# 信息技术
# 安全技术
# 信息技术安全管理指南

第 4 部分：防护措施的选择

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。

# 目录

10.3.2 维护错误

10.3.3 恶意代码

10.3.4 伪装用户身份

10.3.5 消息的错误路由/重新路由

10.3.6 抗抵赖性

10.3.7 软件失效

10.3.8 供应中断（电力和空调）

10.3.9 技术性失效

10.3.10 传输错误

10.3.11 对计算机、数据、服务和应用程序的未授权访问

10.3.12 使用未经授权的程序或数据

10.3.13 对存储介质的未授权访问

10.3.14 用户错误

10.4 可用性的防护措施

10.4.1 破坏性攻击

10.4.2 存储介质的老化

10.4.3 通讯设备和服务中断

10.4.4 火灾，水灾

10.4.5 维护错误

10.4.6 恶意代码

10.4.7 伪装用户身份

10.4.8 消息的错误路由/重新路由

10.4.9 资源滥用

10.4.10 自然灾害

10.4.11 软件失效

10.4.12 供应中断（电力和空调）

10.4.13 技术性失效

10.4.14 盗窃

10.4.15 流量过载

10.4.16 传输错误

## 1 范围

ISO/IEC 13335 的第 4 部分提供了在考虑业务需求和安全关注点的情况如何选择防护措施的指南。第 4 部分描述了根据安全风险和关注点以及组织的特定环境选择防护措施的过程。它展示了如何达到适当的保护以及基线安全的应用是如何支持这一保护的。提供了关于第 4 部分中列出的方法如何支持第 3 部分中提出的 IT 安全管理的方法的解释。

## 2 引用标准

ISO/IEC 13335-1:1997 IT 安全管理指南－第 1 部分：概念和一般模型

ISO/IEC 13335-2:1997 IT 安全管理指南－第 2 部分：IT 安全的管理和策划

ISO/IEC 13335-3:1997 IT 安全管理指南－第 1 部分：IT 安全管理技术

ISO/IEC 10181-2:1996 信息技术－开放系统互联－开放系统安全结构：鉴权框架

ISO/IEC 11770-1:1996 密钥管理－第 1 部分：结构

## 3 定义

ISO/IEC TR 13335 第 1 部分的定义适用于第 4 部分。第 4 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。此外，还需使用下列定义：

3.1 鉴权 ：提供一个实体所声称身份的保证

3.2 识别： 唯一地确定一个实体唯一身份地过程。

## 4 目的

ISO/IEC TR 13335 第 4 部分的目的是为选择防护措施提供指南。这一指南适用于为 IT 系统选择防护措施的决策时使用，防护措施的选择可根据下列因素考虑：

- 根据 IT 系统的类型和特性；
- 根据安全关注点和威胁的广阔评审；
- 依照详细风险分析评审的结果。

除了这一指南之外，也提供相反的参考以展示通过使用包含防护措施的可获得的公用手册可以在那里支持防护措施的选择。

第 4 部分也展示了如何形成组织（或组织的一部分）范围基线安全手册。详细的网络安全防护措施主要在文件所引用的附录 A－H 中。ISO 目前正在开发关于网络安全的几个其他文件。

## 5 概述

第 6 条款介绍了防护措施的选择以及基线安全的概念。第 7 到第 10 条款阐述了如何建立 IT 系统的基线安全。为了选择适当的防护措，无论后续是否进行详细风险评估，都需要进行一些基本评估。这些评估在第 7 条款中描述，主要包括以下方面的考虑：

- 包括什么类型的 IT 系统（也就是说一个独立的 PC 还是与网络连接）；
- IT 系统的位置以及周围的自然环境是什么；
- 已存在的/计划的什么样的安全措施；
- 评估提供的为 IT 系统选择基线防护措施的信息是否充足。

第 8 条款概述了将要选择的防护措施。这些防护措施被分为三类：组织的、物理的（需要根据安全相关需求、关注点和限制来选择的防护措施）和 IT 系统特有的。对每一类的防护措施，都描述了防护措施最典型的类型，包括关于他们所提供的保护的简单介绍。这些类型的特定防护措施以及他们详细的描述，可以在本文件的附件 A－H 引用的基线安全文件中获得。为了便于这些文件的使用，用表格的形式为每种防护类型提供了在这一文件的防护措施类型与在附件中不同的文件的章节之间的交叉参考。

如果确定第 7 条款中描述的评估类型对于防护措施的选择足够详细，第 9 条款为 7.1 条款中描述的每种典型的 IT 系统系统提供了适用的防护措施目录。如果根据 IT 系统的类型来选择防护措施，那么单独的工作站、网络连接的工作站或服务器可能需要不同的基线。为了达到要求的安全水平，需要在特定的环境条件下选择适用的防护措施并将选择的防护措施与已存在的（或计划的）防护措施进行比对，并实施那些尚未实施的防护措施。

如果决定为了选择更有效和适合的防护措施需要更深入的评估，第 10 条款为这一选项提供了支持。第 10 条款考虑了高层安全关注点（根据信息的重要性）以及可能的威胁。因此，本部分建议在识别的安全关注点，考虑相关的威胁，并最后考虑 IT 系统的类型的基础上，建议防护措施。下图概述了在第 7、9 和 10 条款中描述的选择防护措施的方法。

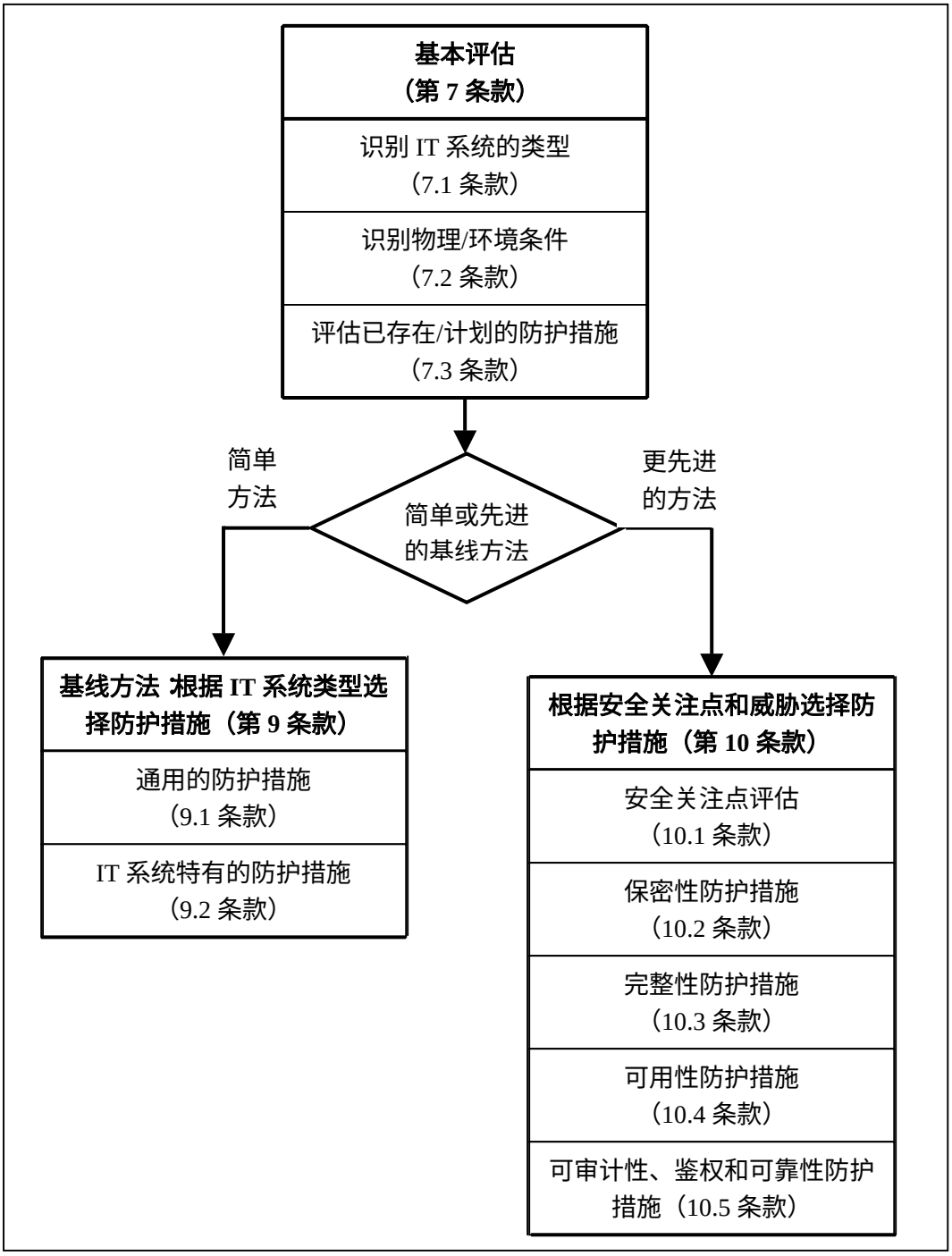


**图 1：根据 IT 系统类型或根据安全关注点和威胁选择防护措施**

第 9 和第 10 条款都描述了从不同的基线安全文档中选择防护措施的方法。这些基线安全文档既可以用于一个 IT 系统，也可以在定义的环境中用来形成一系列的适用于 IT 系统范围的防护措施。通过集中考虑的 IT 系统的类型，第 9 条款中建议的方法造成了一些风险并没有被充分管理，并且选择的一些防护措施并不适宜或必须的可能性。在第 10 条款中，建议的关注于安全关注点和相关威胁的方法可能产生一个更优化的系列防护措施。第 9 和第 10 条款可被用来支持防护措施的选择，而不需要更为详细的评估，无论如何都会落入基线保护的范围。然而，如果采用更为详细的评估，也就是说详细风险分析，第 9 和第 10 条款仍可支持防护措施的选择。

第 11 条款阐述了因为高的安全关注点和需求而需要进行详细风险分析的情况。ISO/IEC TR 13335 第 3 部分提供了关于风险分析的指南。第 11 条款描述了 ISO/IEC TR 13335 第 3 部分和第 4 部分的关系，以及如何将第 3 部分中描述的方法的结果用于支持防护措施的选择。它也阐述了可能影响防护措施选择的其他因素，如必须考虑的任何限制，必须满足的法律和其他要求等。第 11 条款中描述的方法不同于第 9 和第 10 条款中描述的方法。第 9 和第 10 条款中描述的方法为选择系列适合于特定环境提供了指南。这一方法不是基线方法，但是如论如何可用于选择防护措施以作为一些环境下基线防护措施的补充。作为选择，也可以单独使用该方法，而与基线保护无任何关系。

第 12 条款阐述了为整个或部分组织建立基线安全手册（或目录）的方法。为建立基线安全手册（或目录），应考虑以前识别的一个或一组 IT 系统的防护措施，并识别通用的系列防护措施。讨论其优点和缺点以利于组织作出合适的决策。

最后，第 13 条款对第 4 部分进行了总结。参考书目和附录 A－附录 H 概述了第 8 条款中引用的防护措施手册。

## 6 防护措施选择和基线安全概念的介绍

下列条款简单概述了防护措施选择的主题，以及在这一过程中如何和何时使用基线安全的概念。防护措施的选择有两种主要方法，也就是说基线方法和详细风险分析的方法。进行详细的风险分析也有几种不同的方法，其中之一就是在 ISO/IEC TR 13335 第 3 部分中详细介绍的被称为详细风险分析的方法。ISO/IEC TR 13335 第 3 部分也讨论了不同风险分析方法以及据此选择防护措施的优缺点。

进行详细的风险分析有助于更加广泛的理解风险。其可用于选择并实施与风险适宜的防护措施。这可以避免过多或过少的保护。因为这种方法需要花费数目可观的时间、精力和经验，因此可能更适合于处于高风险的 IT 系统，而对较低风险系统实施简单的方法即可。可使用高层风险分析来识别较低风险系统。高层风险分析并不需要正式或复杂的过程。可通过适用的基线安全来选择较低风险系统的防护措施。基线安全是组织为每种类型的 IT 系统规定的安全最低等级。可通过实施被称为基线防护措施的最小系列防护措施来达到这一基线安全等级。

因为防护措施选择过程的不同，本标准中考虑了两种适用于基线方法的不同方式：

- 当根据考虑的 IT 系统的类型和特性推荐防护措施时，使用基线方法；
- 当根据安全关注点和需求并将考虑的 IT 系统考虑在内时，使用基线方法。

将图 1 视作更大的图(图 2 所示)的一部分将有助于对本文件中提供的不同的并行的防护措施选择方式的有一个概要的了解。图 2 解释了 TR 13335 第 3 和第 4 部分的关系。

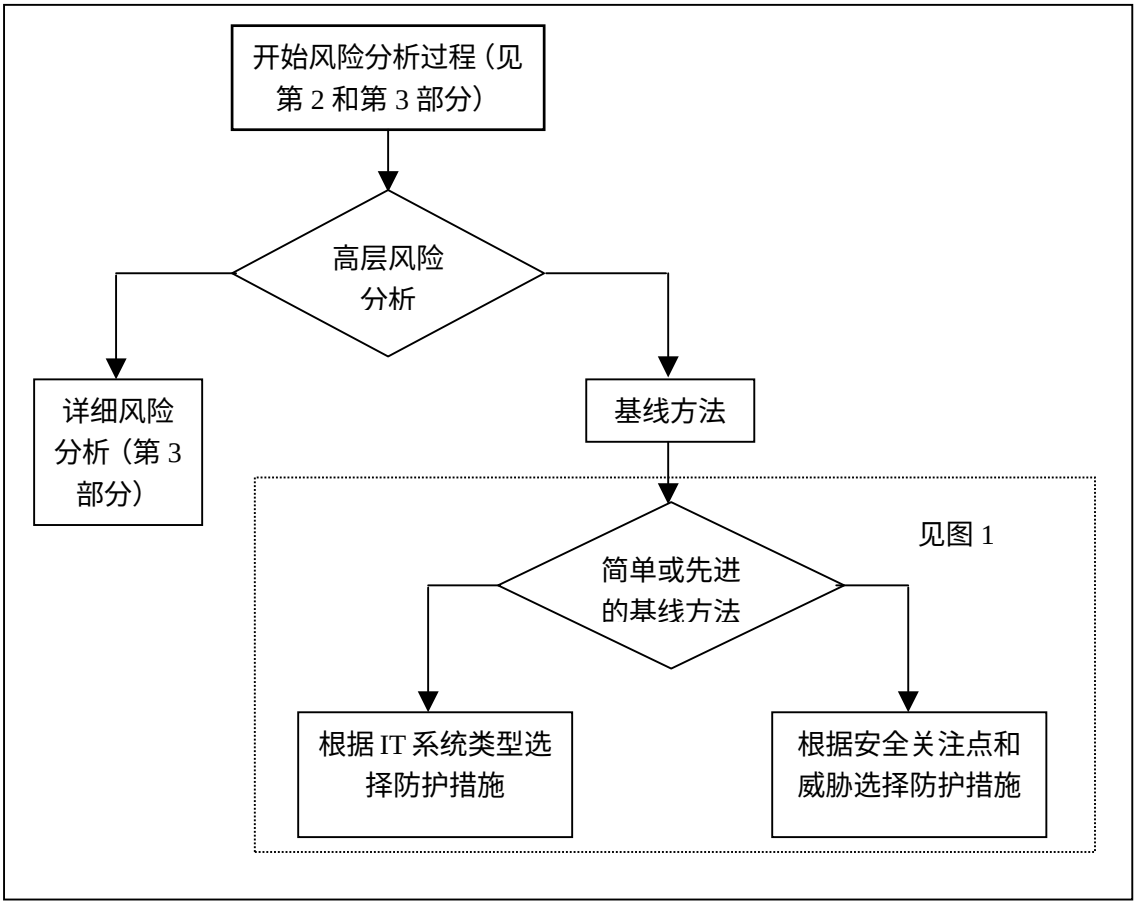


**图 2：防护措施选择的方法**

应根据选择过程所花费的资源、已感知的安全关注点以及考虑的 IT 系统的特点和类型，来选择使用的基线方法。如果组织不希望在防护措施的选择上（无论任何原因）花费过多的时间和精力，建议防护措施而不需进一步评估的基线方法可能是适合的。然而，如果组织的业务运行适度地依赖于 IT 系统或服务，和/或处理地信息是敏感的，可能需要额外的防护措施。在这种情况下，强烈推荐至少对信息的重要性和可能的威胁进行高层风险分析，以更好的关注于最有效的保护 IT 系统所需的防护措施。如果组织的业务运行严重地依赖于 IT 系统或服务，和/或处理的信息是极为敏感的，风险可能很高，详细的风险评估是识别适宜的防护措施的最佳方式。

