信息技术
安全技术
信息技术安全管理指南

第 2 部分：IT 安全管理与策划

注：本文件为个人自行翻译，因译者水平有限，其中错误再所难免，希望大家能够多扔板砖，西红柿亦可以考虑，臭鸡蛋的不要，鲜花尤佳，孔方兄最棒，美女那是我的最爱^_^。

偶，刘青，ID 易水寒江雪，半路出家搞安全管理，希望和大家能够多多交流，也希望各位大虾多多指正。Email:liuq1217@163.com；MSN：liuq1217@msn.com。

内容

1 范围

ISO/IEC TR 13335 第 2 部分的指南阐述了对于 IT 安全管理只管重要的主题，以及这些主题之间的关系。这些指南有助于识别和管理 IT 安全的所有方面。这些指南有助于识别和管理 IT 安全的所有方面。

深入了解第 1 部分介绍的概念和模型对于完全理解第 2 部分的内容至关重要。

2 引用标准

ISO/IEC TR 13335-1：1997 IT 安全管理指南－IT 安全概念和模型

3 术语及定义

ISO/IEC TR 13335 第 1 部分的定义适用于第 2 部分。第 2 部分使用下列术语：可审计性、资产、鉴权、可用性、基线控制方法、保密性、数据完整、影响、完整性、IT 安全、IT 安全策略、可靠性、残余风险、风险、风险分析、风险管理、防护措施、系统完整性、威胁和脆弱点。

4 结构

第 1 部分共包括 17 个条款。第 5 和第 6 条款介绍了有关本文档目标和背景的有关信息。第 7 条款概述了成功 IT 安全管理所涉及的各种活动。第 8 条款到 16 条款详细阐述了这些活动。第 17 条款对第 2 部分进行了总结。

5 目的

第 2 部分的目的是介绍与 IT 安全管理和策略相关的各种活动，以及组织内的相关角色和职责。本部分适用于那些负责 IT 系统的获得、设计、实施或运行的管理人员。除了负责 IT 安全的管理人员之外，它也适用于那些对于使用 IT 系统活动负责的管理人员。总的来说，这一部分内容对于任何对组织 IT 系统负有管理职责的人员都是有用的。

6 背景

政府和商业组织严重依赖于信息的使用以开展他们的业务活动。信息和服务保密性、完整性、可用性、可审计性、鉴权和可靠性的损失，可能对组织造成负面影响。因此对于在组织内保护信息和管理 IT 系统的安全的需求也非常迫切。这种保护信息的要求在今天的环境下显得尤为重要。因为许多组织都通过 IT 系统网络保持内部或外部联系。

IT 安全管理是用于达到和保持保密性、完整性、可用性、可审计性、鉴权和可靠性的适当等级的过程。IT 安全管理功能包括：

- 确定组织的 IT 安全目标、战略和策略；
- 确定组织的 IT 安全要求；
- 识别并分析组织内 IT 系统的资产、脆弱点及对其的威胁；
- 识别并分析安全风险；
- 规定适宜的防护措施；
- 监视必需的防护措施的实施和运行，以一种成本有效的方式保护组织的信息和服务；
- 开发和实施安全意识方案；
- 事故的检测和响应。

为了履行 IT 系统的管理职责，安全应作为组织安全管理计划的内在部分，并被正和到组织的所有概念性流程之中。因此，本部分阐述的几个安全主题有着更加广泛的管理含义。本报告并不试图关注广泛的管理话题，而是关注于主题的安全方面以及他们与管理的大致关系。

7 IT 安全管理

7.1 策划和管理过程概述

IT 安全策划和管理是在组织内建立并保持 IT 安全方案的全部过程。图 1 展示了该过程的主要活动。因管理风格、组织规模和结构的不同，这一过程可以根据使用的环境进行裁剪。重要的是图 1 所识别的所有的活动和功能应在组织的风格、规模和结构以及它的业务运作模式中予以阐述。进行管理评审并作为这些活动和功能的隐含部分。

出发点是为了建立一个清晰的组织 IT 安全目标的印象。这些目标从高层次目标（如，业务目标）依次到组织的 IT 安全战略以及公司的 IT 安全策略（在第 8 条款中详细介绍）。因此公司 IT 安全方针的一部分就是创建一个适宜的、可以确保已定义目标完成的组织结构。

7.2 风险管理概述

风险管理包括四项单独的活动：

- 在公司 IT 安全策略范围内确定适宜于组织的整体风险管理战略；
- 根据风险评估的结果或基线控制方法为单独的 IT 系统选择防护措施；
- 阐述基于安全推荐措施的 IT 系统安全策略以及，需要时，公司 IT 安全策略的更新（适当时，部门的 IT 安全策略）；
- 基于已批准的 IT 系统安全策略构建 IT 安全计划以实施防护措施。

7.3 实施概述

应按照 IT 安全计划的要求，实施每个 IT 系统所需的防护措施。整体 IT 安全意识的改进对于防护措施的有效性是一个非常重要的方面，尽管经常被遗漏。图 1 清楚的展示了这两个任务（防护措施的实施和安全意识方案）应该同时进行，因为用户的行为不可能很快的改变，需要更长的时间持续不断的提高意识。

7.4 后续活动概述

在第 16 条款中阐述的后续活动包括：

- 防护措施的保持，以确保其持续有效地运行；
- 检查防护措施，以确保与已批准的策略和计划保持一致；
- 监视资产、威胁、脆弱点和防护措施的变更，并检测可能影响风险的变更；
- 事故处置，以确保对不期望事件的恰当响应。

