第3章 信息安全管理体系

本章介绍建立信息安全管理体系的6个基本工作步骤，进而引入基本步骤中详细的工作流程、工作方式和工作内容，同时介绍信息安全管理体系认证的相关内容。

3.1 建立信息安全管理体系的工作步骤

不同的组织在建立与完善信息安全管理体系时，可根据自己的特点和具体的情况，采取不同的步骤和方法。但总体来说，建立信息安全管理体系一般要经过下列6个基本步骤：

(1) 信息安全管理体系的策划与准备。

(2) 信息安全管理体系文件的编制。

(3) 建立信息安全管理框架。

(4) 信息安全管理体系的运行。

(5) 信息安全管理体系的审核。

(6) 信息安全管理体系的管理评审。

3.2 信息安全管理体系的策划与准备

ISO/IEC 27001是建立和维持信息安全管理体系的标准，标准要求组织通过确定信息安全管理体系范围，制定信息安全方针，明确管理职责，以风险评估为基础选择控制目标与控制措施等一系列活动来建立信息安全管理体系。信息安全管理体系一旦建立，组织应按体系规定的要求进行运作，保持体系运行的有效性。信息安全管理体系应形成一定的文件，即组织应建立并保持文件化的信息安全管理体系，其中应阐述被保护的资产、组织风险管理方法、控制目标与控制措施、信息资产需要受保护的程度等内容。

组织内部成功实施信息安全管理体系的关键因素如下所示。

(1) 反映业务目标的安全方针、目标和活动。

(2) 与组织文化一致的、实施安全管理的方法。

(3) 来自管理层的有形支持与承诺。

(4) 对信息安全要求、风险评估和风险管理的良好理解。

(5) 向所有管理者及雇员推行信息安全意识。

(6) 向所有雇员和承包商分发有关信息安全方针和标准的导则。

(7) 提供适当的信息安全的培训与教育。

(8) 用于评价信息安全管理绩效及反馈改进建议、并有利于综合平衡的测量系统。

3.2.1 管理承诺

组织最高管理层应提供其承诺建立、实施、运行、监控、评审、维护和改进信息安全管理体系的证据,这是成功实施信息安全管理体系的重要保护,管理承诺如下所示。

(1) 建立信息安全方针。

(2) 建立信息安全目标和计划。

(3) 为信息安全确立角色和责任。

(4) 向组织传达信息安全目标和符合信息安全策略的重要性、组织的责任及持续改进的需要。

(5) 提供足够的资源以开发、实施、运行和维护信息安全管理体系。

(6) 确定可接受风险的水平。

(7) 进行信息安全管理体系的评审。

3.2.2 组织与人员建设

为在组织中顺利建立信息安全管理体系,需要建立有效的信息安全机构,对组织中的各类人员分配角色、明确权限、落实责任并予以沟通。

1. 成立信息安全委员会

信息安全委员会由组织的最高管理层及与信息安全管理有关的部门负责人、管理人员、技术人员组成,定期召开会议,就以下重要信息安全议题进行讨论并做出决策,为组织信息安全管理提供导向与支持。

(1) 评审和审批信息安全方针。

(2) 分配信息安全管理职责。

(3) 确认风险评估的结果。

(4) 对与信息安全管理有关的重大事项做出决策。

(5) 评审与监督信息安全事故。

(6) 审批与信息安全管理有关的其他重要事项。

2. 任命信息安全管理经理

组织最高管理者在管理层中指定一名信息安全管理经理,分管组织的信息安全事宜,具体有以下责任。

(1) 确定信息安全管理标准,建立、实施和维护信息安全管理体系。

(2) 负责组织的信息安全方针与安全策略的贯彻与落实。

(3) 向最高管理者提交信息安全管理体系绩效报告,以供评审信息安全管理体系提供证据。

(4) 就信息安全管理的有关问题与外部各方面进行联络。

3. 组建信息安全管理推进小组

在信息安全委员会的批准下,由信息安全管理经理组建信息安全管理推进小组并对其进行管理。小组成员要懂信息安全技术知识,有一定的信息安全管理技能,并且有较强的分析能力及文档编写能力,小组成员一般是企业各部门的骨干人员。

4. 保证有关人员的作用、职责和权限得到有效沟通

用适当的方式,如通过培训、制定并传达文件等方式,让每位员工明白自己的作用、职责与权限,以及与其他部门的关系,以保证全体员工各司其职,相互配合,有效地开展活动,为信息安全管理体系的建立做出贡献。

5. 组织机构的设立原则

(1) 合适的控制范围:例如,一般情况下,一个经理直接控制的下属管理人员不应超过10人。

(2) 合适的管理层次:例如,公司负责人与基层管理部门之间的管理层数应保持最低程度。

(3) 一个上级的原则。

(4) 责、权、利一致的原则。

(5) 既无重叠又无空白的原则。

(6) 执行部门与监督部门分离的原则。

(7) 信息安全部门有一定的独立性,不应成为生产部门的下属单位。

6. 信息安全管理体系组织结构设立及职责划分的注意事项

(1) 如果现有的组织结构合理,只需将信息安全标准的要求分配落实到现有的组织结构中即可;如果现有的组织结构不合理,则按上面所述组织机构的设定原则对组织结构进行调整。

(2) 应将组织内的部门设置及各部门的信息安全职责、权限及相互关系以文件的形式加以规定。

(3) 应将部门内岗位设置及各岗位的职责、权限和相互关系以文件的形式加以规定。

(4) 日常的信息安全监督检查工作应由专门的部门负责。

(5) 对于大型组织来说,可以设置专门的安全部,安全部设立首席安全执行官,首席安全执行官直接向组织最高管理层负责。

(6) 对于小型组织来说,可以把信息安全管理工作划归到信息部或其他相关部门。

3.2.3　编制工作计划

建立信息安全管理体系是一个复杂的系统工程,它的建立需要半年甚至更长的时间,包

括培训、风险评估、文件编写等大量工作。

为确保体系顺利建立,组织应进行统筹安排,即制定切实可行的工作计划,明确不同时间段的工作任务与目标及责任分工,控制工作进度,突出工作重点,例如以表 3-1 的形式安排总体计划。总体计划被批准后,可针对具体工作项目制定详细计划,例如文件编写计划。

在制定计划时,组织应考虑资源需求,例如人员需求、培训经费、办公设施、聘请咨询公司的费用等。如果寻求体系的第三方认证,还要考虑认证的费用。组织最高管理层应确保提供建立体系所必需的人力与财务资源。信息安全管理体系总体工作计划如表 3-1 所示。

表 3-1 信息安全管理体系总体工作计划

序号	阶段	项 目	负责部门/人	日期
1	准备阶段	(1) 领导决策 • 做出实施 ISMS 的决策 • 成立信息安全管理委员会 • 任命信息安全管理经理	最高管理者	
		(2) 建立信息安全组织机构,并设计方案 • 设立信息安全管理推进小组 • 拟定 ISMS 实施草稿,并由信息安全管理委员会讨论通过	信息安全管理委员会,信息安全管理经理	
		(3) 编制 ISMS 工作计划 • 详细实施计划 • 认证计划 • 培训计划	信息安全管理经理,信息安全管理推进小组	
		(4) 学习培训	信息安全管理经理,人事部	
2	初始状态评审	(5) 初始状态评审 • 了解组织概况、业务类别、企业文化等基本情况,收集适用于组织的法律、法规和其他与信息安全相关的文件和数据 • 评估信息安全风险,选择风险控制措施 • 评估现有信息安全控制措施的适用性 • 评价现行管理体系与 ISO/IEC 27001 的差距	信息安全管理经理,信息安全管理推进小组	
3	体系设计	(6) 确定 ISMS 方针和目标	最高管理者	
		(7) 编制 ISMS 管理方案	推进小组,组织内相关部门	
		(8) ISMS 责任分配及资源配备 • 必要时对组织结构进行调整 • 将各项 ISMS 活动责任分配落实到各职能部门,编制职能分配矩阵表 • 识别资源需求,配置必要的资源	最高管理者,信息安全管理经理	