应基于详细的风险分析识别特定的防护措施，适用于：

- 本报告中考虑的类型不能恰当地代表所考虑的 IT 系统的类型；
- 认为这些条款中建议的解决方案与业务或安全需求不相当；
- 因为潜在的高风险或 IT 系统对于业务的重要性，为稳妥起见需要进行更为详细的评估。

需要注意的是，即使进行风险分析，对 IT 系统实施基线防护措施还是有意义的。

组织必须自己作出的第一个决策是是否是否使用基线方法，或作为更广泛的风险分析战略的一部分（见 ISO/IEC TR 13335 的第 3 部分）。在做这个决策时，需要注意的是，在自己使

用基线方法的过程中，选择防护措施的咨询过程相比采纳更为广泛的风险分析战略而言可能导致较少的优化安全。然而，选择防护措施需要较少的资源和成本，以及至少可以为所有的 IT 系统取得最低等级的安全，可能是组织自己决定采用基线方法的愿意。

可以通过识别和应用一系列适合于多种低风险环境的相关的防护措施来达到 IT 系统的基保护，也就是说，他们至少满足最小的安全需求。例如，可以通过使用目录来识别适当的基线安全防护措施。目录为 IT 系统类型建议了系列的防护措施，以保护他们免受常见威胁的影响。这些防护措施目录包含了防护措施目录和/或详细的防护措施的有关信息，但是通常来说并未指明在特定的环境下应使用那一防护措施。如果组织的（或组织部分的）IT 系统性质和提供的服务相似，那么通过基线方法选择的防护措施可能适用于所有的 IT 系统。图 3 展示了使用在这一文件中讨论的基线方法的不同方法。

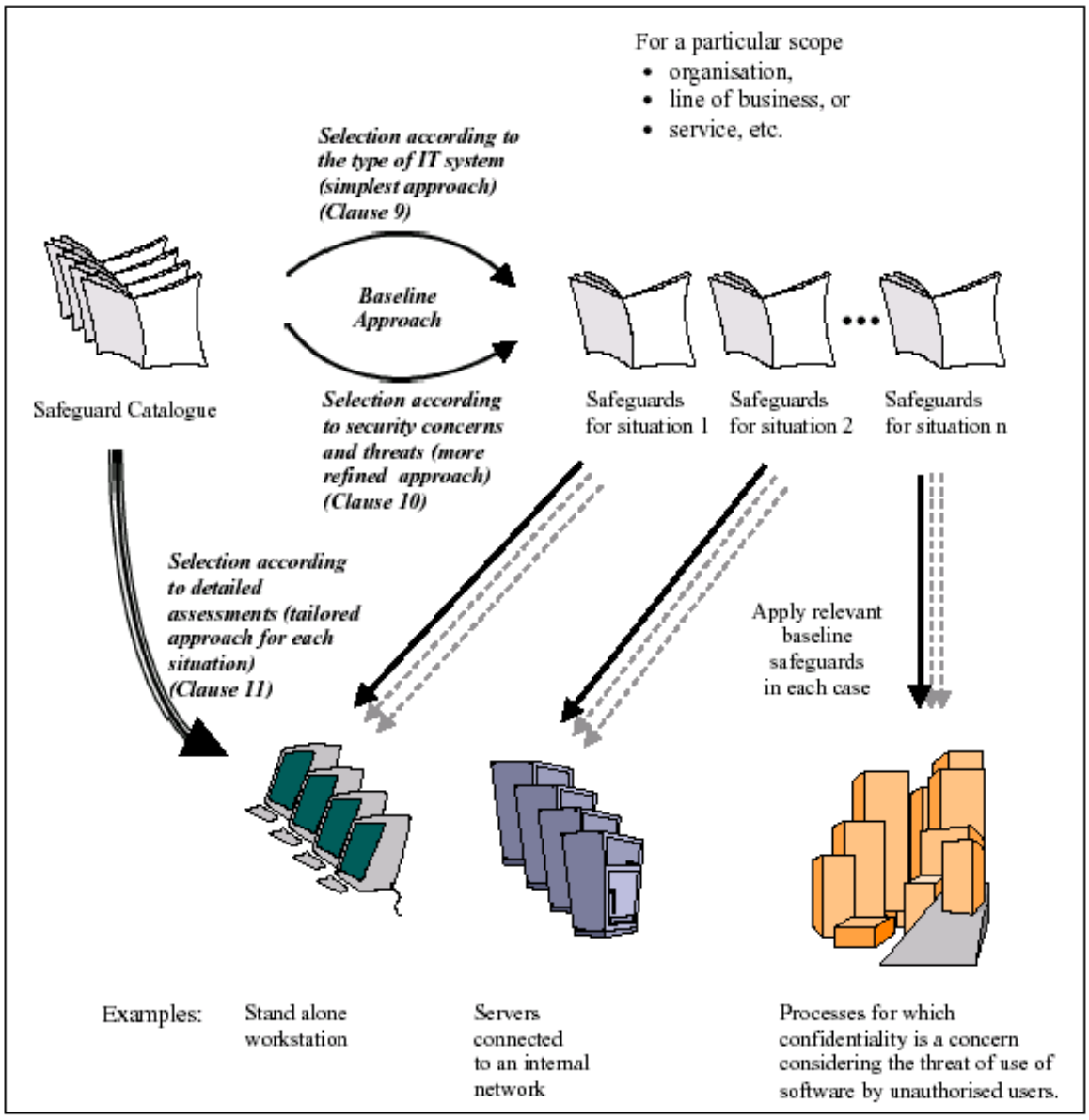


**图 3：防护措施选择的方法**

如果决定对整个或部分组织实施基线安全，那么组织需要决定组织的那些部分适合于使用同样的基线进行保护，以及这一基线应达到的安全等级。在使用基线安全的大多数情况下，不允许较低的安全等级，而且在合理和需要时，还需实施额外的防护措施以管理中等或高风险。基线可以反映组织的平均等级，也就是说，如果是合理的，例如根据风险分析的结果，那么允许低于或高于基线的例外。

基线安全的一个优点是如果它应用于一组 IT 系统，那么在这一组内可以依赖一个特定的安全等级。在这些情况下，开发并文件化组织或部门范围的安全防护措施目录是非常有益的。

## 7 基本评估

在进行防护措施选择时，通常需要了解被考虑的 IT 系统的类型和特性的一些知识。因为者对于为保护系统而选择的防护措施有着重要影响。并且，这也有助于了解基础设施，如，建筑物、房间等。与防护措施选择有个的另外一个重要因素是已存在的和/或计划的防护措施的评估。这可避免不必要的工作以及时间、精力和金钱的浪费。因此，极力推荐将第 7 条款描述的评估作为防护措施选择的基础。在选择防护措施时，也应考虑业务要求和组织对安全的态度（也见 TR 13335 第 2 部分）。最后，需要确定这些评估是否为基线防护措施的选择提供了足够的信息，或是否需要进行详细的评估（如第 10 条款所述）或详细的风险分析（第 11 条款阐述）。

### 7.1 识别 IT 系统的类型

为评估已存在或计划的 IT 系统，应将考虑的 IT 系统与下列组件进行比较，并应识别代表系统的组件。在第 9 条款中为下面列出的每个组件都建议了防护措施。可供选择的组件是：

- 单独的工作站；
- 与网络连接的工作站（没有共享资源的客户）；
- 与网络连接的、分析资源的服务器或工作站。

### 7.2 识别物理/环境条件

环境评估包括识别支持已有的或计划的 IT 系统的物理性基础设施，并识别相关的已有的和/或计划的防护措施。因为所有的防护措施都应与物理环境保持一致，所以这些评估对于成功的选择是至关重要的。当考虑基础设施时，下列问题可能有所帮助。读者也应考虑是否需要将组织的环境和任何特定的环境考虑在内。

- 周界和建筑物
  - 建筑物位于那里——在有周界围墙的自己的地点内，还是在有着大量交通的街道边？
  - 建筑物是单独使用的还是共用的？
  - 如果共用，那么其他使用者是谁？
  - 那些是敏感/关键区域？

- 访问控制
  - ✧ 谁访问建筑物？
  - ✧ 是否存在物理访问控制系统？
  - ✧ 建筑物结构的如何结实？
  - ✧ 门窗等是否结实，以及对他们实行什么样的保护？
  - ✧ 建筑物是否有保安人员？如果有，那么是每天 24 小时值班，还是仅仅在工作时间值班？
  - ✧ 放置关键 IT 设备的建筑物或房间是否安装了入侵报警？
- 实施的保护
  - ✧ 如何保护放置 IT 系统的房间？
  - ✧ 在哪里，安装了什么样的火灾检测、报警和灭火设备？
  - ✧ 在哪里，安装了什么样的水/液体泄漏、报警和除湿设备？
  - ✧ 是否使用了诸如 UPS、管道和空调（控制温度和湿度）等支持性设施？

通过回答这些问题，可以容易地识别已有的物理和相关的防护措施。值得注意的是，当考虑建筑物地点以同时识别关于门、锁、物理访问控制和程序的问题时，这并不是一个浪费时间的行为。

### 7.3 评估已有的/计划的防护措施

评估完物理环境条件和 IT 系统组件后，应识别所有其他已有的或计划的防护措施，以避免重复选择已有的或计划的防护措施。并且，了解已实施的或计划的防护措施，有助于选择与他们共同作用的后续的防护措施。当选择防护措施时，应考虑已有的防护措施与选择的防护措施的符合性。一个防护措施可能与其他防护措施冲突，或阻碍其他防护措施的成功运行和提供保护。

下列活动有助于识别已有的或计划的防护措施：

- 查阅包含防护措施信息的文件（如 IT 安全计划或概念）——如果安全过程被很好的文件化，那么文件应该列出了所有已有的或计划的防护措施以及他们的实施情况；
- 与负责人（也就是 IT 系统安全管理人员、建设管理人员或运行管理人员）和用户共同检查被考虑的 IT 系统的哪一防护措施被真正的实施；
- 巡查建筑物以观察防护措施，将这些防护措施与应采取的防护措施进行比较，并检查已实施的防护措施是否正确和有效地运行。

可能会发现，已有的防护措施超过了目前的安全需求。在这种情况下，应考虑移除这些防护措施。如果考虑移除冗余或不需要的防护措施，应考虑安全和成本两个因素。因为防护措施互相影响，移除一个冗余的防护措施可能会减弱整体的安全。此外，将防护措施置之不理

可能比益处更经济。当然了，如果防护措施的维护成本很高，移除他们可能更经济。

## 8 防护措施

下列条款描述了为改进安全而实施的可能的防护措施。这些防护措施的一部分是机制，其他的是应实施的程序。8.1 条款总结了适合 IT 系统的组织和物理防护措施。8.2 条款考虑了 IT 系统特有的防护措施。应注意的是，只是描述了防护措施而没有提及选择防护措施的方法，也就是说，可以用任何方式来选择这些防护措施中的一些，其他的防护措施可能只能被详细的风险分析所识别。

为更加容易地描述防护措施的不同类型，引入了防护措施目录。下列条款对这些防护措施目录进行了简单介绍，以及什么类型的防护措施与他们有关。此外，提供了在附录 A－H（参见文件末尾的参考目录）中列出的手册参考，并指出了在那里可以获得这里提及的防护措施的更为详细的信息。

### 8.1 组织的和物理的防护措施

在本条款的末尾，与每一子条款相关的表格展示了可以从那里获取提及的防护措施目录的额外的信息。

### 8.1 IT 安全管理和策略

这一防护措施目录包含了关于 IT 安全管理的所有防护措施，应该做什么的计划，为这些过程分配职责以及其他所有相关的活动。这些防护措施已经在 TR 13335 第 1——第 3 部分中介绍过。这些防护措施的目的是在组织内达到一个适当的和一致的安全等级。这列一领域的防护措施在下文列出。

**1. 公司 IT 安全策略**

应开发文件化的公司 IT 安全策略。公司 IT 安全策略描述了在组织内如何管理、保护和分发资产的规则、指南和惯例。它应展示 IT 系统安全策略文件和需要，并为其内容提供指导。

**2. IT 系统安全策略**

应为每个 IT 系统开发 IT 系统安全策略。IT 系统安全策略描述了已有的和应实施的防护措施。为确保这一系统的安全而应遵循的程序，可能时，应总结判定防护措施合理性的安全关注点和/或风险。

**3. IT 安全管理**

IT 安全管理应正式化并在组织内以一种适合于组织规模的方式协调进行，例如，通过建立 IT 安全关注点并为每个 IT 系统的安全指定负责任（通常是 IT 安全管理人员）。

**4. 分配职责**

应根据公司的 IT 安全策略和 IT 系统安全策略，以文件化的形式明确分配组织范围内的 IT 安全职责。

**5. IT 安全组织**

应组织支持 IT 安全（也就是说，获得，与其他组织的协作）的所有业务过程，从而以一种安全的方式提供支持。

**6. 资产识别和赋值**

应识别组织内和每个 IT 系统的所有资产，并评估他们对业务运作的价值。

**7. IT 系统的批准**

应根据 IT 安全策略批准 IT 系统。批准过程的目的在于确保实施的防护措施提供了适当等级的保护。应考虑的是，IT 系统可能包括网络和潜在的通讯。

### 8.1.2 安全符合性检查

保持与所有防护措施、相关的法律法规和策略的符合性是重要的，因为只有用户遵守他们、系统符合他们，任何的防护措施、规则或策略才能起作用。这一良宇的防护措施在下面列出。

**1. 与 IT 安全策略和防护措施的符合性**

应定期进行检查，以确保象在公司 IT 安全策略、相关 IT 系统安全策略和其他相关文件中（如，安全操作程序文件和灾难恢复计划）列出的那些防护措施被正确地实施和正确和有效地使用，需要时，还可进行测试。

