

信息技术-安全技术

信息安全管理体系实施指南

**(Information technology — Security techniques — Information
security management system implementation guidance)**

(ISO/IEC CD 27003)

(2009-12-29)

作者	刘斌
版本	V2.1
备注：该文本为 ISO 27003 2008-06-12 英文版翻译版，文档中还有一些不足之处(附录未认真翻译)请提出宝贵意见，以便相互学习和进步。	
刘斌： MSN: liubin_rocn@hotmail.com QQ:547051328	

目录

1 范围.....	6
2 引用的标准文件.....	6
3 术语和定义.....	6
4 本标准的结构.....	6
4.1 总则.....	6
4.2 图表.....	7
4.2.1 图形符号.....	7
4.2.2 部署与图表.....	9
4.3 ISMS 实施总图	9
4.4 总说明.....	10
4.4.1 实施考虑事项.....	10
4.4.2 中小企业(SME)的考虑事项.....	11
5 获得管理者对实施 ISMS 的正式批准.....	12
5.1 管理者对实施 ISMS 正式批准的概要.....	12
5.2 定义 ISMS 的目标、信息安全需要和业务要求.....	14
5.3 定义最初的 ISMS 范围.....	16
5.3.1 ISMS 范围的概要	16
5.3.2 角色和责任的定义.....	16
5.4 创建业务框架与项目启动计划.....	18
5.5 获得管理者对实施 ISMS 的正式批准和承诺.....	19
6 定义 ISMS 范围和 ISMS 方针.....	22
6.1 定义 ISMS 范围和 ISMS 方针的概要	22
6.2 定义组织的边界.....	24
6.3 定义信息通信技术边界.....	25
6.4 定义物理边界.....	25
6.5 完成 ISMS 范围边界.....	26
6.6 开发 ISMS 方针.....	27
7 进行业务分析	29
7.1 业务分析的概要.....	错误！未定义书签。
7.2 定义支持 ISMS 的信息安全要求.....	错误！未定义书签。
7.3 创建信息资产清单.....	错误！未定义书签。
7.4 产生信息安全评估.....	错误！未定义书签。
8 进行风险评估.....	错误！未定义书签。
8.1 风险评估概要.....	错误！未定义书签。
8.2 风险评估描述.....	错误！未定义书签。
8.3 进行风险评估.....	错误！未定义书签。
8.4 计划风险处理和选择控制措施.....	错误！未定义书签。
8.4.1 风险处理和选择措施选择概要.....	错误！未定义书签。
8.4.2 识别风险处理选择方案.....	错误！未定义书签。

8.4.3 选择控制目标和控制措施.....	错误! 未定义书签。
9 设计 ISMS	43
9.1 设计 ISMS 概要	错误! 未定义书签。
9.2 设计组织的安全.....	错误! 未定义书签。
9.2.1 组织的安全概要.....	错误! 未定义书签。
9.2.2 角色和责任.....	错误! 未定义书签。
9.2.3 方针开发框架.....	错误! 未定义书签。
9.2.4 报告和管理评审.....	错误! 未定义书签。
9.2.5 规划审核.....	错误! 未定义书签。
9.2.6 意识.....	55
9.3 设计 ICT 安全和物理安全	错误! 未定义书签。
9.4 设计监视和测量.....	58
9.4.1 监视和测量的概要.....	错误! 未定义书签。
9.4.2 设计监视.....	错误! 未定义书签。
9.4.3 设计信息安全测量程序.....	错误! 未定义书签。
9.4.4 测量 ISMS 的有效性.....	错误! 未定义书签。
9.5 ISMS 记录的要求	错误! 未定义书签。
9.5.1 ISMS 记录的概要	错误! 未定义书签。
9.5.2 文件要求的控制.....	错误! 未定义书签。
9.5.3 记录要求的控制.....	错误! 未定义书签。
9.6 产生 ISMS 实施计划.....	错误! 未定义书签。
10 实施 ISMS	错误! 未定义书签。
10.1 ISMS 实施概要	错误! 未定义书签。
10.2 执行 ISMS 实施项目.....	错误! 未定义书签。
10.2.1 执行 ISMS 实施项目概要.....	错误! 未定义书签。
10.2.2 角色和责任.....	错误! 未定义书签。
10.2.3 沟通.....	错误! 未定义书签。
10.2.4 协调.....	错误! 未定义书签。
10.2.5 变更.....	错误! 未定义书签。
10.3 监视的实施.....	错误! 未定义书签。
10.4 ISMS 程序和控制文件.....	错误! 未定义书签。
10.5 ISMS 测量程序文件	错误! 未定义书签。
参考书目.....	78
附录 A	79
附录 B	81

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）是专业的世界性标准发布者。ISO 或 IEC 成员的国家，通过各自组织为处理特定技术活动领域所设立的技术委员会，参与开发国际标准。ISO 和 IEC 技术委员会协调合作领域的共同利益。与 ISO 和 IEC 保持联系的其它国际组织（官方的或非官方的）也可参加有关工作。在信息技术领域，ISO 和 IEC 已经设立了一个联合技术委员会，ISO/IEC JTC 1。

国际标准遵照 ISO/IEC 导则第 2 部分的规则起草。

本文件的某些要素有可能涉及一些专利权问题，对此应引起注意。ISO 不负责识别任何专利权的问题。

ISO/IEC 27003 是由信息技术-安全技术 SC 27 小组委员会 ISO/IEC JTC 1 技术委员会制定的。

引言

本标准的目的是为基于 ISO/IEC 27001 的信息安全管理体系（ISMS）提供实用指导。
ISO/IEC 27001 在一个组织内为业务提供信息化管理。信息安全的目的在于：

- a) 保护信息免受各种不同的威胁(例如：故障、信息与服务的损失、盗窃和间谍)；
- b) 支持符合法律、法规和合同的安全要求；
- c) 维护连续性；
- d) 最小化损害；
- e) 促进效率。

本标准旨在支持信息安全管理的过程，确保相关利益方的信息资产(包括信息过程)满足该组织所定义的可接受的风险级别。

本标准所描述的实施过程已经进行了设计，以提供：

- a) 说明以一套基础方针、程序和控制措施所表示的组织的信息安全管理体系；
- b) 持续改进的基础；
- c) 基于业务目标、当前情况差距分析和风险分析的结果考虑时的协调框架。

本标准不包括 ISMS 的运行或监视。ISMS 的最终实施是一个有关技术层面和组织层面的实施项目，那里，需要应用项目管理原理和方法论(见“ISO 项目管理标准”)。

采用 ISMS 是商业与公共管理组织(包括公司、公营机构和慈善团体等)的一项战略性决策。随着 IT 的使用和依赖性的增长，对实施 ISMS 的决定和承诺十分关键。

信息技术-安全技术

信息安全管理体系实施指南

1 范围

本国际标准依照 ISO/IEC 27001，为建立和实施信息安全管理体系提供实用指导。本文件描述 ISMS 的实施，聚焦于从最初批准 ISMS 在组织内实施到 ISMS 运行的开始，相当于 ISMS PDCA 周期的“P”和“D”阶段。

本文件包括有关运行、监视、评审和改进设计活动的解释，虽然这些活动本身不在实施的范围。

本标准适用于所有商业规模和类型的所有组织（例如，商业企业、政府机构、非赢利组织）。本标准旨在为依照 ISO/IEC 27001 实施信息安全管理体系的组织使用，以及为安全专业人员提供指导。

风险管理或测量等有关方面的主题覆盖于 ISMS 标准族的其它标准，并被适当引用。

2 引用的标准文件

下列引用文件对于本文件的应用是必不可少的。凡是注有日期的引用文件，只是引用的版本。凡是不注有日期的引用文件，其最新版本（包括任何修改）适用于本标准。

- ISO/IEC 27001, *信息安全管理体系 - 要求*

3 术语和定义

为了本文件的目的，以下的术语和定义适用于本标准：

- ISO/IEC 27001, *信息安全管理体系 - 概述与词汇*
- ISO/IEC 27001, *信息安全管理体系 - 要求*

4 本标准的结构

4.1 总则

本文件描述信息安全管理体系的实施。实施是一个时间性的活动，而本文件描述为项目活动。实施项目分为多个不同阶段，而每一个阶段在本文中也是一个单独的条款。

每一个 ISMS 实施阶段包含：

- 一个要达到的目标；
- 一个或多个为达到该阶段目标所必需的活动。

活动描述按以下内容结构进行：

活动

定义满足全部或部分该阶段目标所必需的特殊活动。

输入

描述每一个活动的开始点，例如现有形成文件的决定，或来自于其它ISMS实施活动的输出。

实施指南

提供更加详细的信息，以支持该实施阶段的目的和达到该阶段的目标。虽然组织的规模和ISMS范围的最终规模要影响活动的复杂性，但是每一个活动所必需的输出都是同样不依赖这些因素。

输出

描述该活动的结果或可交付的完成产品，例如文件。

其它信息

提供可能有助于达到该阶段目标的补充信息，例如对其它标准的引用文件或另外的SMEs指南。不是所有活动都有其它信息。

整个项目应使用一个图表，图示各个不同的阶段及其输出。而每一个阶段也要有图表，以图示出该阶段内的各个不同工作块。ISMS的实施包括来自其它ISMS系列标准的支持。这些标准在适当时也可作为引用文件，并作为有用的输入在图表中进行描述。

4.2 图表

4.2.1 图形符号

图1提供本文件后面的流程图所使用的图形符号。这些图形为实施ISMS提供很形象的指导和过程。

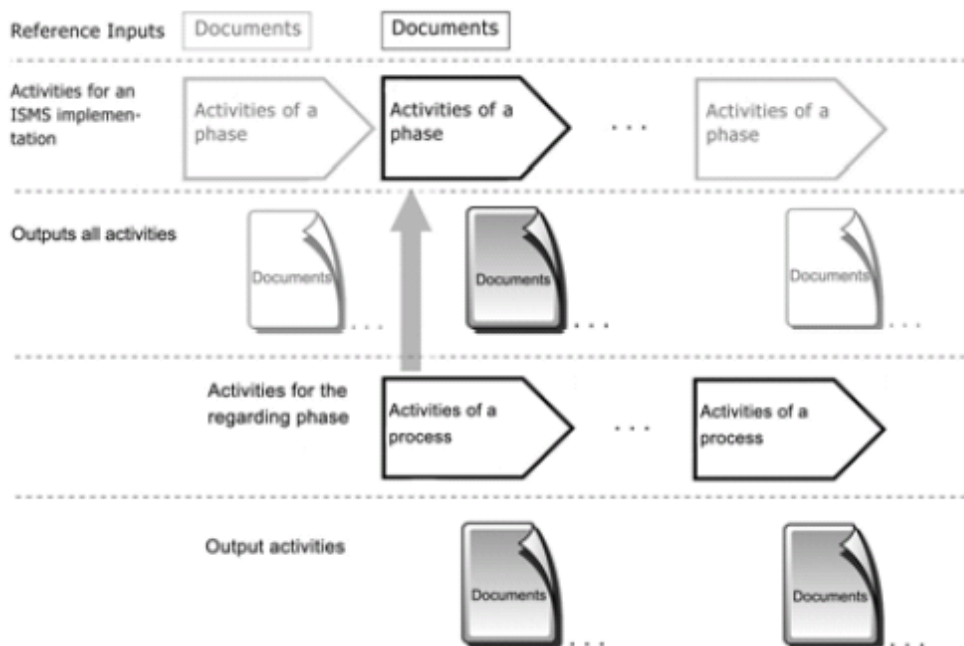


图 1 流程图图形

在本国际标准中，流程图的图形排列是基于以下结构概念：

- 矩形框(无阴影的)：
矩形框提供信息的说明。当执行任务需要超出本标准范围的信息时，以无填充的框图表示，如在图4.1中描述为“必须的信息”。这种必须的信息可以是其它标准引用文件，如ISO/IEC 27002。
- 矩形框(有阴影的)：
矩形框表示“形成文件的结果”。在矩形框，信息以灰色填充，并产生作为本标准的一部分的一个文件。
- 箭头框：
箭头框表示活动或要执行的工作。
- 箭头框可先分成多个子任务/活动，然后以多个新的箭头框表示。所有箭头框的右底部都有一个数字，表示本标准的章节(在图1中，以“x.x”表示)。
- 项目流程是各种活动的顺序流动，并以多个箭头框表示。项目流程可并行地完成。
- 图中的箭头表示时间，并以从左到右的方向。箭头也指出某些活动应在下一个活动开始之前完成，或者可以并行地完成。

4.2.2 部署与图表

所有阶段都被指定为一个条款。首先，每一个条款都有说明该阶段及其主要活动的图表。然后，一个阶段内的每一个主要活动是该条款的一个子节。如果在一个活动中有许多主题，那么这些主题可作为多个子条款进行介绍，但不以图表说明。为了支持正文，也可以插入各种其它的图形或图表，但可不遵循如图1所述的图形符号。

每一个阶段和活动在开始时都有目标，而其内容应支持该目标。

另外的支持性信息，例如例子，应以附录提供。

4.3 ISMS 实施总图

图2 图解 ISO/IEC 27003 的范围。

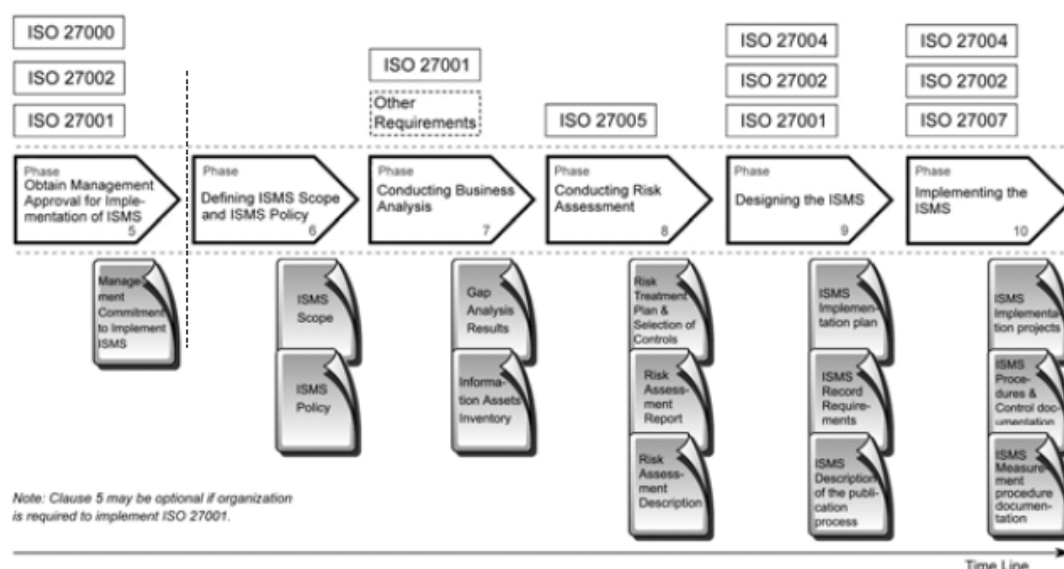


图2 ISMS 项目概要与每一阶段的结果

在图2中，每一阶段的目标概要解释如下：

- 第5章“获得实施ISMS的正式批准”，其目标是：
 - ✧ 定义实施ISMS的目标、信息安全需要和业务要求；
 - ✧ 定义最初的ISMS范围；
 - ✧ 创建业务框架与项目启动计划；
 - ✧ 获得管理者对实施ISMS的正式批准和承诺。
- 第6章“定义详细的ISMS范围和ISMS方针”，其目标是：
 - ✧ 定义ISMS的范围边界；
 - ✧ 获得对ISMS方针的赞同。

- 第7章 “进行业务分析”，其目标是：
 - ✧ 收集ISMS支持的相关要求；
 - ✧ 收集当前ISMS范围内的信息安全状况；
 - ✧ 创建信息资产清单。
- 第8章 “进行风险评估”，其目标是：
 - ✧ 识别风险评估方法；
 - ✧ 识别、分析和评价信息安全风险；
 - ✧ 识别风险处理选择方案；
 - ✧ 选择控制目标和控制措施。
- 第9章 “设计ISMS”，其目标是：
 - ✧ 为基于风险处理选择方案的风险处理，而设计组织的安全；
 - ✧ 为降低风险，结合ICT、物理安全和组织安全，而设计选择的控制目标与控制措施；
 - ✧ 为建立ISMS，设计ISMS特殊的要求，包括监视和测量；
 - ✧ 制定ISMS实施计划。
- 第10章 “实施ISMS”，其目标是：
 - ✧ 根据ISMS项目计划，实施已选择的控制措施和ISMS特殊的要求；
 - ✧ 实施监视和测量；
 - ✧ 创建ISMS程序和控制文件。

4.4 总说明

4.4.1 实施考虑事项

实施的目标是达到符合 ISO/IEC 27001 要求的持续改进的状态。

信息安全是持续动态性变化的，需要进行设计以适应变化。每一个组织都受支配于内部变化和外部变化。由于业务过程、法规环境、任务、基础设施和组织可能发生变化，许多这些变化也影响信息安全。某些主要条件的变化也可能出现，例如，法律约定或合同约定、可用信息和通信技术都可能发生重大变化。为了达到组织的业务目标及其风险耐受度，管理和维护信息安全是必须的。

不仅计划实施业务过程和引入具有商定的信息安全控制措施的新信息系统是重要的，而且计划其应如何运行和有规律地进行检查以确保其如期的有效性和适用性也是重要的。如果脆弱点或改进的机会被发现，则应采取控制措施，进行改进。过程应支持这些改进的计划和实施。当业务过程被终止，或者组分和/或信息系统被更换或关闭，必须考虑相关的信息安全问题，例如授权的取消或硬件的安全删除。

为了应对信息安全需要例如管理过程、支持实施和认可更新需要，一个组织内的相关角色和责任识别于附录 A 中。附录 A 提供信息安全关键角色和责任的指导。

4.4.2 中小企业(SME)的考虑事项

本标准所述的实施项目可以是很复杂的，因为它或多或少涉及到整个组织。应该提出的是，在实际中，大组织实施 ISMS 比小组织更复杂。小组织没有很多角色，而且 ISMS 的边界十分清楚定义，信息资产的控制也更容易完成。

本标准描述实施 ISMS 所需要的活动，特别是中型到大型的企业。较小的组织会发现本标准所提的活动可适用于他们，并可以进行简化。

不管企业的规模如何，对于一个特定组织来说，复杂性和风险都是独特的，而特定的要求会驱动实施的指导。

5 获得管理者对实施 ISMS 的批准

5.1 管理者对实施 ISMS 批准的概要

目标:

- 定义实施信息安全管理体的目标、信息安全的需求和业务要求;
- 定义初始的 ISMS 范围;
- 创建业务框架和启动项目;
- 获得管理者对实施 ISMS 的批准和承诺。

参见 **ISO/IEC 27001: 4.2.1 a), b)**

在本阶段(即“获得管理者对实施 ISMS 的批准”)开始之前,最重要的是要明白什么是 ISMS、ISMS 的业务需求和当前与信息安全相关的组织内的角色与责任的列表。