续表

序号	阶段	项　　目	负责部门/人	日期
4	文件编制	(9) 文件的总体设计 • 确定文件清单，确定 ISMS 文件与 ISO/IEC 27001 标准条款的对照表 • 制定文件编写计划 • 编写指导性文件	信息安全管理经理，推进小组	
		(10) 编写 ISMS 管理手册 • 编写，讨论修改，审核，批准	最高管理者，各部门经理，信息安全管理经理，推进小组	
		(11) 程序文件编写、配套表格设计 • 编写，讨论修改，审核，批准	各部门经理，信息安全管理经理，推进小组	
		(12) 作业指导书编写，配套表格设计 • 编写，讨论修改，审核，批准	相关业务人员，各部门经理，推进小组	
5	实施运行	(13) ISMS 文件的学习	各部门经理，信息安全管理经理	
		(14) 试运行前的准备 • 检查资源配置到位情况 • 制备各类标签、标识用记录表格、表卡等 • 试运行前或试运行初最好把计量工作做好 • 宣传鼓动	信息安全管理经理，各部门经理	
		(15) 宣布试运行	最高管理者	
		(16) 贯彻实施、完善整改	各部门经理	
		(17) 内审员的培训	信息安全管理经理，人事部	
		(18) ISMS 内部审核	内部审核小组	
		(19) 管理评审	最高管理者	
6	审核认证	(20) 申请认证	信息安全管理经理	
		(21) 认证	各部门经理	

3.2.4　能力要求与教育培训

组织的管理体系通常是按照国际标准或国家标准的要求建立起来的，信息安全管理体系建立的依据是 ISO/IEC 27001 信息安全管理体系规范标准。为了强化组织信息安全的意识，明确信息安全管理体系的基本要求，进行信息安全管理体系标准的培训是十分必要和必需的，这也是组织搞好信息安全管理的关键因素之一。

培训工作要分层次、分阶段、循序渐进地进行，而且必须是全员培训。分层次培训是指对不同层次的人员开展有针对性的培训，包括对决策层、管理层、审核验证人员及操作执行人员的培训，而且培训的内容也各有侧重；分阶段是指在信息安全管理体系的建立、实施与保持的不同阶段，培训工作要有计划地安排实施，如在体系建立初期对管理层的宣传贯彻培训、在风险评估前对评估人员所进行的风险评估方法的培训等；培训可以采用外部与内部相结合的方式。

对从事信息安全管理工作的人员，应具有相应的能力要求，在教育经历方面，组织应对其能力做出适当的规定。该规定有以下要点。

(1) 组织应对人员的培训、意识和能力的要求建立文件化的程序。

(2) 人员能力的基本要求。

① 适当的教育程度,通常是指为从事不同的、对信息安全有影响的工作所需的最低学历教育。

② 适当的培训,通常是指为从事某一岗位工作之前需接受的培训,例如对内审员的培训要求。

③ 适当的经历,通常是指为了更有效地完成工作任务所需的工作经验和专业技能。

(3) 保证人员能力的措施。

① 根据任职条件、法律法规要求、组织发展的需要,识别人员能力的需求。

② 提供培训或采取其他措施满足对人员的能力需求。

③ 评价所采取措施的有效性,评价方式有考核、业绩评定、管理人员评价、观察等。

(4) 培训的实施。

① 确定培训需求。

② 制定培训计划。

③ 实施培训。

④ 培训后考核。

⑤ 培训结果的处理。

⑥ 记录保存。

(5) 培训的内容。

① 信息安全知识、安全技能培训,实际操作技能考核等。

② 向所有管理者及雇员进行安全意识的培训。

③ 有关信息安全的法律、法规、制度的培训。

④ 向所有雇员和承包商培训有关信息安全政策和标准。

⑤ 书面的安全方针、策略、规程、作业指导书。

(6) 培训的方式。

① 内部培训、外部培训、实习、自学考试、学术交流。

② 采用不同媒体宣传信息安全,如公司邮件、网页。

③ 安全规则的可视化执行。

④ 模拟安全事故以改善安全规程。

⑤ 员工签订保密协议,了解安全需求。

3.3 信息安全管理体系的设计与建立

3.3.1 编写信息安全管理体系文件

1. ISMS 文件

信息安全管理体系需要编写各种层次的信息安全体系文件,这是建立信息安全管理体系的重要基础性工作。文件应包括管理决策的记录,以确保控制措施可以追溯到管理决策

和方针。重要的是要能够展示从选择的控制措施回溯到风险评估和风险处置过程因果的关系，最终回溯到 ISMS 方针和目标。ISMS 文件应包括如下。

(1) 文件化的 ISMS 方针与策略。

(2) ISMS 范围。

(3) ISMS 的支持性程序和控制。

(4) 风险评估方法的描述。

(5) 风险评估报告。

(6) 风险处置计划。

(7) ISMS 的控制目标与控制措施。

(8) ISMS 管理和具体操作的过程。

(9) 标准中所要求的记录。

(10) 信息系统安全相关职责描述和相关的活动事项。

(11) 适用性声明。

2. 文件的作用

从总体来看，文件的作用如下。

1) 阐述声明的作用

信息安全管理体系文件是客观地描述信息安全体系的法规性文件，为组织的全体人员了解信息安全管理体系创造了必要的条件。组织向客户或认证机构提供《信息安全管理手册》，起到了对外声明的作用。

2) 规定、指导的作用

信息安全管理体系文件规定了组织员工应该做什么、不应该做什么的行为准则，以及如何做的指导性意见，对员工的信息安全行为起到了规范、指导作用。

3) 记录、证实的作用

信息安全管理记录具有记录和证实信息安全管理体系运行有效的作用。其他文件则具有证实信息安全管理体系客观存在和运行适用性的作用。

从评价和改进信息安全管理体系的角度来看，文件具有以下 3 种具体作用。

(1) 评价信息安全管理体系的作用。

(2) 保障信息安全改进的作用。

(3) 平衡培训要求的作用。

3. 文件的层次

ISO/IEC 27001 关于文件的描述中，没有强求将其形成专门的手册形式，没有刻意要求组织将体系文件分成若干层次，但依据成功经验，在具体实施中，为便于运作并具有操作性，建议把 ISMS 管理文件分成以下几个层次，即适用性声明、管理手册、程序文件、作业文件指导书、记录。

1) 适用性声明

适用性声明是组织为满足安全需要而选择的控制目标和控制方式的评论性文件。在适用性声明文件中，应明确列出组织根据信息安全要求(包括风险评估、法律法规、业务三方

面)从 ISO/IEC 27001 中选择的控制目标与控制方式,并说明选择与不选择的理由;如果有额外的控制目标与控制方式也需要一并说明。

2) ISMS 管理手册

ISMS 管理手册是阐明组织的 ISMS 方针,并描述其 ISMS 的文件。ISMS 管理手册至少包括以下内容。

(1) 信息安全方针的阐述。

(2) 信息安全管理体系范围。

(3) 信息安全策略的描述。

(4) 控制目标与控制方式的描述。

(5) 程序及其引用。

(6) 关于手册的评审、修改与控制的规定。

3) 程序文件

程序是为进行某项活动所规定的途径或方法。信息安全管理程序包括两部分:一部分是实施控制目标与控制方式的安全控制程序,另一部分是为覆盖信息安全管理体系的管理与运作的程序。程序文件应描述安全控制或管理的责任及相关活动,是信息安全政策的支持性文件,是有效实施信息安全政策、控制目标与控制方式的具体措施。

4) 作业指导书

作业指导书是程序文件的支持性文件,用以描述具体的岗位和在工作现场如何完成某项工作任务的具体做法,包括作业指导书、规范、指南、图样、报告、表格等,例如设备维护规程或维护手册。作业指导性文件可以被程序文件所引用,对程序文件中整个程序或某些条款进行补充、细化。

5) 记录

记录作为信息安全管理体系运行结果的证据,是一种特殊的文件。组织在编写信息安全方针手册、程序文件及作业指导文件时,应根据安全控制与管理要求确定组织所需要的信息安全记录,组织可以通过利用现有的记录、修订现有的记录和增加新的记录三种方式来获得。记录可以是书面记录,也可以是电子媒体记录,每一种记录应进行标识,记录应有可追溯性。记录内容与格式应该符合组织业务运作的实际并反映活动结果,且方便记录人的使用。

4. 文件的编写

由于 ISMS 文件是信息安全管理体系的基础,组织应当建立恰当的程序对 ISMS 进行管理,在文件生命周期的各个阶段,如编写、审核、批准、发布、使用、保管、回收、销毁等,都需要有适宜的控制措施。

