ISO/IEC 27005:2008

第一版

2008-6-15

Information Technology – Security techniques - Information security risk management

信息技术－安全技术－信息安全风险管理

目 录

前言

ISO（国际标准化组织）和IEC （国际电工委员会）构成世界范围内的标准化专门体系。国家机构作为ISO或IEC的成员，通过由处理特定技术领域的相应组织所建立的技术委员会参与开发国际标准。ISO和IEC的技术委员会在共同关心的领域合作。其他的国际性组织，官方或非官方的，也与ISO和IEC联系，参与部分工作。在信息技术领域，ISO/IEC 建立了联合技术委员会， IEO/IEC JTC 1。

国际标准依据ISO/IEC 指南第2部分起草。

联合技术委员会的主要任务是起草国际标准。被联合技术委员会接受的国际标准草案，将提交过国家机构进行投票。成为国际标准公开发布，则需要至少75%的国家机构投赞成票。

应注意本标准的某些内容可能涉及专利。ISO和IEC不负责识别任何专利。

ISO/IEC 20000-1由ISO/IEC JTC1信息技术联合技术委员会SC27安全技术分起草。

ISO/IEC 27005的第一版作为技术性修订，废弃和替代了ISO/IEC TR 13335-3:1998, and ISO/IEC TR 13335-4:2000。

介绍

本标准为组织的信息安全风险管理提供指南，并特别为遵循ISO/IEC 27001的ISMS提供支持。然而，本标准不会提供任何特定的信息安全风险管理方法。组织根据如ISMS、风险管理的范畴或行业特定等因素，定义自己的风险管理方法。在本标准所描述的框架下，存在多种办法可用于实施ISMS的要求。

本标准适用于关注组织内信息安全风险管理的管理者和员工，以及为这些活动提供支持的外部组织（如果适用）。

信息技术 – 安全技术 – 信息安全风险管理

1. 范围

本国际标准为信息安全风险管理提供指南。

本国际标准支持ISO/IEC 27001所描述的一般概念，并致力于协助实施符合要求的、基于风险管理方法的信息安全。

理解 ISO/IEC 27001 和 ISO/IEC 27002 所描述的概念、模型、过程和术语，对于完整理解本标准是很重要的。

本标准适用于试图管理危及组织信息安全风险的各种类型组织（如，商业企业、政府机构、非盈利组织）。

2. 规范性引用文件

下列参考文件对于本文件的应用是必不可少的。凡是注明日期的引用文件，只有引用的版本适用于本标准；凡是不注日期的引用文件，其最新版本（包括任何修改）适用于本标准。

ISO/IEC 27001:2005，信息技术 – 安全技术 – 信息安全管理体系 – 要求
ISO/IEC 27002:2005，信息技术 – 安全技术 – 信息安全管理使用规则

3. 术语和定义

下列术语和定义以及 ISO/IEC 27001、ISO/IEC 27002 中的术语和定义适用于本标准。

3.1 Impact 影响

给达成的业务目标级别带来不利的变化

3.2 Information Security Risk 信息安全风险

某种特定的威胁利用资产或一组资产的脆弱点，导致这些资产受损或破坏的潜在可能

注：通常用事态的可能性及其后果的组合来测量。

3.3 risk avoidance 风险回避

决定不卷入风险处境或从风险处境中撤出 [ISO/IEC Guide 73:2002]

3.4 risk communication 风险沟通

在决策者或其他利益相关方之间交换或共享有关风险的信息 [ISO/IEC Guide 73:2002]

3.5 risk estimation 风险估算

对风险的可能性和后果进行赋值的过程 [ISO/IEC Guide 73:2002]

注 1：对于风险估算，在本国际标准范畴内，用术语 “活动”替代术语“过程”。

注 2：对于风险估算，在本国际标准范畴内，用术语“可能性”替代术语“概率”。

3.6 risk identification 风险识别

发现、列出并描述风险要素的过程 [ISO/IEC Guide 73:2002]

注 1：对于风险识别，在本国际标准范畴内，用术语 “活动”替代术语“过程”。

3.7 risk reduction 风险降低

采取行动降低风险发生的可能性或减轻负面后果，或同时降低风险发生的可能性和减轻负面后果 [ISO/IEC Guide 73:2002]

注：对于风险降低，在本国际标准范畴内，用术语“可能性”替代术语“概率”。

3.8 risk retention 风险保持

接受特定风险带来的损失或收益 [ISO/IEC Guide 73:2002]

注：在信息安全风险范畴内，风险保持只考虑负面后果（损失）。

3.9 risk transfer 风险转移

与其它组织分担风险的损失或收益 [ISO/IEC Guide 73:2002]

注：在信息安全风险范畴内，转移风险只考虑负面后果（损失）。

4. 本国际标准的结构

本标准包含信息安全风险管理过程及活动的描述。

条款 5 提供背景信息。

条款 6 提供信息安全风险管理过程的概述。

条款 6 提及的所有信息安全管理活动在随后的以下条款中叙述：

- 条款 7 确定风险管理范畴，
- 条款 8 描述风险评估，
- 条款 9 描述风险处置，
- 条款 10 描述风险接受，
- 条款 11 描述风险沟通，

- 条款 12 描述风险监视和评审。

附录提供有关信息安全风险管理活动的补充信息。附录 A（定义信息安全管理过程的范围和边界）为建立风险评估范畴提供支持。附录 B（资产示例）、附录 C（典型威胁示例）和附录 D（典型脆弱点示例）讨论有关资产的识别和赋值以及影响的评估。

附录 E 提供信息安全风险评估方法的示例。

附录 F 表述降低风险的约束条件。

从条款 7 到条款 12 描述的所有风险管理活动采用如下结构：

输入：识别执行活动所必需的任何信息。

活动：活动的描述。

实施指南：提供执行活动的指南。指南的部分内容可能不适用于所有情形，并且执行活动的其他方式可能更为合适。

输出：识别活动执行后所得到的任何信息。

5. 背景

信息安全风险管理的系统化方法对于识别组织有关信息安全要求和建立有效的信息安全管理体系（ISMS）来说是必须的。信息安全风险管理方法应该适合于组织的环境，特别是应该与组织的整体风险管理相一致。应该按照需要的时间和地点，以有效和及时的方式处理风险。信息安全风险管理应该是构成整个信息安全管理活动的一部分，并应该应用于 ISMS 的实施和持续运行中。

信息安全风险管理是一个持续的过程。该过程应该建立范畴，评估风险，并利用风险处置计划来实施建议和决策以处置风险。风险管理分析，是在决定应该做什么和什么时候做之前分析可能发生什么以及可能的后果是什么，以将风险降低到可以接受的级别。

信息安全风险管理应该为以下方面提供帮助：

- 识别风险
- 依据风险造成的业务后果和发生的可能性进行风险评估
- 就风险的后果和可能性进行沟通并达成理解
- 建立风险处置的优先次序
- 对降低风险的活动进行排序
- 在做出风险管理决策时，让利益相关方参与，并及时告知风险管理的状态
- 有效监视风险处置
- 监视风险和风险管理过程，并定期评审
- 收集信息以改进风险管理方法
- 应该对管理者和员工进行有关风险和减轻风险所应采取行动的培训

信息安全风险管理过程可能应用于整个组织，组织的任何部分（如部门、物理区域或某个服务），任何信息系统，现有、计划或特定部分的控制措施（如业务连续性计划）。

6. 信息安全风险管理过程概述

信息安全风险管理过程由确定范畴（条款 7）、风险评估（条款 8）、风险处置（条款 9）、风险接受（条款 10）、风险沟通（条款 11）以及风险监视和评审（条款 12）组成。

如图 1 所示，信息安全风险管理过程可能循环进行风险评估和/或风险处置活动。风险评估的循环方法能够使得每一次循环更加深入和具体。循环方法可以在确保高风险被准确识别和在识别控制措施上花费最小的时间和精力之间寻找平衡。

首先确定范畴。然后进行风险评估。如果风险评估为进行有效决策的提供了充分的信息，以确定将风险降低到可接受级别所需活动，则风险评估任务结束，开始进行风险处置。如果信息不够充分，则进行另外一个修订范畴和风险评估的循环，也可能是整个范围内的部分内容进行循环。

有效的风险处置依赖于风险评估的结果。风险处置可能不会立即将残余风险降低到可以接受的级

别。对于这种情形，可能需要变更风险范畴参数（如风险评估、风险接受或影响的准则）再次进行的风险评估循环，并可能需要进一步的风险处置（参见图 1， 风险决策点 2）。

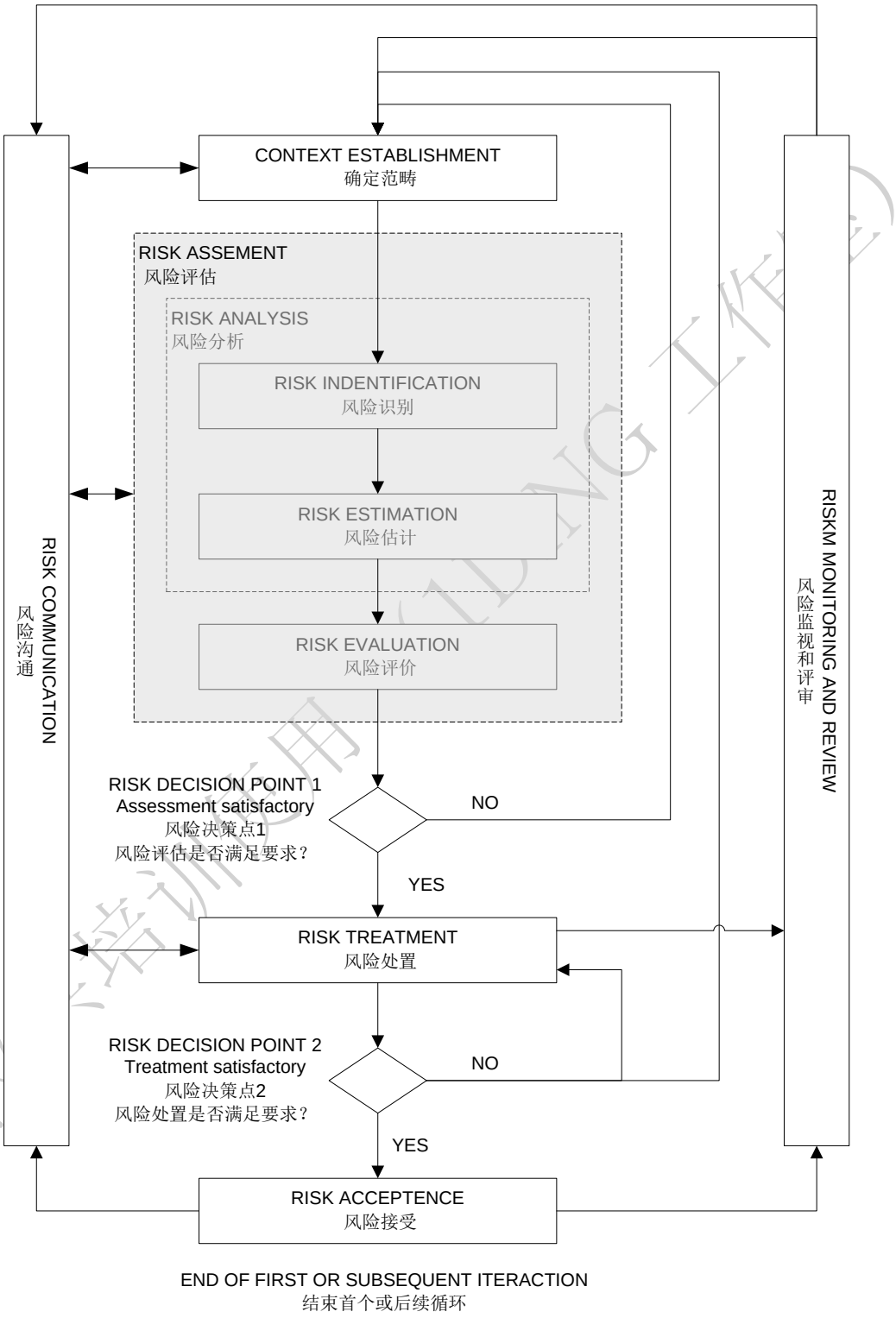

图 1 信息安全风险处理过程

风险接受活动需要确保残余风险被组织的管理者明确接受。对于控制措施被取消或推迟实施（如，因成本问题）的情形，管理层的明确接受就更为重要。

在整个信息安全风险管理过程中，向相应的管理者和员工传达风险和风险的处置是很重要的。甚至在风险处置前，有关已识别的风险信息对于管理事件可能是很有价值的，并可以帮助降低潜在损失。管理者和员工的风险意识、降低风险的现有控制措施的特性以及组织所关心的区域，将为处理事件和非预期事态提供有效的帮助。信息安全风险管理过程的每一活动及两个风险决策点的详细结果应该形成文件。

