信息技术
安全技术
信息技术安全管理指南

第 1 部分：IT 安全的概念和模型

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 包含了关于 IT 安全管理的指南。ISO/IEC TR 13335 的第 1 部分介绍了基础性的管理概念和模型，这些管理概念和模型对于了解 IT 安全至关重要的。这些概念和模型将在剩余部分予以进一步的讨论和发展，以提供更多详细的指导。这些部分可以一起使用，以助于识别和管理 IT 安全的所有方面。第 1 部分的内容对于全面理解 ISO/IEC TR 13335 的后续内容是非常必要的。

2 引用标准

- 信息技术－安全技术－IT 安全术语第 6 号标准文档:1998
- ISO7498-2 ：1998 信息处理系统－开发系统互联－基本参考模型－第 2 部分：安全架构
- ISO/IEC TR 13335-2：IT 安全管理指南 第 2 部分： IT 安全管理和策划
- ISO/IEC TR 13335-3：IT 安全管理指南 第 3 部分： IT 安全管理技术
- ISO/IEC TR 13335-4：IT 安全管理指南 第 4 部分： 防护措施的选择
- ISO/IEC TR 13335-5：IT 安全管理指南 第 3 部分： 网络安全管理指南
- ISO/IEC 13888-1：1997 信息技术－安全技术－抗抵赖性－第 1 部分：通则
- ISO/IEC 15408-1：1998 信息技术－安全技术－IT 安全评估准则－第 1 部分：简介和一般模型
- ISO/IEC SC 27 N 2582 入侵检测框架
- ISO/IEC SC 27 N 2578 TTP 服务使用和管理指南

3 定义

下列定义将在 ISO/IEC TR 13335 的 5 个部分中使用：

3.1 可审计性

确保一个实体的行为可以北唯一地追溯到该实体的特性

3.2 资产

任何对组织有价值的东西

3.3 鉴权

确保一个主体或资源的身份就是其所声称的。鉴权应用于类似用户、进程、系统和信息的实体。

3.4 可用性

一旦授权用户需要，就可以访问和使用的特性

3.5 基线控制

为组织或系统建立的一系列最少的防护措施

3.6 保密性

确保信息不可用或不暴露给未经授权的个人、实体或过程的特性

3.7 数据完整

确保数据不被未经授权的方式替换或破坏的特性

3.8 影响

不期望事件的结果

3.9 完整性

保证数据和系统的完整

3.10 IT 安全

与定义、达到和保持保密性、完整性、可用性、抗抵赖性、可审计性、鉴权和可靠性相关的

所有方面
3.11 IT 安全策略（方针）
在组织及其 IT 系统内指导如何管理、保护和分发包括敏感信息在内的资产的规则、指南和惯例
3.12 抗抵赖性
证明一个已经发生的活动或事件在后来不能被抵赖的能力
3.13 可靠性
持续的预期行为和结果的特性
3.14 残余风险
事实防护措施后仍残留的风险
3.15 风险
假定的威胁利用一个或一组资产的脆弱点导致组织受损的潜在
3.16 风险分析
识别安全风险、确定其程度并识别需要保护的范围的过程
3.17 风险管理
识别、控制和消除或缩减可能影响 IT 系统资源的不希望事件的全部过程
3.18 防护措施
削减风险的惯例、程序或机制
3.19 系统完整
系统以一种无损的方式实现其预期的功能，免受蓄意的或无意的未经授权的系统操作的影响。
3.20 威胁
可能导致不期望事件的潜在原因，该不期望事件可能导致系统或组织受损
3.21 脆弱点
一个或一组资产所具有的、可能被一个或多个威胁所利用的弱点。

4 结构

ISO/IEC TR 13335 第 1 部分结构如下：第 5 条款介绍了本报告的目的，第 6 条款介绍了关于 IT 安全管理要求背景的知识。第 7 条款概述了 IT 安全管理的概念。第 8 条款通过概念性和模型的方式检查了 IT 安全的要素及其相互关系。第 9 条款讨论了用于管理 IT 安全的过程并提供 IT 安全组件模型。最后，第 10 条款对第 1 部分进行了总结。

5 目的

ISO/IEC TR 13335 适用于各种类型的读者，第 1 部分的目的在于描述在 IT 安全管理领域内的各种主题，并提供一个对基本 IT 安全概念和模型的简单介绍。这些材料尽量保持精炼，以提供一个更高级别的管理概述。该部分内容适用于对组织信息安全负有责任的高层管理者，并向那些对该报告其他部分内容感兴趣的读者简单介绍了 IT 安全。第 2、3、4 和 5 部分为那些直接负责事实和监视 IT 安全的个人提供了更为丰富的信息和资料。第 2、3、4 和 5 部分都基于第 1 部分中阐述的概念和模型。
该报告的目的并不是建议采取特定的 IT 安全管理办法，相反，报告以对有用的概念和模型的广泛讨论为开端，以 IT 安全管理、特定技术和工具为结尾。该材料是通用的，适用于不同类型的管理和组织文化。该报告以一种允许对材料进行剪裁以满足组织及其特定管理方式要求的方式组织。

6 背景

政府和商业组织越来越依赖于使用信息以开展他们的业务活动。信息及服务的保密性、完整性、可用性、抗抵赖性、可审计性、鉴权和可靠性的损失可能会对组织造成负面影响。因此，需要在组织内保护信息并管理 IT 安全。信息保护的要求在现在的环境中就显得尤为重要，因为许多组织都通过 IT 系统、网络保持内外部联系。

