ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31722—2015/ISO/IEC 27005:2008

信息技术　安全技术
信息安全风险管理

Information technology—Security techniques—Information security risk management

(ISO/IEC 27005:2008,IDT)

2015-06-02 发布　　2016-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准使用翻译法等同采用 ISO/IEC 27005:2008《信息技术　安全技术　信息安全风险管理》(英文版)。

本标准做了以下修改：

——对引言做了一些编辑性修改。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：中国电子技术标准化研究院、上海三零卫士信息安全有限公司、中电长城网际系统应用有限公司、山东省计算中心、北京信息安全测评中心。

本标准主要起草人：许玉娜、闵京华、上官晓丽、董火民、赵章界、李刚、周鸣乐。

引　言

信息安全管理体系标准族(Information Security Management System,简称 ISMS 标准族)是国际信息安全技术标准化组织(ISO/IEC JTC1 SC27)制定的信息安全管理体系系列国际标准。ISMS 标准族旨在帮助各种类型和规模的组织,开发和实施管理其信息资产安全的框架,并为保护组织信息(诸如,财务信息、知识产权、员工详细资料,或者受客户或第三方委托的信息)的 ISMS 的独立评估做准备。ISMS 标准族包括的标准:a)定义了 ISMS 的要求及其认证机构的要求;b)提供了对整个"规划-实施-检查-处置"(PDCA)过程和要求的直接支持、详细指南和(或)解释;c)阐述了特定行业的 ISMS 指南;d)阐述了 ISMS 的一致性评估。

目前,ISMS 标准族由下列标准组成:

——GB/T 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009)

——GB/T 22080—2008　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2005)

——GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则(ISO/IEC 27002:2005)

——GB/T 31496—2015　信息技术　安全技术　信息安全管理体系实施指南(ISO/IEC 27003:2010)

——GB/T 31497—2015　信息技术　安全技术　信息安全管理　测量(ISO/IEC 27004:2009)

——GB/T 31722—2015　信息技术　安全技术　信息安全风险管理(ISO/IEC 27005:2008)

——GB/T 25067—2010　信息技术　安全技术　信息安全管理体系审核认证机构的要求(ISO/IEC 27006:2007)

——ISO/IEC 27007:2011　信息技术　安全技术　信息安全管理体系审核指南

——ISO/IEC TR 27008:2011　信息技术　安全技术　信息安全控制措施审核员指南

——ISO/IEC 27010:2012　信息技术　安全技术　行业间及组织间通信的信息安全管理

——ISO/IEC 27011:2008　信息技术　安全技术　基于 ISO/IEC 27002 的电信行业组织的信息安全管理指南

——ISO/IEC 27013:2012　信息技术　安全技术　ISO/IEC 27001 和 ISO/IEC 20000-1 集成实施指南

——ISO/IEC 27014:2013　信息技术　安全技术　信息安全治理

——ISO/IEC TR 27015:2012　信息技术　安全技术　金融服务信息安全管理指南

本标准作为 ISMS 标准族之一,为组织内的信息安全风险管理提供指南,特别是支持按照 GB/T 22080 的 ISMS 要求。然而,本标准不提供信息安全风险管理的任何特定方法。由组织来确定其风险管理方法,这取决于诸如组织的 ISMS 范围、风险管理语境或所处行业。一些现有的方法可在本标准描述的框架下使用,以实现 ISMS 的要求。

本标准的相关方包括关心组织内信息安全风险的管理者和员工以及(在适当情况下)支持这种活动的外部方。

信息技术　安全技术
信息安全风险管理

1　范围

本标准为信息安全风险管理提供指南。

本标准支持 GB/T 22080 所规约的一般概念，旨在为基于风险管理方法来符合要求地实现信息安全提供帮助。

知晓 GB/T 22080 和 GB/T 22081 中所描述的概念、模型、过程和术语，对于完整地理解本标准是重要的。

本标准适用于各种类型的组织（例如，商务企业、政府机构、非盈利性组织），这些组织期望管理可能危及其信息安全的风险。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22080—2008　信息技术　安全技术　信息安全管理体系　要求（ISO/IEC 27001:2005，IDT）

GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则（ISO/IEC 27002:2005，IDT）

3　术语和定义

GB/T 22080—2008 和 GB/T 22081—2008 中界定的以及下列术语和定义适用于本文件。

3.1

影响　impact

对所达到业务目标的不利改变。

3.2

信息安全风险　information security risk

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

注：它以事态的可能性及其后果的组合来度量。

3.3

风险规避　risk avoidance

不卷入风险处境的决定或撤离风险处境的行动。

[ISO/IEC Guide 73:2002]

3.4

风险沟通　risk communication

决策者和其他利益相关者之间关于风险的信息交换或共享。

[ISO/IEC Guide 73:2002]

3.5

风险估算　risk estimation

为风险的可能性和后果赋值的活动。

[ISO/IEC Guide 73:2002]

3.6

风险识别　risk identification

发现和列出风险要素并描述其特征的活动。

[ISO/IEC Guide 73:2002]

3.7

风险降低　risk reduction

为降低风险的可能性和(或)负面结果所采取的行动。

[ISO/IEC Guide 73:2002]

3.8

风险保留　risk retention

对来自特定风险的损失或收益的接受。

[ISO/IEC Guide 73:2002]

注：在信息安全风险的语境下，对于风险保留仅考虑负面后果(损失)。

3.9

风险转移　risk transfer

与另一方对风险带来的损失或收益的共享。

[ISO/IEC Guide 73:2002]

注：在信息安全风险的语境下，对于风险转移仅考虑负面结果(损失)。

4　本标准结构

本标准描述了信息安全风险管理过程及其活动。

第5章提供了背景信息。

第6章给出了信息安全风险管理过程的总体概述。

第6章提出的所有信息安全风险管理活动在以下各章中依次进行了描述：

- 第7章 语境建立；
- 第8章 风险评估；
- 第9章 风险处置；
- 第10章 风险接受；
- 第11章 风险沟通；
- 第12章 风险监视与评审。

附录中给出了信息安全风险管理活动的其他信息。附录A(确定信息安全风险管理过程的范围和边界)对语境建立提供支持。附录B(资产示例)、附录C(典型威胁示例)和附录D(典型脆弱性示例)讨论了资产识别和估价以及影响评估。

附录E给出了信息安全风险评估方法的示例。

附录F给出了风险降低的约束。

第7章～第12章给出的所有风险管理活动的表述结构如下：

输入：标识执行该活动所需的任何信息。

动作：描述活动。

实施指南:为执行该动作提供指南。指南中的某些内容可能不适用于所有情况,因此执行该动作的其他方法可能更合适。

输出:标识执行该活动后得到的任何信息。

5 背景

为识别组织的信息安全需求和创建有效的信息安全管理体系(ISMS),一种系统化的信息安全风险管理方法是必要的。这种方法宜适用于该组织的环境,特别是与整个组织风险管理宜保持一致。安全工作宜以有效和及时的方式在需要的地方和时候处理风险。信息安全风险管理宜是所有信息安全管理活动中不可分割的一部分,并既应用于 ISMS 的实施,也应用于 ISMS 的持续运行。

信息安全风险管理宜是一个持续的过程。该过程宜建立语境,评估风险以及按风险处置计划进行风险处置以实现相关的建议和决策。风险管理为将风险降低至可接受的水平,在决定宜做什么和什么时候做之前,分析可能发生什么和可能的后果是什么。

信息安全风险管理将有助于:

- 识别风险;
- 以风险造成的业务后果和发生的可能性来评估风险;
- 沟通和理解这些风险的可能性和后果;
- 建立风险处置的优先顺序;
- 建立为降低风险发生所采取行动的优先级;
- 使利益相关方参与风险管理决策并持续告知风险管理状态;
- 监视风险处置的有效性;
- 监视和定期评审风险及风险管理过程;
- 获取信息以改进风险管理方法;
- 向管理者和员工传授风险知识以及减轻风险所采取的行动。

信息安全风险管理过程可应用于整个组织、组织的任何独立部分(例如,一个部门、一处物理位置、一项服务)、任何信息系统、现有的或计划的或特定方面的控制措施(例如,业务持续性计划)。

6 信息安全风险管理过程概述

信息安全风险管理过程由语境建立(第 7 章)、风险评估(第 8 章)、风险处置(第 9 章)、风险接受(第 10 章)、风险沟通(第 11 章)和风险监视与评审(第 12 章)组成。

如图 1 所示,信息安全风险管理过程可以迭代地进行风险评估和(或)风险处置活动。迭代方法进行风险评估可在每次迭代时增加评估的深度和细节。该迭代方法在最小化识别控制措施所需的时间和精力与确保高风险得到适当评估之间,提供了一个良好的平衡。

首先建立语境,然后进行风险评估。对于有效地确定将风险降低至可接受水平所需行动,如果风险评估提供了足够的信息,那么就结束该风险评估,接下来进行风险处置。如果提供的信息不够充分,那么将在修订的语境(例如,风险评价准则、风险接受准则或影响准则)下进行该风险评估的另一次迭代(见图 1,风险决策点 1)。此次迭代可能是在整个范围的有限部分上进行。

风险处置的有效性取决于该风险评估的结果。风险处置后的残余风险可能不会立即达到一个可接受的水平。在这种情况下,如果必要的话,可能需要在改变的语境参数(例如,风险评估准则、风险接受准则或影响准则)下进行该风险评估的另一次迭代,以及随后的进一步风险处置(见图 1,风险决策点 2)。

风险接受活动要确保残余风险被组织的管理者明确地接受。在诸如由于成本而省略或推迟实施控制措施的情况下,这点尤其重要。

在整个信息安全风险管理过程期间，重要的是将风险及其处置传达至适当的管理者和运行人员。即使是风险处置前，已识别的风险信息对管理事件可能是非常有价值的，并可能有助于减少潜在损害。管理者和员工的风险意识、缓解风险的现有控制措施的性质以及组织关注的领域，这些均有助于以最有效的方式处理事件和意外情况。信息安全风险管理过程的每个活动以及来自两个风险决策点的详细结果均宜记录在案。

GB/T 22080 规定，ISMS 的范围、边界和语境内所实施的控制措施应基于风险。信息安全风险管理过程的应用能够满足这一要求。有许多方法可以在组织内成功地实施此过程。但无论什么方法，组织宜为此过程的每一特定应用，选用最适合自身情况的方法。

在一个 ISMS 中，语境建立、风险评估、风险处置计划制定和风险接受是其“规划”阶段的全部。在此 ISMS 的“实施”阶段，依据风险处置计划，实施将风险降低到可接受水平所需的行动和控制措施。在此 ISMS 的“检查”阶段，管理者将根据事件和环境变化来确定风险评估和风险处置修订的需要。在“处置”阶段，执行所需的任何行动，包括风险管理过程的再次应用。

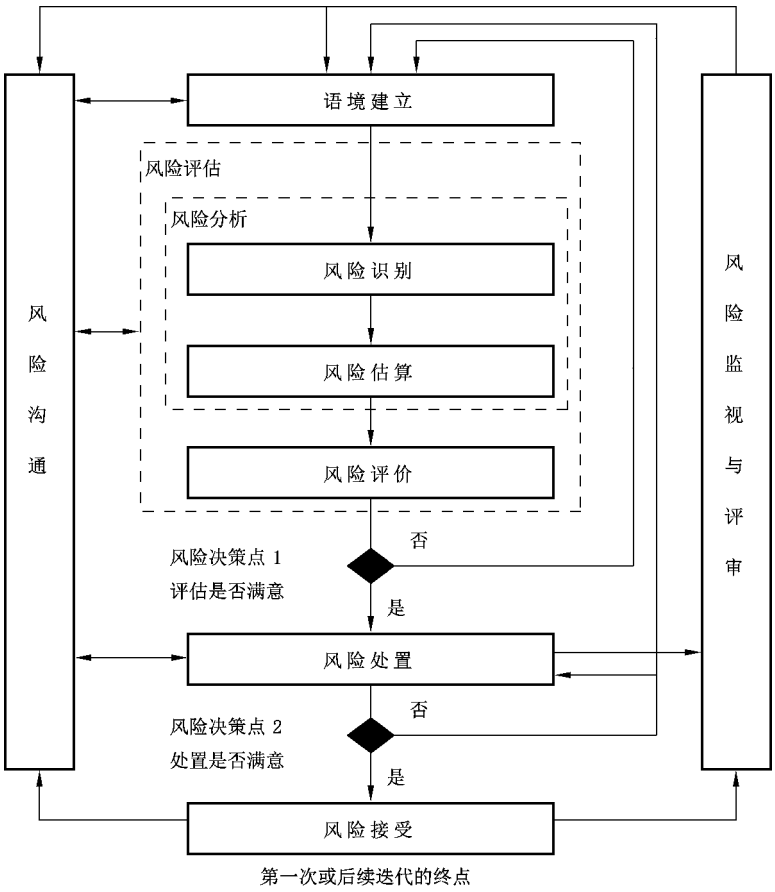

图 1　信息安全风险管理过程

表 1 总结了与 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对照表

ISMS 过程	信息安全风险管理过程
规划	语境建立 风险评估 风险处置计划制定 风险接受
实施	风险处置计划实施
检查	持续的风险监视与评审
处置	信息安全风险管理过程保持与改进