ISO/IEC 27001 规定的 ISMS 的范围、边界和范畴内所实施的控制措施应是基于风险的。信息安全风险管理过程的应用可以满足这项要求。有很多在组织内成功实施风险管理过程的方法。组织每一具体的过程应用所使用的任何过程方法，应该是最适合于自身情形的。

在 ISMS 中，确定范畴、风险评估、开发风险处置计划以及风险接受都是“计划”阶段中的一部分。在 ISMS 的实施阶段中，按照风险处置计划实施降低风险所需的活动和控制措施。在 ISMS 的“检查”阶段，管理者根据事件和环境的变化， 确定是否需要修订风险评估和风险处置。在“改进”阶段，执行任何需要的活动，包括信息安全风险管理过程的补充应用。

下表概述了与 ISMS 过程的四个阶段相关的信息安全风险管理活动：

表 1：ISMS 和信息安全风险管理过程的对应关系

ISMS 过程	信息安全风险管理过程
计划	确定范畴 风险评估 开发风险处置计划 风险接受
实施	实施风险处置计划
检查	持续监视和评审风险
改进	维持和改进风险管理过程

7. 确定范畴

7.1. 总则

输入：与确定信息安全风险管理范畴相关的所有关于组织的信息。

活动：应该确定信息安全风险管理的范畴，这涉及信息安全风险管理所必须的基本准则的设定（条款 7.2），范围和边界的界定（条款 7.3），适合于信息安全管理运行的组织架构的确定（条款 7.4）。

实施指南：

确定信息安全风险评估的宗旨是必要的，因为这将影响整个风险评估过程，特别是对确定风险评估范畴的影响。信息安全风险评估的宗旨可能是：

- 支持 ISMS
- 符合法律和尽职的证据
- 准备业务连续性计划
- 准备事件响应计划
- 描述某个产品、服务或机制对信息安全的要求

确定支持 ISMS 所需要的范畴要素的实施指南，将在条款 7.2、7.3 和 7.4 中作进一步讨论。

注：ISO/IEC 27001 并不使用术语“范畴”。但是，条款 7 的所有内容都与 ISO/IEC 27001 中“定义 ISMS 的范围和边界”（ 4.2.1a）、“定义 ISMS 方针”（4.2.1b）、“定义风险评估方法”（4.2.1c）的要求相关。

输出：对信息安全管理过程的基本准则、范围和边界、以及组织架构的说明。

7.2. 基本准则

根据风险管理的范围和目标的不同，可能采用不同的方法。对于每一循环，所采用的方法也可能不同。

一个合适的风险管理方法应该选择或开发基本准则，如风险评价准则、影响准则、风险接受准则。

另外，组织还应该评估是否具有进行以下活动所需的必要资源：

- 进行风险评附和确定风险处置计划
- 定义和实施方针和程序，包括实施已选择的控制措施
- 监视控制措施
- 监视信息安全风险管理过程

注：也可参见 ISO/IEC 27001（条款 5.2.1）中有关实施和运行 ISMS 所需资源的提供。

风险评价准则

组织应该在考虑以下内容的基础上开发评价组织信息安全风险的风险评价准则：

- 业务信息过程的战略价值
- 相关信息资产的危急程度
- 法律法规的要求和合同的义务
- 运营和业务的可用性、保密性、完整性的重要程度
- 利益相关方的期望和认知，以及对信誉和名声的负面影响

另外，风险评价准则也可能被用于定义风险处置的优先级。

影响准则

应该在考虑以下内容的基础上开发影响准则，并以信息安全事态造成的对组织损害程度或成本的方式加以说明：

- 受影响资产的分类级别
- 信息安全的违背（如保密性、完整性和可用性的丧失）
- 运行的受损（内部或第三方的）
- 损失的业务或财务价值

- 对计划和最后期限的破坏
- 声誉的损失
- 对法律法规或合同要求的违背

注：也可参见 ISO/IEC 27001 （条款 4.2.1d4）关于丧失保密性、完整性和可用性的影响准则的识别。

风险接受准则

应该开发和阐述风险接受准则。风险接受准则的常常依赖于组织的方针、目的、目标以及利益相关方的利益。

组织应该定义自身的风险接受级别的尺度。在开发风险可接受准则时，应该考虑以下方面：

- 风险接受准则可以包括带有风险期望目标级别的多道门槛，但在确定的情形下，提交给高层管理者接受的风险可能超出该级别
- 风险可接受准则可以用估算收益（或业务收益）与估算风险的比值来描述
- 对不同类型的风险可以采用不同的风险接受准则，例如，导致对法律法规不符合的风险可能是不可接受的，但可能允许接受导致违背合同要求的高风险
- 风险接受准则可以包括下一步的补充处置要求，例如，如果认可或承诺在确定的时间内将采取行动以将风险降到可接受级别，则风险可以被接受

风险接受准则可能因预计风险将多长时间存在而不同，例如风险可能与一个临时或短期活动相关。设定风险接受准则时，应该考虑：

- 业务准则
- 法律法规方面
- 运营
- 技术
- 财务
- 社会和人为因素

注：风险接受准则与 ISO/IEC 27001 中条款 4.2.1c)2)所描述的“接受风险的准则，识别可接受的风险级别”相对应。

附录 A 中将提供更多的信息。

7.3. 范围和边界

组织应该定义信息安全风险管理的范围和边界。

需要定义信息安全风险管理过程的范围，以保证在风险评估过程中考虑到所有相关资产。另外，需要定义边界（参见 ISO/IEC 27001 的条款 4.2.1a）以处理在边界处呈现的风险。

应该收集组织的相关信息，以确定其运营环境及其对信息安全风险管理过程的相关性。

在定义范围和边界时，组织应该考虑以下信息：

- 组织的业务战略目标、策略和方针
- 业务过程
- 组织的职能和结构
- 适用于组织的法律法规和合同义务的要求
- 组织的信息安全方针
- 组织风险管理的整体方法
- 信息资产
- 组织的位置及其地理特性
- 影响组织的约束条件
- 利益相关方的期望
- 社会文化环境
- 界面（与环境的数据交换）

另外，组织对任何排除在范围之外的，都应该提供正当的理由。

例如，风险管理范围的可能是一个 IT 应用、IT 基础设施、一个业务过程或组织的某个界定部分。

注：信息安全风险管理的范围和边界与 ISO/IEC 27001 4.2.1a 所要求的 ISMS 的范围和边界相对应。

附录 A 中提供进一步的信息。

7.4. 信息安全的组织架构

应该设置和维持信息安全风险管理过程的组织架构和职责。下面是信息安全风险管理过程组织架构的主要角色和职责：

- 开发适合组织的信息安全风险管理过程
- 识别和分析利益相关方
- 定义组织内、外部各方的角色和职责
- 在组织和相关利益方之间建立必要的联系，如组织高风险管理职能的接口（如运营风险管理），以及与其它项目或活动之间的接口
- 定义决策升级路径
- 说明需要保存的记录

组织架构应该得到组织的合适的管理者的批准。

注：ISO/IEC 27001 要求确定并提供建立、运行、监视、维持和改进 ISMS 所需要的资源（5.2.1a）。可以认为风险管理运营的组织架构是 ISO/IEC 27001 所要求的资源之一。

8. 信息安全风险评估

8.1. 信息安全风险评估综述

注：风险评估活动是指 ISO/IEC 27001 中的风险评估过程。

输入：已确定的信息安全管理过程的基本准则、范围和边界、组织架构。

活动：应该进行识别风险，进行定量或定性的描述，并依据风险评价准则和与组织目标的相关性

进行排序。

实施指南：

风险是非期望事态的发生所带来的后果与事态发生可能性的组合。风险的定量评估或定性描述使得管理者能够按照他们感知的严重程度或其他已确定的准则对风险进行排序。

风险评估由以下活动组成：

- 风险分析（条款 8.2），包括：
  - 风险识别 （条款 8.2.1）
  - 风险估算（条款 8.2.2）
- 风险评价（条款 8.3）

风险评估确定信息资产的价值、识别适用的威胁和（存在或可能存在的）脆弱点、识别现有控制措施及其对已识别风险的影响，确定潜在后果，对风险进行最终的优先级排序，并按照风险范畴中设定的风险评价准则进行排名。

风险评估通常会进行两个（或多个）循环。首先进行纲领性的风险评估以识别需要进一步评估的潜在高风险。下一个循环可能对最初循环中发现的潜在高风险进行进一步的深入考虑。如果风险评估的信息不充分，则需要进行进一步的详细分析，这可能是针对整个范围当中的一部分，也可能采用不同的办法。

组织基于风险评估的目的和目标选择自己的风险评估方法。

可以从附录 E 中找到有关风险评估方法的讨论信息。

输出：已评估的按照风险评价准则进行优先排序的风险清单。

8.2. 风险分析

8.2.1. 风险识别

8.2.1.1. 风险识别介绍

风险识别的目的是确定可能发生什么将导致潜在的损失， 并且洞察可能发生的损失将怎样发生、在哪里发生、为什么发生。在随后条款 8.2.1 中所描述的步骤应该为风险估算活动收集数据。

注：随后条款中所描述的活动可能因所采用的办式不同，而按照不同的次序进行。

8.2.1.2. 资产识别

输入：将要进行风险评估的范围和边界，由所有者、位置、功能等构成的清单。

活动：在已确定范围内的资产应该得到识别（参考 ISO/IEC 27001 的条款 4.2.1d)1)）。

实施指南：

资产是对组织有价值的任何东西，并因此需要加以保护。识别资产时应该铭记的是，一个信息系统不仅仅由硬件和软件组成。

资产识别应该在适合的细节层面进行，以为风险评估提供充分的信息。资产识别的细节层面将影响风险评估中所收集的信息总量。细节层面可以在后续的信息安全评估循环中优化。

应该为每一资产识别资产所有者，以为资产安排职责和责任。资产所有者可能并不拥有资产的所有权，但承担资产的产生、开发、维护、使用以及合适的安全保护的责任。资产所有者通常是确定资产对组织价值的最合适人选 （参见 8.2.2.2 资产赋值）。

审查边界以确定组织已定义的、应由信息安全风险管理过程管理的资产范围。

附录 B 提供有关信息安全的资产识别和赋值的更多信息。

输出：将要进行风险管理的资产清单，以及与资产相关的业务过程清单和相互关系。

8.2.1.3. 识别威胁

输入：从事件评审、资产所有者、使用者或其他来源，包括外部提供的威胁清单中，获得关于威胁的信息。

活动：应该识别威胁和威胁的来源（参考 ISO/IEC 27001 的条款 4.2.1d) 2)）。

实施指南：

威胁对如信息、过程、系统等资产构成潜在损害，并由此给组织带来损害。威胁可能是自然的或人为的， 可能是意外或故意的。意外的或故意的威胁都应该得到识别。威胁可能来自组织内部和外部。应该整体并按类型（如非授权行为、物理损坏、技术失效）识别威胁，从而已识别的通用类别中的单个威胁得到识别。这意味着没有威胁被忽视，包括非预期，但所需要的工作量是有限的。

有些威胁可能影响多个资产。在这种情形，因受影响的资产不同，威胁可能造成不同的影响。

可以从资产所有者或使用者、人力资源员工、设备管理者、信息安全专员、物理安全专家、法律部门以及包括法律机构、气象部门、保险公司和政府机构等获得识别威胁和估算发生可能性所需的输入。在处理威胁时，必须考虑环境和文化因素。

当前进行的评估，应该考虑从事件得到的内部经验和过去进行的威胁评估。在适当时，参考其他的威胁清单（可能是针对某个组织或业务）以完善通用威胁清单。可以从行业机构、政府部门、法律机构和保险公司获得威胁清单和统计资料。

