信息技术
安全技术
信息技术安全管理指南

第 3 部分：IT 安全管理技术

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^_^。
本文件仅为网上共享学习之用，未经书面授权，不得用于任何商业用途。
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。

目录

1 范围

ISO/IEC TR 13335 第3部分介绍了IT安全管理的技术。这些技术都基于ISO/IEC TR 13335 第 2 和 3 部分中介绍的通用性指南。这些指南被设计用来帮助 IT 安全的实施。对第 1 部分介绍的概念和模型以及第 2 部分介绍的关于 IT 安全管理和策略的资料的深入掌握对于充分理解第 3 部分的内容至关重要。

2 引用标准

ISO/IEC TR 13335-1：1996 IT 安全管理指南－IT 安全概念和模型

ISO/IEC TR 13335-2：1997 IT 安全管理指南－IT 安全策划和管理

3 定义

ISO/IEC TR 13335 第 1 部分的定义适用于第 3 部分。第 3 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 3 部分共包括 12 个条款。第 5 条款介绍了有关本文档目的方面的信息。第 6 条款概述了 IT 安全管理过程。第 7 条款讨论了公司 IT 安全的重要性以及它应包含的内容。第 8 条款概述了组织用于识别安全需求的四种不同的方法。第 9 条款详细介绍了推荐的方法，紧接着第 10 条款描述了防护措施的实施。这以条款也对安全意识方案以及支持性过程进行了详细讨论。第 11 条款描述了为确保防护措施有效性所需的后续的几个活动。最后，第 12 条款对第 3 部分进行了简短的总结。

5 目的

第 3 部分介绍并推荐了用于成功实施 IT 安全管理的技术。这些技术可用于评估安全要求和风险，并有助于建立并保持适宜的安全防护措施，如，正确的 IT 安全水平。以这种方式取得的结果可能需要通过额外的由真实的组织和环境规定的防护措施予以提高。ISO/IEC TR 13335 本部分的内容与组织内所有负责 IT 安全的管理和/或实施的人员都有关系。

6 IT 安全管理技术

IT 安全管理过程基于 GMITS 第 1 部分和第 2 部分陈述的原则。适用于整个组织和组织的选择的一部分。图 1 展示了这一过程的主要阶段，以及这一过程的结果如何被反馈到其他的部分。无论是在阶段内，还是在完成一个或几个阶段之后，只要需要随时都应建立反馈环。这个图是 TR 13335 第 2 部分的图 1 的修订版，强调了 TR13335 第 3 部分关注的主题。

IT 安全管理包括：分析安全要求，建立满足这些要求的计划，实施计划以及保持和管理已实施的安全。这一过程以建立组织的 IT 安全目标和战略以及开发公司 IT 安全策略为起点。

IT 安全管理过程的一个重要部分就是评估风险和如何将风险降低到可接受的水平。需要考虑业务目标、组织和环境方面以及每个 IT 系统特定的要求和风险。

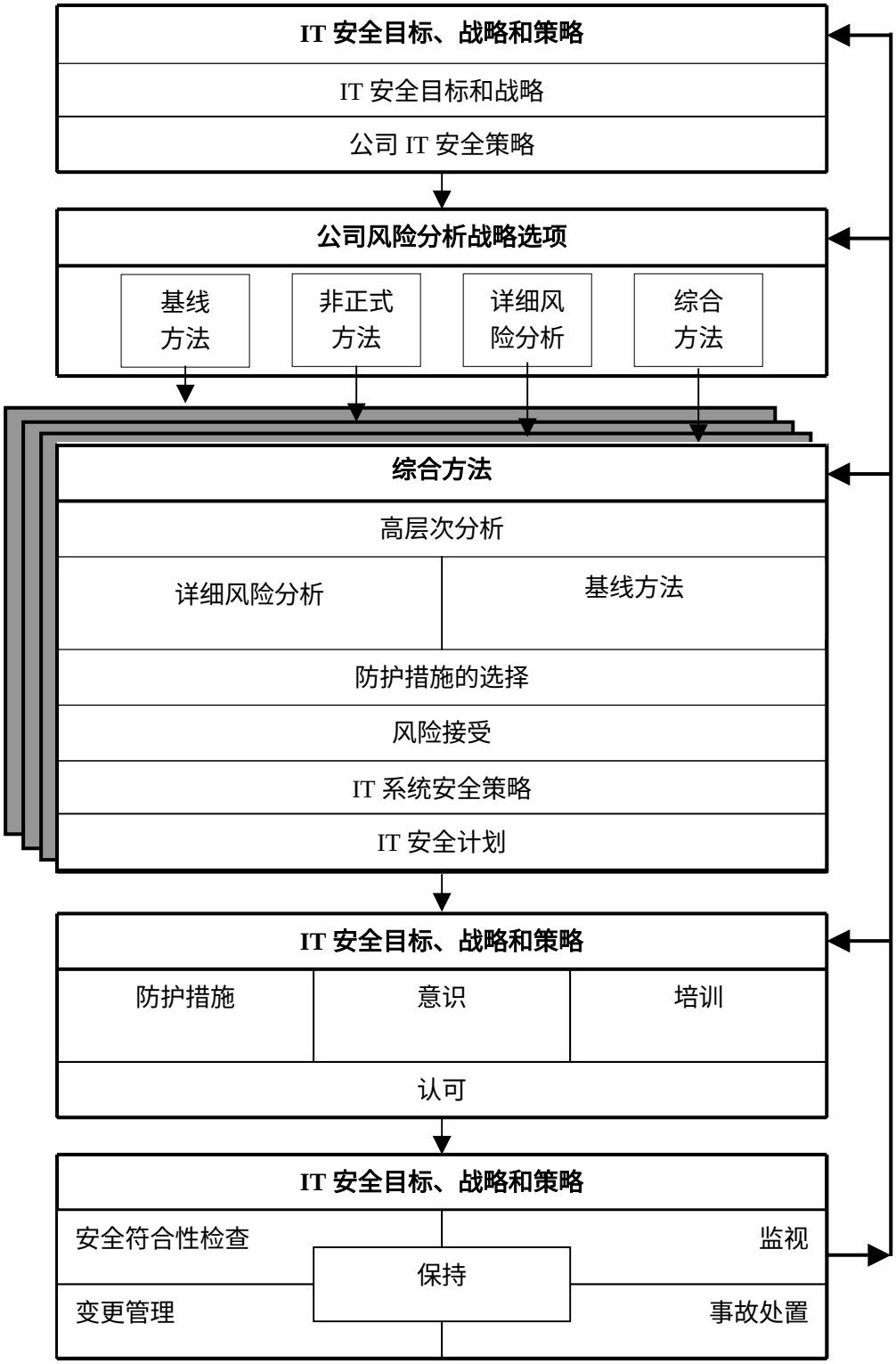

图 1：IT 安全管理

在评估 IT 系统和服务的安全要求之后，建议选择一个公司风险分析战略。主要的战略选项在后面的第 8 条款予以详细讨论。推荐的选项包括，对所有 IT 系统进行高层次的风险分析以识别处于高风险的那些系统。然后，这些系统通过详细的风险分析予以检查，同时对于其他系统应用基线方法。对于高风险系统，详细地考虑资产、威胁和脆弱点，导出详细地风险分析，从而有助于选择与已评估的风险相适宜的有效的防护措施。通过使用这种方法，风险管理可以集中关注那些存在显著风险或最大需求的区域，并使得整体的方案更加成本和时间有效。

伴随着风险评估，为每个系统识别适当的防护措施以将风险降低到可接受的水平。象 IT 安全计划列出的一样实施这些防护措施。实施应得到对防护措施有效性非常重要的意识和培训方案的支持。

另外，IT 安全管理包括处理不同后续活动的持续的任务，这些活动可能导致早期结果或决策的变更。后续的活动包括：保持，安全符合性检查，变更管理，监视和事故处置。

7 IT 安全目标、战略和策略

建立了组织的 IT 安全目标后，应开发 IT 安全战略以作为开发公司 IT 安全策略的基础。公司 IT 安全策略的开发对于确保风险管理过程结果的适宜和有效是至关重要的。为开发并有效地实施策略，需要整个组织的管理支持。非常重要的是，公司的 IT 安全策略应考虑公司目标和组织的特定方面。必须与公司的安全策略和业务策略保持一致。有了一致性，公司 IT 安全策略将有助于最有效地使用资源，并确保安全方法在一系列不同地环境中的一致性。

可能需要为每个 IT 系统开发单独的、特定的安全策略。这一策略应基于风险分析或基线的结果，并与公司 IT 安全策略保持一致，以及考虑与系统相关的安全推荐措施。

7.1 IT 安全目标和战略

IT 安全管理的第一步应考虑这个问题——什么宽度的风险对组织来说是可接受的。可接受风险的适当等级以及安全的适当等级是成功实施安全管理的关键。组要需要满足由 IT 安全目标确定的所需的安全 broad 等级。为评估这些安全目标，应考虑资产以及他们对资产的价值。着主要被 IT 具有的支持组织组织业务活动开展的重要性确定。IT 本身的成本只是其价值的一小部分。在评估组织业务活动对 IT 的依赖程度时可能面临以下问题：

- 哪些重要/非常重要的业务部分没有 IT 支持就无法开展？
- 哪些任务只有在 IT 的帮助下才能完成？
- 哪些重要的决策依赖于 IT 处理设施的准确性、完整性或可用性，或信息是如何更新的？
- 哪些处理的保密信息需要保护？
- 不期望安全事故对组织意味着什么？

回答这些问题有助于评估组织的安全目标。例如，如果重要/非常重要的业务部分依赖于

准确的或更新的信息，那么，组织的安全目标之一就可能是确保当信息被 IT 系统处理时信息的完整性和合时。同样，当评估安全目标时，应考虑重要业务目标以及他们与安全的关系。应在安全目标的基础上，就达到这些目标的战略达成一致。

IT 安全策略用通用术语简述了组织将如何达到它的安全目标。这样的战略应阐述的主题依赖于这些目标的数量、种类和重要性，通常是组织认为重要的、需要在组织范围内正式阐述的那些。主题的性质可以是特别单一的或非常宽泛的。

作为前者的一个例子，一个组织因为其业务的性质原因其所有的系统应保持一个高级别的可用性，可能有一个首要的 IT 安全目标。在这种情况下，一个战略目标可能定位于通过在组织范围内安装反病毒软件来减少病毒的攻击（或所有接收的软件都应通过推荐病毒的选择站点检测）。

为了在更广泛的水平上解释后者，组织可以有一个 IT 安全目标，因为它的业务就是出手 IT 服务，即向组织的潜在顾客证明其系统的安全。在这种情况下，一个战略目标可以是所有系统应经过经认可的第三方的验证以证明其是安全的。

因为特定的目标或将他们联合的原因，IT 安全战略其他可能的主题包括：

- 风险分析战略以及被组织范围内采纳的方法；
- 每个系统的 IT 系统安全策略需求；
- 每个系统的安全操作程序需求；
- 组织范围内信息敏感性分类计划；
- 安全沟通环境的需求，以及在与其他公司沟通前的检查；
- 通用的事故处置计划。

一经确定，安全策略和它的组成主题应包含在公司 IT 安全策略中。

7.2 公司 IT 安全策略

公司的 IT 安全策略应基于认可的公司 IT 安全目标和策略而产生。有必要建立和保持一个与公司业务、安全、IT 策略和与安全有关的法律法规一致的公司 IT 安全策略。

正如 7.1 条款反映的那样，影响公司 IT 安全策略的一个重要因素是一个组织在多大程度上依赖于它使用的 IT。IT 的用处越大，组织对其 IT 依赖越高，就需要越多的安全来保证业务目标的实现。在写公司 IT 安全策略的时候，应考虑文化的、环境的和组织的特点，因为它们可能影响针对安全的方法，例如，一些防护措施在一种环境中可能很容易被接受，但是在其他环境中就可能完全不被接受。

公司 IT 安全策略中描述的与安全相关的活动可以率先起草。起草应基于组织的目标和策略，以前的安全风险评审结果，后续活动的结果，如已实施的防护措施的的安全符合性检查、监视和评审 IT 安全的日常应用以及报告安全相关事故。需阐述在这些活动过程中检

测到的任何严重的威胁或脆弱点，公司的 IT 安全策略也应描述如何处理这些安全问题的组织的整体方法。详细的活动在各种 IT 系统安全策略或其他支持性文档中描述，如，安全操作程序。

在开发公司 IT 安全策略时，以下职能部门的代表应该参加：

- 审计；
- 财务；
- 信息系统（技术人员和用户）；
- 公共设施/基础设施（如，负责建设厂房和宿舍、供电和空调的人员）
- 人员
- 安全
- 高级业务经理。