7　语境建立

7.1　总体考虑

输入：与信息安全风险管理语境建立相关的所有关于组织的信息。

动作：宜建立信息安全风险管理的语境，包括设定信息安全风险管理所必要的基本准则(7.2)，确定其范围和边界(7.3)，并建立运行信息安全风险管理的一个适当组织(7.4)。

实施指南：

确定信息安全风险管理的目的是必不可少的，因为这会影响整个过程，尤其是语境建立。目的可以是：

- 支持 ISMS；
- 遵从法律和证明尽职；
- 准备业务持续性计划；
- 准备事件响应计划；
- 描述产品、服务或机制的信息安全要求。

支持 ISMS 所需的语境建立要素的实施指南在 7.2、7.3 和 7.4 中进一步讨论。

注：GB/T 22080 没有使用术语“语境”。然而，第 7 章的所有内容都与 GB/T 22080 中规定的“确定 ISMS 的范围和边界”[4.2.1 a)]“确定 ISMS 方针”[4.2.1 b)]和“确定风险评估方法”[4.2.1 c)]要求有关。

输出：对信息安全风险管理过程的基本准则、范围和边界以及组织的规定。

7.2　基本准则

根据风险管理的范围和目标，可应用不同的方法。对于每次迭代，其方法可能是不同的。

宜选择或开发一个适当的风险管理方法来确立诸如风险评价准则、影响准则、风险接受准则等基本准则。

另外，组织宜评估下述工作的必要资源是否可用：

- 执行风险评估，建立风险处置计划；
- 确定并实施策略和规程，包括实施所选的控制措施；
- 监视控制措施；
- 监视信息安全风险管理过程。

注：见 GB/T 22080—2008 中 5.2.1 有关实施和运行 ISMS 的资源供给。

风险评价准则

宜通过考虑如下因素，开发风险评价准则来评价组织的信息安全风险：

- 业务信息过程的战略价值；
- 所涉及信息资产的关键性；
- 法律法规和规章制度的要求，以及合同义务；
- 可用性、保密性和完整性对运营和业务的重要性；
- 利益相关方的期望和观点，以及对信誉和和名誉的负面结果。

另外，风险评价准则可被用于规定风险处置的优先级。

影响准则

宜通过考虑如下因素，从信息安全事态给组织带来的损害程度或代价的角度来开发和规定影响准则：

- 受影响的信息资产的级别；
- 破坏信息安全(例如，保密性、完整性和可用性的丧失)；
- 受损的运行(内部或第三方的)；
- 业务和财务价值的损失；
- 计划中断和最终期限；
- 名誉损害；
- 违反法律法规、规章制度或合同要求。

注：见 GB/T 22080—2008 中 4.2.1 d) 4)有关识别丧失保密性、完整性和可用性的影响准则。

风险接受准则

宜开发和规定风险接受准则。风险接受准则通常取决于组织的方针策略、目标和利益相关方的利益。

组织宜对风险接受水平确定其自身的尺度。在开发中宜考虑以下因素：

- 对于一个期望的风险目标水平，风险接受准则可能包括多个阈值，但允许高级管理者在界定的环境下接受高于这一水平的风险；
- 风险接受准则可能表示为估算收益(或其他商业利益)与估算风险的比率；
- 不同的风险接受准则可能适用于不同类别的风险，例如，不符合法律法规或规章制度的风险可能不被接受，然而，如果高风险的接受作为一项合同要求有所规定，则可能允许接受高风险；
- 风险接受准则可能包括对将来附加处置的要求，例如，如果批准并承诺在确定的时间内采取行动将风险降到可接受水平，则此风险可能被接受。

根据风险预计存在时间的长短，例如，风险可能与临时或短期的活动有关，风险接受准则可能不同。风险接受准则的建立宜考虑以下因素：

- 业务准则；
- 法律法规和规章制度方面；
- 运行；
- 技术；
- 财务；
- 社会和人道主义因素。

注：风险接受准则对应于 GB/T 22080—2008 中 4.2.1 c) 2)规定的“制定接受风险的准则，识别可接受的风险级别”。

更多信息可参见附录 A。

7.3 范围和边界

组织宜确定信息安全风险管理的范围和边界。

信息安全风险管理过程的范围需要被确定,以确保所有相关的资产在风险评估中都被考虑到。此外,边界也需要被识别见 GB/T 22080—2008 中 4.2.1 a),以便考虑到通过这些边界可能引起的风险。

宜收集组织的相关信息,以决定其运营所处环境及其与信息安全风险管理过程的关联。

当确定范围和边界时,组织宜考虑以下信息:

- 组织的战略性业务目标、战略和策略;
- 业务过程;
- 组织的功能和结构;
- 适用于组织的法律法规和规章制度以及合同要求;
- 组织的信息安全方针;
- 组织的整体风险管理方法;
- 信息资产;
- 组织场所及其地理特征;
- 影响组织的制约因素;
- 利益相关方的期望;
- 社会文化环境;
- 接口(即与所处环境的信息交换)。

此外,组织宜对从范围中的任何排除提供正当理由。

风险管理范围的例子可能是某个 IT 应用、IT 基础设施、某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 GB/T 22080—2008 中 4.2.1 a)要求的 ISMS 范围和边界有关。

更多信息可参见附录 A。

7.4 信息安全风险管理机构

宜建立并保持信息安全风险管理过程的机构及其职责。该机构的主要角色和职责如下:

- 开发适用于组织的信息安全风险管理过程;
- 识别和分析利益相关者;
- 确定组织内部和外部所有相关方的角色和职责;
- 建立组织和利益相关方之间所需要的联系,以及与组织高层风险管理功能(例如,运营风险管理)的接口和与其他相关项目或活动的接口;
- 确定决策升级路径;
- 规范要保存的记录。

该机构宜得到适当的组织管理者的批准。

注:GB/T 22080 要求确定并提供建立、实施、运行、监视、评审、保持和改进 ISMS 所需的资源 GB/T 22080—2008 中 5.2.1 a)。风险管理运行机构可被看作 GB/T 22080 所要求的资源之一。

8 信息安全风险评估

8.1 信息安全风险评估总体描述

注:在 GB/T 22080 中,风险评估活动被称为过程。

输入:为信息安全风险管理过程而建立的基本准则、范围和边界以及组织。

动作:宜识别风险,量化或定性地描述风险,并按照风险评价准则和组织相关目标按优先顺序排列风险。

实施指南:

风险是有害事态发生所带来的后果与该事态发生的可能性的组合。风险评估量化或定性地描述风

险，并使管理者能根据其感知的严重性或其他已建立的准则按优先顺序排序风险。

风险评估由以下活动组成：

- 风险分析(8.2)包括：
  ——风险识别(8.2.1)；
  ——风险估算(8.2.2)。
- 风险评价(8.3)。

风险评估确定信息资产的价值，识别存在(或可能存在)的适用威胁和脆弱性，识别现有的控制措施及其对已识别风险的效果，确定潜在的后果，最后，按优先顺序排列所得出的风险，并按照语境建立时确定的风险评价准则评定等级。

风险评估通常进行两次(或多次)迭代。首先，进行高层评估来识别潜在的高风险，作为进一步评估的根据。下一次迭代可能对初始迭代所揭示的潜在高风险做进一步的深入考虑。如果这还不能提供足够的信息来评估风险，那么将会进行更加细致的分析，这可能是针对整个范围的某些部分，还可能是使用一种不同的方法。

由组织基于其风险评估的目标和对象，自行选择其自身的风险评估方法。

有关信息安全风险评估方法的讨论可参见附录 E。

输出：按照风险评价准则，按优先顺序排列的已评估风险的列表。

8.2 风险分析

8.2.1 风险识别

8.2.1.1 风险识别介绍

风险识别的目的是决定可能发生什么会造成潜在损失，并深入了解损失可能是如何、在何地、为什么发生。8.2.1 的下列子条款所描述的步骤将会为风险估算活动收集输入数据。

注：以下条款中描述的活动可能会根据所用方法的不同而按不同顺序进行。

8.2.1.2 资产识别

输入：要进行风险评估的范围和边界，包括责任人、地点、功能等要素的清单。

动作：宜识别已确定范围内的资产[对应 GB/T 22080—2008 中 4.2.1 d) 1)]。

实施指南：

资产是对组织有价值的任何东西，因此需要保护。资产识别时宜牢记，信息系统包含的不仅仅是硬件和软件。

资产识别宜在能为风险评估提供足够信息的适当详细程度上展开。资产识别的详细程度将影响在风险评估中所收集信息的总量。这种程度可在风险评估的进一步迭代中不断细化。

宜识别每项资产的责任人，以提供资产的责任和可核查性。资产责任人可能不具有资产的财产所有权，但适当时对其生产、开发、维护、使用和安全负有责任。资产责任人通常是最适合决定资产的组织价值的人选(见 8.2.2.2 中的资产估价)。

评审边界是被规定为信息安全风险管理过程所管理的组织资产边界。

与信息安全有关的资产识别和估价的更多信息可参见附录 B。

输出：要进行风险管理的资产列表、与资产相关的业务过程及其相关性的列表。

8.2.1.3 威胁识别

输入：从事件评审、资产责任人、用户以及其他来源获取的有关威胁的信息，包括外部的威胁目录。

动作：宜识别威胁及其来源[对应 GB/T 22080—2008 中 4.2.1 d) 2)]。

实施指南：

威胁有可能损害资产，诸如信息、过程、系统乃至组织。威胁可能源自自然或人类，可能是意外的或故意的。意外的和故意的威胁源都宜进行识别。威胁可能起因于组织的内部或外部。一般地宜先按类型（例如，未授权行为、物理损害、技术故障）识别威胁，然后在必要时，在所识别的一般类型中识别单个威胁。这意在于不但没有威胁被忽略，包括意料之外的，而且所需的工作量也是有限的。

一些威胁可能影响多项资产。在这种情况下，威胁可能导致不同的影响，这取决于受影响的资产。

用于识别威胁和估算其发生可能性（见 8.2.2.3）的输入可以从资产责任人或使用者、人力资源职员、设施管理人员、信息安全专家、物理安全专家、法律部门及包含法律机构的其他组织、气象权威部门、保险公司和国家政府机关等获取。对待威胁要考虑环境和文化方面。

在当前的评估中，宜考虑来自事件和以往威胁评估的内部经验。查阅其他相关威胁目录（可能是针对某个组织或业务的）来完成一般威胁列表可能是值得的。威胁目录和统计数据可以来自工业部门、政府机关、法律机构、保险公司等。

当使用威胁目录或先前的威胁评估结果时，宜意识到相关威胁是持续变化的，特别是当业务环境或信息系统发生变化时。

威胁类型的更多信息可参见附录 C。

输出：识别了威胁类型和来源的威胁列表。

8.2.1.4 现有控制措施识别

输入：控制措施说明书、风险处置实施计划。

动作：宜识别现有的和已计划的控制措施。

实施指南：

宜识别现有的控制措施以避免不必要的工作或成本，例如，重复的控制措施。此外，识别现有的控制措施时，宜进行检查以确保控制措施在正确地工作——参照已有的 ISMS 审核报告将会减少这项任务所花费的时间。如果控制措施不能按所期望地进行工作，这可能引起脆弱性。为有效处理已识别的风险，宜考虑已选的控制措施（或战略）运行失效的情况以及为此需要补充的控制措施。根据 GB/T 22080，在 ISMS 中，这是由控制措施有效性的测量来支持。估计控制措施有效性的一个途径就是查看其是否降低了威胁可能性和利用脆弱性的容易度，或者事件的影响。管理评审和审核报告也提供有关现有控制措施有效性的信息。

按照风险处置实施计划将要实施的控制措施宜与已实施的控制措施以同样的方式来考虑。

一个现有的或计划的控制措施可能被识别为无效的，或不充分的，或不合理的。如果不合理或不充分，宜检查该控制措施来确定其是否宜被移除，由另一个更适合的控制措施代替，或者比如出于成本原因而仍被保留。

以下活动能有助于识别现有的或计划的控制措施：

- 评审包含控制措施相关信息的文件（例如，风险处置实施计划）。如果信息安全管理的过程已被良好地文件化，那么，所有现有的或计划的控制措施及其实施状态将会是可获得的；
- 就考虑到的信息过程或信息系统实际上实施了哪些控制措施，与信息安全负责人（例如，信息安全官和信息系统安全官，物业经理或运营经理）和用户联系；
- 现场评审物理控制措施，将已实施的控制措施与宜被实施的控制措施列表进行比较，并就已实施的控制措施是否正确有效地发挥作用进行检查；
- 评审内部审核结果。