IT 安全管理是使用过程方法，以达到和保持保密性、完整性、可用性、抗抵赖性、可审计性、鉴权和可靠性的适当级别。IT 安全管理活动包括：

- 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；
- 评估负面的组织影响；
- 识别和分析对组织内 IT 资产的安全威胁；
- 识别和分析组织内资产的脆弱点；
- 识别和分析风险；
- 规定适当的防护措施；
- 监视为保护组织内信息和服务的防护措施以一种成本－有效的方式实施和运行；
- 开发和实施安全意识方案；
- 事件检测和响应。

为落实 IT 系统的管理职责，安全必须成为组织整体安全管理计划的内在部分。结果，本报告中阐述的几个安全主题有着更加广阔的管理含义。本报告并不试图集中于广泛的管理话题，而是关注于主题的安全方面和通常他们是如何与管理相关的。

7 IT 安全管理概念

采纳了概念之后还需要考虑组织运行其中的文化和环境，因为文化和环境可能对于整体的安全方法有着显著的影响。此外，文化和环境可能对于那些负责保护组织的特定部分的人员也有影响。在某些情况下，政府应通过制定和实施法律对此负责并履行职责。在另外一些情况下，所有者或管理人员应对此负责。这一话题可能对于已采取的方法有着相当大的影响。

安全是组织内所有层次管理人员的职责，并且贯穿于系统生命周期的所有阶段。

7.1 方法

需采用系统的方法以识别组织内 IT 安全的要求。这也是实施 IT 安全和持续管理的需求。这一过程通常称为 IT 安全管理，包括如下功能：

- 开发 IT 安全策略；
- 在组织内是些角色和职责；
- 风险管理，包括识别和评估以下内容：
  - 需要保护的资产；
  - 威胁；
  - 脆弱点；
  - 影响；
  - 风险；
  - 防护措施；
  - 残余风险；

- ✧ 限制条件。
- ➢ 配置管理；
- ➢ 变更管理；
- ➢ 中断计划和灾难恢复计划；
- ➢ 选择和实施防护措施；
- ➢ 安全意识；
- ➢ 以及下列内容：
  - ✧ 保持；
  - ✧ 安全设计；
  - ✧ 监视；
  - ✧ 评审
  - ✧ 事件处置。

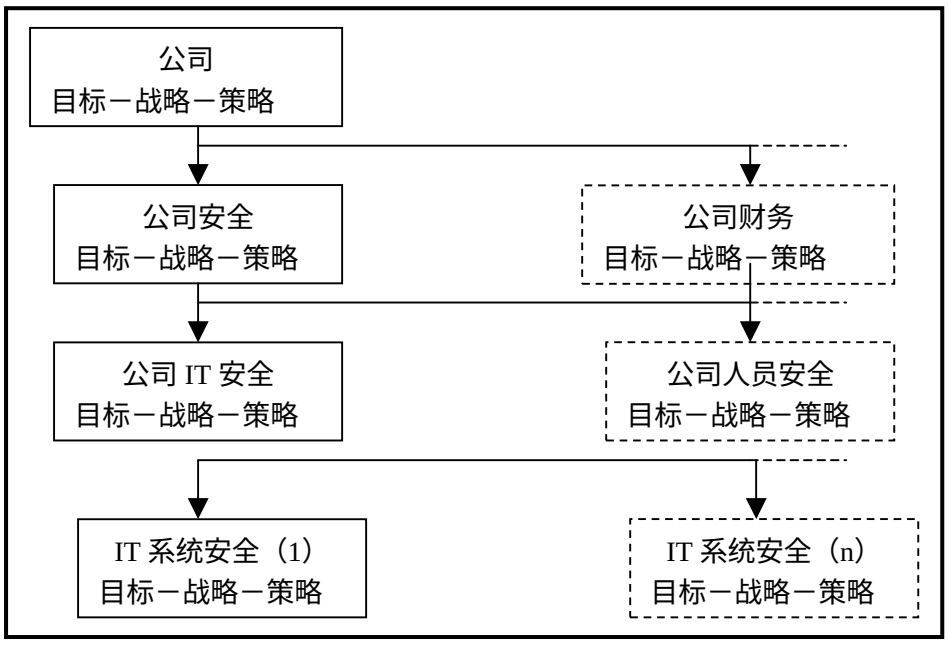
7.2 目标，战略和策略

需在组织内正式阐明公司的安全目标、战略和策略，以作为有效的 IT 安全的基础。他们支持组织的业务，并共同作用以确保所有防护措施之间的一致性。目标是识别我们需要达到什么，战略识别如何达到这些目标，而策略则识别我们需要做什么。

可以开发从公司到组织操作层的等级性的目标、战略和策略。他们应反映组织的要求并考虑任何可能的组织的限制条件，并在每一层次和所有的层次上保持一致性。应保持目标、战略和策略，并在阶段性的安全评审（如，风险分析，安全审计）和业务目标变更的基础上予以更新。

从本质上来说，**公司安全策略**作为一个整体包含了组织的安全准则和指导。公司的安全策略应反映更加广泛的公司策略，包括那些那些阐述个人权利、法律要求和标准的策略。

从本质上来说，**公司 IT 安全策略**应反映适用于公司安全策略和组织内通用 IT 系统的安全准则和指南。



目标、战略和策略的层次

IT 系统安全策略应反映包含于公司 IT 安全策略之中的安全准则和指南。它应包含特定安全系统、拟实施的防护措施以及如何使用他们以确保充分安全的细节。无论如何，采取与组织业务需要相关的方法是有效的是很重要的。

IT 系统安全目标、战略和策略表达的是从 IT 系统安全的角度的期望。通常他们使用自然语言表达，但是有时可能要求他们使用精确的语言以一种更加正式的方式表达。他们通常强调安全的关注点，如：

