第 5 章

信息安全管理控制规范

以往我们对信息安全的认识只停留在技术和产品上，是“只见树木不见森林、只治标不治本”的方式，信息安全的成功三分靠技术、七分靠管理，技术一般但管理良好的系统远比技术高超但管理混乱的系统安全，因此，依据 ISO/IEC 27000 系列建立信息安全管理体系并获得认证已成为世界主流。组织可以参照信息安全管理模型，按照 ISO/IEC 27000 系列标准（也主要参照 GB/T 22239—2019）建立完整的信息安全管理体系并实施与保持，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连续性。

在建立信息安全管理体系过程中，为了对组织所面临的信息安全风险实施有效的控制，需要针对具体的威胁和脆弱性采取适宜的控制措施，包括管理手段和技术方法等。本章根据 ISO/IEC 27001、ISO/IEC 27002、GB/T 22080—2016、GB/T 22081—2016 和 GB/T 22239—2019 等标准，结合组织信息资产可能存在的威胁和脆弱性，详细介绍了信息安全方针、安全组织、资产管理、人员安全、物理和环境安全、通信与操作安全、访问控制、系统开发与维护、安全事件管理、业务持续性管理、符合性保证 11 个控制方面、39 个控制目标、133 项信息安全控制措施的规范内容。

信息安全管理控制规范的组织结构中包括多个安全类别。每个安全类别包括多个控制目标，声明要实现什么目标什么功能，达到什么要求。每个控制目标都会有一个或多个控制措施，被用于实现该控制目标。控制措施是管理风险的方法，是为达成控制目标提供合理保证，并能预防、检查和纠正风险，管理风险的方法包括策略、规程、指南、惯例或组织结构，可以是行政、技术、管理、法律等方面的。每个控制措施又都会有相应的实施指南，实施指南就是对实施该控制措施的指导性说明。此外还有其他信息，即其他需要说明的补充信息。这些控制措施并不是适用于任何场合，也不会考虑使用者的具体环境和技术限制，不可能对一个组织中所有人都适用，需要根据组织的具体情况进行裁剪。

本章在介绍安全方针，信息安全组织，资产安全管理，人员安全管理，物理和环境安全管理，通信和操作安全管理，访问控制，信息系统获取、开发和维护，信息安全事件管理内容时，依据相应的法规制度，结合实际对工作法规制度进行了整理和节选。

5.1 安 全 方 针

【引例 5-1】 某单位领导说：“听说信息安全工作很重要，可是我不知道对于我们单位来说到底有多重要，也不知道究竟有哪些信息是需要保护的。”

安全方针是根据业务要求和相关法律法规制定的，用来提供支持信息安全管理的指导方针。信息安全方针是陈述管理者的管理意图，说明信息安全工作目标和原则的文件。

5.1.1 信息安全方针文件

1. 控制措施

信息安全方针文件应由管理层批准、发布并传达给所有人员和外部相关方。

2. 实施指南

信息安全方针文件需要说明管理的承诺，提出管理信息安全的方法，应包含以下内容。

(1) 信息安全、整体目标和范围的定义，以及在允许信息共享机制下安全的重要性。

(2) 管理者意图的声明，用以支持符合业务策略和目标的信息安全目标和原则。

(3) 设置控制目标和控制措施的框架，包括风险评估和风险管理的结构。

(4) 对组织特别重要的安全方针策略、原则、标准和符合性要求的简要说明。

(5) 信息安全管理(包括报告信息安全事件)的一般和特定职责的定义。

(6) 对支持方针文件的引用。

信息安全方针主要阐述信息安全工作的原则，具体的技术实现问题，如设备的选型、系统的安全技术方案一般不写在安全方针中。信息安全方针应符合实际情况，切实可行。对方针的落实尤为重要。

5.1.2 信息安全方针的评审

1. 控制措施

应按照计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保它持续的适宜性、充分性和有效性。

2. 实施指南

信息安全方针文件应由专人负责其制定、评审和评价。评审应包括评估组织信息安全方针改进的机会和管理信息安全适应组织环境、业务状况、法律条件或技术环境变化的方法。评审过程要注意以下几点。

(1) 应定义管理评审的规程，包括时间表或评审周期。

(2) 评审信息安全方针时，要考虑管理评估的结果。

(3) 应维护好管理评审的记录。

(4) 对修订的方针需要获得管理者的批准。

5.2 信息安全组织

【引例 5-2】 你作为一名网络管理员，发现最近来自外部的病毒攻击很猖獗，要是有15万元买个防毒墙就解决问题了，找谁要这笔钱，谁来采购？

【引例 5-3】 作为一名普通工作人员，我的内网计算机上不了外网，没办法打补丁，我该找谁获得帮助？

在一个组织里，应该有一群人，至少包括单位领导、技术部门和行政部门的人组织在一起，专门负责信息安全的事。下面介绍信息安全组织的控制规范（包括控制目标、控制措施和实施指南），以及组织机构及其职责。