后续活动是一个连续的任务，应包括早期决策的评估。

7.5 集成 IT 安全

如果所有的 IT 安全活动在每个 IT 系统生命周期的开始阶段就在组织内正式地实施，那么这些活动是最有效的。IT 安全过程本身就是一个主要活动的循环，应被集成于 IT 系统生命周期的所有阶段。实时安全是最有效的，如果一开始就被集成到新的系统中。已有的系统和业务活动在任何时候也能从安全集成中及时获益。

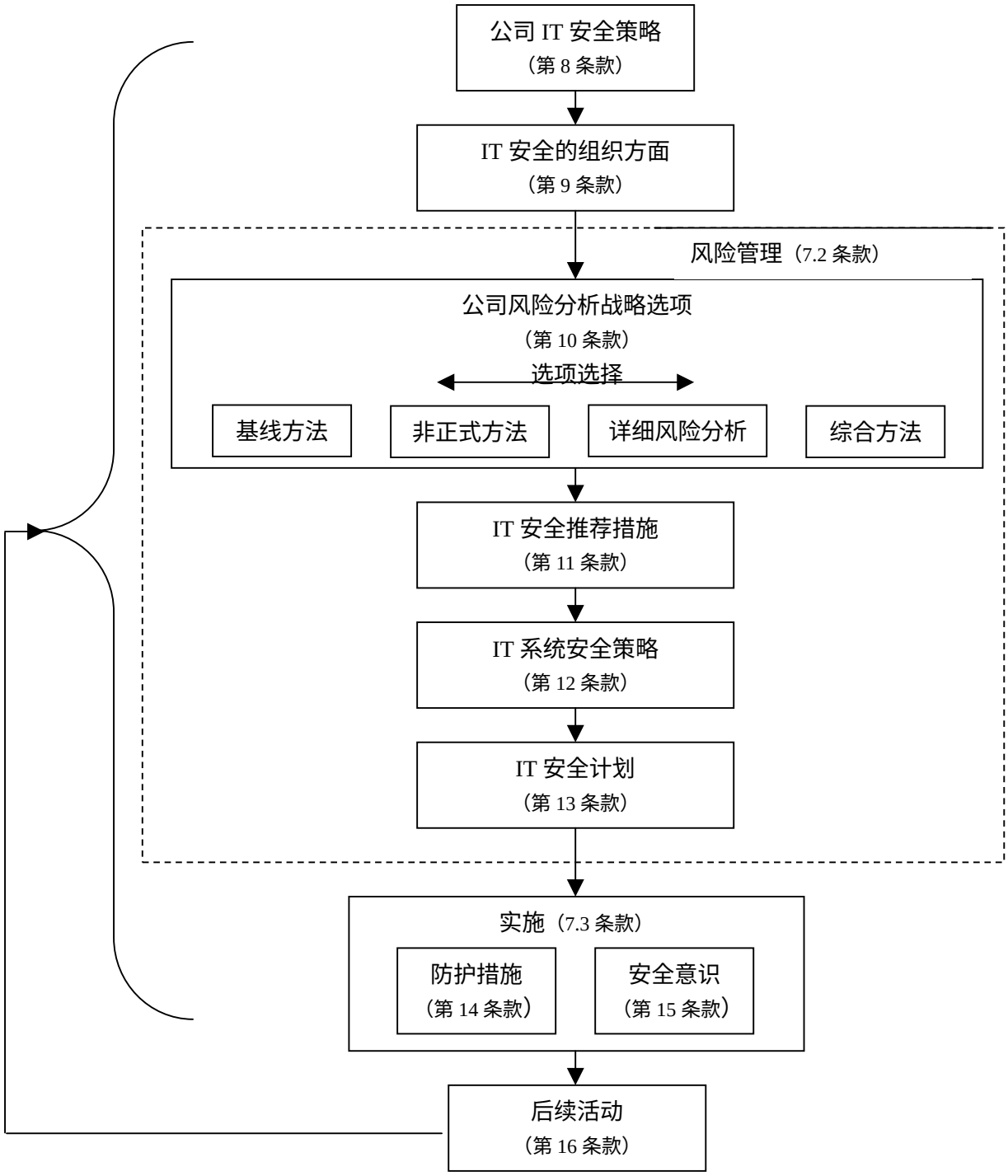

图 1： IT 安全策划和管理概述

IT 系统生命周期可以被分为三个基本阶段。这些阶段中的任何一个用下列方式与 IT 安全保持相关：

- 策划：应在所有的策划和决策活动中，都考虑 IT 安全的需求；
- 获取：IT 安全要求应被集成于系统的设计、开发、购买、升级或其他构建的过程中。集成于这些活动中的安全要求确保了系统在适当的时候引入成本有效的安全特征，而不滞后。
- 运行：IT 安全应被集成到运行环境中。因为使用 IT 系统的目的是为了完成其预期的

使命，它可能经历一系列的升级活动，包括购买新的硬件组件或更改/增添软件。此外，运行的环境也在不断的变化。环境的变化可能产生新的系统脆弱点，无论是削减还是接受，都需要对这些脆弱点进行分析和评估。系统的安全报废或重用也同样重要。IT 安全应成为在 IT 系统的生命周期阶段内及各阶段之间伴随着许多反馈的持续的过程。图 1 只展示了整体的反馈途径。大多数情况下，在 IT 安全过程的所有主要活动内和各项活动之间都会有反馈的发生。贯穿于 IT 系统生命周期的三个阶段的反馈提供一个关于 IT 系统的脆弱点、威胁和防护措施的持续的信息流。

需要注意的是，每个组织的业务领域可能识别出自己独特的 IT 安全要求。通过分享可用于支持管理决策过程的安全方面的信息，这些领域应相互支持并支持整个 IT 安全过程。