本阶段的预期输出是管理者对实施 ISMS 的批准和承诺。因此从此条款可提交包括一个业务框架和一个具有关键重要事件的建议草案。

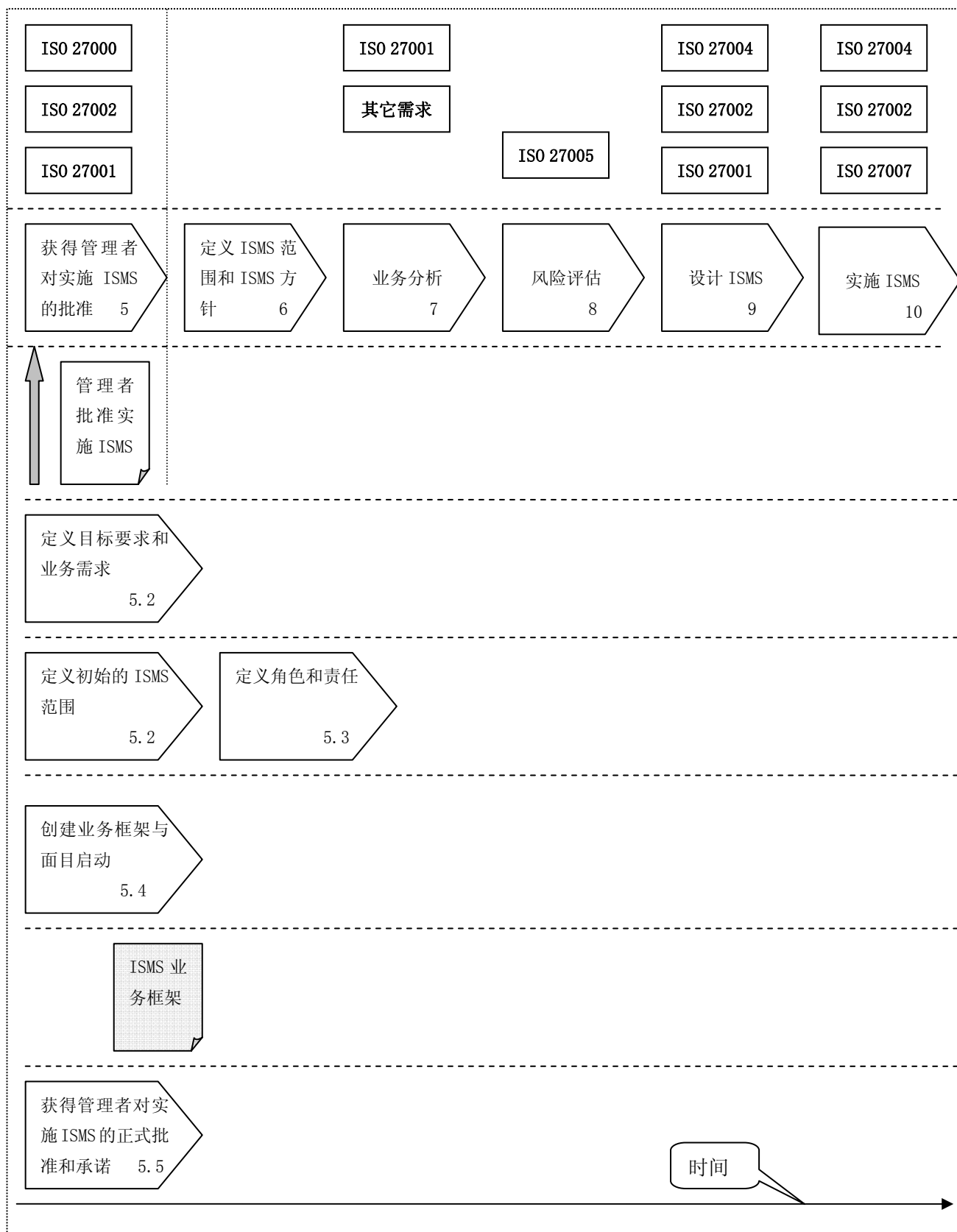


图 3 管理者对实施 ISMS 正式批准的概要

5.2 定义 ISMS 的目标、信息安全需求和业务要求

活动

定义实施ISMS的目标、信息安全需求和业务要求。

输入

按如下信息完成此项活动是很重要的：

- 达到企业的业务目标的途径；
- 了解现有管理体系。

实施指南

实施ISMS时，应考虑如下问题：

- 风险控制 - ISMS如何更好的控制信息安全风险？
- 效率 - ISMS如何提高处理信息安全的效率？
- 业务优势 - ISMS如何创造业务优势？

一些管理目标的实例包括：

- 促进业务连续性和灾难恢复
- 促进对事故的恢复力
- 法律/合同符合性/债务(例：SOX、DPA)
- 支持ISO 9001、14001、20000和27001认证
- 有利于业务发展和定位
- 使风险和安全能够进行测量与度量
- 降低安全控制措施成本
- 保护资产的战略价值
- 促成“企业风险管理”(ERM)过程
- 建立一个达到保证健康的“控制环境与有效控制组件”

上述目标带来的利益包括：

- 法律符合性 - 好的信息安全导致符合整个地区和地方法律；
- 合同符合性 - 好的信息安全改善符合合同的承诺；
- 行业标准符合性 - 将行业标准纳入信息安全流程和信息安全要求，以解决该标准的符合性；
- 效率 - 信息安全设计导致有效使用多个安全流程；
- 业务优势 - 实施信息安全可帮助取得更多新订单，并能够把信息安全计算到该成本中；
- 风险控制 - 信息安全获得适当解决，也就支持了管理风险；
- 信任 - 实施信息安全可使该组织获得更多业务环境方面的信任，如其能够更容易对其它管理组织(外部审核)作出反应、提高反应质量(信任)；
- 环境理解 - 关键的信息活动和保护该类型信息有助于处理继续发生的各种威胁。

因此，管理目标可能是上述的任何一个或多个，也可以是不同的。

ISMS的基本需要应包括该组织所面临的有关信息安全方面的列入清单的更多考虑事项。
组织需要解决的主题包括以下方面：

内部影响和外部影响：

- 要求信息安全的相关法律
 - 什么法律与该组织有关？
 - 一个公众的全球性公司的组织部门需要财务外部报告吗？
- 有关由于缺乏信息安全而导致诉讼的合同协议或商业协议
 - 什么是存储要求？
 - 是否有任何秘密的或质量（例如：服务级别协议- SLA）合同要求？
- 有关需要信息安全的行业要求
 - 有什么特殊的行业要求适用于本组织？
- 有关需要信息安全的环境要求
 - 需要什么类型的保护并预防哪些威胁？
 - 需要保护的信息群有哪些不同的类型？
 - 需要保护的信息活动有哪些不同的类型？
- 敏感或有价值的信息需要信息安全
 - 什么信息属于组织的关键信息？
 - 如果这类信息被泄露给未经授权方会产生什么后果（例如：失去竞争优势、损害组织的品牌/名誉等）？
- 竞争驱动
 - 要考虑信息安全市场最小的要求是什么？
 - 如果实施，什么是创建商业优势的另外的信息安全市场要求？
- 业务连续性要求
 - 对于关键业务流程中断，组织可以忍受多长时间？

通过提出某些基本的设想，作为对上述问题的回答，就可以完成定义信息安全需求的活动目标和高层业务要求。这让该组织了解到他们能从执行ISMS得到什么。

输出

这个活动的结果或成果是：

- 总结ISMS的目标、信息安全需求和业务要求的简短文件。

其它信息

如果ISMS正在一个需要满足某些关键规章的要求的行业实施，需要特别考虑补充信息，这包括符合标准、合同承诺和外部施加的政策或任何其它适用的参考文件。特别详细的有关如何识别和使用满足行业特殊需求的扩展控制措施在实施ISMS的“Plan”和“Do”阶段进行讨论。行业实施的例子也提供于附录中，以帮助本文件的用户更好地实施ISMS。

5.3 定义初始的 ISMS 范围

5.3.1 ISMS 范围的概要

活动

定义初始的ISMS范围。

输入

- ISMS 实施目标、业务要求和信息安全要求的文件；
- 适用于本组织的规章、符合性和行业标准的概要。

实施指南

一个清晰的鉴于目标、业务要求和信息安全的文件为决定初始ISMS范围提供基本信息。为了获得管理者批准，初始的范围是需要的。

当考虑范围和ISO/IEC 27001的实施时，组织应首先识别已经作为其它管理体系标准的开发结果在整个组织实施了的共同要素。

一旦各个不同管理体系的共同要素被识别，该组织就应该认可这些已经实施的不同管理体系的要素和ISO/IEC 27001要求的新要素之间的差别，通过采取改编现有的要素或增加新的要素以符合ISO/IEC 27001。

如果组织已经实施其它遵照标准的管理体系，那么它应该考虑现有管理体系是否可以与ISMS结合成一体。作出这个决定所要考虑的一些事宜包括：

- 这些体系的责任是否在各个不同管理团队的领导之下(例如在不同的附属机构或不同的部门)？
- 产生和需要怎样的介绍材料(例如现有管理体系是以纸质文件形成的，而期望ISMS建立为超文本文件)？
- 现有管理体系的功能是否完全按预期进行运行与维护，并支持该组织的需要？

现有管理体系和所提议的ISMS的共同要素应加以识别。

如果所有体系都要进行整合，那么现有体系应进行改编或增补，以使其符合ISO/IEC 27001。如果各个体系不进行结合，那么应考虑再使用公共要素。

输出

一个描述ISMS范围的高层观点，应考虑现有管理体系、规章、符合性和业务目标的文件。

其它信息

5.3.2条款角色和职责提供组织成功地实施ISMS所需要的角色和职责的细节。下一个条款将对此进行详细描述。

5.3.2 角色和责任的定义

信息安全对整个组织具有特殊的重要性。这个ISMS的组织特性使指定组织内的特殊角色十分必要。适当的任务应分配给每一个角色，而这些角色应由具有这些技能的职员担任。这是确保所有重要方面都被考虑到和所有任务都得以有力地 and 有效地完成的唯一方法，。

促进和实施ISMS所需要的组织结构称作信息安全委员会。处理信息安全的人员的数量、组织的结构和资源随组织的规模、类型和结构而变化。对于较小的组织，几个角色可能由同

一个人员担任。然而，首席信息安全官员总是被指定为负责信息安全的關鍵人。在信息安全管理角色的定义上，最重要的考虑是：

- 规定适当安全任务（因信息安全）的总责任保持在管理层。
- 至少指定一个人（通常是首席信息安全官员）进行促进和协调信息安全过程。
- 每一个员工都要在其工作场所和环境下，平等地负起其原任务的责任和维护信息安全的责任。

以下是许多组织典型的主要角色，并在本文件中使用：

角色	负责
高级管理者（如：COO、CEO、CSO 和 CFO）	高级管理人员负责战略决策和协调活动，以指导和控制组织
首席信息安全官	首席信息安全官全面负责实施 ISMS
信息安全委员会（成员）	委员会负责领导组织内实施 ISMS
信息安全规划小组（成员）	规划小组负责实施 ISMS 活动。在实施 ISMS 期间，规划小组的工作跨越部门边界解决冲突和支持 CISO（首席信息安全官）
专家	负责运营（执行）的专家们是一个组织的专业人士。应该按照他们对 ISMS 事件的想法访问这些专家，因为这涉及到其使用在特定的领域。这些专家应该按照他们对 ISMS 事件的专业知识被访问，因为它关系到所在的具体领域。
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提供实施 ISMS 活动的决定。但专家不可能有很深的商业和该组织的运行知识。
雇员/职员/用户	在其工作场所和环境下，每一个员工都要平等地负起维护信息安全的责任。
首席审核员	首席审核员负责设计如何评估和评价 ISMS。
流程负责人	“流程负责人”是业务流程专家应用系统联系人。此人负责委派任务和处理已经被分配到该业务流程内的信息。
ISMS 范围所涉及的部门代表	相关部门代表可以提供执行风险评估和实施控制措施的决定。
其它相关方	所需要的其它相关方是风险评估和控制措施的实施的负责人。例如过程负责人和应用系统专家。这些相关方应要特别地进行定义，以支持管理者对实施 ISMS 的批准过程。
培训师	培训师实施培训和宣传计划。

表1 主要的信息安全角色和责任

为了在建立规划小组时获得正确的经验，本阶段应解决外部或内部需要的专业知识。为了获得一份合理的 ISMS 实施批准文件，通常的情况下需要与其它角色讨论。例如，为了准备

ISMS批准文件，关键流程的“流程负责人”可能是一个需要进行商讨的角色。

此外，风险评估是在ISMS实施中执行。因此，为了识别、分析和评价风险，需要识别ISMS范围所包括的部门和这些部门的代表应加入到ISMS实施成员。

因此，识别ISMS范围所包括的部门且这些部门的参与代表需要进行识别、分析和评价风险。这些部门不仅是ISMS范围所包括的直接单位，而且也包括间接部门，诸如法律部门和行政部门。例如：为了实施包括一切的“管理”，需要人力资源部的代表。

5.4 创建业务框架与项目启动

活动

创建业务框架与初始项目计划。

输入

收集于管理批准文件中的作为一个以往活动结果的业务框架。

实施指南

业务框架与初始项目启动应包括已估算的时间计划和本标准第6章-第9章所述的主要活动所需要的资源。在本阶段的业务框架中，不可能很详细说明，因为许多因素仍然是未知的，所以应估计未来将执行的活动。这个文件作为项目基础，而且还确保管理者对ISMS实施所需要的资源的承诺和批准。

实施ISMS的业务框架可以由以下主题组成：

- 高层目标；
- 特殊目标；
- 关键流程；
- 已经定义的角色和责任；
- 实施组织；
- 实施考虑事项；
- 假定的时间计划(可分开于各个阶段，如本标准所提出的)；
- 假定的成本框架；
- 已经定义的关键的成功因素。

在管理者批准之后，应制定一个详细的项目计划，包括本标准第6章-9章所述的各个阶段的相关活动。第10章包含控制措施的实施。

输出

此活动的输出产生一个有关业务框架与初始项目启动的文件。

其它信息

下一个条款提供更多管理所需要的关键成功因素的细节。

5.5 获得管理者对实施 ISMS 的正式批准和承诺

活动

获得管理者对实施ISMS的批准和承诺。

输入

此活动的输入为业务框架和项目启动, 以及为获得管理者批准和在ISMS实施期间保持承诺而需要理解的事情。

实施指南

重要的是定义ISMS成功实施的关键因素, 因为这是重要的准则, 以增加到业务计划作为与管理者讨论的一部分。

对于实施ISMS的决定, 重要的是使实施人员认可这些ISMS成功实施所需要的关键因素。此章评审这些ISMS成功实施和了解ISMS的利益所需要的关键因素。在证明实施ISMS是正当决定的过程中, 会产生涉及利益的有关的几个问题, 管理这些问题及其结果涉及到这些关键的成功因素。

实施ISMS关键的成功因素是:

a. 管理者承诺

管理者承诺起始于组织决定实施ISMS的需要并继续使用ISMS以帮助管理和发展业务。管理者承诺常常取决于以业务术语所描述的ISMS目标, 因此重要的是要能将信息安全目标转化成业务目标。这对管理有很大关系。

成功的关键因素, 表明管理层的承诺包括:

- 定期检查把ISMS成功实施与业务捆绑的行动计划;
- 管理者批准和监督ISMS实施;
- 为ISMS实施分配独立的预算;
- 创立该组织的关键相关方参加的“信息管理安全论坛”, 并由流程负责人和管理者分担运作问题;
- 评审在可接受风险级别之下和管理者决定不采取任何措施时在可接受准则之上的残余风险。
- 充分的和具有技能的ISMS实施资源。

b. 管理方法

管理方法是一个实施ISMS重要的和关键的成功因素。特别是组织应清楚理解角色、责任、相关方及其对法律要求的符合性、与ISMS实施的关系。此管理方法是指按照一套过程、方针、法律和制度去指导、管理或控制组织。它包括定义组织的目标、了解相关方及其与ISMS的关系。

信息安全的任务和职责可概括为以下几点:

- 负责信息安全

每一个组织的管理者都要负责与该组织目标保持一致的正确运转, 他们也负责确保对其组织的内部与外部的信息安全。根据国家和组织的类型, 可能有需要理解的各种规章和法律。管理者应明确地表明其负责任的承诺并解释信息安全对所有员工的重要性。

如果创建的ISMS是在整个组织的一部分，那么这个成功因素只适用于其所授权负责的领域。

- 结合信息安全

在组织的所有业务活动中，包括有信息处理和使用信息技术的第三方约定，都应考虑信息安全和适当结合信息安全。这意味着，例如，当获得IT以及当设计业务流程和培训员工时，应考虑信息安全。

- 管理和维护信息安全

管理者应确保信息安全(IS)任务的责任和权力合理地分配给具有适当知识的人员，并被所有IS相关工作的人员接受。这包括：

- 开发、实施和维护IS策略；
- 风险识别、风险评估和风险管理；
- 提供充分资源以支持和管理IS工作。

- 建立可实现的目标

在ISMS范围内，活动的目标应做出很好的规定，并应有文件说明与组织的主要目标的关系。重要的是应明确地描述这些安全目标如何支持完成主要目的和业务目标。这些关系应是可信任的，而由此进行的活动应是现实的和可实现的。

- 信息安全成本利益分析

了解业务流程、资产和任务对信息处理的依赖性是有必要的，这样可以选择适当的信息安全控制措施以及管理和维护ISMS的实施。

- 模范角色的作用

在涉及到信息安全时，管理者应起模范带头作用。这要求管理者除其它事情外也要执行所有指定的安全规章和参与培训事宜。

c. 财务方面的考虑

财务方面的考虑也被认为是实施ISMS关键的成功因素。特别是组织应有适当的机制以监控：

- 对ISMS实施和管理的投资回报；
- 不符合业务的安全策略或维护ISMS失败的成本。

d. 行业/部门特殊考虑

实施ISMS关键的成功因素也应包括考虑特殊的行业(或部门)标准和与组织的业务相关的指导方针。重要的是要认可规章的环境和需要如何实施ISMS以支持业务运行。对于与部门特殊文件和ISMS标准族有关的另外信息可参考ISO/IEC 27000。

e. 风险方面的考虑

风险方面的考虑是一个关键的成功因素。ISMS范围内的风险信息是为把这些风险降低到可接受级别的适当控制措施应获得管理者同意和批准。在这个阶段，应注意评价信息安全风险如何与现有风险管理流程相比进行处理和可以达到的可能收获。

f. 组织内合作和与其它组织合作

组织内合作和跨组织合作对ISMS实施是一个重要的关键成功因素。特别以下事宜被评审和解决：

- 配合现有的安全方针、指南和指导书；
- 跨组织的联系和评估ISMS成功的方法；
- 满足相关方关注事宜所需要的安全要求。

g. 认可变更或更新的需要

另一个重要的成功因素是认可ISMS需要变更或更新时的能力。

h. 利益相关方牵涉事宜

如所定义的不同利益的相关方及其对成功的ISMS的观点应是要考虑的事宜。

这些观点可以是：

- 有关信息安全业绩的报告(包括实施项目的结果)；
- 信息安全的成本；
- 得到的信息安全利益。

进一步的利益相关方牵涉事宜应加以解决，因为他们的牵涉事宜可能在以下方面支持了实际的实施：

- 作为ISMS实施筹划指导委员会的一部分；
- 通过在其它运作活动提出信息安全的重要性，展示他们的兴趣。

输出

这个活动的输出和这个阶段的结果对其它文件是关键的。这是要接收形成文件的管理者对实施ISMS的正式批准和承诺。本章所述的键的成功因素为成功实施ISMS提供了有关如何获得和保持管理者的支持以及需要考虑的事情方面的进一步细节。

其它信息

6 定义 ISMS 范围和 ISMS 方针

6.1 定义 ISMS 范围和 ISMS 方针的概要

目标:

- 定义 ISMS 的范围边界;
- 获得对 ISMS 方针的同意。

参见 ISO/IEC 27001: 4.2.1 a), b)

假定管理者已经批准和支持实施 ISMS。图 4 展示 ISMS 范围和 ISMS 方针的定义概要。

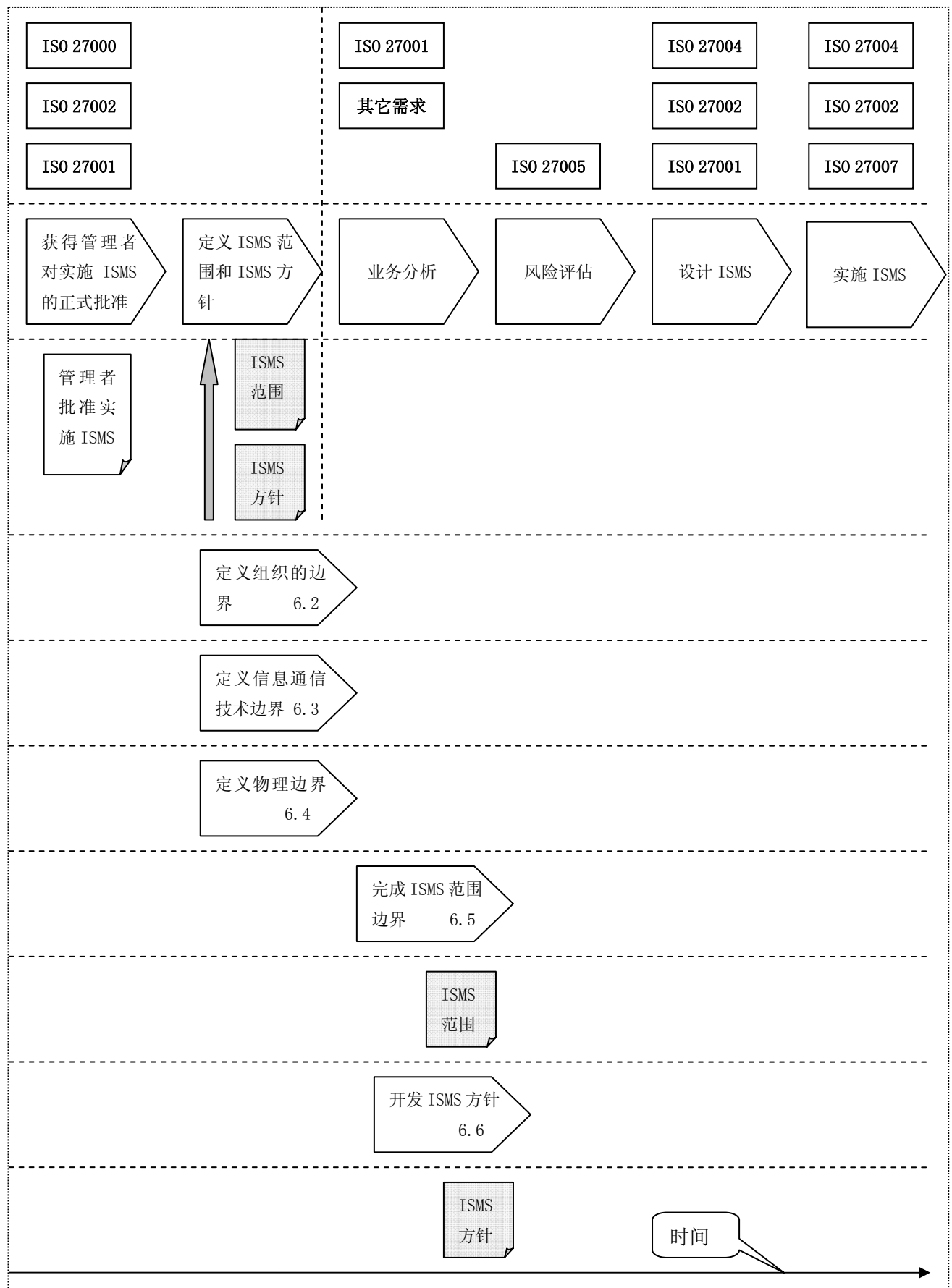


图 4 ISMS 范围和 ISMS 方针的定义概要

为实现本阶段的目标,重要的是要获得可帮助设计该组织的信息安全管理体系及其边界和相关流程的支持性信息。

1. 为建立 ISMS 收集信息

0 分析该组织的业务以定义 ISMS 的范围和边界及其方针。从业务的观点,建立 ISMS 的支持性信息应在本阶段全程进行收集。信息应包括:

- ◆ 关键业务流程;
- ◆ 物理环境;
- ◆ 组织结构。

2. 定义 ISMS 的范围和边界

0 根据管理者的决定和上述分析所收集的信息定义 ISMS 的范围和边界。

为了在组织内建立一个有效的管理体系, ISMS 的适当范围应通过考虑指标性业务的关键信息资产而做出决定。为了确保关键业务领域被包含在这个范围之内,在识别信息资产和评估可行的安全机制方面建立一个共同术语表和系统框架也是重要的。共同框架能容易沟通并使一致的理解能够贯穿所有实施阶段。也可能定义整个企业作为 ISMS 的范围或业务部门的一部分作为 ISMS 的范围。正如为客户提供“服务”的情况,跨职能的管理体系(整个部门或部门的一部分)可以成为 ISMS 的范围,如同组织结构的一些部门的有关管理制度。

在定义 ISMS 的范围时,重要的是要有一个完全的管理体系且其边界要足够清楚以进行逻辑解释。ISMS 的范围和边界应合理地进行定义。

实施 ISMS 的工作量取决于范围大小。这也可影响维护信息安全的所有活动,包括控制措施、管理运行和任务,例如识别信息资产和风险评估。被排除出 ISMS 范围的任何事情应加以解释。

6.2 定义组织的边界

活动

定义组织的业务的边界、组织和 ISMS 处理的资产事宜。

输入

- 5.3 活动的输出 - 管理者关于高层 ISMS 范围(例如整个组织、特殊区域、过程领域)的正式决定。

实施指南

定义组织的边界的一个方法是:识别在组织内不相重叠的责任范围,这些包含关键业务资产或受关键业务流程影响的责任范围被选择作为在 ISMS 控制下的该组织的区域。当采用这个方法时,需要考虑以下事宜:

- 参与 ISMS 管理论坛的各方都将受到影响;
- 负责 ISMS 的管理者应基本上是所有受责任影响范围的负责人(例如组织结构的上层);
- 范围和边界需要进行定义,以确保所有相关的资产在风险评估中被考虑到并处理可能

通过这些边界产生的风险(见 ISO/IEC 27005)；

- 对于组织，范围应进行定义，以能够在该范围内现实 ISMS PDCA 循环。例如，一部分未管理的组织不适合这个范围。

输出

- ISMS 组织边界的描述，包括部分组织被排除出 ISMS 范围的任何正当理由；
- 组织的功能和结构；
- 通过边界的信息资产和信息交换；
- 范围之内和范围之外的信息资产的业务流程和责任。

其它信息

6.3 定义信息通信技术边界

活动

定义ISMS所包含的信息与通信技术和其它技术的边界。

输入

- 5.3 活动的输出 - 管理者关于高层 ISMS 范围（例如：在组织的控制之下的所有 ICT，支持特殊业务或过程的部分 ICT）的正式决定。

实施指南

ICT边界的定义可以通过信息系统(不是IT系统)方法进行识别。处理或传输关键业务信息资产的所有信息系统或关键的信息系统都应归入ISMS范围。

以下事宜是应该考虑的：

- 信息系统可以跨越应进行结合与沟通的组织的边界；
- 当信息系统跨越该组织的边界或国家边界时，应考虑以下事宜：
 - 0 社会文化环境；
 - 0 适用于该组织的法律、法规和合同要求；
 - 0 关键责任的说明；
 - 0 技术约束(例如：可用的带宽和服务的可用性等)。

输出

- ISMS 的 ICT 边界的描述，包括在该组织管理下的 ICT 被排除出 ISMS 范围的任何正当性理由。
- 范围之内和范围之外的信息系统和电信网络的描述。

其它信息

6.4 定义物理边界

活动

定义ISMS所包含的场所方面的物理边界。

输入

- 5.3 活动的输出 - 管理者关于高层 ISMS 范围（例如在组织的控制之下的所有场所，支持特殊业务或过程的部分场所）的正式决定。

实施指南

物理边界的定义包括识别应属于ISMS范围的组织内的建筑物、场所或设施。处理跨越物理边界的信息系统是很复杂的，这需要：

- 0 移动访问；
- 0 远程设施；
- 0 签署第三方服务；
- 0 无线网路。

这些问题应通过定义适当的界面和服务层次加以解决。

输出

- ISMS 物理边界的描述包括在该组织管理下的物理边界被排除出 ISMS 范围的任何正当性理由。
- 范围之内的和范围之外的组织及其地理特征的描述。

其它信息

6.5 完成 ISMS 范围边界

活动

编写ISMS范围和边界文件。

输入

- 5.3 活动的输出 - 管理者关于高层 ISMS 范围的正式决定。
- 6.2 活动的输出 - 组织边界的定义；
- 6.3 活动的输出 - ICT 边界的定义；
- 6.4 活动的输出 - 物理边界的定义。

实施指南

在定义ISMS范围的时候，这些范围和边界可以以许多方法合并在一起。例如：物理场所(如建筑物、数据中心或办公室)和这个物理场所的关键流程应并入该范围内。信息系统的移动访问就是一个例子。

输出

- 描述 ISMS 范围和边界的文件，包括以下信息：
 - 0 组织的业务特性(业务、服务、资产和每一个资产的责任范围和边界等的说明书)；
 - 0 关键业务流程列表；
 - 0 组织的功能和结构文件；

- 0 场所和楼层位置图；
- 0 设备和网络的配置；
- 0 资产列表；
- 0 任何排除出ISMS范围的正当性理由的详细说明。

其它信息

6.6 开发 ISMS 方针

活动

开发初始的ISMS方针。

为了为组织提供信息安全管理的基本观念，ISMS方针是必须的。方针文件也提供一个意图声明，指出组织承担信息安全要求的责任。

输入

- 5.4 活动的输出 - 业务要求和信息安全需求；
- 5.4 活动的输出 - 实施 ISMS 的目标；
- 5.4 活动的输出 - ISMS 实施的项目计划(包括各个重要事件，如执行风险评估、实施、内部审核和管理评审)。

实施指南

定义ISMS方针的过程如下：

- a. 建立基于组织的业务要求和信息安全需求的ISMS目标。
- b. 建立为实现ISMS目标的一般焦点和指南；
- c. 考虑业务要求、法律法规要求和合同安全义务；
- d. 准备组织和风险管理的环境；
- e. 建立评价风险和定义风险评估结构的准则；
- f. 阐明高层管理者的责任，以确保信息安全管理需要；
- g. 获得管理者支持。

从初始阶段到管理者批准所开发的ISMS方针应能反映ISMS流程(如风险评估)的结果。

输出

- 管理核准的初始的 ISMS 方针包含以下内容：
 - 0 ISMS目标和组织对ISMS的指示；
 - 0 有关信息安全的总方向和原则；
 - 0 风险评估考虑的组织的环境和项目；
 - 0 风险管理的风险结构评估准则；
 - 0 业务要求；

- 0 法律或法规要求；
- 0 合同安全义务。

其它信息

7 进行业务分析

7.1 业务分析概要

目标：

- 收集 ISMS 支持的相关需求；
- 收集当前 ISMS 范围内的信息安全状况
- 创建信息资产清单。

参考 ISO/IEC 27001

假定管理层批准实施 ISMS，并定义了 ISMS 的范围和 ISMS 的方针。

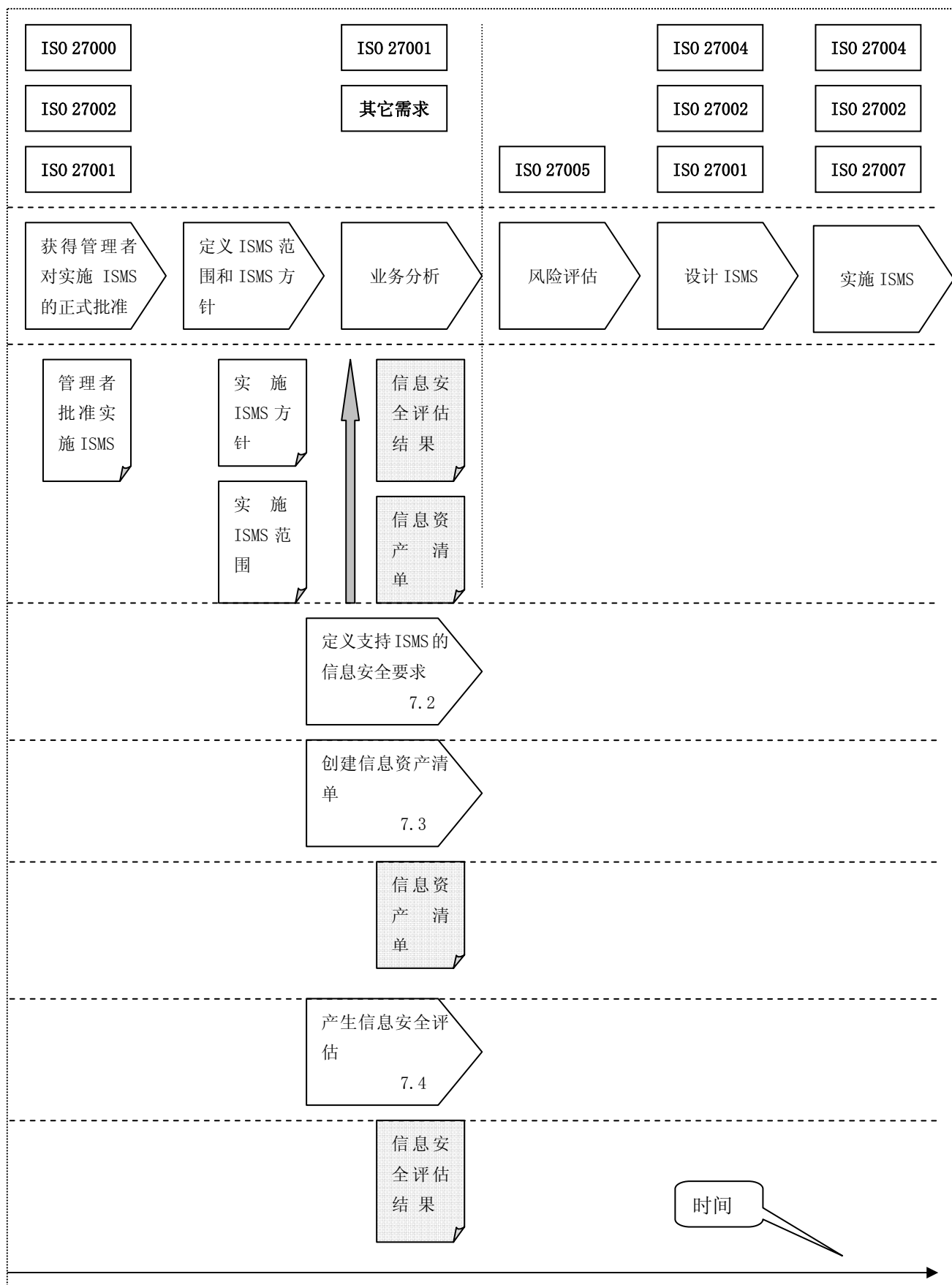


图 5：业务分析阶段的概要

通过业务分析阶段所收集的信息应包括：

- a. 为管理者提供一个起(开始)点(即正确的基本数据)；
- b. 识别并记录实施的条件；
- c. 提供一个清晰的并确认理解的组织设施。
- d. 考虑组织的特殊环境及形势；
- e. 识别信息保护最适宜的级别；
- f. 在所定义的实施范围内，确定支持企业所需要的全部或部分信息。

业务分析可以在一个选定的部门范围内进行，但至少应在所提议的信息安全管理体系所定义的范围内进行。

7.2 定义支持 ISMS 的信息安全要求

活动

建立ISMS信息安全要求。

输入

- 6.5 活动的输出 - ISMS 的范围和边界；
- 6.6 活动的输出 - ISMS 方针；
- 5.4 活动的输出 - 业务要求和信息安全需要；
- 5.4 活动的输出 - 实施 ISMS 的目标；
- ISO/IEC27001；
- ISO/IEC27002。

实施指南

从建立ISMS的业务观点，分析组织的业务情况和收集支持信息。

ISMS的支持性信息应在业务分析阶段的第一步进行收集。对于每一个业务流程和特殊任务，需要根据信息重要性(比如：需要保护的级别)而做出决定。许多内部因素都可能影响信息安全，这些内部因素应加以识别。在此阶段的初，详细描述信息技术不是重要的。对于业务流程和相关的IT应用及系统，应有一个所分析的信息的基本概要。

业务流程的分析阐述了信息安全事故对业务活动的影响。在许多情况下，描述一个很基本的业务流程就足够了。

为了阐明ISMS信息安全要求，应回答以下问题：

- a. 识别组织的主要流程和功能；
- b. 识别重要的信息资产及其在保密性、完整性和可用性方面的保护；
- c. 确认组织的信息安全目标，并识别所确认的目标对未来信息处理要求的影响；
- d. 了解和发现当前信息处理、应用系统、通信网络、活动场所和IT资源等的形势；
- e. 识别所有基本要求(例如法律法规要求、合同义务、业务要求、行业标准、客户和供应商协议，保险条件等)。

输出

本流程产生的一些中间材料应包括：

- 主要流程、功能、场所、信息系统和通信网络的鉴别；
- 组织的信息资产；
- 关键流程/资产分类；
- 组织对保密性、完整性和可用性的要求；
- 组织对法律法规、合同、业务的要求；
- 任何已知的组织脆弱点。

其它信息

7.3 创建信息资产清单

活动

建立信息安全管理体系统所支持的资产清单。

输入

- 6.5 活动的输出 - ISMS 的范围和边界；
- 6.6 活动的输出 - ISMS 方针；
- 7.2 活动的输出 - 信息安全要求。

实施指南

为了创建资产清单，有几种可供选择的方法。一种方法是遵循信息分类方案；如果使用这种方法，处理、操作或传输具有某个类别的信息的资产，可以被插入到资产表中。

另一个供选择的方法是把相关的业务流程分解成组件和业务流程关键资产，并由相关组件产生资产表。如果业务流程具有一定的复杂性，那么分解业务流程可能是一个很艰难的任务。

应包括以下方面的信息：

- a. 流程的唯一名称；
- b. 流程描述；
- c. 流程的关键性(关键的、重要的和支持性的)；
- d. 流程责任人(业务单位)；
- e. 提供各个流程的输入和本流程的输出；
- f. IT 应用支持的流程；
- g. 流程内信息及其：
 - 分类(保密性、完整性、可用性和/或其它重要特性，例如信息可以保存多长时间等)；
 - 流程内处理活动(创建、存储、处理、传输和删除)与支持系统处理的信息。

输出

- 组织的主要流程的描述；
- 组织的主要流程的信息资产清单；
- 主要流程/资产分类。

其它信息

7.4 产生信息安全评估

活动

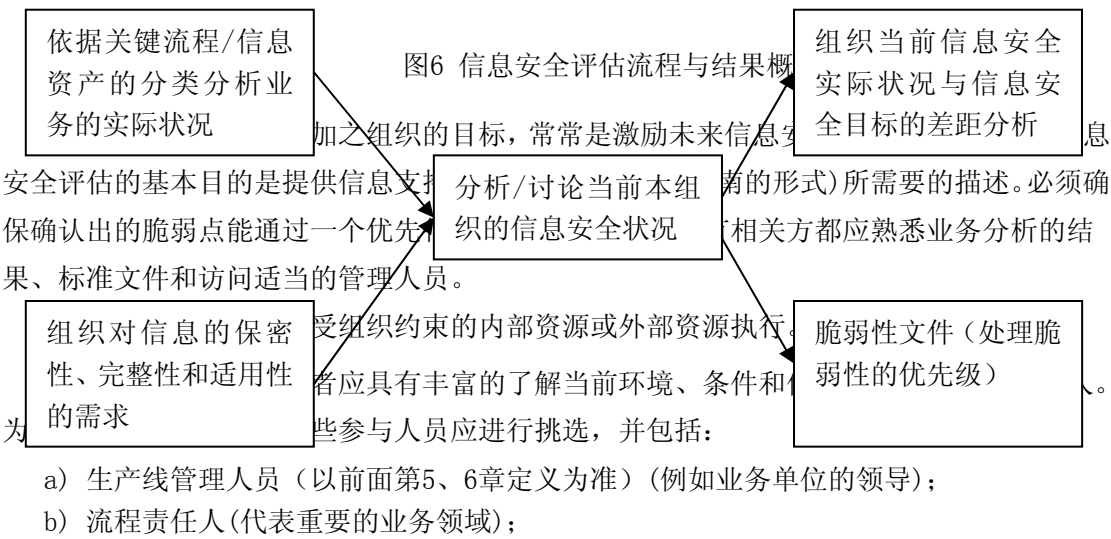
确立组织的信息安全状况，对比想达到的业务目标，从而导致信息安全评估。

输入

- 6.5 活动的输出 - ISMS 的范围和边界；
- 6.6 活动的输出 - ISMS 方针；
- 7.2 活动的输出 - 信息安全要求；
- 7.3 活动的输出 - 信息资产清单；
- ISO/IEC27001；
- ISO/IEC27002。