输出：所有现有的和计划的控制措施及其实施和使用状态的列表。

8.2.1.5 脆弱性识别

输入：已知威胁的列表、资产和现有控制措施的列表。

动作:宜识别可被威胁利用而对资产或组织造成损害的脆弱性[对应 GB/T 22080—2008 中 4.2.1 d) 3)]。

实施指南:

可在以下方面识别脆弱性:

- 组织;
- 过程和规程;
- 管理流程;
- 人员;
- 物理环境;
- 信息系统配置;
- 硬件、软件或通信设备;
- 对外部各方的依赖。

脆弱性本身不会产生危害,只有被威胁利用时才会产生危害。没有相应威胁的脆弱性可能不需要实施控制措施,但是宜关注和监视其变化。宜注意的是,一个没有被正确实施或有缺陷的控制措施,或者没有被正确使用的控制措施,其本身可能就是一个脆弱性。一个控制措施可能是有效的或无效的,这取决于其运行的环境。反之,没有相应脆弱性的威胁不会导致风险。

脆弱性可能与以某种方式或为某种目的而使用的资产特性有关,而不是资产被购买或制造当初的意图。需要考虑不同来源引起的脆弱性,例如,资产内在或外在的。

脆弱性和脆弱性评估方法的示例可参见附录 D。

输出:与资产、威胁和控制措施有关的脆弱性列表、待评审的与任何已识别的威胁无关的脆弱性列表。

8.2.1.6 后果识别

输入:资产列表、业务过程列表、与资产相关的威胁和脆弱性以及相关性列表(如果有)。

动作:宜识别因资产丧失保密性、完整性和可用性而可能造成的后果[见 GB/T 22080—2008 中 4.2.1 d) 4)]。

实施指南:

后果可能是丧失有效性、有害运行状态、业务损失、声誉破坏等。

此项活动识别可能由某事件场景对组织造成的损害或后果。一个事件场景是对在一个信息安全事件中一个威胁利用某个脆弱性或一组脆弱性的描述(见 GB/T 22081 第 13 章)。事件场景的影响是依据在语境建立活动中所定义的影响准则来确定的。它可能影响到一项或多项资产,或者资产的一部分。因此,可以按资产的财务成本和资产破坏或损害时的业务影响,给资产赋值。后果可能是临时性的,也可能是永久的(当资产被毁灭时)。

注:GB/T 22080 把事件场景的发生描述为“安全失效”。

组织宜从以下方面(但不限于)识别事件场景对运行产生的后果:

- 调查和修复时间;
- (工作)时间损失;
- 机会丧失;
- 健康和安全;
- 修复损伤所需专业技能的财务成本;
- 形象和信誉。

技术脆弱性的评估细节可见 B.3 影响评估。

输出:与资产和业务过程相关的事件场景及其后果的列表。

8.2.2 风险估算

8.2.2.1 风险估算方法

风险分析可在不同详尽程度下进行，这取决于资产的关键性、已知脆弱性的程度和组织内以前发生的事件。风险估算方法可以是定性的或定量的，或者是两者组合，这取决于所处环境。在实践中，通常首先使用定性估算，以获取风险级别的总体情况，并发现主要风险。然后，在必要时，对主要风险进行更详尽的或定量的分析，因为定性分析通常没有定量分析那么复杂和昂贵。

分析的形式宜符合建立语境时所制定的风险评价准则。

以下描述估算方法的更多细节：

a) 定性估算：

定性估算使用修饰性的尺度来描述潜在后果的严重程度(例如，低、中和高)，以及这些后果发生的可能性。定性估算的优点是易于所有相关人员理解，而缺点是对尺度主观选择的依赖。

这些尺度能被调整以适合所处环境，不同风险可采用不同的尺度描述。定性估算可被用于：

- 作为一个初步的筛选活动，以识别需要更详细分析的风险；
- 当这种分析适于作决策时；
- 当数值数据或资源不足以做定量估算时。

定性分析宜使用确凿的可用信息和数据。

b) 定量估算：

定量估算使用各种来源的数据，采用数值尺度(而不是定性估算中所用的描述性尺度)来描述后果和可能性。定量分析的质量取决于数值的准确性和完整性，以及所用模式的有效性。大多数情况下，定量估算使用历史事件数据，其优点是它能直接关联到组织的信息安全目标和关注点。但缺点是缺乏关于新的风险或信息安全弱点的这类数据。定量方法的另一个可能缺点是没有可用的确凿的、可审计的数据，使得风险评估的价值和准确性成为一种幻想。

后果和可能性的表达方式以及两者结合以表示风险程度的方式，将根据风险的类型以及风险评估输出的使用目的不同而不同。后果及可能性的不确定性和可变性宜在分析时加以考虑，并有效沟通。

8.2.2.2 后果评估

输入：已识别的相关事件场景列表，包括威胁、脆弱性、受影响的资产、对资产和业务过程造成后果的识别。

动作：宜评估可能的或实际的信息安全事件可能对组织造成的业务影响，同时考虑信息安全破坏的后果，诸如，资产保密性、完整性或可用性的丧失[对应 GB/T 22080—2008 中 4.2.1 e) 1)]。

实施指南：

在识别了评审下的所有资产后，宜在评估后果期间考虑赋予这些资产的价值。

业务影响值可以用定性和定量的形式表示，而任何赋予货币价值的方法通常会为决策提供更多的信息，从而有助于更加有效的决策过程。

资产估价从按资产关键性进行的资产分类开始，资产的关键性体现为资产对实现组织业务目标的重要性。因此，估价使用两种计量来确定：

- 资产的替换价值：彻底恢复和替换信息(如果完全可能)的成本；
- 资产丢失或损害的业务后果，诸如，信息和其他信息资产的泄漏、更改、不可用和(或)破坏对业务和(或)法律法规或规章制度造成的潜在负面后果。

这种估价可从业务影响分析中来确定。由业务后果确定的价值通常显著地高于简单的替换成本，

这取决于资产对于组织在满足其业务目标时的重要性。

资产估价是一个事件场景影响评估的关键因素，因为事件影响的可能不只一项资产（例如，相互依赖的资产），或仅是一项资产的一部分。不同的威胁和脆弱性将对资产产生不同的影响，诸如，保密性、完整性或可用性的丧失。因此，后果的评估与基于业务影响分析的资产估价有关。

后果或业务影响的确定可能是通过模型化一个事态或一组事态的输出，或者通过由实验性研究或历史数据的推断。

后果可能按货币的、技术的或人为的影响准则，或是与组织相关的其他准则来表达。在某些情况下，需要多个数值为不同的时间、地点、团体或情况来说明后果。

测量时间和财务方面的后果宜采用与用于测量威胁可能性和脆弱性的相同方法。不论是定量还是定性方法，一致性要得到保持。

有关资产估价和影响评估的更多信息可参见附录 B。

输出：按照资产和影响准则表达的事件场景评估结果列表。

8.2.2.3 事件可能性评估

输入：已识别的相关事件场景列表，包括威胁、受影响的资产、被利用的脆弱性、对资产和业务过程造成后果的识别。此外，所有现有的和已计划的控制措施及其有效性、实施和使用状况的列表。

动作：宜评估事件场景的可能性[对应 GB/T 22080—2008 中 4.2.1 e) 2)]。

实施指南：

识别事件场景后，有必要使用定性或定量估算技术，评估每个场景和影响发生的可能性。这宜考虑威胁发生的频繁程度和脆弱性被利用的容易程度，并考虑以下因素：

- 对威胁可能性的经验和适用的统计数据；
- 对于蓄意的威胁源：随时间而变的动机和能力，潜在攻击者可用的资源，以及潜在攻击者对资产吸引力和脆弱性的感知；
- 对于突发的威胁源：地理因素（例如，邻近化工或石油工厂）、极端天气情况的可能性、可能导致人为错误或设备故障的因素；
- 单个和聚集的脆弱性；
- 现有的控制措施及其减少脆弱性的有效性。

举例来说，一个信息系统可能存在被用户身份伪装和资源滥用威胁利用的脆弱性。此脆弱性，由于缺乏用户鉴别，被用户身份伪装利用的可能性会高。另一方面，尽管缺乏用户鉴别，因滥用资源的途径有限，资源滥用的可能性会较低。

根据精度的需要，资产可能被组合，也可能有必要被拆分成要素并将事件场景与要素关联。例如，跨越地理位置时，对同类资产威胁的性质可能改变，或者现有控制措施的有效性可能会变化。

输出：事件场景的可能性（定量的或定性的）。

8.2.2.4 风险级别估算

输入：事件场景列表，包括事件场景与资产和业务过程相关的后果以及事件场景发生的可能性（定量的或定性的）。

动作：宜估算所有相关事件场景的风险级别[对应 GB/T 22080—2008 中 4.2.1 e) 4)]。

实施指南：

风险估算为风险的可能性和后果赋值。这些值可以是定量的或定性的。风险估算是基于所评估的后果和可能性。此外，当适于风险评价时，它可能考虑成本效益、利益相关者的关注点和其他变量。估

算出的风险是事件场景的可能性和其后果的组合。

不同信息安全风险估算方法的示例可参见附录E。

输出:被赋予级别值的风险列表。

8.3 风险评价

输入:被赋予级别值的风险列表和风险评价准则。

动作:宜将风险级别与风险评价准则和风险接受准则比较[对应GB/T 22080—2008中4.2.1 e) 4)]。

实施指南:

关于风险评价的决策类型以及用于做出这些决策的风险评价准则,在建立语境时就已被确定。在本阶段,当了解到更多有关已识别的特定风险时,宜更详尽地重新审视这些决策及其语境。为评价风险,组织宜将已估算的风险(使用附录E讨论的被选方法或途径)与在语境建立时确定的风险评价准则进行比较。

用于决策的风险评价准则宜与确定的外部和内部信息安全风险管理语境保持一致,并考虑组织的目标和利益相关者的观点等。在风险评价活动中做出的决策主要基于风险的可接受级别。然而,风险识别和分析中得到的后果、可能性和可信度宜一并考虑。多个中低风险的聚合可能导致更高的整体风险,需要关注到。

宜考虑:

- 信息安全特性:如果一个准则与组织不相关(例如,保密性丧失),那么影响此准则的所有风险可能都与组织不相关;
- 由一个特定资产或一组资产支撑的业务过程或活动的重要性:如果过程被确定为低重要性,则与之相关的风险,相对于影响更重要的过程或活动的风险而言,宜给予较少考虑。

风险评价使用风险分析所得的关于风险的理解来对未来的行动做决策。决策宜包括:

- 是否宜采取活动;
- 考虑已估算的风险级别来排列风险处置优先级。

在风险评价阶段,除了被估算的风险外,还宜考虑合同、法律法规和规章制度要求等因素。

输出:与导致这些风险的事件场景相关的,依据风险评价准则按优先顺序排列的风险列表。

9 信息安全风险处置

9.1 风险处置总体描述

输入:与导致这些风险的事件场景相关的,依据风险评价准则按优先顺序排列的风险列表。

动作:宜选择控制措施以降低、保留、规避或转移风险,并制定一个风险处置计划。

实施指南:

风险处置有四种选项:风险降低(见9.2)、风险保留(见9.3)、风险规避(见9.4)和风险转移(见9.5)。

注:GB/T 22080—2008中4.2.1 f) 2)使用术语“接受风险”而不是“保留风险”。

图2显示了图1所示的信息安全风险管理过程中的风险处置活动。

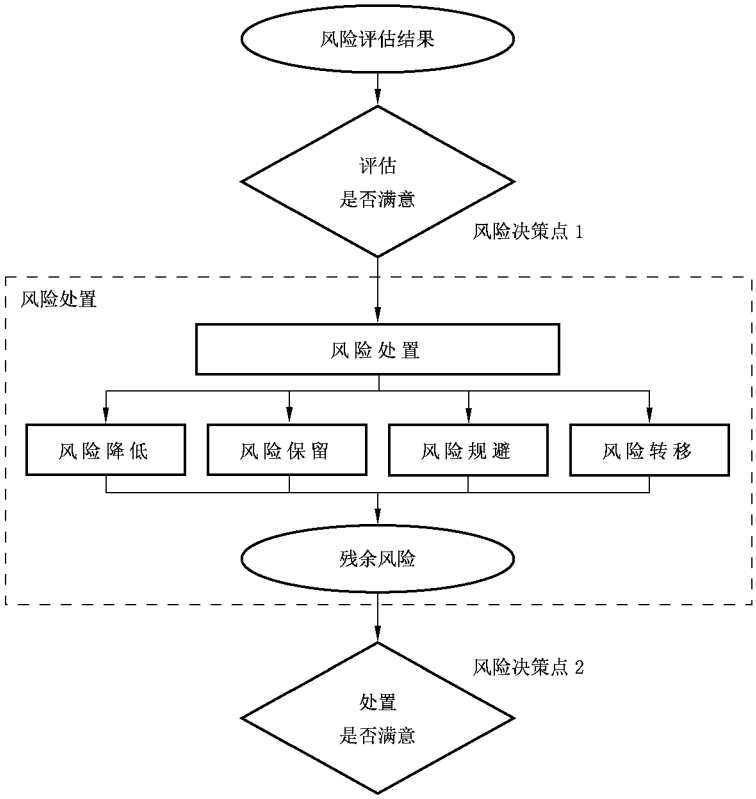

图 2　风险处置活动

选择风险处置选项时，宜基于风险评估结果以及实施这些选项的预期成本和收益。

宜实施那些以相对较低的支出就可大量减少风险的选项。进一步改进的选项可能是不经济的，需要判断其是否是合理的。

通常情况下，如果合理可行，宜尽量降低风险的负面后果，无需考虑任何绝对准则。管理者宜考虑罕见的但严重的风险。在这种情况下，可能需要实施严格经济意义上不合理的控制措施（例如，考虑覆盖特定高风险的业务连续性控制措施）。