1) 文件编写的原则

(1) ISMS 文件层次清楚、结构合理。

(2) ISMS 文件应保持其相对的稳定性和连续性。

(3) ISMS 文件不是信息安全管理现状的简单写实,应随着 ISMS 的不断改进而完善。

(4) 编写 ISMS 文件时,要继承以往的有效经验与做法。

(5) 应发动各部门有实践经验的人员集思广益,共同参与。

(6) ISMS 文件应当可以作为组织 ISMS 有效运行并得到保持的客观证据，向相关方、第三方证实组织 ISMS 的运行情况。

(7) 文件的编制和形式应考虑组织的业务特点、规模、管理经验等。文件的详略程度应与人员的素质、技能和培训等因素相适宜。

2) 编写前的准备

(1) 指定编写主管机构，指导和协调文件的编写工作。

(2) 收集整理组织现有文件。

(3) 对编写人员进行培训，使之明确编写的要求、方法、原则和注意事项。

(4) 为了使 ISMS 文件统一协调，达到规范化和标准化的要求，应编写指导性文件，就文件的要求、内容、体例和格式做出规定。

3) 编写的策划与组织

确定要编写的文件目录，制定编写计划，落实编写、审核、批准人员，拟定编写进度。

5. 文件的管理

1) 文件控制

组织必须对各种文件进行严格的管理，结合业务和规模的变化，对文档进行有规律、周期性的回顾和修正，ISMS 要求的文件应得到保护和控制，主要控制措施如下。

(1) 文件发布须得到批准，以确保文件的充分性。

(2) 必要时对文件进行审批与更新，并再次批准。

(3) 确保文件的更改和现行修订状态得到识别。

(4) 确保在使用处可获得适用文件的有关版本。

(5) 确保文件保持清晰、易于识别。

(6) 确保文件可以为需要者所获得，并根据适用于他们类别的程序进行转移、存储和最终的销毁。

(7) 确保外来文件得到识别，并控制其分发。

(8) 确保在控制状态下进行文件的发放。

(9) 防止作废文件的非预期使用。

(10) 若因任何原因而保留作废文件时，对这些文件进行适当的标识。

当某些文件不再适合组织的信息安全管理策略需要时，必须将其废弃。但值得注意的是，某些文档虽然对组织来说可能已经过时，但由于法律或知识产权方面的原因，组织可以将相应文档确认后保留。

2) 记录控制

在实施 ISMS 的过程中，需要对发生的各种与信息安全相关的事件进行全面的记录，从而提供符合要求和信息安全管理体系的有效运行的证据。记录应该做到以下要求。

(1) 安全事件记录必须清晰，明确记录每个相关人员当时的活动。无论是书面的还是电子版的安全事件记录，都必须适当保存并进行维护，保证记录在受到破坏、损坏或丢失时容易挽救。

(2) 记录应保持清晰，易于识别和检索。

(3) 应编制文件化的程序，以规定记录的储存、保护、检索、保存期限和处置所需的控制。

(4) 应保留概要的过程绩效记录和所有与信息安全管理体系有关的安全事故发生的记录。

3.3.2 建立信息安全管理框架

组织建立 ISMS,首先要建立合理的信息安全管理框架,要从整体和全局的视角,从信息系统的所有层面进行整体信息安全建设,并从系统本身出发,通过建立资产清单,进行风险分析、需求分析和选择信息安全控制措施等步骤,建立信息安全管理体系并提出安全解决方案。

信息安全管理框架的建立必须按规范的程序进行。组织首先应根据自身的业务性质、组织特征、资产状况和技术条件定义 ISMS 的总体方针和范围,然后在信息安全风险评估的基础上进行风险分析,并确定信息安全风险管理制度,选择控制目标,准备适用性声明。

1. 定义信息安全策略

信息安全策略(Information Security Policy)从本质上说是描述组织具有哪些重要信息资产,并说明这些信息资产如何被保护的一个计划,其目的就是对组织中成员阐明如何使用组织中的信息系统资源,如何处理敏感信息,如何采用安全技术产品,在使用信息时应当承担的责任,详细描述对员工的安全意识和技能要求,列出被组织禁止的行为。

信息安全策略可以分为两个层次,一个是信息安全方针,另一个是具体的信息安全策略。

所谓信息安全方针就是组织的信息安全委员会或管理部门制定的高层文件,用于指导组织如何对资产(包括敏感性信息)进行管理、保护和分配的规则进行指示。信息安全方针必须要在 ISMS 实施的前期制定出来,阐明最高管理层的承诺,提出组织管理信息安全的方法,由管理层批准,指导 ISMS 的所有实施工作。

除了总的信息安全方针,组织还要制定具体的信息安全策略。信息安全策略是在信息安全方针的基础上,根据风险评估的结果,为降低信息安全风险,保证控制措施的有效执行而制定的具体明确的信息安全实施规则。

信息安全策略的制定要在风险评估工作完成后,在对组织的安全现状有明确了解的基础上,有针对性地编写,用于指导风险的管理与安全控制措施的选择。

根据组织业务特征、组织结构、地理位置、资产和技术等实际情况确定 ISMS 方针,ISMS 方针如下。

(1) 包括建立目标的框架,并建立信息安全活动的总方向和总原则。

(2) 考虑业务和法律法规要求,以及合同安全义务。

(3) 根据组织战略性的风险管理框架,建立和保持 ISMS。

(4) 定义风险评估的结构和建立风险评价的准则。

(5) 经过管理层的批准。

2. 定义 ISMS 的范围

根据组织业务特征、组织结构、地理位置、资产、技术等实际情况来确定 ISMS 范围。

ISMS 的范围可以根据整个组织或者组织的一部分进行定义,包括相关资产、系统、应

用、服务、网络和用于各种业务过程中的技术、存储以及通信的信息等，ISMS 范围可以包括如下几项。

（1）组织所有的信息系统。

（2）组织的部分信息系统。

（3）特定的信息系统。

3. 实施信息安全风险评估

风险评估是进行安全管理必须要做的最基本的一步，它为 ISMS 的控制目标与控制措施的选择提供依据，也是对安全控制的效果进行测量评价的主要方法。

首先，组织应当确定风险评估方法。

（1）确定适用于 ISMS、已识别的业务信息安全和法律法规要求的风险评估方法。

（2）确定风险接受准则，识别风险的可接受水平。

（3）风险评估方法的选择应确保可以产生可比较的、可重复的结果。

其次，组织利用已确定的风险评估方法识别风险。

（1）识别 ISMS 范围内的资产及资产所有者。

（2）识别资产的威胁。

（3）识别可能被威胁利用的脆弱点。

（4）识别资产保密性、完整性、可用性损失的影响。

最后，组织进行分析并评价风险：

（1）评估安全失效可能导致的组织业务影响，考虑因资产保密性、完整性、可用性的损失而导致的后果。

（2）根据资产的主要威胁、脆弱性、有关的影响以及已经实施的安全控制，评估安全措施失效发生的现实可能性。

（3）估计风险的等级。

（4）根据已建立的准则，判断风险是否可接受或需要处理。

4. 实施信息安全风险管理

该阶段主要是根据风险评估的结果进行相应的风险管理。信息安全风险管理主要包括以下几种措施。

（1）接受风险。在确定满足组织策略和风险接受准则的前提下，有意识地、客观地接受风险。

（2）规避风险。有些风险很容易避免，通过消除风险的原因和后果来规避风险，如在识别出风险后放弃系统某项功能或关闭系统，或通过采用不同的技术、更改操作流程、采用简单的技术措施等。

（3）转移风险。通过使用其他措施来补偿损失，从而转移风险，将相关业务风险转嫁给他方，如保险公司、供方等。该措施一般用于低概率、而一旦风险发生时会对组织产生重大影响的风险。

（4）降低风险。实施适当的控制措施，把风险降低到一个可接受的水平。

5. 确定控制目标和选择控制措施

确定控制目标、选择控制措施,应考虑接受风险的准则以及法律法规和合同要求,以满足风险评估和风险处置过程所识别的要求。

从 ISO/IEC 27001 标准附录 A 中选择的控制目标和控制方式应作为这一过程的一部分,并满足这些要求。附录 A 的控制目标和控制方式并不详尽,可以选择其他的控制目标和控制方式。