8 公司 IT 安全策略

8.1 目标

可以在公司的每个层次上和每个业务单元或部门分别定义目标（应该完成什么），战略（如何完成这些目标）和策略（完成目标的规则）。为了达到有效的 IT 安全，需要为每个组织层次和业务单元分配不同的目标、战略和策略。虽然可能受到不同观点的影响，相应文件之间的一致性是非常重要的，因为许多威胁是通用的业务问题（如系统攻击、文件删除和火灾）。

8.2 管理承诺

高层管理人员对于 IT 安全的承诺是重要的，应形成一个正式的、达成一致的文件化的公司 IT 安全策略。公司的 IT 安全策略应由公司的安全策略导出。

8.3 策略关系

适当时，公司的 IT 安全策略可能包含在公司的技术和管理策略的范围内，二者共同建立了公司 IT 安全战略声明的基础。该声明应包括一些关于安全重要性的劝导性的陈述，尤其当安全对于战略的符合性是必须的。图 2 展示了不同策略之间的关系，不管文件还是组织所采用的组织结构，重要的是要阐述策略所描述的不同信息并保持一致。

此外，对于特定系统和服务或一组 IT 系统和服务要求更为详细的 IT 安全策略。这通常被称为 IT 系统安全策略。基于业务和技术的原因，清楚的定义 IT 系统安全策略的范围和边界是管理的一个重要方面。

8.4 公司 IT 安全策略元素

公司 IT 安全策略至少应涵盖以下主题：

- IT 安全要求，例如，尤其是基于资产所有者的角度考虑的保密性、完整性、可用性、鉴权、可审计性和可靠性；
- 组织的基础设施和职责分配；
- 将安全整合到系统开发和获取中；
- 指南和程序；
- 定义信息分类的种类；
- 风险管理战略；
- 中断计划；
- 人员问题（尤其要关注那些要求信任的职位，如维护人员和系统管理员）；
- 意识和培训；

- 法律法规责任；
- 外包管理；
- 事件处置。

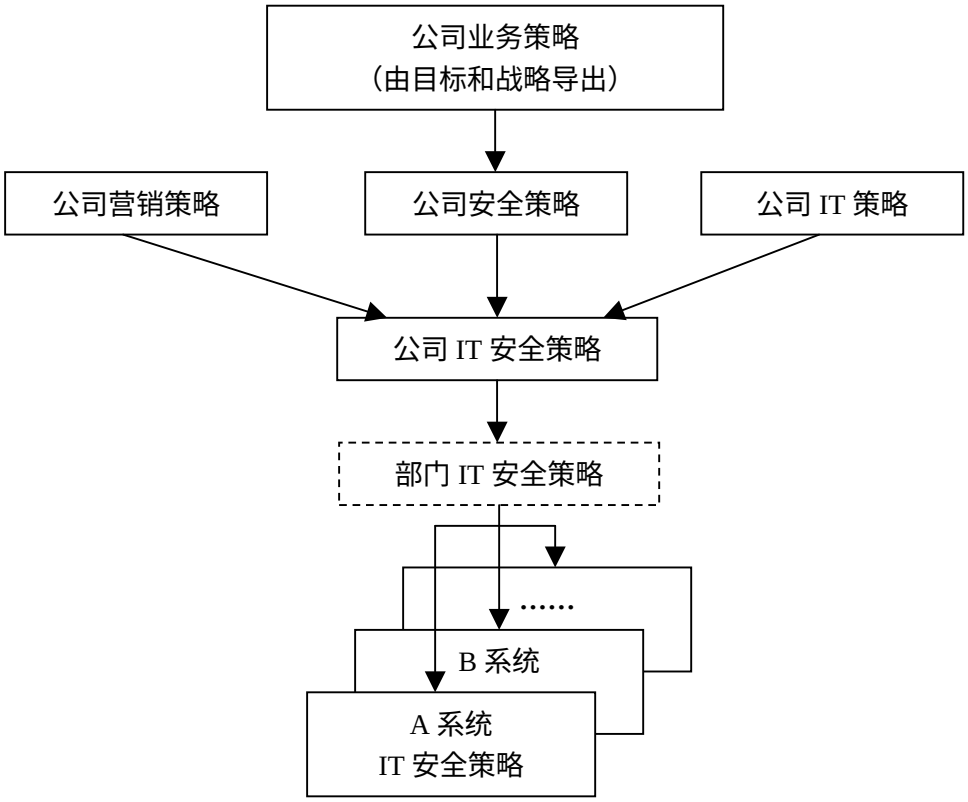

图 2：策略关系

9 IT 安全的组织方面

9.1 角色和职责

IT 安全是一个多学科的主题，并与每个 IT 项目和系统以及组织内所有 IT 用户都有关系。应适当的授予并划分职责，以确保可以完成所有重要的任务并以一种有效的方式运行。

虽然这一目标可以通过不同的组织框架来完成，依赖于组织的规模和结构，下列角色在任何组织中都应涉及：

- IT 安全论坛，典型的包括多学科主题和批准指南和标准；
- 公司的 IT 安全管理人员，作为在组织内所有 IT 安全方面的核心。

应明确规定 IT 安全论坛和 IT 安全管理人员的责任，并充分优先确保公司 IT 安全策略的承诺。组织应为 IT 安全管理人员提供清晰定义的沟通渠道、职责和授权。其责任应经过 IT 安全论坛的批准。这些责任的履行可能需要使用外部咨询人员作为补充。

