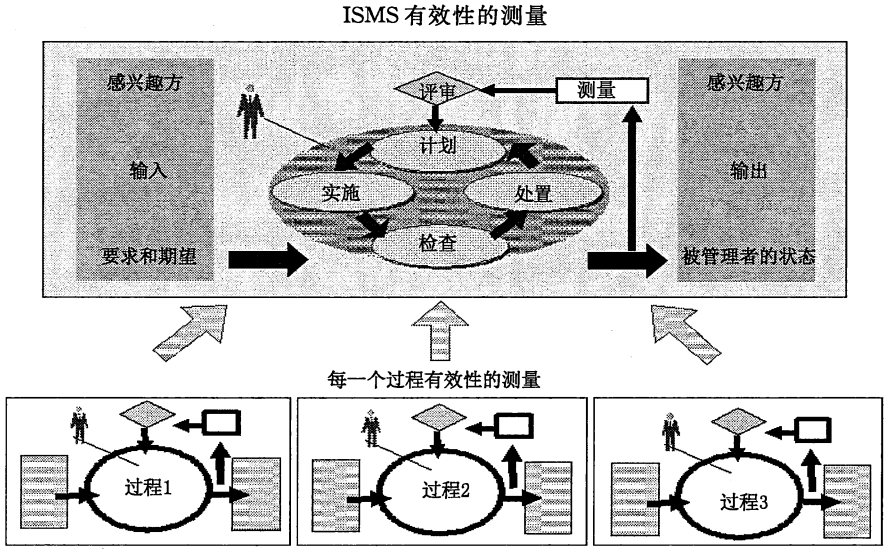


图 E.2　两方面的有效性的测量：ISMS 的 PDCA 过程和组织内过程的示例

在使用测量结果来评价 ISMS、控制目标和控制措施的有效性时，管理者了解信息安全测量方案的范围，这一点是最根本的。测量方案的负责人在信息安全测量方案发布之前，宜获得管理者对该范围的批准。

注 1：GB/T 22080—2008 中有关有效性测量的要求是："测量控制措施或控制措施集"（见 GB/T 22080—2008 的 4.2.2 d）。

注 2：GB/T 22080—2008 中有关 ISMS 有效性的要求仅是"整个 ISMS 有效性的评审"，而对"整个 ISMS 的测量"没有要求（见 GB/T 22080—2008 的 0.2.2）。

实际执行测量时，可使用内部人员或外部人员，或两者相结合。在评价内部或外部资源时，组织的规模、结构和文化都是要考虑的因素。小型和中等规模的公司相比大型组织而言，在使用外部支持时会得到更多的益处。使用外部资源的结果也可能提供一个更有效的结果，这取决于组织文化。如果组织习惯于内部审核，那么内部资源同样有效。

参 考 文 献

[1] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则(IDT ISO/IEC 27002:2005)

[2] GB/T 31497—2015 信息技术 安全技术 信息安全管理 测量(IDT ISO/IEC 27004:2009)

[3] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理(IDT ISO/IEC 27005:2008)

[4] GB/T 25067—2010 信息技术 安全技术 信息安全管理体系审核认证机构要求(IDT ISO/IEC 27006:2007)

[5] ISO 9001:2008 质量管理体系 要求(Quality management systems—Requirements)

[6] ISO 14001:2004 环境管理体系要求及使用指南(Environmental management systems—Requirements with guidance for use)

[7] ISO/IEC 15026(所有部分) 系统和软件工程 系统和软件保证[1)](Systems and software engineering—Systems and software assurance)

[8] ISO/IEC 15408-1:2009 信息技术 安全技术 IT安全评估准则 第1部分:介绍和一般模型(Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model)

[9] ISO/IEC 15408-2:2008 信息技术 安全技术 IT安全评估准则 第2部分:安全功能组件(Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional components)

[10] ISO/IEC 15408-3:2008 信息技术 安全技术 IT安全评估准则 第3部分:安全保证组件(Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance components)

[11] ISO/IEC TR 15443-1:2005 信息技术 安全技术 IT安全保证框架 第1部分:概述和框架(Information technology—Security techniques—A framework for IT security assurance—Part 1: Overview and framework)

[12] ISO/IEC TR 15443-2:2005 信息技术 安全技术 IT安全保证框架 第2部分:保证方法(Information technology—Security techniques—A framework for IT security assurance—Part 2: Assurance methods)

[13] ISO/IEC TR 15443-3:2007 信息技术 安全技术 IT安全保证框架 第3部分:保证方法分析(Information technology—Security techniques—A framework for IT security assurance—Part 3: Analysis of assurance methods)

[14] ISO/IEC 15939:2007 系统和软件工程 测量过程(Systems and software engineering—Measurement process)

[15] ISO/IEC 16085:2006 系统和软件工程 生存周期过程 风险管理(Systems and software engineering—Life cycle processes—Risk management)

[16] ISO/IEC 16326:2009 系统和软件工程 生存周期过程 项目管理(Systems and software engineering—Life cycle processes—Project management)

---

1) 部分已发布。

参 考 文 献

[17] ISO/IEC 18045:2008 信息技术 安全技术 IT安全评估方法学(Information technology—Security techniques—Methodology for IT security evaluation)

[18] ISO/IEC TR 19791:2006 信息技术 安全技术 操作系统的安全评估(Information technology—Security techniques—Security assessment of operational systems)

[19] ISO/IEC 20000-1:2005 信息技术 服务管理 第1部分:规范(Information technology—Service management—Part 1: Specification)

[20] ISO/IEC 27001:2005 信息技术 安全技术 信息安全管理体系 要求(Information technology—Security techniques—Information security management systems—Requirements)

[21] ISO 21500:2012 项目管理 项目管理操作(Project management—Guide to project management)

GB/T 31496-2015

*

书号:155066·1-51118

定价: 48.00元

打印日期:2015年8月10日 F009