实施指南

为了保护组织业务的连续性，本阶段的下一个步骤称为信息安全评估，识别现有的信息安全等级(即：组织当前的信息保护程序)。



c) 其它具有丰富的了解当前环境、条件和信息安全相关知识的个人。

为了成功地执行信息安全评估，重要的是：

a) 识别和列出组织的相关标准和标准化文件(例如ISO/IEC 27002)；

b) 识别来自方针的已知控制要求、法律法规要求、合同义务、过去的审核发现或过去执行的风险评估发现；

c) 使用上述这些作为参考文件，可以粗略评估组织当前的有关信息安全等级。

应该考虑业务分析所做出的优先顺序组成安全预防和检查的基础。

执行信息安全评估的方法如下：

a) 选择重要的流程和流程涉及需求类型(可用性、完整性和保密性)的步骤。

b) 创建一个综合流程图涵盖组织的主要流程，包括基础设施(逻辑的和技术的)，如果这在业务分析中尚未提出或执行。

c) 组织中合适的键人物以小组讨论的方式分析。

d) 就要求的类型(可用性、完整性和保密性)，讨论和分析组织当前的状况。哪些流程是关键的，他们当前的工作对可用性、完整性和保密性起怎样作用？(其结果用于后面的风险评估)

e) 通过将现有的控制措施与前面确认的控制要求进行比较，确定控制脆弱点。

f) 完成以上流程，并编写成文件。

输出

- 组织目前的信息安全状况和风险评价文件；
- 经过组织评估与评价的脆弱性文件。

其它信息

8 进行风险评估

8.1 风险评估概要

假定管理层已经批准实施 ISMS，并定义了 ISMS 的范围和方针，经过业务分析已获得信息资产及信息安全评估结果。图 7 是风险评估阶段的概要。

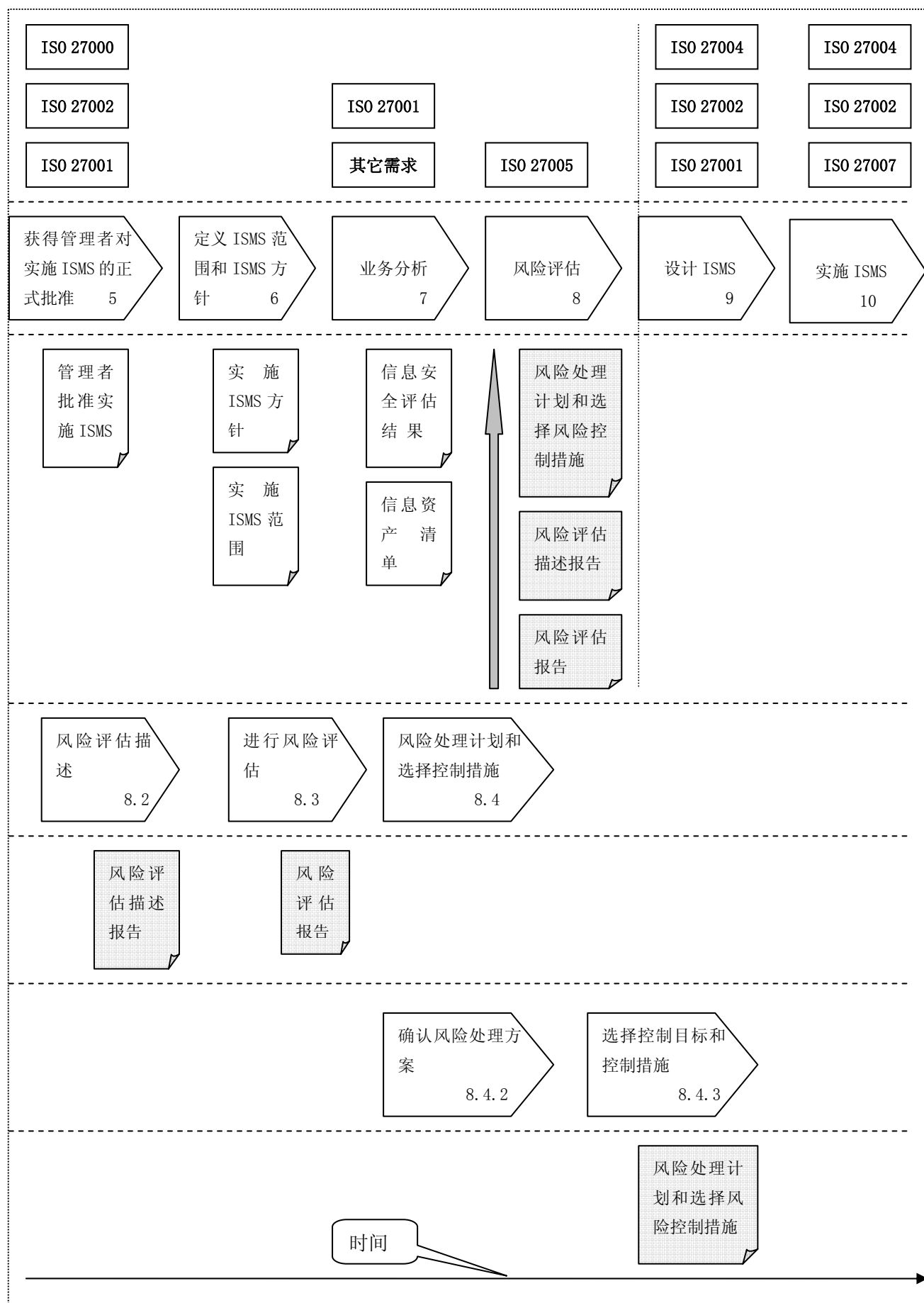


图 7 风险评估阶段的概要

8.2 风险评估描述

活动

通过识别适用于ISMS的风险评估方法和已确定的信息安全要求，确认组织的风险评估方法。

输入

- 6.5 活动的输出 - ISMS的范围和边界；
- 7.2 活动的输出 - 信息安全要求；
- ISO/IEC27001；
- ISO/IEC27005。

实施指南

风险评估方法定义步骤。组织的ISMS范围之内所有操作的业务风险都要进行确认。风险评估方法应通过以下考虑事项进行确认。

- 组织的ISMS范围和边界；
- 法律法规要求、合同义务、组织的业务要求。

风险评估方法是每一个信息安全管理体的主要部分，为了确定风险，关键威胁应根据潜在影响、系统发生事件的可能性及其频率进行确认。

风险评估方法有很大变化，取决于应用、组织的边界条件、组织的类型和所期望的信息安全级别。信息安全管理应选择适于组织的类型和规模的方法。有关更深一层的ISMS风险评估指南可参考ISO/IEC 27005。

输出

- 风险评估范围；
- 已批准的风险评估方法，包括：
 - 风险评估方法的描述；
 - 风险评估(风险识别和风险评价)；
 - 风险评价；
 - 风险处理决定；
 - 风险接受准则；
 - 风险记录和报告。

其它信息

8.3 进行风险评估

活动

识别、分析和评价信息安全风险。

输入

- 6.5 活动的输出 - ISMS的范围和边界;
- 6.6 活动的输出 - ISMS方针;
- 7.2 活动的输出 - 信息安全要求;
- 7.3 活动的输出 - 信息资产;
- 7.4 活动的输出 - 信息安全评估结果;
- 8.2 活动的输出 - 风险评估方法;
- ISO/IEC27001;
- ISO/IEC27005。

实施指南

本阶段的下一个步骤被称为风险评估。基于业务与信息安全评估结果,了解实施ISMS的风险评估对成功实施ISMS十分关键。评估风险的详细方法在ISO/IEC 27005中描述。

在执行风险评估时,要考虑的关键问题包括:

- a. 什么是业务方面的关键脆弱点?
- b. 什么是信息安全评估结果?
- c. 什么是潜在的威胁?
- d. 这些威胁发生的可能性是什么?
- e. 这些威胁对资产有什么影响?
- f. 什么是管理者接受的最小级别?

全面分析可以以小组讨论的方式进行;参与讨论的代表来自组织的不同部门,讨论的代表可以不具有非常丰富和专业的安全知识但应具有识别影响业务安全的能力;应指定一个富有经验的内部或外部讨论代表主持和推动小组讨论。

风险评估的参与者应具有丰富的有关组织的目标知识和信息安全知识(例:如能识别到当前对组织的目标产生的威胁)的人员。为了能广泛代表组织,这些参与人员应进行挑选,并包括:

- a. 高级管理者(例如 COO, CEO, CSO 和 CFO);
- b. 生产线管理人员(例如业务单位领导);
- c. 业务过程责任人(代表重要的业务部门);
- d. 其它人员-具有丰富的有关组织的目标知识和安全知识(例如能识别当前组织的目标面临的威胁)的人员。

深度风险评估由具有解决其部门问题的能力的代表执行;然而,具有业务和技术两方面能力的表现也很重要。组织的基本目标和任务是所有业务流程、专业程序和活动(包括信息安全)的基础。信息通信技术应对组织的目标和业务流程提供有积极的支持;因此,

为了建立一个适用的信息安全管理体系，每个组织都应该考虑该组织最重要的业务流程和专业任务以及其对信息的依赖性。通过一个综合风险评估为信息安全管理方针制定可接受的风险级别，但其拥有可供指导的资源是很重要的。整个组织面临的威胁和风险应在风险评估阶段进行识别。

深入的风险评估可以帮助识别可以接受的风险级别，包括了解一整套规章制度，这样形成了工作目标的指导方针。如果发现综合风险评估不覆盖整个组织或一个或者多个业务流程尚未被满意的突显出来，或者那些明显的风险没有记录，则管理者可能需要一次深度风险评估。在开发ISMS时，应考虑相关风险和评审下列问题：

- a. 组织的业务目标；
- b. 组织的安全目标；
- c. 法律要求和规章制度；
- d. 客户要求和现有合同；
- e. 内部的主要条件(例如，组织范围内的风险管理或IT基础设施)；
- f. (IT-支持的) 业务流程和任务；
- g. 由于信息安全风险而造成对商业活动的全球性威胁（例如，损害形象、违反法律、违反合同义务、盗窃研究成果）；

当残余风险(或计划)低于可接受风险级别时，管理者应检查和批准业务保持适当的风险。

依据风险评估的结果，评审ISMS的范围、边界定义和ISMS方针，并确定其适用性。

输出

- 综合风险评估文档；
- 关键部门的深度风险评估要求；
- 深度风险评估文档；
- 管理者批准接受残余风险文档；
- 管理者批准实施和运行ISMS的文档；
- 已批准的ISMS方针；
- 已批准的ISMS范围和边界定义。

其它信息

有关ISMS风险评估的更多指导，请参考ISO/IEC 27005。

8.4 风险处理计划和选择控制措施

8.4.1 风险处理和控制措施选择概要

活动

为了降低风险，要确认并评估风险处理方案，然后选择适当控制目标和控制措施。

输入

- 7.4 活动的输出 - 信息安全评估结果；
- 8.3 活动的输出 - 风险评估结果；
- ISO/IEC27001；
- ISO/IEC27005。

实施指南

在已确认的各种风险中，有些风险需要进行处理；按照ISO/IEC 27005，有4种处理风险的方法；ISMS的焦点在于力图降低风险发生的可能性；在某些少见的情况下，致力降低风险产生的影响也很重要；总之，焦点应放在减少事件发生的可能性；这些事宜应写成风险处理计划，例如从ISO/IEC 27002选择适当的控制措施以控制某个风险。控制措施的选择应形成文档并编写于适用性声明(SOA)中。

输出

- a. 各种风险及其确认的风险处理方案；
- b. 为降低风险选择的控制目标和控制措施。

其它信息

8.4.2 确认风险处理方案

风险处理计划就是要确认风险处理方案和制定风险处理列表。

风险处理方案是：

- a. 降低风险，通过选择适当的控制目标和控制措施；
- b. 保持风险，通过接受风险，即风险明显地满足组织的安全方针和风险接受准则；
- c. 避免风险，通过避免某些特殊风险；
- d. 转移风险，通过把风险转移到其它方。

风险处理列表阐明各种风险与风险处理方案之间详细的关系。在降低风险的方案中风险处理列表应指定哪些控制目标与控制措施降低风险。（想得到进一步的指导，请参考ISO/IEC 27005）

根据第8章的风险处理列表至第9章（设计选择风险处理控制目标和控制措施）的风险处理计划，以下过程可以作为降低风险的方法。

- a. 风险处理列表描述实现风险处理控制目标与控制措施的适当策略。
- b. 实施正确的控制措施降低数个相关风险，这意味着这些控制措施是为了降低风险而选择的，这被称为选择控制目标和控制措施。
- c. 第8章风险处理计划完成确认风险处理方案和选择风险处理控制目标与控制措

施，第9章帮助设计选择控制目标与控制措施，第10章支持实施它们。

- d. 其它的风险处理方案，如保持风险、避免风险和转移风险描述于第9章和第10章。

8.4.3 选择控制目标和控制措施

ISO/IEC 27001中的“附录A控制目标和控制措施”，可用于选择风险处理的控制目标和控制措施，如果“附录A”中没有适当的控制目标和控制措施，可以创建另外的控制目标和控制措施，重要的是根据风险评估和风险处理过程的结果证明这个选择是正确的。

ISO/IEC 27001的附录A可用作支持性信息。ISO/IEC 27001附录A所规定的范围并不是很完备的，这就是为什么可以进一步从其它领域选择控制目标和控制措施的原因，为了支持业务及ISMS的特殊需求需要识别特殊的控制措施，已进行的业务分析、状况和风险评估可作为支持性信息加以利用。

适应性声明的准备应作为信息安全管理工作的—部分。

参与者应包括具有丰富的有关组织的目标的知识和安全知识(例如能识别到当前对组织目标产生的威胁)的人员；为了能广泛代表组织，这些参与人员应进行挑选。分析工作由具有解决其部门的问题能力的代表执行，然而，具有业务和技术两方面能力的表现也很重要。

例如，应包括以下角色：

- a. 高级管理者(例如 COO, CEO, CSO 和 CFO)；
- b. 生产线管理人员(例如业务单位领导)；
- c. 流程责任人(代表重要的运作领域)；
- d. 其它人员-具有丰富的有关组织的目标的知识和安全知识(例如能识别到当前对组织的目标产生威胁)的人员。

9 设计 ISMS

9.1 设计 ISMS 概要

目标：

- 基于风险处理方案，设计组织的安全风险处理；
- 结合 ICT 安全、物理安全和组织安全来设计控制目标和控制措施以降低风险。
- 设计 ISMS 特定的需求，包括对建立 ISMS 的监控和测量；
- 制定 ISMS 实施计划。

参考 ISO/IEC 27001：4.2.2 a)–e)，h)

假定管理层已经批准实施 ISMS，并定义了 ISMS 的范围和方针，信息资产及信息安全评估结果为已知。此外，描述风险和风险处理方案的风险处理列表，识别选择的控制目标和可用的控制措施。图 8 是设计 ISMS 阶段的概要。

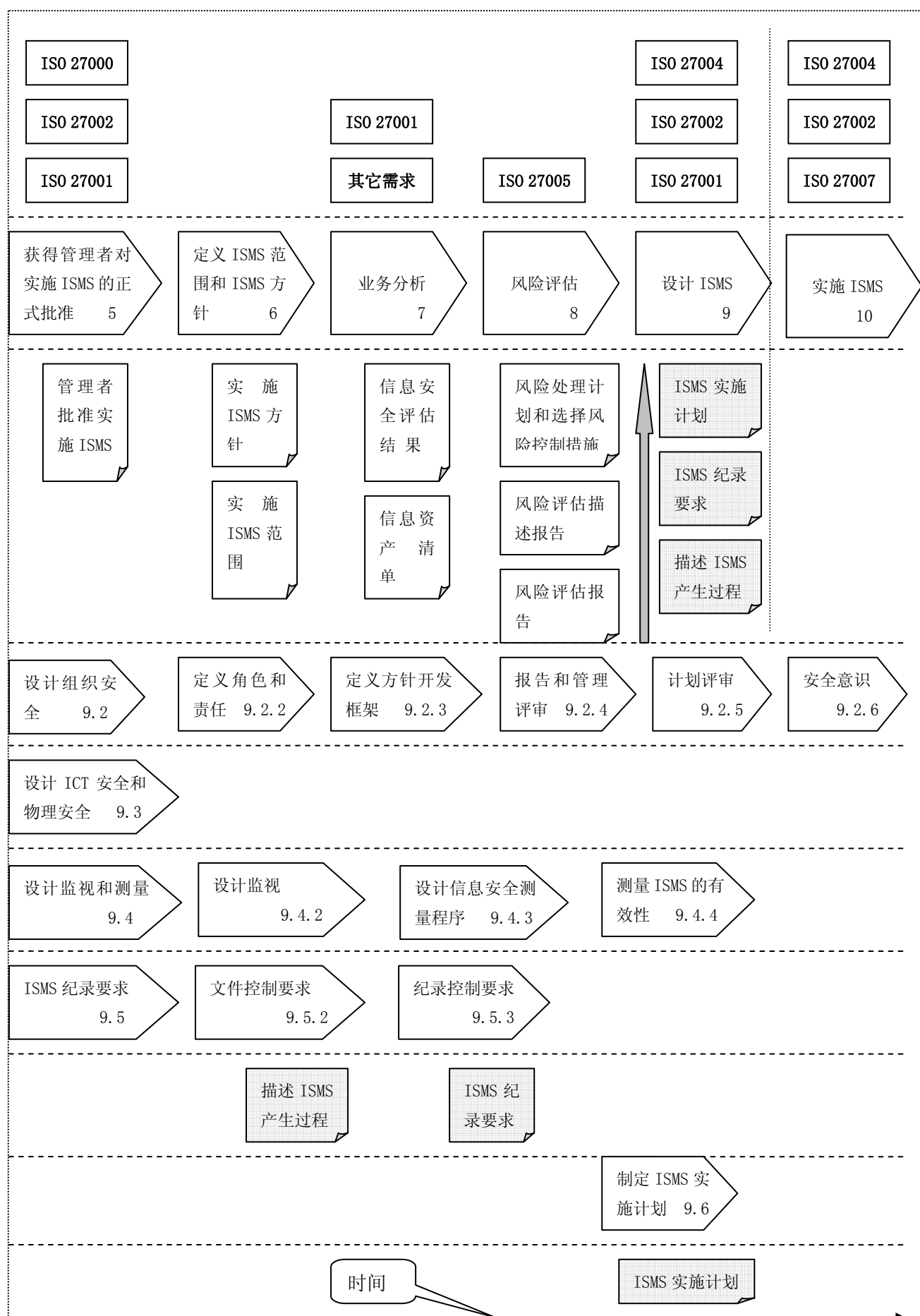


图 8 设计 ISMS 阶段的概要

为了制定实施计划以及下一阶段的正式要求，需要执行许多活动。为了获得设计结构，最好是将其分为4个主要方面：

- a. 组织安全 - 包含信息安全管理方面所涉及的风险处理(不仅包括降低风险,而且包括保持风险、避免风险和转移风险)上业务运行的责任。还包括要建立方针、目标、过程和程序等一系列活动以处理和改进与信息安全相关的业务需求和风险。
- b. ICT安全 - 包括与降低ICT运行风险责任相关的信息安全方面。这要达到为降低风险所实施业务和技术控制措施所建立的要求。
- c. 物理安全 - 包括与降低处理物理环境(如:建筑物和建筑结构)风险相关的信息安全方面。这要达到为降低风险所实施业务和技术控制措施建立的要求。
- d. ISMS特殊活动 - 包括除了上述3个领域之外的ISO/IEC 27001规定的ISMS不同特殊要求方面。焦点应放在以实现ISMS正常运行所实施的执行的某些活动。尤其是以下活动:
 - 监视;
 - 测量;
 - 内部ISMS审核;
 - 培训与意识教育;
 - 管理评审;
 - ISMS改进包括纠正措施和预防措施;
 - 编写文件和形成记录。

设计各种不同控制措施的实施,意味着要与上述4个方面的责任人互动。ISMS第四个方面要求与管理者对话以评审(a)处理特殊的要求(b)信息安全体系设计的责任人或项目经理。

9.2 设计组织安全

9.2.1 组织安全概要

活动

为了组织内信息安全的风险处理(例如:降低风险,也包括保持风险、避免风险和转移风险),建立组织的职能和责任。

输入

- 6.5 活动的输出 - ISMS的范围和边界;
- 6.6 活动的输出 - ISMS方针;
- 7.2 活动的输出 - 信息安全要求;
- 7.3 活动的输出 - 信息资产;
- 7.4 活动的输出 - 信息安全评估;
- 8.3 活动的输出 - 风险评估结果;

- 8.4 活动的输出 - 已确认的风险处理方案；
- 8.4 活动的输出 - 已选择的控制目标和控制措施；
- ISO/IEC27001；
- ISO/IEC27002。

实施指南

设计组织的安全包括以下活动：

- 设计角色和责任；
- 开发信息安全方针；
- 设计报告和管理评审；
- 设计ISMS特殊要求，例如：内部审核和意识教育。

输出

- 组织结构及其角色和责任；
- 信息安全方针文件；
- 报告和管理评审过程；
- ISMS特殊设计，例如：内部审核和意识教育。

其它信息

9.2.2 角色和责任

实施ISMS的组织结构类似于ISMS运行所需的结构，另一方面，ISMS运行的组织结构应增加其他一些方面。例如，如何监视和记录的方法应作为ISMS运行的一部分。

根据上述观点，ISMS运行的结构应基于实施ISMS的结构进行设计，应考虑以下问题：

- 实施ISMS的每一个角色是否是ISMS运行所需要的？
- 所定义的角色是否不同于ISMS实施的角色？
- ISMS实施应增加什么角色？

例如，一个负责ISMS运行的人还应具有以下责任：

- 每一个部门的信息安全运行；
- 每一个部门的ISMS测量。

顺着以下要点进行考虑，通过修订实施ISMS的结构和角色，有助于决定ISMS运行的结构和角色。

1. 信息安全委员会角色

信息安全委员会应该负责处理一个组织所拥有的信息资产，也应该对信息安全的指挥任务非常了解，并能够让事情得以解决。。

信息安全委员会应是组织内ISMS的领导角色。下面列举了信息安全委员会的职责。

- 考虑风险管理环境要做的准备；
- 制定ISMS文件计划，负责确定这些文件的内容，并获得管理者的授权；

- 计划采购新设备和/或使用组织现有的设备；
- 处理建立ISMS时可能发生的问题；
- 根据实施和测量ISMS的结果，考虑改进的方法。

2. 信息安全规划组角色

在规划项目时，ISMS规划组的其他对ISMS范围内重要信息资产有广泛认识的成员和在处理信息方面有丰富经验的成员应协助处理相关工作。例如：当决定如何处理信息资产时，在ISMS范围内的各个部门之间可能有不同的方案，因此就可能需要调整计划的正面的与负面的影响。规划组需要协调各部门的工作。这一项工作就要求他们具备一定的交际能力，当然也是建立在丰富的经验、调解能力以及对安全有很高的认识的基础之上。