图 3 提供了一个公司 IT 安全管理人员、IT 安全论坛和来自组织其他领域代表（如，其他安全功能，用户沟通和 IT 人员）之间关系的典型示例。这些关系可能是直线管理或功能性的。图 3 中所描述的组织 IT 安全的示例覆盖了 3 个组织层次，这可以根据组织的需要增加或减少层次，以更好的适合于组织。小型或中型的组织可以选择拥有一个公司的 IT 安全管理人员，其职责涵盖了所有的安全角色。当功能集中时，须确保适宜的检查并保持平衡，以

避免权力过于集中而导致无法对其施加影响或控制的可能性。

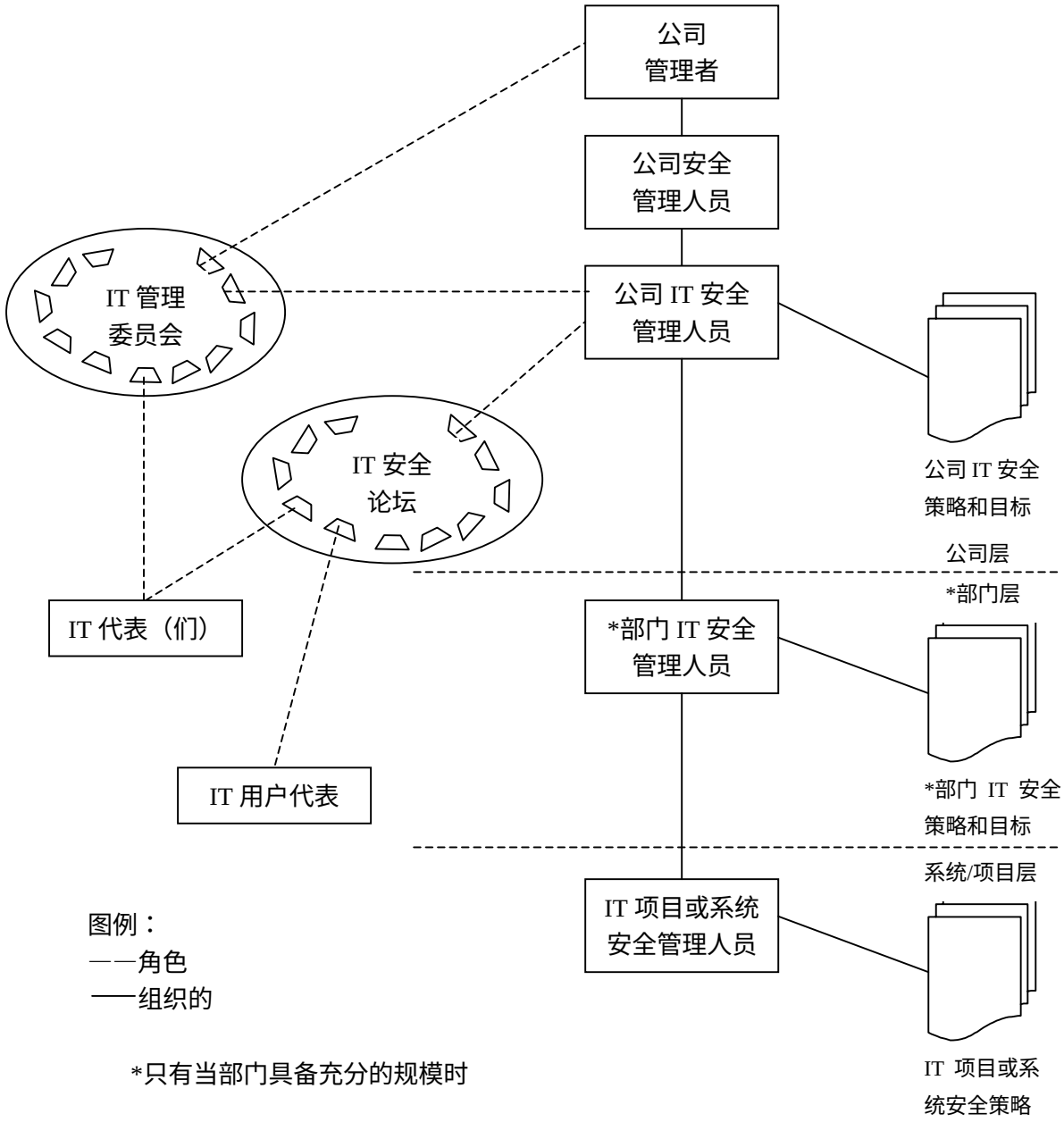

图 3：IT 安全组织示例

9.1.1 IT 安全论坛

论坛的人员应具备必需的识别要求、阐述策略、起草安全方案、评审成绩并指导公司 IT 安全管理人员的技能。可能已经有一个适宜的论坛，当然如果是一个单独的 IT 安全论坛更好。类似论坛和委员会的职责是：

- 向 IT 管理委员会提出关于战略安全策略的建议；
- 阐述支持 IT 战略的公司 IT 安全策略，并经过 IT 管理委员会的批准；
- 将公司的 IT 安全策略转化为 IT 安全方案；
- 监视 IT 安全方案的实施；
- 评审公司 IT 安全策略的有效性；
- 提高 IT 安全意识；

- 关于支持策划过程和 IT 安全方案实施所需资源的建议。

为了获得更好的效果，论坛应包括拥有安全和 IT 系统技术方面的成员，以及 IT 系统提供者和用户的代表。开发一个可操作性的公司 IT 安全策略需要所有这些领域的知识和技能。