控制目标的确定和控制措施的选择原则是成本不超过风险所造成的损失。由于信息安全管理是动态的系统工程,组织应实时对选择的控制目标和控制措施加以校验和调整,使组织的信息资产得到有效、经济、合理的保护。

6. 准备信息安全适用性声明

适用性声明(Statement of Application,SoA)是适合组织需要的控制目标和控制措施的评论,需要提交给管理者、职员以及具有访问权限的第三方认证机构。适用性声明应包括以下两方面内容。

(1) 组织选择的控制目标和控制措施,以及选择的原因。

(2) 附录 A 中控制目标和控制措施的删减,以及删减的合理性。

适用性声明提供了一个风险处置决策的总结。通过判断删减的合理性,再次确认控制目标没有被无意识地遗漏。SoA 的准备,一方面是为了向组织内的人员声明面对信息安全风险的态度,另一方面则是为了向外界表明组织的态度和作为,表明组织已经全面、系统地审视了组织的信息安全系统,并将所有应该得到控制的风险控制在能够被接受的水平内。

3.4 信息安全管理体系的实施与运行

信息安全管理体系文件编制完成后,组织应按照文件的控制要求进行审核与批准并发布实施,至此,信息安全管理体系将进入运行阶段。体系文件在试运行中必然会出现一些问题,全体员工应将实践中出现的问题和改进意见如实反馈给有关部门,以便采取纠正措施,将体系试运行中暴露出的问题,如体系设计不周、项目不全等进行协调、改进。

3.4.1 信息安全管理体系的试运行

在信息安全管理体系试运行过程中,在重点注意以下问题。

1. 领导动员,以身作则

最高管理层的支持是 ISMS 有效运行的重要基础,ISMS 试运行前应该召开全体员工大会,由最高管理层作宣传动员,并承诺对组织中实施信息安全体系的支持,明确提出对各级员工的信息安全职责要求,并以身作则,带头执行 ISMS 的有关规章制度。

2. 有针对性地宣传贯彻 ISMS 文件

ISMS 文件的培训工作是体系运行的首要任务,培训工作的质量直接影响体系运行的

结果。组织应该按照培训工作计划的安排并按照培训程序的要求对全体员工实施各种层次的培训。培训包括信息安全意识、信息安全知识与技能和 ISMS 运行程序的培训。

3. 完善信息反馈与信息安全协调机制

体系运行过程中必然会出现一些问题，全体员工应当将实践中出现的问题，如体系设计不周、项目不全等问题进行反馈。信息安全管理体系的运行涉及组织体系范围的各个部门，在运行过程中，各项活动往往不可避免地发生偏离标准的现象，因此，组织应按照严密、协调、高效、精简、统一的原则，建立信息反馈与信息安全协调机制，对异常信息加以反馈和处理，对出现的问题加以改进，完善并保证体系的持续正常运行。

4. 加强 ISMS 运行信息的管理

加强有关体系运行信息的管理，不仅是信息安全管理体系本身的需要，也是保证试运行成功的关键。所有与信息安全管理体系活动有关的人员都应按照体系文件的要求，做好信息安全的信息收集、分析、传递、反馈、处理与归档工作。

3.4.2　实施和运行 ISMS 工作

实施和运行信息安全管理体系工作，主要包括以下内容。

(1) 阐明风险处理计划。为管理信息安全风险，识别适当的管理措施、资源、职责和优先顺序。

(2) 实施风险处理计划。为达到已识别的控制目标，应考虑资金需求以及角色和职责分配。

(3) 实施选择的控制措施。实施风险分析之后选择的控制措施，以满足控制目标的需要。

(4) 评价控制措施的有效性。确定如何测量所选择的控制措施或控制措施集的有效性，并指明如何用来评估控制措施的有效性，以产生可比较的和可再现的结果。

(5) 实施培训和意识教育计划。组织应通过合适的方式，如提供能力培训(必要时聘用有能力的人员)，以确保有关 ISMS 职责的人员具有相应的执行能力。

(6) 管理 ISMS 的运行。

(7) 管理 ISMS 资源。

(8) 实施能够迅速检测安全事态和响应安全事件的程序和其他控制措施。

可执行的风险处置计划，必然要包括以下内容。

(1) 计划的任务内容。

(2) 任务展开与执行需要的职务、权限、责任的指派。

(3) 处置计划中的技术方案与资金预算。

(4) 资源提供，包括充足数量的具备实施技术方案相应能力的人员、软件或硬件产品与工具、必要的设备等。

针对风险评估的结果，需要进行处置的风险往往不止一项，风险处置计划当然也就不止一项。对于已经识别的不可接受的风险，风险处置的目的是要将风险水平降低到可接受水平以下；出于其他业务经营的需要，组织也可能制定风险处置计划，以改变原来的可能性或后果。

针对组织的信息安全管理现状和“适用性声明”的内容,风险处置计划中的任务内容可能包括如下内容。

(1) 制定管理信息安全相关活动的规程。

(2) 对基础设施和物理安全系统进行安全加固或技术更新。

(3) 对信息系统的硬件或软件实施安全加固或技术更新。

(4) 对人员进行信息安全相关知识、技能、工具使用等项目的培训,对人员进行有关风险后果的意识教育。

(5) 就信息安全管理规程的要求对人员进行培训,并推行信息安全规程。

(6) 与第三方服务提供方就信息安全管理事项进行沟通和协商等。

风险处置计划的实施应在受控条件下进行,做到责任分工明确。记录计划的实施和实施结果,这些数据将可作为对信息安全管理绩效和风险处置计划实施后风险的变化进行评估的输入。

3.5 信息安全管理体系的审核

3.5.1 审核概述

1. 审核的概念

体系审核是组织为获得审核证据并对其进行客观的评价,以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程。

ISMS 审核是 ISMS 审核人员为了获得审核证据,而独立地、客观地、正式地和有计划地评估被评审组织的 ISMS,确定其对 ISMS“审核准则”符合程度所进行的一系列活动。审核的结果产生书面的“审核报告”。

ISMS 审核包括管理和技术两方面的审核,管理性审核主要是定期检查有关信息安全方针、策略与规程是否被正确有效地实施;技术性审核是指定期检查组织的信息系统符合信息安全实施标准的情况,技术性的审核需要信息安全技术人员的支持,必要时会使用系统审核工具。

2. 审核的目的

组织应建立并保持审核方案和规程,定期开展信息安全管理体系的审核,以保证它的文件化过程,信息安全活动以及实施记录能够满足 ISO/IEC 27001 的标准要求和声明的范围,检查信息安全实施过程符合组织的方针、目标和策划要求,并向管理者提供审核结果,为管理者的信息安全决策提供支持。

ISMS 审核的主要目的如下所示。

(1) 检查 ISO/IEC 27001 的实施程度与标准的符合性情况。

(2) 检查满足组织安全策略与安全目标的有效性和适用性。

(3) 识别安全漏洞与弱点。

(4) 为管理者提供信息安全控制目标的实现状况,使管理者了解信息安全问题。

（5）指出存在的重大的控制弱点，证实存在的风险。

（6）建议管理者采用正确的校正行动，为管理者的决策提供有效支持。

（7）满足法律、法规与合同的需要。

（8）提供改善 ISMS 的机会。

3．审核的分类

ISMS 审核可分为两种：一是内部信息安全管理体系审核，也称第一方审核，是组织的自我审核；二是外部信息安全管理体系审核，也称第二方、第三方审核。第二方审核是客户对组织的审核，第三方审核是第三方性质的认证机构对申请认证组织的审核。这两种审核在审核目的、审核方组成、审核依据、审核人员及审核后的处理等方面均不同。表 3-2 列出了它们的区别。