**2. 与法律法规要求的符合性**

应进行上文提及的符合性检查，以确保满足 IT 系统所处国家的法律法规的要求。如果存在类似的法律，可能包括关于数据和隐私保护、软件版权、组织记录的保护、IT 系统滥用或加密的法规。

### 8.1.3 事故处置

组织内的每个人都应该了解尽快报告安全事故的需要。安全事故包括软件失效和发现的弱点。组织应为其提供一个报告计划。事故处置包括：

**1. 报告安全事故**

每位员工均有报告安全事故的义务。安全事故可以是被发现的也可以是工具报告的。为了更加有效的处置安全事故，组织应在组织内提供一个报告计划和联络点。

**2. 报告安全弱点**

如果用户发现了任何安全相关的弱点，他们应尽快向有关责任人报告。

**3. 报告软件失效**

如果用户发现了任何安全相关的软件失效，他们应尽快向有关责任人报告。

**4. 事故管理**

应建立支持事故保护的管理过程，以检测、报告和适当响应事故。应收集并评价事故有关信息，以在今后避免事故，以及如果发生事故减少损害。

### 8.1.4 人员

这一类的防护措施应减少因人员（永久或临时）的错误、无意或蓄意的违反安全规则所导致的安全风险。下文列出了这一领域的防护措施。

**1. 针对永久和临时雇员的防护措施**

所有的雇员应了解他们的安全职责和角色。应用文件的形式阐述人员所应遵守的所有安全相关的程序。在雇佣前应进行招聘检查，需要时，还应签订保密协议。

**2. 针对合同人员的防护措施**

应对合同人员（如，清洁或维护人员）和其他参观人员进行控制。尤其是长期的合同人员在访问（物理或逻辑的）组织的 IT 设施前应签署保密协议。

**3. 安全意识和培训**

所有使用、开发、支持和访问 IT 设备的人员应定期接受安全意识简报和资料。这应确保人员意识到处理的信息对于业务的重要性、相关的威胁、脆弱点和风险，进而理解为什么需要防护措施。应对用户进行使用 IT 设施的培训，以避免错误。对于选定的人员，如，IT 安全管理人员、安全管理者，可能需要更多的特定安全培训。

**4. 惩戒过程**

所有的雇员应意识到违反（无论是蓄意的还是无意的）组织范围和特定的 IT 系统安全策略或其他文件化的安全协议的后果。

### 8.1.5 操作问题

这一领域的防护措施目的在于保持安全的所有程序，以及使用的 IT 设备和相关系统的正确和可靠的功能。这些防护措施的大多数可以通过实施组织的程序来实现。操作性防护措施需和其他防护措施联合使用，如物理性和技术性的防护措施。操作问题这一领域的防护措施在下文列出。

**1. 配置和变更管理**

配置管理是追溯 IT 系统变更的过程。它的首要安全目的是确保 IT 系统的变更不降低防护措施的有效性和提供的整体安全。变更管理有助于当 IT 系统发生变化时识别新的安全隐患。

**2. 容量管理**

容量管理用于避免因容量不足而导致的故障。当评估 IT 系统所需容量时，应考虑未来的容量需求和当前的趋势。

**3. 文档**

IT 配置和操作的所有方面应形成文件，以确保连续性和一致性。IT 系统的安全也应在 IT 系统安全策略、安全操作程序文件、业务连续性战略报告和计划中形成文件。文件应是更新的并可获得。

**4. 维护**

应正确维护设备以确保其持续的可靠性、可用性和完整性。应在合同中全面规定维护提供者应满足所有的安全要求。维护应根据供应商的合同进行，并只能由授权人员实施。

**5. 监视安全相关变化**

应监视影响、威胁、脆弱点、风险以及他们相关特性的变化。监视应包括已存在的和新的方面。也应监视系统所处环境的变化.

**6. 审计踪迹和日志**

应利用服务提供商的审计和日志能力（如，审计踪迹记录和分析设施）、网络（如，防火墙或路由器的审计设施）和应用程序（如，消息应用程序或传输应用程序的审计设施）来记录安全相关事件的详细信息。这包括轻易识别的未授权的或错误事件的详细信息，以及貌似正常的可能需要后续分析的事件的详细信息。应定期评审审计踪迹和日志，以检测未授权的活动并允许采取适当的纠正措施。应分析日志中重复发生的类似时间，这可能揭示了不充分的防护措施所暴露的脆弱点和威胁。这样的分析可能解释，用貌似不相关事件的方式所采取的未授权的活动或安全问题的根本原因。

[注：本文所使用的系统和应用程序的“审计能力”和“日志能力”是同一意思。有时，这样的能力可用于支持更广泛的财务完整性审计，他们仅仅满足了这样活动的部分要求，读者应了解这一技术术语的使用。]

**7. 安全测试**

应进行安全测试以确保所有的 IT 设备和所有相关软件组件以安全方式运行。安全测试应包括在 IT 系统安全策略中定义的安全要求、测试计划，并应建立接受准则以展示达到了的安全要求等级。

**8. 介质控制**

价值控制包括为磁带、硬盘、打印输出和其他介质提供物理和环境保护以及可审计性的许多防护措施。这包括标识、日志、完整性验证、物理访问控制、环境保护、传输和安全处置。

**9. 确保存储销毁**

当信息不再需要时，应保证存储设备中以前写入信息的保密性。应确保含有保密资料的文件被消除或物理性覆盖或其他的破坏方式——删除功能通常做不到这一点。用户应可获得经负责人批准的用于完全和安全销毁的设施。

**10. 指责分离**

为了减少风险和特权滥用的可能性，需要并且可能时，应实施职责分离。尤其是当职责和功能联合时，可能导致欺骗防护措施或审计时，或员工可能获得不应有的利益时，应实施职责分离。

**11. 正确使用软件**

应确保无拷贝授权的资料的拷贝，并且遵守产权软件的许可证协议。

**12. 软件变更控制**

当进行变更时（软件变更控制仅仅适用于软件，而在本条款中第一个防护措施领域中描述

的配置和变更管理作为一个整体适用于 IT 系统和他们的环境），应实施软件变更控制以保持软件的完整性。应建立软件变更控制程序。软件变更控制程序应管理所有的变更，并确保在整个过程中保持安全。这包括变更的授权、中间方案的安全考虑和最后方案的安全检查。

### 8.1.6 业务连续性计划

为保护业务尤其是关键业务过程免受重大故障和灾难的影响并减少因类似事件所造成的损失，应建立有效的业务连续性计划。业务连续性计划包括中断/灾难恢复计划、战略和计划。这包括下列的防护措施。

**1. 业务连续性战略**

应基于因不可用、修改或破坏所导致的已识别的潜在的负面业务影响，来开发与考虑的 IT 系统有关的，包括中断计划/灾难恢复计划、战略的业务连续性计划，并形成文件。

**2. 业务连续性计划**

应基于业务连续性战略来开发包括中断和灾难恢复计划的业务连续性计划，并形成文件。

**3. 业务连续性计划的测试与更新**

在接受以前，应对业务连续性计划进行彻底测试以确保其在发生灾难或故障时可以真正发挥作用，并且确保组织相关的人员都知晓该计划。因为业务连续性计划很容易就过期了，所以定期对其进行更新是重要的。需要时，也应更新业务连续性战略。

**4. 备份**

应备份所有的重要文件、其他的业务数据和重要系统程序和文档。备份的频率应与信息的重要性和业务连续性计划保持一致。备份资料应实施安全的异地存储，并定期检查其恢复的可靠性。

### 8.1.7 物理安全

这一领域的防护措施主要是针对物理保护的。他们应和 7.2 条款中讨论的环境的识别一起考虑。下列几个项目适用于建筑物、安全区域、计算机房间和办公室。防护措施的选择依赖于被考虑的建筑物的那哪一部分。这一领域的防护措施在下文列出。

**1. 具体保护**

保护建筑物的物理性防护措施包括围墙，物理访问控制、，结实的墙壁、门和窗户。建筑物内的安全区域应通过诸如物理访问控制、警卫等保护以免受未授权的访问。支持重要业务活动的 IT 设备（如服务器）和有关的软件和数据可能需要安全区域。对类似安全区域的访问应限制在必需的最少人员，并详细记录在日志中。应安全存储所有的检测和控制设备，并严格控制其使用。

**2. 火灾防护**

应保护设备和周围区域，包括对他们的访问，免受从建筑物其他区域或临近建筑物蔓延火灾的影响。应最小化位于放置设备的房间/区域周围的火灾警报。也应防范期起火点和/或

影响放置关键设备的所有房间/区域。防护措施包括火灾和烟雾探测，报警和灭火。需要注意的时，火灾保护并不能保护 IT 系统免受会或其他灭火方法的影响。

**3. 水/液体防护**

应在可能发生严重洪水的区域或其他液体可能泄漏的区域，安置必要的设备。当显著的洪水威胁存在时，应提供适当的保护。

**4. 自然灾害保护**

放置关键设备的建筑物应免受闪电的影响。并且，也应保护关键设备本身免受闪电的影响。可以通过远离可能发生自然灾害的区域或实施业务连续性战略和计划的方式来防范自然灾害。

**5. 防范盗窃**

为实施严格的控制，设备的所有项目都应该具有唯一的可识别性，并保持一个清单。应鼓励保安人员和/或接待员检查未经授权带离建筑物的房间/区域的设备和介质。应适当保护存储敏感信息和产权软件的便携式介质（如软盘）。

**6. 电力和空调**

如果需要时，应保护所有的 IT 设备免受断供电中断的影响。应提供适宜的电力供应，需要时，应引入不间断电力供应。保护的另一个目的是确保可容忍的温度和湿度。

**7. 电缆**

应保护传输数据或支持 IT 服务的电力和通讯电缆免遭窃听、损害和过载。应对电力实施物理性保护以使其免受无意或蓄意的损害，并根据其目的进行适当的选择和铺设。如果计划时仔细考虑将来的发展可以避免许多问题。只要可行，就应确保电缆免受窃听的威胁。

**表 8.1.1－IT 安全管理和策略**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 公司 IT 安全策略 | **3.1** | **--** | **1.1,1.2** | **5.1** | ***.3.1.1** | **3** | **--** | **5.1,5.2** |
| 2. IT 系统安全策略 | **--** | **--** | **1.1,1.2** | **5.2,5.3** | ***.3.1.1** | **3** | **--** | **5.2,5.3** |
| 3. IT 安全管理 | **4.1.1,4.1.2** | **--** | **1.1,1.2** | **6** | ***.3.1.1** | **4** | **2.1** | **6** |
| 4. 职责分配 | **4.1.3** | **--** | **1.3** | **2.4,2.5,3** | ***.3.1.1** | **4** | **2.1** | **2.4,2.5,3** |
| 5. IT 安全组织 | **4.1** | **--** | **1.2** | **3.5** | **--** | **4** | **2.2** | **3.5** |
| 6. 资产识别和赋值 | **5** | **--** | **2.2** | **7.1** | **--** | **5.6,7.1** | **5.1** | **7.1** |
| 7. IT 系统的批准 | **4.1.4** | **--** | **--** | **8** | **5** | **--** | **6.7** | **8,9** |

*代表介于 6-11 之间的任何数字。

**表 8.1.2－安全符合性检查**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 与 IT 安全策略和防护措施的符合性 | **12.2** | **--** | **1.2** | **10.2.3** | **--** | **10.2** | **7.1，7.2** | **9.4，10.2.3** |
| 2. 与法律法规要求的符合性 | **12.1** | **--** | **3.1，3.2** | **6.3，10.2.3** | **6.3.11** | **8.18，10.2** | **8.1** | **1.5，2.9，6.3，10.2.3** |

**表 8.1.3－事故处置**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 报告安全事故 | **6.3.1** | **--** | **M2** | **12** | **--** | **10.4** | **--** | **12** |
| 2. 报告安全弱点 | **6.3.2** | **--** | **M2** | **12** | **--** | **10.4** | **--** | **12** |
| 3. 报告软件故障 | **6.3.3** | **--** | **M2** | **12** | **--** | **10.4** | **--** | **12** |
| 4. 事故管理 | **8.1.3** | **--** | **M2** | **12** | **--** | **10.4** | **--** | **18.1.3** |

**表 8.1.4－人员**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 针对永久和临时人员的防护措施 | **6.1** | **--** | **3.2，M3** | **10.1** | ***.3.9** | **9.2** | **4.1，2.2** | **10.1** |
| 2. 针对合同人员的防护措施 | **6.1** | **--** | **--** | **10.3** | ***.3.9** | **9.2** | **4.1，2.2** | **10.3** |
| 3. 安全意识和培训 | **6.2** | **--** | **3.2，M3** | **13，10.1.4** | ***.3.9** | **9.1** | **4.2，2.2** | **13，10. 1.4** |
| 4. 惩戒过程 | **6.3.4** | **--** | **3.2，M3** | **--** | ***.3.9** | **9.2.6** | **2.2.1** | **13.1** |

*代表介于 6-11 之间的任何数字。

**表 8.15－操作性问题**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 配置和变更管理 | **8.2，10.5** | -- | -- | **14.3，8.4.1** | -- | **7.4** | **9** | **14.3，8.4.1，8.4.4** |
| 2. 容量管理 | **8.2.1** | -- | -- | -- | -- | -- | -- | -- |
| 3. 文件 | **8.1.1，8.6.3** | -- | **M2** | **14.6** | -- | **8.4.6，8.5.7，8.7** | -- | **14.6** |
| 4. 维护 | **7.2.4** | -- | **M2** | **14.7** | ***.3.6** | **8.1.4，8.10，5，10.1** | **6.5** | **14.7** |
| 5. 监视安全相关变化 | -- | -- | **1.2** | **7.3.3** | -- | **7.4，8.1.3，8.2.5，8.3.7** | **6.7** | **7.3.3．8.4.4** |
| 6. 审计踪迹和日志 | **8.4** | -- | **M2** | **18** | -- | **7.3，8.1.8，8.2.10，8.9.5** | **6.7** | **（18）** |
| 7. 安全测试 | -- | -- | **M2** | **8.4.3** | -- | **8.3.5，** | **6.7，3** | **8.4.3** |
| 8. 介质控制 | **8.6** | -- | **8，M2** | **14.5** | ***.3.5** | **8.4-8.14** | **5** | **14.5** |
| 9. 保证存储删除 | -- | -- | **M4** | -- | -- | **8.1.9** | **6.3，5** | **14.5.7** |
| 10. 职责分离 | **8.1.4** | -- | **M2** | -- | -- | -- | -- | **10.1.1** |
| 11. 正确的软件使用 | **12.1.2** | -- | **M2** | -- | ***.3.8** | **8.3** | **6.3** | **14.2** |
| 12. 软件变更控制 | **10.5.1，10.5.3** | -- | **M2** | -- | ***.3.8** | **8.3.7** | **6.3** | **8.4.4，14.2** |