9.1.2 公司 IT 安全管理人员

因为 IT 安全的职责被分配了，这就可能导致一个风险，即最后没有任何人感觉到有职责。为了避免这一点，应将职责赋予单个的个人。公司的 IT 安全管理人员应作为组织内所有 IT 安全方面的中心。可能已经有一个适宜的人员，他承担了额外的职责，虽然我们推荐设立一个专职的岗位。选择一个有安全和 IT 背景的人作为公司 IT 安全管理人员是最好的。其主要的职责是：

- 监控 IT 安全方案的实施；
- 与 IT 安全论坛和公司安全管理人员保持联系并向其报告；
- 维持公司的 IT 安全策略和指南；
- 协助进行事件调查；
- 管理公司范围的安全意识方案；
- 确定 IT 项目和系统安全管理人员所引用的术语（或相关部门 IT 安全管理人员）。

9.1.3 IT 项目安全管理人员和 IT 系统安全管理人员

通常将那些对单个项目或系统的安全负责的人员称为 IT 安全管理人员。在一些情况下，可能有一个专职的岗位。公司 IT 安全管理人员（或者是 IT 安全部门的管理人员）负有对这些管理人员的职能管理职责。安全管理人员应作为所有项目、系统或一组系统安全方面的关注焦点。该岗位的主要职责是：

- 与公司的 IT 安全管理人员（或者是 IT 安全部门的管理人员）保持联系并向其汇报；
- 发布并维持 IT 项目或系统的安全策略；
- 开发和实施安全计划；
- IT 防护措施的实施和使用的日常监视；
- 发起并协助事件的调查。

9.2 承诺

各级管理人员对于个人所进行的努力的支持对于有效的 IT 安全是至关重要的。对于 IT 阿起那目标的业务范围的承诺包括：

- 理解组织的整体需求；
- 理解组织内 IT 安全的需求；
- 展示对 IT 安全的承诺；
- 积极阐述 IT 安全需求；
- 积极为 IT 安全分配资源；
- 最高管理层的意识－IT 安全意味着什么或包含的范围和程度。

IT 安全目标应在组织内得到传播。每个雇员或合同人员应知道他们的角色和职责、他们对 IT 安全的贡献以及委托他们达到这样的目标。

9.3 一致性方法

IT 安全的一致性方法应用于所有的开发、保持和运行活动。应在信息和 IT 系统的从策划

到处置整个生命周期内确保适宜的保护。如图 3 所示的组织结构能够在组织内支持 IT 安全的协调的方法。这需要对标准的承诺的支持。标准可以包括根据组织 IT 安全需求选择和应用的国际、国家、地区、航行也部门和企业的标准或准则。技术性的标准可以用实施准则和指南以及使用和管理作为补充。

使用标准的益处包括：

- 整合安全；
- 多学科；
- 一致性；
- 简便性；
- 规模经济；
- 组织间的相互作用。

10 公司风险分析战略选项

任何希望提高安全的组织应实施适合于组织环境的、包含以一种有效的方式阐明风险的方法的风险管理战略。当需要并确保一个成本和时间有效的方法时，要建立一个集中于安全努力的战略。

对所有系统进行详细的分析并不是一种资源或成本的有效，不能阐述严重风险也是无效的分析。一种方法在这些极端的之间提供了一种平衡，即实施高水平的评审以确定系统的 IT 安全需求并进行与这些需求一致的深层分析。任何组织的安全需求依赖于其规贸、业务类型以及它的环境和文化。选择的公司风险分析战略选项应直接与这些实际相关。

在一些情况下，组织可能决定不采取任何措施或延迟防护措施的实施。这一管理决策仅应在组织完成了高水平评审之后才能作出。然而，如果需要作出类似的决策，管理层应充分了解风险和可能的负面影响以及不期望事件发生的可能性。没有这些知识，组织就可能违反法律法规，并将资产暴露于潜在的损失。只有在对这些和其他可能的负面影响进行认真考虑之后，才采纳不采取任何措施或延迟防护措施的决策和判断。基于高层评审的结果，削减风险的防护措施可以从下面描述的四个选项中选择一个。下列章节对于每种选项的优点和确定都进行了介绍。

10.1 基线方法

第一个选项就是选择一系列的防护措施以达到所有系统的基线保护水平。在基线文档和实施规范中建议了许多标志性的防护措施。在检查了基本需求之后，这些防护措施可以根据其他的组织改编，如国际和国家标准、组织、行业部门标准或推荐或其他有着相似性的公司（例如，业务目标、规模、IT 系统和应用程序）。

这一方法有很多优点：

- 不需要进行详细风险分析所需的资源，减少花费在防护措施选择上的时间和精力。一般来说，识别基线防护措施并不需要太多的资源。
- 同样或类似的基线防护措施可以从其他组织改编而来，不需要太多的努力。如果一个组织的许多系统都运营于同样的环境，并且如果业务需求是可比较的，基线防护措施可以提供一个成本有效的解决方案。

这一选项的缺点在于：

- 如果基线水平定的过高，那么可能需要太多的花费或对于某些系统的限制性安全；如果基线水平定的过低，那么对于某些系统来说就不安全。
- 管理相关的变化比较困难。例如，如果系统升级，评估原有的基线防护措施是否仍旧充分就有些困难。

10.2 非正式方法

第二种方法是对所有系统进行非正式的、注重实效的风险分析。非正式方法并不基于结构性的方法，而是利用个人的知识和经验。如果没有内部安全专家，外来咨询人员也可以进行这一分析。

这种方法的优点在于：

- 进行非正式分析并不需要学习额外的技能，并且实施起来比详细的风险分析快。因此，这个方法可能成本有效，适合于小型组织。

也有几个缺点：

- 没有结构化的方法，增加了遗漏某些风险和关注领域的可能性；
- 因为是非正式的方法，结果可能会收到评估者的主官观念和判断的影响；
- 对于防护措施的选择几乎没有任何解释，因此，要证明防护措施的花费是正当的是很困难的；
- 随着时间的变迁，不进行重新评审而管理安全相关的变更是很困难的。