表 3-2　内、外部 ISMS 体系审核比较表

项　　目	内部 ISMS 审核	外部 ISMS 审核
目的	审核 ISMS 的符合性、有效性，采取纠正措施，使体系正常运行和持续改进	第二方：选择合适的合作伙伴；证实合作方持续满足规定要求；促进合作方改进信息安全管理体系。 第三方：导致认证、注册
审核方	第一方	第二方、第三方
依据	ISO/IEC 27001 标准 ISMS 文件 适用于组织的有关 ISMS 法规及其他要求	第二方：合同，ISMS 文件；适用于被审核方的 ISMS 法规及其他要求。 第三方：ISO/IEC 27001 标准；ISMS 文件；适用于被审核方的 ISMS 法规及其他要求
审核方案	集中式/滚动式审核	集中式审核
审核员	有资格的内审员，也可聘请外部审核员	第二方：自己或外聘审核员。 第三方：注册审核员
文件审查	根据需要安排	必须进行
审核报告	提交不符合报告和采取纠正措施的建议	只提交不符合报告
纠正措施	重视纠正措施。对纠正措施计划可提方向性意见供参考；对纠正措施完成情况不仅要跟踪验证，还要分析研究其有效性	对纠正措施不能做咨询服务，对纠正措施计划的实施要跟踪验证
监督检查	无此内容	认证或认可后，每年至少进行一次监督检查

4．审核的步骤

ISMS 审核的主要步骤如下。

（1）审核计划。

(2) 审核准备。

(3) 现场审核。

(4) 编写审核报告。

(5) 纠正措施的跟踪。

(6) 全面审核报告的编写和纠正措施计划完成情况的汇总分析。

3.5.2 ISMS 内部审核

1. 内部审核基本内容

组织应按策划的时间间隔进行 ISMS 内部审核,以确定组织 ISMS 的控制目标、控制措施、过程和程序是否达到下述要求。

(1) 符合标准及相关法律法规的要求。

(2) 符合已识别的信息安全要求。

(3) 得到有效的实施和保持。

(4) 按期望运行。

应策划审核方案,考虑被审核区域的审核过程和区域的状况及重要性,以及审核的结果。应规定审核准则、范围、频次和方法。审核员的选择和审核的实施应保证审核过程的客观和公正。审核员不能审核自己的工作。

应建立文件化的程序,以规定策划和实施审核、报告结果和保持记录的职责和要求。

被审核区域的负责人应确保立即采取措施以消除发现的不符合项及其原因。跟踪活动应包括所采取措施的验证以及验证结果的报告。

2. 内部审核流程

1) 内部审核策划

内部审核周期及范围:正常情况下,信息安全管理体系的内部审核至少每年组织一次,两次时间间隔不得超过 12 个月。出现下列情况时可由管理者决定是否增加信息安全管理体系的内部审核次数。

(1) 组织结构和职能分工出现重大变化。

(2) 业务内容出现重大变化。

(3) 信息安全管理体系出现重大变化。

(4) 采用标准、适用法律或验证方法出现重大变化。

(5) 出现重大客户投诉或信息安全事故。

(6) 其他需要增加内审的情形。

信息安全管理体系审核对象为组织信息安全管理体系所涉及的部门和活动。审核范围可以是对组织进行整体审核,也可以按部门或过程进行局部审核。正常情况下,管理体系所涉及的所有部门和过程每年至少应覆盖一次。其中各部门或各过程的审核频次还应取决于其现状和重要程度,并考虑以往审核的结果。计划外的追加审核由管理者根据实际情况确定。

2）内部审核组织

（1）由管理者负责组织内审小组，并填写《内审组长、内审员任命书》。

（2）内部审核员通常要求由接受过信息安全管理体系内部审核培训并取得资格证书的人员组成；内审员应与被审核的活动无直接责任；内审员不应审核自己的工作，以保证审核的独立性；内部审核员应在组织内各部门挑选并经公司任命。

（3）内审组长应由管理者从内审员中指定，管理者可以自己担任审核组长。

3）内部审核计划

（1）内审组长负责组织制定和提出《内部审核计划》。

（2）《内部审核计划》应包含审核目的、审核范围、审核时间和进度安排、审核小组成员、审核的注意事宜等；审核时间的安排需要和被审核部门事先协调。

（3）《内部审核计划》由管理者审批后实施；管理者自己担任内审组长的情况下，需要组织内审小组其他成员对计划进行审核。

4）内部审核准备

（1）各审核员应准备好并熟悉本次审核所依据的文件，如标准、信息安全管理手册、有关程序文件、合同、法律法规、客户及相关方要求等。

（2）内审小组成员根据分工，编制《内审检查表》，并报内审组长批准。

5）内部审核实施

内部审核实施可划分为首次会议、现场审核和末次会议三个阶段进行。

由内审组长召开首次会议，参加的人员由内审员及被审核部门负责人组成。在会议上，内审组长将：

（1）介绍内审小组成员，审核目的、范围。

（2）介绍审核方法、依据和程序。

（3）提出审核要求，确认审核日程安排等。

（4）公布末次会议日期、时间、会议内容及参加人员。

（5）介绍审核计划中需说明的其他问题。

现场审核包括下述内容。

（1）现场审核时，内审员根据《内审检查表》逐项进行审核，通过观察、提问、查阅文件和记录、抽样、问题追踪等方法，以验证审核情况与体系的符合性。

（2）内审员应如实记录审核的情况，对发现的不符合项应详细记录并由被审核部门负责人或直接责任人确认，以保证不符合项已经得到被审核部门的理解，以便于纠正和预防。

（3）现场审核结束后，内审组长召开内审小组成员会议，听取内审员的审核情况汇报，复核发现的不符合项，编写《不符合项报告及纠正报告单》。

（4）内审组长应与受审核部门领导进行沟通，提出《不符合项报告及纠正报告单》，由被审核部门签字确认，并责成相关部门按要求制定纠正及预防措施，并填写在《不符合项报告及纠正报告单》上。

末次会议包括以下内容。

（1）末次会议由内审组长主持，由内审小组成员、受审核方负责人、不符合项相关人员参加。

（2）由内审小组通报审核结果，内容可包括：报告审核情况；通报不符合项及其严重程

度；提出制定纠正措施、改进对策的限期；本次审核结论。

6）内审报告

完成信息安全管理体系内审后，由内审组长起草编写审核报告，审核报告内容需包括：

(1) 审核目的、审核范围、审核依据和审核时间。

(2) 内部审核组成员及其分工。

(3) 被审核的部门。

(4) 内部审核情况综述。

(5) 不符合项的综合分析。

(6) 对被审部门的评价、审核结论。

(7) 存在问题的分析及管理体系改进措施的建议。

《内审报告》经管理者批准后，打印或以电子文档的方式分发给被审核部门。《内审报告》由内审小组负责整理归档。

7）纠正不符合项

《不符合项报告及纠正报告单》由内审小组统计后分发到各责任部门，由责任部门分析不符合原因，制定纠正措施，经内审组长确认后，由责任部门组织实施。

8）跟踪和验证

(1) 审核小组在限定时间内对纠正措施的实施情况进行复审，以确认不符合项的纠正情况并验证其有效性。

(2) 责任部门已完成纠正措施后，通知内审员验证其完成情况和有效性，并由内审员在《不符合项报告及纠正报告单》上签名认可。

(3) 不符合项经复审仍不符合的项目，其部门负责人应说明原因并考虑是否需要重新制定纠正预防措施。

(4) 如在规定的日期内不能完成纠正的，内审员应检查不能完成的原因，无正当理由的应报管理者批准后，重新开出《不符合项报告及纠正报告单》并且必须在规定的日期内完成。

(5) 内部审核实施和验证情况由内审组长向管理者报告。

(6) 审核记录归档。

本程序所涉及的所有记录(内部审核计划、内审检查表、内审报告等)由内审小组按《记录控制程序》统一归档保存。

3. 实施策略

(1) 管理者负责成立内审小组，并任命内审组长，发布《内审组长、内审员任命书》。

(2) 内审组长负责组织编写并审核批准《内部审核计划》。

(3) 各内审员根据分工编写《内审检查表》。

(4) 由内审组长召开首次会议，并填写首次会议的《会议签到记录表》。

(5) 各内审员根据计划进行内审，发现不符合项，填写《不符合项报告及纠正报告单》，跟踪不符合项的解决。

(6) 由内审组长召开末次会议，并填写末次会议的《会议签到记录表》。

(7) 内审结束后，内审组长负责编写《内审报告》。

3.6　信息安全管理体系管理评审

1. 管理评审的定义

管理评审主要是指组织的最高管理者按规定的时间间隔对信息安全管理体系进行评审，以确保体系的持续适宜性、充分性和有效性。管理评审过程应确保收集到必要的信息，以供管理者进行评价，管理评审应形成文件。

管理评审应根据信息安全管理体系审核的结果、环境的变化和对持续改进的承诺，指出可能需要修改的信息安全管理体系方针、策略、目标和其他要素。

管理评审总目标是检查信息安全管理体系的有效性，至少每年一次，以识别需要的改进和采取的行动。在确定目前的安全状态是否令人满意的同时，应注意技术的变化和业务需求的变化及新威胁和脆弱点的发生，以预测信息安全管理体系未来的变化，并确保其在未来持续有效。

管理层应按策划的时间间隔评审组织的信息安全管理体系，以确保其持续的适宜性、充分性和有效性。评审应包括评价信息安全管理体系改进的机会和变更的需要，包括安全方针和安全目标。评审的结果应清楚地文件化，应保持管理评审的记录。

2. 职责与权限

(1) 组织最高管理者。主持召开管理评审大会，批准《管理评审报告》。

(2) 管理者。批准《管理评审计划》，组织召开管理评审会，组织撰写《管理评审报告》。

(3) 主管体系建设部门。制定《管理评审计划》，负责搜集并提供管理评审资料，负责对评审后的纠正，对预防措施进行跟踪和验证。

(4) 各部门。准备、提供与本部门工作相关的评审所需的资料，负责实施管理评审中提出的相关的纠正及预防措施。

3. 评审输入

管理评审的输入应包括以下几个方面的信息。

(1) 信息安全管理体系审核和评审的结果。

(2) 相关方的反馈。

(3) 可以用于组织改进其信息安全管理体系绩效和有效性的技术、产品或程序。

(4) 预防和纠正措施的状况。

(5) 以往风险评估没有足够强调的威胁或脆弱性。

(6) 以往管理评审的跟踪措施。

(7) 任何可能影响信息安全管理体系的变更。

(8) 改进的建议。

4. 评审输出

管理评审的输出应包括与以下几个方面有关的任何决定和措施。

(1) 对信息安全管理体系有效性的改进。

(2) 风险评估和风险处置计划的更新。

(3) 修改影响信息安全的程序,必要时,回应内部或外部可能影响信息安全管理体系的事件,包括以下的变更。

① 业务要求。

② 安全要求。

③ 业务过程影响现存业务的要求。

④ 法规或法律环境。

⑤ 合同义务。

⑥ 风险的等级和/或可接受风险的水平。

(4) 资源需求。

(5) 如何测量控制措施有效性的改进。

5. 制定年度管理评审计划

组织主管部门根据信息安全管理体系的运营情况,根据《信息安全管理手册》以及 ISO/IEC 27001 的标准要求,于每年年初制定《年度管理评审计划》。管理评审计划由管理者审批后方可生效。

管理评审计划的主要内容包括:审核目的、审核范围、审核准则、审核组的组建、审核员的资质、审核的时间、参与评审的部门等要求。

管理评审一般每年进行一次,一般在同一年度最后一次内部审核完成后进行,也可根据需要安排。当出现下列情况之一时可适当增加管理评审频次。

(1) 组织机构、服务范围、资源配置发生重大变化。

(2) 发生重大 IT 服务事故/安全事故或客户关于 IT 服务/信息安全有严重投诉或投诉连续发生。

(3) 当法律、法规、标准及其他要求有变化。

(4) 市场需求发生重大变化。

(5) 即将进行第二、三方审核。

(6) 审核中发现严重不符合项。

管理评审实施计划由主管体系建设部门组织制定。主管体系建设的部门于每次管理评审前一个月编制《管理评审计划》,报管理者审批。计划主要内容如下。

(1) 评审时间。

(2) 评审目的。

(3) 评审依据。

(4) 评审内容。

(5) 评审范围及评审重点。

(6) 参加评审部门及人员。

(7) 各部门应该准备的资料以及提交时间。

6. 资料准备

预定评审前一周，主管体系建设的部门组织、指导、督促各部门完成本部门应该提交的资料，以书面形式向管理者汇报。管理者认为资料准备不全，信息不够充分的，主管体系建设的部门组织相关责任部门按照管理者的要求进一步补充完善。

7. 管理评审会议

管理评审会议召开前 2～7 天，会议组织者应向与会人员以书面或邮件形式发送《管理评审会议通知》，并整理与会人员的反馈，以确定与会人员的实际人数。

管理者主持管理评审会议，各部门负责人和有关人员对评审输入做出评价，对于发现的不符合项或潜在的不符合项提出纠正和预防措施，确定责任人和整改时间。

管理者对所涉及的评审内容做出结论，包括进一步调查、验证等。

管理评审采取什么方式进行由管理者请示最高管理者后决定，一般默认情况下以会议形式进行。

管理评审会议应指定专人做会议记录。

8. 管理评审报告

管理评审大会结束后，由体系主管部门根据管理评审输出的要求和管理评审大会的会议记录进行总结，在管理者的指导下撰写《管理评审报告》，经管理者审核、批准后，发至相关部门并由主管体系建设的部门负责监控执行。

如果评审结果引起文件更改，应执行《文件控制程序》。

管理评审产生的相关的记录应由主管体系建设的部门按《记录控制程序》保管，包括《管理评审计划》、评审前各部门准备的评审资料、评审会议记录及《管理评审报告》等。

9. 相关支持性文件和记录

(1)《文件控制程序》。
(2)《记录控制程序》。
(3)《内部审核程序》。
(4)《管理评审计划》。
(5)《管理评审会议通知》。
(6)《管理评审报告》。
(7)《管理评审会议记录》。
(8)《年度管理评审计划》。

10. 管理评审的后续工作

管理评审的结果应予以记录并保存，如管理评审计划、各种输入报告、管理评审报告、纠正措施及其验证报告等。

信息安全管理部门的负责人员还要组织有关部门对管理评审中的纠正措施进行跟踪验证，验证的结果应记录并上报最高管理层及有关人员。

3.7 信息安全管理体系的改进与保持

3.7.1 持续改进

组织应通过应用信息安全策略、安全目标、审核结果、监视事件的分析、纠正预防措施和管理评审,持续改进 ISMS 的有效性。

组织应定期进行:

(1) 实施 ISMS 已识别的改进;

(2) 采取适当的纠正和预防措施,总结从其他组织或组织自身的信息安全经验得到的教训;

(3) 与所有相关方沟通措施和改进,沟通的详细程度应与环境相适宜,必要时应约定如何进行;

(4) 确保改进活动达到了预期的目的。

3.7.2 纠正措施

组织应采取措施,消除与 ISMS 要求不符合的原因,以防止再发生。纠正措施文件程序应规定以下方面的要求。

(1) 识别不符合。

(2) 确定不符合的原因。

(3) 评价确保不符合不再发生所需的措施。

(4) 确定和实施所需的纠正措施。

(5) 记录所采取措施的结果。

(6) 评审所采取的纠正措施。

3.7.3 预防措施

组织应采取措施,以消除与 ISMS 要求潜在不符合的原因,以防止发生不符合,所采取的预防措施应与潜在问题的影响相适宜。预防措施文件程序应规定以下方面的要求。

(1) 识别潜在的不符合及其原因。

(2) 评价预防不符合发生所需的措施。

(3) 确定并实施所需的预防措施。

(4) 记录所采取措施的结果。

(5) 评审所采取的预防措施。

预防不符合的措施通常比纠正措施更有效。组织应识别发生变化的风险,并通过关注变化显著的风险来识别预防措施要求,应根据风险评估结果来确定预防措施的优先级。

3.8 信息安全管理体系的认证

3.8.1 认证基本含义

1. 认证的定义

认证是第三方依据程序对产品、过程、服务符合规定的要求给予书面保证(合格证书),认证的基础是标准,认证的方法包括对产品特性的抽样检验和对组织体系的审核与评定,认证的证明方式是认证证书与认证标志。认证是第三方所从事的活动,通过认证活动,组织可以对外提供某种信任与保证,如产品质量保证、信息安全保证等。

信息安全认证包括两类:一类为 ISMS 认证,另一类为信息安全产品认证。

组织实施信息安全管理体系认证,就是根据 ISO/IEC 27001 标准,建立完整的信息安全管理体系,达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式,用最低的成本,达到可接受的信息安全水平,从根本上保证业务的持续性。

2. 认证的目的和作用

信息安全管理第三方认证为组织的信息安全体系提供客观公正的评价,使组织在信息安全管理方面有更大的可信性,并且能够使用证书向利益相关的组织提供保证;同时,认证能够促进组织间的贸易关系,提高跨行业的信息安全管理水平,从整体上有利于全球贸易的开展。

信息安全管理体系可以保证组织提供可靠的信息安全服务,对该体系进行认证可以树立组织信息安全形象,为客户、合作者提供信息安全信任感,有利于组织业务活动的开展,特别是当信息安全构成组织所提供产品或服务的一个质量特性时,如金融、电信等服务组织,开展 ISO/IEC 27001 体系认证对外具有很强的质量保证作用。

ISMS 第三方认证为组织的信息安全管理体系提供客观公正的评价,使组织在信息安全管理方面具有更大的可信性,并且能够使用证书向利益相关的组织提供保证。信息安全管理体系认证的目的和作用一般包括以下几个方面。

(1) 获得最佳的信息安全运行方式。
(2) 保证业务安全。
(3) 降低风险,避免损失。
(4) 保护核心竞争优势。
(5) 提高商业活动中的信誉。
(6) 增加竞争能力。
(7) 满足客户要求。
(8) 保证可持续发展。
(9) 符合法律法规要求。

3. 认证范围

在向认证机构表达认证范围时要注意,组织寻求的认证范围应该与信息安全管理体系

建立的范围是相同的。例如,组织可能有几个办公地点,安全管理系统在这几个地点进行,但是可能只需申请对一个办公地点的认证。

认证范围定义是审核员确定评估计划的基础。认证机构将选择需要评估的功能和活动,并评估审核的时间,以及选择有适当背景的审核员与技术专家。

认证范围声明应该表达清楚,易于阅读,并吸引潜在的合作伙伴的注意。在拟定认证范围时,需要考虑下列因素。

(1) 文件化的适用性声明。

(2) 组织的相关活动。

(3) 要包含在内的组织的范围。

(4) 地理位置。

(5) 信息系统边界、平台。

(6) 所包含的支持活动。

(7) 例外情况。

(8) 在开展认证过程之前认证机构需要对认证范围进行认可。

3.8.2 认证的基本条件与认证机构和证书

1. 认证条件

组织按照 ISO/IEC 27001 标准与适用的法律法规要求,建立并实施文件化的信息安全管理体系,并满足以下基本条件以后,可以向被认可的认证机构提出认证申请。

(1) 遵循法律、法规的工作已被相关机构认同。

(2) 信息安全管理体系文件完全符合标准要求。

(3) 信息安全管理体系已被有效实施,即组织在风险评估的基础上识别出需要保护的关键信息资产、制定信息安全方针、确定安全控制目标与控制方式并实施、完成体系审核与评审活动并采取相应的纠正预防措施。

2. 被认可的认证机构

认证,指的是由第三方组织去审核企业,然后发证。认可,指的是国家主管机构审核第三方组织,以确认它们是否有认证资质。组织在具备体系认证的基本条件时,就可以寻求认证机构申请体系认证。

中国信息安全认证中心是经中央编制委员会批准成立,由国务院信息化工作办公室、国家认证认可监督管理委员会等八部委授权,依据国家有关强制性产品认证、信息安全管理的法律法规,负责实施信息安全认证的专门机构。中国信息安全认证中心为国家质检总局直属事业单位,基于国际标准 ISO/IEC 27001:2013 实施信息安全管理体系认证。

组织在选定认证机构后,就可以与之联系提交认证申请,在双方协商一致的情况下签订认证合同,认证费用是按照审核员的审核人日数(包括文件审核与完成审核报告的人日)与每人日的审核价格来计算。认证合同中应明确认证机构保守组织商业秘密,在组织现场遵守组织的有关信息安全规章的要求。审核所需的人日数取决于以下因素。

(1) 被审核组织认证范围的员工数。

(2) 认证范围持有的信息量。
(3) 场所数据与地理位置分布。
(4) 与外界的接触面。
(5) 所利用的信息技术的复杂程度。
(6) 组织是否已具有一个相关的管理体系认证证书。
(7) 业务功能。
(8) 企业类型。
(9) 风险程度。

3. 证书与标志

组织采取了必要的纠正措施之后，由认证机构验证通过，认证机构将为组织颁发 ISMS 证书，证书包括的内容如下。

(1) 组织全称，涉及的相关组织。
(2) 业务的相关地点。
(3) 业务的流程。
(4) 相关的业务功能与活动。
(5) 认证的范围。
(6) 适用性声明和特定版本的描述。
(7) 关于信息安全系统满足 ISO/IEC 27001 认证标准的声明。
(8) 证书开始生效的时间。
(9) 证书号。

只有认证机构认可了组织的认证范围，才能在证书上显示认可标志。

3.8.3　信息安全管理体系的认证过程

信息安全管理体系认证的总体流程如图 3-1 所示。

1. 认证的准备

在认证之前，认证方与被认证方都要进行相应的准备活动。

被认证方需要按照 ISO/IEC 27001 建立信息安全管理体系，在确认满足认证基本条件的情况下，被认证方向认证机构递交正式申请；认证机构对认证方的申请资料进行初步检查，确定是否受理申请。如受理申请，认证机构将评估认证费用和正式审核时间。

组织可以选择认证的类型，如整个组织，包括所有的信息设施、特定的信息系统。

组织要为认证做的准备工作，包括文件化的信息安全方针、策略、程序、适用性声明及其他文件。

确定 ISMS 范围，以及此范围内的组织结构、人员组成、业务场所的数目、功能、信息安全的应用、业务特性、风险程序等相关材料；已建立适当的安全组织和必要的基础设施，与信息安全相关的员工已落实明确的安全责任的相关说明资料；ISMS 范围业务体系的描述，与外界的接口；法律、法规、合同的附加要求；采用有效的风险评估和风险管理方法，对认证范围所有信息系统进行了风险评估，根据 ISO/IEC 27001 的标准要求，建立有效文件，将

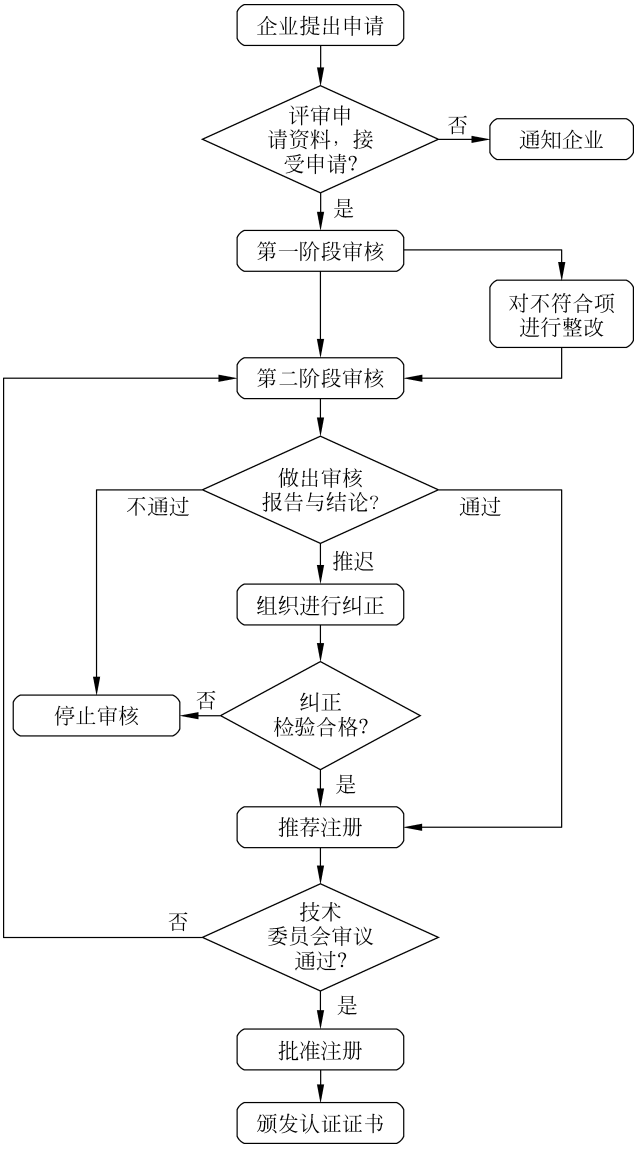

图 3-1 ISMS 认证的过程

所有类型的安全风险和 ISO/IEC 27001 控制联系起来，并成功地选择安全控制目标与控制措施；组织有适当的风险接受的处理程序；文件化的信息安全检查列表，可以证明安全控制正在被正确地实施，并经过相关测试；文件化的安全维护和管理的过程；文件化的体系审核和管理评审报告。

2. 认证的实施

1) 文件审核与初访

第一阶段主要是从总体上了解被审核方 ISMS 的基本情况，确认被审核方是否具备认证审核条件，为第二阶段的审核策划提供依据。审核的重点在于审核 ISMS 文件是否符合

ISO/IEC 27001 标准的要求，了解被审核方的活动、产品或服务的全过程，判断风险评估与风险管理状况，并对被审核方 ISMS 的策划及内审情况等进行初步审查。

(1) 文件审核。通常文件审核包括以下内容。

① 认证范围、适用性声明。

② 信息安全方针、策略、程序、作业指导书。

③ 信息系统环境文件(信息基础设施、网络拓扑结构、信息系统相关人员)。

④ 风险评估与风险管理文件。

⑤ 业务持续性计划。

⑥ 体系审核和管理评审报告。

⑦ 法律、法规、合同的要求。

⑧ 信息安全记录。

(2) 第一阶段现场审核准备，包括以下内容。

① 确定现场审核日期。

② 编制第一阶段现场审核计划。

③ 编制检查表。

(3) 第一阶段现场审核，包括以下内容。

① 见面会：审核组织与被审核组织的管理者、信息安全管理经理及有关人员会面，说明第 1 阶段审核的目的、范围、内容、程序和方法，识别评审难点，并陈述保密声明。

② 现场检查。

③ 与信息安全管理经理交谈，了解被审核组织基本情况以及信息安全管理体系整体运行情况。

④ 到现场调查，了解信息资产、威胁、脆弱点识别是否有遗漏，风险评估与风险管理程序是否适宜，主要方式是审核文件、查阅记录。

⑤ 检查组织的法律、法规获取识别情况以及法律、法规符合性。

⑥ 检查并评审组织的内审情况。

⑦ 检查并评审组织的 ISMS 策划的可行性和适用性，包括 ISMS 方针、策略、程序、控制目标、控制措施、运行策划等。

⑧ 证实管理评审已实施。

⑨ 开不符合项报告。

⑩ 交流会：现场审核结束前，召开交流会，审核组长向被审组织通报第一阶段审核结论，指出存在的不符合项，提出纠正要求，并确定第二阶段审核的条件和具体事宜。

(4) 第一阶段审核报告，报告的编制包括：审核的实施情况与审核结论、发现的问题及下一步的工作重点。

第一阶段与第二阶段审核的差异如表 3-3 所示。

2) 全面审核与评价

第二阶段审核是对信息安全管理体系的全面审核与评价，目的是验证组织的信息安全管理体系是否按照认证标准与组织体系文件要求予以有效实施，组织的安全风险是否被控制在组织可以接受的水平内，根据审核发现对组织的信息安全管理体系运行状况是否符合标准与文件规定做出判断，并据此对被审核方能否通过信息安全管理体系认证做出结论。

表 3-3 第一阶段与第二阶段审核的差异

项 目	第 一 阶 段	第 二 阶 段
目的	• 了解 ISMS 状况,确认被审核方是否具备认证审核条件; • 确定第二阶段审核的可行性; • 确定第二阶段审核的重点	• 评价被审核方的 ISMS 是否有效实施; • 决定被审核方能否通过认证审核并取得注册
范围	• 被审核方的 ISMS 文件和有关资料; • 与重要信息资产极高风险源有关的现场	• 所有现场和有关文件与资料
审核人日	• 较少(约占总人日的 1/3～1/4)	• 较多(约占总人日的 2/3～3/4)
审核内容	• 适用的法律、法规的识别与满足的基本情况; • 风险评估、风险管理方法策划的充分性; • 方针、策略、控制目标、控制措施的连贯性、适宜性; • 对实现信息安全方针与目标的策划; • 组织内容与管理评审的实施情况	• 涉及标准的安全要素; • 受审核方的所有部门
审核报告	• 第一阶段的审核结论主要是对体系策划的充分性,风险评估和法律要求符合的充分性,以及体系文件的符合性进行评价	• 整个审核的结论,对体系的符合性、有效性与适应性进行全面评价

(1) 第二阶段的审核准备。

审核组综合考虑第一阶段审核结论及被审核方对不符合项的纠正情况,确定进行第二阶段审核的时机和条件是否成熟。在此基础上,审核组进行第二阶段审核的准备工作:确定现场审核日期、编制第二阶段现场审核计划、编制检查表。

(2) 第二阶段的现场审核,工作内容如下。

首次会议;现场检查、收集审核证据;内部评定,由审核组汇总分析审核证据结论,被审核申请方不参加内部评定;末次会议,审核组向被审核的组织领导包括信息安全管理经理等,报告审核过程总体情况,发现的不符合项、审核结论、现场审核结束后的有关安排等,主要有以下内容:

① 审核范围的再次确认。

② 不符合项的概要,纠正措施要求。

③ 任何观察资料及建议性活动的概述。

④ 审核的综合评论。

⑤ 宣布审核结论建议。

⑥ 建议或认证的其他方面。

⑦ 审核机密性的再次确认。

审核的期限取决于但并不局限于下列因素:

① 要面谈人员的数量。

② 所持的数据量。

③ 地点的数目。

④ 与外界的接口。

⑤ 使用的信息技术的复杂度。

⑥ 组织是否已经有了相关鉴定的管理系统证书。

⑦ 业务功能。

⑧ 行业类型。

⑨ 风险程度。

(3) 编制审核报告。

现场审核后,审核组应编制审核报告,做出审核结论。审核组将审核报告提交认证机构、申请方等。审核报告包括以下方面。

① 审核场所。

② 组织及适用的 ISO/IEC 27001 控制要求,参阅审核计划与适用性声明。

③ 组织关键文件的发布日期与版本,包括:方针、策略、程序、范围、适用性声明等文件。

④ 适用于组织的额外的强制性或自愿性标准或规则。

⑤ 审核结果的综合评论。

⑥ 不符合项和观察报告的编号识别及类别。

⑦ 审核涉及的人员。

审核结论有以下 3 种情况。

① 信息安全管理体系已建立,运行有效,无严重不符合项和轻微不符合项,同意推荐认证通过。

② 信息安全管理体系已建立并正常运行,在审核过程中发现少数轻微不符合项或个别严重不符合项,要求组织在规定的时间内实施纠正措施,同意在验证纠正措施的实施后推荐认证通过。

③ 信息安全管理体系仍有缺陷,在审核过程中发现较多的不符合项,需要在实施纠正措施后安排复审,本次不予以推荐认证通过。

3. 维持认证

审核和证书颁布并不代表认证结束。通过执行每年至少一次的监督审核,认证机构将继续监控 ISMS 符合标准的情况。这些监督审核的重点是抽样检查系统的某些领域,所以比最初的审核时间短,审核时间约为初始现场审核时间的三分之一。尽管审核团队可能会随时间不同而变化,但是对他们的能力要求和最初审核人员是一样的。

被认证机构有义务通知认证机构组织所发生的可能影响到系统或者证书的变更。这些变更包括:组织变更、人员变更、业务核心变更、技术变更、外部接口变更等。

认证的有效期一般为三年。三年之后,系统需要认证机构重新进行审核。

对于被认证组织而言,认证后要定期进行自我评估活动,监控和检查 ISMS,包括:

(1) 检查 ISMS 的范围是否充分;

(2) 进行定期 ISMS 有效性检查;

(3) 进行定期的规程文档的审查,以实施 ISMS;

(4) 审查可接受的风险水平,考虑组织变更、技术、业务目标的变化;

(5) 实施 ISMS 的改善;

(6) 采取适当的校正或者预防行动。

思考题

1. 叙述信息安全管理体系总体工作计划的主要内容。
2. 试述信息安全管理体系所包括的主要文件、文件的作用和文件的层次。
3. 试归纳信息安全管理体系内部审核流程。
4. 试归纳信息安全管理体系管理评审流程。
5. 解释确定信息安全管理体系认证范围需考虑的因素。
6. 叙述信息安全管理体系认证的目的、作用和认证过程。