- 保密性；
- 完整性；
- 可用性；
- 抗抵赖性；
- 可审计性；
- 鉴权；
- 可靠性。

目标、战略和策略将建立组织安全等级、风险接受的门槛以及组织的中断要求。

8 安全要素

下列条款在高层次上描述了安全管理过程所涉及的要素，对每个要素都做了介绍，并识别主要的贡献因素。在本报告的其他部分，对这些要素和他们的相互关系进行了更为详细的描述和讨论。

8.1 资产

对资产的适当管理对于组织的成功是至关重要的，并且也是各级管理层次的主要职责。组织的资产可包括：

- 物理资产（如，计算机硬件，通讯设施，建筑物）；
- 信息/数据（如，文件，数据库）；
- 软件；
- 提供产品和服务的能力；
- 人员；
- 无形资产（如，信誉，形象）。

这些资产的全部或大部分都是有价值的，值得适当程度的保护。需采取风险评估以确定这些资产是否被充分保护。

从安全的角度来看，如果组织的资产未被识别，那么实施和保持一个成功的安全方案是不可能的。在许多情况下，识别资产并赋值的过程可以在一个非常高的层次上完成，并且可能也不需要太多的成本、详细的和耗费时间的分析。分析的详细水平可根据事件、成本以及资产的价值来衡量，无论如何，详细的水平应基于安全目标来确定。在许多情况下，对于一组资产是非常有益的。

应考虑包括资产价值和/或敏感程度以及任何内在的防护措施在内的资产的性质，保护资产的要求受其保护给特定威胁的脆弱点的影响。如果这些方面是显而易见的，则资产的所有者应在该阶段将其捕获。组织运行于其中的环境、文化和法律系统可能会影响资产的价值和

他们的特性。例如，有些文化认为保护个人信息是非常重要的，然而其他文化对于这一话题给予了低级别的关注。这些环境的、文化的和法律的差异对于那些国际组织和他们使用的跨越国界的 IT 系统有着显著的影响。

8.2 威胁

资产暴露于许多威胁。威胁有潜力导致一个不期望的事件，该事件可能对系统或组织及其资产造成损害。这些损害可能是对 IT 系统和服务所处理信息的直接或间接的攻击。例如，对信息的未经授权的破坏、泄漏、修改、腐败、不可用或丢失。一个威胁需要利用资产已经存在的脆弱点以成功地对资产造成损害。威胁可以是自然地或人为的，也可以是无意的或蓄意的。应识别无意的和蓄意的威胁，并评估他们的等级和可能性。

威胁举例：

人员		环境
蓄意	无意	
窃听 信息修改 系统攻击 恶意代码 偷盗	错误和倏忽 文件删除 错误路径 物理事件	地震 闪电 洪水 火灾

可以获得许多类型资产威胁的统计数据。组织在风险评估过程中应获取并使用这些数据。威胁可能影响组织的特定部分，例如对个人计算机的破坏。某些威胁对于系统或组织所在特定地区的周边环境是常见的，例如，飓风或闪电对建筑物的损坏。威胁可能来自于组织内部，如雇员的蓄意破坏，也可能来自于组织外部，如恶意代码攻击或商业间谍。不期望事件导致的损害可能是暂时的，也可能是永久的，如对于建筑物的破坏。

因威胁导致的损害可能也不尽相同，例如：

- 软件病毒可能因其行为的不同而导致不同程度的伤害；
- 特定地区的地震可能每次有不同的强度。

类似的威胁可能有不同的严重等级，例如：

- 病毒可以区分为破坏性的或非破坏性的；
- 地震的强度可以用里氏强度来表示。

一些威胁可能影响多个资产。不同资产其所遭受威胁的影响可能也不相同。例如，单独的个人计算机上的软件病毒的影响是有限的或局部的。然而同样的病毒在基于文件服务器的网络上可能产生大范围的影响。

威胁自己就提供了关于其特性的有用信息。类似信息可包括：

- 来源，如内部和外部；
- 动机，如获得经济利益，竞争优势；
- 发生的频率；
- 威胁的严重性。

组织运行其中的环境和文化对于如何处理组织的威胁有着显著的关系和影响。在某些极端

情况下，某些威胁在其他文化认为根本不具有破坏性，当阐述威胁时，必须考虑环境和文化的方面。

根据威胁评估的结果，可以用高、中、低予以衡量。

8.3 脆弱点

与资产相关的脆弱点包括在物理布局、组织、程序、人员、管理、行政、硬件、软件或信息。他们可能被那些对 IT 系统或业务目标产生损害的威胁所利用。脆弱点本身并不会导致损害，一个脆弱点仅仅是一个或一系列的状态，这些状态可能允许一个威胁影响资产。需要考虑多种来源的脆弱点，例如那些资产本身固有的脆弱点。脆弱点可能仍旧存在，除非资产因自身变更而导致脆弱点不再适用。

脆弱点包括系统的脆弱点，该脆弱点可被利用并可能导致不期望的结果。威胁可能会利用这些机会导致损害。例如，缺少访问控制机制就是一个脆弱点，该脆弱点允许入侵威胁的发生和资产的受损。在特定的系统或组织内，并不是所有的脆弱点都容易受到威胁的影响。对应威胁的脆弱点应予以立即关注。然而，因为环境的动态变化，应监视所有的脆弱点，以识别那些可能暴露给新的或旧的威胁的脆弱点。