风险处置的四个选项不是互相排斥的。有时，组织可以大幅受益于选项的组合，如降低风险的可能性，减轻其后果，并转移或保留任何残余风险。

某些风险处置能有效地解决多个风险（例如，信息安全培训和意识）。宜制定风险处置计划，明确标识出各风险处置的实施优先顺序和时限。优先级可以通过各种技术来确立，包括风险排序、成本效益分析。组织的管理者有责任决定实施控制措施的成本与预算安排之间的平衡。

就成本比较而言，现有控制措施的识别可能得出这些现有控制措施已超出当前需要的结论，包括维护。如果考虑去除多余的或不必要的控制措施（尤其是如果这些控制措施需要高昂的维护成本），那么宜考虑信息安全和成本因素。由于控制措施会相互影响，去除多余的控制措施可能会降低现有的整体安全。此外，保留而不是去除多余的或不必要的控制措施可能更便宜。

考虑风险处置选项时，宜考虑到：

- 受影响方怎样感知风险；
- 告知这些受影响方的最适当方式。

语境建立（见 7.2 中的风险评价准则）提供了有关组织需符合法律法规和规章制度要求的信息。违规是组织面临的风险，宜实现处置选项以限制这种可能性。在语境建立活动中识别的所有约束（组织的、技术的、结构的等）宜在风险处置期间予以考虑。

一旦确定了风险处置计划，就需要确定残余风险。这需要在考虑到所建议的风险处置的预期效果

下，进行风险评估的更新或再次迭代。如果残余风险仍不能满足组织的风险接受准则，则转入风险接受之前，可能有必要进行风险处置的进一步迭代。更多信息可见 GB/T 22081—2008 的 0.3。

输出：组织管理者决定接受的风险处置计划和残余风险。

9.2 风险降低

动作：宜通过选择控制措施来降低风险级别，使残余风险能够再被评估时达到可接受的级别。

实施指南：

宜选择适当的和合理的控制措施来满足风险评估和风险处置所识别的要求。这一选择宜考虑风险接受准则以及法律法规、规章制度和合同要求。这一选择也宜考虑实施控制措施的成本和时限，或者技术、环境和文化方面。通常可以通过适当选择的信息安全控制措施来降低系统的总拥有成本。

通常，控制措施可提供下列保护类型中的一种或多种：纠正、消除、预防、影响最小化、威慑、检测、恢复、监视和意识。在选择控制措施时，重要的是权衡获取、实施、管理、运行、监视和保持控制措施的成本与被保护资产的价值。而且，宜考虑某些控制措施在风险降低和开拓新业务机会的潜力方面带来的投资回报。此外，宜考虑到确定和实施新的控制措施或修改现有控制措施时所需的专业技能。

GB/T 22081 提供了有关控制措施的详细信息。

有许多约束会影响控制措施的选择。技术约束，诸如，性能要求、可管理性（运行支持要求）和兼容性问题，可能会妨碍某些控制措施的使用或导致人为失误，致使或者控制措施无效，产生安全错觉，或者比没有控制措施还甚至增加风险（例如，要求复杂的口令，但没有适当的培训，导致用户将口令写下）。而且，控制措施可能会影响性能。管理者宜设法找出解决方案以保证足够的信息安全的同时满足性能要求。这一步骤的结果是可能的控制措施的列表，包括成本、效益和实施优先级。

选择和实施控制措施时宜考虑各种不同约束。典型考虑如下：

- 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；
- 人员约束；
- 集成新的和现有控制措施的约束。

关于风险降低约束的更多信息可参见附录 F。

9.3 风险保留

动作：宜根据风险评价做出的不采取进一步行动的风险保留决策。

注：GB/T 22080—2008 中 4.2.1 f) 2)“在明显满足组织方针策略和接受风险的准则的条件下，有意识地、客观地接受风险”描述同样的活动。

实施指南：

如果风险级别满足风险接受准则，那么没有必要实施额外的控制措施，并且风险可被保留。

9.4 风险规避

动作：宜规避引起特定风险的活动或状况。

实施指南：

当所识别的风险被认为过高，或实施其他风险处置选项的花费超过了收益时，可作出从计划的或现有的活动或一组活动中的撤出，或者改变活动赖以进行的状况的决定，以此来完全地规避风险。例如，对于由自然界引起的风险，物理上把信息处理设施移到风险不存在或处于控制下的地方，可能是成本效益最好的选择。

9.5 风险转移

动作：宜将风险转移给能有效管理特定风险的另一方，这取决于风险评价。

实施指南：

风险转移需做出与外部相关方共担某些风险的决策。风险转移能产生新的风险或更改现存的、已识别的风险。因此，额外的风险处置可能是必要的。

转移的实现可以是通过保险来补偿后果，或者分包给合作伙伴来监视信息系统和立即采取行动阻止攻击以防造成超过规定程度的损害。

宜注意的是，转移管理风险的责任是可能的，但是转移影响的责任通常是不可能的。客户通常会将负面影响归于组织的过错。

10 信息安全风险接受

输入：组织管理者决定接受的风险处置计划和残余风险。

动作：宜做出并正式记录接受风险的决策及相应责任[对应 GB/T 22080—2008 中 4.2.1 h)]。

实施指南：

风险处置计划宜描述被评估的风险如何被处置以满足风险接受准则(见 7.2 中的风险接受准则)。对于负有责任的管理者来说，重要的是评审和批准建议的风险处置计划及其残余风险，并记录与此批准相关的任何条件。

与只决定残余风险是否高于或低于某个单一阈值，风险接受准则可能更加复杂。

在某些情况下，由于所用的风险接受准则没有考虑当前的环境，残余风险级别可能不满足风险接受准则。例如，由于伴随风险的利益非常诱人，或者降低风险的成本太高，可能会主张有必要接受风险。这种情况表明风险接受准则是不充分的，如有可能宜进行修订。然而，及时修订风险接受准则不总是可能的。在这种情况下，决策者可能不得不接受不符合正常接受准则的风险。如果这是必要的，决策者宜明确地给出对风险的意见，并给出其不按正常风险接受准则做决策的理由。

输出：被接受风险的列表，以及接受那些不符合组织正常风险接受准则的风险的理由。

11 信息安全风险沟通

输入：从风险管理活动(见图 1)中获得的所有风险信息。

动作：有关风险的信息宜在决策者和其他利益相关方之间进行交换和(或)共享。

实施指南：

风险沟通是一项在决策者和利益相关者之间就如何通过交换和(或)共享有关风险信息来管理风险而达成一致的活动。风险信息包括但不限于风险的存在、性质、形式、可能性、严重程度、处置和可接受性。

利益相关者之间的有效沟通是重要的，因为它可能对决策有显著的影响。沟通将确保那些实施风险管理的负责人和那些既得利益者，理解决策的基础和所需特定行动的原因。沟通是双向的。

当利益相关者涉及到面临的风险或问题时，对风险的感知可能因他们的假设、概念与需求、问题与

关注点的不同而不同。利益相关者很可能基于他们对风险的感知来判断风险可接受性。尤其重要的是确保识别和文件化利益相关者对风险和利益的感知,并明确地理解和解决其根本原因。

宜进行风险沟通以达到如下目的:

- 为组织的风险管理结果提供保障;
- 收集风险信息;
- 共享风险评估结果,提出风险处置计划;
- 避免或减少由于决策者和利益相关者之间缺少相互理解而导致的信息安全破坏和其后果;
- 支持决策;
- 获取新的信息安全知识;
- 与其他方协作,制定响应计划以降低任何事件的后果;
- 使决策者和利益相关者具有风险责任感;
- 提高意识。

组织宜为正常运行以及突发情况制定风险沟通计划。因此,宜持续执行风险沟通活动。

可以通过成立一个委员会来实现主要决策者和利益相关者之间的协作,风险及其优先级、适当处置和接受可在这个委员会上讨论。

重要的是与组织内适当的公共关系部门或对外沟通部门进行合作,以协调所有有关风险沟通的任务。这在危机沟通行动中至关重要,例如,响应特殊的事件。

输出:对组织的信息安全风险管理过程和结果的持续理解。

12 信息安全风险监视和评审

12.1 风险因素的监视和评审

输入:从风险管理活动(见图 1)中获得的所有风险信息。

动作:宜监视和评审风险及其因素(例如,资产的价值、影响、威胁、脆弱性、发生的可能性),以便在早期阶段识别出组织语境中的任何变化,并保持对整个风险状况的总体了解。

实施指南:

风险不是静态的。威胁、脆弱性、可能性或后果可能会在没有任何迹象的情况下突然改变。因此,有必要持续监视以发现这些变化。这可以由提供有关新威胁或脆弱性信息的外部服务来支持。

组织宜确保以下事项得到持续监视:

- 风险管理范围内的新资产;
- 资产价值的必要更改,例如,由于已变化的业务要求;
- 活跃于组织内部和外部且未被评估的新威胁;
- 新的或增加的脆弱性被威胁利用的的可能性;
- 正暴露于新的或再现威胁的已识别的脆弱性;
- 已评估的威胁、脆弱性和风险因聚合而增加的影响或结果,进而导致不可接受的风险级别;
- 信息安全事件。

新的威胁或脆弱性、可能性或后果的变化可能会提高先前被评估为低级别的风险。评审低级别的和已接受的风险时,宜分别考虑每个风险以及所有这些风险的聚合,以评估其潜在的累加影响。如果风险没能归入到低级别的或可接受的风险类别中,宜使用第 9 章中给出的一个或多个选项来处置这些风险。

影响威胁发生的可能性和后果的因素以及影响各种处置选项的适用性或成本的因素都可能发生变化。影响组织的重要变化宜作为进一步详尽评审的理由。因此,宜定期重复风险监视活动,并定期评审所选的风险处置选项。

风险监视活动的结果可作为其他风险评审活动的输入。组织宜定期和当重要变化发生时评审所有的风险[按照 GB/T 22080—2008 中 4.2.3)]。

输出:风险管理与组织的业务目标和风险接受准则的持续一致。

12.2 风险管理监视、评审和改进

输入:从风险管理活动(见图 1)中获得的所有风险信息。

动作:必要和适当时,宜持续监视、评审和改进信息安全风险管理过程。

实施指南:

为确保风险评估和风险处置的语境和结果以及风险管理计划保持对所处环境的相关性和适用性,有必要进行持续监视和评审。

组织宜确保信息安全风险管理过程及相关活动适合目前环境并被遵循。任何商定的风险管理过程改进或增进风险管理过程符合性所需的活动,宜通知到适当的管理者,以确保没有风险或风险要素被忽视或低估,并确保采取必要的行动和做出决策,以提供对现实风险的了解和响应能力。

此外,组织宜定期验证风险及其要素的测量准则依然有效并与业务目标、战略和策略保持一致,以及在信息安全风险管理过程中充分考虑了业务语境的变化。监视和评审活动宜关注(但不限于):

- 法律和环境语境;
- 竞争语境;
- 风险评估方法;
- 资产价值和类别;
- 影响准则;
- 风险评价准则;
- 风险接受准则;
- 总拥有成本;
- 必要的资源。

组织宜确保有持续可用的风险评估和风险处置资源来评审风险、解决新的或改变的威胁或脆弱性,并提出相应的管理建议。

风险管理监视可能导致所使用方式、方法或工具的修改或添加,这取决于:

- 已识别的变化;
- 风险评估迭代;
- 信息安全风险管理过程的目标(例如,业务连续性、抵御事件的能力、符合性);
- 信息安全风险管理过程的对象(例如,组织、业务单元、信息过程、技术实现、应用、与互联网的连接)。