根据安全目标和组织为实现这些目标而采取的战略，应选择适当详细水平的公司 IT 安全策略。公司 IT 安全策略至少要描述：

- 它的范围和目的；
- 与法律法规责任以及业务目标相关的安全目标；
- IT 安全要求，根据信息的保密性，完整性，可用性，可审计性，鉴权和可靠性。
- 覆盖组织和个人的责任和权力的信息安全管理；
- 组织所采纳的风险管理方法；
- 确定实施防护措施优先顺序的方法；
- 安全宽度水平和管理人员所寻找的残余危险；
- 访问控制的通用准则（对建筑物、房间、系统和信息的逻辑访问控制和物理访问控制）；
- 组织安全意识和培训的方法；
- 检查和保持安全的程序；
- 与所有人员沟通策略的方法；
- 应进行策略评审的环境；
- 控制策略变更的方法。

如需要更详细的公司 IT 安全策略，应考虑以下问题：

- 组织范围内的安全模型和程序；

- 标准的使用；
- 防护措施的实施程序；
- 后续活动的方法，如
  - 安全一致性检查；
  - 防护措施的监督；
  - 与安全有关的事故的处置；
  - 监视 IT 系统的使用。
- 雇用外来安全顾问的环境。

附录 A 给出了公司安全管理策略内容列表的例子。

正如这个条款中前面讨论的那样，前面风险管理评审、安全符合性检查和安全事故的结果可能会影响公司的 IT 安全策略。依次，可能需要对以前定义的战略或策略进行评审或修订。

公司的 IT 安全策略应经过最高管理层的批准，以确保对所有安全相关的措施的支持。

应编写基于公司的 IT 安全策略的指南，该指南对所有管理人员和员工都具有约束力。这可能要求组织内的每一个员工都在文件上签字，承认其安全职责。此外，应开发并实施安全意识方案。

应指定专人负责公司的 IT 安全策略，并确保策略反应了公司的要求和实际情况。这个人通常是公司的 IT 安全管理人员，他在其他事情中负责后续活动。这包括安全符合性评审，事故和安全弱点的处置，以及根据这些活动的结果可能需要的对公司 IT 安全策略任何变更。

8. 公司风险分析战略选项

注：为确保 ISO/IED TR 13335 这部分的完整和一致，并能不依赖 ISO/IEC TR 13335－－2 而阅读，该条款阐述了同 ISO/IEC TR 13335－2 中的条款 10 一样的主题。

在开始任何风险分析活动前，组织应为这一分析制定战略，其组成部分（方法，技术等）应在公司 IT 安全策略中形成文件。应在组织内就风险分析方法的选择方法和准则达成一致。风险分析战略应确保选择的方法适合环境，并集中安全努力于那些真正需要的地方。下面给出的选项描述了四种不同的分析方法。各种选项之间的基本区别是风险分析的深度。对所有 IT 系统进行详细风险分析是无效的，只是关注严重风险的外围也是无效的，因此需要在这些选项之间进行平衡。

除了什么都不做和接受会暴露给许多未知大小和严重程度的风险可能性之外，一个公司风险分析策略还有四种基本选项：

- 对所有的系统使用同样的基线方法，不考虑系统面临的风险，并接受并不总是恰当的安全水平；
- 使用非正式方法进行风险分析并且把注意力集中到那些被察觉到暴露于高风险的 IT 系统；
- 对所有系统使用正式方法进行详细风险分析；
- 开始时，进行“高层”风险分析来识别那些暴露于高风险和对业务有决定性作用的 IT 系统，继而对这些系统进行详细风险分析，并对其他所有系统采用基线安全。

在后面将讨论这些阐述安全风险的不同的可能性，然后对提出的方法做了个推荐。

如果一个组织决定在安全方面什么都不做，或者延迟防护措施的实施，管理人员应该清楚这个决定可能的含义。有时这不需要时间、金钱、人员和其他资源，但是有很多缺点。除非一个组织确信他的 IT 系统不是必要的，它可以把自己置于严重后果。一个组织可能会不遵守法律法规，如果它遭受安全的破坏，其名声可能遭受影响，并表明组织没有采取预防措施。如果一个组织基本不关注 IT 安全，或没有任何重要的业务系统，那么这可能是个可实行的战略。然而，组织处于一种不知道真正的形式是好还是坏的状态，对大多数组织来说这不太可能是一个好的解决方案。

8.1 基线方法

就第一个选项而论，一个组织可以通过选择标准防护措施对所有 IT 系统实施基线安全。在基线文档和操作指南中建议了各种标准防护措施。我们也可以在 9.2 条款中找到对这种方法更详细的解释。

这种方法有一些优点，如：

- 风险分析和每个防护措施的实施管理只需要最少数量的资源，并且在选择防护措施时花费更少的时间和努力；
- 基线防护措施可提供一个成本有效性的解决方案，因为如果组织的大量系统都在普通环境下运行并且如果安全需要类似，那么很多系统都可以采用相同或相似的基线防护措施而不需要太多的努力。

这种选项的缺点是：

- 如果基线水平设置的过高，有些 IT 系统可能会有过高的安全等级；如果基线水平设置的过低，有些 IT 系统可能会缺少安全，导致更高层次的暴露；
- 在管理与安全有关的变更时，可能会有苦难。例如，如果一个系统升级了，就很难评估原来的基线防护措施是否充分。

如果组织的所有 IT 系统只有低水平的安全要求，那么这可能是最具成本效率的战略。在这种情况下，必须选择能够反映大多数 IT 系统要求的保护程度的基线。多数组织将总是

需要满足最低标准以保护敏感数据并符合法律法规，如数据保护法。然而，当组织的系统在业务敏感度、规模和复杂性方面各不相同时，对所有系统实施通用的标准既不明智的也不具有成本有效性。

8.2 非正式方法

这一选项是实施非正式的、注重失效的风险分析。非正式方法不是基于结构化方法，而是利用个人的知识和经验。

这种选项的优点是：

- 一般不需要大量的资源或时间。进行这种非正式分析不需要学习额外的技能，而且要比详细的风险分析更加快捷。

然而，这种选项也有许多缺点：

- 没有几种正式的方法或广泛的检查列表，可能会增加丢失一些重要细节的可能性；
- 要证明为防范用这种方法评估的风险而实施的防护措施的合理性很困难；
- 在分析风险方面几乎没有任何经验的人对完成这个任务几乎毫无帮助；
- 一些方法以前已被脆弱点驱动，也就是说防护措施的实施是基于已识别的脆弱点，但是没有考虑是否真的需要这些防护措施；
- 存在一定程度上的主观性；评估者的特有的偏见也会影响结果；
- 如果进行非正式风险分析的人离开组织，可能会出现问题。

基于以上的缺点，这个选项对很多组织而言并不是一种有效的风险分析方法。

8.3 详细风险分析

第三种选择是对组织内的所有 IT 系统进行详细风险分析的评审。详细风险分析包括资产的深度识别和赋值，评估针对这些资产的威胁并评估脆弱点。然后这些活动的结果被用于评估风险和识别已被证明是合理的防护措施。这一方法将在 9.3 条款中详细描述。

这种方法的优点是：

- 有可能为所有系统识别出适当的防护措施；
- 详细分析的结果可用于安全变更管理。

这种方法的缺点是：

- 为了获得最佳结果，可能需要相当多的时间、努力和专业知识。关键系统的安全需求可能阐述的太晚，因为所有的 IT 系统都被同样详细的考虑，并且完成这个

分析需要大量的时间。

因此，并不建议对所有的 IT 系统都进行详细风险分析。如果选择了这种方法，就有许多可能的实施方法：

- 使用标准方法，来满足 TR13335 反映的准则（例如，9.3 条款中描述的方法）；
- 用适合组织的不同的方式来使用标准方法；使用‘ 风险模型技术 ’（在 9.3 条款中描述）可能会对一些组织有好处。

8.4 综合方法

第四种选择是先对所有的 IT 系统做最初的高层风险分析，每种情况下都集中于 IT 系统的业务价值和它所暴露于的严重威胁。对已识别的对组织的业务很重要和/或暴露于高风险的 IT 系统，应该优先进行详细风险分析。对所有的其他系统，应选用基线方法。这种方法从某种意义上来说，是 8.1 和 8.3 所描述的选项的最佳结合点，在最小化识别防护措施所花费的时间和努力的同时，又仍确保高风险系统被适当地保护之间提供了良好的平衡。

这种方法额外的优点是：

- 合并了初始的快速而简单的方法，可能获得对风险分析方案的接受；
- 使快速建立组织的安全方案的战略蓝图称为可能，也就是说有助于进行良好的策划；
- 可以把资源和金钱用到最有益的地方，并且优先阐述可能最需要保护的系统；
- 后续活动会更成功。

唯一的潜在缺点是：

- 因为最初的风险分析处于高层，并且潜在地不够精确，一些系统可能不会被识别为需要进行详细风险分析。然而，这些系统还是被基线安全覆盖。而且这些系统在任何需要检查是否需要不止一个方法的时候能被再次访问。

采用高层风险分析的方法，结合基线方法和适用时的详细风险分析，为大多数组织指明了最有效的前进之路。第 9 条款推荐了这种方法，并且会详细地检查它。

9 联合方法

这一部分为实施前面推荐的综合风险分析方法提供了指南。

9.1 高层风险分析

首先，需要进行最初高层风险分析以识别每个 IT 系统适用哪种方法（基线或详细风

险分析)。这种高层风险分析考虑 IT 系统及其处理信息的业务价值，以及从组织业务角度考虑的风险。关于哪种方法适合于哪个 IT 系统的决策的输入，可以从以下考虑中获得：

- 使用 IT 系统要实现的业务目标；
- 组织的业务依赖于 IT 系统的程度，也就是说，组织认为对其生存或有效开展业务至关重要的功能是否依赖于这一系统，或依赖于这一系统所处理信息的保密性、完整性、可用性、可审计性和可靠性。
- 这一 IT系统的投资水平，根据开发、维护或替换这一系统；
- 组织直接赋予 IT 系统的资产的价值。

评估完这些项目之后，就比较容易作出决策。如果系统目标对于组织业务开展非常重要，如果系统替代成本太高，或资产的价值处于高风险，那么就需要对这个系统进行详细的风险分析。这些条件中的任何一个都足以证明进行详细风险分析是合理的。

一个普遍适用的准则是：如果 IT 系统安全的缺乏能导致对一个组织，它的业务过程或它的资产产生重大危害或破坏，那么就需要进行详细的风险分析（9.3 条款）以识别潜在的风险。在其他情况下，实施基线方法（9.2 条款）可提供适当的保护。

9.2 基线方法

基线保护的目标是建立一系列最少的防护措施以保护组织的所有或部分 IT 系统。使用这种方法，有可能在组织范围内应用基线保护，并且像上面反映的那样，附加地使用详细风险分析评审以保护处于搞风险或对业务至关重要的 IT 系统。适用基线方法可以减少组织在实施风险评估评审（8.1 条款）方面所需的投资。

通过使用防护措施目录来识别适当的基线保护，该目录建议了一系列保护 IT 系统免受大多数常见威胁的防护措施。基线安全水平可根据组织的需要进行调整。不需要对威胁、脆弱点和风险进行详细评估。实施基线保护所需要做的全部工作就是从防护措施目录中选择那些与考虑的 IT 系统相关的部分。识别完已经存在的防护措施之后，需与基线目录中列出的那些防护措施进行比较。应实施那些尚未实施的或适用的防护措施。

基线目录可能会详细说明需要采用的防护措施，或者他们会建议阐述一系列的适用于考虑的系统防护措施的安全要求。这两种方法都有优点。在 ISO/IEC TR 13335—4 的附录中可以找到两种类型的目录。基线方法的一个目标就是在组织范围内保持安全防护措施的一致性，两种方法都可以达到这一点。

有几个文件已经提供了系列基线防护措施。并且，有时也可以考虑同行业公司间环境的相似性。在检查了基本需求之后，就可以参照基线防护措施的目录。例如，基线防护措施的目录可以从以下方面获得：

- 国际或国内标准化组织；
- 行业标准或推荐；

- 具有相似业务目标和规模相当的其它公司。

当然，组织也可以建立自己的基线，以适应自身的典型环境和业务目标。

8.3 详细风险分析

正如 8.3 条款所简要说明的那样，IT 系统的详细风险分析包括识别相关的风险并评估他们的程度。这通过不期望事件的潜在负面业务影响评估和他们发生的可能性来完成。不期望事件可能对业务、人员或组织的任何其他有价值的实体造成负面影响。不期望事件的负面影响由与处于风险的资产价值相关的可能损坏组成。发生的可能性依赖于资产对于潜在攻击者的吸引力、威胁发生的可能性以及脆弱点被利用的难易程度。风险分析的结果导致对安全防护措施的识别和选择，以将已识别的风险降低到可接受的等级。