5.2.1　内部组织

内部组织管理的目标是在组织内管理信息安全。

1. 信息安全的管理承诺

1）控制措施

管理者应通过清晰的说明、可证实的承诺、明确的信息安全职责分配及确认，来积极支持组织内的安全。

2）实施指南

根据组织规模的不同，可由一个专门的管理协调小组或一个已存在的机构来承担对信息安全管理承诺的职责。在管理承诺中，要做以下工作。

（1）检查并批准信息安全方针和总的责任。

（2）评审和跟踪验证信息安全方针实施的效果。

（3）为信息安全提供所需的资源和其他支持。

（4）启动计划和程序来保持信息安全意识。

（5）确保整个组织内部的信息安全控制措施的实施是相互协调的。

高层管理者参与信息安全建设，负责重大决策，提供资源，并对工作方向、职责分配给出清晰的说明。高层管理者就是可以“给人、给钱、给设备”，提出工作要求，给予资源保障的人。

2. 信息安全协调

1）控制措施

信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行协调。

2）实施指南

通常，信息安全协调包括管理人员、业务人员、行政人员、应用设计人员、审核员和安全专员，以及法律、IT 或风险管理等领域的专家的协调和协作，其活动包括：

（1）确保安全活动的实施与信息安全方针相一致。

（2）批准组织内的信息安全专门的角色和职责分配。

（3）核准信息安全的特殊方法和程序，如风险评估、安全分级系统。

（4）识别重大的威胁变更和暴露在威胁下的信息和信息处理设施。

（5）评估信息安全控制措施实施的充分性和协调性。

（6）加强整个组织内的信息安全教育、培训和意识。

（7）评价适当性并协调对新系统或服务的特殊安全管理措施的实施。

不仅仅由信息化技术部门参与，与信息安全相关的部门（如行政、人事、安保、采购、外联）都应参与到组织体系中各司其职、协调配合，因此需要协调，并在机构内部达成共识。信息安全工作和其他工作一样，不是某个个人、某个部门就可以完成的。信息技术部门是信息安全组织中的重要执行机构，但不是全部。

3. 信息安全职责的分配

1）控制措施

所有的信息安全职责都应赋予清晰的定义。

2）实施指南

信息安全职责的分配要与信息安全方针相一致。各个资产的保护和执行特定安全过程的全局或局部的职责都应能被明确。这些职责在必要时能够加以补充，从而为特定的地点和信息处理设施提供更详细的指南。

信息资产的所有权人可以把他们的安全责任委派给单独的管理者或服务提供商，但所有权人对资产的安全仍负有最终责任，并且所有权人应能够确定任何责任错误分配的情况。对每一个职责相关的领域都要清晰地规定，特别是在下列情况发生时。

（1）对每个特殊系统相关的资产和安全过程都要进行识别并清楚地定义。

（2）要分配每一笔资产或安全过程的实体职责，并且该职责的细节要形成文件。

（3）清楚地划分授权等级，并形成文件。

为有效实施信息安全管理，保障和实施系统的信息安全，应在机构内部建立信息安全组织，明确角色和职责。在一个机构中，安全角色与责任的不明确是实施信息安全过程中的最大障碍，建立安全组织与落实责任是实施信息安全管理的第一步。

4. 信息处理设施的授权过程

1）控制措施

新信息处理设施应定义和实施一个管理授权过程。

2）实施指南

授权过程应考虑以下要求。

（1）新的信息处理设施应当有相应的用户管理授权，以批准其用途和使用，还要获得负责维护本地系统安全环境的管理人员的授权，以确保满足所有相关安全方针和需要。

（2）必要时检测硬件和软件，以确保它们与系统的其他部分相兼容。

（3）使用个人或私有信息处理设施（如便携式计算机、手持设备等）处理业务信息，可能引入新的脆弱性，因此需要进行评估和授权。

5. 保密性协议

1）控制措施

应识别并定期评审反映组织信息保护需要的保密性或不泄露协议的要求。

2）实施指南

保密性或不泄露协议通过使用合法的可实施条款来解决保护保密信息的问题，并且保密性或不泄露协议的要求应进行周期性评审，当发生影响这些要求的变更时，也要进行评审。协议内容应包括：