在使用威胁清单或前期的威胁评估成果时，应该注意到的一点是，相关威胁是持续变化的，特别当业务环境或信息系统发生变化时。

从附录 C 中可以找到有关威胁类型的更多信息。

输出：带有类型和来源的威胁识别清单。

8.2.1.4. 识别现有控制措施

输入：控制措施文档，风险处置实施计划

活动：应该识别现有的和已计划的控制措施。

实施指南：

应该识别现有控制措施，以避免不必要的工作和成本，如重复的控制措施。另外，在识别现有控制措施时，应该进行检查以确保控制措施在有效工作 – 参考已有的 ISMS 审计报告可以减少这项工作所花费的时间。如果控制措施没有按预期进行工作，将会形成脆弱点。应该关注已选择的控制措施（或策略）的运行失效，并因此需要补充控制措施以有效处理风险。按照 ISO/IEC 27001，一个 ISMS 由控制措施的有效性测量来支持。估算控制措施效果的一个方式是，看控制措施怎样降低威胁发生的可能性、消除暴露的脆弱点或降低事件的影响。管理评审或审计报告也将提供有关现有控制措施有效性的信息。

按照风险处置计划将要实施的控制措施应该视同已经实施的控制措施。

现有或计划的控制措施可能被识别为无效的、不充分的或不合理的。应该检查不充分或不合理的控制措施，以确定是否应该取消、由其他更有效的控制措施替代或继续保持（如，因为成本因素）。

以下活动可能为识别现有或计划的控制措施提供帮助：

- 评审包含控制措施信息的文件（如，风险处置计划）。如果信息安全管理过程得到了很好的文件化，应该可以获得所有的现有或计划的控制措施及其现状；
- 与信息安全责任人（如信息安全官和信息系统安全官、大楼管理员和运行管理员）和用户联系，以确认对所考虑的信息过程或信息系统的哪些控制措施得到了真正的实施；
- 对照应该已实施的控制措施清单，对物理控制措施进行现场评审，并检查已实施的控制措施是否正确、有效工作；或
- 评审内部审核的结果

输出：所有现有或计划的控制措施清单，控制措施的实施和使用状况。

8.2.1.5. 识别脆弱点

输入：已知的威胁清单，资产清单和现有控制措施清单

活动：应该识别可能被威胁利用以对资产或组织造成损害的脆弱点。

实施指南：

可以从以下领域识别脆弱点：

- 组织架构
- 过程和程序
- 管理惯例
- 人员
- 物理环境
- 信息系统配置
- 硬件、软件或通讯设备
- 对外部的依赖

脆弱性的存在本身不会形成损害， 它需要被某个威胁所利用。如果脆弱性没有对应的威胁，则可以不需要实施控制措施，但应该注意并监视所发生的变化。应该注意到控制措施实施的不合理、控制措施故障或控制措施的错误使用本身也是一个脆弱点。控制措施因其运行的环境，可能有效或无效。相反，一个威胁如果没有对应的脆弱点，也不会导致风险的发生。

脆弱点可能与资产的使用方式、目的等属性有关，而不论资产购买和构建时的意图。需要考虑不同来源的脆弱点，内在的或外来的。

可以从附录 D 中找到脆弱点的示例和脆弱性评估的方法。

输出：与资产、威胁和控制措施相关的脆弱点清单；待评审的与任何已识别的威胁不相关的脆弱点清单。

8.2.1.6. 后果的识别

输入：资产清单、业务过程清单、威胁和脆弱点清单，适当时，包括相关资产及相互关系。

活动：资产丧失保密性、完整性和可用性的后果应该得到识别（参见 ISO/IEC 27001 条款 4.2.1d) 4)）。

实施指南：

后果可能是有效性的丧失、不利的运行环境、业务的丧失、名誉的损失和损害等。

本阶段的活动识别由某个事件情景导致对组织的损害或后果。事件情景，是对在信息安全事件（参见 ISO/IEC 27002 条款 13）中威胁利用某个特定的脆弱点或一组脆弱点的描述。根据在确定范畴活动中所定义的影响准则，确定事件情景的影响。事件情景可能影响一个、多个资产或单个资产的一部分。因此，可以按资产的财务成本和资产破坏或损坏后带来的业务影响，给资产赋值。资产受到损害时，后果可能是临时性的，也可能是长期的。

注：ISO/IEC 27001 中用“安全失效”描述事件情景的发生。

组织应该识别事件情景在以下方面（但不限于）的运营后果：

- 调查和修复时间
- （工作）时间的损失
- 机会的丧失
- 健康和人身安全
- 修复损伤所需特殊技能的财务成本
- 信誉和形象

可以在 B.3 影响评估中找到有关技术脆弱性评估的具体信息。

输出：与资产和业务过程相关的事件情景清单。

8.2.2. 风险估算

8.2.2.1. 风险估算办法

风险分析根据资产的重要性、已知脆弱点的范围以及以前与组织相关的事件，而进行到不同的具体深度。估算办法根据条件，可以是定性的、定量的或者是两者的组合。实际上，通常首先采用定性估算以获得一般性的风险级别指示和发现重大风险。

随后可能需要对重大风险进行更明确的或定量分析，因为通常定性分析比定量分析要简单，而且花费要少。

分析的形式应该与作为确定范畴的一部分而制定的风险估算准则相一致。

估算办法更具体的内容描述如下：

(a) 定性估算：

定性估算采用尺度分级属性（如低、中、高）来描述潜在后果的严重性和潜在后果发生的可能性。定性估算的优点是易于所有相关人员的理解，同时其弱点是尺度选择对主观判断的依赖。

可以对尺度进行修订或调整，以适应当时的情况，并为不同的风险采用不同的描述。定性分析可以用于：

- 作为最初的筛选活动，以识别需要进一步具体分析的风险
- 当定性分析对决策来说是合适时
- 当量化数据不足以进行定量估算时

定量分析应该使用可用的真实的信息和数据。

(b) 定量估算：

定量估算通过不同来源的数据，使用数字化的尺度来描述后果和可能性（而不是定性评估中所使用的描述性尺度）。分析的质量依赖于量化数字的准确性和完整性，以及所使用模型的有效性。在很多情况下，定量估算使用历史的事件数据，优势是其直接与信息安全目标和组织所关心的问题相关。不足是缺乏新的风险或信息安全弱点的数据。当无法获得真实和可审计数据时，将显示定量估算的不足，因为这将导致风险评估准确性和价值的假象。

后果和可能性的表达方式，以及其组合形成的风险等级的表达方式，将随着风险的类型和风险评估输出的使用目的不同而变化。在进行有效分析和沟通时，应该考虑后果和可能性的不确定性和可变性。

8.2.2.2. 后果的评估

输入：已识别的相关事件情景，包括识别威胁、脆弱点、受影响的资产、对资产和业务过程的后果。

活动：应该在考虑违背信息安全，如丧失资产的保密性、完整性、可用性的基础上，评估可能或实际的信息安全事件可能导致的对组织业务的影响（参考 ISO/IEC 27001 条款 4.2.1e) 1)）。

实施指南：

在识别所有资产并评审后，在评估后果的同时应该给资产赋值。

业务影响可以用定性或定量来表示，但任何采用货币赋值的办法，一般可以为决策提供更多的信息，从而有助于更有效的决策过程。

资产的赋值从按资产对满足业务目标的重要程度对资产进行分类开始。通过以下两种措施来确定资产价值：

- 资产的替代价值：恢复清理和替换信息所需的成本（如果可行），以及
- 资产丧失或损坏的业务后果，如信息或其他信息资产的泄密、修改、不可用和/或破坏带来的潜在业务负面影响和/或法律后果

可以从业务影响分析来赋值。资产价值根据资产对满足组织业务目标的重要性，由业务后果来确定，通常比简单的替代成本高很多。

对事件情景，资产价值是影响评估的关键因素，因为事件可能影响到不只一个资产（如，关联资产），或仅仅是资产的一部分。不同的威胁或脆弱点将对资产带来不同的影响，如丧失保密性、完整性或可用性。因此后果的评估与基于业务影响分析的资产价值相关。

后果或业务影响可以由一个或一系列事态的输出模型来确定，或由实验研究或历史数据来推断。

后果可以用货币、技术或人身影响准则，以及与组织相关的其它准则来描述。在某些情形，对不

同的时间、地点、分类或环境需要多个价值数值来描述后果。

应该用相同的方法测量威胁的可能性和脆弱点在时间和财务上的后果。需要保持定性和定量方法的一致性。

附录 B 提供有关资产赋值和影响评估的更多信息。

输出：用资产和影响准则来表示事件情形评估后果的清单。

8.2.2.3. 评估事件可能性

输入：已识别的相关事件情景，包括识别的威胁、受影响的资产、暴露的脆弱点、对资产和业务过程的后果。此外，所有现有和计划的控制措施清单，以及控制措施的有效性、实施和使用状态。

活动：应该对事件情景的可能性进行评估（参考 ISO/IEC 27001，条款 4.2.1e) 2)）。

实施指南：

在识别事件情景后，需要利用定性或定量评估技术对每一情景的可能性和产生的影响进行评估。这应该考虑威胁发生经常性和脆弱点被利用的容易程度，并考虑以下内容：

- 威胁发生可能性的经验值或可用的统计数据
- 对于来自故意的威胁：随时间的变化动机和能力，资源对可能进行攻击者的可用性，以及资产对可能攻击者的吸引力和脆弱点
- 对来自意外的威胁：地理因素，如在化工厂或石油工厂的附件，极端天气的可能性，可能导致人员过错或设备故障的因素
- 脆弱点， 单个脆弱点以及脆弱点的组合
- 现有控制措施及其怎样有效降低脆弱性

比如，某个信息系统可能存在能够被冒名用户不当使用的威胁所利用的脆弱点。因为缺乏用户的验证，冒用用户身份的脆弱性可能很高。另一方面，尽管缺乏用户验证，但资源不正当使用的可能性很低，因为不正当使用资源的方式很少。

根据对精确性的要求，可能对资产进行分类，也可能需要将资产分解到组件，并将事件情景与组件相关联。例如，对跨区域的同一类型的资产，威胁的特性可能会有变化，或者现有控制措施的有效性可能不同。

输出：事件情景的可能性（定性的或定量的）

8.2.2.4. 风险级别的估算

输入：事件情景清单，及其对资产和业务过程的后果和可能性（定性的或定量的）。

活动：应对所有相关的事件情景进行风险级别评估（参考 ISO/IEC 27001 条款 4.2.1 e) 4)）

实施指南：

风险估算：对风险的可能性和后果进行赋值。赋值可以是定性的或定量的。风险评估是基于后果和可能性的评估。另外，可能考虑成本效益、相关利益方的疑虑，以及其他对风险评价适用的因素。风险估算是某个事件情景的可能性及其后果的组合。

附录 E 提供不同信息安全评价的方法和办法的示例。

输出：分配有风险级别数值的风险清单。

8.3. 风险评价

输入：分配有风险级别数值的风险清单和风险评价准则。

活动：应该将风险级别与风险评价准则和风险接受准则进行比较（参考 ISO/IEC 27001，条款 4.2.1 e) 4)）。

实施指南：

在建立风险范畴时已经确定用于风险决策的风险评价和风险评价准则的特性。在这一阶段，已经知悉已识别风险的更多具体信息，应该对风险决策和范畴进行回顾。为评价风险，组织应该将已