详细风险分析包括对图 2 所示的每个步骤的深入评审，使得选择合理的防护措施成为风险管理的一部分。这些防护措施的要求将用文件化的形式在 IT 系统安全策略和相关 IT 安全计划中记录。许多可能影响系统安全要求的许多事故和外部影响，使得重新考虑部分或全部的风险分析成为需要。这些影响可能是：系统最近的显著变化、计划变更或需要处理的事故得后果。

通过对所有的系统进行详细风险评审，只需要必须的时间和金钱投资，就可以确定风险分析需求。而接下来的详细风险分析评审只针对高风险或关键系统，如 8.4 条款中所推荐的。可以使用自动的（计算机辅助）或基于产品的人工方法。

实施风险分析得方法有很多种，从基于方法得检查列表到基于技术的结构性分析。无论组织采用何种方法或产品，至少应说明后续条款中标识的主题，采用适合组织文化的方法也很重要。

一旦系统详细风险分析评审在第一时间完成，评审结果-资产及其价值、威胁、脆弱点和风险等级以及识别的防护措施-应被保留，例如存放在数据库中。很明显，使用软件工具支持的分析方法使这件事更容易。这种表述有时称之为模型，可用于随着时间的推移发生的显著变更的影响，这些变更可能是配置、处理的信息类型和威胁假设等。只有变化需要作为输入，以便确定对必需防护措施的影响。而且这样的模型可以用于快速检查不同的方法，如在系统开发过程中或用于另一个本质相似的系统。

9.3.1 建立评审边界

如图 2 所示，在为资产识别和赋值收集输入之前，应定义评审的边界。在这个阶段认证定义边界可以避免不需要的工作并提高风险评估的质量。边界描述应清晰定义当对考虑的系统进行风险分析评审时需要考虑下列那些内容：

- IT 资产（如，硬件、软件、信息）；
- 人员（如，职员、承包商、其他外部人员）；
- 环境（如，建筑物、设备）；

- 活动（运行）。

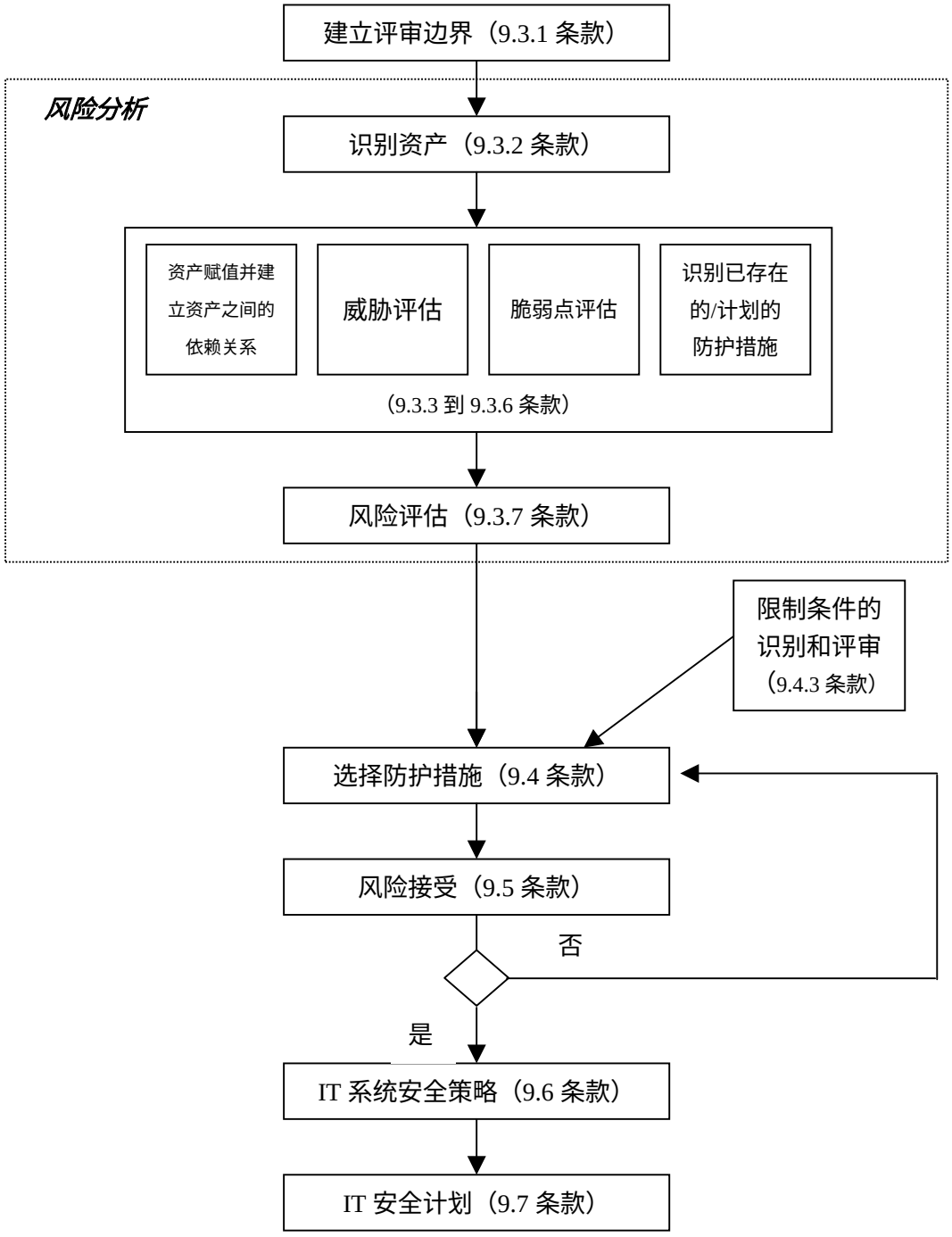

图 2：包含详细风险分析的风险管理

9.3.2 识别资产

资产是一个整体系统的组件或部分，组织直接为其赋值因此需要组织对其进行保护。当进行资产识别时，我们要记住 IT 系统不仅是由硬件和软件组成的。例如，资产类型可以是下列的任何一种：

- 信息/数据（如，包含支付细节的文件，产品信息）；
- 硬件（如计算机，打印机）；

- 软件，包括应用程序（如文字处理程序，为特定目的开发的程序）；
- 通信设施（如电话，铜电缆，光纤）；
- 固件（如软盘，只读存储器光盘，可编程只读存储器）；
- 文件（如合同）；
- 资金（如在 ATM 机中）；
- 制造的产品；
- 服务（如信息服务，计算资源）；
- 服务中的信用和信任（如支付服务）；
- 环境设备；
- 人员；
- 组织形象

建立的评审边界范围内（见 9.3.1）所有资产都要被识别。相反地，评审边界之外的任何资产，不管什么原因，都要进行其他的评审以确保他们没有被忘记或忽视。

9.3.3 资产赋值并建立资产间的依赖关系

在用列举评审范围内 IT 系统的所有资产的方式完成了资产识别的目的之后，应对这些资产进行赋值。这些价值代表了资产对组织业务而言的重要性。这可以用因信息和其他 IT 系统资产的泄漏、修改、不可用和/或破坏而造成的负面的业务影响来表达。因此，基于组织业务需求的资产识别和赋值是决定风险的主要因素。

资产的所有者和使用者应提供资产赋值的输入。开展风险分析的人员会列出资产。他们应该从那些参与业务计划、财务、信息系统和其他相关活动的人员处寻求帮助以每项资产的价值。资产的机制应与获得并维护这些资产的费用有关，还应与由于保密性、完整性、可用性、可审计性、鉴权和可靠性的丧失而造成的潜在的负面业务影响有关。识别的每项资产对于组织来说都应该是有价值的。然而，没有一种直接或简单的方法可以为所有的资产建立货币价值。因此，组织需要用非货币的术语，如定性的，来建立价值或重要程度。否则识别保护水平和确定组织为保护资产需要投入的资源的数量，都是困难的。例如，这样一个赋值的尺度可以是低、中和高的区别，或者，更具体一点：

可忽略的——低——中——高——很高。

在附录 B 中，通过考虑可能的损害给出了用于资产赋值的更详细的可能的尺度。无论使用那种尺度，在资产赋值过程中都要因以下情况所导致的可能的损害：

- 违反法律法规；
- 业务运行的损失；

- 信誉损失/名声上的负面影响；
- 个人私密信息的泄漏；
- 人身安全受到危害；
- 法律执行受到的负面影响；
- 商业秘密泄漏；
- 公共秩序的破坏；
- 财务损失；
- 业务活动中断；
- 环境安全受到威胁。

组织可能需要考虑其业务的其他重要准则，并将其添加到附录 B 中使用的准则。并且，组织必须定义其自己的损害限制象“低”或“高”。例如，一个资金损失对于一个小公司而言可能是灾难性的，而对一个非常大的公司来说则可能是低或可忽略的。

在这一阶段需要强调的是，评估的方法可以是定量的赋值，在定量的赋值是不可能的或不明智的情况下（如，潜在的人员丧生或业务信誉的损失），也可采用定性的赋值。应给出所使用的价值尺度的解释。

应识别资产对于其他资产的依赖。因为这可能会影响资产的价值。例如，应在数据处理的全过程中保持其保密性，也就是说，数据处理程序的安全需求应直接与代表被处理数据的保密性价值相关。并且，如果一个业务过程依赖于程序所产生的特定数据的完整性，这一程序的输入数据应具有适当的可靠性。此外，数据的完整性也依赖于用于存储和处理数据的硬件和软件。并且，硬件依赖于电力供应可能还有空调。因此，关于依赖的信息有助于识别相关的威胁和特定的脆弱点，也有助于确保给资产赋予其真正价值（通过依赖关系），由此确保保护的适当水平。

依赖于其他资产的资产的价值可以用下列方式予以修订：

- 如果依赖的资产（如，数据）价值低于或等于被考虑的资产的价值（如，软件），其价值保持不变；
- 如果依赖的资产（如，数据）价值较高，那么被考虑的资产的价值（如，软件）应根据下列条件予以增加：
  - ✧ 依赖的程度；
  - ✧ 其他资产的价值。

组织有些资产是可用性的而不是一次性的，象软件程序的拷贝或在大多数办公室使用的同样类型的 PC。当进行资产赋值时，应着重考虑这一情况：一方面，这些拷贝等容易被忽略，因此必须认真识别他们的所有；另一方面，他们可以用来减少可用性的问题。

这一步骤的最终输出是资产的列表以及资产的价值。资产的价值与泄漏（保护保密性)、修改（保护完整性)、不可用和破坏（保护可用性）以及替代的成本有关。

9.3.4 威胁评估

威胁是可能对评审的 IT 系统及其资产造成损害的源泉。如果威胁发生，就可能用导致不期望事件从而造成负面影响的方式对 IT 系统造成冲击。威胁可能来自于自然的或人为的，也可能是蓄意的或无意的。因识别无论是无意的还是蓄意的威胁源，并评估他们发生的可能性。关键是不要遗漏任何相关的威胁，因此这可能导致 IT 系统安全的失效或弱点。

应从资产的所有者和使用者，人事部门的人员，设施策划和 IT 专家以及负责组织保护的人员那里获得威胁评估的输入。其他组织如法人实体和国家政府权威机构也可以提供帮助，如通过提供威胁的统计资料。常见的可能威胁列表有助于实施风险评估。附录 C 中给出了个例子。然而参考其它威胁目录（对针对你的组织或业务）是值得的，因为没有目录可以无遗漏。一些最常见的威胁是：

- 错误和疏忽；
- 欺诈和盗窃；
- 雇员的蓄意破坏；
- 物理和支持性基础设施的损失；
- 恶意攻击，如，通过伪装；
- 恶意代码；
- 商业间谍。

在使用威胁目录或早期的威胁评估结果时，应该意识到威胁是在不断变化的，特别是当业务环境或 IT 发生变化时。例如 90 年代的病毒比 80 年代的复杂的多。此外还要注意到一个很有趣的现象，那就是防护措施的实施，如病毒检查软件，似乎总是导致了可以对抗现有防护措施的新病毒的开发。

识别完威胁源（谁和什么导致了威胁）和威胁目标（系统的什么元素会受威胁的影响）后，需要评估威胁的可能性。这应该考虑到：

- 威胁的频率（多长时间会发生一次，根据经验、统计资料等)，如果统计资料等可以运用；
- 动机，察觉到的和必要的能力，可能的攻击者可获得的资源，以及就蓄意的威胁源而言可能的攻击者所察觉到的 IT 系统资产的吸引力和脆弱点；
- 地理性因素，如靠近化学或右油工厂，处于可能发生极端气候条件的地区，以及就无意威胁源而言的那些可能影响人为错误或设备故障的因素。