3. 专家和外部顾问

在建立ISMS之前，组织应根据其成本选择成员(如可能，成员具有一个唯一角色)。然而这些成员需要对“信息安全”领域有丰富地知识和经验，如“IT”、“行政决定”和“业务的理解”。一个组织负责某些运行的人员对此最了解。应该按照专家对ISMS事件的想法访问他们，因为这涉及到其使用在特定的领域。专家与必要的丰富知识之间的权衡也是很重要的。即使有时外部顾问并不精通具体的业务细节和组织的运行细节方面的知识，但他们可以根据对组织的宏观认识和其它类似场合的经验来做决定。上述例子所使用的术语，如“信息安全委员会”和“信息安全规划组”并不重要，重要的是要理解每一个结构的职能。最理想的应有内部结构负责协调组织内信息安全沟通和各技术部门紧密的合作。

4. 联系人

每一个业务过程和特定的应用都应指定一个联系人；这个联系人担任所谓的“过程责任人”的角色，负责处理这个业务过程中与数据处理有关的所有信息安全问题。举个例子来说，联系人或过程负责人是主要负责委派所分配的任务并处理该任务处理过程中的信息。

对于转移风险、避免风险和保持风险的情况，应该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，那么应该通过利用合同、保险协议和组织结构（如合作的企业和合资企业）来采取适当的措施。

图10展示一个建立ISMS的组织结构的例子。基于这个例子，下面列出组织的主要角色和责任。

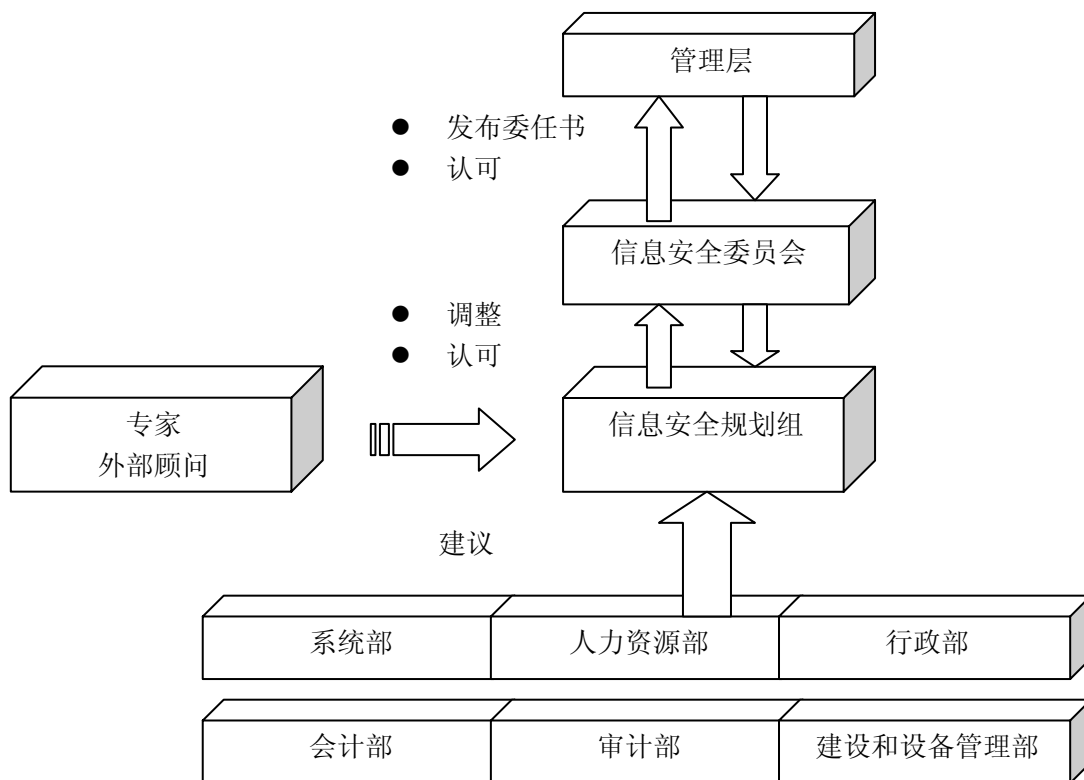


图 10 建立 ISMS 的组织结构例子

与组织互动

所有相关方都应评审并熟悉当前保护组织资产、ISMS 范围和 ISMS 方针的要求。业务分析的参与者应包括那些对组织及其运行环境非常了解的人员。为了能广泛代表组织，这些参与人员应进行挑选，包括：

- a. 高级管理者(例如 COO和CFO)；
- b. 信息安全委员会的成员；
- c. 信息安全规划组的成员；
- d. 生产线管理员(例如业务单位领导)；
- e. 业务过程责任人(代表重要的业务领域)；
- f. 专家和外部顾问。

9.2.3 方针开发框架

9.2.3.1 设计信息安全方针

信息安全方针详细证明了管理者和行政领导为了达到整个组织的信息安全目标所持的战略立场。

这个方针应体现组织的信息安全要求，并起到指导和推动的作用。在方针中，管理者概述其战略目的、角色和责任或组织内的职务分配。

信息安全方针概括地描述如何在组织、目的、资源和结构上建立信息安全。它包含组织期望达到的信息安全目标和所要遵循的信息安全策略。

信息安全方针应描述可接受的风险级别，这个风险级别应符合公共机构的安全等级或不超过组织的信息安全目标。因此信息安全方针是安全级别的要求和声明，这个安全级别应在组织内所有层面上都应达到。图 10 展示信息安全方针的内容。

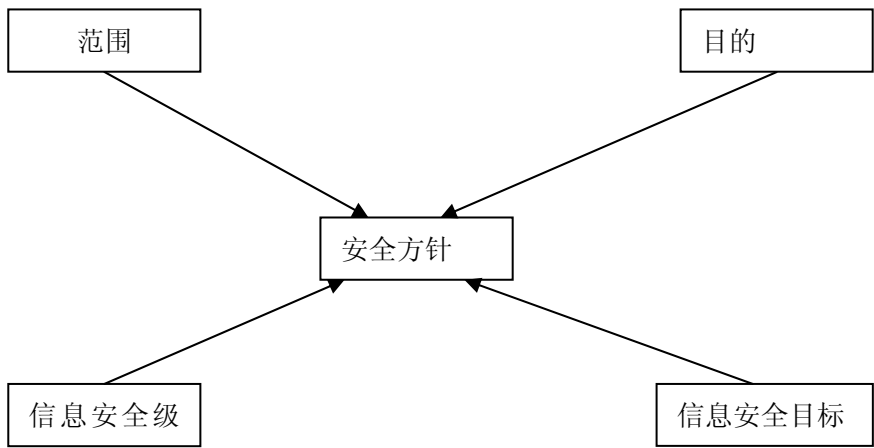


图 10 信息安全方针的内容

信息安全方针的输入数据是基于以下过程的结果：

- a. 总的组织管理原则和方针；
- b. 管理者对信息安全的管理体系的理解和承诺；
- c. 业务分析；
- d. 信息安全评估；
- e. 综合风险评估；
- f. 现有的组织和其它管理体系是如何组成的。

如果制定方针时使用了不完整的或不正确的输入数据，那么就会有方针不能反映本组织对安全方面的要求的大风险。

为了定义信息安全方针中表述的信息安全目标，可以邀请外部信息安全专家参与。为了达到期望的信息安全等级，组织的目标应考虑到信息安全要求和实施信息安全控制措施上有限的可用资源。特别重要的是要识别可用性、完整性和机密性的实际要求，因为高级别的信息安全通常涉及到高成本的实施。因此，最好是把各个要求进行合理的优先排列，这作为后

阶段安全处理过程中资源规划的基础。

为了能广泛代表组织，参与成员应进行挑选；例如，应包括以下角色：

- a. 高级管理者(例如COO, CEO, CSO 和 CFO)；
- b. 生产线管理员(例如业务单位领导)；
- c. 过程责任人(代表重要的业务领域)；
- d. 其它对现有的环境、条件、现有管理体系和信息安全相关知识非常了解的人员。

基于上述的信息和知识制定方针。为了激励组织，管理者在以前的分析中所识别的重要事情，应在方针中明显地标出，并加以强调，指出如果不遵守方针会发生的事情也很重要。影响组织的法律法规也应强调。许多例子可引自参考文献、国际互联网、利益协会和行业协会。典型例子可引自年度报告、其它方针文件或管理者支持的其它文件。

关于方针的实际范围可能有许多不同的解释和要求。简而言之，职员要能够理解。此外，应充分辨别需要什么目标去应对相关的规章和业务目标。一个方针的篇幅可以是 2-4 页。如果选择非常简短的方针，那么应附加一个更全面的模板文件，可为下一阶段引入信息安全管理的过程使用。

方针应是全面的并定期的地进行评审。任何人对方针都有责任且它的维护应列入方针和/或规章中，例如：在“跟踪”和“符合性”条款之下。

对于大型组织和复杂组织(例如：有很多不同的操作区域)，有必要制定一个总方针和许多基本的运行合理的方针。

方针的组成应包括以下方面：

- a. 信息安全的定义、总目标与范围，安全的重要性促进以安全的方式与其他方进行信息共享；
- b. 声明管理者支持信息安全目标与原则的战略目的；
- c. 简短介绍一般性的安全政策、原则、指南和对本组织有重要意义的需要遵从的要求。例子包括：
 - 符合法律、条例、协议和其它外部安全要求；
 - 安全培训要求；
 - 组织的连续性计划；
 - 忽视安全方针的后果；
 - 风险评估；
 - 信息安全(包括报告事故)的一般责任和特殊责任的定义；
 - 参考其它管理文件和各个信息系统常规或其它应遵守的安全规章。

方针应传达到整个组织内受影响的所有人员。

被提议的方针(有版本号和日期)应在组织内由操作管理员(需要斟酌)进行反复核对和制定。在得到管理层或相关人员核准后，操作管理员批准信息安全方针。然后，信息安全方针以一种相关的、可访问的和可以理解的方式传达给组织内的每一个人。

9.2.3.2 运行计划和流程

在信息安全处理过程中，涉及整个组织或特殊工作的标准和流程应加以开发。程序规定或将要采取的措施应该被记录下来，以此作为工作场所内每一位员工的行为规范。这些规则应加以编辑并适合每个目标小组使用。这些标准和程序应适用于整个组织或定义边界。

这些结果为组织内信息安全工作奠定了基础。整套法律法规要求应包括应达到“什么”目标，而流程也应达到“如何”去达到所要求的总体水平。例如，应实施的子过程和应存在的安全防范需要进行定义。

这些工作应包含标准和流程两方面的内容，这是为了提供足够的支持以使组织引入和形成更多详细的流程（在下一级别，已形成的流程“如何”适应应执行的工作）。

标准和流程应由管理者指派的代表进行开发。

安全标准和流程应适用于组织内的任何人，并可作为制定更详细的应用流程时的支持性信息使用。结果应可用于检查组织工作是否遵循标准。

拟定信息安全标准和流程需要以下内容：

- a. ISMS 范围和边界；
- b. ISMS 方针；
- c. 风险评估结果（综合风险评估、深度风险评估）；
- d. 适用性声明，包括可控制的目标和已选择的控制措施；
- e. 风险处理计划；
- f. 信息安全方针；

ISMS 范围所包含的组织的各个不同部门的代表应参与标准和流程的开发过程。组织的参与部门应包括编制规章和过程的所有方面。为了建立尽可能好的适用操作的程序，各个代表应与相关职业部门一起进行创建工作。然后，精细加工成操作层面的程序和规则。

组织的参与者应具有观察能力，这样组织认同其参与者并能够提出问题。这些参与者应有权力并是组织的代表。与各自区域管理者保持良好关系是很重要的。重要的是创建一个尽可能小的，具有所需要的特殊能力的编辑组。——不通

第一版应很快地写出。旧规章应该进行评价，例如：如果旧规章可以进行精炼并进一步开发成新版本，特别是旧版本应该被一个全新的版本所代替。

在初期就应该清楚说明制定过程。持续的制定常常是需要的。制定一个关于有关结果的信息应如何分发的策略。

为了开发出适应性强的信息安全标准和程序，成员应从组织的各个不同部门进行挑选。例如，应该包括以下角色：

- a. 各个信息安全管理者；
- b. 各个物理安全代表；
- c. 各个信息系统责任人；
- d. 各个战略区域和操作区域的过程责任人。

对于信息安全标准，重要的是要反映出对于整个组织总体的和普通的要求是什么。子条

款的适用性结果就决定了应该制定哪些标准和流程。风险分析的结果就决定了按照不同标准应该提出的安全级别。

起草和制定规章是在组织内完成。任何工作组的每一个成员都可以负责其所分配的规章子条款的制定。起草标准和更详细的流程可以通过各条款的分条款来完成。

组织（条款）的制定工作主要通过磋商进行。这个工作可能很花时间，取决于组织的规模、管理动机和成熟度。

以下是信息安全标准和程序的结果。

- a. 包括组织基线的信息安全标准；
- b. 达到信息安全标准的信息安全流程。

9.2.4 报告和管理评审

管理评审是一系列过程。在这些过程中，管理者找出 ISMS 的有效性并决定进行改进。ISMS 管理评审应按规定的时间间隔进行执行，至少每年一次。

在还没有实施 ISMS 时，关于管理评审的唯一活动就是在暂时通知管理者初步的管理评审应在什么时候进行和如何进行，以及决定要对评审者报告什么。

管理评审的前提是基于已建立的和已运行的 ISMS 所收集到的信息。这些信息供管理者确定 ISMS 的改进。详细的“前提”信息应根据 ISO/IEC 27001 的 7.2 节“管理评审输入”的要求进行编写。应该指出管理评审应包括风险管理评审，在计划的时间间隔内，考虑到环境的变化，如组织和技术上的变化，评审风险评估的方法和结果。确保风险管理评审符合 ISO/IEC 27001 4.2.3 d) 的要求。

在计划评审时，要设想谁参与并预先通知他们有关评审的必要性和目的。这可能要包括很多角色，例如：

(1) 风险评估评审

应选择能够识别和评价每项资产的风险、能够判断环境变化的成员。例如，应包括以下角色：

- 高级管理者(例如 COO, CEO, CSO 和 CFO)；
- 生产管理员(例如业务单位领导)；
- 信息安全员；
- 信息系统责任人，各个战略区域和操作区域的过程责任人。

(2) 管理评审

应选择管理者和能够收集管理评审的输入所需要的信息的成员。例如，应包括以下角色：

- 高级管理者(例如 COO, CEO, CSO 和 CFO)；
- 生产线管理员(例如业务单位领导)；
- 信息安全员。

确定管理评审输入的各种信息的类型是有用的，例如：

- a. 监视结果；
- b. ISMS 测量结果；
- c. 能影响 ISMS 的环境变化(例如：组织内部和外部的所有变化，如商业环境的变化、社会和技术环境、法律规章对组织造成的变化)；
- d. 建议；
- e. 利益共享者的反馈，包括承受者、业务伙伴、办公室工作人员和行政机构等的反馈；
- f. 内部审核或外部审核的结果(例如：认证机构或注册机构指出的不符合项和所观察到的问题)；
- g. 有关可用的新技术信息、新产品信息和供应商发布的服务信息等；
- h. 已经采取的纠正措施和预防措施的实际情况和效果；
- i. 尚未考虑的财政、环境或法规问题时，决定关于对风险评估的脆弱点和威胁作评估的必要性；
- j. 有关过去管理评审的结果是否得到适当处理的跟踪报告。

9.2.5 规划审核

内部审核和独立审核应定期地对ISMS的实施进行评价。这些审核也用于日常工作中的整理和评价。为了实施ISMS，必须在这个阶段计划出审核的方式。

在 ISMS 审核期间，审核的结果应是基于证据而做出的决定。因此，ISMS 运行到一定时期就需要收集适当的证据。图 11 展示审核规划的概要。

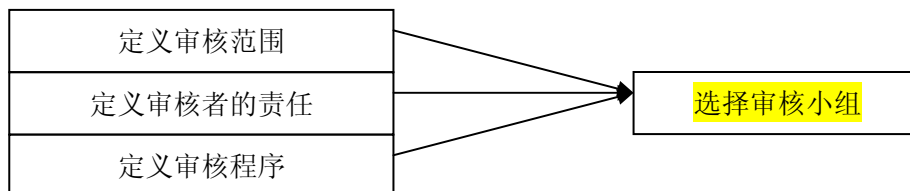


图11 审核规划的概要

注：在执行审核之前，ISMS的PDCA周期应全部实施了。

独立于内部ISMS审核范围的组织单位或个人应作为管理者选定的审核员。这些审核员对内部ISMS审核，应制定计划、执行、报告和跟踪的内部ISMS审核以获得管理者的承诺。

内部ISMS审核应定期执行和评价ISMS的控制目标、控制措施和程序是否符合ISO/IEC 27001的要求和相关法律法规的要求，是否符合已识别的信息安全要求，是否得到有效的实施和维护。

然而，对于小组织来说，挑选内部ISMS审核员可能有一定困难。如果没有足够的可用的

资源供内部有经验的员工执行各类审核工作，那么应聘请外部专家执行审核活动。邀请外部审核员的好处是可以避免员工偏袒自己工作的情况。当组织使用外部审核员时，应考虑以下事宜：外部审核员熟悉内部ISMS审核；然而，他们没有足够的有关组织的业务环境的知识，而应从内部员工补充足够的信息。相反，内部审核员可能没有足够的有关ISMS审核的知识，但是他们能够通过考虑组织的业务环境，而执行仔细而准确的审核。组织应认可内部审核员和外部审核员执行内部ISMS审核的特征。

控制措施实施的有效性和功效(见ISO/IEC 27004)应在内部审核的范围内进行检查。如果内部没有足够的可用资源(有经验的内部员工)来执行各类审核，那么应聘请外部专家代替执行审核活动。

重要的是参与安全目标规划和设计的人员不能执行审核，因为他们难于找到其自己的错误。根据组织的规模，邀请外部审核员的好处是可以避免员工偏袒自己工作的情况。

这个步骤的成员由执行审核的人员(即内部ISMS审核员)和受审核的人员组成。管理者既可作为受审核的人员，又可作为执行审核的负责人。

- 高级管理者(例如：COO, CEO, CSO 和 CFO)；
- 内部ISMS审核员(内部员工或外部专家)；
- 所有成员(除了与ISMS范围有关的管理者)都是受审成员，例如，
 - 安全产品的使用者；
 - 信息系统负责人；
 - 信息安全负责人；
 - 所有操作者和安全控制措施负责人。

在内部ISMS审核期间，应检查ISMS是否如期望的那样被有效执行和维护。由于内部ISMS审核应根据计划执行，因此审核员在编制审核程序计划以及审核结果时，应考虑审核管理目标、控制措施、过程和流程的状况和重要性。

在执行审核期间，审核的准则、适用范围、频度和方法应形成文件。

在挑选审核员时，应确保审核过程的客观性和公平性。但重要的是审核员应具有安全操作或管理等各种不同的能力。例如，在执行一系列审核程序时，审核员要求具备以下方面的能力：

- a. 规划和执行审核；
- b. 报告结果；
- c. 建议纠正措施和预防措施等。

此外，组织需要在程序文件中定义审核员的责任和审核过程。

如果在组织内没有满足要求的审核员，那么可以聘请外部审核员。注意，为了确保客观性，审核员不能审核自己的工作。负责审核过程的管理者应确保及时采取措施删除所发现的不符合项并找出原因。这不意味着不符合项应立即加以纠正。此外，所执行的纠正措施应包括已采取的措施的验证和验证结果的报告。

从管理的观点，内部ISMS审核可以作为部分进行有效的审核，或者作为整个组织的业务审计进行审核。在执行审核时，最好查阅“ISMS ISO/IEC 27006，ISMS 审核认证机构的要

求”，以及有关审核的“ISMS ISO/IEC27007”。

也可以使用信息安全审核系统或体系审核系统，邀请外部专家执行内部ISMS审核。

管理评审的重要输入之一是内部ISMS审核的结果。ISMS认证准则对内部ISMS审核进行了详细的定义。

9.2.6 安全意识

信息安全关系到所有员工（无一例外）。每位员工认真工作的时候应具备安全意识，这样可以避免损害并对组织的成功作出贡献。提高信息安全意识，为所有员工以及所有管理人员提供适当的教育是组织的首要任务。为了能够如期执行安全控制措施，员工应具有必要的基本技能和实践实施技能。此外，具有关于安全管理机制应如何设计和运作方面的知识也很重要。这就包括对安全控制措施和目标的理解。