实施指南：

风险处置有四个选项：风险降低（参见 9.2），风险保持 （参见 9.3），风险回避（参见 9.4）和风险转移（参见 9.5）。

注：ISO/IEC 27001 4.2.1f)2) 用术语“接受风险”代替“保持风险”。

图 2 表示在图 1 所描述的信息安全风险管理过程中的风险处置活动。

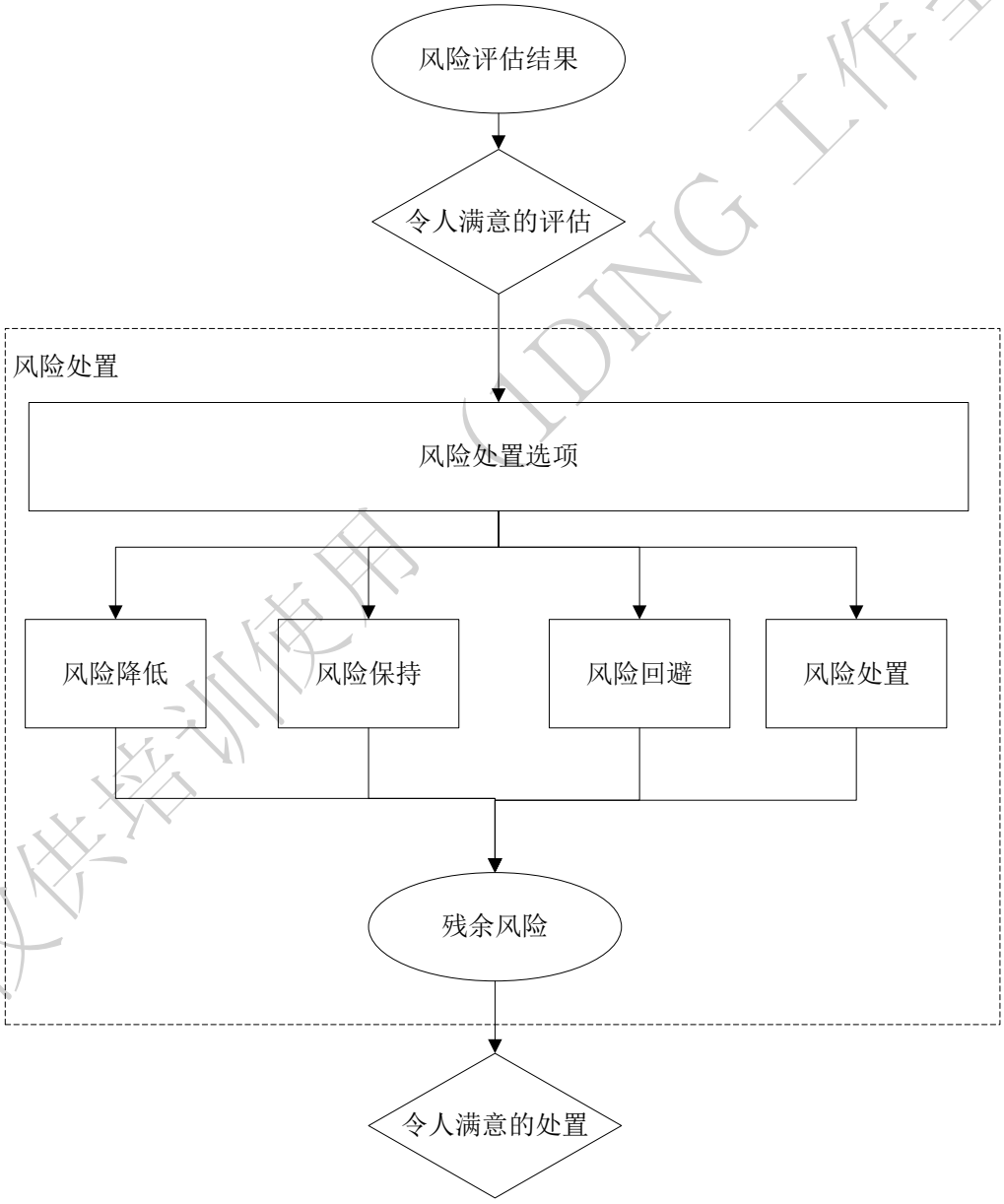

图 2：风险处置活动

应该基于风险评估的结果、实施这些选项的预计成本及预期收益来选择风险处置选项。

如果通过某一选项可以通过相对较低的花费大幅度降低风险，则应该实施该选项。如果下一步的改进选项可能是不经济的，则需要判断是否合理。

一般而言，不论任何绝对准则，应该在切实可行的范围内降低风险的负面后果。管理者应该考虑罕见但严重的风险。在这种情形下，可能需要实施控制措施，而不会严格按经济性进行判断（例如为应对特定的高风险，而考虑业务连续性控制措施）。

风险处置的四个选项并不互相排斥。有时，组织可以通过选项的组合充分获益，如降低风险的可能性、降低风险的后果，并转移或保持残余风险。

某些风险处置可能有效处理多个风险（如信息安全培训和意识教育）。风险处置计划应该清晰定义所列出的单个需要实施的风险处置项的优先级，以及实施的时间框架。可以用不同的技术来确定优先级，包括风险级别和成本效益分析。平衡实施控制措施的成本和预算安排，是组织管理者的职责。

识别现有控制措施，可以通过与成本（包括控制措施的维护）相比较的方式，确定现有控制措施确定是否超过当前的要求。如果考虑取消多余或不必要的控制措施（特别是控制措施存在很高的维护成本时），应该考虑信息安全和成本因素。由于控制措施相互影响，取消多余的控制措施可能降低现有的整体安全。另外，可能保留现有的多余或不必要的控制措施比取消这些控制措施的成本更低。

风险处置选项，应该考虑：

- 受影响方对风险的感知是怎样的
- 与这些受影响方进行沟通的最合适方式

范畴的确定（参见 7.2 – 风险评价准则）提供了组织需要满足的法律法规要求方面的相关信息。应该实施限制组织符合性失效风险的发生可能性的处置选项。在风险处置中应该考虑在范畴确定活动中识别的所有限制 ----- 组织的、技术的、架构等。

风险处置计划一旦被界定，则需要确定残余风险。考虑建议的风险处置的预期效果，进行风险评估的更新或再次循环。

如果残余风险仍不满足组织的风险接受准则，在提交以进行接受风险前，可能需要进行一步的风险处置循环。可以从 ISO/IEC 27002 0.3 条款中获得更多的信息。

输入：提交风险处置计划和残余风险给组织管理者以进行风险接受决策。

9.2. 风险降低

活动：通过选择控制措施，风险级别应该被降低，使可以进行残余风险的再评估，以便可以被接受。

实施指南：

应该选择适当和合理的控制措施，以满足风险评估和风险处置中识别的要求。控制措施的选择应该考虑风险接受则以及法律、法规和合同义务的要求。还应该考虑实施控制措施的成本和时间表，以及技术、环境、文化等因素。合理选择信息安全控制措施，常常会降低系统的整体拥有成本。

一般而言，控制措施可以提供以下一个或多个方面的保护：纠正、消除、预防、将影响最小化、制止、检测、恢复、监视和意识。在选择控制措施时，权衡控制措施的采购、实施、管理、运行、监视和维护的成本与被保护资产的价值。此外，在投资回报率中应该考虑特定控制措施所带来的风险的降低和潜在的开发新业务的机会。另外，还应该考虑定义、实施新的控制措施或修改现有控制措施所需的特定技能。

ISO/IEC 27002 提供有关控制措施的具体信息。

有很多可能影响控制措施选择的约束条件。如性能要求、可管理性（运行支持的要求）和兼容性问题，可能妨碍某些控制措施的使用或可能导致人为错误及控制措施失灵，使得对安全的感知失灵、甚至导致风险比没有控制措施时还要高（如要求使用强密码，但缺乏合适的培训，导致用户将密码写下来）。

此外，可能的情形是控制措施对影绩效的影响。管理者应该尝试识别在满足绩效要求的同时保证充分的信息安全的解决方案。该步骤的结果是，可能的控制措施清单以及措施的成本、收益和实施的优先次序。

在选择和实施控制措施时，应该考虑多种约束条件。特别是以下约束：

- 时间约束
- 财务约束
- 技术约束
- 运行约束
- 文化约束
- 道德约束
- 环境约束
- 法律约束
- 易用性约束
- 人员约束
- 整合新建和现有控制措施的约束

可以从附录 F 中获得更多有关降低风险的约束的信息。

9.3. 风险保持

活动：根据风险评估，决定不采取进一步的活动而保持风险。

注：与 ISO/IEC 27001 4.2.1 f) 2)中 “在明显满足组织方针策略和接受风险的准则的条件下，有意识的、可能的接受风险”所表达的意思相同。

实施指南：

如果风险级比满足风险接受准则，则不需要实施额外的控制措施，而风险可能被保持。

9.4. 风险回避

活动：应该规避导致特定风险的活动或条件。

实施指南：

如果认为所识别的风险太高，或实施其它控制处置选项成本超过了收益，则可以做出完全回避风险的决策，取消计划的或现有的活动（或一系列活动），或者改变运行环境。如对于来自自然的风险，将信息处理设施物理的转移到没有风险或风险受控的位置，可能是最符合成本经济效益的选择。

9.5. 风险转移

活动：根据风险评估结果，对于特定风险最有效的管理，可能是将风险转移给其他方。

实施指南：

风险转移涉及与外部分担风险的决策。风险转移可能产生新的风险或改变现有的、已识别的风险。由此，可能需要额外的风险处置。

风险转移可以通过保险公司来分担后果，或将监视信息系统并在攻击形成已定义级别损害前立即采取行动制止攻击的职责外给合作伙伴。

应该指出的是，有可能转移风险管理的责任，但它通常不能够转移影响的法律责任。客户通常认为是由于组织的过失导致的负面影响。

10. 信息安全风险的接受

输入：将风险处置计划和残余风险的评估提交给组织的管理者以进行接受风险的决策。

活动：应该正式记录风险接受决策的出台和相关的决策责任。（参考 ISO/IEC 27001 4.2.1h)）。

实施指南：

风险处置计划应该描述怎样处置被评估的风险以满足风险接受准则 （参见条款 7.2 风险接受准则）。承担责任的管理者对被提议的风险处置计划和随之而来的残余风险的评审和批准，并记录与批准相关的任何先决条件，是很重要的。

风险接受准则可能会很复杂，而不仅是是判断残余风险在门槛之上还是之下。

在某些情形，残余风险的级别可能不满足风险接受准则，因为目前适用的准则，没有考虑到当前的情形。例如，可以认为有必要接受风险，因为伴随风险的收益可能是非常有吸引力的，或降低风险的成本太高。这些情形表明风险接受准则可能是不合适的，如果可能应该进行修订。然而，不太可能总能及时的修订风险接受准则。

在这些情形，决策者可能必须接受不满足正常风险接受准则的风险。 如果必须如此，决策者应该明确说明风险，包括跳过正常风险接受准则的决策理由。

输出：未能满足正常风险接受准则的，但被接受的风险清单，并附带接受的理由。

11. 信息安全风险的沟通

输入：从风险管理活动中获得的所有风险信息（参见图 1）。

活动：应该在决策者和其他利益相关方之间进行交换和/或共享有关风险的信息。

实施指南：

风险沟通是通过在决策者或其他相关利益方之间交换和/或共享风险信息以达成协议的活动。 这些信息包括但不限于，风险的存在、性质、形式、可能性、严重性、处置和可接受性。

利益相关方之间有效沟通是重要的，因为这将对必须作出的决策有很大的影响。沟通将确保实施风险管理的责任人以及重大利益相关方理解决策出台的基础和为什么需要特定的活动。沟通应是双向的。

因风险或讨论议题相关的假设、概念、需求、问题以及利益相关方关注点的不同，对风险的认知可能会不同。利益相关方可能会基于他们对风险的理解来判断风险的可接受性。确保能够识别利益相关方的风险认知以及他们对收益的认知，并形成文件，以及深层的原因得到理解和处理，是非常重要的。

应该进行风险沟通以满足：

- 为组织的风险管理成果提供信心
- 收集风险信息
- 分享风险评估的结果和展示风险处置计划
- 为了避免或减少由于决策者和利益相关方之间缺乏相互理解，而导致的违背信息安全事项的发生和后果
- 为决策提供支持
- 获得新的信息安全知识
- 与其它各方进行协调，并计划应对措施以降低任何事件的可能性
- 为了让决策者和利益相关方意识到关于风险的责任
- 提高意识

组织应该为正常的运行和紧急情形制定风险沟通计划。因此， 风险沟通活动应该持续进行。

可以通过成立讨论风险、风险优先次序、合适的处置方式和接受可能性的委员会来达到主要决策者和利益相关方之间的协调。

重要的是要配合适当的公共关系或组织内部的沟通部门，协调所有有关的风险沟通的任务。这对危机时的沟通活动是至关重要的，例如，应对特定的事件。

输出：对组织风险管理过程和结果的持续的理解。

12. 信息安全监视和评审

12.1. 监视和评审风险因子

输入：从风险管理活动中获得的所有风险信息（参见图 1）。

活动：应该监视和评审风险和风险要素（如资产的价值、影响、威胁、漏洞、发生的可能性），以及在早期识别的组织范畴的任何变化，并维护风险的完整景象。

事实指南：

风险不是静态的。威胁、弱点、可能性或后果可能发生没有任何迹象的突变。因此必须持续进行监视以发现这些变化。也可以通过外部服务提供的有关新的威胁或脆弱点，来获得对监视活动的支持。

组织应该确保对以下方面的持续监视：

- 新的资产被包含到风险管理范围内
- 资产价值的必要变更， 如因业务要求的变化
- 未被评估的、能够在组织内部和外部发生作用的新的威胁
- 新的或增加的脆弱点，以及允许威胁利用这些新的或变化的脆弱点的可能性
- 确定被新的或再现的威胁所利用的已识别的脆弱点
- 已评估威胁、脆弱点的影响或后果的增大和风险的聚集，形成令人无法接受的风险级别
- 信息安全事件