出于正确性的需要，可能有需要把资产分成他们的组件，并考虑每个组件的威胁。例

如，一个物理资产可能刚开始会被看作“中心数据服务器”，但是当这些服务器处于不同的地理位置这一情况被识别后，应将其分成“中心数据服务器 1”和“中心数据服务器 2”，因为一些相关的威胁可能不同，并且其他的处于不同的水平。相似地，一个软件资产刚开始可能会被看作是“应用软件”，但是后来分为两个或更多的“应用软件”的例子。一个关于数据资产的例子，可以是在开始时它被确定为“犯罪记录”，但是后来分成“犯罪记录文本”和“犯罪记录图像”。

威胁评估完成时，会产生一个已识别的威胁列表，以及他们可能影响的资产或资产组，以及衡量威胁发生可能性的尺度，如，高、中或低。

9.3.5 脆弱点评估

评估包括识别物理环境、组织、程序、人员、管理、行政、硬件、软件或通信设备中的、可被威胁源所利用从而对资产以及资产所支持的业务造成损害的弱点。存在的脆弱点在本质上并不会导致损害，因为必须有显现的威胁利用它。没有相关威胁的脆弱点不要求实施防护措施，但是应当注意并监视其变化。需要注意的是，一个未被正确实施或失效的防护措施，或未被正确使用的防护措施，其自身就可能是一个脆弱点。

除了弱点之外，脆弱点还与资产使用的方式或目的的特性或性质有关，而不是在购买或制造资产时的预期特性或性质有关。例如，EEPROM（电可擦除可编程只读存储器）的特性之一就是上面存储的信息可以被擦除和替换。这是 EEPROM 的设计标准之一。然而，这个特性也意味着对存储在 EEPROM 上的信息的未被授权的破坏是可能的。因为允许存储信息被擦除的特性是一个设计标准，所以通常不认为它是一个弱点，但是它可能是一个脆弱点。

这个评估识别了可能被威胁利用的脆弱点，并评估了他们弱点的可能水平，也就是被利用的难易程度。例如，一些资产可能很容易被销毁、隐藏或传输－所有这些特性都会与脆弱点有关。应从资产的所有者和使用者，设备专家和硬件和软件方面的专家处获得脆弱点评估的输入。脆弱点的例子是：

- 未被保护的连接（例如因特网）；
- 未被训练的用户；
- 口令的错误选择和使用；
- 不适当的访问控制（逻辑的和/或物理的）；
- 没有信息或软件的备份拷贝；
- 位于易遭受洪水的地方。

在附录 D 中可以找到关于脆弱点的更多的例子。

评估脆弱点的严重程度是重要的，换句话说它们会多容易地被利用。脆弱点评估与在特定环境中利用它的每个威胁有关。例如，一个系统可能存在可被伪装用户身份和资源滥用的威胁所利用的脆弱点。因为缺乏用户鉴权，伪装用户身份的脆弱点可能会很高。另一方面，滥用资源的脆弱点可能比较低，因为即使缺乏用户鉴权，资源被滥用的方式是有限的。

这一步骤的结果应该是脆弱点列表和可被利用的难易程度的评估，例如，用高、中和低的尺度。

9.3.6 识别已存在的/计划的防护措施

伴随着风险分析评审的已识别的防护措施之外，还需要识别任何已经存在或计划的防护措施。识别这样的已经存在和计划的防护措施并将其作为这一过程的一部分对于避免额外的工作和成本是重要的，例如在成倍的防护措施中。也可能会发现已经存在的或计划的防护措施是不合理的。在这种情况下，应检查是否应将这个防护措施去除，用其他更适合的防护措施替代，或是否应该保持现状（如，因为成本的原因）。

另外，应进行检查以确定根据风险分析评审（见 9.4 条款）的结果所选择的防护措施是否与已存在或计划的防护措施兼容，选择的防护措施和已存在的防护措施不能相互妨碍。

在识别已存在的防护措施时，应进行检查以确定这个防护措施是否在正确地工作。依赖于正确的工作但在业务过程中不起作用的防护措施是一个可能的脆弱点的来源。

这一步骤的结果是所有已存在的和计划的防护措施的目录，已经他们的实施及使用状况。

9.3.7 评估风险

这一步的目的是识别和评估 IT 系统及其的资产暴露于的风险，以识别并选择适当的和合理的防护措施。风险是处于风险中的资产的价值的功能，导致潜在负面业务影响的威胁发生的可能性，脆弱点被己识别的威胁利用的难易程度，和任何已存在的或计划中的可以降低风险的防护措施。

有不同的方法来联系这些因素：如综合赋予资产的价值、脆弱点和威胁来获取测量风险的价值。对基于资产评估价值、脆弱点和威胁的不同种类的风险分析方法的详细考虑在附录 E 中可以找到。

无论采用什么方式来评估风险的尺寸，这一步的结果应该是考虑的 IT 系统的每项资产的泄漏、修改、不可用和破坏的每项影响的可测量的风险列表。此外，风险衡量有助于在选择防护措施时识别那些风险应首先被处理。使用的方法应该可重复和可追溯。

像前面反映的，许多自动软件工具可以被用来支持全部或部分的风险分析过程。如果一个组织决定使用工具，应小心确保使用的方法应与组织的 IT 安全策略和策略一致。并且，应该努力获得正确的输入，并进行面谈等活动，因为一个工具只能工作的像它的输入允许的那样精确。

9.4 选择防护措施

应识别和选择合适的和被证明是正当的防护措施，以将被评估的风险降到可接受的水平。为作出适当的选择，应考虑已存在的和计划中的防护措施、IT 安全架构和各种类型的

限制条件（见 9.3.6、9.4.2 和 9.4.3 条款）。

9.4.1 识别防护措施

应基于以前步骤所确定的风险的衡量，来识别适当保护所需的所有防护措施。

为了选择有效地抵抗评估的风险的防护措施，应考虑风险分析的结果。对关联威胁的脆弱点显示出哪里需要额外的保护，应该采取什么样的形式。

有许多的替代措施，可以根据考虑的防护措施的费用来决定。防护措施适用的领域包括：

- 物理环境；
- 人员；
- 行政；
- 硬件/软件；
- 通信。

应根据费用（包括维护）比较的原则来重新检查已存在的和计划的防护措施，如果它们不足够有效，要有除去（或无法实施）或改进它们的观点。这里需要注意的是，有时候去除一个不合适的防护措施的费用比维持现状的费用还要高，可以需要增加其他的防护措施。同样可能的是，一个防护措施可能为评审边界之外的资产提供保护。

考虑需要保护的脆弱点以及可能利用这些脆弱点的关联威胁，有助于防护措施的识别。通常来说，有许多降低风险的可能性：

- 避免风险；
- 转嫁风险（如，保险公司）；
- 减少威胁；
- 减少脆弱点；
- 减少可能的影响；
- 检测不期望事件，响应并从中恢复。

这些可能性中的那个（或他们的联合）是最合适的，依赖于环境。防护措施目录也可能有所帮助。然而，在在选择防护措施时，重要的是对他们进行裁剪以适合组织的特定需要。

防护措施选择的另一个重要方面是成本的因素。推荐那些实现和维护起来比它们设计的要保护的资产的价值还昂贵的防护措施是不合适的。推荐比组织分配给安全的预算还昂贵的防护措施也是不合适的。然而，需要非常谨慎，如果预算减少了要实施的防护措施的数量或质量，因为这可以导致对比计划的更大的危险的隐含接受。已建立的防护措施的预算，只

应作为一个需要仔细考虑的限制因素。

在选择基线方法来保护 IT 系统的地方，防护措施的选择相对简单。防护措施目录建议了一套保护 IT 系统抵抗最觉见威胁的防护措施。这些推荐的防护措施同存在的或计划的防护措施相比较，那些已经不存在的或策划的防护措施形成一个为获得基线保护而实施的防护措施列表。

防护措施选择应该总是包括操作性（非技术性）和技术性防护措施的平衡。操作性防护措施包括那些提供物理，人员和行政安全的防护措施。

物理防护措施包括内部建筑墙体的强度，密码门锁，消防系统和警卫。人员安全包括人员招聘检查（特别是在‘信任岗位’的人），员工监督和安全意识方案。

程序性安全包括安全操作程文件、应用开发和接受程序以及事故处置程序。与这一类别有关的，为每个系统开发合适的中断计划/灾难恢复战略和计划是非常重要的。这一计划应包括关键职能的细节和恢复的优先顺序，过程需要，以及如果发生灾难或服务中断时应遵循的组织程序。这样的计划必须包括在保护处理的敏感信息同时仍允许组织开展业务步骤。

技术安全包含硬件和软件安全以及通讯防护措施。这些防护措施根据风险来选择，以提供安全功能和保证。这个功能包括，例如，识别和鉴权、逻辑访问控制要求、审计踪迹/安全日志需求、拨号安全、信息鉴权和加密等等。保证要求用文件的形式规定了安全功能需要的信任水平，以及为确保这一水平所需要的检查和安全测试等的数量和类型。在决定操作性和技术性防护措施的良好混合时，会有不同的选择来实施技术安全需要。应对每个选择定义一个技术性安全框架来帮助识别安全可如要求的那样提供，并且用现有的技术是切实可行的。

组织可能选择使用己评估的产品和系统作为最终系统解决方法的一部分。所谓评估的产品是指那些已被第三方检查的产品。这个第三方可以是同一组织的另一部分或者是专门从事产品和系统评估的独立组织。评估可以逆着专门为被建设的系统创建的一套预先定义的标准执行，或它可能是可用于各种条件的通用的系列标准。评估标准可能规定功能要求和/或保证要求。已经存在一些评估计划，它们中的很多是由政府和国际标准化组织发起的。当要求所实施的系列功能是所要求的信任时，或当它需要这一功能实施的正确性和完整性的信任时，组织应决定采用被评估的产品和系统。

当选择实施的防护措施时，应考虑许多因素，包括：

- 防护措施的易用性；
- 用户的透明度；
- 提供给用户的实现其功能的帮助；
- 防护措施的相关强度；
- 执行的功能的类型—预防、威慑、探测、恢复、纠正、监视和意识。

一般来说，一个防护措施会履行不止一个这些功能——履行的越多越好。在检查整体的安全性或要使用的系列防护措施时，如果根本可能的话，应在各种类型的功能间保持平衡。这有助于整体安全的更有效和更有效率。可能要求进行成本效益分析和交替使用分析（一种方法，使用一系列与特定条件有关的用于衡量相关重要性的准则比较彼此竞争的替代方案）。

9.4.2 IT 安全框架

IT 安全框架作为整个系统框架的一部分，描述了一个 IT 系统的安全要求是如何被满足的。因此，在防护措施选择过程中要着重考虑 IT 安全框架。

当开发新系统和对现有系统进行较大变更时，可使用 IT 安全框架。基于风险分析或基线方法的结果，它提取了安全要求，并把它们改善成为一套为系统满足这些要求的技术性安全服务。在某些情况下，特别是对现有系统进行变更时，一些要求可以采用拟使用的具体的防护措施的形式

IT 安全框架关注于技术型的安全服务以及他们如何实现安全目标。在进行的过程中，需要考虑相关的非技术性的安全防护措施。即使这个构造可以用一些不同的角度和方法来建造，一个基本原则应被考虑。一定不允许一个独特的安全领域（有相同或相似的需求和防护措施的区域）的安全问题对另一独特安全领域的安全造成负面影响。正常情况下， IT 安全框架包括一个或多个安全领域。安全领域应尽可能紧密跟随组织使用的和已经建立的业务领域。这些业务领域可能跟随特定的业务功能分工，如工资表、制造或顾客服务，或者他们可能跟随业务服务分工，如，电子邮件服务或办公服务。

安全领域因一个或多个的以下性质而不同：

- 领域内可获得的信息的水平，种类或类型；
- 适用这个领域的操作；
- 领域内有关系的利益团体（COI）；
- 与其他领域和环境的关系；
- 功能的类型或领域内 COI 要求的信息访问。

在构建 IT 安全框架时，下列问题应予以阐述，包括：

- 特定安全领域间的相互关系和相互依赖；
- 削弱安全服务的相互关系和相互依赖的影响或含义；
- 为纠正、控制或对抗任何弱点所要求的额外的服务或预防。

IT 安全框架不是孤立的，而是依赖于其它文件并与其它文件交互。这些里边最重要的是系统框架和其他相关联的框架，如硬件、通信和应用程序。IT 安全框架不会包含对系统的完整的描述，它只阐述与安全有关的技术性的方面和组件。IT 安全框架的目的旨在在确保环境处于最佳保护的同时，尽可能减少对用户的负面影响。

许多文件与 IT 安全框架有关或依赖于它。这些文件包括：

- IT 安全设计；
- IT 安全使用概念；
- IT 安全计划；
- IT 系统安全策略；
- IT 系统认证和认可文件，如果需要。

9.4.3 识别/评审限制条件

有很多可能影响防护措施选择的限制条件。在进行推荐或实施过程中，必须考虑这些限制条件。典型的限制条件是：

时间限制：

可能存在许多类型的时间限制。例如，防护措施应在管理层能接受的时间段内实现。另外一种时间限制是，一个防护措施能否在系统的生命周期内实施。第三类时间限制可能是管理层所决定的那段时间，是可以接受把系统暴露给特定风险的一段时间。