如果员工被雇用或现有员工调换了新任务，那么他们应接受全面的培训以便能迅速地了解和投入到新的环境。这包括工作上的安全方面的培训。如果员工离开组织或者变更了角色和责任，那么这种情况应配备相应的安全控制措施（例如，撤消授权、归还钥匙和ID卡）。

教育与培训教材应包括以下内容：

- a. ISMS 范围和边界；
- b. ISMS 方针；
- c. 风险评估结果；
- d. 适用性声明，包括控制目标和已选择的控制措施；
- e. 风险处理计划；
- f. 信息安全方针、标准和程序。

在大型组织，一套培训教材一般是不够的。因此必须有多种不同的培训教材，以应对适合每个目标群体范围的信息安全的重要性和复杂性的范围和内容。例如，与文职人员或行政助理相比，IT管理员或软件开发者需要具备信息安全技能和知识。在起草信息安全培训材料的最初阶段，要分配组织的员工到目标组，这样方便他们定制专业材料。重要的是要确保每一个员工直接地或间接地被分配到这些目标组中，确保培训材料可用并进行培训。

ISMS范围内的所有工作成员都应接受培训和意识教育程序。这包括负责规划、提供培训和意识教育计划的成员。例如：应包括以下角色：

- a. 负责培训的管理者（例如人事部经理）；
- b. 培训的支持管理者（例如信息安全员、信息系统职员）；
- c. 负责执行培训的管理者；
- d. 负责执行培训的雇员。

信息安全培训材料应与组织的其它培训教材（特别是IT用户培训教材）紧密协调准备。应考虑把信息安全培训专题归并到IT用户课程。至关重要的是讲师要有专业技术并示范适当的技能。培训课程的设计应涵盖用户信息安全的内容。

信息安全培训教材至少应包含以下要点：

- a. 关于信息安全的风险和威胁；；
- b. 信息安全的基本术语和基本因素；
- c. 清晰定义组织信息安全事故是如何识别和如何通过适当的目标组进行处理；
- d. 组织的信息安全方针、标准和程序；
- e. 组织内的责任和报告渠道；
- f. 如何能有助于信息安全？
- g. 如何判断信息安全事故是否已经发生并应该怎么办？
- h. 如何自我教育并获得有关信息安全的信息？

取决于IT使用的类型和深度，对于特殊目标组应包括另外的专题，例如：

- a. 安全的电讯；
- b. 特殊 IT 系统和应用系统的安全要求；
- c. 安全的软件开发；
- d. 信息安全流程的拟定和审核；

对于每一种情况，都必须检查哪些主题可以通过组织的内部员工进行处理和哪些主题最好通过外部课程进行处理。由于技术变化的速度很快，以前获得的知识很快过时。新系统、新威胁、脆弱点和缓解控制措施，强制要求信息安全知识要不断地加以更新和扩大。因此，这些要点的培训应提供给新员工和有经验的雇员。以及增补的课程也应定期地提供给有经验的用户。

重要的是培训教材要定期地更新。管理者负责贯彻教育与培训以确保被分配的角色中的所有员工具有完成所要求工作的能力。理想情况是执行教育与培训的内容应帮助所有人员理解其所参与的信息安全活动的意义和重要性，并为如何达到 ISMS 的目标而作出贡献。

重要的是要评价已经执行的教育与培训的有效性，以及其结果能证明个人具有胜任的能力。所需要的能力取决于工作内容。建立、实施、运行和维护 ISMS 所需要的可能的能力范围如下面表 2 所列。

与信息安全管理有关的能力	通用信息安全管理理论和领导能力等。
与信息的安全审核有关的能力	通用信息安全审核理论和审核实践等。
与安全技术有关的能力	网络安全、服务器应用安全、操作系统安全、防火墙、渗透探测系统、病毒、安全编程和加密技术等理论和实践。

表 2 能力范畴

以下内容应由信息安全教育与培训过程提供：

- a. 信息安全教育与培训教材；
- b. 信息安全教育与培训的人员组成，包括他们的角色和责任；
- c. 信息安全教育与培训计划；
- d. 显示雇员信息安全教育与培训的结果的实际记录。

9.3 设计 ICT 安全和物理安全

活动

为风险处理设计选择的控制目标和控制措施，包括ICT安全和物理安全领域。

输入

- 6.5 活动的输出 - ISMS的范围和边界；
- 6.6 活动的输出 - ISMS方针；
- 7.2 活动的输出 - 信息安全要求；
- 7.3 活动的输出 - 信息资产；
- 7.4 活动的输出 - 信息安全评估；
- 8.3 活动的输出 - 风险评估结果；
- 8.4 活动的输出 - 已确认的风险处理方案；
- 8.4 活动的输出 - 已选择的控制目标和控制措施；
- ISO/IEC27002。

实施指南

为了风险处理设计选择的控制目标和控制措施，至关重要的是设计ICT安全和物理安全领域以及组织的安全领域。ICT安全不仅涉及信息系统和网络而且涉及操作要求。物理安全涉及所有方面的访问控制、信息资产及其存储/保存的物理保护，以及安全控制措施本身的保护手段。

8.4 节所述的选择的控制措施，应按照对处理风险和达到控制目标的结构化实施计划进行实施。如果已识别的控制措施得到适当地和有效地实施，那么结构化实施计划是必要的。信息安全管理者负责制定实施计划。

为了制定结构化实施计划，以下内容是特别需要的：

- a. ISMS 范围和边界；
- b. ISMS 方针；
- c. 风险评估结果；
- d. 反映风险和已识别的风险处理选择方案的风险处理清单；
- e. 包括已选择的控制目标和控制措施的适用性声明。

以下方面的内容应写进实施计划中：

- a. 负责控制措施的实施人员的姓名；
- b. 被实施的控制措施的优先级；
- c. 处理风险的对策；
- d. 实施控制措施的任务或活动；
- e. 实施控制措施的时间声明；
- f. 控制措施实施完成后，应报告的人员；
- g. 实施资源（人力、物力要求、空间要求、费用）。

实施计划不仅要定义初始实施过程的责任而且也要定义实际实施过程的责任。这在初

始设计过程和实际实施过程之间有一定区别，例如，系统开发是组织为了实现和实施组织的最好实践。

初始实施过程的责任一般包括：

- a. 控制目标的规范与期望的计划状态的描述；
- b. 选择的控制措施的适当对策，以处理风险达到控制目标；
- c. 资源的分配（工作量，财力资源）；
- d. 实施控制措施的实际时间目标；
- e. ICT安全、物理安全和组织安全的综合方案。

实际实施过程的责任包括：

- a. 在工作场所的操作层面上，设计ICT领域、物理领域和组织领域选择的对策；
- b. 实施主项目的详细任务的开发；
- c. 提供的程序和信息为安全意识促进控制措施和培训课程；
- d. 提供的援助和在工作场所实施的控制措施的。

取决于控制措施的类型（ICT的，物理的，或组织的），初始过程和实际实施过程之间不可能总是做出一个严格的定义。控制措施的实施常常需要几个不同组织之间的合作。例如：为了获得、安装和维护技术设施，需要有系统责任的人员。另一方面，例如：为了建立和编写有关技术设施使用的适当规则，需要有组织责任的人员。

信息安全应归并到组织范围的程序和过程。如果实施有困难，那么相关组织应立即进行沟通以至可确定一个决议。例如，典型的解决方案是修改程序和过程、分派角色和责任、改编技术程序。

以下方面是实施ISMS控制措施的结果：

- a. 实施计划：规定控制措施实施的细节，例如时间表和实施团队的组织结构等；
- b. 实施结果的文件和记录。

输出

- 实施项目计划的初始实施过程选择的ICT和物理安全领域的安全控制措施；
- 实施项目计划的实际实施过程选择的ICT和物理安全领域对策。

其它信息

9.4 设计监视和测量

9.4.1 监视和测量的概要

活动

为ISMS支持管理评审，设计ISMS特殊的要求，包括安全监视和测量程序。

输入

- 6.5 活动的输出 - ISMS的范围和边界定义；
- 6.6 活动的输出 - ISMS方针；

- 7.2 活动的输出 - 信息安全要求；
- 7.3 活动的输出 - 信息资产；
- 7.4 活动的输出 - 信息安全评估；
- 8.3 活动的输出 - 风险评估结果；
- 8.4 活动的输出 - 已确认的风险处理选择方案；
- 8.4 活动的输出 - 已选择的控制目标和控制措施；
- ISO/IEC27001；
- ISO/IEC27002；
- ISO/IEC27004。

实施指南

通过以下活动，设计ISMS特殊的要求，包括安全监视和测量。

- 设计监视(见9.4.2)；
- 设计测量(见9.4.3)。

输出

在这个活动完成之后，要产生一个概述实施说明书和项目计划的文件用于：

- 监视；
- 测量。

其它信息

9.4.2 设计监视

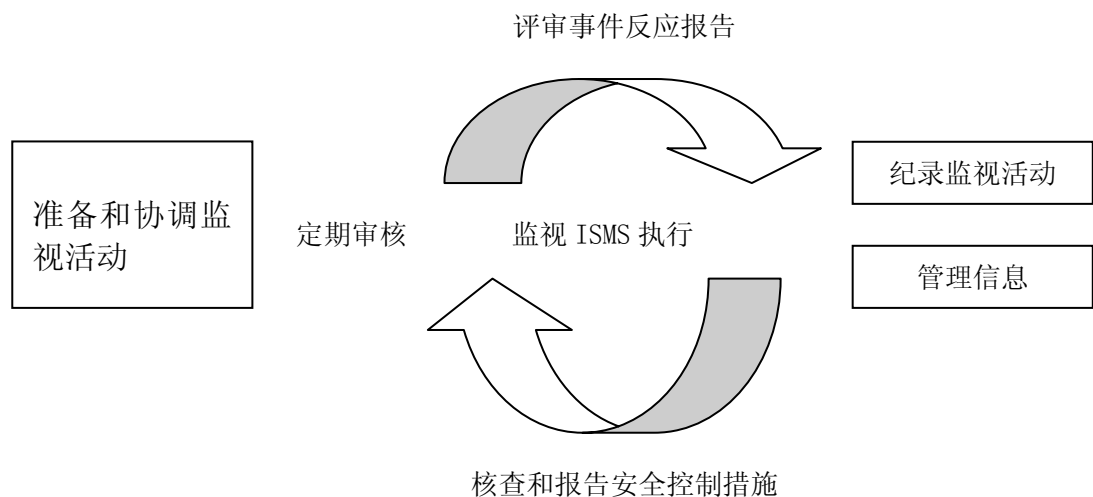


图 12 监视过程流程

9.4.2.1 准备和协调：识别监视的相关资产

注意：监视过程是一个持续的过程，因此设计应考虑监视过程的建立以及设计实际监视的需要和活动。这些活动需要进行协调，这也是设计的一部分。

根据以往的信息建立的范围和定义的资产，结合风险分析的结果和控制措施的选择就可以定义监视的目标。这些目标应包括：

- 监视的内容；
- 监视的时机；
- 监视的对象。

在实际中，以往设置的业务活动/过程和相关联的资产是监视的基本范围(这就是上述的“针对什么”)。从信息安全的角度看，监视重要资产是必要的。为了找出在资产和相关的业务活动/过程方面应监视的对象，应考虑风险处理选择的控制措施(这将设置“发现什么”和“什么时候”)。

监视可能涉及到法律方面的问题，因此要检查监视的设计使其不与任何法律有牵连。

从设计的观点，重要的是协调并设计最终的监视活动。

9.4.2.2 监视活动

为了保持信息安全的级别，应正确应用已被识别的信息安全控制措施；发现安全事故应及时解决，定期监视信息安全管理体的执行情况。从信息安全角度看，应该定期审核以了解是否所有控制措施都按计划使用并实施。这应包括检查技术控制措施(例如有关配置)和组织的控制措施(例如过程、程序和操作)是否符合要求。检查应主要针对补救中缺陷。如果检查获得通过，作为检查的目标，重要的是要得到所有相关人员承认。在检查期间，重要的是要与参与者讨论问题的办法，并准备适当的补救措施。

检查应做好充分准备，以确保最有效地达到目标，同时尽量少中断日常工作。实施一般的检查应预先与管理者进行协调。设计活动可能有 3 个不同的基本形式：

- 事故报告；
- 验证或控制功能性的不符合项；
- 其它定期检查。

下一步介绍如何根据记录和向管理者提交的信息制定活动的结果

编制的正式文件来描述整个设计，其中包含基本活动、目标以及各种不同的责任。

9.4.2.3 监视结果要求

结果是：

- a. 监视活动的记录（达到所要求的详细程度）

作为监视活动的结果，应提供一个管理报告。为了完成管理和监督任务而要求的所有信息都应以所要求的详细程度加以记录。

- b. 在紧急情况有关管理层作出的决策方面的信息

管理报告都要有清晰的按优先序列出的推荐方案列表，以及对每一个方案所期望实施成本的评估。这确保管理者立即作出必要的决定。

9.4.3 设计信息安全测量程序

9.4.3.1 设计信息安全测量程序的概要

测量过程应与项目或组织的ISMS周期紧密结合，而且测量还能不断改进组织或项目的安全相关的过程和结果。这就是所谓信息安全测量程序（原文是否有问题？）（ISO/IEC27004）。程序的设计需要观察ISMS周期。下图描述测量过程如何在ISMS周期内引入。

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，例如建立必要的PDCA循环；测量输出及检验其有效性；为过程管理者提供测量结果的反馈。为了能正确测量，以往产生的信息是至关重要的，特别是：

- a. ISMS 方针，包括范围和边界；
- b. 风险评估结果；
- c. 选择的控制措施；
- d. 控制目标；
- e. 特殊的信息安全目标；
- f. 指定的过程和资源及其分类。

管理者应参与整个测量过程。在实施测量过程时管理者应：

- a. 认可测量的要求，详情见ISO 27004；
- b. 提供所需要的信息，详情见ISO 27004；
- c. 通过以下方面调动员工参与：
 - 组织应通过某些措施证明其承诺，例如组织的测量方针、责任和义务的分配、培训和预算与其它资源的分配。
 - 委任测量程序的负责人或组织单位。
 - 管理者要支持负责在整个组织内传达ISMS测量的重要性和测量结果的人员或组织单位，以确保得到接受和使用。
 - 确保ISMS测量数据得以收集、分析和向CIO和其它相关方报告。
 - 教育管理者使用ISMS测量结果制定方针、分配资源和决定预算。

信息安全测量程序和设计应包括以下角色：

- 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。

制定信息安全测量程序是为了掌握ISMS、控制目标和控制措施的有效性。这个程序描述于ISO/IEC27004。

“Plan阶段”（即“计划”阶段）适当测量的结果应进行管理以完成这些目标。适当的“信息安全测量程序”可以根据组织的结构又所差别：

- a. 规模；
- b. 复杂性；
- c. 信息安全的综合风险概况/需要。

一般情况，组织越大和越复杂需要的测量程序就越广。但综合风险的等级也影响测量程序的广度。比较之下如果缺乏信息安全的影响是严重的较小的组织可能需要更全面的测量程

序以涵盖风险，而大组织不会面临同样的影响。测量程序的广度可以根据需要选择的控制措施和风险分析的结果进行评价。

9.4.3.2 设计信息安全测量程序

信息安全测量程序负责人必须考虑以下事宜：

- a. 范围；
- b. 测量要点；
- c. 执行测量；
- d. 测量的周期；
- e. 报告。

测量程序的范围至少应包含ISMS的范围、控制目标和控制措施。特别是应根据业务、组织、位置、资产、技术以及包括对任何ISMS范围删减（这可以是单一控制措施、流程、系统、功能区域、整个企业、单一场所，或多场所组织）的详细说明和正当性理由等方面的特性确定ISMS测量的目标和边界。

在选择测量“要点”时，ISO/IEC 27004的“信息安全测量过程”规定起点就是测量对象。为了建立测量程序，首先要确定对象。这些对象可以是流程或资源（详情见ISO/IEC27004）。在定义程序时，ISMS范围所定义的对象常常被分解以发现应被测量的真实对象。这个定义过程可以用下面的例子加以说明。组织是总体对象—业务流程A或IT系统X是该对象的一部分，在这个过程中本身也构成一个对象。为了观察保护信息的实际效果，影响信息安全的该过程内的众多对象（人员、规则、网络、应用系统和设施等）是测量的对象。

在实施“信息安全测量程序”时，应注意可以服务于ISMS范围内的许多业务流程和随后对ISMS的有效性和控制目标又有很大影响的测量对象。一般来说，在程序范围内这些对象一般应优先考虑，例如，安全组织和相关的流程、机房和信息安全合作者等。

测量的周期可能有很大变化，但为了配合管理评审和整合持续改进 ISMS 流程，最好是测量在一定时间间隔内执行或总结。程序的设计应包括此内容。

结果的报告应进行设计，确保按照 ISO27004 进行沟通。

“信息安全测量程序”的设计应形成文件，并注明由管理者批准的程序。此文件应包括以下内容：

- a. “信息安全测量程序”责任；
- b. 沟通责任；
- c. 测量范围；
- d. 如何执行（使用的基本方法、外部执行和内部执行等）；
- e. 应什么时候执行；
- f. 如何报告。

如果组织开发其自己的测量要点，那么作为设计阶段的一部分这些要点必须形成文件，（详情见 ISO/IEC 27004）。此文件可能十分全面并不必由管理者签署。这也是因为细节可能在实施时发生变化。

9.4.4. 测量 ISMS 的有效性

制定将要实施的“信息安全测量程序”的范围时，应注意使对象不太多。最好把测量程序划分成几个不同部分。这些部分的范围可看作单独的对照测量。但普遍存在主要目的是结合测量提供了一个评价ISMS有效性的指示。这些次级范围通常是一个确定清晰边界的组织单位。在这些次级范围内，将许多业务流程中的众多对象与众多对象的测量结合在一起，就可形成“信息安全测量程序”的适当范围。这也可看作一系列具有两个以上流程/对象构造的ISMS活动。因此，整个ISMS的有效性可以根据这些具有两个以上流程/对象的测量结果进行测量。

由于目标是测量ISMS的有效性，测量控制目标和控制措施很重要。足够数量的控制措施是一方面，而这些控制措施要能足以评价ISMS的有效性则是另一方面。（在ISO/IEC 27004中提及了限定“信息安全测量程序”的范围的其它理由。）

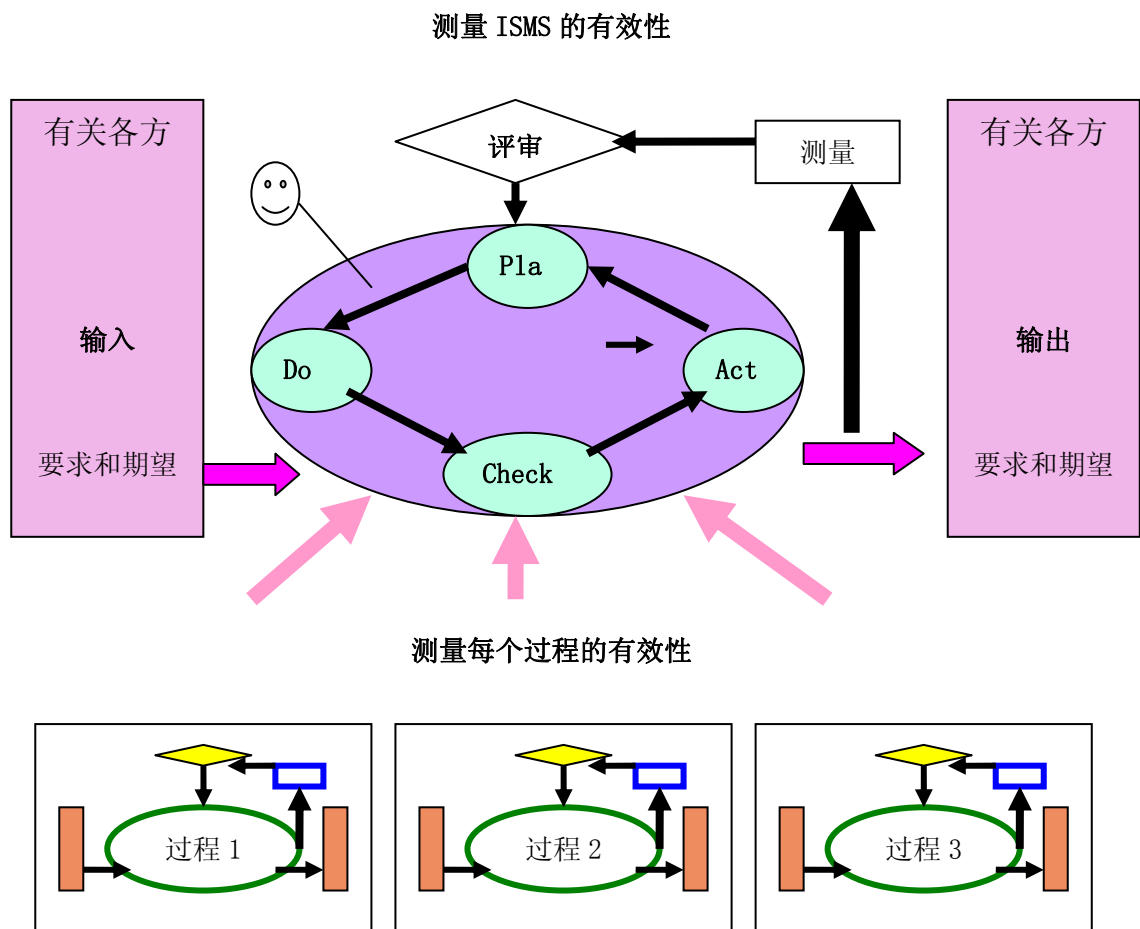


图 13 ISMS 的 PDCA 过程有效性的测量，和组织内过程有效性的测量

在使用评价 ISMS、控制目标和控制措施的有效性的测量结果时，重要的是管理者知道“信息安全测量程序”的范围。测量程序负责人应获得管理者对“信息安全测量程序”的范围的批准。