输出:信息安全风险管理过程与组织的业务目标或更新过程的持续适宜。

附 录 A
（资料性附录）
确定信息安全风险管理过程的范围和边界

A.1 组织的调研

a) 评价组织：通过调研组织重新认识界定组织身份的特征要素。这涉及组织的目的、业务、使命、价值和战略。这些要素宜与有助于其发展的要素（例如，分包）一起被识别。

这一活动的难度在于准确理解组织是如何构成的。识别组织的真实结构将有助于理解每个部门在实现组织目标中的角色和重要性。

例如：信息安全管理者向最高管理者而不是IT管理者报告可表明最高管理者对信息安全的介入。

b) 组织的主要目的：组织的主要目的可被定义为其存在的理由（其活动领域、其市场分割等）。

c) 组织业务：由组织雇员的技术和专门知识决定的组织业务，能使其完成使命。它对组织的活动领域是特定的，并通常决定其文化。

d) 组织使命：组织通过完成其使命来实现其目的。为明确其使命，宜识别为最终用户提供的服务和制造的产品。

e) 组织价值：价值是应用于业务实践的主要原则或良好的行为准则。它可能涉及人员、与外部机构（客户等）的关系、提供的产品或服务的质量。

以提供公共服务为目的、从事运输业务、接送孩子上下学的组织为例，其价值可能是服务的准时和运输过程的安全。

f) 组织结构：

1) 有不同类型的结构：

- 部门结构：每个部门受负责该部门的战略、管理和运行决策的管理者领导。
- 功能结构：在规程、工作性质和某些时候的决策或规划（例如，生产、IT、人力资源、市场等）中行使功能职权。

2) 备注：

- 具有部门结构的组织中的某部门可按职能结构划分，反之亦然。
- 如果某组织具有两种类型的结构，则可称之为具有矩阵结构。
- 任何组织结构中，可划分为如下层次：

——决策层（定义战略方向）；

——领导层（协调和管理）；

——运行层（生产和支持活动）。

g) 组织结构图：组织结构可以以组织结构图来示意表示。这种表示宜强调报告和授权的路线，还宜包括其他关系，即使它们不是基于任何正式授权，但仍然是信息流的路线。

h) 组织战略：这有赖于组织指导原则的一个正式表达。组织战略决定了为了从面临的重大课题和计划中的重大改革中获益而需要的方向和发展。

A.2 影响组织的约束列表

所有影响组织和决定其信息安全方向的约束宜被考虑。它们可能源于组织内部或组织外部，对组织内部的约束可以有某种控制，但对组织外部的约束通常不可协商。资源约束（预算、人员）和紧急情况

约束属于最重要的约束之类。

组织设定其目标(涉及其业务、行为等),通过一定的路线来实现,可能需要一段较长的时期。它确定了想成为什么以及所需的实现手段。在说明这种路线时,组织宜考虑技术和专门知识的发展、用户所表达的意愿、客户等。这一目标可以以具有针对性的运行或发展战略的形式来表达,例如,削减运行成本、改进服务质量等。

这些战略可能包括有助于其应用的信息和信息系统(IS)。因此,因信息安全方面的违反可能导致重新思考这些战略目标时,涉及组织身份、使命和战略的特征是分析问题的基本要素。另外,对信息安全要求的建议,与组织中现行的规则、使用和手段保持一致是至关重要的。

约束列表包括但不限于:

a) 政策性约束:这可能涉及政府管理部门、公共机构或须履行政府决定的任何组织。它们通常是由政府部门或决策机构做出的涉及战略或运行方向的决定,宜被应用。
例如:发票或公文的计算机化引入了信息安全问题。

b) 战略性约束:约束可能产生于组织结构或方向上有计划的或可能的变化。它们被表述在组织的战略和运行计划中。
例如:在共享敏感信息方面的国际合作可能有必要就安全交流达成协议。

c) 领土性约束:组织结构和(或)目的可能引入特定约束,诸如,场所分布于整个国家领土或海外。这类示例,包括邮政服务、大使馆、银行、大型工业集团的子公司等。

d) 经济和政治形势产生的约束:组织运行可能因诸如罢工或国内外危机这类特定事件发生深刻的变化。
例如:某些服务甚至在严重的危机中宜能够持续。

e) 结构性约束:组织结构的性质(部门的、功能的或其他)可能导致特定的信息安全策略和安全组织的调整以适应该结构。
例如:一个国际性的结构宜能适应每个国家特定的安全要求。

f) 功能性约束:功能性约束直接产生于组织的一般或特定使命。
例如:24 小时运行的组织宜确保其资源的持续可用。

g) 人员方面的约束:这类约束的性质差别很大。它们与责任级别、聘用、资格、培训、安全意识、动机、可用性等关联。
例如:国防机构的全体人员宜具有处理高度保密信息授权。

h) 组织日程表产生的约束:这类约束可能来自因改组或建立新的国家或国际策略而施加的某些期限。
例如:创建一个安全部门。

i) 方法相关的约束:适合组织专有技术的方法需要被强加于诸如项目规划、规范、开发等方面。
例如:典型的这种约束是需要将组织的法律义务纳入安全策略。

j) 文化约束:在某些组织中工作习惯或主要业务已在组织内导致一种特定的“文化”,它可能与安全控制不兼容。这种文化是组织员工的一般参考框架,可能取决于多个方面,包括教育、指导、专业经验、工作以外经验、看法、人生观、信仰、社会地位等。

k) 预算约束:建议的安全控制措施可能有时成本很高。当基于成本效益来衡量安全投资不总是适合时,组织的财务部门通常要求给出经济上的合理理由。
例如:在私营部门和某些公共机构中,安全控制措施的总成本不宜超过风险潜在后果的代价。因此,如果想避免过高的安全成本,最高管理层宜评估和掌握计算出的风险。

A.3 适用于组织的法律法规和规章制度参考列表

宜识别适用于组织的法规要求。这些可能是法律法规、规章制度、组织领域中的特定规章或组织内部/外部的规章。这也涉及合同和协议以及更一般地来讲法律法规或规章制度性质的任何义务。

A.4 影响到范围的约束列表

通过识别约束,有可能列出影响到范围的那些约束,并确定哪些适合采取行动。这些约束被加到或可能修改上述确定的组织约束。以下给出一个未尽的可能的约束类型列表:

a) 现有过程产生的约束:应用项目不一定是同时开发。一些项目依赖已有的过程。即使一个过程能够被分解成多个子过程,这个过程并不一定受另一个已有过程的所有子过程的影响。

b) 技术约束:与基础设施相关的技术约束通常产生于已安装的软硬件,以及承载过程的房间或场所:
   - 文件(有关组织、介质管理、访问规则管理等方面的要求);
   - 总体结构[有关拓扑结构(集中式、分布式、客户端/服务器式)、物理结构等方面的要求];
   - 应用软件(有关具体软件设计、市场标准等方面的要求);
   - 套装软件(有关标准、评价级别、质量、合规、安全等方面的要求);
   - 硬件(有关标准、质量、合规等方面的要求);
   - 通信网络(有关覆盖范围、标准、容量、可靠性等方面的要求);
   - 建筑基础设施(有关土木工程、建筑、高压、低压等方面的要求)。

c) 财务约束:安全控制措施的实施经常受到组织能承诺的预算的限制。但是,由于分配给安全的预算可以在安全研究基础上进行协商,宜最后考虑财务约束。

d) 环境约束:环境约束产生于过程实施所处的地理或经济环境:国家、气候、自然风险、地理状况,经济形势等。

e) 时间约束:实施安全控制措施所需的时间宜根据升级信息系统的能力来考虑;如果实施时间过长,控制措施所解决的风险可能已改变。时间是选择解决方案和优先级的一个决定因素。

f) 方法相关的约束:宜使用适合组织专有技术的方法进行项目规划、规范、开发等。

g) 组织约束:以下各种约束可能产生于组织的要求:
   - 运行(有关交货时间、服务提供、监督、监视、应急计划、降级运行等方面的要求);
   - 维护(对事件的故障排除、预防措施、快速纠正等方面的要求);
   - 人力资源管理(有关操作员和用户培训、诸如系统管理员或数据管理员的上岗资格等方面的要求);
   - 行政管理(有关责任等方面的要求);
   - 开发管理(有关开发工具、计算机辅助软件工程、验收计划、机构设立等方面的要求);
   - 外部关系管理(有关第三方关系组织、合同等方面的要求)。

附 录 B
（资料性附录）
资产识别和估价以及影响评估

B.1 资产识别示例

为了进行资产估价，组织首先需要识别其资产（在适当的详细程度上）。可分为两类资产：

- 主要资产：
  ——业务过程和活动；
  ——信息。
- 各种类型的支撑性资产（范围内的主要要素所依赖的）：
  ——硬件；
  ——软件；
  ——网络；
  ——人员；
  ——场所；
  ——组织结构。

B.1.1 主要资产的识别

为了更准确地描述范围，此活动主要在于识别主要资产（业务过程和活动、信息）。这种识别由代表过程的（管理者、信息系统专家和用户）联合工作组来进行。

主要资产通常是范围内活动的核心过程和信息。其他诸如组织过程的主要资产也可以被考虑，这对制定信息安全方针策略和业务持续性计划更适合。根据不同的目的，一些研究将不需要详尽地分析构成范围的所有要素。在这种情况下，研究边界可以限定在范围的关键要素。

主要资产分为两类：

a) 业务过程（或子过程）和活动，例如：
   - 其丧失或降级会使组织的使命无法履行的过程；
   - 含有秘密处理或涉及专有技术的过程；
   - 如果被修改可能极大地影响组织使命完成的过程；
   - 组织符合合同、法律法规或规章制度要求所必要的过程。

b) 信息

   更一般地来说，基本信息主要包含：
   - 要害信息，为执行组织的使命或业务所需要的；
   - 个人信息，在关于隐私的国家法律意义上可能被特别定义的；
   - 战略信息，为实现由战略方向确定的目标所需要的；
   - 高成本信息，收集、存储、处理和传输需要长时间和（或）含有高获取成本的。

此活动之后没有被识别为敏感的过程和信息，在后续研究中将没有定级。这意味着，即使这种过程或信息被损害，组织仍将成功完成其使命。

但是，它们通常受益于已实施的保护敏感过程和信息的控制措施。

B.1.2 支撑性资产清单和描述

范围由宜被识别和描述的资产组成。这些资产存在脆弱性，可被威胁利用来损害范围内的主要资

产(过程和信息)。支撑性资产具有不同类型:

a) 硬件:硬件类型由所有支撑过程的物理要素组成。

1) 数据处理设备(主动的):自动信息处理设备,包括独立运行所需的项目。

2) 可移动设备:便携式计算机设备。

例如:笔记本电脑、个人数字助理(PDA)。

3) 固定设备:组织场所内所用的计算机设备。

例如:服务器、作为工作站使用的微机。

4) 外围处理设备:为输入、传送或传输数据,通过通信端口(串行、并行链接等)连接到计算机的设备。

例如:打印机、可移动硬盘驱动器。

5) 数据介质(被动的):存储数据或功能的介质。

6) 电子介质:可连接到计算机或计算机网络用于数据存储的信息介质。尽管体积小巧,这些介质可能含有大量的数据。它们可与标准的计算设备一起使用。

例如:软盘、CD ROM、备份磁带、可移动硬盘、存储钥匙、磁带。

7) 其他介质:含有数据的静态的、非电子的介质。

例如:纸张、幻灯片、胶片、文件、传真。

b) 软件:软件类型由所有实现数据处理操作的程序组成。

1) 操作系统:操作系统包括所有那些奠定其他程序(服务或应用)运行基础的计算机程序。它包括内核和基本功能或服务。根据不同的体系结构,操作系统可能是单体式的或由一个微内核和一套系统服务组成。操作系统的主要要素是所有那些设备管理服务(CPU、内存、磁盘和网络接口)、任务或过程管理服务和用户权限管理服务。

2) 服务、维护或管理软件:补充操作系统服务但不直接对用户或应用提供服务的软件(尽管通常其对信息系统的整体运行是基本的、甚至不可缺少的)。

3) 套装软件或标准软件:标准软件或套装软件是那些带有介质、发布和维护的完整的商业化产品(而不是一次性或特定的开发)。它们为用户和应用提供服务,但不是个性化的或按业务应用定制的。

例如:数据库管理软件、电子消息软件、群件、目录软件、Web 服务器软件等。

4) 业务应用:

- 标准业务应用:这是一种商业软件,被设计成让用户在其专业语境下直接从其信息系统访问其需要的服务和功能。具有非常广泛的、理论上无限的领域范围。

例如:会计软件、机床控制软件、客户服务软件、人员能力管理软件、行政管理软件等。

- 特定业务应用:这是一种为各种不同方面(主要支持、维护、升级等)专门开发的软件,让用户直接从其信息系统中访问其需要的服务和功能。应用范围广泛,理论上无限的,可以是各个领域。

例如:电信运营商客户的发票管理、火箭发射的实时监控应用。

c) 网络:网络类型由所有用于将多个物理远程计算机或信息系统组件相互连接的通讯装置组成。

1) 介质和支撑设备:通信和电信介质或设备主要以设备的物理和技术特点(点对点、广播)以及通信协议(链接或网络——OSI 七层模型的第 2 层和第 3 层)为特征来描述。

例如:公共交换电话网(PSTN)、以太网、千兆比特以太网、非对称数字用户线路(ADSL)、无线通信协议规范(例如,WiFi 802.11)、蓝牙、火线。

2) 被动或主动中继:此子类包括所有不是通信的逻辑终点(信息系统视角)而是中间或中继的设备。中继以所支持的网络通信协议为特征来描述。除了基本的中继,它们往往使用带有过滤器的通信交换机和路由器,来包含路由和(或)过滤功能和服务。它们经常可以

被远程管理，并通常能够产生日志。

例如：网桥、路由器、集线器、交换机、自动交换机。

3） 通信接口：处理单元的通信接口用于连接处理单元，以介质和所支持的协议，所安装的过滤、日志或报警功能及其容量，以及远程管理的可能性和要求为特征来描述。

例如：通用分组无线服务(GPRS)、以太网适配器。

d） 人员：人员类型由所有涉及信息系统的小组人员。

1） 决策者：决策者是主要资产(信息和功能)的负责人和组织或具体项目的管理者。

例如：最高管理者、项目负责人。

2） 用户：用户是那些在其活动语境下处理敏感要素和在这方面具有特定职责的人员。他们可能具有访问信息系统的特定权限来进行日常工作。

例如：人力资源管理者、财务管理者、风险管理者。

3） 运行/维护人员：运行/维护人员是那些负责运行和维护信息系统的人员。他们具有访问信息系统的特定权限来进行日常工作。

例如：系统管理员、数据管理员、备份/服务台/应用部署操作员、安全官。

4） 开发人员：开发人员负责开发组织的应用。他们具有访问部分信息系统的高级权限，但不能对生产数据采取任何行动。

例如：业务应用开发人员。

e） 场所：场所类型由所有容纳运行所需的范围或部分范围以及物理手段的地方组成。

1） 位置：

- 外部环境：这涉及组织的安全手段不能应用的所有位置。

例如：个人家庭、另一个组织的辖区、组织场所以外的环境(市区、危险区)。

- 辖区：此地点以组织与外面接壤的周边为界。这可能是通过建立物理屏障或者采用建筑物周边监视手段而获得的物理保护边界。

例如：院落、楼宇。

- 保护区：保护区是在组织辖区内由物理保护边界形成的隔离区。它通过在组织的信息处理基础设施周边建立物理障碍来获得。

例如：办公室、限制访问区，安全区。

2） 基础服务：

组织设备运行所需的所有服务。

- 通信：运营商提供的电信服务和设备。

例如：电话线、程控交换机(PABX)、内部电话网。

- 公用设施：

——为信息技术设备和外围设备提供电力所需的服务和手段(电源和线路)；

例如：低压电源、变压器、电路头端。

——供水；

——废物处置；

——冷却和净化空气的服务和手段(设备、控制)。

例如：冷却水管道、空调。

f） 组织：组织类型描述组织框架，由所有分配了任务的人员结构和控制这些结构的规程组成。

1） 权力部门：这是那些被调研组织从其得到授权的组织。它们可能是合法的分支机构或外部机构。这将在规章、决策和行动方面约束被调研组织。

例如：行政机关、组织的总部。

2） 组织结构：这由在组织管理层控制下的其各分支机构组成，包括跨职能活动。

例如:人力资源管理、IT 管理、采购管理、业务部管理、楼宇安全服务、消防服务、审计管理。

3) 项目或系统组织:这是为特定项目或服务成立的组织。

例如:新应用开发项目、信息系统迁移项目。

4) 分包商/供应商/制造商:这是那些按照合同提供服务或资源的组织。

例如:设施管理公司、外包公司、咨询公司。

B.2 资产估价

资产识别后的下一步是对资产估价用的尺度和基于该尺度为每项资产赋值的准则达成一致。由于在大多数组织中所发现资产的多样性,某些资产可能具有以当地货币单位估价的已知货币值,而其他一些资产可能被赋以给定范围(例如,从"很低"到"很高")内的定性值。使用定量尺度还是定性尺度完全取决于组织的偏好,但宜与被估价的资产相适应。两种估价类型可用于相同的资产。

用于资产定性估价的典型措词包括诸如忽略、很低、低、中等、高、很高和关键这样的词。适合组织的这种措词的选择和范围很大程度依赖于组织的安全要求、规模和其他特定因素。

a) 准则:

作为每项资产赋值基础的准则宜以明确的措施写出来。这经常是资产估价的最困难方面之一,因为某些资产价值可能要主观决定而且可能由许多不同的人作出决定。用于决定资产价值的可能准则包括资产的原始成本、更换或再造成本或者其抽象价值(例如,组织名誉的价值)。

资产估价的另一个基础是因事件导致保密性、完整性和可用性的损失而付出的成本。抗抵赖性、可核查性、真实性和可靠性也宜在适当时被考虑。这种估价,除了更换成本外,将提供资产价值的另外重要维度,即基于一组假定环境下安全事件导致对业务负面影响的估算。值得强调的是,这种方法已考虑到作为风险评估必要因素的后果。

许多资产在估价过程中可能有数个值被赋予。例如,业务计划可能基于开发计划的劳务花费来估价,也可能基于输入数据的劳务花费来估价,还可能基于其对竞争对手的价值来估价。每一个赋值都很可能相当不同。最终赋值可能是所有可能值的最大值,也可能是部分或全部可能值的和。归根结底,哪个值或哪些值被赋予某项资产宜谨慎决定,因为最终赋值作为决定保护该资产所需花费资源的输入。

b) 归一到共同基准:

最终,所有资产估价需要归一到一个共同基准上。这可在如下的准则帮助下来做到。用于评估由资产的保密性、完整性、可用性、抗抵赖性、可核查性、真实性或可靠性的损失而导致可能后果的准则有:

- 法律法规和(或)规章制度的违反;
- 经营业绩的损害;
- 声誉损失/对名誉的负面影响;
- 个人信息的侵害;
- 人身安全的危及;
- 对执法的不利影响;
- 保密性的破坏;
- 公共秩序的破坏;
- 财务损失;
- 业务活动的中断;
- 环境安全的危及。

评估后果的另一种方法可能是:

- 服务中断:

  ——没有能力提供服务。

- 客户信心的丧失：
  ——内部信息系统可信性的丧失；
  ——名誉的损害。
- 内部运行的中断：
  ——组织自身的中断；
  ——额外的内部成本。
- 第三方运行的中断：
  ——与组织交易的第三方中断；
  ——各种类型的伤害。
- 法律法规/规章制度的违反：
  ——没有能力履行法律义务。
- 合同的违背：
  ——没有能力履行合同义务。
- 对人员/用户安全的危害：
  ——对组织人员和(或)用户的危害。
- 对用户私生活的侵犯；
- 财务损失；
- 应急或修复的财务成本：
  ——人员成本；
  ——设备成本；
  ——研究和专家报告成本。
- 货物/资金/资产的损失；
- 客户损失、供应商损失；
- 司法诉讼和处罚；
- 竞争优势的丧失；
- 技术领先的丧失；
- 效力/信任的丧失；
- 技术信誉的丧失；
- 谈判能力的消弱；
- 产业危机(罢工)；
- 政府危机；
- 解散；
- 物资损失。

这些准则是资产估价时考虑问题的示例。进行估价时，组织需要选择与其业务类型和安全要求相关的准则。这可能意味着上面列出的某些准则是不适用的，而其他准则可能需要加到列表中。

c) 尺度：

建立所考虑的准则之后，组织宜就组织范围内使用的尺度达成一致。第一步是决定使用的等级数。对于最适合的等级数没有一定之规。越多的等级提供越细的等级粒度，但有时过细的区别使得难以在整个组织做到一致的赋值。通常，在3(例如，低、中和高)和10之间的任何等级数可被使用，只要它与组织用于整个风险评估过程的方法一致。

组织可以定义自己的资产价值界限，像“低”“中”或“高”。宜根据所选的准则对这些界限进行评估(例如，对于可能的财务损失，宜给出它们的货币值，但对于如危及人身安全的这类考虑，货币估价可能因复杂而不适用于所有组织)。最后，决定什么才算“低”或“高”后果完全取决于组织自己。对于一个小

型组织可能是灾难性的结果,对于一个特大型组织可能是低或甚至忽略。

d) 依赖:

一项资产支持的业务过程越相关和越多,该资产的价值就越大。资产与业务过程和其他资产的依赖宜被识别,因为这可能影响到资产价值。例如,数据保密性宜在其生存周期的所有阶段(包括存储和处理)得到保持,即数据存储和处理程序的安全需要宜直接关联到反映所存储和处理数据的保密性价值。同样,如果业务过程依赖一个程序所产生数据的完整性,那么该程序的输入数据宜具有适当可靠性。此外,信息的完整性将取决于用于其存储和处理的硬件和软件。同样,硬件将依赖电力供应,还可能是空调。因此,有关依赖的信息将有助于威胁、特别是脆弱性的识别。另外,还将有助于确保赋予资产其真实的价值(通过依赖关系),从而表明适当的保护等级。

被其他资产依赖的资产的价值可按如下方式修正:

- 如果依赖资产(例如,数据)的价值低于或等于所考虑资产(例如,软件)的价值,则所考虑资产的价值保持不变;
- 如果依赖资产(例如,数据)的价值大于所考虑资产(例如,软件)的价值,则所考虑资产的价值宜根据如下因素进行增加:
  ——依赖程度;
  ——依赖资产的价值。

组织也许有一些资产可多次使用,像软件程序的拷贝或在大多数办公室内使用的同类型计算机。重要的是在进行资产估价时考虑到这一事实。一方面,这些资产容易被忽视,因此宜注意识别所有它们;另一方面,它们可能被用于减少可用性问题。

e) 输出:

此步骤的最终输出是一张资产列表及其相对如下付出成本的价值:泄露(保密性的保持)、篡改(完整性、真实性、抗抵赖性和可核查性的保持)、不可用和毁坏(可用性和可靠性的保持)以及更换。

B.3 影响评估

信息安全事件可能影响多项资产或一项资产的一部分。影响与事件的成功度有关。因此,资产价值与事件导致的影响之间有重要的区别。影响被认为具有或者当前的(运行的)影响或者未来的(业务的)影响,包括财务和市场后果。

当前的(运行的)影响或者是直接的或者是间接的。

a) 直接的:
   1) 替换损失的资产或部分资产的财务价值;
   2) 购置、配置和安装新资产或备份的成本;
   3) 因事件暂停运行直到提供服务的资产恢复期间的代价;
   4) 信息安全破坏导致的影响。

b) 间接的:
   1) 机会代价(更换或修复资产需要的财务资源本可用于别处);
   2) 中断运行的代价;
   3) 通过安全破坏所获信息的潜在滥用;
   4) 法律法规或规章制度义务的违反;
   5) 道德行为准则的违反。

因此,首次评估(没有任何控制措施)将估算出一个非常接近所关注的(组合)资产价值的影响。对于这项(这些)资产的任何复评,影响将因所实施控制措施的出现和效力而不同(通常更低)。

附 录 C
（资料性附录）
典型威胁示例

表 C.1 给出典型威胁的示例，可在威胁评估过程中使用。威胁可能是故意的、意外的或环境的（自然的），并可能导致，例如，基本服务的损害或丧失。表 C.1 指出每个威胁的类型，包括 D（故意的）、A（意外的）、E（环境的）。D 表示针对信息资产的所有故意行为，A 表示可能意外地损害信息资产的所有人为行为，E 表示不是基于人为行为的所有事件。威胁组没有优先顺序。

表 C.1 典型威胁示例

类型	威胁	来源
物理损害	火灾	A、D、E
	水灾	A、D、E
	污染	A、D、E
	重大事故	A、D、E
	设备或介质毁坏	A、D、E
	灰尘、腐蚀、冻结	A、D、E
自然灾害	气候现象	E
	地震现象	E
	火山现象	E
	气象现象	E
	洪水	E
基本服务丧失	空调或供水系统故障	A、D
	电力供应失去	A、D、E
	电信设备故障	A、D
辐射干扰	电磁辐射	A、D、E
	热辐射	A、D、E
	电磁脉冲	A、D、E
信息损害	对阻止干扰信号的拦截	D
	远程侦探	D
	窃听	D
	介质或文件偷窃	D
	设备偷窃	D
	回收或废弃介质的检索	D
	泄露	A、D
	来自不可信源的数据	A、D
	硬件篡改	D
	软件篡改	A、D
	位置探测	D

表 C.1（续）

类型	威胁	来源
技术失效	设备失效	A
	设备故障	A
	信息系统饱和	A、D
	软件故障	A
	信息系统可维护性破坏	A、D
未授权行为	未授权的设备使用	D
	软件的伪造复制	D
	假冒或盗版软件使用	A、D
	数据损坏	D
	数据的非法处理	D
功能损害	使用中的错误	A
	权限滥用	A、D
	权限伪造	D
	行为否认	D
	人员可用性破坏	A、D、E