资金限制：

计划实施的防护措施不应比它们被设计用来保护的资产的价值更高。应进行各种努力以不超出设计的预算。然而，在一些情况下，不大可能在预算限制内获得期望的安全和风险接受水平。因此，关于这种条件的解决方案就成为管理层的决策。

技术限制：

技术问题，像程序或硬件的兼容性，如果在选择防护措施的过程中考虑，那就很容易避免。并且，对现有系统的回顾性的的防护措施的实施经常被技术限制所阻碍。这些困难可能使防护措施的平衡向安全的程序或物理方面倾斜。

社会学的限制：

对防护措施选择的社会学限制可能对一个国家、一个部门、一个组织，甚至一个组织里的一个部门都是具体的。不可忽视他们，因为很多技术性防护措施依赖于全体员工的积极支持。如果员工不理解防护措施的需要或没有发现它在文化上可接受，经过一段时间之后，这个防护措施有可能就会失效。

环境限制：

环境因素可能影响防护措施的选择，如空间的可用性、极端的气候条件、周围的自然和城市地理，等等。

法律限制：

法律因素如个人数据保护或信息处理的犯罪密码提供，可能影响防护措施的选择。非 IT 专门法律法规如消防部门规定、劳务关系法等等，也会影响防护措施的选择。

9.5 风险接受

在选择防护措施和识别这些防护措施会实现的风险的削减后，总是会有残余风险——没有系统是绝对安全的。这些残余风险，对组织来说可分为‘可接受的’或‘不可接受的’。可以通过评审与那些风险相关的潜在的负面业务影响来获取这种分类。很明显，不可接受的风险在没有经过进一步考虑的情况下是不可容忍的。这些风险是否会因为其他限制条件（像成本，或简单预防的可能性——就像飞机撞击建筑物或地震的情况一样；然而从这些事故中恢复的计划还是可以做）而被接受，或者是否选择额外的和可能昂贵的防护措施来削减不可接受风险，是一个管理决定。

9.6 IT 系统安全策略

IT 系统安全策略应包含需要的防护措施的细节并描述为什么需要它们。系统的 IT 安全计划处理如何去实施它们。

很多系统需要它们自己的基于风险分析评估的安全策略。对大型和复杂的系统或介绍独特的和具体的而在组织的其他系统中没有的考虑的系统，这是通常惯例。IT 系统安全策略应与公司 IT 安全策略相容，并应避免任何冲突。它应在比公司 IT 安全策略低的水平上阐述问题。IT 系统安全策略基于风险分析评审和系统防护措施的识别的结果，并被根据被评估风险而选择的系列防护措施所支持。这些防护措施确保系统获得充分水平的保护。

IT 系统安全策略应基于下列信息，而不考虑公司使用的风险战略，而且应包含被考虑的系统为达到适当安全水平的所需的防护措施和程序。IT 系统安全策略和所有相关的支持性文件应涉及：

- IT 系统的定义以及组件和边界的描述（这一描述应保护构成系统的梭鱼哦的硬件、软件、人员、环境和活动）；
- IT 系统业务目标的定义——这会对系统的 IT 安全策略、风险分析方法的选择以及防护措施的选择和实施的有限顺序产生影响；
- 系统安全目标的识别；
- 对 IT 系统的依赖的宽阔程度，根据组织因 IT 系统的损失或损害而对组织业务造成多少危害，这一 IT 系统要实现的任务和处理的信息；
- IT 的投资水平，按照开发、维护和替换 IT 系统的费用和资本，运行和替代场所的费用；
- 为 IT 系统选择的风险分析方法；
- 组织要保护的 IT 系统的资产；

- 这些资产的价值，按照如果这些资产被损坏会对组织造成什么样的影响（信息含有的价值应根据因信息的泄露、修改、不可用和破坏而造成的潜在的负面业务影响来描述）；
- 对 IT 系统和处理信息的威胁，包括资产和威胁之间的关系以及这些威胁发生的可能性；
- IT 系统的脆弱点，包括对会被威胁利用的固有的弱点的描述；
- 作为以下结果的 IT 系统的安全风险：
  - ✧ 对组织业务的潜在负面影响；
  - ✧ 威胁发生的可能性；
  - ✧ 脆弱点被利用的难易程度。
- 为保护 IT 系统已识别的防护措施列表；
- IT 安全的估计费用

如果一个系统被证明只需要基线保护，那么提供以上标题涵盖下的信息是可能的，即使在一些情况下会有比进行详细风险分析的系统更少的细节。

9.7 IT 安全计划

IT 安全计划是一个定义了为实施 IT 系统所要求的防护措施所需采取行动的协作文件。这一计划应包含上述评审的结果，为在短期、中期和长期的时间框架内达到和保持适当的安全水平需要采取的行动，费用，以及一个实施计划表。它应包含每个系统的：

- 安全目标，按照保密性、完整性、可用性、可审计性、鉴权和可靠性；
- 为 IT 系统决定的风险分析选择（见第 8 条款）；
- 实施完识别的防护措施后，对期望的和接受的残余风险的评估（见 9.4 条款）；
- 选择的要实施的防护措施的列表（见 9.4 条款），以及一个已存在或策划的防护措施的列表，包括他们有效性的决定和防护措施需要的升级；这一列表包括：
  - ✧ 实施选择的防护措施以及升级已存在系统的优先顺序；
  - ✧ 这些防护措施如何在实践中工作。
- 这些防护措施的安装和运行费用评估；
- 实施这些防护措施以及后续活动所需人力资源的评估；
- 实施的详细工作计划，包含：
  - ✧ 优先顺序；
  - ✧ 与优先顺序有关的实施计划表；

- ✧ 需要的预算；
- ✧ 职责；
- ✧ 为确保防护措施的有效性所需的对 IT 人员和终端用户的安全意识和培训程序；
- ✧ 需要时，需采取的支持性过程计划表；
- ✧ 后续程序的计划表。

此外，IT 安全计划应描述用于控制纠正防护措施实施过程的便利条件，象：

- ➢ 定义报告程序的过程；
- ➢ 识别可能的困难的重新；
- ➢ 确认上面列出各点的重新，包括在需要时修订单个部分或计划本身的可能性。

这一步骤的结果应该是每个系统的详细 IT 安全计划，基于 IT 系统安全策略。IT 系统安全策略考虑了第 9 条款中描述的评审的结果。应确保防护措施及时地实施，依照 IT 系统的风险决定的优先顺序，并且要与如何实施防护措施和如何达到适宜的安全水平的描述相一致。还应包含维持这个安全水平的后续程序计划表。后续程序在第 11 条款中详细描述。

10 IT 安全计划的实现

安全防护措施的正确实施严重依赖于一个良好构造和文件化的 IT 安全计划。与每个 IT 系统相关的安全意识和训练应同步进行。当 IT 安全计划的实施完成时，在系统或设备投入实际应用前，需要批准所有的防护措施。

10.1 防护措施的实施

为了防护措施的实施，应执行在 IT 安全计划中描述的所有的必需步骤。负责这个计划的人（一般是 IT 系统安全管理人员），应确保遵循 IT 安全计划中列出的优先顺序和计划表。

为确保连续性和一致性，防护措施的文档是 IT 安全文档的一个重要部分。这个过程可用一些不同的方式实现。它应该是许多安全文件的一部分，也就是安全计划，中断计划，风险分析文件以及安全策略和程序。它应设被设计成满足经理、用户、系统管理员、维护人员和那些参与配置和变化管理的人员的需要。它需要是最近的和足够详细的来帮助消除安全过失和疏忽，也提供能保证安全操作被正确的和有效地执行的信息。很多文件，尤其是关于威胁、脆弱点和风险的，可能是极为敏感的必须保护以防止未经授权的泄露。因此，多数组织需要谨慎地处理这个文档并可能希望使用‘可信’的分发程序。如果使用这样的程序，他们也要用描述如何存储、访问和使用防护信息的敏感部分的方式予以文件化。此外，这个程序应识别谁对如何存储防护措施的决策负责，谁可以访问和使用它。在设计分发程序时，防护措施的可访问性应考虑特殊因素，如在灾难或其他不可预见的事故过程中，而时间非常关键，发现和使用中断计划的需要。最后，还需要对防护措施文档实施严格的配置控制，以确

保不能进行未经授权的变更。这些变更可能是无意的或无知的，但是可能降低防护措施的效果。

一旦 IT 安全计划被责任职能完成和结束，必须实施防护措施、安全符合性检查和测试。应实施安全符合性评审以确定防护措施已被正确实施，它们被有效地使用和恰当地测试。安全测试可作为这一评审的一部分来进行。测试是确保执行已被开展和正确完成的一种重要的技术。安全测试应被安全测试计划所指导。安全测试计划描述了测试方法、计划表和环境。如果评估的风险证明其合理性，那么可以使用穿透测试。应编写详细的安全测试程序和使用的标准化的测试报告。其目的是以一种方式来实施执行和测试。该方式确保 IT 安全计划的要求得到满足，风险像规定的那样被降低。

10.2 安全意识

安全意识方案的目的是将组织内将意识水平提高到安全成为一种习惯和过程变成全体雇员都能够很容易遵循的常规地步。方案应确保 IT 人员和终端用户具备 IT 系统（硬件和软件）的足够的知识，并且让他们理解为什么需要防护措施以及如何正确使用。只有当 IT 人员和终端用户接受防护措施时，防护措施才能真正的发挥作用。

安全意识方案的输入应来自于组织的所有层次。它应包括公司 IT 安全策略并且应覆盖组织 IT 安全计划的所有目标。意识小组需要所有部门的管理层支持。具体来说，下列主题应被安全意识方案中的课程、谈话或其他活动所覆盖：

- IT 系统的正确使用，包括硬件和软件；
- 安全对于组织和个人的重要性的解释；
- IT 系统的安全需要和目标，根据保密性、完整性、可用性、可负责任、鉴权和可靠性；
- 隐藏的目标和对公司 IT 安全策略、任何安全指南和指导以及风险管理战略的解释，从而理解风险和防护措施；
- IT 系统需要的保护及风险；
- 限制对 IT 区域（被授权的人员、门锁、证件、进入登记）和信息（访问控制、读/更新权力）的访问，以及为什么需要这些限制；
- 安全事故对组织和个人的含意；
- 报告安全的破坏或企图的需要；
- 程序、职责和工作描述；
- IT 人员和终端用户因安全原因而不能做的任何事情；
- 如果发生安全破坏，员工所需要负担的后果；
- 实施 IT 系统安全计划并检查防护措施；
- 为什么需要这些防护措施，以及如何正确使用它们；

- 有关安全符合性检查的程序；
- 变更和配置管理。

安全意识方案的开发以对安全战略、目标和策略的评审为开端。这一过程应由那些所在的岗位可以识别组织的关键性职能和获得高级管理层全力支持的一组人员来进行。

评审组必须根据公司的 IT 安全策略来确定要求的破坏。这应与整体的安全问题结合起来，并用各种形式发布，如意识海报、期刊、公司通告和内部邮件。

然后，这个小组应就安全关注点做一个特殊的简报。应对要求进行彻底的评审，以建立简报所需信息的基础。每个简报都应有固定的时间间隔（如每六个月）以确保所有员工都熟悉现代信息技术的固有的风险。

确定意识方案的目标和内容的职责应在高级管理层上分配给 IT 安全论坛(见 ISO/IEC TR 13335 第 2 部分)。其开发和实施职责应分配给公司 IT 安全管理人员和安全意识开发小组。这应该同公司其他的培训和教育活动联合起来做。然而，评审和熟悉他们工作环境的安全策略和程序是每个人的职责，因此，安全意识方案应在组织的所有层次上实施。

要开发一个成功的安全意识方案，下列组件应包括在其中：

10.2.1 需求分析

为确定目标群体（决策者，管理者和雇员）内已经存在的意识水平以及传递新信息给他们的最能接受的方法，需要进行安全知识需求分析。需求分析检查策略、程序、态度、安全知识和与目前真实表现相比的期望表现。

10.2.2 方案实施

一个广泛的安全意识方案应包括交互式的和促进的方法。一个安全意识方案这部分的关注点应是通过需求分析发现的不足。雇员需要获得这样的正确评价和理解，那就是 IT 资产是有价值的，对它们的威胁是真实的。

从这样一个组织性安全意识方案得到的好处是，它为雇员提供了一个参与安全方案的机会。交互式的方法（员工会议、训练课程等）提供了允许参与者和安全人员确认源自需求分析的概念和要求双向交流的机会。促进的方法（视频、电子邮件安全标志、海报、出版物等等）是是单向交流方式，它们允许管理层以一种廉价的方式广泛传播概念，信息和态度。