*代表介于 6-11 之间的任何数字。

**表 8.1.6－业务连续性计划**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 业务连续性战略 | **11.1.1，11.1.2** | -- | **3.3，M6** | **11.2。，11.3，11.4** | ***.3.3** | **8.1.9，8.1.7，8.4.5，8.5.5，8.6.5，8.7.5，8.8.3，8.19 8.19** | **7.3，7.4，7.5** | **11.2，11.3，11.4** |
| 2. 业务连续性计划 | **11.1.3，11.1.4** | -- | **3.3，M6** | **11.5** | ***.3.3** | | -- | **11.5** |
| 3.测试并更新业务连续性计划 | **11.1.5** | -- | **3.3，M6** | **11.6** | ***.3.3** | | -- | **11.6** |
| 4. 备份 | **8.4.1** | -- | **3.4** | **14.4** | ***.3.2.4** | -- | **7.1，7.2** | **14.4** |

*代表介于 6-11 之间的任何数字。

**表 8.1.7－物理安全**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 原料保护 | 7.1 | -- | 4.1，4.3，M1 | 15.1 | *.3.1.2 | 8.1.1，8.6.2，8.9.1 | 3.1，3.4.4 | 15.1 |
| 2. 火灾保护 | 7.2.1 | -- | -- | 15.2 | *.3.1.4 | 8.1.1，8.6.2，8.9.1 | 3.1，3.2，7.5 | 15.2 |
| 3. 水/液体保护 | 7.2.1 | -- | M2 | 15.5 | *.3.1.4 | 8.1.1，8.6.2，8.9.1 | 7.5 | 15.5 |
| 4. 自然灾害保护 | 7.2.1 | -- | M2 | 15.4 | *.3.1.4 | 8.1.1，8.6.2，8.9.1 | 7.5 | 15.4 |
| 5. 防范盗窃 | 7.1 | -- | 1.2 | 15.1 | *.3.1.3 | 8.1.1，8.6.2，8.9.1 | 3.3，3.4.4 | 15.1 |
| 6. 电力和空调 | 7.2.2 | -- | M2 | 15.6 | *.3.4 | 8.1.1，8.6.2，8.9.1 | 3.2，7.3 | 15.6 |
| 7. 线缆 | 7.2.3 | -- | 4.2，M1 | -- | -- | 8.1.1，8.6.2，8.9.1 | 8.2 | 15，15.1，15.7 |

*代表介于 6-11 之间的任何数字。

### 8.2 IT 系统特有的防护措施

在本条款的末尾，与个子条款有个的表格提供了从那里获取关于涉及的防护措施目录的额外信息。

#### 8.2.1 识别和鉴权（I&A）

识别是用户向系统提供声称身份的方法。鉴权是验证这一声明的方法。下列方式如何实现识别和鉴权（也可以用其他方法分类 I&A 机制）的几个示例。

**1. 基于用户所知的 I&A**

口令是最典型的提供基于用户所知的并与用户识别过程联系的 I&A 方法。应控制口令的分配和定期更换。如果是用户自己选择口令，那么用户必须了解口令设计和处置的通用规则。可用软件来支持，例如通过限制通常口令或模式和字母的使用。需要时，应安全存储口令的拷贝，以允许授权的访问，当用户不可用或忘记口令时。基于用户所知的 I&A 也可利用加密方法和鉴权协议。这一类型的识别和鉴权也可以用于远程 I&A。

**2. 基于用户所有的 I&A**

用户所有的用于 I&A 的客体可以是记忆标记或智能标记。记忆标记就是通常应用在信用卡的背面使用的磁性物质。基于用户所有的（卡）和用户所知（PIN）来提供鉴权。智能标记的典型应用是智能卡。

**3. 基于用户所是的标记**

生物鉴权技术使用个体独特的特征或特性以验证用户的身份。这可以是指纹、掌纹、视网膜模式和声音模式或手写签名等。有关的详细信息可以被安全的存储在智能卡或系统中。

#### 8.2.2 逻辑访问控制和审计

这一领域的防护措施被用来：

- 限制对信息、计算机、网络、应用程序、系统资源、文件和程序的访问；
- 在审计踪迹中记录错误或用户行为的详细信息并分析记录的详细信息，以用一种适当的方式检测和处置安全违规。

执行访问控制的一个常用方法就是联合使用 I&A 和访问控制列表。访问控制列表规定了用户允许访问那些文件、资源等，以及访问采取的形式。在下文列出了逻辑访问控制和审计领域的防护措施。

**1. 访问控制策略**

应为每一个或每一组用户规定清晰的访问控制策略。这一策略应根据业务要求，例如可用性、生产率和“须知”原则，来授予访问权限。通常的观点是“和需要一样多的权力，尽可能少的权力”。分配访问控制权限时，应考虑组织对待安全的态度（如，开放的还是限制的），满足业务需求的文化并被用户所接受。

**2. 用户对计算机的访问**

应实施计算机的访问控制以防止对计算机的未授权访问。如果可能，应识别并验证每个授权用户的身份，并记录成功的和不成功的登陆尝试。可以将口令和其他任何的 I&A 方法作为计算机的访问控制的补充。

**3. 用户对数据、服务和应用程序的访问**

应实施访问控制以保护计算机或网络内的数据和服务免受未授权的访问。这可以在适当的 I&A 机制（见上面的 8.2.1 条款）的帮助下进行，网络服务和网络配置的适当交互也可以确保只能对 IT 服务进行授权访问（权限的严格分配）。为了放置对应用程序的未授权访问，应引入基于角色的访问控制。基于角色的访问控制根据用户的业务功能来允许访问。

**4. 访问权限的评审和更新**

如果安全或对访问的业务需求发生变化，那么需要定期评审并更新赋予用户的所有访问权限。应更为频繁的对特殊的访问控制权限进行评审，以确保他们没有被滥用。如果不再需要访问权限时，应立即收回。

**5. 审计日志**

应记录 IT 支持所完成的所有工作，并定期检查这些日志；这包括成功和不成功的登陆系统的企图，对数据访问的日志，使用的 IT 系统功能等。也应记录错误，并定期评审这些日志。应按照数据保护和隐私法律的规定来使用这些数据。例如，他们只被存储限定的时间，并且仅用于安全违规的检测。

### 8.2.3 防范恶意代码

可以通过外部的连接、便携式硬盘中的文件和软件，将恶意代码引入系统。除非实施了适宜的防护措施，否则在损失发生之前，可能无法检测恶意代码的存在。恶意代码可能导致安全防护措施的破坏（如，口令的捕获和泄漏）、信息的不期望泄漏、信息的不期望变更、系统完整性的损失、信息的破坏和/或系统资源的未授权使用。恶意代码可能是下列类型：

- 病毒；
- 蠕虫；
- 特洛伊木马。

恶意代码的携带者可能是：

- 可执行软件；
- 数据文件（包含，可执行的宏，如，word 处理文件或电子表格）；
- WWW 网页的可执行内容。

恶意代码可以通过下列途径传播：

- 软盘；
- 其他可移动介质；
- 电子邮件；

- 网络；
- 下载。

恶意代码的引入可以是用户蓄意行为的结果，或通过用户无法察觉的系统层次的相互作用。可以使用下列的防护措施来防范恶意代码：

**1. 扫描**

可以用特殊的扫描软件和完整性检查来检测和清除不同形式的恶意代码。扫描软件可以用在线或离线的方式运行。扫描软件的在线运行提供了主动的保护，也就是说在感染发生和对 IT 系统造成损害之前检测（和清除，可能时）恶意代码。扫描软件可以用于单独的计算机、工作站、文件服务器、电子邮件服务器和防火墙。然而，用户和管理员应意识到不能依靠扫描软件来检测所有的恶意代码（或，甚至一个特定类型的所有恶意代码），因为新形式的恶意代码总是不断地出现。

**2. 完整性检查**

典型的，需采用其他形式的防护措施以增强扫描提供的保护。例如，用校验求和来检查一个程序是否已经被修改。完整性检查软件应该是提供防范恶意代码的技术性防护措施的内在部分。这一技术仅仅被用于数据文件和程序，不能保持进一步使用的状态信息。

**3. 可移动介质的流通控制**

未对介质（尤其是软盘）的流通进行控制可能导致向组织的 IT 系统引入恶意代码的风险的增加。对介质流通的控制可以通过使用下列措施来实现：

- 特殊软件；
- 程序性防护措施（见下文）。

**4. 程序性防护措施**

应开发用户和管理员指南。指南应列出用于最小化引入恶意代码可能性的程序和惯例。这样的指南应涵盖安装游戏和其他可执行软件，使用不同类型的互联网服务，和输入不同类型的文件。需要时，对源代码或可执行代码进行独立评审。应为不遵守文件化的恶意代码预防程序和惯例，建立安全意识培训和惩戒措施以及相关的程序。

### 8.2.4 网络管理

这一领域包括网络策划、运行和管理的主题。网络的适当配置和管理是减少风险的有效方法。ISO 目前正在起草几个包含关于网络安全详细的防护措施信息的文件。下文列出了网络管理领域的防护措施。

**1. 操作性程序**

为确保网络的正确和安全操作，需建立操作性的程序和职责。这包括文件化的操作程序，以及为响应安全相关事故（也见 8.1.3）所建立的程序。

**2. 系统策划**

为确保可靠的功能和充足的网络容量，需要进行预先的策划和准备并实施监视（包括流量

统计）。应实施新系统的接受准则，并对变更进行控制和影响（也见 8.1.5）。

**3. 网络配置**

一个适当的网络配置对于网络的可靠运作是至关重要的。这包括在组织服务器配置的标准化的方法，并且，非常重要的是要形成文件。此外，应确保服务器只被用于其预期的特定目的（也就是说防火墙不涉及其他任务），并且应实施充分的电力中断保护。

**4. 网络隔离**

为了减少风险和运行网络滥用的可能性，处理关键业务问题和信息的区域应实行物理或逻辑隔离。并且，开发设施应和操作设施分离。

**5. 网络监视**

应监视网络以识别已存在的网络配置的弱点。它允许因流量分析导致的重新配置，并有助于识别攻击者。

**6. 入侵检测**

应检测进入系统或网络的企图和成功未经授权的进入，由此组织可以用一种适宜的和有效的方式对此作出响应。

### 8.2.5 密码学

密码学是为了确保数据安全而进行的数据转换的系统性方法。它可以用于 IT 安全的许多不同目的，例如，密码学可以提供数据的保密性和/或完整性、抗抵赖性和先进的 I&A 方法。在使用密码方法时应非常谨慎地遵守这一领域的所有法律法规。密码学最重要的方面之一就是一个充分的密钥管理体系。这一话题将在 ISO/IEC 11770-1 中详细讨论。更多的关于密码应用的分类信息可以在 ISO/IEC 11770-1 的附录 C 中找到。用于 I&A 的密码学将在 8.2.1 条款中讨论。时间标签服务可以用于支持几个密码防护措施的实施。下文将讨论使用密码学的不同方法。

**1. 数据保密性保护**

在保护保密性非常重要的条件下，也就是说信息特别敏感，应考虑对信息进行加密存储和通过网络传播的防护措施。当决定采用加密方法的防护措施是，应考虑：

- 相关的政府法律和法规；
- 密钥管理的要求，以及为确保实现真正的安全提高而不传造新的脆弱点需要克服的困难；
- 使用的加密机制与开发环境和需要保护程度的适宜性。

**2. 数据完整性保护**

在保护存储或处理的数据的完整性非常重要的条件下，应考虑使用哈希函数、数字签名和/或完整性防护措施以保护存储或传输的信息。完整性防护措施（如，使用消息鉴别码（MACs））提供防范偶然的或蓄意的替换，信息的增加或删除。数字签名防护措施也可以提供类似消息完整性的保护，但是同时也具有允许使他们具有抗抵赖性的特性。当决定使用数字签名或其他完整性防护措施时，需考虑下列因素：

- 有关的政府法律法规；
- 相关的公共密钥基础设施；
- 密钥管理的要求，以及为确保实现真正的安全提高而不传造新的脆弱点需要克服的困难；

**3. 抗抵赖性**

密码技术（也就是说基于数字签名的使用）可以被用来证明，通讯或传输的消息地发送、传输、提交、传递、接收通知等，或相反地。

**4. 数据鉴权**

在数据的鉴权特别重要的条件下，可以使用数字签名来证明数据的正确性。尤其是当使用来自第三方的源索引数据，或当一个大的通讯依赖于索引数据的正确性时，这种需要尤为强烈。数字签名也可用来证明数据是来自特定人员的事实。

**5. 密钥管理**

密钥管理包括了为支持任何密码机制的使用所需的技术的、组织的和程序的方面。密钥管理的目的是密码密钥和相关信息的安全管理。密钥管理包括密码材料的产生、登记、注册、注销、分发、安装、存储、存档、撤消、引导和破坏。此外，重要的是要设计适当的密钥管理以减少密钥损坏和为授权人员使用的风险。密钥管理程序依赖于使用的算法、密钥的预期用途和安全策略。关于密钥管理的更多信息，参见 ISO/IEC IS 11770-1。

**表 8.2.1－识别和鉴权（I&A）**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 基于用户所知的 I&A | **9.2.3，9.3.1，9.4.，9.5.1** | **4.2.1,5.2.1, 附录 A** | **M4** | **16.1** | ***.3.2.1** | **7.2.1,7.2.2** | **6.2** | **16.1** |
| 2. 基于用户所有的 I&A | | | -- | **16.2** | ***.3.2.1** | | **6.2** | **16.2** |
| 3. 基于用户所是的 I&A | | | -- | **16.3** | ***.3.2.1** | | **6.2** | **16.3** |

*代表介于 6-11 之间的任何数字。

**表 8.2.2－逻辑访问控制和审计**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1.访问控制策略 | **9.1** | -- | **M2** | **17.1，17.2，17.3** | ***.3.2.1** | **7.2，8.1.2，8.2.2，8.4.1** | **6.4** | **17.1，17.2，17.3** |
| 2. 用户对计算机的访问 | **9.2，9.3，9.5** | **4.2.4，5.2.4 附录 A** | **M4** | | ***.3.2.1** | | **6.2，6.3** | |
| 3. 用户对数据、设施和应用程序的访问 | **9.4，9.6** | | **M4** | | ***.3.2.1** | | **6.4** | |
| 4. 评审并更新访问权限 | **9.1，9.2.4** | -- | **M2** | **17.4** | ***.3.2.1** | | -- | **17.4** |
| 5. 审计日志 | **9.7** | -- | **M4** | **18** | ***.3.2.2** | **7.3，8.2.10** | **6.7** | **18** |

*代表介于 6-11 之间的任何数字。

**表 8.2.3－防范恶意软件**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 扫描工具 | **8.3** | -- | **M4** | -- | ***.3.10** | **8.3.11，8.3.16** | **7.4** | **4.6，5.2.1，6.4，8.4.4，11** |
| 2. 完整性检查人员 | **8.3** | -- | **M4** | -- | -- | **8.3.11，8.3.16** | **7.4** | -- |
| 3. 可移动介质的流通控制 | **7.3.2** | -- | -- | -- | -- | -- | -- | -- |
| 4. 程序性的防护措施 | **8.3** | -- | **M4** | -- | ***.3.10** | **8.3.11，8.3.16** | **7.4** | **6.2.2，9.3，12，14.2** |