注 1:

ISO/IEC 27001 有关有效性的测量的要求是“控制措施或系列控制措施的测量”（见 ISO/IEC 27001 的 4.2.2d）

注 2:

ISO/IEC 27001 有关整个 ISMS 的有效性的要求是“整个 ISMS 的有效性的评审”，而“整个 ISMS 的测量”是不要求的（见见 ISO/IEC 27001 的 0.2.2）

实际测量的执行可使用内部人员或外部人员或两者结合。在评价内部资源或外部资源时，要考虑组织的规模、结构和文化因素。小的和中等规模的组织使用外部支持获得的利益要比大型组织的多。根据文化，使用外部资源的结果也获得一个有效的结果。如果组织进行内部审核，那么内部资源可能是有效的。

9.5 ISMS 记录的要求

9.5.1 ISMS 记录的概要

活动

为记录和发布正式的ISMS信息，建立必要的格式。

输入

- 6.5 活动的输出 - ISMS的范围和边界定义；
- 6.6 活动的输出 - ISMS方针；
- 9.2 活动的输出 - 组织的安全；
- 9.3 活动的输出 - ICT 和 物理安全；
- 9.4 活动的输出 - 监视和测量；
- ISO/IEC27001；
- ISO/IEC27002。

实施指南

设计ISMS记录包括以下活动：

- 设计文件要求(见9.5.2)；
- 设计记录要求(见9.5.3)。

要求ISMS文件应包括管理决定的记录，确保行动可追溯到管理决定和方针，而已形成的记录结果可以重用。

重要的是能够展示以下关系：从所选择的控制措施可追溯到风险评估结果和风险处理过程，而后再追溯到ISMS方针和目标。在ISMS活动中，风险评估和风险处理过程要与管理者指示的ISMS方针和目标一起执行，并根据结果选择控制措施。

文件指出根据风险评估的结果和风险处理选择控制措施的证据，这些过程要随同ISMS方针和目标一起执行。每个人对风险评估的流程和有效性的测量有不同的解释。然而，在这种情况下，不同的人比较结果是困难的而且这使得有效管理信息安全有一定难度。

文件重要是再现这些结果和各种程序。至于选择的控制措施、建立和形成文件的程序需要一个人执行。

ISMS文件要求要阐明ISMS方针和目标、ISMS的范围、支持ISMS的流程和控制措施、风险评估方法的描述、风险评估报告、风险处理计划和适用性声明。

输出

在这个活动完成之后产生一个文件：

- 依据已选择的安全控制措施，实施规范说明和实施项目计划；
- 依据运行的要求，实施规范说明和实施项目计划。

其它信息

9.5.2 文件控制要求

ISMS文件必须有版本号、可受管理、可为需要人员在必要时使用。必须建立ISMS文件管理的行政管理程序；必须管理的文件包括文件发布前得到适当批准、更新文件、确保文件的更改和现行修订状态得到识别；必须把ISMS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适用文件相关版本，确保文件保持清晰、易于识别，并依照其适用的类别的程序进行传输、贮存和最终销毁。此外，确保外来文件得到识别，而文件的分发得到控制，防止滥用作废文件；如果作废文件因任何目的而保留时，应对这些文件进行适当的标识。

9.5.3 记录控制要求

记录应被创建、保持和控制，并作为组织的 ISMS 符合 ISO/IEC 27001 和展示运行效果的证据。

在整个 PDCA 阶段，也必须保持实施状况的纪录，所有 ISMS 安全故障和事故的纪录(例如事故与事件记录)，教育、培训、技能、经历与资格、内部审核、纠正与预防措施和组织的纪录。

为了控制记录应执行以下任务：

- a. 编写的控制措施的文件需要对数据进行标识、保存、保护、查询和废弃，并编写数据保存期限的文件；
- b. 定义应记录的事宜、范围和操作管理流程；
- c. 当任何保存期是由商业法规(Commercial Code)或任何其它法律指定时，保存期应与法律要求相符合；

9.6 制定 ISMS 实施计划

活动

完成ISMS项目实施阶段的项目计划，需要实施包括组织安全、ICT安全和物理安全所选择的控制措施的活动，以及如ISO/IEC 27001所述的有关ISMS的正式活动。

输入

- 6.5 活动的输出 - ISMS范围和边界定义；
- 6.6 活动的输出 - ISMS方针；
- 9.2 活动的输出 - 组织安全；
- 9.3 活动的输出 - ICT 和 物理安全；
- 9.4 活动的输出 - 监视和测量；
- 9.5 活动的输出 - 文件和记录；
- ISO/IEC27001；
- ISO/IEC27002。

实施指南

控制措施选择的结论以及其它所计划的ISMS相关活动和如何对其实施都应正式地写入项目计划。项目计划应遵循处理项目的通用准则，并可用通用工具和方法进行支持。由于ISMS

项目包括组织内许多不同的角色，所有重要的是活动要明确地指派负责人，项目的策划人和负责人要在整个项目和组织内进行广泛的交流。

对于所有项目，重要的是项目负责人应保证该项目所需要的足够资源已进行了计划，并进行了分派。

输出

在这个活动完成之后产生一个实施项目计划文件。

- 初始实施流程(见9.3 ICT 和物理安全)；
- 实际实施流程(见9.3 ICT 和物理安全)。

其它信息

10 实施 ISMS

10.1 ISMS 实施概要

目标:

- 基于 ISMS 项目计划，实施所选择的控制措施和 ISMS 特殊要求；
- 实施监视和测量；
- 创建 ISMS 程序和控制文件。

参考 ISO/IEC 27001: 4.2.2 b)-e), h)

假设管理层已经批准实施 ISMS，并定义了 ISMS 的范围和方针，经过业务分析已获得信息资产及信息安全评估结果，风险评估计划、风险评估描述和评估报告也可用，现在 ISMS 实施计划、记录和发布过程也可用。图 14 是实施阶段及其主要活动的概要。

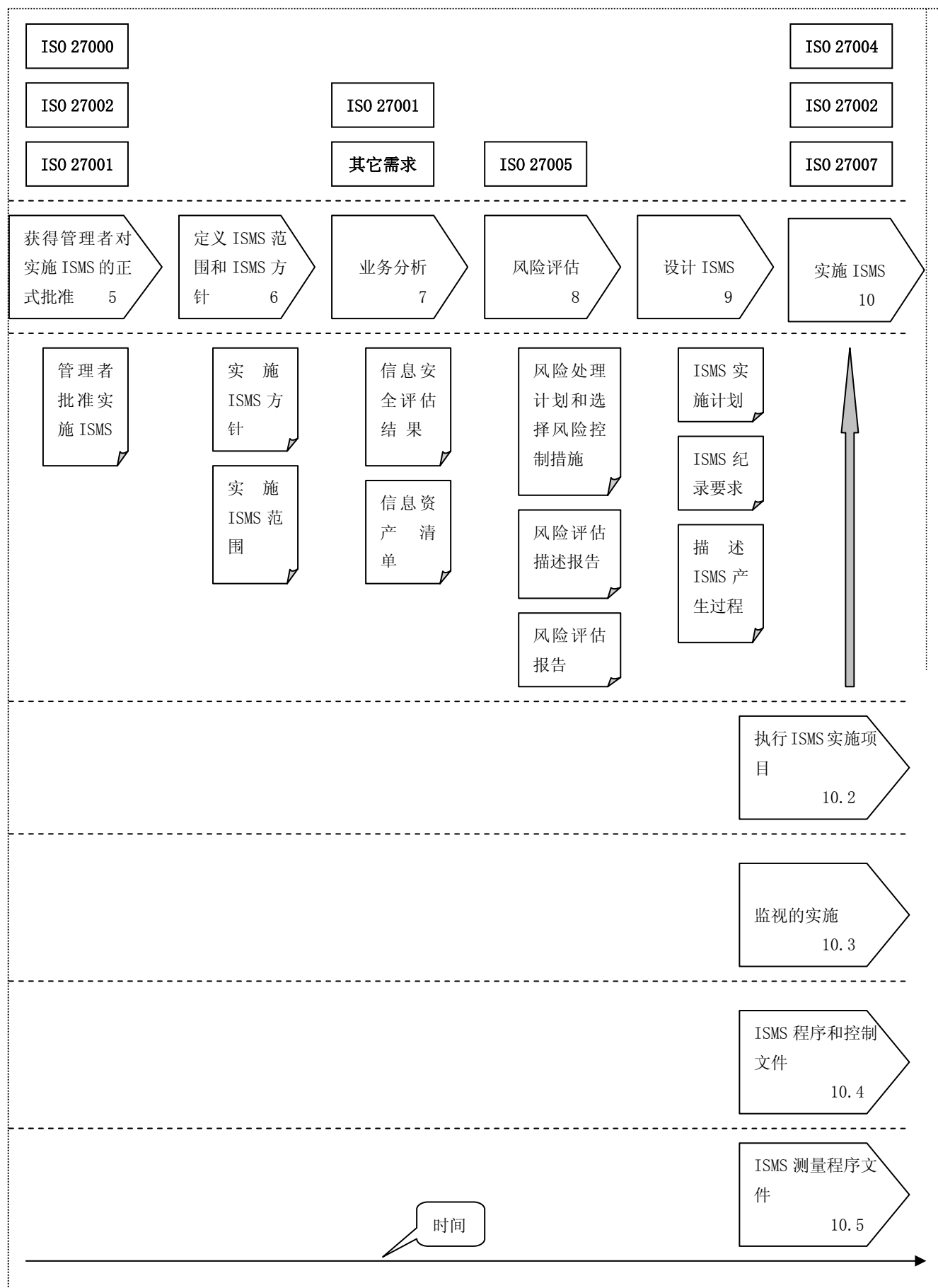


图 14 实施阶段及其主要活动概要

组成整个项目的各种不同活动有自己的目标，这些目标主要与 ISO/IEC 27002 中的控制措施以及其它所选择的控制措施(控制措施的实施例子见附录 B) 相关；如上所述与 ISO/IEC 27001 相关的活动也包括在内。

本阶段主要是执行实施计划中所设计的活动，如果能适当执行这些活动，则目标就能达到。

10.2 执行 ISMS 实施项目

10.2.1 执行 ISMS 实施项目概要

活动

实施选择的控制措施和ISMS相关主题的子项目。

输入

- 6.5 活动的输出 - ISMS的范围和边界定义；
- 6.6 活动的输出 - ISMS方针；
- 9.2 活动的输出 - 组织的安全；
- 9.3 活动的输出 - ICT 和 物理安全；
- 9.4 活动的输出 - 监视和测量；
- 9.5 活动的输出 - 文件和记录；
- 9.6 活动的输出 - 实施计划；
- ISO/IEC27001；
- ISO/IEC27002。

实施指南

执行ISMS实施项目应考虑以下方面：

- 角色和责任(见10.2.2)；
- 沟通(见10.2.3)；
- 协调(见10.2.4)；
- 变更(见10.2.5)。

输出

活动完成之后，其结果将形成文件。

- 实施的项目计划和通过所选择的安全控制措施得出的实际结果。

其它信息

10.2.2 角色和责任

在设计ISMS时，已经定义了许多项目，这些项目应指派各种不同的责任(请见附录X-角

色的例子)。项目的前提是管理者应按ISO/IEC 27001中5.2.1条款的规定分派足够的资源。

10.2.3 沟通

项目的负责人除了以合适的方式处理项目以外,即使那些意见不合的人不积极参与项目活动,该项目的负责人应就实施事宜定期与他们定期沟通。

如果管理者能够以内部沟通的方式传达项目的重要性,也会对实施有好处。

10.2.4 协调

实质是为了完成项目实施,责任人应跟踪各种不同的活动,以获得各个事件的合理程序,尤其是上图所提及的特殊活动。例如,在执行广泛的培训活动中,如果没有适当的指导或者缺乏技术解决方案,那就没有意义。

10.2.5 变更

实施ISMS基本上涉及整个组织的范围,这个实施流程需要一段时间,而且很可能有变更。成功实施ISMS就必须熟悉整个项目并具有处理变更的能力,而且能针对变更作出适当的调整,如果有很重大的影响应报告给管理者。典型的变更有:

- a. 组织内的变更,例如:
 - 管理变更(新的承诺应得到保证);
 - 部门改组等;
 - 合并;
 - 外包。
- b. 技术环境上的变更,例如:
 - 新系统;
 - 新平台;
 - 新通信;
 - 新建筑物。
- c. 法律或合同的变更,例如:
 - 新客户义务;
 - 新法律。

重要的不是在实施项目流程中作较大的变更,而是要知道许多变更都可能影响初始决定的范围和目标以及所选的控制目标。

除了考虑威胁整个实施的成功的变更情况外,许多变更情况不需要,但它应该被管理者清楚地声明

10.3 监视的实施

活动

实施常规检查,如监视。

输入

- 6.5 活动的输出 - ISMS的范围和边界定义;
- 6.6 活动的输出 - ISMS方针;
- 9.2 活动的输出 - 组织的安全;
- 9.3 活动的输出 - ICT 和 物理安全;
- 9.4 活动的输出 - 监视和测量;
- 9.5 活动的输出 - 文件和记录;
- 9.6 活动的输出 - 实施计划;
- ISO/IEC27001;
- ISO/IEC27002。

实施指南

作为监视的一部分,常规检查是一项在ISMS实施中其它子项目中所描述的已经实施的控制措施的日常工作,这需要特别指出,这可能包括检查职工所作的工作是否符合控制措施所描述的内容(例如,在追查债务时检查旧发票、确定管理报告中数量的分析、跟踪客户询问、调查IDS异常信息或系统故障等)。在检查过程中,可能检查出错误或安全事故,这些应以一致的方式进行报告和修正。

监视的目标是使目标和结果保持一致性,改变表达方式如下。

监视活动应在“Do”阶段的组织标准和程序中预先确定,在这个步骤中,应持续地执行监视,并根据上面预先定义的规则累积监视结果。通过这些持续的监视活动,应能迅速发现处理结果中的错误,并能迅速识别已经发生或尚未发生的安全问题和事故。

独立执行监视活动时并不会按照期望的那样执行。执行这些活动应考虑与其它活动的关系,特别是与其它“Check”阶段的活动、评审、测量和审核的关系。如果发生安全问题或事故或在处理结果中发现错误,那么应确保对监视活动做出迅速有效的反应。为改进使用,累积的监视结果应审查或应用于审计。

另一方面,也应认识到执行持续的监视活动是为了检查ISMS,但在“Do”阶段的ISMS日常运行中也应执行这些活动。

为了正确地实施监视工作,应完成以下事宜:

- a. 制定组织关于监视的标准和程序,并按照这些规则执行;
- b. 让负责监视的每一个人都知道这些规则。如果需要的话,可以计划实施培训。

当然,持续执行符合规则的监视工作应通过执行ISMS得到保持;此外,所有员工(特别是监督员工)都执行监视工作是很重要的。监督责任包括决定适当的程序获得满意地执行。

输出

在这个活动完成之后,活动的结果要形成文件。

- 实施监视的实际结果。

其它信息

10.4 ISMS 程序和控制文件

活动

创建和更新必须的ISMS 程序和控制文件。

输入

- 6.5 活动的输出 - ISMS的范围和边界定义;
- 6.6 活动的输出 - ISMS方针;
- 9.2 活动的输出 - 组织的安全;
- 9.3 活动的输出 - ICT 和 物理安全;
- 9.4 活动的输出 - 监视和测量;
- 9.5 活动的输出 - 文件和记录;
- 9.6 活动的输出 - 实施计划;
- ISO/IEC27001;
- ISO/IEC27002。

实施指南

该执行文件取决于所选择的控制措施、记录要求和ISMS设计期间所提出的发布程序。

一般情况下,必要的文件程序和控制措施应记录到即使人事发生了变化也能达到信息安全为准的程度;文件应有逻辑结构且易于更新。

该文件应适用于以下活动的实施计划,特别是:

- a. ISMS审核程序文件;
- b. ISMS培训程序文件;
- c. ISMS监视程序文件;
- d. ISMS评审程序文件。

除了组织内信息安全的规章制度文件之外,还有其它对成功实施ISMS的重要文件。这些文件包含于ISMS实施项目中,其详细程度可有很大变化,取决于实施计划,由于这类文件通常是在ISMS的实施完成之后创建的,因此不可能包含于实际的ISMS实施阶段中。但重要的是在实施阶段要知道这些类型文件的需要,以下是应该考虑的文件类型:

1. 技术文件和工作程序文件(目标组:专家)

当故障或信息安全事故发生时,把业务流程恢复到希望得到的正常状态应是可能的。因此技术细节和工作程序应写成文件以保证在合理的时间内就可以完成恢复工作。例子文件是各种指导书,包括安装IT应用系统指导书、备份数据指导书、恢复数据备份指导书、电源故障后重新启动应用服务器指导书,以及测试文件、正式批准程序,和有关故障或信息安全事故发生时所要做的事情方面的指导书。

2. 用户说明书(目标组:用户)

工作程序、组织的规定和技术的信息安全测量方法都应该写成文件,这样可以避免由于缺乏知识或错误引起的信息安全事故。这方面的例子包括e-mail 和 Internet的使用、病毒感染的预防或如何认识社会工程,以及信息安全事故发生时的用户行为准则等安全指

南。

3. 管理任务报告(目标组:管理层)

管理者为了完成其管理与监督义务而需要的所有信息都应以所要求的详细程度加以记录(例如审核的结果、有效性的测量、信息安全事故报告)。

改进的问题、成功和机会应给以指出。管理报告应包含管理层需要的有关信息安全流程中管理方面的所有信息。

这类信息包括,例如:

- a. 当前信息安全流程概要;
- b. 前面的管理评价之后所记录的跟踪报告;
- c. 客户和员工的反馈;
- d. 已经出现的新威胁和安全脆弱性概要。

管理层应关注管理报告并做出必要的相关决定,例如对安全过程的改进、对资源的需求以及安全分析的结果(如:风险的减少、吸收或接受)。

4. 管理决定记录(目标组:管理层)

管理层应记录和说明所选择的信息安全策略;而且在其它所有层面上所采取的影响安全的决定也应该加以记录,以确保其能够在任何时候被理解和重复。

监视应以通常的工作监督方式执行。当员工遇到问题时应采取以下措施:

- a. 适当地报告问题;
- b. 找出问题的解决方案;
- c. 找出更好的工作方法。

这些问题可能是真实的或潜在的信息安全问题,也可能是正常的业务。

输出

在这个活动完成之后,活动的结果应形成文件。

- 实施程序和控制文件的实际效果。

其它信息

10.5 ISMS 测量程序文件

活动

编写信息安全测量程序范围之内需要的程序文件等。

输入

- 6.5 活动的输出 - ISMS的范围和边界定义;
- 6.6 活动的输出 - ISMS方针;
- 9.2 活动的输出 - 组织的安全;
- 9.3 活动的输出 - ICT 和 物理安全;
- 9.4 活动的输出 - 监视和测量;

- 9.5 活动的输出 - 文件和记录;
- 9.6 活动的输出 - 实施计划;
- ISO/IEC27001;
- ISO/IEC27002;
- ISO/IEC 27004。

实施指南

在实施阶段期间，基本工作是考虑应如何解决有效的测量。关于信息安全测量程序的信息详情可参见ISO/IEC 27004。

输出

在这个活动完成之后，活动的结果应形成文件。

- 实施测量程序的实际效果。

其它信息

参考书目

ISO/IEC 27004

ISO/IEC 27005

ISO/IEC 27006

ISO/IEC 27007

ISO/IEC 31000

参考书目

ISO/IEC 27004

ISO/IEC 27005

ISO/IEC 27006

ISO/IEC 27007

ISO/IEC 31000

附录 A

信息安全角色的例子

信息安全是一个影响整个组织的广泛领域。清晰地定义安全责任主要是为了成功的实施。由于相关安全角色和责任可有很大变化，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。附录A中的表格略述相关安全角色和责任。应注意，这些角色一般的。而特殊的角色描述是ISMS的每一个单独实施所需要的。