10.2.3 安全意识方案的监视

这里有两个包含对安全意识方案实施有效监督的不同部分：

- 定期的表现评估——通过监视安全相关的活动来确定一个意识方案的有效性，并识别那里可能需要变更，以促进方案的实施；

- 意识变更管理——只要整体安全方案变更（也就是，策略或战略变化、引入新资产或技术、威胁的变种出现等等），就需改变安全意识方案以更新现存的技术和技巧水平来反映这些变化。

10.3 安全训练

除了适用于组织内每个人的通用安全意识方案之外，还需要对履行与 IT 安全相关的任务和职责的人员进行专门的安全培训。安全培训的深度应依赖于 IT 安全对组织的整体重要性，也应该根据实施角色的安全需要而变化。如果需要，应该提供更广泛的教育如参加高校讲座、课程等。应开发覆盖所有与组织有关的安全需求的 IT 安全培训计划。在确定哪些员工需要专门的安全培训时，应考虑以下因素：

- 对 IT 系统的设计和开发负主要责任的人员；
- 对 IT 系统操作负主要责任的人员；
- 公司、IT 项目和 IT 系统安全管理人员；
- 负有安全管理职责的人员，如访问控制或通讯录管理。

另外，需检查现有的和计划的任务、项目等是否需要特殊的安全培训。只要有特殊安全要求的任务或计划一开始，应确保在项目启动之前就开发出相应的安全培训方案，并且活动要按时开展。

安全培训课程的主题应依赖于参加培训的角色和职能。一般问题可以是：

- 安全是什么：
  - ✧ 预防保密性、完整性和可用性的破坏；
  - ✧ 对组织或个人的潜在的负面业务影响；
  - ✧ 信息敏感度分类方案。
- 整体的安全过程：
  - ✧ 整体过程的描述；
  - ✧ 风险分析组件。
- 防护措施和须符合防护措施的培训；
- 角色和职责；
- IT 系统安全策略。

防护措施的正确实施和使用是安全培训方案所覆盖的最重要的问题之一。当然，每个组织必须根据自己的需要和已经存在或计划的防护措施来开发自己的安全培训方案。以下是与应被涉及的主题相关的防护措施的例子，重点在于平衡非技术性和技术性防护措施的需要：

- 安全基础设施：
  - 角色和职责；
  - 安全策略；
  - 定期的安全符合性检查；
  - 安全事故处置。
- 物理安全：
  - 建筑物；
  - 办公区域，设备房间；
  - 设备。
- 人员安全；
- 介质安全；
- 硬件/软件安全：
  - 识别和鉴权；
  - 访问控制；
  - 记帐清单和安全审计；
  - 实际存储清除；
  - 通信安全；
  - 网络基础设施；
  - 网桥、路由器、网关、防火墙；
  - 因特网和其它外部连接。
- 灾难恢复/业务连续性计划。

10.4 IT 系统的批准

组织应对所有或选择的 IT 系统使用批准过程，以确保他们满足 IT 系统安全策略和 IT 安全计划的要求。批准过程应基于如安全符合性检查、安全测试和/或系统评估这类技术。程序可根据内部或外部标准，执行批准过程的主体可能是组织内部的或外部的。

批准过程旨在确定 IT 系统实施和维持的安全防护措施提供适当水平的保护。它对于已定义的运行环境和在 IT 系统安全策略或计划中陈述的已定义的时间阶段有效。当已实施的安全防护措施或安全相关操作程序发生显著变化时，可能需要重新批准。IT 系统安全策略中应包括激发重新批准的准则。

批准过程主要包括文件评审、物理检查和技术性评估（也就是安全符合性检查）。为

了实现这一目标，需阐述下列关键问题：

- 须策划批准的过程，从而裁剪特定 IT 系统的方法；这个第一步也有助于定义计划表、需要的资源和职责；
- 应收集这个过程中应用的文件；
- 应进行文件评审以检查它们的完整性和同其他文件的内部一致性；
- 应完成 IT 安全计划中描述的准则的逆向评审和测试；
- 应形成报告，该报告总结了批准过程的结果，并陈述系统安全是否有全部的、部分的、有限的或根本没有批准，任何放弃和他们的有效期，以及处理过程中的任何限制；
- 如果 IT 系统或其环境发生变化，应重新批准；在一个批准期结束时也应发生。

一旦批准过程完成，就应实施后续程序。后续活动将有助于检测和调查系统及其安全和环境的变化。伴随着检测还需实施升级，在这种情况下需要进行重新批准。

对于一个组织而言，可能需要以及已达成的基线安全或实践指南来批准贸易伙伴的 IT 系统：

- 希望建立自己的基线安全或实践指南的剪裁版本，并在允许连接到其 IT 设施之前，为了符合性和批准的目的，将其传达给它的供应商/贸易伙伴；
- 同其他公司进行贸易往来并希望进行 IT 连接，但是在这么做之前，需作为一个整体来展示一个可接受的依据基线安全或实践指南的安全轮廓；
- 希望建立安全风险水平和安全轮廓。安全风险水平与其他公司连接到本公司 IT 设施相关。安全轮廓将排除其他公司的连接。这将使公司有能力执行批准，基于安全符合性检查所揭示的与基线安全或实践指南其他部分的符合性。基线安全或实践指南应与它的安全轮廓保持一致。

11 后续活动

即使经常被忽视，后续活动是 IT 安全的最重要的方面之一。已实施的防护措施只有它们在实际业务周期中被检查时才能有效地工作。必须确保它们被正确地使用，并且检测和处置任何的安全事故和变更。后续活动的主要目的是确保防护措施像实施的那样继续发挥作用。经过一段时间后，任何服务或机制的表现都有退化的趋势。后续活动预期用来检测退化并发起纠正措施。这是保持保护 IT 系统所需的安全水平的唯一方法。本条款所描述的程序构成了一个有效的后续活动方案的基础。IT 安全管理是一个持续的过程，不应在实施完 IT 安全计划后就止步不前。

11.1 保持

多数防护措施都需要保持和管理支持以确保在他们的生命周期内履行正确和适当的

功能。应对这些活动进行策划（维持和管理），并在一个固定的计划基础上实施。这种方式可以缩减费用并且保护了防护措施的价值。

需要进行定期检查以检测失效。从未检查过的防护措施几乎没有价值，因为没有办法知道可以依赖它什么。

保持活动包括：

- 清空日志文件；
- 修改参数来反映变化和附加物；
- 种子价值和计数器的再初始化；
- 用新版本升级。

当在不同的防护措施间进行评估和选择时，应将保持和管理的非要作为一个影响因素予以考虑。这是因为保持和管理的费用在不同防护措施中会有很大差别。因此，这常常成为防护措施选择中的重要决定因素。一般来说，只要可能，都希望将保持和管理的费用降至最低，因为它们代表的与其说是一次性费用，还不如说是重复的费用。

11.2 安全符合性检查

安全符合性检查是对已实施的防护措施的评审和分析。它被用来检查 IT 系统或服务是否遵守了在 IT 安全策略和 IT 系统安全计划中文件化阐述的安全要求。安全符合性检查也可用来检查以下的符合性：

- 在他们已经被实施完成后的新的 IT 系统和服务；
- 经过一段时间（如，每年）后，存在的系统或服务；
- 当改变 IT 系统安全策略时，已经存在的 IT 系统和服务，判断哪种调整对保持所需的安全水平是必要的。

安全符合性检查可由外部或内部人员来实施，并且基本上基于与 IT 系统安全策略相关的检查列表的使用。

可通过下列方法检查保护 IT 系统的防护措施：

- 进行定期的检查和测试；
- 监视抵抗实际事故发生的操作性能力；
- 实施地点检查，以检查安全水平的状态和在特定敏感或关注区域的目标。

为帮助做任何安全符合性检查，关于 IT 系统的活动的有价值的信息可以从以下方面获得：

- 用于记录事件的软件包的使用；
- 使用审计踪迹，以追溯时间的全部历史。

为了批准和其后的定期检查，安全符合性检查必须基于达成协议的、源于最近一次风险分析的结果的防护措施列表，基于 IT 系统安全策略以及 IT 管理层已经签署的安全操作性程序，包括事故报告。目的是确定防护措施是否被实施，是否正确实施，是否正确使用、和那里有关、是否被测试。

一个安全符合性检查者/视察者应在正常工作日内穿过建筑，并观察防护措施被使用的方式。访问当然也重要——但是结果应尽可能多的被交叉检查。某人所说的可能就是他认为的，但是事情可能并非如此：与他的同事进行交叉检查。

这帮助获得一个广泛的检查列表和同意的报告格式——这些不能被低估。这些检查列表应包括通用的识别信息，例如配置细节、安全责任、策略文档、周围地点。物理安全应阐述外部方面，像外部建筑，包括检修孔盖的可访问性，和内部方面，如建筑的完好、锁、火灾检测和预防（包括警报方面），同样的，水/液体检测，断电等等。

有许多需要检测的东西，如：

- 对物理渗透或绕行控制开放的区域；例如，应位于键区和卡系统下面的操作的门下面的楔形物；
- 不正确的机械，或机械的不正确的安装，如缺少或很少分配，或错误类型的探测设备。烟/热探测器对这个地方是不是充足，是不是在正确的高度？是否存在对警报的充分响应？警报是否适当地与一个控制点相连？是否有新的危险源——有人忽然使用一个房间来存放易燃品？是否有足够的电力备份和故障程序？是否使用了正确类型的线缆，是否位于锋利盘子的边缘？

为了检查其他安全方面存在的安全差劲，下列问题可能会有帮助：

- ***人员安全***，注意雇佣的程序。真的收到介绍信了么？检查雇用差距了吗？人员确实明白和了解安全吗？是否依赖关键职能的某个人呢？
- ***管理安全***，文件是如何真正处置的？一般使用的文件是最新的么？风险分析、状态检查和事故报告实施上像它们应该的那样被使用了吗？中断计划的覆盖面是正确和通用的吗？
- ***硬件/软件安全***，在要求的水平有无冗余？用户身份/口令选择和程序是如何好？审计追踪包括错误登陆和可追溯问题到正确的粒度和选择了吗？评估的产品满足了同意的要求吗？
- ***通迅安全，***有没有要求的冗余？有没有拨号设备，需要的设备和软件在适当的位置和被适当地使用吗？如果需要加密和/消息鉴权，关键的管理系统和相关的操作如何有效？

总的来说，安全符合性检查不是个小任务，要成功地完成它确实需要丰富的经验和知

识。这一活动和内部审计评审是不一样的。

11.3 变更管理

IT 系统及其运行环境是不断变更的。这些变化是新特征和服务可用性的结果，或者是发现新威胁和脆弱点的结果。这些变更也可导致新的威胁和脆弱点。IT 系统的变更包括：

- 新程序；
- 新特征；
- 软件升级；
- 硬件更新；
- 包括外部群体和匿名群体的新用户；
- 附加的网络和内部连接。

当 IT 系统策划或发生变更时，只要可能，确定变更对于系统的安全造成什么影响是非常重要的。如果系统有一个配置控制委员会或其它组织结构来管理技术性系统变更，IT 系统安全管理人员或其代表，应被分配到委员会中，并赋予作出关于变更是否会影响安全、如果是如何影响的决策的职责。对于包括购买新的硬件、软件或服务的重要变更，需要进行分析以确定新的安全要求。另一方面，系统的许多变更本身较小，不需要重大变更所需的那种广泛的分析，但是确实需要一些分析。对于这两种类型的变更，都需要进行考虑收益与成本的风险分析。对于较小的变更，可以在会议上非正式地实施，但是结果和管理决策应记录在文件中。

11.4 监视

监视是一项持续的活动，它检查系统及其用户和环境是否保持在 IT 安全计划所展示的安全水平。应准备日常的监视计划，为确保持续的安全运行提供额外的指南和程序。应定期咨询用户、操作人员和系统设计者，以确保所有安全问题被充分地阐述和 IT 安全计划保持最新。

为什么监视是保持 IT 安全的一个重要部分的原因之一，是它是检测与安全相关变化的一种方法。应被监视的一些方面是资产和它们的价值、资产的威胁和脆弱点以及保护资产的防护措施。

监视资产以检测他们价值的变化和 IT 系统安全目标的变化。这些变化的可能原因是以下的变化：

- 组织的业务目标；
- IT 系统中运行的应用程序；

- IT 系统处理的信息；
- 组织的 IT 设备。

监视威胁和脆弱点以检测他们严重程度的变化（例如，由环境、基础设备和技术可能性的变化引起的），并在早期检测其他威胁和脆弱点的出现。资产的变化可能会影响威胁和脆弱点的变化。

监督防护措施以检查随着时间的推移他们的成绩和效力。应确保它们是充分的并按照所需的保护水平来保护 IT 系统。资产、威胁和脆弱点的变化有可能影响防护措施的效力和充分性。

另外，当引入新的 IT 系统或对存在的系统进行变更时，可能需要确保这样的变更不影响已存在的防护措施的状态，并确保新系统的引入伴随着充分的的防护措施。

在发现安全异常时，需要为防护措施的可能评审而进行调查并向管理层报告，或者，在严重的情况下，调查 IT 系统安全策略评审并启动风险分析活动。

为确保与 IT 系统安全策略保持一致，应投入适当的资源以维持日常监督的适当水平：

- 已存在的防护措施；
- 引入的新系统或服务；
- 对已存在的系统或服务策划的变更。

很多防护措施以事件发生日志的形式产生输出。应使用统计技术对这些日志进行分析，以允许趋势变化的早期检测，并检测重复发生的事故。应分配分析这些日志的职责。

在分布式环境中，日志可能只记录有关单个环境的信息。为了真正理解复杂事件的本质，需要把不同日志的信息合到一起并把他们合并成一个单独的事件记录。应将这些合并的事件记录用于分析。事件记录合并是个复杂的任务，它的最重要的方面是自信地识别允许不同日志记录合并的那些参数。

控制日常监视的管理方法是为所需的活动准备一个计划。这个计划描述了为了确保保持所有系统和服务安全水平并且不随着时间的推移而被破坏的所有要求的活动。

更新安全配置的程序应形成文件。它们应包括调整安全参数和更新任何安全管理信息地界面。必须记录这些变化并被配置管理过程记录批准。应建立实施常规维护的程序以确保安全不被损害。适用时，应为每个安全组件描述可信的分发渠道。

需描述监视安全防护措施的程序。应陈述安全日志评审的方法和频次。应描述所使用的统计分析方法和工具。应就如何在不同操作环境下调整审计门槛给出指导。

11.5 事故处置

为识别风险并衡量他们的严重程度，已经强调了所需的风险分析。需要关于安全事故的信息来支持风险分析和提高结果。这个信息应该用一种安全的方式收集和分析，可以认为是提供收益。因此，实施适当构建和组织的 IT 事故分析计划是很重要的，并且他们收集和处理的信息应该可以用来支持风险分析和管理以及其他安全相关的活动也很重要。

为了获得成功并满足用户和潜在用户的需要，IAS 应基于用户的要求构造。此外，在任何现场操作之前，安全意识方案中需要一个重要的事故处理范围，以确保可能涉及的全部人员理解 IAS 包括什么、提供的好处和获得的结果如何应用到：

- 提高风险分析和管理评审；
- 帮助事故的预防；
- 提高 IT 安全相关问题的意识水平；
- 使用诸如计算机应急响应小组（CERTs）提供预警信息。

任何一个 IAS 应阐述的与这些有关的重要方面是：

- 当不期望事件发生时，处理他们的预先确定的计划建立，无论是由外部或内部的逻辑和物理攻击导致的，还是事故、设备故障或人为错误所引起的；
- 任命的事故调查人员的培训，例如，组成 CERTs.

CERTs 可能或多或少地被正式化作为定义的一组人。他们调查 IT 事故的起因，研究潜在的未来的发生，或对历史数据进行定期的研究和分析。其结论可以提高补救措施。

有了计划和经过培训的人员，当发生不期望事件时，可以避免草率的决定，可以保存可用于追溯和识别事故源的证据，可以更迅速地建立对有价值资产的保护，可以减少事故和响应的成本。此外，可以减少任何负面地公开。

任何组织都应为事故准备和计划一个处于适当位置的有效的 IAS，包括：

- 准备——预先文件化的预防措施，事故处置指南和程序（包括证据保护，事件日志的维护和处理公共关系），需要的文件和中断计划；
- 通知——报告事故的程序、方式和职责，以及向谁报告；
- 评估——调查事故和决定它们严重性的程序和职责；
- 管理——处置、限制事故的损害、根除事故以及通报给高级管理层的程序和职责；
- 恢复——重新建立正常服务的程序和职责；
- 评审——事后措施的程序和职责，包括法律的牵连和趋势分析。

值得强调的是，尽管单个组织可以从 IAS 的使用中获得益处，一些组织可能认为同其它组织共享事故信息以提供获取警报、快速识别趋势和激活保护的更加宽广的基础，以产生更多的益处。为了推动这一想法，应使用一个 IAS 数据库结构，它足够灵活可以覆盖所有的（所有部门，威胁类型和影响）要求和部分的威胁/影响特定的需要。无论是内部或外部组织，每个连接到 IAS 的将都使用相似的拓扑、尺度和结果来记录事故信息。这将允许比较和分析。使用一个通用的结构对于更广泛结果的可用性非常关键，尤其是对于一个更坚实的快速警报识别基础而言，在某些情况下这些警报不能通过单独的 IAS 被识别。

如上所示，IAS 和风险分析和管理方法之间接口的完成可以显著地改进结果，从而增加了要从 IAS 获得的好处。

关于威胁发生的信息会极大地改善威胁评估的质量，进而风险分析的质量。此外，在事故调查或事故过程中，可能会收集到新的和额外的关于脆弱点和它们被利用的方式的信息。利用 IAS 使用户能够识别并评估脆弱点，从而给风险分析方法提供有价值的输入。这会部分基于被介绍的关于威胁的信息，和部分基于 CERTs 所说的事故调查结果。例如，逻辑渗透的威胁（攻击者的存在和被处理信息的吸引力）可以联合逻辑渗透的脆弱点（访问控制机制的不充足或缺乏），从而产生风险。因此，为识别和评估脆弱点，可以通过使用已经输入数据库的那些已经被报告的事故的威胁信息，并联合其他来源的信息，尤其是 CERT 可能揭示以前未识别的脆弱点的调查和研究，从而使用 IAS。

需要注意的是，IAS 根据己报告的关于己发生事故的数据起作用。因此，任何 IAS 都不能直接提供那些可能在用户组织中已经出现但在 IT 事故中还未被发现的脆弱点的信息。此外，在进行统计和趋势分析时应谨慎使用 IAS 数据，因为输入可能会不完整或错误识别。然而，CERT 的调查结果可能就以前的未预见的脆弱点提供一些看法。总的来说，为风险分析和管理评审所做的 IAS 的定期输入，有助于提高威胁、风险和脆弱点评估的质量。

12 总结

第 3 部分检查了一些对 IT 安全管理很重要的技术。这些技术基于第 1 部分提供的概念和模型以及第 2 部分讨论的管理过程和责任。本部分的讨论展示了风险分析四种可能策略的优点和缺点。联合方法和几个对它的实施有用的技术被详细地描述。一些组织，特别是小组织，可能不会确切地以被描述的方式来实现这部分提供的所有方法。然而，以适合组织的方式来阐述每个技术，是重要的。

附录 A:公司 IT 安全策略内容目录示例

内容

附录 B：资产赋值

（非正式版）

组织资产的赋值在整个风险分析过程中是必不可少的步骤。为每项资产赋予的价值应用与资产和包括的业务实体有关的术语表示。要进行资产赋值，组织首先要识别它的所有资产。为保证所有资产都被考虑到，把它们按类型归类是很有帮助的，如信息资产、软件资产、物理资产和服务。指定一个负责确定资产价值的资产所有者也很有价值。

下一步是就要用的量度和为资产赋予特定价值的标准达成一致。由于多数组织资产的多样性，有可能一些有已知的货币价值的资产会被用当地货币单位来估价，而其它的有更多的可以被赋予定性价值资产，可被赋予从“很低”和“很高”范围内的价值。组织可以根据自己的喜好来选择基于量度的定量方法或定性方法，但是要与被赋值的资产有关。

资产的定性赋值的典型术语包括：可忽略的，很低，低，中等，高，很高和灾难的。适用于组织的术语的选择和范围主要依赖于组织的安全需要、组织的规模和其它组织的具体因素。

用作为每个资产赋予价值的基础的准则应用明确的术语写出。这经常是资产赋值最困难的方面之一，因为许多资产的价值要被主观地确定，并且可能会有很多人做决策。用于确定资产价值的可能标准包括：它的初始费用、它的替代和再创造费用或者它的价值是抽像的，例如，一个公司的好名声或信誉的价值。

资产赋值的另一个基础是因不期望事故所造成的保密性、完整性和可用性的损失而导致的费用。这样一个赋值会为资产价值提供三个重要的尺度，除了替代费用之外，基于在一系列假设环境下的安全事故导致的对资产的潜在损坏或负面业务影响的评估。需要强调的是，这种方法陈述了需要被考虑进风险评估公式的损害和其它影响的费用。

许多资产在赋值的过程中可能会被赋予多个价值。例如：一个业务计划可以基于开发这个计划所花费的人力来估价，可以按照输入数据的人力来估价，也可以基于它对竞争者的价值来估价。每个被赋予的价值可能相当不一样。赋予的价值可能是所有可能价值的最大值，或者可以是部分或所有可能价值的总和。在最后分析时，哪个价值要赋予给这个资产必须谨慎地决定，因为赋予的最后价值进入了为保护资产所花费的资源的决策。

最后，所有的资产赋值都需减到一个通用的基础。这可以在如下所列的标准的帮助下完成。可用于评估由资产的保密性、完整性和可用性的丧失而导致的可能的损害的准则是：

- 违反法律法规；
- 经营业绩的损害；
- 信誉的丧失/声望上的负面影响；
- 有关员工信息的破坏；

- 对个人安全的危害；
- 法律执行的负面影响；
- 商业机密的破坏；
- 公共秩序的破坏；
- 财务损失；
- 商业活动的中断；
- 环境安全的损害。

这些准则是资产赋值时需考虑的问题的例子。当进行赋值时，组织需选择与组织的业务类型和安全要求相关的准则。这可能意味着上面列出的一些标准是不适用的，并且可能需要将其他标准添加倒目录中。

在建立了要考虑的标准后，组织应对要在组织范围内使用的量度达成一致，第一步是确定要使用的等级的数量。关于最适合的等级的数量没有规定。更多的等级提供了更加细化的水平，但是有时太好的区别使得在组织范围内得出一致的赋值比较困难。一般来说，介于 3-10 之间的数量都可以使用，只要它与组织用于整体风险评估过程的方法保持一致。

而且，一个组织必须定义它自己对资产价值的限制，像“低”、“中”和“高”。应根据选择的准则对这些限制进行评估，例如对可能的财务损失，它们应当以货币价值给出，但是当考虑到对人员安全的危害时，货币赋值就显得不适合。最后，完全由组织决定什么被认为是“低”或“高”的损失——对于小型组织来说可能是灾难性的损失对于一个很大的组织而言可以是低的甚至是可忽略的。

附录 C：可能的威胁类型目录

下面的目录给出了典型威胁的例子。这个目录可用于威胁评估过程。威胁可由一个或多个蓄意的、偶然的或环境的（自然的）事件引起。下面的目录展示了 D（蓄意的）、A（偶然的）和 E（环境的）每种威胁的类型。D 用于所有针对 IT 资产蓄意的行为，A 用于所有偶然地损害 IT 资产的人为的行为，E 用于所有不是基于人类行为的事故。

地震	E
洪水	D，A，E
飓风	E
闪电	E
工业活动	D，A
炸弹攻击	D，A
使用武力	D，A
火灾	D，A
恶意破坏	D
断电	A
水供应失效	A
空调故障	D，A
硬件失效	A
电力波动	A，E
极端的温度和湿度	D，A，E
灰尘	E
电磁辐射	D，A，E
静电干扰	E
偷窃	D
存储介质的未授权的使用	D
存储介质的老化	E
操作人员错误	D，A
维护错误	D，A
软件失效	D，A

软件的未授权用户使用	D，A
用未授权方式使用软件	D，A
用户身份冒充	D
软件的非法使用	D，A
恶意软件	D，A
软件的非法进口/出口	D
未授权用户的网络访问	D
用未授权的方式使用网络设备	D
网络组件的技术性失效	A
传输错误	A
线路损坏	D，A
流量过载	D，A
窃听	D
通信渗透	D
流量分析	D
信息的错误路径	A
信息重选路由	D
拒绝	D
通讯设备失效（如网络设备）	D，A
人员短缺	A
用户错误	D，A
资源的滥用	D，A

附件 D：常见脆弱点举例

下面的目录给出了处于不同安全区域的脆弱点的例子，包括可能利用这些脆弱点的威胁举例。在脆弱点评估的过程中，这些例子能够提供帮助。要强调的是，在一些情况下其他的威胁也可能会利用这些脆弱点。