脆弱点就是检查可能被已识别的威胁所利用的弱点。分析必须考虑环境和存在的防护措施。暴露给威胁的特定系统或资产的脆弱点是容易状态的陈述，系统或资产可能因其而受损。

根据脆弱点评估的结果，可以用高、中、低来衡量。

8.4 影响

影响是影响资产的不期望事件的后果，无论其是蓄意的还是无意的。后果可能是特定资产的破坏，IT 系统受损，保密性、完整性、可用性、抗抵赖性、可审计性、鉴权或可靠性的损失。直接后果可能包括资金的损失、市场份额或公司形象的丧失。影响的衡量应平衡不期望事件的后果和为防范不期望事件所采取的防护措施的成本。需考虑不期望事件发生的频率。当每次损害比较低，但是长时间的许多事件的综合影响比较大，在这种情况下应考虑不期望情况的频率。影响评估对风险评估和防护措施的选择是非常重要的因素。

定性和定量的影响评估可以用数字的方式完成，例如：

- 建立资金成本；
- 为严重程度赋予真实的等级，如从 1 到 10；
- 从预先定义的列表中选择形容词汇，如，低、中和高。

8.5 风险

假定的威胁利用资产的脆弱点，从而对组织造成损害的潜在。单个或多个威胁可能利用单个或多个脆弱点。

风险假设描述了一个或一组特定的威胁利用一个或一组脆弱点，从而把资产暴露给损害。风险特性可以通过两个要素的结合来描述：不期望事件发生的可能性及其影响。资产、威胁、脆弱点和防护措施的任何变化都可能对风险造成显著影响。早期的检测，环境或系统变更的

知识，都可能增加采取适当措施以降低风险的机会。

8.6 防护措施

防护措施是防范威胁、减少脆弱点、限制不期望事件的影响、检测期望事件和加速回复的惯例、程序或机制。有效的安全通常要求不同防护措施的结合以为资产提供分层的安全。例如，应用于计算机的访问控制机制应被审计控制、人员程序、培训和物理安全所支持。某些防护措施已经作为环境的一部分或作为资产固有的一部分而存在，或已经存在于系统或组织。

防护措施可能实现一个或多个下列功能：

- 保护；
- 威慑；
- 检测；
- 限制；
- 纠正；
- 恢复；
- 监视
- 意识。

选择适宜的防护措施对于安全方案的适当实施是非常重要的。许多防护措施能够履行多个职能。选择能够履行多个功能的防护措施通常具有更高的成本有效性。可以使用防护措施的区域包括：

- 物理环境
- 技术环境（硬件、软件和通讯）
- 人员
- 管理

安全意识是与人员领域相关的一种防护措施。因为其重要性，将在第 9.1 条款中予以讨论。组织运行其中的环境和文化可能对组织防护措施的选择以及安全意识有影响。特定的防护措施清晰地反映了组织对于安全的态度。就此而言，选择与组织运行其中的文化和社会不冲突的防护措施是非常重要的。

特定的防护措施包括：

- 访问控制机制；
- 防病毒软件；
- 加密以确保保密性；
- 数字签名；
- 防火墙；
- 监视和分析工具；
- 冗余电力供应；
- 信息备份。

8.7 残余风险

通常，防护措施只能部分地减少风险。达到风险部分减少的程度通常是可能达到的，如果

要减少更多的风险则必须花费更多的成本。这就意味着通常会有残余风险的存在。判断针对组织的需求而言安全是否恰当是接受残余风险的一部分。这一过程被称为风险接受。

管理人员应了解所有残余风险的影响和事件发生的可能性。接受残余风险的决策应由以下两种人员作出：其职位可以接受影响或不希望事件发生的后果；如果残余风险的等级不可接受，其可以授权实施附加的防护措施。

8.8 限制条件

限制条件通常是由组织的管理层设定或承认的，并且受组织运行环境的影响。必须考虑一些限制条件，例如：

- 组织的；
- 业务；
- 资金的；
- 环境的；
- 人员的；
- 时间；
- 法律；
- 技术
- 文化或社会。

选择和实施防护措施时通常需要考虑这些因素。必须评审阶段性的、已经存在的和新的限制条件，并识别任何的变更。需要注意的是，限制条件可能随着时间、地理位置、社会变迁和组织文化的变化而变化。组织运行其中的环境和文化可能与几个安全要素有关联，尤其是威胁、风险和防护措施。

8.9 模型

许多已经存在的 IT 安全管理的模型已经得到认可。下列模型提供了一些对于理解 IT 安全管理话题所必需的概念。将描述下列模型：

- 安全要素关系；
- 风险管理关系；
- IT 安全过程管理。

前面介绍的概念以及组织的业务目标共同形成了组织 IT 安全的计划、战略和策略（见图 1）。主要的目的是确保组织保持业务运作的能力并将风险限于可接受的水平之内。安全没有完全有效的，因此从不期望事件中恢复的计划以及构建安全以限制损害的范围是非常重要的。

8.10 安全要素关系

IT 系统安全是一个可以从不同的交付考虑的多维问题。因此，为了确定并实施一个整体的和一致的 IT 安全战略和策略，组织必须考虑所有相关的方面。图 2 展示了资产是如何潜在地暴露于一系列的威胁的。随着时间的推移，威胁的集合也在不断变化，而只能部分地被了解。

模型表示了：

- 包含限制条件和威胁地环境在不断地变化，且只能部分地被了解；

- 组织的资产；
- 这些资产的脆弱点；
- 选择的防护措施以保护资产并降低威胁的后果；
- 改变风险的防护措施；
- 组织可接受的残余风险。

正如图 2 所示，一些防护措施在降低与多个威胁和/或多个脆弱点有关的风险方面是有效的。有时要采取一些防护措施以将残余风险降低到一个可接受的水平。一些情况下，如果认为风险是可以接受的，那么即使是威胁是显现的，也可能不实施防护措施。在另外一些情况下，脆弱点可能存在，但是并没有已知的威胁可以可以利用它。可能实施防火措施以监视威胁环境以确保没有威胁开发那些可以被利用的脆弱点。限制条件也影响着防护措施的选择。