新的威胁、脆弱点以及可能性或后果的变化，可能增大以前被评估为低风险的风险。对低风险或已接受风险的评审应该考虑针对每一风险单独进行，并对这类风险作为一个整体进行考虑，以评估潜在的累积风险。如果风险没有降到低风险或可接受风险级别，则应该利用条款 9 中所考虑的一个或多个选项进行处置。

影响威胁发生的可能性和后果的因素可能发生变化，并可能影响处置选项的适宜性或成本。应该查找影响组织的主要变化的原因，以进行更具体的评审。因此，风险监视活动应该定期重复进行，并周期性评审风险处置的选项。

风险监视活动的输出可能输入到其它风险评审活动中。（按照 ISO/IEC 27001，条款 4.2.3）当发

生重大变化时，组织应该定期评审所有风险。

输入：不断调整的风险管理，以与组织的业务目标和风险接受准则相一致。

12.2. 风险管理监视、评审和改进

输入：从风险管理活动中获得的所有风险信息（参见图 1）

活动：应该根据需要和适宜性，持续对信息安全风险管理过程进行监视、评审和改进。

实施指南：

为确保范畴、风险评估和风险处置的结果，以及管理计划保持对当前环境的相关性和适宜性，持续进行监视和评审是必要的。

组织应该确保信息安全管理过程和相关活动对当前环境的适宜性，并得到跟踪管理。任何商定的过程改进或更好地遵循这一过程所需要活动，应该通知到合适的管理者，以确保没有风险或风险要素被忽视或低估，并且必要的行动被执行和决策得以出台，以提供现实的风险理解和应对能力。

此外，该组织应该定期评审用来测量风险及风险要素的准则仍然是有效的，并符合业务目标、战略和方针，并在信息安全管理过程中考虑到业务范畴的变更。监视和评审活动应该处理以下内容（但不限于）：

- 法律和环境范畴
- 竞争范畴
- 风险评估方法
- 资产价值和分类
- 影响准则
- 风险评价准则
- 风险接受准则
- 整体拥有成本
- 所需要的资源

组织的使命 组织通过完成其使命达到组织的意图。为了识别组织的使命， 应该识别提供给最终用户的相关服务和生产的产品。

组织的价值 价值是业务运作的主要原则或明确的行为守则。这可能关系到人员、与外部各方（客户等）的关系、提供的服务或产品的质量。

例如，某个组织的意图是公众服务，业务是交通运输，其使命是儿童上学的接送。其价值可能是准时的服务和安全的运送。

组织的架构 组织的架构有多种不同的形式：

- 事业部型架构：每个事业部被置于事业部经理权力之下，由事业部经理负责其部门的战略、管理和业务运作
- 职能型：基于程序、工作的性质，有时包括决策或计划，来设定职能授权（如生产、IT、人力资源、市场等）

注释：

- 在事业部型组织内的事业部可能采用职能型的架构，或者相反
- 如果组织同时采用以上两个形式，则可以称为混合型
- 任何类型的组织可以分为以下各个级别：
  - 决策层（确定战略方向）
  - 领导层（协调和管理）
  - 操作层（生产或支持活动）

组织结构图 组织的结构通过组织结构图进行纲要性的表述。组织结构图应该突出报告和授权的路径，还应该包括其他关系，因为这些关系即使不是基于任何正式的授权，却是信息流的路径。

组织的战略 要求有一个关于组织指导性原则的正式描述。组织的战略确定方向和发展的需要，以从利益攸关的议题和计划的重大变化中获益。

A.2 影响组织的约束清单

应该考虑影响组织和确定组织信息安全方向的所有约束。 约束的来源可能是组织内部，对于这种情形，可以对他们实施一些控制；有些约束来自外部，因此通常是不能协商的。资源的约束（预算、人员）和紧急情形的约束是最为重要的约束之一。

组织设定其目标（关于其业务、行为等），通过一定的路径来实现，并可能需要一段较长的期限。组织的目标定义期望达到的状态和需要实施的方式。在确定实现路径时，组织应该考虑技术和知识的发展、用户或客户表达的期望。目标可以通过运营或发展的战略目的的形式来表示，如降低运行成本、提高服务质量等。

这些战略可能包括有助于战略应用的信息和信息系统（IS）。由于在信息安全方面的违背可能会导致重新思考这些战略目标，由此，有关组织特性、使命、战略的特征是问题分析的基本要素。另外，至关重要的是，信息安全要求的建议要与组织推行的规则、用法和手段保持一致的。

约束的清单包括但不限于：

政治性的约束

这可能涉及政府管理部门、公众机构或更一般性的适用于任何组织的政府决策。它们通常是由政府部门或决策机构制定的关于战略或经营方向的决策，并应该得到应用。

如发票的电子化，或介绍信息安全问题的行政文件。

战略性的约束

约束可能产生于组织架构或目标的计划或可能的变化。战略性约束通常在组织战略或运营计划中表述。

例如，在共享敏感信息方面的国际合作可能需要就安全交流达成协议。

区域性约束

组织的架构和/或意图可能会导致特定的约束，如跨越整个国家区域或海外的分布网点。

例如，邮政业、大使馆、银行、大型工业集团的分支机构，等。

来自经济和政治气候的约束

组织的运营可能因特定事件引起重大变化，如罢工、国家或国际危机。

例如，某些服务即使在严重危机时也应该得以继续。

结构性约束

组织架构（事业部型、职能型或其它）的特性可能导致适用于该架构的特定的信息安全方针和信息安全组织结构。

例如，一个国际性的结构应该能够使每一国家特定的安全要求相融合。

功能性约束

功能性约束直接来自组织一般或特定的使命。

例如，一个组织 24 小时运作，则应该确保其资源的持续可用。

人员性约束

这些约束的差异很大。相关的有：职责的等级、招聘、资质、培训、安全意识、激励、可用性，等等。

例如，防卫组织的所有人员应该具有处理高保密信息的授权。

来自组织日程表的约束

这些约束可能来自组织的重组或设定新的、并具有最后期限的国内国际方针。

例如，成立一个新的安全部门。

与办法相关的约束

需要实施与组织知识相符合的办法，如项目计划、规范、开发等。

例如，这类约束的典型例子就是将组织的法律法规的义务整合到安全方针中。

文化特性的约束

在有些组织，工作习惯或主要业务会在组织内形成特定的、与安全控制措施可能不协调的“文化”。这种文化是人员的一般参考框架，可能由很多方面来确定，包括教育、指导、专业经验、工作之外的经验、观点、理念、信仰、社会地位等。

预算约束

有时，建议的安全措施的成本可能很好高。由此，基于安全的投资成本效益，并不总是合适的，通常还需要组织的财物部门从经济状况进行调整。

例如，在私营机构或公众部门，安全措施的总体成本应该不超过风险潜在后果的成本。 最高管理层如果想避免过度的安全成本，因此应该评估和计算风险。

A.3 适用于组织的法律法规的参考清单

应该识别适用于组织的法律法规。可能是针对组织所在领域的法律、政令等特定的法规或其他内外部法规。这也涉及合同、协议以及在更广泛的任何法律或规章性质的义务。

A.4 影响范围的约束清单

通过识别可能影响范围的约束清单，并确定哪些仍然需要采取行动。这些可能需要加到上面确定的组织约束，或者对组织约束进行修订。下面的章节提供这类约束的非详尽的可能类型的清单。

来自现有过程的约束

应用项目不一定是同时开发的。有些应用依赖于现有过程。虽然某个过程可以分解为子过程，但

该过程不一定受另外一个过程所有子过程的影响。

技术约束

与基础设施相关的技术约束，通常来自于已安装的硬件、软件以及过程的托管房间或地点。

- 文件（涉及组织、介质管理、访问规则的管理等要求）
- 一般架构（涉及拓扑（集中、分布、客户端-服务器端）、物理架构等要求）
- 应用软件（涉及特定软件设计、市场标准等要求）
- 软件包（涉及标准、评估等级、质量、规范的符合性、安全等）
- 硬件（涉及标准、质量、规范符合性等要求）
- 通讯网络（涉及覆盖范围、标准、容量、可靠性等要求）
- 建筑设施（涉及土木工程、建筑、高电压、低电压等要求）

财务约束

安全措施的实施常常受组织能够提供的预算的限制。

然而，仍应该最后考虑财务约束，因为安全的预算安排能够基于安全分析进行协商。

环境约束

环境约束来自过程所实施的地理和经济环境：国家、气候、自然风险、地理环境、经济气候等。

时间约束

应该考虑实施安全控制所需的时间，以及升级信息系统的能力。如果实施时间过长，则所设计的控制措施可能需要变更。时间是选择解决方案和确定优先级的决定性因素。

与办法相关的约束

需要实施与组织知识相符合的办法，如项目计划、规范、开发等。

组织性约束

不同的约束可能来自组织结构的要求：

- 运营（与交货时间、服务的提供、监管、监视、应急计划、降级运行等相关的要求）
- 维护（关于事件的排错、预防性活动、快速的纠正等要求）
- 人为失误的管理（关于操作人员、用户的培训， 如系统管理员、数据管理员等岗位的任职资格等要求）
- 行政管理（关于职责等要求）
- 开发管理（有关开发工具、计算机辅助软件工程、接受计划、将要设置的组织结构等要求）
- 外部关系的管理（有关第三方关系、合同等要求）

附录 B （资料性） 资产的识别和赋值以及影响评估

B.1 资产识别的例子

为进行资产赋值，组织首先需要识别资产（在合适的细节水平）。可以分为两类资产：

- 基本资产
  - 业务过程或活动
  - 信息
- 所有类型的支持性资产（基本资产所依赖的范围）
  - 硬件
  - 软件
  - 网络
  - 人员
  - 场所
  - 组织架构

B.1.1 基本资产的识别

为更精确的描述范围，该活动由识别基本资产构成（业务过程和活动、信息）。该识别活动由来自过程的代表构成混合工作组（管理人员、信息系统专家和用户）执行。

基本资产通常是范围内的活动的核心过程和信息。也应该考虑其他基本资产，如组织的过程，这将是更适合于制定信息安全方针或业务连续性计划。根据意图的不同，一些研究并不需要详尽分析范围内的所有要素。在这种情形，分析的边界可能只限于范围内的关键要素。

基本资产有两类：

1 – 业务过程（或子过程）和活动， 例如：

- 一旦丧失或降格将导致不能执行组织使命的过程
- 包括保密处理或专有技术的过程
- 如果被修改，可能极大影响组织使命的完成
- 组织满足合同、法律法规要求所需要的过程

2 – 信息

更一般性的，基本信息主要有：

- 组织使命和业务运行的关键信息
- 个人信息，特别是作为国家法律所定义的个人隐私
- 完成战略方向所确定目标的所需战略性信息
- 高成本信息，收集、存储、处理、传输需要很长时间和/或导致很高的采购成本

在该活动后，没有被识别为敏感的过程和信息，将在后续的研究中没有明确的分级。这意味着，即使该过程或信息被损害，组织仍然可以成功的完成其使命。

但他们常常会从识别为敏感的过程或信息中继承已实施的控制措施。

B.1.2 支持性资产的清单和描述

应该识别和描述范围内的支持性资产。这些资产具有被威胁利用来损害范围内的基本资产（过程和信息）的脆弱点。下面是支持性资产的不同类型：

硬件

硬件的类型包括用于支持过程的物理要素。

数据处理设备（主动）

自动的信息处理设备，包括独立运行所需项。

可移动设备

可移动的计算机设备。

例如，笔记本电脑、个人数字助理（PDA）。

固定设备

组织场所使用的计算机设备

例如：服务器、作为工作站的微型计算机

周边处理设备

通过通讯端口（串口、并口等）连接到计算机的设备，用于输入或传送数据。

例如，打印机、可拆除磁盘驱动器

数据介质（被动）

用于存储数据或功能的介质。

电子介质

可以连接到计算机或计算机网络，用于数据存储的信息介质。

尽管其尺寸紧凑，这些媒体可能包含了大量的数据。他们可以用于标准的计算机设备。

例如：软盘、光盘、备份磁带、可拆卸硬盘、内存棒、磁带

其他介质

包含数据的静态的、非电子介质。

例如：纸张、幻灯片、透明胶片、文件、传真。

软件

软件包含所有有助于数据处理的程序。

操作系统

操作系统包括构成计算操作基础的所有程序，在此之上可以运行所有其他程序（服务或应用）。它包括内核、基本功能或服务。根据架构的不同，操作系统可以是整体的，或者由一个微核和一组系统服务组成。操作系统的主要要素是所有设备的管理服务（CPU、内存、磁盘和网络接口）、任务或进程的管理服务、以及用户权限的管理服务。