10.3 详细的风险评估

第三种方法是进行详细的风险评估。详细的风险评估包括识别资产并赋值，评估资产威胁的等级以及这些资产的脆弱点。这一输入被用于评估风险。通过这样做，风险分析支持基于资产已识别的威胁所证明的的防护措施的识别、选择和采取，并将这些风险减低到组织预先定义的可接受的水平。详细的风险分析是一个非常耗费资源的过程，因此需要仔细地建立边界和持续地管理关注。

这一方法的有点在于：

- 为每一系统的安全需求识别一个适宜的安全等级；
- 安全相关变更的管理将从详细风险分析获得的额外信息中获益。

这一方法主要的缺点是：

- 为了获得可行的结果，需要数量客观的时间、经历和专家的意见。

10.4 综合方法

第四种方法是使用高水平的风险分析方法以先识别处于高风险或对组织运行非常关键的那些系统。基于这些结果，可以将系统分为两类：一类要求进行详细的风险分析以达到适当的保护；一类进行基线保护就足够了。

这一方法是 10.1 条款描述的基线方法和 10.3 条款描述的详细风险分析方法的最佳结合点。因此，它提供了一个良好的平衡，在最小化识别防护措施时所花费的时间和精力的同时，又确保所有系统得到适当的保护。

这种方法的优点在于：

- 在提交重要资源之前，使用简单的、高水平的方法以收集所需的信息可能使风险管理

方案更易被接受；
- 建立组织的安全方案的快速战略蓝图成为可能，其可以被用作良好策划的辅助工具；
- 可以把资源和金钱用于最得益的地方，并可以早期阐明哪些系统可能处于高风险。

这种方法的缺点是：
- 如果高级风险分析的结果不准确，那么有些需要进行详细风险分析的系统可能就没有被阐述。如果对高级风险分析的结果进行适当检查，这种情况是不可能发生的。但是无论如何，这样的系统仍旧会被基线防护措施所掩盖。

在大多数情况下，这种方法提供了最好的成本有效性，对于大多数组织来说是高度推荐的风险分析方法。

11 IT 安全推荐措施

第 10 条款中的任何一种方法都应提供许多的推荐措施以将风险降低到可接受的水平。这些推荐措施应经过管理层的批准，可包括：
- 确定考虑的 IT 系统的风险可接受等级的准则；
- 选择可将风险降低到可接受水平的防护措施；
- 与这些防护措施实施有关的收益，以及通过这些防护措施所达到的风险的降低；
- 当所有的防护措施已经被实施后，接受仍旧存在的残余风险。

11.1 选择防护措施

防护措施有几种类型：那些预防、减少、监视、检测或纠正不期望事件的防护措施，以及从不期望事件中恢复的防护措施。预防措施包括对不期望行为震慑以及提高安全意识的活动。防护措施应用的主要领域以及各个领域的部分例子如下：
- 硬件（备份，密钥）；
- 软件（电子签名，日志，防病毒工具）；
- 通讯（防火墙，数据加密）；
- 物理环境（围墙，证章）；
- 人员（全体职员意识，雇员终结程序）；
- 行政（授权，硬件处置，license 控制）。

防护措施并不是彼此独立的，通常是联合作用。在选择的过程中必须考虑防护措施的互相依赖关系。在选择防护措施的过程中，应进行检查以确保没有残留的漏洞。这样的漏洞可能会绕过已经存在的防护措施，而允许偶然的威胁造成损害。对于新的系统，或已经存在系统发生重大变更，防护措施的选择可能包括安全框架。安全框架作为整体系统结构的一部分，描述了 IT 系统的安全要求是如何被满足的。它阐述了技术性的防护措施，同时也考虑非技术性方面。

需要对所有的防护措施进行管理以确保其有效的运行，并且为了保持的目的许多防护措施也需要行政的支持。在防护措施的选择过程中应牢记这些因素。

重要的是，有效地实施防护措施而不产生不适当的用户和管理费用。如果防护措施可能产生显著的变化，那么他们应该与安全意识方案、变更管理和配置管理共同实施。

11.2 风险接受

实施选择的防护措施之后，通常仍会有残余风险的存在。这是因为没有系统是绝对安全的，并且也存在有意识地未对特定资产实施保护的情况（例如，因为假定的低风险，或与需要保护的资产评估价值相比高昂的推荐防护措施的成本）。

风险接受过程的第一步就是评审选择的防护措施并识别和评估所有的残余风险。下一步就是将残余风险分类为组织可接受的或不可接受的。

非常明显的是，不可接受的风险是不可容忍的，因此需要考虑采取额外的防护措施以限制这些风险的影响或后果。在每个这样的情况，都必须作出业务决策。无论是认为可接受的风险，还是为了将风险降低到可接受的水平而采取的额外的防护措施，都必须经过批准。

12 IT 系统安全策略

IT 系统安全策略的开发应基于公司和部门的安全策略。这些系统的安全策略包括一系列的系统和服务保护的准则和规则。通过对系统和服务实施适当的防护措施以实施策略，确保达到较高级别的保护。

IT 系统安全策略必须经过高层管理者的批准，作为强制性的系列的准则和规则，以确保他们的应用和执行所需资金和人力资源的投入。

当确定每个 IT 系统安全策略时，需要考虑的关键问题是：

- 定义考虑的 IT 系统及其边界；
- 定义系统达到的业务目标，以及那些可能对系统安全策略、防护措施的选择和实施有影响的因素；
- 潜在的负面业务影响，来自：
  - ✧ 服务或资产（包括信息）的不可用、拒绝服务或破坏；
  - ✧ 信息或软件的未授权修改；
  - ✧ 信息的未授权泄漏。