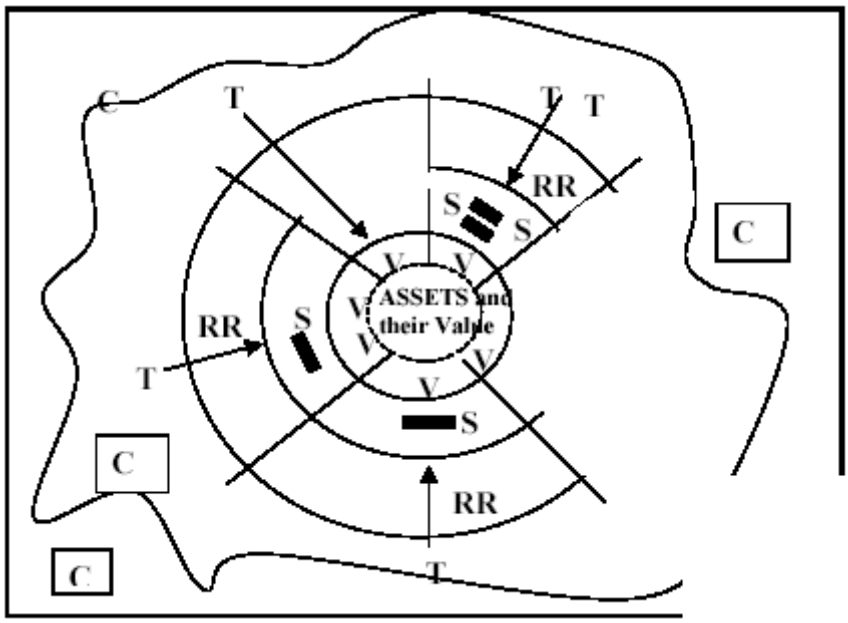


图 2 ：安全要素关系

8.11 风险管理关系

图 3 展示了通常与风险有关的要素之间的关系。为了清晰起见，只展示主要的关系。

图 3 展示的组件之间存在许多关系。下列的图表对这些关系进行了介绍。为了清晰起见，斜体部分内容直接引用了图 3 中的一个或多个组件。

任何系统都包含资产（尤其是信息，但也有硬件、软件、通讯服务等）。这些资产对于组织业务的成功是非常重要的。这些资产对组织是*有价值的*。价值通常用当信息未授权泄漏、修改/替换，信息或服务的不可用/破坏时对组织的业务运作所产生的*潜在负面影响*来衡量。首先要确定这些影响以确保识别资产的真正价值，无论影响是由什么威胁引起的。然后阐述什么威胁可能导致类似的影响以及可能性的问题，例如，*资产可能暴露于许多威胁*。再阐述什么威胁可能利用那些脆弱点而造成影响，如，*威胁可能利用脆弱点以暴露资产*。然后综合资产的价值（潜在的负面业务影响）、威胁的等级和脆弱点来确定风险。*这些组件中的任何*

一个，如价值、威胁和脆弱点都可能增加风险。然后，风险的衡量展示了整体保护要求，这些要求可以*被防护措施的实施影响或满足*。实施防护措施以*降低风险、防范威胁并切实减少脆弱点。*

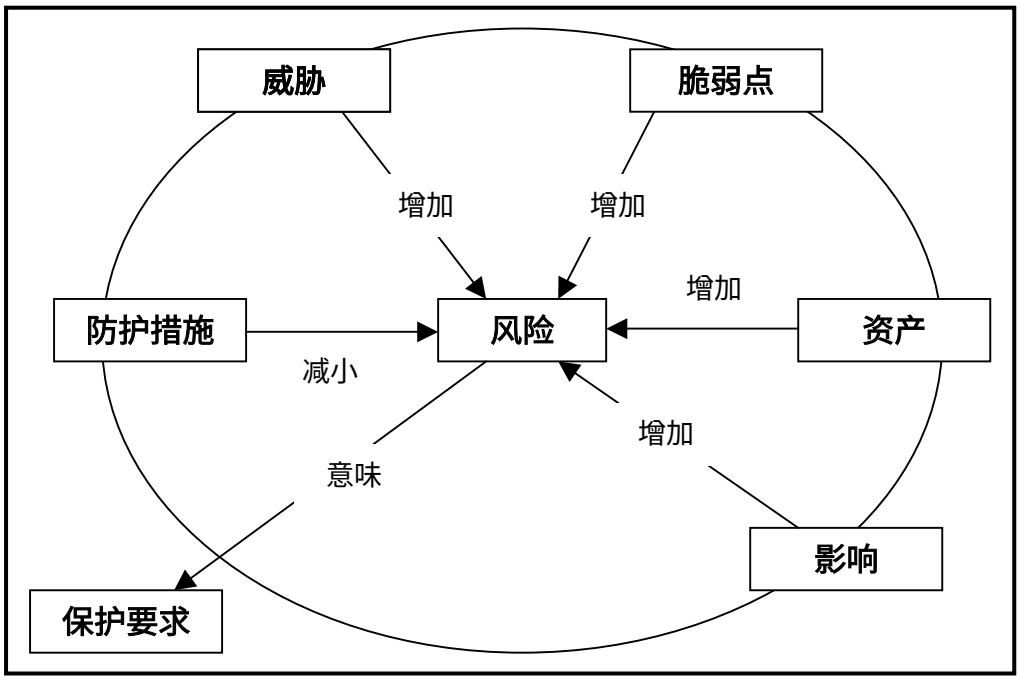


图 3：风险关系模型

图 4、5、6 分别展示了保护要求与威胁、脆弱点和资产之间的关系。一些 IT 安全管理方法可能注重于这些关系的某一方面。然而类似的方法可能忽略了一些重要的方面。因此，图 3 提供了一个更加通用的方法，并作为 ISO/IEC TR 13335 的第 2 和第 3 部分的基础。