1. 环境和基础设施

建筑物、门和窗缺乏物理保护

（例如，可被盗窃的威胁所利用）

不充分或不小心地使用建筑或房间的访问控制

（例如，可被蓄意破坏的威胁所利用）

不稳定的供电网络

（例如，可被电压波动的威胁所利用）

处于易受洪水影响的区域

（例如，可被洪水的威胁所利用）

2. 硬件

缺乏定期更新计划

（例如，可被存储媒介老化的威胁所利用）

对电压波动敏感

（例如，可被电压波动的威胁所利用）

对温度变化敏感

（例如，可被极端温度的威胁所利用）

对湿度、灰尘和污染敏感

（例如，可被灰尘的威胁所利用）

对电磁辐射敏感

（例如，可被电磁辐射的威胁所利用）

存储介质的不充分维护/安装错误

（例如，可被错误维护的威胁所利用）

缺乏有效的配置变更控制

（例如，可被人员的操作错误的威胁所利用）

3． 软件

提供给开发者的规范不明确或不完整

（例如，可被软件失效的威胁所利用）

没有或不充分的软件检测

（例如，可被未授权用户使用软件的威胁所利用）

复杂的用户界面

（例如，可被操作人员错误的威胁所利用）

缺乏象用户鉴权那样的逻辑访问控制机制

（例如，可被伪装用户身份的威胁所利用）

缺乏审计追踪

（例如，可被用未授权方式使用软件的威胁所利用）

广为人知的软件缺陷

（例如，可被未收取用户使用软件的威胁所利用）

未经保护的口令表

（例如，可被伪装用户身份的威胁所利用）

口令管理不力（容易猜测的口令、口令存储、变更的频次不充分）

（例如，可被伪装用户身份的威胁所利用）

访问权限的错误分配

（例如，可被用未授权方式使用软件的威胁所利用）

未控制的下载和使用软件

（例如，可被恶意软件的威胁所利用）

当离开工作站时没有注销

（例如，可被软件失效的威胁所利用）

缺乏有效的变更控制

（例如，可被未授权用户使用软件的威胁所利用）

缺少文档

（例如，可被错误人员错误的威胁所利用）

缺少备份拷贝

（例如，可被恶意软件和火灾的威胁所利用）

存储媒质未经适当清理就被重新使用或处置

（例如，可被未授权用户使用软件的威胁所利用）

4. 通讯

没有保护的通讯线路

（例如，可被窃听的威胁所利用）

连接电缆

（例如，可被通讯渗透的威胁所利用）

缺乏发送者和接受者的识别和鉴权

（例如，可被冒充用户身份的威胁所利用）

用明文传输口令

（例如，可被未授权用户网络访问的威胁所利用）

缺乏发送和接受消息的证明

（例如，可被抵赖的威胁所利用）

拨号线路

（例如，可被未授权用户网络访问的威胁所利用）

未经保护的敏感通讯

（例如，可被窃听的威胁所利用）

不充分的网络管理（路径选择的弹性）

（例如，可被流量过载的威胁所利用）

未经保护的公共网络连接

（例如，可被未授权用户使用软件的威胁所利用）

5. 文件

未经保护的存储

（例如，可被盗窃的威胁所利用）

处理时不小心

（例如，可被盗窃的威胁所利用）

未控制的复制

（例如，可被盗窃的威胁所利用）

6． 人员

人员缺乏

（例如，可被人员缺少的威胁所利用）；

外部或清洁人员的工作缺乏监督

（例如，可被盗窃的威胁所利用）；

不充分的安全培训

（例如，可被操作错误所利用）；

缺乏安全意识

（例如，可被用户错误所利用）；

硬件和软件不正确的使用

（例如，可被操作错误所利用）；

缺乏监督机制

（例如，可被未经授权的使用软件的威胁所利用）；

不充分的招聘程序

（例如，可被竞争对手或蓄意破坏的威胁所利用）

7．普遍适用的脆弱点

单点故障

（例如，可被通信服务失效的威胁所利用）

不充分的服务维护响应

（例如，可被硬件失效的威胁所利用）

附件 E：风险分析方法的类型

（非正式版）

风险分析有很多阶段，这些阶段已经在这个技术报告的这里或其它部分讨论过了。这些阶段是：

- 资产识别和赋值；
- 威胁评估；
- 脆弱点评估；
- 已存在的/计划的防护措施评估；
- 风险评估。

这个附件关注的是评估所有风险的最后阶段。就像前面识别的那样，只要针对资产的威胁存在，那些具有价值和一些程度的脆弱点的资产就处于风险之中。风险评估综合了不期望事件的潜在负面业务影响以及评估的脆弱点和威胁的等级。风险是对于系统及相关组织可能暴露程度的有效衡量。风险由下列因素决定：

- 资产的价值；
- 可能威胁资产的威胁以及他们发生的可能性；
- 脆弱点被威胁利用导致不期望影响的难易程度；
- 已存在或计划的防护措施，这些防护措施可能减少威胁、脆弱点和影响的严重程度。

风险分析的目的是识别并评估 IT 系统及其资产可能暴露的风险，以识别并选择适当的和合理的安全防护措施。分析基于资产的价值、威胁和脆弱点的等级以及已经存/策划的防护措施。换句话说，当评估风险时，需要考虑几个方面，包括影响和可能性。

影响评估的方法有多种，包括定量（也就是说用货币单位）和定性（可以基于象中等或严重等形容词的使用）的衡量，或者是二者的联合。为了评估威胁发生的可能性，应建立一个资产有价值或需要被保护的时间框架。威胁发生的可能性受下列因素的影响：

- 资产的吸引力，当考虑蓄意的人为威胁时适用；
- 资产转化为报酬的难易程度，当考虑蓄意的人为威胁时适用；
- 威胁代理的技术能力，适用于蓄意的人为威胁；
- 威胁的可能性；
- 脆弱点被利用的难易程度，适用于技术性的和非技术性的脆弱点。

很多方法使用了表格，并将主观的与经验的衡量联合起来。当前，使用的方法没有对错之分。更重要的是组织用什么方法觉得适宜、自信并能够产生可重复的结果。下面给出了基于方法的一些表格的例子。

例子 1 预先确定价值矩阵

在这种风险分析方法里面，实际的或计划的物理资产的价值依据替代或重建成本（也就是说，定量的评估）。然后这些成本转化为与数据资产使用的一样的定性量度（见下面）。实际或计划的软件资产的赋值采用同物理资产一样的方法，使用识别的购买或重建成本，然后将这些成本转化为与数据资产使用的一样的定性量度。此外如果发现应用软件有自己固有的保密性或是完整性要求的时候（例如，源码本身具有商业敏感性），它将采用同数据资产一样的赋值方法。

数据信息的价值是从与被选定的业务人员（数据所有者）的会晤中得到的，这些人对于数据的解释是非常权威的，以确定使用的、存储的、处理的或访问的数据的真实价值和敏感程度。会晤可以促进数据资产价值和敏感程度的评估，依据最坏的场景假设。最坏的场景假设可以从因未授权的泄漏、未授权的更改、抵赖、不同时间段的不可用以及破坏所造成的负面业务影响中合理的推断。

可以使用数据资产赋值指南来完成赋值，它包括了下列问题：

- 人身安全；
- 人员信息；
- 违反法律法规；
- 法律执行；
- 商业和经济利益；
- 财务损失/活动的破坏；
- 公共秩序；
- 业务策略和运行；
- 信誉损失。

指南促进了用数据尺度表达的价值的识别，例如在下面示例矩阵中，写出来的 1 到 4 的尺度，因此使得定量的价值在可能和合理的地方获得承认，在定量价值不能发挥作用的地方，建立了定性价值，比如说人员生命安全。

下一个主要的活动就是完成许多关于每一种威胁类型和与威胁类型相关的一组资产的调查问卷，以能够评估威胁的等级（发生的可能性）和脆弱点的等级（被威胁利用从而导致负面影响的难以程度）。给每一个问题的回答打分。通过知识基础和比较的范围累积这些分数。识别的威胁等级用高到低的量度表示，脆弱点的等级也一样，就如同下面的示例矩阵一样，来区别这两个有关的影响类型。完成的调查问卷的信息应该是用合适的技术、人员和

寄宿人员、可能的物理位置检查和文件评审中收集到的。

考虑的威胁类型广泛地包括：人们蓄意的未授权的行为、上帝的行为、人们的错误以及设备/软件/线路失效。

与每种影响类型相关的资产价值、威胁和脆弱点的级别，都列在下面的矩阵里，在评分 1 到 8 中联合确定风险的有关衡量标准，通过一种构造方法把价值放置在矩阵中，下面举了一个例子

	威胁等级	低			中			高		
	脆弱点等级	L	M	H	L	M	H	L	M	H
资产价值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

表 1

对于每一项资产，都要考虑与它相关的脆弱点和脆弱点相应的威胁。如果脆弱点没有相关的威胁，或者是威胁没有相关的脆弱点，就不会存在风险（但是要小心万一这种局面改变）。现在，适当的行表示的是资产的价值，适当的列表示的是威胁和脆弱点的严重程度。例如，如果资产的价值是 3，威胁是高，并且脆弱点是低，那么风险值是 5。假设资产的价值是 2，也就是说资产价值变化了，威胁等级是低，并且脆弱点是高，那么风险值是 4。矩阵的规模可以根据根据组织的需要进行调整，矩阵的规模由威胁严重程度分类的数量、脆弱点严重程度分类和资产赋值分类的数量确定。如果需要进行额外的风险评估，那么需要增加额外的行和列。

例 2 风险评估的威胁性排序

矩阵表可以用于联系影响因素（资产价值）和威胁发生的可能性（考虑脆弱点方面）。第一步是在预先定义的量度上评估影响（资产价值），也就是说每个被威胁的资产值（表中的 D 列）介于 1 到 5 之间。第二步是在预先定义的量度上评估威胁发生的可能性，也就是说威胁发生的可能性介于 1 到 5 之间（表中 C 列）。第三步是用乘法计算风险值（bxc）。最后，威胁会根据它们‘暴露’的要素进行排序。注意，在这个例子中，是作为最低的影响和最小的发生可能性。

威胁表述 (a)	影响（资产）价值 (b)	威胁发生的可能性（c）	风险值 (d)	威胁排序 (e)
威胁 A	5	2	10	2
威胁 B	2	4	8	3
威胁 C	3	5	15	1
威胁 D	1	3	3	5
威胁 E	4	1	4	4
威胁 F	2	4	8	3

如上所述，这个程序，允许具有不同影响和发生可能性的不同的威胁进行比较和按优先顺序排序，象上面那样。在一些情况下，把货币价值和使用经验的得分联系起来是很有必要的。

例 3，评估风险的可能损害和频率的价值

在这个例子里，重点是放在非预期事件的影响和决定给哪个系统优先权的问题上。，这是通过评估每个资产和风险的两个值完成的，它们联合起来决定每一个资产的得分。当系统所有的资产分数加起来得到一个总和以后，IT 系统风险评估结果也就确定了。

首先，为每个资产赋值。这个价值和因发生风险而导致的资产潜在损失有关。对每一种适用于资产的威胁，资产价值被赋予给资产。

其次，评估频率值。它是通过把威胁发生的可能性和脆弱点被利用的难易程度的结合起来进行评估。见表 3

威胁等级	低			中			高		
脆弱点等级	低	中	高	低	中	高	低	中	高
频率值	0	1	2	1	2	3	2	3	4

接着，在表 4 中找到资产价值和频率值的交叉点就可以得出资产/威胁的分数，资产/威胁的分数合计，计算出一个资产总分，这个数字能被用于区分构成系统部分的资产。

资产价值	0	1	2	3	4
频率值					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

最后一步是为系统的资产合计所有的资产总分，得出一个系统分，它可以被用于区分系统或决定给哪个系统保护优先权。

下面例子里，所有的价值都是随机选定的，假定系统有三个资产 A1，A2，A3，在假定系统 S 有两个威胁 T1 和 T2，假定 A1 价值为 3，类似，把 A2 价值为 2，A3 价值为 4。

如果对于 A1 和 T1，威胁的可能性低，脆弱点被利用的难易程度是中等，那么频率值是 1，（见表 3）。

资产/威胁的分数 A1/T1 能通过表 4 资产价值 3 和频率值 1 的交叉点获得，也就是 4，类似地，当威胁可能性是中级，脆弱点被利用的难易程度是高级，就能得到 A1/T2 的分数 6，现在，总体资产的分数就可以算出，也就是 10，为每项资产和适用的威胁计算资产总分。把 A1T+A2T+A3T 加起来，得到系统的总分 S7。

现在，不同的系统可以为了建立优先级进行比较，同一系统中的不同资产也可以这样做。

例 4，可容忍的风险和不可容忍的风险的区分

衡量风险的另一种方法是只区分可容忍的风险和不可容忍的风险。这一活动的背景是风险评估只被用来根据那里最迫切需要采取措施的风险排序，仅需很少的努力就可以达到同样的目的。

用这种方法，矩阵表可以不包含数字，只是简单地包含 N 和 T，代表相应的风险是否可以容忍，例如，方法 3 的矩阵表可以变成

表 5

损失值	0	1	2	3	4
频率值					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

不过，这仅仅是一个例子，在可容忍的风险和不能容忍的风险之间，在什么地方画线留给读者去完成。