*代表介于 6-11 之间的任何数字。

**表 8.2.4－网络管理**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 操作程序 | **8.5.1** | -- | **M2** | -- | -- | **8.2，8.3** | **8.2** | **14.6** |
| 2. 系统策划 | **8.2** | -- | **M2，M4** | **8.4** | -- | | **6.1** | **8.4** |
| 3. 网络配置 | -- | -- | **M4** | -- | -- | | **9，6.1** | **14.3** |
| 4. 网络隔离 | **9.4.6** | -- | **M2** | -- | -- | -- | **3.1** | -- |
| 5. 网络监视 | **9.7** | -- | **M2** | **18.1.3** | -- | **8.2.7** | -- | **18.1.3** |
| 6. 入侵检测 | -- | -- | -- | **18.1.3** | -- | -- | **6** | **18.1.3** |

*代表介于 6-11 之间的任何数字。

**表 8.2.5－密码学**

| | 信息安全管理实施指南 | ETSI 基线安全标准——特征和机制 | IT 基线保护手册 | NIST 计算机安全手册 | 安全分类和保护信息系统 | TC68 信息安全指南 | 计算机工作站推荐 | 加拿大信息技术安全手册 |
|---|---|---|---|---|---|---|---|---|
| 1. 数据保密性保护 | **10.3.2** | **4.2.2，5.2.2 附录 A** | **M4** | **19.5.1** | **--** | **8.23** | **8.1** | **19.5.1** |
| 2. 数据完整性保护 | **10.3.3** | **4.2.3，5.2.3 附录 A** | **M4** | **19.5.2** | **--** | **8.23** | **8.1** | **19.5.2** |
| 3. 抗抵赖性 | **10.3.4** | **4.2.6，5.2.6 附录 A** | **--** | **19.5.3** | **--** | **8.23** | **8.1** | **19.2.3** |
| 4. 数据鉴权 | **10.3.2** | **4.2.3，5.2.3 附录 A** | **M4** | **19.5.4** | **--** | **8.23** | **8.1** | **19.5.2** |
| 5. 密钥管理 | **10.3.5** | **4.2.5，5.2.5 附录 A** | **--** | **19.3** | | **8.23** | **8.1** | **19.3** |

## 9. 基线方法：根据 IT 系统的类型选择防护措施

如第 8 条款所述，存在两套不同的适用于保护 IT 系统的防护措施、机制和/或程序。一方面，如果特定的环境需要防护措施并且不考虑单独的组件，通常大多数组织的防护措施目录适用于每个 IT 系统。这些防护措施的选择在 9.1 条款中阐述。因为他们的通用性，所以总是需要考虑来自这些目录的防护措施。并且，他们的大多数实施起来也并不昂贵，因为他们是基于介绍性的组织结构和程序。

另一方面，也存在 IT 系统特有的防护措施（如 8.2 所述）——根据被考虑的 IT 系统的类型和特性来选择这些防护措施。这些防护措施的选择在 9.2 条款中阐述。

当然，这些防护措施目录中的一个或多个或特定的防护措施通常可能不适用于一个 IT 系统。例如，如果发送或接收的信息没有保密性的要求，那么可能就不需要进行加密，否则可以检查完整性。另外，只能通过考虑更多的信息来作出更为详细的选择（见第 10 和第 11 条款）。

在识别完适用于被考虑的 IT 系统的所有防护措施的类型之后，可以从第 8 条款和在附录 A-H（在第 9 条款末尾的表中提供了与第 8 条款的联系）中总结的一个或多个文档中获得关于这些防护措施类型和特定防护措施的更多信息。在实施选定的防护措施之前，应对照已有的/计划的防护措施进行仔细检查。

应考虑进行更详细的分析（见第 10 和/或第 11 条款）以选择额外的防护措施。如果根据不同的标准（也就是说基线防护措施和额外的防护措施）选择防护措施，那么在实施最后系列的防护措施时，应谨慎地将他们融合到一起。评审完几个 IT 系统后，应考虑是否可以建立一个组织范围地基线（见第 12 条款）。

不通过详细考虑而选择防护措施的另一个办法是实施特定适用的基线。例如，对于通讯、保健、银行（见附录 B/E/F）和更多的方面都有其基线手册。当使用这些手册时候，可以对照推荐的防护措施来检查已有的/计划的防护措施。但是在选择实施那一防护措施之前，仔细考虑安全需求或关注点仍是有帮助的。

### 9.1 通用防护措施

通用的防护措施的种类是：

- IT 安全管理和策略（8.1.1）；
- 安全符合性检查（8.1.2）；
- 事故处置（8.1.3）；
- 人员（8.1.4）；
- 操作性问题（8.1.5）；
- 业务连续性计划（8.1.6）；
- 物理安全（8.1.7）。

这些种类的防护措施构成了成功的 IT 安全管理的基础，不应被轻视。此外，确保这些防护措施与下面考虑的更多的技术性防护措施互相作用也是非常重要的。组织决定在这些领域做到什么程度取决于组织的需要和关注点（见第 10 条款）和可获得的资源。

当然，许多其他的防护措施种类在大多数情况下也同样适用，但是实施的方式通常特定于特殊的环境（例如，网络的访问控制防护措施与单独的计算机的访问控制防护措施就大不相同）。

当从通用的防护措施种类中选择防护措施时，考虑组织的规模和安全需求是有益的，因为这影响了这些防护措施实施的程度。例如，一个小型组织既不需要也没有相应的人员来建立 IT 安全委员会，但是，无论如何应该有人履行这项职能。因此，可以根据对 8.1 条款中列出的所有防护措施进行适当的裁剪。

### 9.2 IT 系统特有的防护措施

除了通用的防护措施之外，还应为每个系统组件的相关类型选择 IT 系统特有的防护措施。下表给出了一个如何开始选择 IT 系统特有防护措施的过程。在这个例表中，X 代表在正常情况下应实施的防护措施，（X）代表在部分情况下需要的防护措施。通过考虑 8.2 条款中表述的防护措施来持续进行防护措施的选择过程，需要时，可以从附录 A-H 中列出的基线防护措施文件中获得更多的信息。

| | 单独的工作站 | 与网络连接的工作站（客户没有共享的资源） | 与网络连接的有共享资源的服务器或工作站 |
|---|---|---|---|
| **I&A** | | | |
| 基于用户所知的 I&A | X | X | X |
| 基于用户所有的 I&A | X | X | X |
| 基于用户所是的 I&A | （X） | （X） | （X） |
| **逻辑访问控制和审计** | | | |
| 访问控制策略 | | | X |
| 用户对计算机的访问 | X | X | X |
| 用户对数据、设施和应用程序的访问 | X | X | X |
| 评审并更新访问权限 | | | X |
| 审计日志 | X | X | X |
| **恶意代码** | | | |
| 扫描工具 | X | X | X |
| 完整性检查人员 | X | X | X |
| 可移动介质的流通控制 | X | X | X |
| 程序性的防护措施 | X | X | X |
| **网络管理** | | | |
| 操作性程序 | | | X |
| 系统规划 | | | X |
| 网络配置 | | | X |

| | 单独的工作站 | 与网络连接的工作站（客户没有共享的资源） | 与网络连接的有共享资源的服务器或工作站 |
|---|---|---|---|
| 网络隔离 | | | X |
| 网络监视 | | | X |
| 入侵检测 | | | X |
| **密码学** | | | |
| 数据保密性保护 | （X） | （X） | （X） |
| 数据完整性保护 | （X） | （X） | （X） |
| 抗抵赖性 | | （X） | （X） |
| 数据鉴权 | （X） | （X） | （X） |
| 密钥管理 | （X） | （X） | （X） |

## 10. 根据安全关注点和威胁来选择防护措施

在本条款中描述的根据安全关注点和威胁来选择防护措施可以使用下列方式：

- 第一步是识别并评估安全关注点。应考虑保密性、完整性、可用性、可审计性、鉴权和可靠性的要求。选择的防护措施的强度和数量应与评估的安全关注点相适宜。
- 第二步，列出针对每个安全关注点的典型威胁，并根据被考虑的 IT 系统来建议针对每个威胁的防护措施。7.1 条款介绍了不同类型的 IT 系统，在随后的第 8 条款中概述了可能的防护措施。用这种方法，可能满足特定的安全需求并且保护真正需要的地方。

### 10.1 安全关注点评估

为了以一种有效的方式来选择适宜的防护措施，需要理解被考虑的 IT 系统所支持的业务运行的安全关注点。在已识别的安全关注点的帮助下并考虑可能实现这些关注点的相关威胁，就可以选择防护措施。如第 10.2-10.5 条款所述。

如果根据本条款的评估证明了极高的安全关注点，那么推荐更为详细的方法，以实现适当的保护。对此的支持可以在第 11 条款中找到。安全关注点可以包括：

- 保密性的丧失；
- 完整性的丧失；
- 可用性的丧失；
- 可审计性的丧失；
- 鉴权的丧失；
- 可靠性的丧失。

评估应包括 IT 系统本身、IT 系统存储或处理的信息以及它实现的业务运行。这识别了防护措施将要选择的目的。IT 系统或存储和处理的信息的不同部分可能有不同的安全关注点。重要的是，要将安全关注点直接与资产联系起来，因为这影响了可能适用的威胁并提高防护

措施的选择。

可以通过考虑安全失效或破坏是否会对组织的业务运行造成损失（损失可以是严重的、小的或没有任何损失），来评估安全关注点。例如，如果将 IT 系统处理的公司保密信息未授权的泄漏给竞争对手，那么可能使这一竞争对手提供更廉价的供给，因此对组织的业务造成严重损害。另一方面，如果 IT 系统所处理的信息是在公共领域就可以获得的，那么未授权的泄漏可能不会造成任何损失。考虑可能的威胁（见 10.2-10.5 条款）可能有助于明确安全关注点。应对每一资产单独进行下面讨论的评估，因为不同资产的安全关注点可能是不同的。然而，在充分了解安全关注点的前提下，可以将具有同样或类似业务要求和安全关注点的资产合并为一组予以考虑。

如果 IT 系统处理的信息不止一类，那么需要对不同类型的信息进行单独考虑。IT 系统应为处理的所有信息的类型提供充分的保护。因此，如果有些信息具有高的安全关注点，整个系统应被适当的保护。如果一个 IT 系统处理的具有高安全关注点的信息只是非常小的一部分，并且与业务过程一致，就值得考虑是否将这些信息转移至其他系统。

如果确定所有保密性、可用性、完整性、可审计性、鉴权和可靠性的可能损失只可能导致微小的损坏，那么 10.2 条款之前描述的方法就可以为考虑的 IT 系统提供充分的保护。如果确定这些损失中的一个可能导致严重的后果，那么无论是否选择 10.2 到 10.5 中建议的额外的防护措施，都应对其进行评估。在 TR13335 的第 3 部分和第 11 条款给出了进行更为详细的评估并根据评估结果选择防护措施的建议。无论如何，10.2 条款之前建议的防护措施可以用来作为优化选择的基础。

### 10.1.1 保密性的丧失

考虑因被评估资产保密性的丧失（无意或蓄意的）可能导致什么损失。例如，保密性的丧失可能导致：

- 公共信心的丧失或公共形象的损失；
- 法律责任，包括由于破坏数据保护法律可能导致的责任；
- 对组织策略的负面影响；
- 危害人员安全；
- 财务损失。

根据上述问题的答案来判断因保密性的丧失可能导致的全部损失的程度（严重的、微小的还是没有任何损失）。这一决定应形成文件。

### 10.1.2 完整性的丧失

考虑因被评估资产完整性的丧失（无意或蓄意的）可能导致什么损失。例如，完整性的丧失可能导致：

- 决策错误；

- 欺诈；
- 业务功能的损失；
- 公共信心的丧失或公共形象的损失；
- 财务损失；
- 法律责任，包括由于破坏数据保护法律可能导致的责任。

根据上述问题的答案来判断因完整性的丧失可能导致的全部损失的程度（严重的、微小的还是没有任何损失）。这一决定应形成文件。

### 10.1.3 可用性的丧失

考虑因应用程序和信息可用性的丧失（除了短期之外）可能导致什么损失，也就是说如果中断，可能导致哪一业务功能的无法满足的响应或完整时间。也应考虑可用性丧失的极端情况，如数据的永久丢失和/或硬件或软件的物理损坏。例如，关键应用程序或信息可用性的丧失可能导致：

- 决策错误；
- 无法完成关键任务；
- 公共信心的丧失或公共形象的损失；
- 财务损失；
- 法律责任，包括可能因破坏数据保护法律和无法满足合同规定的底线导致的责任；
- 高昂的恢复成本。

需要注意的是，因不可用造成的损失可能因不可用时间长短的不同而不同。事实上，建议考虑因不同中断时间所导致的不同损失，并评估每一中断时间的损失程度，如严重、微小或根本没有任何损失（这一信息将被用于防护措施的选择）。

根据上述问题的答案来判断因可用性的丧失可能导致的全部损失的程度（严重的、微小的还是没有任何损失）。这一决定应形成文件。

### 10.1.4 可审计性的丧失

从用户利益的角度考虑因系统用户和主体（如软件）可审计性的丧失可能导致什么损失。这一考虑应包括自动产生的可能导致响应行为的消息。例如，可审计性的丧失可能导致：

- 系统被用户操纵；
- 欺诈；
- 商业间谍；
- 行为的不可追溯；

- 错误指控；
- 法律责任，包括由于破坏数据保护法律可能导致的责任。

根据上述问题的答案来判断因可用性的丧失可能导致的全部损失的程度（严重的、微小的还是没有任何损失）。这一决定应形成文件。

### 10.1.5 鉴权的丧失

考虑因数据和信息鉴权的丧失可能导致的损失，不管他们是否被人们或系统所使用。这在分布式系统决定在更大团体内进行分布的决策时或使用索引信息时，尤为重要。例如，鉴权的丧失可能导致：

- 欺诈；
- 正确的过程使用不正确的数据导致错误的结论；
- 被组织外部人员所操纵；
- 商业间谍；
- 错误指控；
- 法律责任，包括由于破坏数据保护法律可能导致的责任。

根据上述问题的答案来判断因鉴权的丧失可能导致的全部损失的程度（严重的、微小的还是没有任何损失）。这一决定应形成文件。

### 10.1.6 可靠性的丧失

考虑因系统可靠性的丧失而导致的损失。阐述功能性（可靠性的一个属性，见 ISO9126）也很重要。例如，鉴权的丧失可能导致：

- 欺诈；
- 市场份额的丧失；
- 士气低沉；
- 不可靠的供应商；
- 顾客信心的丧失；
- 法律责任，包括由于破坏数据保护法律可能导致的责任。

根据上述问题的答案来判断因可靠性的丧失可能导致的全部损失的程度（严重的、微小的还是没有任何损失）。这一决定应形成文件。

## 10.2 针对保密性的防护措施

下文列出了可能危及保密性的威胁类型以及防范这些威胁的建议的防护措施。下文也给出

了第 8 条款描述中所提及的防护措施。如果选择相关的防护措施，那么应该将 IT 系统的类型和特性考虑在内。

需要注意的是，8.1 条款中列出的大部分防护措施提供了更为“ 通用 ”的保护，也就是说他们面向的是威胁的范围，并通过支持整体有效的 IT 安全管理来提供保护。因此，他们在比并不详细列出，但是不能低估他们的作用。应实施这些防护措施以获得整体有效的保护。威胁按字母顺序排列。