（1）定义要保护的信息。

（2）信息的所有权。

（3）协议期望持续的时间。

（4）签署者的职责、权力和行为，以避免未授权信息的泄露。

（5）对涉及保密信息的活动的审核和监视的权力。

(6) 未授权泄露或保密信息破坏的通知和报告过程。

(7) 违反协议和协议终止时所需要采取的条款或措施。

6. 与政府及部门的联系

1) 控制措施

应保持与相关政府及部门的适当联系。

2) 实施指南

要有规程指明什么时候与哪个部门联系,以及对已识别的信息安全事件怀疑可能触犯了法律时,应如何及时报告。受到来自互联网攻击的组织可能需要外部第三方,如互联网服务提供商(Internet Service Provider,ISP)或电信运营商采取措施以应对攻击源。

保持这样的联系是支持信息安全事件管理或业务持续性管理的基本要求。与法律法规相关管理部门的联系有助于组织预先知道必须遵守的法律法规方面的变化,并为应对这些变化做好准备;与其他部门的联系包括公共设施、紧急服务和健康安全等部门,如消防局(与业务持续性有关)、电信供应商(与路由和可用性有关)、供水部门(与设备的冷却有关)。

7. 与其他相关组织的联系

1) 控制措施

应保持与其他安全专家组和专业协会等相关组织的适当联系。

2) 实施指南

考虑成为其他相关组织或安全专家组的成员,以便于:

(1) 增进对最佳实践和最新相关安全信息的了解,获得信息安全专家的建议。

(2) 确保全面了解当前的信息安全环境。

(3) 尽早收到关于攻击和脆弱性的预警、建议和补丁。

(4) 分享和交换关于新的技术、产品、威胁和脆弱性信息。

(5) 提供处理信息安全事件时适当的联络点。

8. 信息安全的独立评审

1) 控制措施

组织管理信息安全的方法及其实施(如信息安全的控制目标、控制措施、策略、过程和程序)应按计划的时间间隔进行独立评审,当安全实施发生重大变化时,也要进行独立评审。

2) 实施指南

独立评审应包括评估安全方法改进的机会和变更的需要,包括方针和控制目标,这对于确保一个组织管理信息安全方法持续的适宜性、充分性和有效性是必要的。

独立评审应由管理者启动,但要由独立于评审范围的具备适当技能和经验的人员来执行,如内部审核部门、独立的管理人员或第三方组织。完成后记录评审结果报告给启动评审的管理者。

如果独立评审识别出组织管理信息安全的方法和实施不充分,或不符合信息安全方针,管理者应考虑纠正措施。

5.2.2 外部各方

外部各方管理的目标是保持组织被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全。

1. 与外部各方相关风险的识别

1）控制措施

应识别涉及外部各方业务过程中组织的信息和信息处理设施的风险，并在允许访问前实施适当的控制措施。

2）实施指南

在允许外部方访问组织的信息处理设施或信息前，应进行风险评估以识别特定控制措施的要求，必要时可签订合同规定外部方连接或访问，以及工作确保安全的条款和条件。关于外部方访问的风险识别应考虑以下问题。