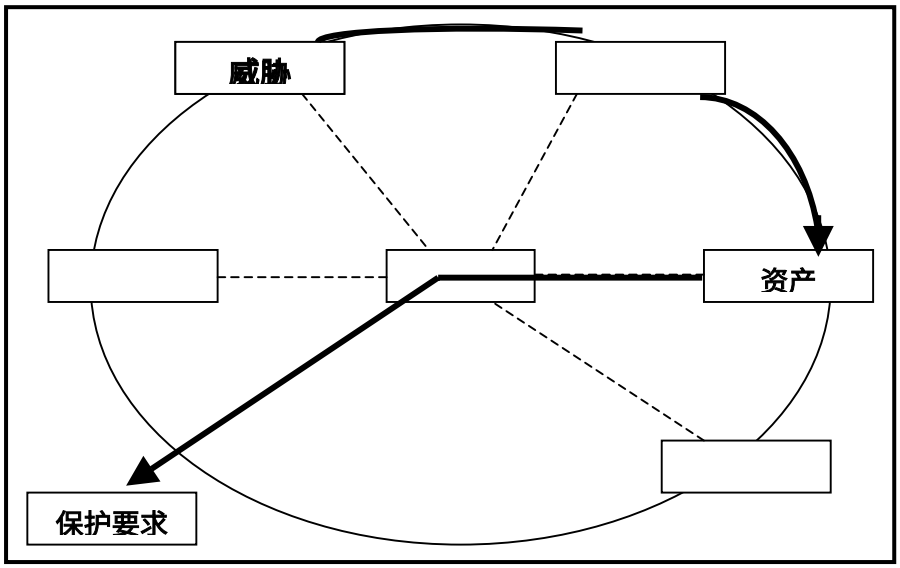


图 4：威胁图解

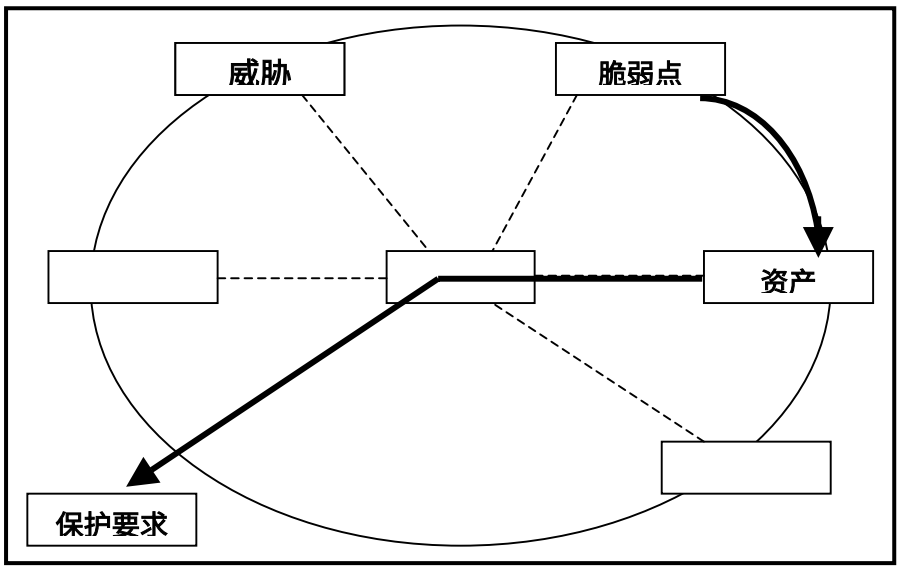


图 4：脆弱点图解

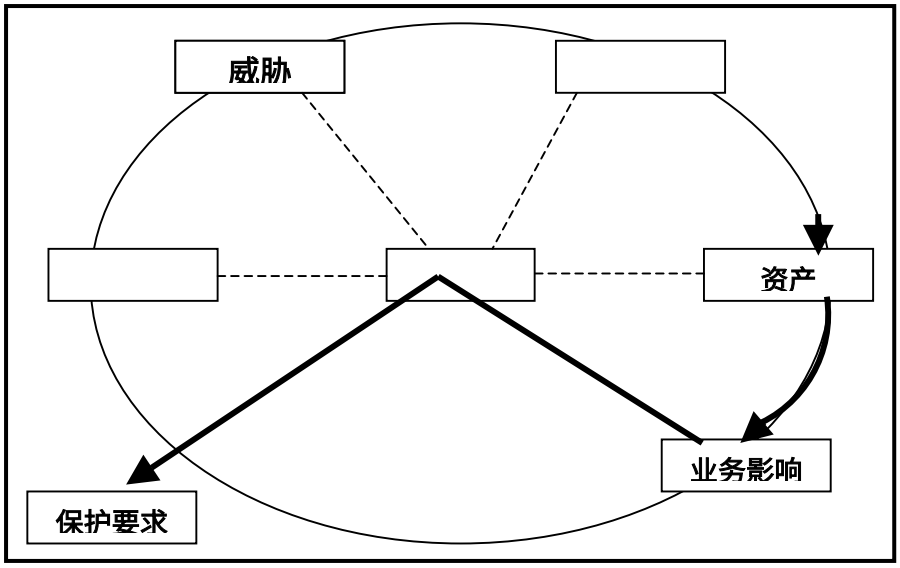


图 4：影响图解

9 IT 安全管理的过程

IT 安全管理是一个包含许多其他过程的持续的过程。一些过程，如配置管理和变更管理，适合于纪律而不是安全。经验表明，风险管理和它的子过程－风险分析，对于 IT 安全管理是非常有用的。图 2 展示了 IT 安全管理的几个方面，包括风险管理、风险分析、变更管理和配置管理。