宜特别注意人为威胁源。对此表 C.2 具体地逐项列出。

表 C.2　人为威胁源示例

威胁源	动　机	威胁行为
黑客、解密高手	挑战； 自负； 叛乱； 地位； 金钱	● 黑客行为； ● 社会工程(欺骗)； ● 系统入侵、入室盗窃； ● 未授权的系统访问
计算机犯罪	信息销毁； 信息非法泄露； 金钱利益； 未授权的数据更改	● 计算机犯罪(例如，网际盯梢)； ● 欺诈行为(例如，重放、假扮，拦截)； ● 信息贿赂； ● 欺骗； ● 系统入侵
恐怖分子	勒索； 摧毁； 非法利用； 复仇； 政治利益； 媒体报道	● 炸弹/恐怖主义； ● 信息战； ● 系统攻击(例如，分布式拒绝服务)； ● 系统渗透； ● 系统篡改

表 C.2（续）

威胁源	动　机	威胁行为
工业间谍 （情报机构、公司、外国政府、其他政府利益集团）	竞争优势； 经济侦探	● 国防优势； ● 政治优势； ● 经济剥削； ● 信息窃取； ● 个人隐私侵犯； ● 社会工程（欺骗）； ● 系统渗透； ● 未授权的系统访问（访问涉密的、专有的和（或）技术相关的信息）
内部人员 （缺乏训练的、心怀不满的、恶意的、疏忽的、不诚实的或终止劳动关系的雇员）	好奇心； 自负； 情报； 金钱利益； 复仇； 无意的错误和遗漏（例如，数据输入错误、编程错误）	● 袭击雇员； ● 勒索； ● 浏览的专有信息； ● 计算机滥用； ● 诈骗和盗窃； ● 信息贿赂； ● 伪造和损坏数据的输入； ● 拦截； ● 恶意代码（例如，病毒、逻辑炸弹、特洛伊木马）； ● 个人信息出售； ● 系统错误； ● 系统入侵； ● 系统破坏； ● 未授权的系统访问

附 录 D
（资料性附录）
脆弱性和脆弱性评估方法

D.1 脆弱性示例

表 D.1 给出在各种安全领域中脆弱性的示例，包括可能利用这些脆弱性的威胁示例。该列表能够在威胁和脆弱性评估中提供帮助，来确定相关事件场景。值得强调的是，在某些场合，其他威胁同样可能利用这些脆弱性。

表 D.1 脆弱性示例

类型	脆弱性示例	威胁示例
硬件	存储介质的维护不足/错误安装	信息系统可维护性破坏
	定期更换计划的缺乏	设备或介质毁坏
	对潮湿、灰尘、污染的敏感性	灰尘、腐蚀、冻结
	对电磁辐射的敏感性	电磁辐射
	有效配置变更控制的缺乏	使用中的错误
	对电压变化的敏感性	电力供应失去
	对温度变化的敏感性	气候现象
	未保护的存储器	介质或文件偷窃
	废物谨慎处置的缺乏	介质或文件偷窃
	未控制的复制	介质或文件偷窃
软件	软件测试的缺失或不足	权限滥用
	软件中众所周知的缺陷	权限滥用
	离开工作站时未“退出”	权限滥用
	未适当擦除的存储介质的废弃或再使用	权限滥用
	审计跟踪的缺乏	权限滥用
	访问权限的错误分配	权限滥用
	广泛分布的软件	数据损坏
	将应用程序在时间意义上用到错误的数据	数据损坏
	复杂的用户界面	使用中的错误
	文件化的缺乏	使用中的错误
	不正确的参数设置	使用中的错误
	不正确的日期	使用中的错误
	标识与鉴别机制（如用户鉴别）的缺乏	权限伪造
	未保护的口令表	权限伪造

表 D.1（续）

类型	脆弱性示例	威胁示例
软件	糟糕的口令管理	权限伪造
	不必要的服务开启	数据的非法处理
	不成熟或新的软件	软件故障
	不清晰或不完整的开发者规范	软件故障
	有效变更控制的缺乏	软件故障
	未控制的软件下载和使用	软件篡改
	备份的缺乏	软件篡改
	建筑物和门窗物理保护的缺乏	介质或文件偷窃
	未能出示管理报告	未授权的设备使用
网络	发送或接收消息证据的缺乏	行为否认
	未保护的通信线路	窃听
	未保护的敏感通信	窃听
	糟糕的联合布线	电信设备故障
	单点故障	电信设备故障
	发送者和接受者的标识与鉴别的缺乏	权限伪造
	不安全的网络体系结构	远程侦探
	口令明文传输	远程侦探
	不足的网络管理(路由的恢复力)	信息系统饱和
	未保护的公共网络连接	未授权的设备使用
人员	人员缺席	人员可用性破坏
	不足的招聘规程	设备或介质毁坏
	不足的安全培训	使用中的错误
	软件和硬件的不正确使用	使用中的错误
	安全意识缺乏	使用中的错误
	监督机制缺乏	数据的非法处理
	对外部或清洁人员的工作无监督	介质或文件偷窃
	电信介质和通讯的正确使用策略缺乏	未授权的设备使用
场所	建筑物和房间物理访问控制使用的不足或疏忽	设备或介质毁坏
	位于洪水多发地区	洪水
	不稳定的电网	电力供应失去
	建筑物和门窗物理保护的缺乏	设备偷窃

表 D.1（续）

类型	脆弱性示例	威胁示例
组织	用户注册和注销的正式规程缺乏	权限滥用
	访问权限审查(监督)的正式过程缺乏	权限滥用
	与客户和(或)第三方合同中安全规定缺乏或不足	权限滥用
	信息处理设施的监视规程缺乏	权限滥用
	定期审计(监督)缺乏	权限滥用
	风险识别和评估规程缺乏	权限滥用
	管理员和操作员日志中记录的故障报告缺乏	权限滥用
	不足的服务维护响应	信息系统可维护性破坏
	服务水平协议(SLA)缺乏或不足	信息系统可维护性破坏
	变更控制规程缺乏	信息系统可维护性破坏
	ISMS 文件化控制的正式规程缺乏	数据损坏
	ISMS 记录监督的正式规程缺乏	数据损坏
	公开可用信息授权的正式过程缺乏	来自不可信源的数据
	信息安全责任的适当分配缺乏	行为否认
	持续性计划的缺乏	设备失效
	电子邮件使用策略的缺乏	使用中的错误
	在运行系统中引入软件的规程缺乏	使用中的错误
	管理员和操作员日志中的记录缺乏	使用中的错误
	涉密信息处理的规程缺乏	使用中的错误
	职位描述中信息安全责任缺乏	使用中的错误
	与雇员的合同中信息安全规定缺乏或不足	数据的非法处理
	对信息安全事件缺乏明确的纪律过程	设备偷窃
	移动计算机使用的正式策略缺乏	设备偷窃
	组织辖区外资产的控制缺乏	设备偷窃
	“清空桌面和清空屏幕”策略缺乏或不足	介质或文件偷窃
	信息处理设施授权的缺乏	介质或文件偷窃
	对安全破坏的监视机制缺乏	介质或文件偷窃
	定期管理评审的缺乏	未授权的设备使用
	报告安全弱点的规程缺乏	未授权的设备使用
	遵守知识产权规定的规程缺乏	未授权的设备使用

D.2 技术脆弱性评估方法

诸如信息安全测试这样的主动方法可被用于识别脆弱性，这随信息与通信技术(ICT)的关键性和

可用资源(例如,分配的资金、可用的技术、具有专门技能进行测试的人员)而定。测试方法包括:

- 自动脆弱性扫描工具;
- 安全测试和评价;
- 渗透测试;
- 代码审查。

自动脆弱性扫描工具被用于扫描主机群或网络中已知的易受攻击服务(例如,系统允许匿名文件传输协议(FTP)、邮件中继)。然而,宜注意到自动扫描工具识别的某些潜在脆弱性在系统环境的语境下可能并非真正的脆弱性。例如,这些扫描工具中的一些在评估潜在脆弱性时并没有考虑场所的环境和要求。被自动扫描软件标记为脆弱性中的一些对特定场所可能实际上不是脆弱性,而可能是其环境需要那种配置。因此,这种测试方法可能误报。

安全测试与评价(STE)是另一种可被用于风险评估过程中识别 ICT 系统脆弱性的技术。它包括测试计划(例如,测试脚本、测试规程和期望的测试结果)的开发和执行。系统安全测试的目的是测试 ICT 系统的安全控制措施被应用在运行环境中的有效性。目标是确保所应用的控制措施满足被批准的软件和硬件安全规范,并实现组织的安全策略或满足行业标准。

渗透测试可被用于补充安全控制措施的审查和确保 ICT 系统的不同方面是安全的。当用在风险评估过程中时,渗透测试可被用于评估 ICT 系统低档故意绕过系统安全企图的能力。其目标是从威胁源的视角测试 ICT 系统,并识别 ICT 系统保护方案中的潜在问题。

代码审查是最彻底的(但也是最昂贵的)脆弱性评估方法。

这些安全测试类型的结果将帮助识别系统的脆弱性。

重要的是要注意到渗透工具和技术可能给出错误的结果,除非脆弱性被成功利用。为了利用特定脆弱性,需要知道被测系统上确切的系统/应用/补丁设置。如果在测试时不知道这些数据,就不太可能成功地利用特定脆弱性(例如,获得远程反向 shell);然而,仍可能损毁或重启被测过程或系统。在这种情况下,被测对象宜同样被视为脆弱的。

评估方法可能包括下列活动:

- 访谈人员和用户;
- 问卷调查;
- 物理检查;
- 文件分析。

附 录 E
（资料性附录）
信息安全评估方法

E.1 高层信息安全风险评估

高层评估为定义行动的优先级和时间顺序提供可能。由于各种原因，诸如预算，不太可能同时实施所有控制措施，只有最关键的风险能通过风险处置过程来解决。同样，如果一两年后才打算实施控制措施，开始详细风险管理可能太早。为达到上述目标，高层评估可从后果的高层评估开始，而不是一开始就进行威胁、脆弱性、资产和后果的系统分析。

从高层评估开始的另一个原因是与关系到变更管理（或业务持续性）的其他计划同步。例如，完全地保护一个计划在不久将来外包的系统或应用是不明智的，尽管为了确定外包合同仍值得进行风险评估。

高层风险评估这一轮的特性可能包括：

- 高层风险评估可关注组织及其信息系统更全局的一面，将技术方面作为独立于业务问题来考虑。这样，语境分析更集中在业务和操作环境而非技术要素。
- 高层风险评估可关注属于所确定域的更有限的威胁和脆弱性列表，或者，为了加速评估过程，可聚焦于风险或攻击场景而非它们的要素。
- 在高层风险评估中呈现的风险常常是更一般的风险领域而非特定的被识别风险。由于场景或威胁按域进行组织，风险处置按域提出控制措施列表的建议。因而，风险处置活动首先试图建议和选择对整个系统有效的共同控制措施。
- 然而，因为很少关注技术细节，高层风险评估更适合提供组织的和非技术的控制措施以及技术控制措施的管理方面，或者关键和共同的技术性安全措施（诸如备份和抗病毒）。

高层风险评估的益处如下：

- 并入最初的简单方法很可能获得风险评估计划的认可。
- 有可能建立组织信息安全计划的战略蓝图，即这将有助于良好的规划。
- 资源和资金能够被用于最有效益的地方，并且可能最需要保护的系统会被首先关注到。

由于初始风险分析是在高层且可能不太准确，唯一的潜在不利是某些业务过程或系统可能没被识别出，因此需要第二轮、详细的风险评估。如果有了关于组织及其信息和系统的所有方面的足够信息，包括从信息安全事件评估中获得的信息，这种不利可能避免。

高层风险评估考虑信息资产的业务价值和从组织业务视角的风险。在第一次决策点（见图 1），几个因素帮助决定高层评估对处理风险是否足够；这些因素可能包括如下方面：

- 通过使用各种信息资产达成的业务目标；
- 组织业务依赖每项信息资产的程度，即组织认为对其生存或有效开展业务的关键功能是否依赖每项资产，或者资产所存储和处理的信息的保密性、完整性、可用性、抗抵赖性、可核查性、真实性和可靠性；
- 在开发、维护或更新资产方面对每项资产上投资程度；
- 被组织直接赋予价值的信息资产。

当这些因素被评估时，决定就变得更容易。如果资产的目标对组织开展业务极为重要，或者资产处在高风险，则宜对特定信息资产（或资产的部分）进行第二轮、详细风险评估。

适用的一般规则是：如果信息安全的缺乏可能导致对组织或其业务过程或其资产的严重不良后果，

则有必要在更详细的程度上进行第二轮风险评估以识别潜在风险。

E.2 详细信息安全风险评估

详细信息安全风险评估过程包括资产的深层识别和估价、对这些资产的威胁的评估和脆弱性的评估。然后,这些活动的结果用于评估风险和识别风险处置。

详细评估步骤通常需要相当的时间、精力和专门技能,并因此可能是最适合处于高风险的信息系统。

详细信息安全风险评估的最终阶段是评估整体风险,这是本附录的重点。

后果可能以几种方式被评估,包括使用定量(例如,货币)和定性(可基于诸如中等或严重这样的形容词)的测度,或者两者的组合。为了评估威胁发生的可能性,宜建立资产具有价值或需要保护的时限。特定威胁发生的可能性受如下因素影响:

- 资产的吸引力或可能影响,适用于考虑故意人为威胁时;
- 利用资产脆弱性获得收益的容易度,适用于考虑故意人为威胁时;
- 威胁发起者的技术能力,适用于故意人为威胁;
- 脆弱性易被利用的程度,适用于技术和非技术脆弱性。

许多方法使用表格,并组合主观和经验测度。重要的是,组织使用对其适用的、使其有信心的和产生可重复结果的方法。下面给出几个基于表格的技术示例。

E.2.1 示例 1:具有预定义值的矩阵

在这种类型的风险评估方法中,实际或建议的物理资产以更换或重建成本来估价(即定量测量)。然后将这些成本转换成用于估价信息的同等定性尺度(见下面)。实际或建议的软件资产以与物理资产同样的方式来估价,即识别购置或重建成本,然后转换成用于估价信息的同等定性尺度。另外,如果发现任何应用软件对保密性或完整性具有自身内在的要求(例如,源代码本身是商业敏感的),则以与信息同样的方式来估价。

信息的价值通过选择能权威地谈论数据的业务管理者(即“数据负责人”)进行访谈来获得,从而决定数据在实际使用、存储、处理或访问中的价值和敏感性。访谈帮助从最坏场景方面评估信息的价值和敏感性,最坏场景完全可能因未授权泄露、未授权修改、各种时段的不可用和毁坏导致不良业务后果而发生。

信息估价使用信息估价指南来完成,涉及的问题诸如:

- 人身安全;
- 个人信息;
- 法律法规和规章制度义务;
- 执法;
- 商业和经济利益;
- 财务损失/活动中断;
- 公共秩序;
- 业务策略和运营;
- 声誉损失;
- 与客户的合同或协议。

信息估价指南帮助以数字尺度识别信息价值,诸如下面的矩阵例子中所示的 0～4 尺度,从而使识别可能的、逻辑的定量值和识别定量值不可能的定性值(例如,对人生命的危害)成为可能。

接下来的主要活动是完成每种威胁类型以及与某种威胁类型相关的每组资产的成对调查问卷,使

得对威胁等级(发生的可能性)和脆弱性等级(被威胁利用引起不良后果的容易度)的评估成为可能。每个问题答案得出一个评分。这些评分通过知识库被积累并与值域比较。这样将威胁等级识别为高至低的尺度,脆弱性等级也是类似,如表 E.1 矩阵例子所示,后果类型之间的差别是相对的。宜汇总来自适当的技术、人事和后勤部门人员的访谈,以及物理位置查看和文件审查的信息来完成调查问卷。

将与每种后果类型相关的资产价值以及威胁和脆弱性等级,同下面所示的这种矩阵进行匹配,从而为每个组合在 0～8 的尺度上识别相关的风险测度。这种风险值以有序的方式布置在矩阵中。下面给出了一个示例(见表 E.1):

表 E.1

威胁发生的可能性		低			中			高		
脆弱性利用的容易度		低	中	高	低	中	高	低	中	高
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

对于每项资产,相关脆弱性和这些脆弱性的相应威胁被考虑。如果一个脆弱性没有相应威胁,或者一个威胁没有相应脆弱性,则目前并没有风险(但是宜小心这种情形的变化)。这里用资产价值识别矩阵中适当的行,用威胁发生的可能性和脆弱性利用的容易度识别适当的列。例如,如果资产价值为 3,威胁为“高”,脆弱性为“低”,则风险测度为 5。假定资产价值为 2,威胁(例如,修改)等级为“低”,脆弱性利用容易度为“高”,则风险测度为 4。矩阵规模,威胁可能性、脆弱性利用容易度和资产估价等级类别的数量,可根据组织的需要进行调整。额外的列和行将需要额外的风险测度。这种方法的价值在于排列所关注的风险。

如表 E.2 所示的一个类似矩阵的结果是来自将事件场景的可能性与估算的业务影响联系起来这种考虑而得到的。事件场景的可能性由威胁利用脆弱性的某种可能性给出。该表将这种可能性与事件场景相关的业务影响联系起来。风险结果以 0～8 的尺度来测量,并可对照风险接受准则来评价。这种风险尺度还可能被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。

表 E.2

事件场景的可能性		很低 (极不可能)	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:由风险测度排列威胁

如表 E.3 所示的矩阵或表格可被用于将后果(资产价值)和威胁发生可能性(考虑到脆弱性方面)两因素进行关联。第一步是以一个预先为受到威胁的每项资产定义的尺度(例如,1～5)评估后果(资产价值)(表中“b”列)。第二步是以一个预先为每个威胁定义的尺度(例如,1～5)评估威胁发生的可能性(表中“c”列)。第三步是通过相乘(b×c)计算风险测度。最后,威胁可按照其相关的风险测度来排列。注意,在这个示例中,1 被视作最低后果和最低发生可能性。

表 E.3

威胁描述符 (a)	结果(资产)值 (b)	威胁发生的可能性 (c)	风险测度 (d)	威胁排序 (e)
威胁 A	5	2	10	2
威胁 B	2	4	8	3
威胁 C	3	5	15	1
威胁 D	1	3	3	5
威胁 E	4	1	4	4
威胁 F	2	4	8	3

如表 E.3 所示,这一规程允许具有不同后果和发生可能性的不同威胁进行比较和按照优先顺序排列。在某些情况下,有必要将货币价值与这里使用的经验尺度进行关联。

E.2.3 示例 3:评估风险的可能性和可能后果的值

在这个示例中,重点放在信息安全事件的后果(即事件场景)和决定哪个系统宜给予高优先级。这是通过评估每项资产和风险这两个值,组合后决定每项资产的评分。当系统的所有资产评分加起来后,该系统的风险测度便被决定了。

首先,为每项资产赋一个值。该值与资产受到威胁时可能引起的潜在不良后果相关。对于每个威胁适用的资产,都为该资产赋予这样一个资产值。

然后评估可能性值。这是通过威胁发生的可能性和脆弱性利用的容易度组合来评估,见表示事件场景可能性的表 E.4。

表 E.4

威胁的可能性	低			中			高		
脆弱性的程度	低	中	高	低	中	高	低	中	高
事件场景的可能性值	0	1	2	1	2	3	2	3	4

接下来,通过在表 E.5 中找到资产值和可能性值的交叉点来赋予资产/威胁评分。资产/威胁评分的合计产生一个资产总评分。这个数字可被用于区分组成系统各部分的资产。

表 E.5

资产值		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

最后一步是合计系统各项资产的所有资产总评分，产生系统评分。这个评分可被用于区分系统和决定哪个系统保护宜给予高优先级。

在下面的例子中，所有值都是随机选取的。

假设系统S有三项资产A1、A2、和A3。还假设存在适用于该系统的两种威胁T1和T2。设A1值为3，同样地，设A2值为2，A3值为4。

如果对A1和T1来说，威胁可能性为低，脆弱性利用的容易度为中，则可能性值为1(见表E.4)。

资产/威胁评分A1/T1可从表E.5导出，也就是资产值3和可能性值1的交叉点，即为4。同样地，对A1/T2，设威胁可能性为中，脆弱性利用的容易度为高，则得出A1/T2评分为6。

至此可以计算资产总评分A1T，即为10。对每项资产和适用威胁计算其资产总评分。系统总评分ST通过相加(A1T＋A2T＋A3T)计算得出。

至此可以比较不同系统来建立优先级，对于一个系统中的不同资产也是同样。

上述例子是针对信息系统的，然而类似的方法可适用于业务过程。

附 录 F
（资料性附录）
风险降低的约束

当考虑风险降低的约束时，宜考虑下列约束：

时间约束：

可能存在许多类型的时间因素。例如，控制措施宜在对组织管理者可接受的时间段内实施。另一种类型的时间约束是控制措施能在信息系统的生存周期内得到实施。第三种类型的时间约束可能是组织管理者决定的暴露在特定风险中的可接受时间段。

财政约束：

控制措施的实施或维护不宜比其要防范的风险值更昂贵，除非是强制的合规要求（例如，符合法律法规）。每一努力都不宜超过所分配的预算，并宜通过控制措施的使用实现的财政利益。但是，在某些情况下由于预算的约束或许不可能达到期望的安全和风险接受程度。因此，这取决于组织管理对解决这种情形的决定。

宜十分注意因预算减少所要实施的控制措施数量或质量而可能导致隐含保留超出计划的更大风险。为控制措施建立的预算宜充分考虑后才用作限制因素。

技术约束：

如果在控制措施选择过程中加以考虑，技术问题（如程序或硬件的兼容性）可容易避免。此外，对现有过程或系统追加实施控制措施往往受到技术约束的妨碍。这些困难可能改变控制措施在安全的规程和物理方面的平衡。为实现安全目标可能有必要修改信息安全计划。这可能发生在控制措施达不到不降低生产力的前提下减小风险的期望结果。

运行约束：

运行约束（诸如需要 24×7 运行且还要完成备份）可能导致控制措施实施的复杂性和高成本，除非从一开始就在设计中考虑到了。

文化约束：

选择控制措施的文化约束对于一个国家、一个行业、一个组织或者甚至组织内的一个部门可能是特定。不是所有控制措施能够适用于所有国家。例如，执行提包搜查在部分欧洲国家也许是可能的，但在部分中东国家却不可能。文化方面不能忽视，因为许多控制措施依赖员工的主动支持。如果员工不理解控制措施的需要或没有找到其在文化上的可接受性，控制措施将随时间变得无效。

伦理约束：

由于伦理基于社会规范而变化，伦理约束可能对控制措施构成重大问题。这可能阻止实施控制措施，诸如在某些国家的电子邮件扫描。信息的隐私保护也可能根据地区或政府的伦理而变化。这些可能在某些行业比其他行业更受到关注，例如，政府和医疗保健。

环境约束：

环境因素可能影响控制措施的选择，诸如空间的可用性、极端的气候条件、周围的自然环境和城市地理。例如，抗震可能在某些国家需要，而在另一些国家则不必要。

法律约束：

诸如针对信息处理的个人数据保护或刑法规定这样的法律因素可能影响控制措施的选择。法律法规和规章制度的符合性可能强制某些类型的控制措施，包括数据保护和财务审计；也可能阻止某些控制措施的使用，例如，加密。其他法律法规和规章制度，诸如劳动关系法、消防部门/卫生与安全部门/经济

部门规章等,同样可能影响控制措施的选择。

易用性:

不佳的人与技术接口将导致人为错误并可能使控制无效。宜选择在达到业务残余风险的可接受程度的同时,提供最佳易用性的控制措施。难以使用的控制措施将影响它们的有效性,因为用户可能试图尽量绕过或忽视它们。组织内复杂的访问控制措施可能促使用户寻找替代的、未授权的访问方法。

人员约束:

宜考虑实施控制措施的专门技能的可用性和薪金成本,以及在处于不利操作条件下的场所之间调动员工的能力。可能没有现成可用的专门技能来实施计划的控制措施,或者专门技能可能对组织过于昂贵。其他方面,诸如某些员工歧视没有经过安全审查的其他员工,可能对安全策略和实践构成重大问题。同样,雇用合适人员工作的需要和找到合适人员可能导致完成安全审查后才能雇用。在雇用前完成安全审查的要求是正常的和最安全的实践。

整合新的和现有控制措施的约束:

在现有基础设施中整合新的控制措施和控制措施之间的相互依赖常常被忽视。如果新的控制措施不适宜或与现有控制措施不兼容,则可能不易被实施。例如,物理访问控制使用生物令牌的计划可能引起与现有基于密码键盘(PIN-pad)进行访问控制的系统冲突。将现有控制措施改变为计划的控制措施的成本宜包括在风险处置总成本之中。实施与当前控制措施冲突的被选控制措施是不太可能的。

参 考 文 献

[1] ISO/IEC Guide 73:2002,Risk management—Vocabulary—Guidelines for use in standards(风险 词汇 在标准中的使用指南)

[2] ISO/IEC 16085:2006,Systems and software engineering—Life cycle processes—Risk management(系统和软件工程 生存周期过程 风险管理)

[3] AS/NZS 4360:2004,Risk Management(风险管理)

[4] NIST Special Publication 800-12,An Introduction to Computer Security:The NIST Handbook(计算机安全介绍:NIST 手册)

[5] NIST Special Publication 800-30,Risk Management Guide for Information Technology Systems,Recommendations of the National Institute of Standards and Technology(信息技术系统的风险管理指南,美国国家标准与技术研究所建议)

中 华 人 民 共 和 国
国 家 标 准
信息技术　安全技术
信息安全风险管理
GB/T 31722—2015/ISO/IEC 27005：2008
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址：www.gb168.cn
服务热线：400-168-0010
010-68522006
2015 年 6 月第一版
*
书号：155066・1-51115

GB/T 31722-2015