### 10.2.1 窃听

窃听是访问敏感信息的一种方式，例如，通过搭线或偷听会议谈话。下文列出了防范这一威胁的防护措施。

- **物理性防护措施：**使窃听变成不可能或非常困难的房间、墙壁、建筑物等。另外的一种方法就是增加干扰。这种类型的保护在第 8 条款并未明确提及。就电话而言，适当的线缆可以提供一些防范窃听的保护。这一保护在这里并未涉及，在 ISO/IEC TR 13335 的第 5 部分中可以找到。
- **IT 安全策略：**避免窃听的另一方法就是为何时、何地和采用何种方式交换敏感信息规定严格的准则；
- **数据保密性保护：**防范窃听的另一方法就是在交换前对消息进行加密。关于这一防护措施的更多信息可以在 8.2.5 条款中找到。

### 10.2.2 电磁辐射

攻击者可利用电磁辐射来获取关于 IT 系统处理的信息的知识。下文列出了防范电磁辐射的防护措施。

- **物理性防护措施：**这些措施可以是为房间、墙壁等增加覆层。覆层应可以组织电磁辐射穿越。这一类型的防护措施在 8.1.7 条款中并未明确阐述（这并不是防范电磁辐射最经济的方式）。
- **数据保密性保护：**详细的细节参见 8.2.5 条款。需要注意的是这一保护仅仅适用于加密的信息，对于处理的、显示的和打印的信息并不适用。
- **使用低辐射 IT 设备：**这一防护措施在第 8 条款中也并未明确阐述，但是可以获得内置保护的设备。

### 10.2.3 恶意代码

恶意代码可以导致保密性的丧失，如，通过捕获和泄漏口令。下文列出了防范恶意代码的防护措施。

- **防范恶意代码：**关于防范恶意代码的细节参见 8.2.3 条款。
- **事故处置：**如果发生恶意代码攻击，及时报告异常事故可以减少损失。入侵检测可以用于检测访问系统或网络的企图。关于入侵检测的更多信息参见 8.1.3 条款。

### 10.2.4 伪装用户身份

伪装用户身份可以绕过鉴权和所有相关的其他服务和安全功能。总之，无论这种伪装是否可以访问敏感信息，都可能导致保密性问题。下文列出了这一领域的防护措施。

- **I&A：**如果实施基于联合用户所知、用户所有和用户的本质特征的防护措施，那么伪装会变得更困难。
- **逻辑访问控制和审计：**逻辑访问控制并不能区分授权用户和伪装成授权用户的人员，但是使用逻辑访问控制可以减少受影响的区域（见 8.2.2 条款）。审计日志的评审和分析可以检测未授权活动。
- **防范恶意代码：**获得口令的方式之一就是引入恶意代码从而捕获口令，因此应实施防范这类软件的保护。
- **网络管理：**获得敏感信息的另一种方法就是伪装成正在通讯的用户，如，email。ISO 目前正在起草包含关于网络的详细安全防护措施的更多信息的文档。
- **数据保密性保护：**如果因为某些原因上述类型的保护是不可行的或不充分，那么可以使用敏感数据的存储加密来提供额外的保护（见 8.2.5 条款）。

### 10.2.5 消息的错误路由或重放

错误路由可能是蓄意或无意的错误信息导向，而重放则可是好的或恶意的目的。例如，进行重放可能是为了保持可用性的完整。如果允许对这些消息的未授权访问，那么错误路由和重放可能导致保密性的损失。下文列出了防范消息的错误路由或重放的防护措施。

- **网络管理：**防范错误路由和重放的防护措施可以在其他的文件中找到。ISO 目前正在起草包含更多关于网络安全防护措施信息的文件。
- **数据保密性保护：**如果发生错误路由或重放，为了避免未授权的访问，可以对信息进行加密。更多信息详见 8.2.5 条款。

### 10.2.6 软件失效

如果软件用于保护保密性，那么软件失效可能危及保密性，例如，访问控制或加密软件，或者如果软件失效可能导致操作系统的漏洞。下文列出了这一领域保护保密性的防护措施。

- **事故处置：**任何发现软件失效的人员应向负责人报告，因此可以尽快采取措施。更多信息参见 8.1.3 条款。
- **操作性问题：**一些软件失效是可以避免的，通过在使用前进行彻底的测试和通过软件变更控制（见 8.1.5 条款）。

### 10.2.7 盗窃

如果被盗的 IT 组件含有敏感信息，而盗窃者又可以访问这些信息，那么盗窃可能危及保密性。下文列出了防范盗窃的防护措施。

- **物理性防护措施：**这可以是实物性的保护，使得对建筑物、放置 IT 设备的区域或房间的访问更为困难，或防范盗窃的特定防护措施（二者在 8.1.7 条款中都有阐述）；
- **人员：**应实施针对人员（控制外部人员、保密协议等）的防护措施使得盗窃更为困难（见 8.1.4 条款）；
- **数据保密性保护**：如果包含敏感信息的 IT 设备可能被盗窃，那么应实施这一防护措施，如膝上电脑。更多信息详见 8.2.5 条款。
- **介质控制：**应保护任何含有敏感材料的介质，防止盗窃。

### 10.2.8 对计算机、数据、服务和应用程序的未授权访问

如果对计算机、数据、服务和应用程序的访问可以接触到敏感性材料，那么未授权的访问就可能是一个威胁。防范未授权访问的防护措施包括适当的识别和鉴权、逻辑访问控制、IT 系统层的审计以及网络层的网络隔离。

- **I&A**：可以联合使用适当的识别和鉴权以及逻辑访问控制，以防止未授权的访问；
- **逻辑访问控制和审计**：通过使用访问控制机制将 8.2.2 条款描述的防护措施用于提供逻辑访问控制。审计日志的评审和分析可以检测有权访问系统的人员的未授权活动。
- **网络隔离**：为了使未授权的访问更困难，应实施网络隔离（见 8.2.4 条款）。
- **物理访问控制：**除了逻辑访问控制之外，还应实施物理访问控制以提供保护（见 8.1.7 条款）。
- **介质控制：**如果敏感信息被存储在其他介质上（如，软盘），应实施介质控制（见 8.1.5 条款）以保护介质免受未授权的访问。
- **数据保密性保护：**如果因为某些原因上述类型的保护是不可行的或不充分，那么可以使用敏感数据的存储加密来提供额外的保护（见 8.2.5 条款）。

### 10.2.9 对存储介质的未授权访问

如果介质中存储了敏感信息，那么对存储介质的未授权访问和使用可能危及保密性。下文列出了保护保密性的防护措施。

- **操作性问题：**例如，可以通过对介质的物理性保护和可审计性，以及保证存储销毁从而保证没有人可以从以前销毁的介质中获得保密性资料（见 8.1.5），来进行介质控制。应更为谨慎地保护便于移动的介质，如软盘、备份磁带和纸张。
- **物理安全：**对房间和安全设施进行适当的保护（结实的墙壁和窗户以及物理访问控制）可以防范未授权的访问。
- **数据加密性保护：**对存储介质中的敏感信息的额外保护可以通过对材料进行加密来获得。需要一个良好的密钥管理体系以允许加密的顺利使用（见 8.2.5）。

### 10.3 针对完整性的防护措施

下文列出了可能危及完整性的威胁类型以及防范这些威胁的建议的防护措施。下文也给出了第 8 条款描述中所提及的防护措施。如果选择相关的防护措施，那么应该将 IT 系统的类型和特性考虑在内。

需要注意的是，8.1 条款中列出的大部分防护措施提供了更为“ 通用 ”的保护，也就是说他们面向的是威胁的范围，并通过支持整体有效的 IT 安全管理来提供保护。因此，他们在比并不详细列出，但是不能低估他们的作用。应实施这些防护措施以获得整体有效的保护。威胁按字母顺序排列。

#### 10.3.1 存储介质的老化

存储介质的老化可能危及存储在介质中的信息的完整性。如果完整性是重要的，那么应实施下列防护措施。

- **介质控制**：充分的介质控制包括完整性验证（见 8.1.5），即检测存储文件是否已经被破坏；
- **备份：**应对所有的重要文件和业务数据进行备份。如果通过介质控制或备份检查发现丧失了完整性，那么应使用备份或以前生成的备份来恢复文件的完整性。关于备份的更多信息详见 8.1.6 条款。
- **数据完整性保护：**加密方法可以用于保护存储数据的完整性。更多信息详见 8.2.5 条款。

#### 10.3.2 维护错误

如果不作定期维护或在维护过程中出错，那么可能危及所有相关信息的完整性。下文列出了针对这一情况保护完整性的防护措施。

- **维护：**正确的维护是避免维护错误的最佳方法（见 8.1.5）。这包括已经验证的文件化的维护程序以及适当的工作监视。
- **备份**：如果发生维护错误，那么可以用备份来恢复受损数据的完整性。
- **数据完整性保护：**加密方法可以用于保护存储数据的完整性。更多信息详见 8.2.5 条款。

#### 10.3.3 恶意代码

恶意代码可能导致完整性的损失。也就是说，在恶意代码的帮助下可以进行未授权访问人员或恶意代码本身可以替换文件。下文列出了防范恶意代码的防护措施：

- **防范恶意代码：**关于防范恶意代码的详细信息，参见 8.2.3 条款。
- **事故处置**：如果发生恶意代码攻击，及时报告异常事故可以减少损失。入侵检测可以用于检测访问系统或网络的企图。关于入侵检测的更多信息参见 8.1.3 条款。

### 10.3.4 伪装用户身份

伪装用户身份可以绕过鉴权和所有相关的其他服务和安全功能。总之，无论这种伪装是否可以访问敏感信息，都可能导致完整性问题。下文列出了这一领域的防护措施。

- **I&A：**如果实施基于联合用户所知、用户所有和用户的本质特征的防护措施，那么伪装会变得更困难。
- **逻辑访问控制和审计：**逻辑访问控制并不能区分授权用户和伪装成授权用户的人员，但是使用逻辑访问控制可以减少受影响的区域（见 8.2.2 条款）。审计日志的评审和分析可以检测未授权活动。
- **防范恶意代码：**获得口令的方式之一就是引入恶意代码从而捕获口令，因此应实施防范这类软件的保护。
- **网络管理：**获得敏感信息的另一种方法就是伪装成正在通讯的用户，如，email。ISO 目前正在起草包含关于网络的详细安全防护措施的更多信息的文档。
- **数据完整性保护：**如果因为某些原因上述类型的保护是不可行的或不充分，那么可以使用象数字签名这样的密码学方法来提供额外的保护（见 8.2.5 条款）。

### 10.3.5 消息的错误路由或重放

错误路由可能是蓄意或无意的错误信息导向，而重放则可是好的或恶意的目的。例如，进行重放可能是为了保持可用性的完整。如果消息被替换然后再发给原来的地址，那么错误路由和重放可能导致完整性的损失。下文列出了防范消息的错误路由或重放的防护措施。

- **网络管理：**防范错误路由和重放的防护措施可以在其他的文件中找到。ISO 目前正在起草包含更多关于网络安全防护措施信息的文件。
- **数据保密性保护：**如果发生错误路由或重放，为了避免替换，可以使用哈希函数和数字签名。更多信息详见 8.2.5 条款。

### 10.3.6 抗抵赖性

当需要证明消息已经被发送/接收以及网络已经传输了消息时，应实施针对抗抵赖性的防护措施。8.2.5 中描述的特定的加密学防护措施作为抗抵赖性的基础。

### 10.3.7 软件失效

软件失效可能危及在这一软件帮助下处理的数据和信息的完整性。下文列出了保护完整性的防护措施。

- **报告软件故障：**如果发生软件故障，那么尽快报告软件故障可以减少损失（见 8.1.3）。
- **操作性问题**：安全测试可用于确保软件正确履行功能，软件变更控制可以避免因升级或其他软件变更导致的软件问题（见 8.1.5）。
- **备份：**备份，例如以前生成的，可以用于恢复不能正确履行功能的软件所处理的信息的

完整性。（见 8.1.6）

- **数据完整性保护：**密码学方法可以用于保护信息的完整性。更多的信息参见 8.2.5 条款。

### 10.3.8 供应中断（电力和空调）

供应中断可能导致完整性问题，如果因为他们的中断而导致其他中断。例如，电力中断可能导致硬件故障、技术性失效或存储数据的问题。方法这一特定问题的防护措施可以在各自的子部分中找到。下文列出了防范供应中断的防护措施。

- **电力和空调：**当需要时应使用适宜的电力供应和与空调有关的防护措施，如供电波动保护，以避免可能由于供应中断导致的任何问题。
- **备份**：应使用备份来恢复受损信息（见 8.1.6）。

### 10.3.9 技术性失效

例如，网络的技术性失效可能破坏该网络存储或处理的任何信息的完整性。下文列出了技术性失效的防护措施。

- **操作性问题**：可以使用配置管理、变更管理以及容量管理来避免任何 IT 系统或网络的失效。文档和维护被用于确保任何 IT 系统或网络的顺利运行（见 8.1.5）。
- **网络管理：**应使用操作性程序、系统策划和适当的网络配置来减少技术性失效的风险（见 8.2.4）。
- **电力和空调：**当需要时应使用适宜的电力供应和于空调有关的防护措施，如供电波动保护，以避免可能由于供应中断导致的任何问题。
- **备份：**应使用备份以恢复任何受损的信息（见 8.1.6）。

### 10.3.10 传输错误

传输错误可能破坏被传输信息的完整性。

- **电缆：**电缆的仔细规划和铺设可以避免传输错误，例如，由过载导致的错误（见 8.1.7）。
- **网络管理：**网络设备的适当操作和维护可以避免传输错误。ISO 目前正在起草几个包含更多网络安全防护措施的详细信息的文件。可以使用该文件来防范传输错误。
- **数据完整性保护：**可以使用通讯协议中的校验求和或循环冗余代码来防范无意的传输错误。如果发生蓄意攻击，可以采用密码的方法来保护传输数据的完整性。更多信息详见 8.2.5 条款。

### 10.3.11 对计算机、数据、服务和应用程序的未授权访问

对计算机、数据、服务和应用程序的未授权访问对于信息的完整性可能是一个威胁，如果可以对数据进行未授权的替换。防范未授权访问的防护措施包括适当的识别和鉴权、逻辑访问控制、IT 系统层的审计以及网络层的网络隔离。

- **I&A**：可以联合使用适当的识别和鉴权以及逻辑访问控制，以防止未授权的访问；
- **逻辑访问控制和审计**：通过使用访问控制机制将 8.2.2 条款描述的防护措施用于提供逻辑访问控制。审计日志的评审和分析可以检测有权访问系统的人员的未授权活动。
- **网络隔离**：为了使未授权的访问更困难，应实施网络隔离（见 8.2.4 条款）。
- **物理访问控制：**除了逻辑访问控制之外，还应实施物理访问控制以提供保护（见 8.1.7 条款）。
- **介质控制：**如果敏感信息被存储在其他介质上（如，软盘），应实施介质控制（见 8.1.5 条款）以保护介质免受未授权的访问。
- **完整性保护：**可以使用密码方法来保护存储或传输的数据的完整性。更多信息详见 8.2.5 条款。