9.1 风险管理

风险管理是一个比较评估的风险和防护措施的收益或/和成本，并导出与公司 IT 安全策略和业务目标相一致的实施策略和系统安全策略的过程。应考虑不同类型的防护措施并实施成本和/或收益分析。选择防护措施时，应考虑风险及潜在影响。必须考虑残余风险的可接受等级。在最小化识别和实施防护措施时所花费的时间与资源和确保所有系统适当的保护方面提供一个良好的平衡是非常重要的。

风险管理是一个持续的活动。对于一个新的和正处于策划阶段的系统而言，风险管理应成为设计和开发过程的一部分。对于已经存在的系统来说，应在适当的时机引入风险管理。在策划系统重大变更时，风险管理应成为策划过程的一部分。应将组织内所有的系统考虑在内，而不是独立地应用于某一个系统。

需要注意的是，防护措施本身也可能包含脆弱点并导致新的风险。因此在选择适当的防护措施时，必须非常谨慎，既要降低风险也要避免引入潜在的新风险。

下面的条款提供了风险管理过程的另外细节。

9.2 风险分析

风险分析识别了需要控制或接受的风险。就 IT 安全而言，IT 系统的风险分析包括资产价值、威胁和脆弱点分析。风险可以用潜在的影响来评估，影响可能是因为保密性、完整性、可用性、抗抵赖性、可审计性、鉴权或可靠性的破坏而导致的。风险分析评审的结果是对资产可能风险的陈述。

风险分析是风险管理的一部分，可以通过对所有系统的原始的简单分析完成，而不需要在时间和资源上的非必需的投资。风险分析可以确定哪些系统可以用惯例或基线控制方法的原则予以适当保护，哪些系统将从详细的风险分析评审中获益。

惯例原则包含了一系列的指南和基线控制方法，其可以用作协议的通用基础和满足基线保护要求的最佳惯例。

9.3 可审计性

有效的安全要求可审计性，并明确的授予和承认安全职责。需赋予资产所有者、IT 系统的提供者和用户职责和可审计性。因此，资产的所有者关系和相关的安全职责以及安全功能的审计对于有效的安全是非常重要的。

9.4 监视

应监视防护措施的使用，以确保他们适当的工作不因环境的变更而失效，并执行可审计性。系统日值的自动评审与分析是一种有效的工具，有助于确保预期的作用。这些攻击可以用来检测不期望事件，并产生威慑的效果。

应定期验证安全防护措施的有效性。这可以通过监视和符合性检查来完成，以确保防护措施以预期的方式使用并实现功能。许多防护措施会产生一个输出，如日志和告警报告，应检查显著的安全事件。从安全的角度来说，通用的系统审计功能可以提供有用的信息，并且可以用于这一点。

9.5 安全意识

安全意识对于有效的安全是一个更本性的要素。组织内人员安全意识的缺乏以及恶劣的安全惯例可以显著降低防护措施的有效性。组织内的人员通常被认为是安全链条上最薄弱的环节。为了确保组织内存在较高的安全意识水平，建立和保持有效的安全意识方案是非常重要的。安全意识方案的目的是向雇员、合作伙伴和供方解释：

- 安全目标、战略和策略；
- 安全的需要以及他们的相互角色和职责。

此外，应设计这些方案以激发雇员、合作伙伴和供方的兴趣并确保他们接受其安全职责。

应在组织内从最高管理者倒负责日常活动的个人的所有层次上实施安全意识方案。通常需要针对组织不同部分、不同角色和职责的人员开发和传递不同的意识材料。用阶段的方式来开发和传递广泛的安全意识方案。每个阶段都建立在以前的经验和教训的基础上，以安全概念和工作开始直到实施和监视安全的职责。

组织内的安全意识方案可能包括一系列的活动。安全意识材料（如海报、公告、小册子或简报）的开发和分发就是这样的一个活动。另外的活动就是为特定的雇员提供有关适当安全惯例的培训课程。最后，需要在每一个特定的安全主题领域提供专业水平的教育课程。

在一些情况下，将企业的安全信息包含在其他培训方案中是一种有效的方法。除了安全意识方案之外，还应该考虑该方法，或者是将该方法作为一种替代方案。为了开发综合了既定组织的文化和惯例要求的安全意识方案，需考虑下列步骤：

- 需求分析；
- 方案实施；
- 监视；
- 意识方案内容。

9.6 配置管理

配置管理或控制是保持系统配置的过程，可以是正式的或非正式的。配置管理的首要安全目标是确保维持系统配置文件的及时更新，确保以变更不减弱防护措施和组织整体安全有效性的方式对系统已批准的变更进行管理。

配置管理预期用来管理已批准的变更。它并非用于阻止对 IT 系统的以安全为基础的变更。配置管理的相关目标是为了确保系统的变更在其他文件中予以反映，例如灾难恢复和中断计划。如果变更是一个主要方面，那么需要重新分析系统的部分或全部的防护措施。