服务、维护和管理软件

事实上，软件的特点是补充操作系统服务，而不是直接服务于用户或应用程序（即使它对于信息系统的整体运行，通常是非常重要的，甚至不可或缺）。

软件包或标准软件

标准软件或软件包是带有介质、版本和维护的完整商业化软件（而不是一次性的或特意开发的）。它们为客户或应用服务，但不是个性化的或按业务过程定制的。

例如：数据库管理软件、电子消息软件、群组软件、目录软件、web 服务器软件等。

业务应用

标准业务应用

一种商业软件，旨在让用户在其专业范畴内直接访问信息系统的服务和功能。标准业务应用的范围很广泛，理论上是无限的，可以是各个领域。

例如：财务软件、机床控制软件、客户管理软件、个人能力管理软件，行政管理软件，等等。

特定的业务应用

特定的业务应用软件中的各个方面（主要是支持、维护、升级等）已进行专门开发，让用户从信息系统中直接访问他们需要的服务和功能。标准业务应用的范围很广泛，理论上是无限的，可以是各个领域。

例如：电信运营商的客户发票管理、火箭发射的实时监控应用程序。

网络

网络类包括信息系统中多个计算机或组件之间物理远程互连的所有通讯设施。

介质和支持设施

通讯和通讯介质或设备的特性主要按设备的物理或技术（点对点，广播）特性以及通讯协议（连接或网络 OSI 7 层模型的第 2 和第 3 层）进行区分。

例如， 公众电话交换网（PSTN）、以太网、千兆以太网、非对称数字用户线路（ADSL）、无线协议规范（如， WiFi 802.11）、蓝牙、火线。

主动或被动中继

该小类包括（从 IS 视点看）所有非逻辑终端的中间或中继设备。中继按所支持的网络协议来区分。另外，对基本中继，通常包括路由和/或通过通讯交换机和路由器的过滤设施实现的过滤功能或服务。这些设备通常可以通过远程管理，并常常具有产生日志的能力。

例如：网桥、路由器、集线器、交换机、自动交换设备。

通讯接口

处理单元的通讯接口用于连接处理单元，但由介质和所支持的协议、所安装的过滤设施、日志或告警的产生功能、能力、远程管理的可能性和要求来区分。

例如，通用分组无线服务（GPRS），以太网接头。

人员

人员包括信息系统涉及的所有小组的人员。

决策者

决策者是基本资产（信息和过程）的所有者，并管理组织或特定项目。

例如，最高管理层、项目主管

用户

用户是在其活动范畴内处理敏感要素，并在这方面具有特定职责的人员。它们可能具有特定的信息系统访问权限以进行每天的任务。

例如：人力资源管理人员、财务管理人员、风险经理

运行/维护人员

负责信息系统运行和维护的人员。它们可能具有特定的信息系统访问权限以进行每天的任务。

例如：系统管理员、数据管理员、备份、服务台、应用部署操作人员、安全官。

开发人员

开发人员负责组织内应用的开发。 他们具有部分信息系统的高级权限，但不对生产数据作任何处理。

例如， 业务应用开发人员。

场所

场所包括包含范围或部分范围的所有地点，以及场所运作所需要的物理设施。

位置

外部环境

这涉及所有组织的安全方式不能适用的位置。

例如，个人家庭，另一组织的场所、场所外的环境（市区、危险区）。

房屋

该地点的范围是直接与外部接触的楼宇边界。

可能是通过建立物理栅栏或建筑物周围其它监视措施来进行物理保护的边界。

例如：宅院、大楼。

区域

区域是组织房屋内由物理保护界线内形成分区。它通过在信息处理基础设施周围建造物理边界而形成。

例如：办公室、限制进入区、安全区。

基本服务

组织设备运行所必需的所有服务。

通讯

由控制器提供的通讯服务和设备。

例如：电话线、PABX、内部电话网

工具

为信息技术设备和周边设施提供电力的服务或手段（资源或线路）。

例如：低电压电源、变压器、电路前端。

供水

垃圾处理

冷却或净化空气的服务和方式（设备、控制）

例如：冷却水管，空调。

组织

组织类描述组织性的框架，包括分配有职责的人员结构和控制这些结构的程序。

权力机构

这些组织是所研究组织的获得授权的来源。他们可能是法律上的分支机构或外部机构。这将在法规、决策和行动方面约束所研究的组织。

例如：行政机构、组织的总部

组织的结构

包含组织的不同分支，包括其管理控制下的跨职能活动。

例如：人力资源管理、IT 管理、采购管理、业务部门管理、大楼安保服务、消防服务、审计管理。

项目或系统的组织

这涉及组织设立特定的项目或服务。

例如：新应用开发项目、信息系统迁移项目。

分包方/供应商/生产商

这些组织向组织提供服务或资源，并通过合同进行界定。

例如：设备管理公司、外包公司、咨询公司。

B.2 资产赋值

资产识别后的下一个步骤是，就是商定将要使用的尺度以及对每一资产基于其价值分配其尺度值的准则。由于在多数组织内存在多种资产，某些资产具有已知的资金价值，可以通过本地货币赋值；另外一些资产可以通过价值范围进行定性赋值，如从“很低”到“很高”。依据组织的偏好确定使用定性尺度还是定量尺度，但都应该与需要赋值的资产相关。对于同一资产可以使用定性和定量两种形式。

用于资产定性赋值的典型术语包括，如：忽略不计、很低、低、中、高、很高、关键。适用于组织的术语的选择和范围，很大程度上依赖于组织对安全的要求、组织的规模以及组织的其他特定要素。

准则

应该用明确的术语，通过书面形式描述作为每一资产赋值基础的准则。资产赋值常常是很困难的，因为需要对某些资产进行客观的赋值，但不同的人员可能做出不同的判断。用于判断资产价值的可能准则包括，资产的原始价值、替代或重建的成本、资产的抽象价值，如组织声誉的价值。

资产赋值的另一基本要素是，由事件导致资产丧失保密性、完整性和可用性所带来的成本。如果适用、还应该考虑不可否认性、可审计性、真实性和可靠性。因此这样的赋值，在资产替代成本之外，在估算假定一系列信息安全事件情景导致的负面业务后果的基础上，为资产价值提供重要度量。必须强调的是，在该方法中，对后果的考虑是进行风险评估的必要要素。

某些资产在资产赋值过程中可能被赋予多个价值。如，业务计划可以通过基于开发计划的所花费的劳动力赋值，也可以基于输入数据的劳动力来赋值，还可以基于其对竞争对手的价值进行赋值。每一赋值可能有很大的不同。最终赋值可以是取所有赋值的最大值，也可以是所有可能的平均值。总之，应该谨慎确定资产最终的一个或多个赋值，因为最终赋值将决定保护资产所需花费的资源。

简化到共同基础

归根结底，所有的资产赋值必须简化到一个共同的基础。这可以借助随后的准则来完成。准则用于评估资产丧失保密性、完整性、可用性、不可否认性、可审计性、真实性或可靠性所带来的可能后果，可以是：

- 法律法规的违背
- 对业务绩效的影响
- 好形象的丧失/声誉的负面影响
- 与个人信息相关的违背
- 危机个人人身安全
- 对法律实施的负面影响
- 保密性的违背
- 对公共秩序的违背
- 财务损失

- 业务活动的中断
- 危及环境安全

另外一个评估后果的方法是：

- 服务中断
  - 不能提供服务
- 客户丧失信心
  - 内部信息系统丧失可信性
  - 信誉的损害
- 内部运营的中断
  - 对组织自身的中断
  - 导致内部成本的增加
- 第三方运营的中断
  - 第三方与组织交易的终端
  - 各种类型的损害
- 法律法规的违反
  - 不能完成法律义务
- 违背合同
  - 不能完成合同义务
- 危及个人或用户安全
  - 伤害组织员工和/或用户
- 妨碍用户个人生活
- 财务损失
- 应急或修复的成本
  - 对个人的
  - 对设备的
  - 对研究和专家报告的
- 物品/资金/资产的损失

- 丧失客户和供应商
- 引起诉讼和惩罚
- 丧失竞争优势
- 丧失技术上的领先
- 效率或信任的丧失
- 丧失技术上的信誉
- 降低谈判能力
- 行业危机（罢工）
- 政府危机
- 解雇
- 材料损毁

这些准则是资产赋值所考虑的议题示例。为进行资产赋值，组织需要选择与其业务类型和安全要求相关的准则。这意味着，以上所列的某些准则可能是不适用的，需要将其他的准则加到清单中。

尺度

在建立准则后需要考虑的是，组织应该就在组织范围内所使用的尺度达成一致。第一步要确定所要使用的尺度等级的数量。没有任何关于尺度等级数量的最佳规则。等级数量越多，提供的更小的尺度粒度，但有时过细的区分给在整个组织内赋值的一致性带来困难。一般，只要其与组织用来整个风险评估过程的方法相一致，可以利用 3（例如，低、中、高）到 10 之间的任何尺度等级数量。

组织可以定义自己的资产赋值限制规则，如“低”、“中”、“高”。应该按照所选择的准则（如可能的财务损失，它们应该赋予货币价值；但对考虑如人身安全的危害，货币赋值可能很复杂而且可能不适用于所有组织）评估这些限制规则。总之，什么应该被考虑为“低”或“高”，完全由组织确定。某个后果对小型组织可能是灾难性的，但对特大型组织可能是很低的，甚至是可以忽略的。

依赖关系

某个资产所支持的或相关的业务过程越多，则该资产的价值越高。应该识别资产与业务过程以及其他资产的依赖性，因为这可能影响资产的价值。例如，数据的保密性应该在数据的整个生命周期的所有阶段得到保持，包括存储和处理，如数据存储和处理程序的安全要求应该直接与被存储和处理的数据的保密价值相关。同样，如果某个业务过程依赖于程序所产生的特定数据的完整性，则该程序的输入数据应该具有合适的可靠性。此外，信息的完整性依赖于存储和处理信息的硬件和软件。同样，硬件依赖于电源，可能还依赖于空调。因此，信息的关联性将有助于识别威胁和特定脆弱点。另外，也有助于确保资产赋值的真实性，由此指明合适的保护等级。

资产的其他资产依赖性价值，可能因以下原因而进行修订：

- 如果依赖性资产（如数据）的价值低于或等于所考虑的资产的价值，则资产的价值不变
- 如果依赖性资产（如数据）的价值更高，则应该按以下几点增加所考虑的资产的价值：
  - 依赖性程度
  - 其他资产的价值

组织的某些资产可能存在于多处，如软件程序的多个拷贝或很多办公室内使用的统一类型的计算机。在进行资产赋值时应该考虑这一因素。一方面，这些资产很容易被忽略，因此应该注意识别所有这些资产；另一方面，这些资产可以用于降低可用性问题。

输出

本步骤的最终输出是资产清单及其与泄密（保密性保护）、篡改（完整性、真实性、不可能否认性和可审计性的保护）、不可用和损坏（可用性和可靠性防护）相关的价值，以及替代成本。

B.3 影响评估

某个信息安全事件可能影响多个资产或是只是单个资产的一部分。影响与事件作用的程度相关。因资产价值的不同，事件所导致的后果也会有很大的不同。可能存在对资产的即时（运行）影响或后期（业务）的影响，包括财务或市场上的后果。

即时（运行）影响可能是直接的或间接的。

直接的：

a) 资产（或部分资产）所丧失价值的替代成本
b) 新的或备份资产的采购、配置、安装成本
c) 事件导致运营暂停，直至资产所提供的服务得到恢复的成本
d) 违背信息安全的影响

间接：

a) 机会成本（替代或修复需要使用的资产的财务资源）
b) 运营中断的成本
c) 违背信息安全获得的信息的潜在误用
d) 法律法规义务的违背
e) 违背道德行为准则

依此，首次评估（没有任何形式的控制措施）中的影响估算将与相关资产（或资产组合）的价值非常接近。随后对该资产的任何评估循环，影响将不同于（通常是低于）价值，因为实施了有效的控制措施。

附录 C （资料性） 典型威胁示例

下表给出典型威胁的示例。下表的威胁清单可以用于威胁评估过程。威胁可能是故意的、意外的或环境的（自然的），例如损害或丧失基本服务。下表的清单表明每一类威胁（D 故意的，A 意外的，E 环境的）是相互关联的。D 是指所有针对信息资产的故意行为，A 是指所有可能导致信息资产意外受损的人为活动，E 是指非人为的所有意外事件。每类威胁的排序不分优先级。