  用定量的结果，例如直接或间接的资金的损失，以及定性的结果，例如形象的损失、人员的伤亡、个人隐私的泄漏。
- IT 投资水平；
- 对 IT 系统及处理信息的显著的威胁；
- 脆弱点，包括使 IT 系统遭受已识别威胁的损害的弱点；
- 要求的安全防护措施，这些防护措施应与已识别的威胁相当；
- IT 安全的成本，例如，保护 IT 资产的支出（IT 安全的成本应作为 IT 系统所有者关系的成本的一部分予以考虑）；
- 外包提供者的关系以及选择准则（例如，计算中心，PC 支持）。

IT 安全需要策划的方法，不应该孤立的考虑。应在战略策略的过程中就体现其特征，然后确保从一开始就将安全策划和设计进系统中。在大多数情况下，后来增加一些防护措施会更昂贵，或甚至不可行。

13 IT 安全计划

IT 安全计划是一份文件，该文件规定了为实施 IT 系统安全策略而采取的各种协调的活动。

这一计划应包含在短期、中期和长期范围内所需要采取的首要的活动，以投资、运营成本、工作量的观点的相关成本，以及实施时间表。它应包括：

- 整体安全框架和设计；
- 对 IT 系统的简短评审，以确保与组织安全目标保持一致，评审结果用最大化的资金损失、尴尬和公司的形象等名义反映；
- 识别符合已评估的风险的防护措施，并经过管理层的保持和确认；
- 评估防护措施的保密性的真实水平，包括确定他们的有效性；
- 在给定系统或应用程序的情况下，残余风险评估的概述；
- 为实施防护措施，识别并规定各项活动以及他们各自的优先顺序；
- 防护措施实施的详细的工作计划，包括优先顺序，预算和时间表；
- 项目控制活动，包括：
  - ✧ 资源提供和职责分配；
  - ✧ 规定过程报告程序。
- IT 人员和最终用户的安全意识和培训要求；
- 安全操作和管理程序的开发要求。

此外，计划应包括程序，该程序规定了为确认前述的每个活动的条件和措施，包括计划本身的修改。

14 防护措施的实施

建立 IT 安全计划之后，就需要实施它。通常，IT 系统安全管理人员对此负责。在安全实施过程中，应牢记下列目标。应确保：

- 防护措施的成本保持在批准的范围内；
- 按照 IT 安全计划的要求正确地实施防护措施；
- 按照 IT 安全几乎的要求实施和管理防护措施。

大多数技术性的防护措施都需要用操作性的或管理性的程序作为补充，而不能通过单纯技术性的手段来实施。因此程序应得到直线管理人员的支持和执行。

安全意识和培训也被认为是一种防护措施。因为它的重要性，将在第 15 条款对意识进行讨论。安全意识同时应用于所有的人员，应对以下人员实施特定的安全培训：

- 负责 IT 系统开发的人员；
- 负责 IT 系统操作的人员；
- IT 项目和系统安全管理人员；
- 负责安全行政性管理的人员，如，访问控制。

当 IT 安全计划实施完成后，应进行批准在特定 IT 系统安全计划中规定的防护措施的实施的正式过程。获得批准后，为 IT 系统或服务授权以投入运行。在某些团体中，授权的过程被称为委派。

IT 系统或服务的任何显著的变化应导致 IT 系统或服务的重新检查、重新测试和重新批准。

15 安全意识

应在组织从最高管理层到用户的所有层次上实施安全意识方案。没有在所有用户层次人员

的接受和参与，安全意识方案不可能取得成功。用户需要理解他们对于方案成功的重要性。意识方案应传递有关公司 IT 安全策略的知识，并确保安全指南和适宜行为的完全理解。另外，安全意识方案应覆盖系统安全计划的所有目标。方案至少应阐述下列主题：

- 信息安全保护的基本需求；
- 安全事件对于用户以及组织的含义；
- 隐藏的目标、公司 IT 安全策略的解释和风险管理战略，从而完全理解风险和防护措施；
- 实施的 IT 安全计划及检查防护措施；
- 信息分类；
- 数据所有者的职责；
- 职责，工作描述和程序；
- 报告以及调查安全违规或企图的需要；
- 未按授权模式做的后果（包括惩戒措施）；
- 安全符合性检查；
- 变更和配置管理。

一个有效的安全意识方案将使用许多媒介，例如，小册子、手册、海报、视频、时事通讯、传递实践经验、车间、研讨会和演讲。重要的是，在实施意识方案时要考虑社会、文化和心理方面的因素并开发一个充分承认安全重要性的文化。

安全意识应关注组织内的每个人，并影响他们的行为，导致所有职责的增加。一个关键的因素就是让管理层意识到安全的需求。确保人员的安全意识是所有管理者职责的一部分。因此，他们需策划一个相应的预算。就大型组织而言，IT 安全意识是公司 IT 安全管理人员的职责。

安全意识方案的目的是使那些人员相信，存在着针对 IT 系统的威胁，以及信息损失、未授权的修改或删除可能对组织和雇员产生严重的后果。

最好能够组织与组织环境有关的意识会议。应给出相关的易于理解例子，如基于公司实际的例子，这些例子相对于那些新闻媒介报告的案例能够产生更大的影响。这样的会议为雇员和指导者之间的交互提供了更多的机会。

应监视雇员的防护措施的符合性，以评价安全意识会议的影响并评估会议的内容。如果结果不令人满意，那么就需要相应地修订安全意识会议地内容。

应定期报告安全意识会议，这样既可以更新原有人员的知识，有可以告知新人员。此外，应给予每个新员工、每个新调岗人员、每个新提升的人员新的职责方面的指导。将 IT 安全方面整合到其他课程中也是可取的。

需要强调的是，安全意识是一个持续的过程，永远没有终点。

16 后续活动

所有的防护措施都要求保持以确保以一种预期的和适宜的方式持续的运行。安全的这一方面是最重要的之一，但是通常只是得到最少的关注。更多的情况是，系统或服务已经存在，

而安全只是作为时候的想法而增加的，然后就被遗忘。忽略已经实施的防护措施已经称为一种趋势，对于保持或提高安全则根本不予以关注。此外，应通过策划的活动而不是偶然发现防护措施的荒废。此外，还需要检查安全的符合性，监视运行的环境，进行日志记录评审以及处置事件以确保持续的安全。

16.1 保持

防护措施的保持（包括行政管理），是组织安全方案最根本的部分。它是所有层次管理人员的职责，以确保：

- 分配组织的资源以保持防护措施；
- 定期对防护措施进行重新确认，以确保他们持续预期的运行；
- 当发现新的要求时升级防护措施；
- 建立清晰的保持防护措施的职责；
- IT 系统硬件和软件的修改和升级并不改变已存在的防护措施的预期性能；
- 先进的科技并不引入新的威胁或脆弱点。

当上述的所有维持活动都完成时，已存在的防护措施将持续预期的运行，避免代价高昂的负面影响。

16.2 安全符合性

安全符合性检查，也被称为安全审计和安全评审，是用于确保一致和 IT 系统安全策划一致性的非常重要的活动。

为了确保 IT 安全适当等级保持有效，实施符合和持续符合 IT 项目和系统安全计划中规定的防护措施要求的防护措施是至关重要的。对所有的 IT 项目和系统而言，这必须是真实的当：

- 设计和开发；
- 操作性寿命；
- 替换和处置。

安全符合性检查可以由外部或内部人员（如，审计员）实施，并且根本上基于与 IT 项目或系统安全方针相关的检查列表的使用。

应对安全符合性检查进行策划并将其整合到其他策划活动中。

现场检查在确定操作支持人员和用户是否符合特定防护措施和程序时尤其有用。

应实施检查以确保实施正确的安全防护措施，正确地实施，正确地使用，适当时还有正确地测试。当发现某些防护措施不符合安全时，应拟定并实施纠正措施计划，并对结果进行评审。

16.3 监视

监视是整个 IT 安全周期中至关重要的一部分。如果实施得当，它可以给予管理者一份清晰的印象：

- 与设定的目标和低限相比已经取得了什么；

- 无论结果是否令人满意和特定的发起人员在哪里里或不在哪里工作。

对于资产、威胁、脆弱点和防护措施的所有变化潜在的都可能对风险造成显著的影响，变更的早期检测允许采取预防措施。

许多防护措施产生安全相关事件的输出日志。对这些日志最起码应该进行定期评审，如果可能的话应使用统计技术进行分析，以尽早检测趋势的变化、不利事件的重复发生。如果仅仅将日志作为事后分析的工作，那么这其实是对一种继有潜力的、具有重要作用的安全机制的忽视。

监视应包括定期向相关的 IT 安全管理人员和管理层报告的程序。

16.4 事故处置

安全事故的发生是不可避免的。对每件事故的调查深度应与事故所造成的损害相适宜。事故的处置提供了对无意或蓄意破坏正常 IT 系统运行的响应能力。因此应开发适合于整个组织 IT 系统和服务的报告和调查计划。此外，还应考虑联合内部组织的报告计划以获得发生的 IT 安全事故、相关的威胁以及他们对 IT 资产和业务运行的想光影响方面的更加广阔的见解。IT 安全事故调查的基本目标是

- 以一种明智和有效的方式对事故作出响应；
- 从事故中学习，以此防止今后类似不利事故的发生。

一个包括提前定义的决策、有准备的行动计划将允许组织在合理的时间内作出反应，用辅助的方法限制进一步的损害和持续损害业务相关的区域。事故处置计划必须包括所有事故和行动的按时间顺序排列的文档。这应该有助于识别事故源。这是为达到第二个目标而形成的一个前提，也就是说通过提高防护措施减少今后的风险。事故的积极影响之一在于增加了对防护措施投资的意向。

重要的是进行事故分析并形成文件。文件应阐述下列问题：

- 发生了什么，什么时间发生的？
- 员工是否执行了计划？
- 员工是否可以按时获得所需的信息？
- 下次员工将提出什么样不同的建议？

回答这些问题将有助于理解事故。通过更新相关的 IT 安全策略和计划，这被轮流用来降低风险（例如，提高防护措施，减少脆弱点并变更安全意识方案）。

17 总结

第 2 部分讨论了与有效的 IT 安全方案有关的管理过程和职责。这些讨论希望让管理者熟悉主要的 IT 过程和在 IT 安全方面扮演角色的职能。本部分提供的信息可能不能直接用于所有的组织。尤其对于小型组织而言，不可能有全部的资源以完全实施所描述的某些功能。在这种情况下，用一种适宜于组织的方式阐述基本的概念和功能就显得很重要。即便是在一些大型的组织中，可能也无法象描述的那样精确地完成本部分讨论的功能。第 3 部分将检查可用于实现第 2 部分阐述的这些功能的几个技术。其他部分将阐述防护措施的选择以及适用于外部连接的特定防护措施。