### 10.3.12 使用未授权的程序或数据

使用未授权的程序或数据会危及其使用于其中的网络所存储或处理的信息的完整性，如果程序和数据被用于未授权的替换信息，或使用的程序或数据含有恶意代码（如，游戏）。下文列出了防范这一类型威胁的防护措施。

- **安全意识和培训**：所以的雇员都应意识到这一事实：未经 IT 系统安全管理人员或系统安全负责人的许可，不得安装和使用任何软件（也见 8.1.4）。
- **备份**：使用备份以恢复受损信息（见 8.1.6）。
- **I&A：**可以联合使用适当的识别和鉴权以及逻辑访问控制，以防止未授权的访问。
- **逻辑访问控制和审计**： 8.2.2 条款描述的逻辑访问控制应确保仅授权人员才能应用软件来处理和替换信息。审计日志的评审和分析可以检测未授权的活动。
- **防范恶意代码**：所有的程序和数据在使用前都应进行恶意代码检查。

### 10.3.13 对存储介质的未授权访问

对存储介质的未授权访问和使用可能危及完整性，因为她允许对存储在这些介质中的信息进行未授权的替换。下文列出了保护完整性的防护措施。

- **操作性问题：**例如，可以通过对介质的物理性保护和可审计性来避免未授权访问，并进行完整性验证以检测介质存储信息的完整性的任何损坏（见 8.1.5）。应更为谨慎地保护便于移动的介质，如软盘、备份磁带和纸张。
- **物理安全：**对房间和安全设施进行适当的保护（结实的墙壁和窗户以及物理访问控制）可以防范未授权的访问。
- **完整性保护：**可以使用密码方法来保护存储或传输的数据的完整性。更多信息详见 8.2.5 条款。

### 10.3.14 用户错误

用户错误可能破坏信息的完整性。下文列出了防范用户错误的防护措施。

- **安全意识和培训**:应对所有用户进行适当的培训,以避免处理信息时发生用户错误(也见 8.1.4)。这应该包括关于为特定活动规定的程序的培训，如操作性或安全程序。
- **备份：**备份，如以前生成的备份，可以用来恢复因用户错误而破坏的信息完整性。

## 10.4 针对可用性的防护措施

下文列出了可能危及可用性的威胁类型以及防范这些威胁的建议的防护措施。下文也给出了第 8 条款描述中所提及的防护措施。如果选择相关的防护措施，那么应该将 IT 系统的类型和特性考虑在内。

需要注意的是，8.1 条款中列出的大部分防护措施提供了更为“ 通用 ”的保护，也就是说他们面向的是威胁的范围，并通过支持整体有效的 IT 安全管理来提供保护。因此，他们在比并不详细列出，但是不能低估他们的作用。应实施这些防护措施以获得整体有效的保护。

可用性的要求涵盖了从没有时间关键性的数据或系统（但是这类数据的损失和系统的不可用仍被认为是严重的）到高度时间关键性的数据或系统。前者可以用备份的方法予以保护，而后者可能要求提供一些弹性系统。威胁按字母顺序排列。

### 10.4.1 破坏性攻击

信息可以被破坏性攻击所破坏。下文列出了防范破坏性攻击的防护措施。

- **惩戒过程**：所有雇员都应了解破坏（无意的或蓄意的）信息的后果（也见 8.1.4）。
- **介质控制：**应对所有介质实施物理保护和可审计性，以适当的保护他们免受未授权访问的威胁（见 8.1.5）。
- **备份：**应对所有重要文件和业务数据进行备份。如果文件或其他任何信息不可用，那么可以使用备份或以前生成的备份来恢复信息。更多信息详见 8.1.6 条款。
- **实质性保护**：应使用物理访问控制以避免利于未授权破坏 IT 设备或信息的未授权访问。
- **I&A：**可以联合使用适当的识别和鉴权以及逻辑访问控制，以防止未授权的访问。
- **逻辑访问控制和审计：**8.2.2 条款所描述的逻辑访问控制应确保不发生允许破坏信息的未授权访问。审计日志的评审和分析可以检测未授权活动。

### 10.4.2 存储介质老化

存储介质的老化可能危及存储在介质中的信息的可用性。如果可用性是重要的，那么应实施下列防护措施。

- **介质控制：**对存储介质进行定期测试，期望在信息真正不可用前检测出老化。介质应以一种任何外部的影响都不会导致介质老化的方式存储。
- **备份：**应对所有的重要文件和业务数据进行备份。如果文件或其他任何信息不可用，那么应使用备份或以前生成的备份来恢复信息。关于备份的更多信息详见 8.1.6 条款。

### 10.4.3 通讯设备故障和服务中断

通讯设备故障和服务中断可能威胁通过这些设施传递的信息的可用性。根据导致失效的原因，考虑 10.4.11 软件失效、10.4.12 供电中断或 10.4.13 技术性失效也是有帮助的。下文列出了保护可用性的防护措施。

- **冗余和备份：**通讯设施组件的冗余可以用于降低通讯设施故障的可能性。根据最大的可接受中断时间，备用的设备也可以用于满足这一要求。无论如何，应备份配置和规划数据以确保发生紧急情况时的可用性。关于备份的通用信息参见 8.1.6 条款。
- **网络管理：**ISO 目前正在起草几个包含更多网络安全防护措施的详细信息的文件。可以使用该文件来防范通讯设备故障或服务的中断。
- **电缆：**电缆的仔细规划和铺设可以避免损害。如果怀疑可能损害线路，应对其进行监视（也见 8.1.7）。
- **抗抵赖性：**如果需要证明网络的传输和信息的发送和接受，应实施抗抵赖性（见 8.2.5 条款）；然后可以轻易的检测通讯失效和信息丢失。

### 10.4.4 火灾、水灾

火灾和/水灾可能破坏信息和 IT 设备。下文列出了防范火灾和水灾的防护措施。

- **物理性保护：**所有放置 IT 设备和存储重要信息的介质的建筑物和房间都应被适当保护以防范火灾和水灾（见 8.1.7 条款）。
- **业务连续性计划：**为了保护业务免受火灾和水灾的灾难性的影响，应实施业务连续性计划并保持所有重要备份信息的可用。

### 10.4.5 维护错误

如果不作定期维护或在维护过程中出错，那么可能危及所有相关信息的可用性。下文列出了针对这一情况保护完整性的防护措施。

- **维护：**正确的维护是避免维护错误的最佳方法（见 8.1.5）。
- **备份**：如果发生维护错误，那么可以用备份来恢复丢失信息的可用性。

### 10.4.6 恶意代码

恶意代码可以被用于绕过鉴权和所有与此相关的服务和安全功能。总之，恶意代码可能导致可用性的损失。也就是说，在恶意代码的帮助下可以进行未授权访问人员或恶意代码本身可以破坏文件。下文列出了防范恶意代码的防护措施：

- **防范恶意代码：**关于防范恶意代码的详细信息，参见 8.2.3 条款。
- **事故处置：**如果发生恶意代码攻击，及时报告异常事故可以减少损失。入侵检测可以用于检测访问系统或网络的企图。关于入侵检测的更多信息参见 8.1.3 条款。

### 10.4.7 伪装用户身份

伪装用户身份可以绕过鉴权和与此相关的所有服务和安全功能。总之，无论这种伪装是否可以移除或破坏信息，都可能导致可用性问题。下文列出了这一领域的防护措施。

- **I&A：**如果实施基于联合用户所知、用户所有和用户的本质特征的 I&A 防护措施，那么伪装会变得更困难（见 8.2.1）。
- **逻辑访问控制和审计：**逻辑访问控制并不能区分授权用户和伪装成授权用户的人员，但是使用逻辑访问控制可以减少受影响的区域（见 8.2.2）。审计日志的评审和分析可以检测未授权活动。
- **防范恶意代码：**获得口令的方式之一就是引入恶意代码从而捕获口令，因此应实施防范这类软件的保护（见 8.2.3）。
- **网络管理：**获得敏感信息的另一种方法就是伪装成正在通讯的用户，如，email。ISO 目前正在起草包含关于网络的详细安全防护措施的更多信息的文档。
- **数据备份：**数据备份并不能防范伪装用户身份，但是可以降低由此导致的破坏事件的影响（见 8.2.5 条款）。

### 10.4.8 消息的错误路由或重放

错误路由可能是蓄意或无意的错误信息导向，而重放则可是好的或恶意的目的。例如，进行重放可能是为了保持可用性的完整。消息的错误路由可能导致消息可用性的丧失。下文列出了防范消息的错误路由或重放的防护措施。

- **网络管理：**防范错误路由和重放的防护措施可以在其他的文件中找到。ISO 目前正在起草包含更多关于网络安全防护措施信息的文件。
- **抗抵赖性：**如果需要证明网络传递或消息的发送或接收，那么需要应用抗抵赖性（见 8.2.5）。

### 10.4.9 资源滥用

资源的滥用可能导致信息或服务的不可用。下文列出了防范资源滥用的防护措施。

- **人员：**所有人员都应意识到滥用资源的后果；需要时，可实施惩戒过程（见 8.1.4）。
- **操作性问题：**应监视系统的使用以检测未授权的活动，应实施职责分离以最小化特权滥用的可能性（见 8.1.5）。
- **I&A：**应联合使用逻辑访问控制和适当的 I&A 防护措施，以防止未授权的访问。
- **逻辑访问控制和审计：**8.2.2 条款所描述的逻辑访问控制应确保不发生允许破坏信息

的未授权访问。审计日志的评审和分析可以检测未授权活动。

- **网络管理**：应实施适当的网络配置和隔离以最小化网络资源滥用的可能性（见 8.2.4）。

### 10.4.10 自然灾害

为了防范由于资产灾害导致的信息和服务的损失，应实施下列的防护措施。

- **自然灾害保护：**应尽可能的保护所有的建筑物免受自然灾害的影响（见 8.1.7）。
- **业务连续性计划：**应为每一建筑物建立业务连续性计划并充分测试，应保持所有重要信息备份、服务和资源的可用性。

### 10.4.11 软件失效

软件失效可能破坏相关软件处理的数据和信息的可用性性。下文列出了保护可用性的防护措施。

- **报告软件失效：**如果发生软件失效，那么尽快报告软件故障可以减少损失（见 8.1.3）。
- **操作性问题**：安全测试可用于确保软件正确履行功能，软件变更控制可以避免因升级或其他软件变更导致的软件问题（见 8.1.5）。
- **备份：**备份，例如以前生成的，可以用于恢复不能正确履行功能的软件所处理的信息。（见 8.1.6）

### 10.4.12 供应中断（电力和空调）

供应中断可能导致可用性问题，如果因为他们的中断而导致其他中断。例如，电力中断可能导致硬件故障、技术性失效或存储介质的问题。防范这一特定问题的防护措施可以在各自的子部分中找到。下文列出了防范供应中断的防护措施。

- **电力和空调：**当需要时应使用适宜的电力供应和与空调有关的防护措施，如供电波动保护，以避免可能由于供应中断导致的任何问题。
- **备份**：应对所有重要文件和业务数据等进行备份。如果文件或其他信息因供应中断而丢失，那么可以使用备份来恢复信息。关于备份的更多信息，参见 8.1.6 条款。

### 10.4.13 技术性失效

例如，网络的技术性失效可能破坏该网络存储或处理的任何信息的完整性。下文列出了防范技术性失效的防护措施。

- **操作性问题**：可以使用配置管理、变更管理以及容量管理来避免任何 IT 系统或网络的失效。文档和维护被用于确保任何 IT 系统或网络的顺利运行（见 8.1.5）。
- **网络管理：**应使用操作性程序、系统策划和适当的网络配置来减少技术性失效的风险（见 8.2.4）。
- **业务连续性计划：**为了保护业务免受技术性失效的灾难性影响，应实施业务连续性计

划，并保持所有重要信息的备份、服务和资源的可用性。

### 10.4.14 盗窃

很明显，盗窃肯定会危及信息和 IT 设备的可用性。下文列出了防范盗窃的防护措施。

- **物理性防护措施：**这可以是实物性的保护，使得对建筑物、放置 IT 设备的区域或房间的访问更为困难，或防范盗窃的特定防护措施（二者在 8.1.7 条款中都有阐述）；
- **人员：**应实施针对人员（控制外部人员、保密协议等）的防护措施使得盗窃更为困难（见 8.1.4 条款）；
- **介质控制：**应保护任何含有重要材料的介质，防止盗窃（见 8.1.5）。

### 10.4.15 流量过载

流量过载可能威胁通过这些设施传输的信息的可用性。下文列出了保护可用性的防护措施。

- **冗余和备份：**通讯设施组件的冗余可以用于降低流量过载的可能性。根据最大的可接受中断时间，备用的设备也可以用于满足这一要求。无论如何，应备份配置和规划数据以确保发生紧急情况时的可用性。关于备份的通用信息参见 8.1.6 条款。
- **网络管理：**网络和通讯设施的适当配置和管理可以用来避免过载（见 8.2.4）。
- **网络管理：**ISO 目前正在起草几个包含更多网络安全防护措施的详细信息的文件。可以使用该文件来防范流量过载。

### 10.4.16 传输错误

传输错误可能破坏被传输信息的可用性。下文列出了保护可用性的防护措施。

- **电缆：**电缆的仔细规划和铺设可以避免传输错误，例如，由过载导致的错误（见 8.1.7）。
- **网络管理：**网络管理并不能防范传输错误，但是可以用来发现因传输错误导致的问题，并在此情况下发出警报。这允许对这些问题作出及时反映。ISO 目前正在起草几个包含更多网络安全防护措施的详细信息的文件。可以使用该文件来防范传输错误。

### 10.4.17 对计算机、数据、服务和应用程序的未授权访问

对计算机、数据、服务和应用程序的未授权访问对于信息的可用性可能是一个威胁，如果可能对数据进行未授权的破坏。防范未授权访问的防护措施包括适当的识别和鉴权、逻辑访问控制、IT 系统层的审计以及网络层的网络隔离。

- **I&A**：可以联合使用适当的 I&A 防护措施以及逻辑访问控制，以防止未授权的访问；
- **逻辑访问控制和审计**：通过使用访问控制机制将 8.2.2 条款描述的防护措施用于提供逻辑访问控制。审计日志的评审和分析可以检测有权访问系统的人员的未授权活动。

- **网络隔离**：为了使未授权的访问更困难，应实施网络隔离（见 8.2.4 条款）。
- **物理访问控制：**除了逻辑访问控制之外，还应实施物理访问控制以提供保护（见 8.1.7 条款）。
- **介质控制：**如果敏感信息被存储在其他介质上（如，软盘），应实施介质控制（见 8.1.5 条款）以保护介质免受未授权的访问。

### 10.4.18 使用未授权的程序或数据

使用未授权的程序或数据会危及其使用于其中的网络所存储或处理的信息的可用性，如果程序和数据被用于未授权的删除信息，或使用的程序或数据含有恶意代码（如，游戏）。下文列出了防范这一类型威胁的防护措施。

- **安全意识和培训**：所以的雇员都应意识到这一事实：未经 IT 系统安全管理人员或系统安全负责人的许可，不得安装和使用任何软件（也见 8.1.4）。
- **备份**：使用备份以恢复受损或丢失的信息、服务或资源（见 8.1.6）。
- **I&A：**可以联合使用适当的识别和鉴权以及逻辑访问控制，以防止未授权的访问。
- **逻辑访问控制和审计**： 8.2.2 条款描述的逻辑访问控制应确保仅授权人员才能使用软件来处理和删除信息。审计日志的评审和分析可以检测未授权的活动。
- **防范恶意代码**：所有的程序和数据在使用前都应进行恶意代码检查（见 8.2.3）。

### 10.4.19 对存储介质的未授权访问

对存储介质的未授权访问和使用可能危及可用性，因为它可能导致对存储在这些介质中的信息进行未授权的破坏。下文列出了保护可用性的防护措施。

- **操作性问题：**例如，可以通过对介质的物理性保护和可审计性来避免对介质存储信息的未授权访问（见 8.1.5）。应更为谨慎地保护便于移动的介质，如软盘、备份磁带和纸张。
- **物理安全：**对房间和安全设施进行适当的保护（结实的墙壁和窗户以及物理访问控制）可以防范未授权的访问。

### 10.4.20 用户错误

用户错误可能破坏信息的可用性。下文列出了防范用户错误的防护措施。

- **安全意识和培训：**应对所有用户进行适当的培训，以避免处理信息时发生用户错误（也见 8.1.4）。这应该包括关于为特定活动规定的程序的培训，如操作性或安全程序。
- **备份：**备份，如以前生成的备份，可以用来恢复因用户错误而破坏的信息。

### 10.5 针对可审计性、鉴权和可靠性的防护措施

在不同的领域内，可审计性、鉴权和可靠性的范围可能差异很大。这些差别意味着许多不同的防护措施都是适用的。因此，下文只是列出了通用指南。

需要注意的是，8.1 条款中列出的大部分防护措施提供了更为“ 通用 ”的保护，也就是说他们面向的是威胁的范围，并通过支持整体有效的 IT 安全管理来提供保护。因此，他们在比并不详细列出，但是不能低估他们的作用。应实施这些防护措施以获得整体有效的保护。

#### 10.5.1 可审计性

为了保护可审计西，应关注任何可能导致对特定实体或主题的所采取的行为的不可追溯的威胁。这些威胁的例子是帐户共享，缺乏行为追溯，伪装用户身份，软件失效，对计算机、数据、服务和应用程序的未授权访问，以及弱的身份鉴权。

应该考虑可审计性的两种类型。一种类型是关于识别用户对信息或 IT 系统采取的特定活动的可审计性。审计日志可以提供这一点。另外一种类型是关于系统用户之间的可审计性。抗抵赖性服务、知识分割或双重控制可以实现这一点。

许多防护措施可以用于或有助于实现可审计性。针对可审计性的适用的防护措施涵盖了从安全策略、安全意识和逻辑访问控制和审计到一次性口令和介质控制。信息所有者关系策略的实施是实现可审计性的先决条件。特定防护措施的选择取决于这一领域内可审计性的特定用途。

#### 10.5.2 鉴权

如果威胁可能导致人员、系统或过程无法确定一个客体是否就是其声称的，那么任何这种威胁都可能降低对鉴权的信心。可能导致发生这种情况的例子是，未受控的数据变更、未检查的数据源以及未保持的数据源。

许多防护措施可以用于或有助于实现鉴权。适用的防护措施涵盖了从使用标签索引数据、逻辑访问控制和审计到使用数字签名。特定防护措施的选择取决于这一领域内可审计性的特定用途。

#### 10.5.3 可靠性

任何可能导致系统或过程不一致行为的威胁，都可能导致可靠性的降低。这类威胁的部分例子是不一致的系统表现和不可靠的供应商。可靠性的丧失可能导致顾客服务的贫乏或顾客信心的丧失。

许多防护措施可以用于或有助于实现可靠性。适用的防护措施涵盖了从业务连续性计划、引入物理结构的冗余和系统维护到识别和鉴权以及逻辑访问控制和审计。特定防护措施的选择取决于这一领域内可审计性的特定用途。

## 11 根据详细评估来选择防护措施

根据详细评估并遵循前面条款所提的同样准则来选择防护措施。实施详细的风险分析允许考虑 IT 系统及其资产的特定要求和状况。与使用前面所述条款的区别在于努力的水平以及评估过程中收集的细节。因此，可能高质量的判断选择的防护措施的合理性。11.1 条款阐述了如何将这一技术报告的第 3 部分描述的风险分析方法应用于第 4 部分的防护措施选择过程。选择的准则将在 12 条款中阐述。

### 11.1 本技术报告第 3 部分和第 4 部分的关系

在 ISO/IEC TR 13335 的第 3 部分介绍了 IT 安全管理技术。除了其他问题之外，也讨论了可能的公司风险分析战略选项和风险分析推荐方法。组织使用的主要战略选项是：

- 对所有的 IT 系统使用基线方法；
- 对所有的 IT 系统使用详细风险分析；
- 使用“ 推荐方法 ”，也就是说先对所有的 IT 系统进行高层风险分析，然后对低风险 IT 系统使用基线方法，对高风险 IT 系统使用详细风险分析。

如果决定对所有的 IT 系统都实施详细风险分析以识别防护措施，那么在第 4 部分的 11.2 条款给出了关于如何选择防护措施和如何有效地使用详细风险分析结果的信息。无论如何，在第 4 部分的第 8 条款到第 10 条款中包含的关于防护措施、特定系统的防护措施以及安全关注点、威胁和防护措施之间关系的信息仍然是有用的。

### 11.2 选择的准则

一个防护措施可参数四个基本的方面，即影响、威胁、脆弱点和风险本身。当决定降低或避免风险而不是接受时，就阐述了风险本身（降低风险的一个例子是购买保险，避免风险的一个例子是将敏感信息转移到其他计算机）。共同作用构成风险的组件，即影响、威胁和脆弱点是防护措施的主要目标。防护措施可以用以下方式阐述这些方面：

- **威胁**——防护措施可以降低威胁发生的可能性（如，认为用户错误可能导致数据丢失的威胁，那么为用户提供培训课程可以降低这些错误的数量），或，就蓄意攻击而言，可以通过增加成功实施攻击的技术的复杂性来威慑。
- **脆弱点**——防护措施可以消除脆弱点，或使得利用脆弱点的难度加大（例如，如果连接到外部网络的内部网是未授权访问的一个脆弱点，那么实施适当的防火墙可以使得这种连接具有更少的脆弱性，如果断开连接则消除了这一脆弱点）。
- **影响**——防护措施可以减少或避免影响（如果负面影响是信息的不可用，那么可以通过采用信息备份并异地存储的方式以及准备激活的业务连续性计划来减少影响）。拥有良好的审计踪迹记录、分析和报警装置有助于事故的尽早检测并降低负面业务影响。

防护措施的使用方式和区域对于其实施收益会造成很大差异。通常，威胁会利用多个脆弱点。因此，如果使用一个防护措施来组织威胁的发生，那么需要同时阐述几个脆弱点。反之

也是正确的——保护脆弱点的防护措施可以同时阐述几个威胁。如果可能，那么在选择防护措施时应考虑这些收益。通常应将这些额外的收益形成文件，以对任何防护措施满足的安全要求有一个全面的了解。

一般而言，防护措施可以提供下列保护类型中的一个或多个：预防、威慑、检测、降低、恢复、纠正、监视和意识。至于那一属性是最可取的，依赖于特定的环境和每一防护措施预期实现的目标而定。在许多情况下，防护措施将提供多个属性，也就是说提供了额外的收益。如果可能，应优先寻找那些确实可以提供多个收益的防护措施。

在阐述上述影响时，安全应总是保持合理的平衡。如果过多的关注某一类型的防护措施，那么整体的安全不可能有效。例如，如果单独使用大多数的威慑性防护措施，而没有使用充分的检测性防护措施来识别当威慑不起作用时，那么整体的安全将是无效的。

在实施前，应将建议的防护措施与已存在的防护措施进行比对，以评估是否存在可扩展或升级的防护措施。如果存在，那么对愿意的防护措施进行扩展或升级可能比引入新的防护措施更为经济。

在选择防护措施的过程中，重要的是要平衡防护措施的实施成本和被保护资产的价值，以及用风险削减表明的投资收益。防护措施的实施和维护成本可能远远高于防护措施本身的成本，因此在选择防护措施时，应考虑实施和维护成本。

技术性限制象性能要求、可管理性（操作性支持要求）和兼容性问题可能影响特定防护措施的使用。在这些情况下，系统和安全管理人员应共同工作以识别最佳的解决方案。但是防护措施也有可能减低性能。此外，系统和安全管理人员应共同努力以识别在允许所需的性能的同时又保证充分安全的解决方案。

象隐私法律和法学方面可能要求实施特定的防护措施，因此应定义使用或识别的基线的不可变更的元素。

## 12 开发组织范围的基线

当组织决定对整个组织或部分组织实施基线安全时，应考虑下列问题：

- 组织或系统的哪些部分可以使用同样的基线，哪一部分需要特殊的考虑，或同一基线是否可以在整个组织范围内应用？
- 基线（或不同的基线）应达到的安全等级？
- 如何确定沟通不同（如果需要）基线的防护措施。

下图展示了使用基线安全的不同方法。

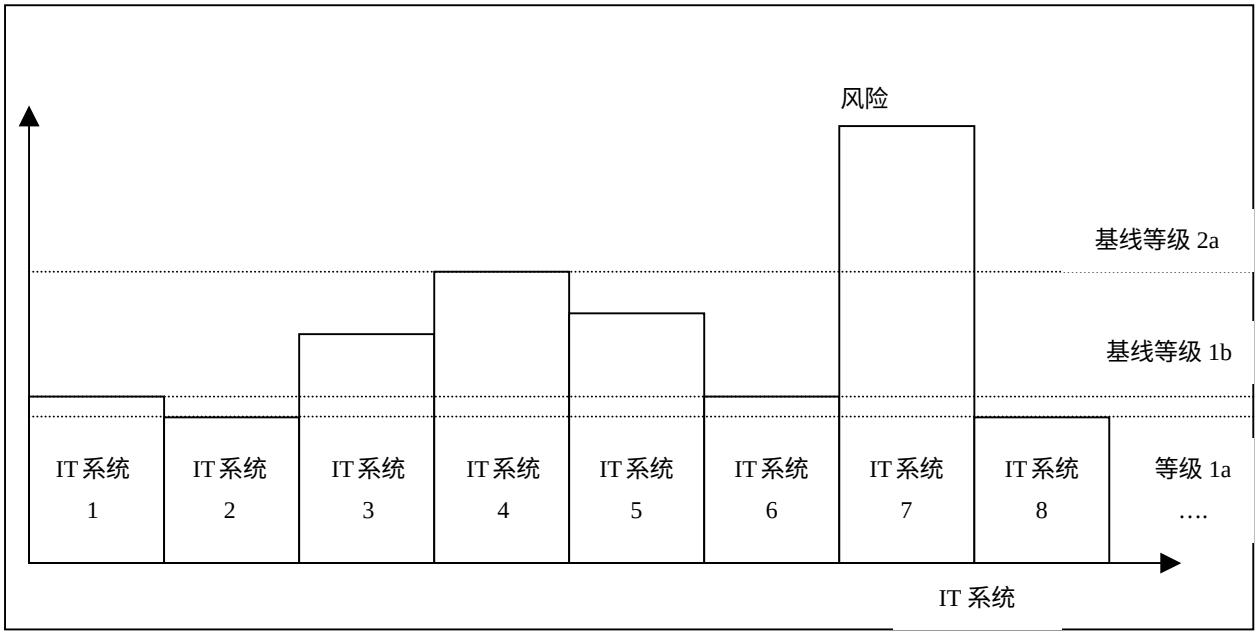


**图 4：不同的基线等级**

在组织内实施不同基线等级的优点是多数系统都可以得到适当的保护，即保护不是太少也不是太多（象图 4 中所示的 IT 系统 1、2、6 和 8 使用基线等级 1，IT 系统 3、4 和 5 使用基线 2)。如果具有不同安全要求的 IT 系统“确实”是不同的（也就是说，保护每一 IT 系统所需的防护措施的大多数都是不同的)，那么推荐组织使用不同基线。如果安全要求存在着根本上的不同，那么需要重新考虑使用基线方法的决策。

另一方面，如果不同基线等级之间仅有的差异知识需要采取一些额外的防护措施以形成更高的基线等级，那么可能并不值得实施几个不同的基线等级。如果只实施一个基线等级，可以大大降低组织的费用，并且组织内的每个人都可以依赖于呈现的同一等级的安全。

当然，基线安全等级的目的与一个或多个基线安全等级是否可以合理的实施有关。如果选择不同的基线等级，那么可以对这些等级进行相当精确的调整以满足他们预期保护的 IT 系统的要求。总的来说，任何一个基线等级都不应针对低于要保护的 IT 系统的最低安全要求的安全（象低于图 4 中的 IT 系统 2 的要求)。比较明智的做法是针对对预期保护的 IT 系统的全部（基线等级 1b）或大多数（图 4 中的基线等级 1a）而言是充分的等级。通常建议针对被基线安全措施保护的 IT 系统的最高安全等级，因为这样通常并不昂贵而且又可以为所涉及的所有系统提供充分的安全。需要仔细的考虑涉及的 IT 系统，以作出关于哪些 IT 系统应使用同样的基线进行保护的最后决策。一些 IT 系统在性质和/或保护要求方面非常相似——在这种情况下，使用同样的基线来保护他们是非常有益的。另一方面，如果一些 IT 系统在他们的保护要求方面是完全不同的，那么通常比较容易的办法就是单独考虑他们。

如果组织决定实施组织范围的同一基线，也是一样的。这一基线可以针对三个不同的等级：

- 低等级，增加特定的防护措施以保护具有较高要求的所有 IT 系统；
- 中等等级，增加特定的防护措施以保护具有较高要求的所有 IT 系统；
- 高等级可以充分保护预期使用基线安全来保护的所有的 IT 系统。

正如前面解释的那样，许多组织采取中等或高等级的基线安全是明智的，其目的在于实现充分的保护，整个组织内的可靠安全并降低组织的费用。最后，应根据组织的安全策略和考虑的 IT 系统的安全要求来作出决策。

## 13 总结

第 4 部分讨论了选择防护措施的方法。这些防护措施可以用来实现基线保护，或支持第 3 部分中描述的技术。第 4 部分也概述了遵循上述的任何一种方法选择的通用防护措施，并引用了包含这些描述的防护措施的更多细节的多个基线防护措施手册。最周，描述了开发组织范围基线的不同方法，以及替代选项的优缺点。任何希望选择防护措施来保护其 IT 系统的组织，无论大型组织还是小型组织，都可以使用第 4 部分。

## 参考书目


| | | |
|---|---|---|
| [A] | **信息安全管理实施指南** | 见附录 A |
| [B] | **ETSI 基线安全标准——特征和机制** | 见附录 B |
| [C] | **IT 基线保护手册** | 见附录 C |
| [D] | **NIST 计算机安全手册** | 见附录 D |
| [E] | **医疗信息学——安全分类和医疗信息系统保护** | 见附录 E |
| [F] | **TC68 银行及相关金融机构——信息安全指南** | 见附录 F |
| [G] | **保护那些未被官方保密法所涵盖的敏感信息——计算机工作站推荐** | 见附录 G |
| [H] | **加拿大信息技术安全手册** | 见附录 H |