9.7 变更管理

当 IT 系统发生变更时，变更管理是用于识别新的安全要求的过程。

IT 系统及其运行环境处于不断变化之中。这些变化是新的 IT 特征和服务可用性的结果，或是发现了新的威胁和脆弱点。IT 系统的变更包括：

- 新的程序；
- 新特征；
- 软件升级；
- 硬件更新；
- 包括内部和匿名组的新用户；
- 其他的网络和互联。

当策划和实施 IT 系统变更时，如果有的话，确定变更可能对系统安全造成那些影响。如果系统有关一个配置控制委员会或其他组织机构以管理技术性的系统变更，IT 安全官员应分派至该委员会并赋予作出有关变更是否影响安全，如果是那么如何影响的决策的职责。在一些情况下，这可能就是作出减弱安全的决策的原因。在这些情况下，应评估安全性的减弱

并基于所有相关因素评估的基础上作出管理决策。换言之，系统的变更必须充分阐述安全关注点。对于主要变更包括购买硬件、软件和服务，应进行分析以确定新的安全要求。换句话说，系统的许多变更从本质上来说比较小，并不需要象主要变更那样进行广泛的分析。对于这两类变更，应进行考虑收益与成本的风险评估。对于较小的变更，可以用会议的实行非正式地实施，但是结果和管理决策应在文件中体现。

9.8 业务连续性计划

业务连续性计划包括中断和灾难恢复计划。

应建立在整个组织内开发和保持业务连续性地管理过程。在制定业务连续性计划之前，组织应确保关于全部业务连续性方法的策略已开发。策略应基于业务应先分析的结果以及相关的协议的最小资源、处所、IT 基础设施和通讯要求，以及协议的恢复时间阶段。

中断计划包含当支持过程（包括 IT 系统）受损或不可用时如何运作业务的信息。这些计划应阐述一系列可能的组合，包括：

- 不同的中断长度；
- 不同种类设施的损失；
- 物理访问边界的全部损失；
- 恢复到未发生中断状态的需要；

灾难恢复计划描述了如何将受不期望事件影响的 IT 系统恢复操作。灾难恢复计划包括：

- 构成灾难的准则；
- 激活恢复计划的职责；
- 不同恢复活动的职责；
- 恢复活动的描述；
- 测试恢复计划有效性的职责。

9.9 IT 安全要素

下图展示了 IT 安全要素。

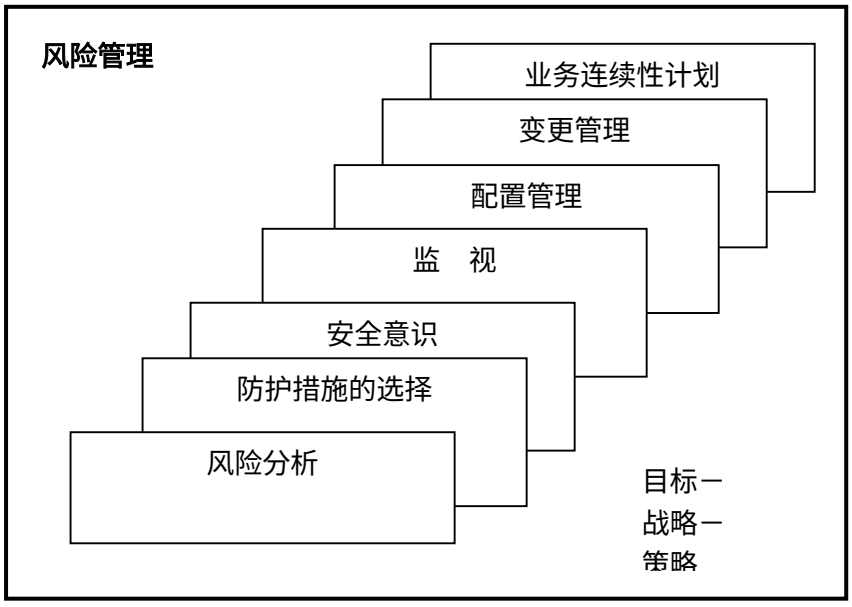


图 7： IT 安全组件模型

9.10 IT 安全管理过程

IT 安全管理是一个持续的过程，必须考虑安全生命周期。这些方面将在 ISO/IEC TR 13335 第 2 部分予以检查。第 3 部分阐述了用于安全管理的技术。在图 8 中展示的过程模型展示了 IT 安全管理的过程模型。

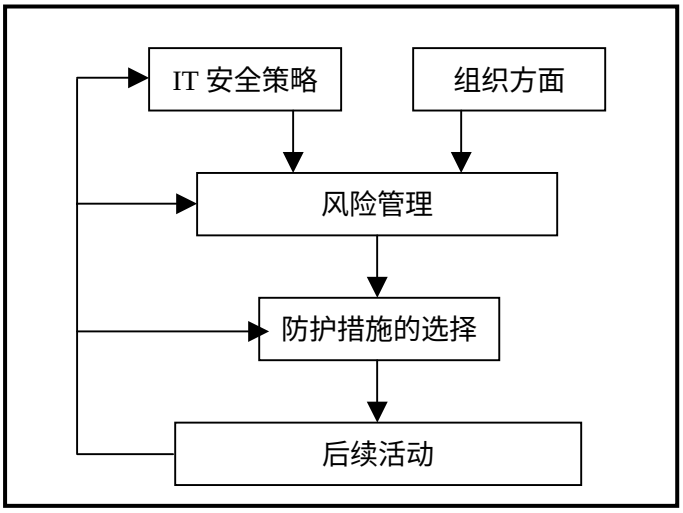


图 8：IT 安全管理过程模型

10 总结

在 ISO/IEC TR 13335 本部分讨论的概念和模型可以用于开发保护组织 IT 资产的战略。在组织内，需要不断的评审战略和相关的安全策略，并考虑在技术的开发和使用以及信息服务方面的快速变化。ISO/IEC TR 13335 其他部分内容将进一步描述这些概念和模型如何在组织内被有效的使用。