表3 信息安全角色和责任的例子

角色	责任的简短描述
高级管理者(例如 COO, CEO, CSO 和 CFO)	高级管理者负责想象、战略决定和协调活动，指导和控制组织。
首席信息安全官员	首席信息安全官员是信息安全的总负责人，确保信息资产的正确处理。
信息安全委员会(有会员)	该委员会负责处理信息资产，在组织中具有ISMS的领导角色。
信息安全规划组(有组员)	规划组负责ISMS正在建立时的运作。规划组跨部门工作，解决各种冲突，直到ISMS被建成。
质量保障流程责任人	“流程责任人”是业务流程和专门应用系统的联系人，负责委派任务和处理被分配给其自己的业务流程内信息。
相关方	<p>从其它角色描述的关系看，这里信息安全相关方主要被定义为除了正常业务如董事会、业主（包括两方面业主：组织的业主（如果组织是一个集团或政府组织的一部分）和直接业主（作为私人公司的股份持有者））以外的人员/机构。</p> <p>其它信息安全相关方可以是有关联的公司、客户、供应商或公共组织，如政府财政控制机构或相关的证券交易所。</p>
系统管理员	系统管理员负责IT系统。
IT 经理	所有IT资源的经理（例如IT部门经理）
物理安全员	负责物理安全(例如建筑物等)的人员，通常称为“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、风险处理和风险监控)的人员。
法律顾问	许多信息安全都有法律方面的问题。法律顾问负责考虑法律方面的问题。
人力资源	对员工负全面责任。
档案	所有组织都有含有至关重要信息的档案。这些信息需要长期保存。信息可能存在多媒体上。需要有一个负责信息保存。

个人数据	如果国家法律有要求，那么可能要有一个负责联系数据检查机构或类似于处理个人的诚实性和秘密问题的官方组织。
系统开发者	如果组织开发其自己的信息系统，那么就应有人负责这个开发工作。
专家/行家	负责组织中某些业务工作的专家和行家。
外部顾问	外部顾问可以根据其对组织的观点和行业经验，提出决定意见。然而，顾问不可能有很深的该组织的业务和运作的知识。
雇员/职员/用户	每一个雇员都应在其工作场所和环境内，同等地负责维持信息安全。
审核员	审核员负责评估和评价ISMS。
培训师	培训师负责实施培训和意识计划。
地方组织IT安全或信息安全责任人	在一个大型组织内，常常有人负责地方组织IT安全事宜，也可能是信息安全事宜。
拥护者(有影响力的人员)	拥护者不是一个负责任的角色，但在大型组织的实施阶段有很大帮助。这些人有很深的有关ISMS的实施的知识，可在组织的后面支持理解和推动。他们能够给出正面的影响意见，可以称为“大使”。

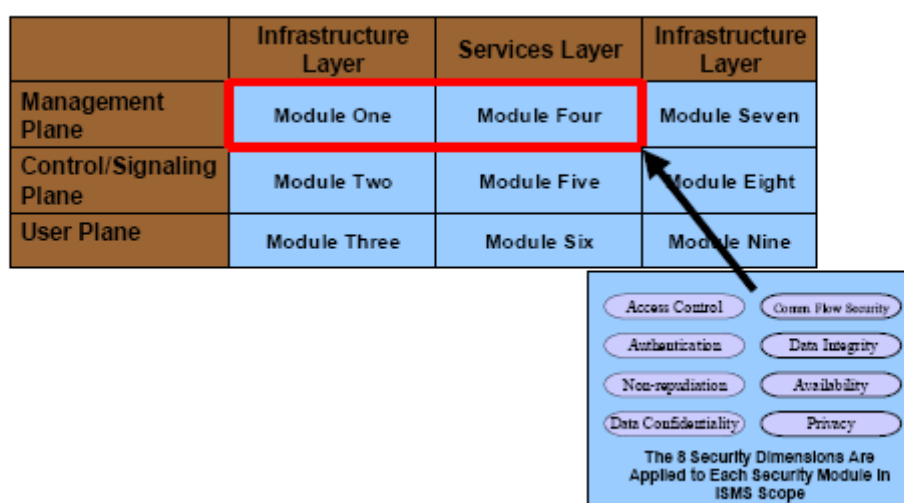
附录 B

案例研究

例1：支持ISMS ISO/IEC 27001的实施

本案例研究的目的是论证使用ISO/IEC 27001/2去建立、实施和运行信息安全管理体（ISMS）的一个行业例子。这个例子显示一个部门特殊的可行框架，使用需要适用于端对端网络的ISO/IEC 27001/2相关控制措施。

ISO/IEC 27001在组织的综合业务活动和所面临的风险框架内，为建立、实施、运行、监视、评审、保持和改进ISMS提供模型。虽然ISO/IEC 27001提供了为完成上面各个阶段而必须执行的许多步骤，但是在每一步骤执行所需要的特殊措施方面，另外的技术指南对网路指导是需要的。这个技术指南通过图A. 1提供。



图A. 1 适用于ISMS范围的网路安全要求表

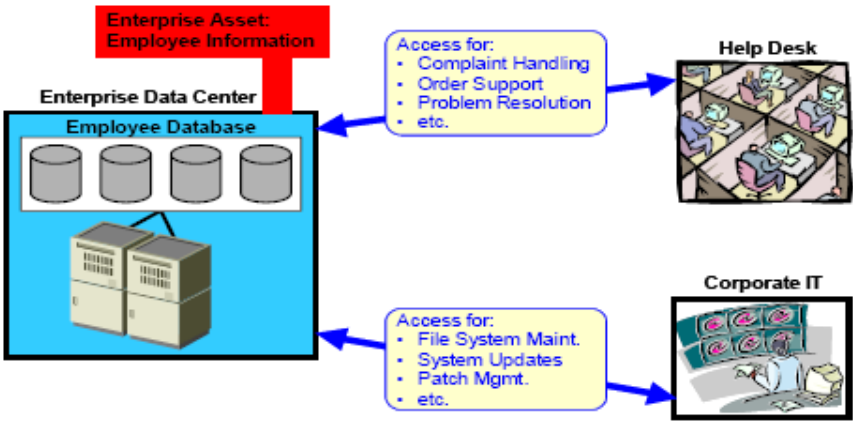
如图A. 1所示，对于一个特定的ISMS范围，分解IT产品、服务或解决方案为有层次的设备与设施组，以标准的方式检查在每层出现的各种活动。其组成包括：（1）基础设施安全，（2）服务安全，（3）应用系统安全。此外，可以出现3种活动：（1）管理或称作运作安全，（2）发信号安全，（3）最终用户安全。

ISO/IEC 27001/2控制目标和控制措施应进行识别，以减轻威胁和脆弱点。图A. 1所示的8个安全机制提供实施和运行ISO/IEC 27001/2控制措施所需要的更进一步的指导，并为ISO/IEC 27001附录A没有列出的另外的控制目标，提供基础。

安全平面和层次的交叉点代表一个可被包括进去或被排除在外的安全模块，取决于所建立的ISMS的范围。从图可见，ISMS正在建立信息基础设施和信息服务的管理。模块1和模块2是在范围内。

这个案例研究的目的是，考虑为大企业（其数据中心存放有雇员信息的大企业）的信息基础设施和服务的管理，建立、实施和运行ISMS。

范围如图A. 2所示。这个范围不表示出企业ISMS的实施所需要的每件事物，但足以示出如何使用ISO/IEC 27001/2，去建立、实施和运行信息安全管理体系 (ISMS)。如果应用系统、控制面和最终用户也包括在ISMS范围之内，那么执行同样类型的活动。

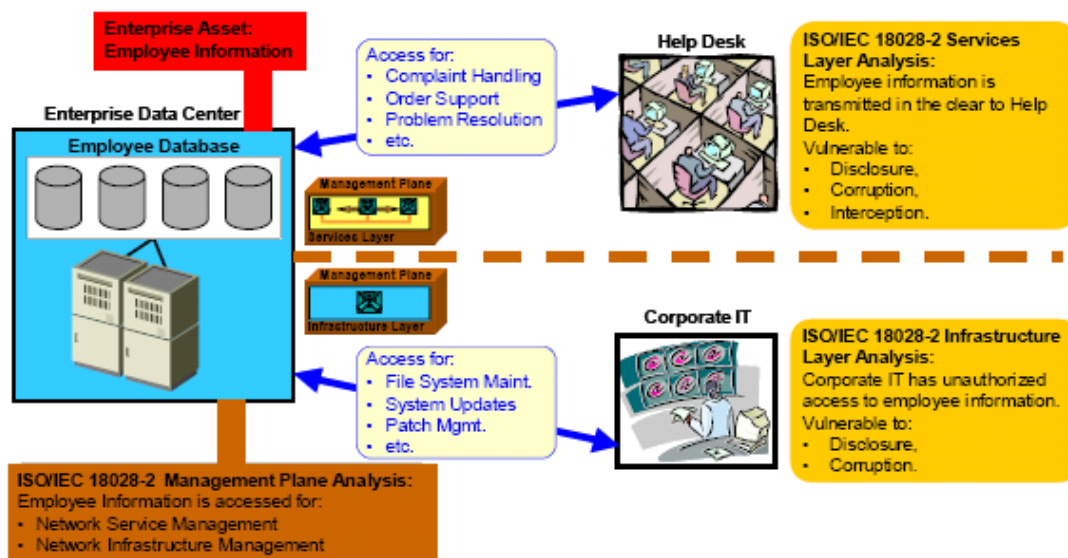


图A. 2 企业资产的访问设想

存放在数据中心的雇员信息也包括只限于授权用户使用的个人信息。保护雇员信息，应在ISMS的范围和边界之内进行定义，并通过ISMS资产识别与评价过程，被鉴别为需要保护的基本资产。雇员信息可被企业所雇用的几个支持组织访问。其中之一的组织是服务台。另外，数据中心及其所包含的系统由法人的IT组织进行维护。

如图A. 2所示，服务台访问雇员信息是为了处理投诉、支持新IT服务的订单和解决雇员获得IT服务的问题(例如远程访问)等。另外，法人的IT组织访问雇员信息是其维护活动的一部分，包括系统维护、系统更新和补丁管理等。

作为对信息基础设施和服务的管理，建立、实施和运行ISMS工作的一部分，技术管理、基础设施和雇员信息的服务应进行分析，作为风险评估工作的一部分。这个分析显示雇员信息可被企业的服务台访问，作为其一部分服务管理工作（例如管理雇员远程访问服务），以及雇员信息可被企业的法人的IT组织访问，作为其一部分基础设施管理工作(例如执行备份)。在这方面，分析工作应与ISMS风险评估合作，识别在雇员信息的基础设施与服务的技术管理上或维护活动上的威胁和脆弱点。在这个例子中，分析显示，法人的IT组织的成员可以察看和修改雇员信息，从而使它在基础设施层容易被泄露和破坏。另外，作为执行问题决议的一部分，雇员信息完全可以在数据中心和服务台之间进行传输，从而，使它在服务层容易被泄露、破坏和拦截，如图A. 3所示。



图A.3 企业资产的威胁和脆弱性分析

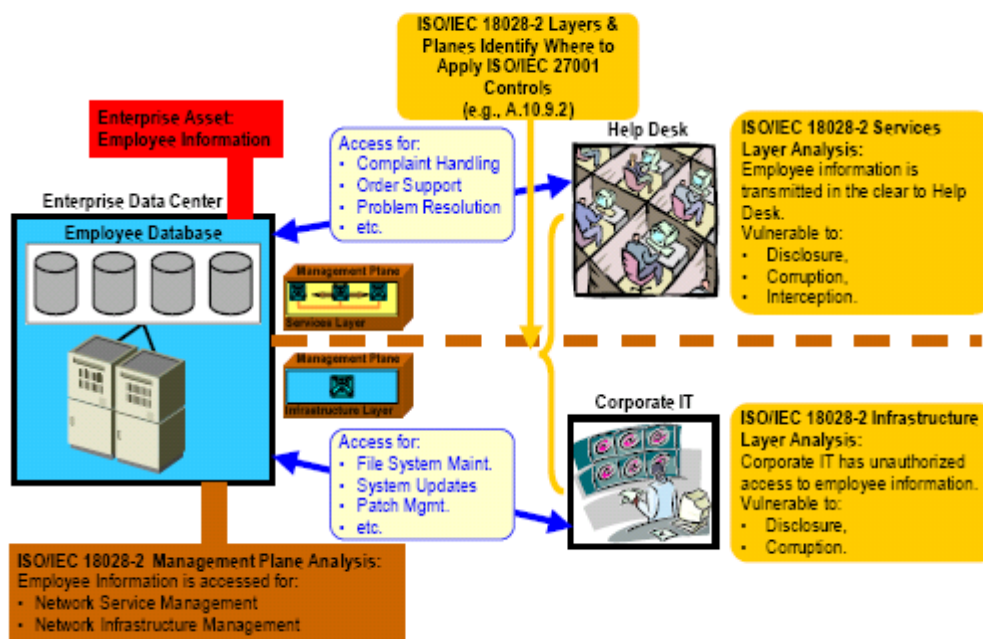
根据建立ISMS所使用的过程，执行风险分析，评估可能由雇员信息安全故障产生的业务影响，以及根据主要的威胁、脆弱点和当前企业实施的控制措施，评估这些安全事故出现的现实的可能性。这个分析的终结是组织作出决定，应用控制措施、接受风险、避免风险，或转移风险。

对于本案例研究的目的，风险分析的结论是为了使雇员信息不受先前所识别的威胁和脆弱点的影响，需要采用控制措施。因此，作为建立ISMS的一部分工作，控制目标和控制措施必须加以识别和选择，以防范在基础设施和服务层的管理面上，雇员信息受威胁和脆弱点的影响。

ISO/IEC 27001的A.10.9.2 控制措施应被识别和选择，作为在服务和基础设施层，保护雇员信息管理的控制措施，如图A.4所示。

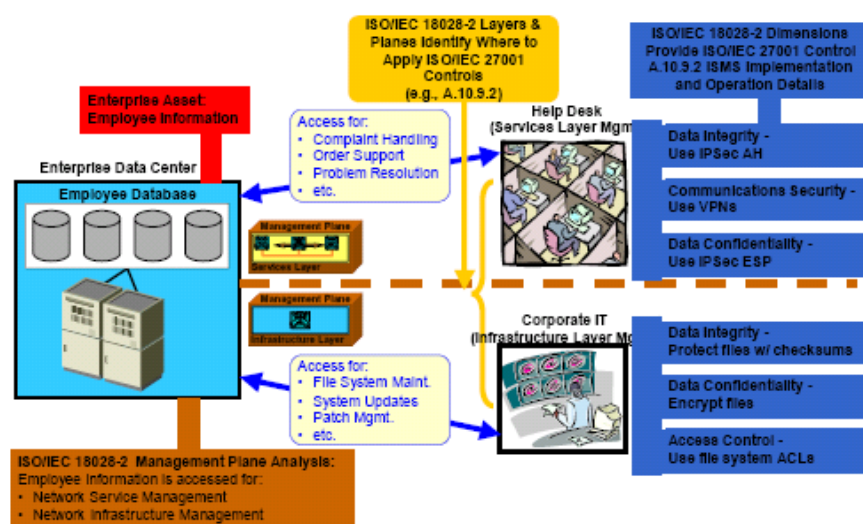
ISO/IEC 27001的A.10.9.2控制措施规定“在在线交易中的有关信息应加以保护，以防止不完全传输、错误路由、未授权的消息篡改、未授权的泄露、未授权的消息复制或重放。”

然后，获得管理者对残余风险的批准和授权实施和运行ISMS，并准备适用性声明以提供关于风险处理决定的概要，作为建立ISMS的剩余步骤。



图A. 4 使用部门特殊的指南确定应用ISO/IEC 27001控制措施

作为实施和运行企业的ISMS的一部分，图A. 4所示的部门特殊的信息，为雇员信息资产在服务与基础设施层，对A. 10. 9. 2控制措施，提供清晰的实施和运行指导。图A. 5描述如何需要A. 10. 9. 2控制措施保护雇员信息资产。



图A. 5 ISO/IEC 27001控制措施行业特殊实施与运行细节

在服务上，“通信流程安全”确保信息只在已被授权的端点之间流动(由于信息在这些端点之间流动，所以信息不被转移或被拦截)，因此防止VPNs错误路由。

“数据完整性”确保数据的正确性或精确性(即数据只由已被授权的过程或人员或装置处理)。数据可防范未授权的更改、删除、创造和复制,并提供这些未授权活动的指示。数据完整性规定了IPSec AH1在服务层的使用,防止不完全传输、错误路由、未授权的消息更改和复制,以及防止消息重放。在基础设施上,数据完整性维数规定了文件校验和的使用,侦查未授权更改。

“数据机密性”保护数据免遭未授权的泄露,并规定了IPSec ESP2在服务层的使用,防止未授权的泄露。数据机密性维数规定了文件密码术的使用。

在基础设施上,“访问控制”为网络资源的使用提供授权。“访问控制”确保只有已被授权的人员或装置才能允许访问网络要素、存储的信息、信息流、服务和应用系统。“访问控制”规定文件系统访问控制清单(ACLs)的使用,防止未授权复制。

因此,作为为了建立、实施和运行ISMS而使用部门特殊的信息的结果,企业决定用鉴别标题(IPSec AH)和封装的安全协议(IPSec ESP)配置IPSec VPNs,使雇员信息能够在数据中心和服务台之间传输。企业也决定用ACLs保护雇员识别数据库,以及数据库加密与包含校验和,以保护雇员信息不受未授权访问。

最后,为了完成实施并开始运行ISMS,企业执行以下ISO/IEC 27001所包含的活动:

- 制定和实施风险处理计划。
- 定义如何测量控制措施的有效性,以及定义这些测量方法如何用于评估控制措施的有效性。
- 实施培训和意识计划。
- 管理ISMS资源的运作。
- 实施程序和其它控制措施,以在对安全事故反应中,能够迅速发现安全事件。

总之,本案例研究示范行业特殊的网络安全标准如何增强ISO/IEC 27001。

在应得到应用的资产和活动方面,必要的ISO/IEC 27001标准的要求控制了尺度水准。另一的尺度水准是ISO/IEC 27001控制措施对不同层面的实施和运行的指导。本案例研究以完整的标准化的方式,通过应用、实施、运行安全控制措施,提供全面的端对端的安全。

关于 IPSec AH的信息见<http://www.ietf.org/rfc/rfc1825.txt>.

关于IPSec ESP的信息见<http://www.ietf.org/rfc/rfc1825.txt>

X. 4. 1. 1 与ISO/IEC 27001相对应的行业例子

图A. 1显示电讯网络划分为3层设备和设施组：(1) 基础设施安全层，(2) 服务安全层，(3) 应用系统安全层。这就定义了在这一层可以发生的3种类型的活动，称为安全面。在每一层存在的3种安全面或活动是：(1) 管理安全面，(2) 控制/发信号安全面，(3) 最终用户安全面。为了确保每一安全层/面结合，更进一步的尺度可通过考虑安全机制而达到。

这个例子定义指南，支持ISO/IEC 18028-2安全层、安全面、安全度应用到ISMS的建立、实施和运行的ISO/IEC 27001模型。

X. 4. 1. 2 映射例子

下面提供两个例子。

[A.] 5. 1. 1 信息安全方针文件

控制措施

信息安全方针文件应获得管理者批准、发布并传达给所有员工和外部相关方。

网络安全：可适用 X 不可适用

安全层或资产：全部

安全面或活动：全部

尺度或机制：全部

基本原理：信息安全方针文件规定，方针必须陈述组织管理信息安全的方法。信息安全方针识别组织对每个技术安全尺度安排的优先顺序，并提供组织对每个资产和活动，管理信息安全的方法。

[A.] 10. 9. 2 在线交易

控制措施

在在线交易中的有关信息要加以保护，以防止不完全传输、错误路由、未授权的消息篡改、未授权的泄露、未授权的消息复制或重放。

网络安全：可适用 X 不可适用

安全层或资产：服务，基础设施，应用系统

安全面或活动：管理或运行，最终用户

尺度或机制：数据完整性，数据机密性，通信安全和访问控制

基本原理：为了保护在线交易中的有关信息，资产和活动要加以使用，以确定必要的控制措施(在10. 9. 2控制措施的情况)，和在什么地方需要采用。尺度指定实施和运行控制措施所需要的方法。例如，实施数据完整性尺度的IPSec AH，以防止服务层未授权的消息篡改，和实施数据机密性尺度的IPSec ESP，以防止服务层未授权的泄露。