类型	威胁	来源
物理损坏	火灾	A, D, E
	水灾	A, D, E
	污染	A, D, E

类型	威胁	来源
	重大事故	A, D, E
	设备或介质损坏	A, D, E
	灰尘、腐蚀、严寒	A, D, E
自然灾难	气候现象	E
	地震现象	E
	火山现象	E
	气象现象	E
	洪水	E
基础服务失效	空调或供水系统失效	A,D
	电源失效	A,D,E
	通讯设备故障	A,D
辐射干扰	电磁辐射	A,D,E
	热辐射	A,D,E
	电子脉冲	A,D,E
信息的损害	截取损害干扰信号	D
	远程间谍	D
	偷听	D
	偷取介质或文件	D
	偷取设备	D
	获取循环利用或废弃的介质	D
	泄密	A,D
	来自非信任源的数据	A,D
	损坏硬件	D
	损坏软件	A,D
	位置检测	D
技术故障	设备失效	A

类型	威胁	来源
	设备故障	A
	饱和的信息系统	A,D
	软件故障	A
	信息可维护性的违背	A,D
未经授权的活动	设备的未经授权的使用	D
	非法的软件拷贝	D
	使用盗版软件	A, D
	破坏数据	D
	非法处理数据	D
功能受损	误用	A
	滥用权限	A,D
	盗用权限	D
	拒绝服务	D
	个人可用性的违背	A,D,E

应该特别关注来自人为的威胁。下表是具体的清单：

威胁来源	动机	可能后果
黑客	挑战 自负 逆反 身份 金钱	• 黑客攻击 • 社会工程 • 系统入侵 • 未经授权的系统访问
计算机犯罪	毁坏信息 非法信息泄密 获取经济利益 非法修改数据	• 计算机犯罪（如网上跟踪） • 欺诈行为（如回放、伪装、窃听） • 信息贿赂 • 欺骗 • 系统入侵

威胁来源	动机	可能后果
恐怖活动	邮件勒索 破坏 擅自利用 报复 政治获益 媒体报道	• 爆炸/其它恐怖手段 • 信息战 • 系统攻击（如拒绝服务） • 系统渗透 • 系统篡改
行业间谍（情报公司、外国政府、其他政府利益）	竞争优势 经济间谍活动	• 国防优势 • 政治优势 • 经济宣传 • 窃取信息 • 个人隐私入侵 • 社会工程 • 系统渗透 • 未经授权的系统访问（访问保密的、私有的和/或 技术相关信息）
内部人员（缺乏培训、泄愤、恶意、疏忽、诚实或被解雇的员工	好奇 自负 情报 经济利益 报复 无意的行为和疏忽（数据出入错误、编程错误）	• 攻击员工 • 敲诈勒索 • 浏览专有信息 • 计算机滥用 • 欺骗和窃取 • 信息贿赂 • 输入伪造或错误数据 • 窃听 • 恶意代码（如病毒、逻辑炸弹、木马） • 销售个人信息 • 系统漏洞

威胁来源	动机	可能后果
		• 系统入侵 • 系统破坏 • 未经授权的系统访问

附录 D （资料性）脆弱点和脆弱性评估方法

D.1 脆弱点示例

下表给出不同安全领域的脆弱点示例，包括可能利用这些脆弱点的威胁示例。这些示例清单可以帮助威胁和脆弱点的评估，以确定相关的事件情形。需要强调的是，在某些情形，其他的威胁也可能利用这些脆弱点。

类型	脆弱性示例	威胁示例
硬件	维护不善/存储介质的错误维护	违背信息系统的可维护性
	缺乏定期更换计划	设备或介质地损坏
	受潮湿、灰尘、污染的影响	灰尘、腐蚀、严寒
	对电磁辐射的敏感	电磁辐射
	缺乏有效的变更控制	错误的使用
	受电压波动的影响	电力供应不善
	受温度变化影响	气象现象
	缺乏防护的存储	窃取介质或文件
	对废弃处置缺乏关注	窃取介质或文件
	不受控的拷贝	窃取介质或文件
	没有或不受控	权限的滥用
软件	众所周知的软件缺陷	权限的滥用
	离开时，没有登出终端	权限的滥用
	存储介质的处置和再利用前没有正	权限的滥用

类型	脆弱性示例	威胁示例
	缺乏发送者和接受者的认证	伪装
	不安全的网络架构	远程间谍
	明文传输密码	远程间谍
	错误的网络管理（路由的健壮性）	信息系统的渗透
	不受保护的公共网络连接	未经授权的设备使用
人员	人员缺乏	人员可用性的违背
	不合适的招聘程序	设备或介质的损坏
	缺乏安全培训	误用
	软、硬件的不正确使用	误用
	缺乏安全意识	误用
	缺乏监视机制	非法处理数据
	缺乏对由外部或清洁工完成的工作的监督	非法处理数据
	缺乏正确使用电子媒介和电子消息的方针	未经授权的设备使用
场所	建筑物或房间的不合适或随意的物理访问控制	设备或介质的损坏
	位于易受洪水影响的区域	洪水
	不稳定的电网	缺乏电力供应
	缺乏建筑物、门、窗的物理防护	窃取设备
组织	缺乏正式的用户注册和注销程序	伪装
	缺乏访问权限评审过程（监督）	伪装
	与客户和/或第三方直接的合同中缺乏（关于安全）的条款，或不充分	权限的不正当使用
	缺乏监视信息处理设施的程序	权限的不正当使用

类型	脆弱性示例	威胁示例
	缺乏定期审计（监督）	权限的不正当使用
	缺乏风险识别和评估	权限的不正当使用
	缺乏管理员和操作员日志中记录的错误报告	权限的不正当使用
	不充分的服务维护响应	违背信息系统可管理性
	缺乏服务等级协议或不充分	违背信息系统可管理性
	缺乏变更控制	违背信息系统可管理性
	缺乏 ISMS 文件控制程序	数据损坏
	缺乏 ISMS 纪录控制程序（监督）	数据损坏
	缺乏公众可用信息的认可过程	来自非信任源的数据
	缺乏合适的信息安全职责分配	拒绝行动
	缺乏连续性计划	设备失效
	缺乏 e-mail 使用方针	误用
	缺乏向操作系统导入软件的程序	误用
	缺乏管理员和操作员日志记录	误用
	缺乏保密信息处理程序	误用
	在工作说明书中缺乏安全职责	误用
	与员工合同中缺乏（关于信息安全）条款或不足	非法处理数据
	缺乏一旦发生信息安全事件时的记录处理过程	窃取设备
	缺乏正式的移动计算机的方针	窃取设备
	缺乏组织场所外设备的控制	窃取设备
	缺乏“清空桌面和屏幕”方针	窃取介质或文件
	缺乏信息处理设施的授权	窃取介质或文件
	缺乏确定的信息安全违背监视机制	窃取介质或文件

类型	脆弱性示例	威胁示例
	缺乏定期评审	未经授权的使用设备
	缺乏报告信息安全弱点的程序	未经授权的使用设备
	缺乏保证知识产权复合型的程序	使用盗版软件

D.2 评估技术性脆弱点的方法

可以根据信息和通讯（ICT）系统的重要程度和可用资源（如分配的资金、可以使用的技术、进行测试的专业人员），采用前摄性的方法识别脆弱点，如信息系统测试。测试办法包括：

- 漏洞自动扫描工具
- 安全测试和评估
- 渗透测试
- 代码评审

漏洞自动扫描工具用于针对已知的脆弱服务，扫描一组主机或网络（如系统允许匿名的文件传输协议(FTP)，邮件转发）。然而，应该注意，自动识别的某些潜在脆弱点在系统环境范畴内可能并不是真正的脆弱点。例如，某些扫描工具在对潜在脆弱点进行分级时，并不考虑场所环境和要求。自动扫描软件标识的某些脆弱点对于特定场所可能并不是脆弱点，而且因环境要求必须如此配置。因此，测试方法可能报告虚假脆弱点。

安全测试和评估（STE）是在风险评估过程中识别 ICT 系统脆弱点的另外一个方法。它包括开发和执行一个测试计划（如，测试脚本、测试过程和预期的测试结果）。系统安全测试的目的是测试已经应用到某个运行环境中的 ICT 系统的安全控制措施的有效性。目标是保证应用的控制措施满足已认可的软、硬件安全规范，满足组织的安全方针或行业标准。

渗透测试可以用作安全控制措施评审的补充，以保证 ICT 系统的不同方面都是安全的。如果在风险评估过程中使用渗透测试，则可用于评估一个信息和通信技术系统的防止企图绕过系统安全措施的能力。其目的是从威胁源的视点来测试 ICT 系统，以识别 ICT 系统保护方案的潜在失效点。

代码评审是最为彻底（也可能是最为昂贵）的漏洞评估方式。

这些安全测试的结果将有助于识别系统的脆弱点。

特别需要注意的是，渗透的工具和技术可能提供虚假的结果，除非脆弱点被成功利用。为利用特定的脆弱点，需要知道被测试系统的系统、应用、补丁的准确设置。如果在进行测试时，不知道这些数据，可能难以成功利用特定的脆弱点（例如，获取远程逆转界面）；然而，还是可能导致崩溃或重新启动进程和系统。在这种情形，应该认为被测试对象是存在脆弱点的。

办法可能包括以下活动：

- 人员和用户访谈
- 调查问卷
- 物理检查
- 分析文件

附录 E （资料性）信息安全风险评估方法

E.1 纲领性信息安全风险评估

纲领性评估定义活动的优先级和时间表。由于多种原因，如预算，可能不会同时实施所有安全措施，并且只有对重大风险按风险处置过程进行处理。另外，如果控制措施设想在一两年后实施，则进行详细风险管理可能太早。为达到上述目标，纲领性的评估可以从对后果的纲领性评估着手，而不是开始进行威胁、脆弱点、资产和后果的系统性分析。

从纲领性评估开始的另外一个原因，是协调其他与变更管理（或业务连续性）相关的计划。例如，如果计划在将来进行外包，则不可能对系统和应用进行全面的安全防护，即使进行风险评估对定义外包合同是有帮助的。

纲领性风险评估循环的特征可能包括：

- 纲领性风险评估可能从组织的全局和信息系统的视点出发，将技术层面和业务问题独立考虑。

通过这些，范畴分析更集中于业务和运行环境而不是技术要素。

- 纲领性风险分析可能只处理更为有限清单中的威胁和已定义域中脆弱点，为加速这一过程，可能关注在风险或攻击的情景而不是其要素。
- 纲领性风险评估中表述的风险常常是较为广泛性的风险域而不是特定的已识别风险。由于情景或威胁被分成域，因此风险处置针对这些域来建议控制措施清单。风险处置活动首先尝试建议和选择对整个系统有效的通用控制措施。
- 然而，纲领性风险评估，由于很少处理技术细节，更合适于提供组织性的、非技术的控制措施，以及管理方面的技术控制措施，或者关键并通用的技术安全措施，如备份和防病毒。

纲领性风险评估的优点如下：

- 最初的简单方法的组合是最可能被接受的风险评估方案。
- 可能建立组织信息安全方案的策略愿景，例如，它将有助于良好的规划。
- 资源和资金能够用到收益最大的地方，而且系统可能最需要防护的地方最先得到处理。

由于最初的风险分析是纲领性的，而且可能缺乏准确性，唯一可能的弱点是某些业务过程或系统没有被识别需要进行进一步的详细的风险评估。这可以通过获得组织、组织的信息和信息系统所有方面的准确信息来避免，包括从信息安全事件评估中获得的信息。

纲领性风险评估考虑资产的业务价值，以及从组织业务视点的看待风险。在第一决策点（参见图1）， 有几个因素有助于判断纲领性评估对处理风险是否充分，这些要素可以包括：

- 通过利用不同信息资产，以达到的业务目标
- 组织业务对某一信息资产的依赖程度，如， 组织认为对生存和有效经营业务的关键功能是否依赖于某一信息资产， 或该资产所保存和处理的信息的保密性、完整性、可用性、不可否认性、可问责性、真实性和可靠性；
- 以开发、维护或替代资产的形式对某一资产的投资水平，
- 组织直接赋值的信息资产。

当这些因素得到评估时，决策就变得更容易。如果资产的目标对组织运营业务极端重要，或资产处于高风险中，则应该进行对特定的信息资产（或资产的一部分）进行第二循环、更详细的风险