（1）外部方对信息和信息处理设施的访问类型。

（2）所涉及信息的价值和敏感性，以及对业务运行的关键程度。

（3）为保护不希望被外部方访问的信息而采取的必要控制措施。

（4）能够识别组织或人员如何被授权访问、如何授权验证、及需要确认的时间。

（5）外部方在存储、处理、传送、交换信息时使用的方法和控制措施。

（6）因外部方需要而无法访问，以及由于外部方输入或接收不正确产生的影响。

（7）处理信息安全事件或潜在破坏的规程时，外部方持续访问的条款和条件。

（8）需考虑与外部方有关的法律法规要求和其他合同责任。

（9）这些安排对其他利益相关人的利益可能造成怎样的影响。

2. 处理与组织外的人或实体有关的安全问题

1）控制措施

应在允**许组织外的人或实体**访问组织信息或资产之前处理所有确定的安全要求。

2）实施指南

要在允许组织外的人或实体访问组织任何资产前解决安全问题，应考虑以下条款。

（1）保护组织资产，以及判定资产是否受到损害的规程。

（2）组织外的人或实体访问的不同原因、要求和利益。

（3）有关的访问控制策略。

（4）对信息错误（如个人信息错误）、安全事件和安全违规进行报告、通知和调查的安排。

（5）服务的目标级别和服务的不可接受级别。

（6）组织和组织外的人或实体各自的权利和义务。

（7）相关法律问题和如何确保满足法律要求，包括知识产权等相关问题。

3. 处理第三方协议中的安全问题

1）控制措施

涉及访问、处理或管理组织的信息或信息处理设施及与之通信的第三方协议，或在信息处理设施中增加产品或服务的第三方协议，应涵盖所有相关的安全要求。

2）实施指南

应确保在组织和第三方之间不存在误解，组织应使第三方的保证满足自己的需要。为满足对可能存在相关风险的识别要求，协议中应重点考虑以下条款。

（1）确保资产保护的控制措施（如各种保护机制、控制规程与策略等）。

（2）关于硬件和软件安装与维护的责任。

（3）服务的目标级别和服务的不可接受级别。

（4）可验证的性能准则的定义、监视和报告。

（5）监视和撤销与组织资产有关的任何活动的权利。

（6）审核协议中规定的责任、第三方实施的审核等权利。

（7）相关法律问题和如何确保满足法律要求，包括知识产权相关问题。

（8）涉及具有次承包商的第三方，要对这些次承包商需要实施安全控制措施。

5.3　资产安全管理

【引例5-4】 某单位欲安装一台网络防火墙，却发现没有人可以说清楚当前的真实网络拓扑情况，也没有人能说清楚系统中有哪些服务器，这些服务器运行了哪些应用系统。

【引例5-5】 某单位的信息安全评估发现大部分服务器安全状况良好，只有一台服务器存在严重漏洞。研究整改措施时，发现平时没有人对该服务器的安全负责。

由上述例子可以看出，单位没有做到事事有人做，人人有事做。为保护信息资产的安全，所有的信息资产都应该具有指定的属主并且可以被追溯责任。

5.3.1　对资产负责

资产是信息资源的重要内容。对资产负责，就是要实现和保持对组织资产的适当保护。

1. 资产清单

1）控制措施

应清晰地识别所有资产，编制并维护所有重要资产的清单。

2）实施指南

组织应识别所有资产并将资产的重要性形成文件。资产清单应包括为从灾难中恢复必需的所有信息，包括资产类型、格式、位置、备份信息、业务价值等，并且应该为每一项资产确定责任人、信息分类和保护级别等。

编制一份资产清单是风险管理的一个重要的先决条件。

2. 资产责任人

1）控制措施

与信息处理设施有关的所有信息和资产应由组织的指定部门或人员承担责任。

2）实施指南

资产责任人应确保与信息处理设施相关的信息和资产已进行适当的分类，并定期地

评审访问限制和类别，同时要考虑可应用的访问控制策略。

日常任务可以委派给其他人，如委派给一个管理人员每天照看资产，但责任人仍保留职责。

3. 资产的合格使用

1）控制措施

与信息处理设施有关的信息和资产使用允许规则应被确定、形成文件并加以实施。

2）实施指南

具体规则由管理者提供。使用或拥有访问组织资产权限的本单位人员、承包方和第三方人员应意识到他们使用信息处理设施相关的信息、资产及资源时的限制条件，应遵循信息处理设施可接受的相关使用规则，并对他们职责许可的使用负责。

5.3.2 信息分类

为了更好地保护资产等信息资源，需要对这些信息资源进行分类，从而能有针对性地对信息资源进行适当程度的保护。

1. 分类指南

1）控制措施

应按照信息资源对组织的价值、法律要求、敏感性和关键性进行信息资源分类。一般应分为“公开”“内部”“秘密”“机密”“绝密”。

2）实施指南

信息资源的分类及相关保护控制措施应考虑共享或限制信息资源的业务需求，以及与这种需求相关的业务影响。分类指南应包括根据预先确定的访问控制策略进行初始分类，以及一段时间后进行重新分类的惯例。

一般来说，给信息资源分类是确定该信息资源如何予以处理和保护的简便方法。

应考虑分类类别的数目和使用中获得的好处。过度复杂的分类可能使用起来不方便、不经济或不实际。在解释从其他组织获取的文件分类标记时更要小心，因为其他组织可能对于相同或类似命名的标记有不同的定义。

2. 信息的标记和处理

1）控制措施

应按照组织所采纳的分类机制来建立和实施一组合适的信息标记和处理程序。

2）实施指南

信息资源标记的规程需要涵盖物理和电子格式的信息资产。

对于包含分类为敏感或关键信息资源的系统输出，应在该输出中携带合适的分类标记，对每种分类级别，应定义包括安全处理、存储、传输、删除、销毁等的处理规程，还应包括一系列对安全相关事件的监督和记录规程。

标识信息类别，表明文件的密级、存储介质的种类（如内网专用 U 盘），规定重要敏感信息的安全处理、存储、传输、删除和销毁的程序。

3）月维护

月维护原则上由密码管理人员或其指定的人员完成，每月最后一周安排半天时间对

现用密码装备进行维护。

基本要求是对机器进行较全面的维护保养和检查，使其保持良好的技术性能。

4）季检修

季检修由专职工作干部完成。在季末结合月维护安排一天时间进行检修。

基本要求是对机器进行全面的维护保养，调试、检测机器各项技术性能和指标。

5）年检查

年检查应结合普查或安全保密检查进行，通常由单位统一组织。

基本要求是解决日常维护中不易解决的一些遗留问题和其他难度较大的问题，检查系统参数，进行软硬件性能测试或根据上级统一部署调整系统参数。

年检查要对机器运行环境进行综合检查、清理。一是清除机器内部积灰积尘，检查配电系统的安全性，测量接地电阻；二是检查、测试防电磁辐射措施和安全防护设施设备是否可靠有效；三是检查消防设备、空调系统等是否正常，确保密码使用环境安全。

6）注意事项

在维护修理过程中，严禁带电操作；非专职人员不得随便拆装。

5.4　人员安全管理

【引例5-6】 汇丰控股公司发布公告，其旗下汇丰私人银行（瑞士）的一名IT员工，曾于三年前窃取了银行客户的资料，失窃的资料涉及1.5万名在瑞士开户的现有客户。有鉴于此，汇丰银行三年来共投入1亿瑞士法郎，用来将IT系统升级并加强。借用《论语》中的一句话："吾恐季孙之忧，不在颛臾，而在萧墙之内也。"

【引例5-7】 某单位负责信息化工作的领导说："为什么要买防火墙？我们盖楼时是严格按照国家消防有关规定施工的呀！"

5.4.1　任用前

在人员任用前，要确保本单位人员、承包方人员和第三方人员理解其职责，考虑其承担的角色是适合的，以降低设施被破坏、偷盗、欺诈和误用的风险。

1. 角色和职责

1）控制措施

组织应根据其自身的信息安全方针对本单位人员、承包方人员和第三方人员的安全角色和职责进行分类、确定并形成文件。

2）实施指南

要对安全角色和职责进行定义，并在任用前清晰地传达给任用的候选者。

安全角色和职责要满足以下要求。

（1）按照组织的信息安全方针实施和运行。

（2）保护资产免受未授权访问、泄露、修改、销毁和干扰。

（3）执行特定的安全过程或活动。

（4）确保职责分配给可采取措施的个人。

(5) 向组织报告安全事件、潜在事件或其他安全风险。

2. 审查

1) 控制措施

关于所有任用的候选者、承包方人员和第三方人员的背景验证核查应按照相关法律法规、道德规范和对应的业务要求、被访问信息的类别和察觉的风险来执行。

2) 实施指南

验证核查要考虑所有相关的隐私、个人数据库,相关的法律,并在允许时考虑:

(1) 个人资料的可用性。

(2) 申请人履历的核查。

(3) 声称的学术、专业资质的证实。

(4) 个人身份的核查。

(5) 其他细节核查。

3. 任用条款和条件

1) 控制措施

作为合同义务的一部分,本单位人员、承包方人员和第三方人员应同意并签署他们的任用合同条款和条件,这些条款和条件应声明他们和组织的信息安全职责。

2) 实施指南

任用条款和条件在反映组织安全方针的情况下,还要符合以下内容。

(1) 所有访问敏感信息的本单位人员、承包方和第三方人员应在给予权限之前签署保密协议。

(2) 本单位人员、承包方和其他人员的法律责任和权利。

(3) 与本单位人员、承包方和第三方人员操作的信息系统和服务有关的信息分类和组织管理资产的职责。

(4) 本单位人员、承包方和第三方人员操作来自其他外部方信息的职责。

(5) 组织处理人员信息的职责,包括由于组织任用或在组织任用过程中产生的信息。

(6) 扩展到组织场所以外和正常工作时间之外的职责,如在家中工作的情形。

(7) 如果本单位人员、承包方和第三方人员漠视组织的安全要求应采取的措施。

5.4.2 任用中

在人员任用中,要确保所有的本单位人员、承包方人员和第三方人员知悉信息安全威胁和利害关系、他们的职责和义务,并准备好在其正常工作中支持组织的安全方针,以减少人为过失的风险。

1. 管理职责

1) 控制措施

管理者应要求本单位人员、承包方人员和第三方人员执行组织已建立的方针和程序。

2) 实施指南

如果本单位人员、承包方人员和第三方人员没有意识到他们的安全职责,或感觉被组织方低估,他们可能会对组织造成相当大的破坏,而被激励的人员则更可靠并能减少信息