评估。

一个通用的规则是：如果缺乏信息安全防护可能对组织、组织的业务过程或资产带来重大的负面后果，则进行风险评估的第二循环，以在更详细的级别上识别潜在风险。

E.2 详细的信息安全风险评估

详细的信息安全风险评估过程涉及更深层次的资产识别和赋值、资产所面临威胁的评估和脆弱点的评估。这些活动的结果将被用于评估风险和识别风险处置措施。

详细的步骤通常需要大量的时间、精力和专业知识，因此可能适合于高风险的信息系统。

详细信息风险评估的最后阶段是评估整体风险， 这也是本附录的关注点。

可以使用多种方式评估后果，包括使用定量（如货币）和定性（基于所使用的形容词，如中度、重度）的测量方式，或者两种方式的组合。为评估威胁发生的可能性，应该建立资产价值和保护需求的时间框架。特定威胁发生的可能性受以下因素影响：

- 资产的吸引力或可能的后果，在考虑人为故意的威胁时适用
- 利用资产的脆弱点转化成资金回报的容易程度，在考虑人为故意的威胁时适用
- 威胁的技术能力，适用于人为故意的威胁，以及
- 脆弱点的利用便利程度，适用于技术和非技术脆弱点

很多办法利用表格，并结合主观和经验值。组织使用适合于自身的办法是很重要的，使得组织充满自信，以形成可重复的结果。下面是几个基于表格办法的示例。

E.2.1 示例 1：预定值矩阵

在本类型的风险评估方法中，实际的或建议的物理资产按替代或重建的成本赋值（如定量测量方式）。这些成本转换到对应的参考定性尺度（参见下文）。实际的或建立的软件资产如同物理资产一样，按替代或重建的成本赋值，并转换到对应的参考定性尺度。另外，如果任何应用软件本身有自己的安全性或完整性方面的要求（如源代码自身的商业敏感性），也按照相同的参考方式

赋值。

信息的价值通过对选定的拥有对数据的权威话语权的业务管理人员（“数据所有者”）进行访谈的方式获得，以确定数据在实际使用、存储、处理和访问中的价值和敏感性。访谈有助于，在相当大的程度预期可能发生的，由未经授权的泄密、修改、不同时间段的不可用或损坏导致的负面业务后果的最糟糕的情形下，信息价值和敏感性的评估。

赋值通过利用资产赋值指南来完成，并覆盖以下问题：

- 人身安全
- 个人信息
- 法律法规义务
- 法律的实施
- 商务和经济利益
- 财务损失/活动中断
- 公共秩序
- 业务方针和运行
- 声誉的丧失
- 与客户的合同或协议

指南有助于定义数字尺度值，如示例矩阵中的 0~4，这是使得能够在可行时给威胁在合乎逻辑条件下的分配级别值，以及在不能进行定量时给出定性值，如危及人员生命。

下一个主要活动是完成针对每一类型威胁、以及每一类型威胁相关的每一组资产的调查问卷，以便评估威胁的级别（发生的可能性）和脆弱性的等级（被威胁利用以形成造成不良后果的容易程度）。每一问题的回答对应一个分值。这些分值通过知识库和大范围的比较来累积。这将识别威胁的高低等级尺度，对于脆弱性也是同样的，如下面示例矩阵表所示，按相关性区分不同类型的后果。应该通过对合适的技术、人员、住所和物理位置的检查，以及对文件的评审来获得完成问卷的信息。

资产的价值、威胁和脆弱性的等级、相关的每一类型的后果，在下表的矩阵中进行匹配，以识别

每一组合的相关风险在0~8之间的风险等级尺度。相关数值以结构化的方式填入矩阵。示例如下：

表 E.1 a)

	威胁发生的可能性	低 (L)			中 (M)			高 (H)		
	脆弱性被利用的容易程度	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

对于每一资产，其相关的脆弱性及对应的威胁都得到了考虑。如果一个脆弱点没有对应的威胁，或者威胁没有对应的脆弱点，则表示没有风险（不过应该考虑状况发生变更的情形）。矩阵中由资产价值确定合适的行，威胁发生的可能性和脆弱性被利用的容易程度则确定合适的列。例如，如果资产价值是 3，威胁时高“H”，脆弱性是低“L”，则风险测量值是 5。 假定资产对于被修改的价值是 2， 威胁等级是低“L”，脆弱性是高“H”，则风险测量值是 4。矩阵表的大小可以根据组织的需要进行调整，并通过威胁可能性的分类数量、脆弱性被利用的容易程度的分类数量、资产价值的分类数量来确定的。附加的行或列将使得附加的风险评估成为必要。该方法的值即为需要进行处理的风险的排序。

表 E.1 b) 所示的简单矩阵是从考虑某个事件情景的可能性对照估算的业务影响所得出的结果。威胁利用脆弱点的确定可能性来给出事件的可能性。下表将与事件情景相关的可能性与业务影响相对照。得出的风险按 0~8 进行分级，以对照风险接受准则进行评价。这种风险分级也可以映射到一个简单的整体风险评级，例如：

低风险：0-2

中风险：3-5

高风险：6-8

	事件情景的可能性	很低（很不可能）	低（不太可能）	中（可能）	高（很可能）	很高（频繁）
业务影响	很低	0	1	2	3	4
	低	1	2	3	4	5
	中	2	3	4	5	6
	高	3	4	5	6	7
	很高	4	5	6	7	8

E.2.2 示例 2：通过风险值进行威胁评级

如表 E.2 所示的矩阵或表格，可以用于关联后果要素（资产价值）和威胁发生的可能性（同时考虑脆弱性方面）。第一步是按预定义的尺度评估后果（资产价值），例如用从 1 到 5 来定义被威胁的资产（表中的 b 列）。第二步是按预定义的尺度评估威胁发生的可能性，例如用从 1 到 5 来定义每一威胁（表中的 c 列）。第三步是通过乘法（b x c）计算风险值。最后，将威胁按照相关的风险值进行评级。注，在本示例中，1 表示最低的后果和最低的发生可能性。

表 E.2

威胁编号 (a)	后果（资产）值 (b)	威胁发生可能性 (c)	风险值 (d)	威胁评级
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

如上表所示，该程序将具有不同后果和不同可能性的不同威胁进行比较并进行评级排序。在某些情况下，货币计量方式需要使用如这里所用的经验值来协助。

E.2.3 示例 3：为风险的可能性和可能的后果赋值

在本示例中，重点放在信息安全事件（如事件情景）的后果以及确定系统的优先排序上。这可以通过为每一资产和风险分配两个值来实现，这两个值的组合可以确定每一资产的分值。将系统的所有资产的分值合计，则得到系统的风险值。

首先，为每一资产赋值。该赋值与资产被威胁时可能导致的负面后果相关。根据资产适用的每一威胁，对资产进行赋值。

其次是可能性评估。该评估组合威胁的可能性和脆弱性被利用的容易程度，参见表 E.3 所表示的事件情景的可能性。

表 E.3

威胁可能性	低			中			高		
脆弱性等级	L	M	H	L	M	H	L	M	H
事件情景的可能性值	0	1	2	1	2	3	2	3	4

再次，通过寻找表 E.4 中资产值和可能性的交叉点，给资产/威胁分配分值。资产/威胁分值共同形成资产的汇总分值。该方式可以用于区别系统中的不同资产。

表 E.4

资产价值	0	1	2	3	4
可能性值					
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

最后一步是汇总系统中所有资产的分值，以形成系统分值。这可以用于区分不同系统，并确定系统保护的优先级。

下面的示例的有数值都是随机选取的。

假定系统 S 有三个资产 A1、 A2、A3，并假定有两个威胁 T1、T2 适用于系统 S。设定 A1 值为 3、A2 为 2、A3 为 4。

如果对 A1 和 T1，威胁的可能性为低，脆弱性被利用的容易程度为中，则可能性值为 1（参见表 E.3）。

资产/威胁的等级值 A1/T1 可以从表 4 中，资产值 3 和可能性值 1 的交叉点找到，为 4。同样，对于 A1/T2 设定可能性为中，脆弱性被利用的容易程度为高，则得到 A1/T2 值为 6。

现在，可以计算资产的汇总值 A1T，为 10。资产的汇总值通过计算每一资产和对应威胁得到。系统的汇总值 ST 可以通过 A1T + A2T + A3T 得到。

至此，可以将不同的系统进行比较以确定优先级，对于同一系统内的不同资产也是同样的。

上面的示例是信息系统的形式，然而类似的方法也适用于业务过程。

附录 F （资料性）降低风险的约束

在考虑降低风险的约束时，应该考虑以下约束：

时间约束：

可能存在多种形式的时间约束。例如，控制措施应该在组织管理层可以接受的时间内实施。另一种时间约束是，控制措施是否能够在信息或系统的生命周期内得以实施。第三种时间约束是，在组织管理层决定可以接受的时间段被暴露给特定的风险。

财务约束：

所设置的控制措施的实施和维护不应该比风险价值更昂贵，除非有强制性的符合性要求（如法律

要求）。每一行动都不应该超出预算并通过利用控制措施来达成财务优势。然而，在某些情况下，由于预算的限制，不太可能达到期望的安全和风险接受水平。因此，这一情形的解决将成为企业管理者的决策问题。

如果预算导致将要实施的控制数量的减少或质量的降低，应该予以特别注意，因为这可能导致比计划隐含更大的风险。控制措施的既定预算应该只作为需要重点关注的一个限制因素。

技术约束：

技术问题，如程序或硬件的兼容性，如果在选择控制措施时，予以考虑，则很容易避免。另外， 对现有过程或系统追加实施控制措施常常受技术约束妨碍。这些困难可能导致控制措施的平衡倒向程序和物理安全方面。可能需要修订信息安全计划以满足安全目标。这可能发生在不降低生产效力，控制措施将不能达到降低风险的预期结果时。

运行约束：

运行约束，如需要 7x24 小时运行，但需要进行备份，可能导致复杂而昂贵的控制措施，除非从一开始就内置在设计中。

文化约束：

选择控制措施的文化约束可能针对国家、领域、组织、甚至组织的一个部门。不是所有的控制适用于所有的国家。例如，对包裹的搜查可以在部分欧洲国家实施，但不能在中东的一些地方实施。不能忽略文化方面的约束，因为很多控制措施有赖于员工的主动支持。如果员工不理解控制措施的必要性，或发现与文化不相容，则控制措施随着时间的推移而变得无效。

道德约束：

道德约束可能对控制措施有重大影响，因为道德基于社会规范而变化。这可能在一些国家阻止实施某些控制措施，如 email 扫描。隐私信息也随区域的道德观念或政府而可能发生变化。在某些行业比其他行业可能更需要关注，如政府和医疗卫生。

环境约束：

环境约束可能影响控制措施的选择，如可用空间、极端气候条件、周边的自然和城市地形。例如在一些国家需要进行地震试验，而另一些国家则不需要。

法律约束：

法律因素，如个人数据保护或信息处理的犯罪条款可能影响控制措施的选择。法律法规的符合性可能强制要求某些特定形式的控制措施，包括数据保护和财务审计；这些可能妨碍其他控制措施的使用， 如加密。另外，一些法律法规，如劳动相关的法律、消防部门、健康和安全、以及经济方面的法规等，也同样有可能影响控制措施的选择。

易用性：

一个糟糕的人机界面将导致人为错误，并导致控制措施无效。应该选择提供最佳易用性的控制措施，以将对业务的风险降低到可接受级别。难以使用的控制措施，将影响其效力，因为用户可能尝试绕过或尽可能忽略这些控制措施。组织内复杂的访问控制，可能促使用户寻找 k 一个替代的、未经授权的访问方式。

人员约束：

应该考虑实施控制措施的专业技术的可用性和工作成本，以及在不利的操作条件下调动员工之间位置的可能性。

实施计划中控制措施的专业技术可能不容易获得，或对组织来说太过昂贵。其他方面，如一些员工有歧视其他员工的倾向，而没有进行安全筛选，可能会对安全方针和实践有重大影响。同时，可以在进行安全筛选后雇佣，以为工作雇佣和寻找合适的人员。在雇佣前完成安全要求的筛选是正常、安全和实用的。

整合新的和已有控制措施的约束：

在现有基础设施中整合新的控制措施以及控制措施之间的相互依赖关系，常常被忽视。如果新建

控制措施与现有控制措施不协调或不兼容，将很难实施。例如，在物理访问控制中采用生物特征令牌可能与现有的基于密码键盘的访问控制系统相冲突。从现有控制措施变更到计划的控制措施的成本应该计算到风险处置的总体成本中。可能因妨碍现有的控制措施，而无法事实一个选定的控制措施。

参考书目

[1] ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards

[2] ISO/IEC 16085:2006, Systems and software engineering — Life cycle processes — Risk management

[3] AS/NZS 4360:2004, Risk Management

[4] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

[5] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology