信息技术—安全技术—信息安全管理—测量

27004 N6614 (FCD)

标准草案

目录

0 介绍

0.1 概述

本国际标准就测度和测量的开发和使用提供了指南和建议，以评估信息安全管理体系（ISMS）的有效性，包括ISO/IEC 27001中用来实施和管理信息安全的ISMS策略、控制目标和安全控制措施。

通过使用信息安全测度，组织能识别现有信息安全管理体系的充分性，包括策略、风险管理、控制目标、控制措施、过程和规程，并支持组织进行过程的修订，决定哪些ISMS过程或控制措施应该变更和改进。

对该方法的实施组成了一个信息安全测量项目。信息安全测量项目将帮助管理层识别和评价不符合和无效的控制措施，以及排列与这些控制措施改进或变更相关行动的优先次序。测量项目也能帮助组织展示与ISO/IEC 27001标准的符合程度，并能产生管理评审过程的输入。

对信息安全测量项目的实施，应该优先保证向利益相关方提供了关于各种最严重（或是最高优先级别）风险及其处置/控制措施状态的可靠信息。本国际标准假定开发测量的起点是对组织和利益相关方所面临信息安全风险的充分理解，并且风险评估过程已经按照ISO/IEC 27001要求得到了正确地实施。

一个有效的信息安全测量项目应改进利益相关方对可提供状态信息的各种测量的信心，并使利益相关方能使用这些测量有效持续改进信息安全和信息安全管理体系。

本国际标准的使用能够支持对一段时间内信息安全目标达成情况的比较，以作为组织信息安全管理体系持续改进过程的一部分。

本指南包括：

a) 开发测度；

b) 实施和运行一个信息安全测量项目；

c) 向利益相关方收集、分析和沟通测度；

d) 使用所收集的测度来帮助信息安全管理体系的相关决策；

e) 使用所收集的测度来有效改进信息安全管理体系的控制目标和控制措施；

f) 促进信息安全测量项目的持续改进。

本国际标准提供了模板，可能对测量的管理有所帮助。

0.2 管理层概述

ISO/IEC 27001 要求管理层“定义怎样测量所选择的一个或一组控制措施的有效性，并指明这些测度是怎样被用来评估控制措施有效性，以产生可比较和可再现的结果。”

公认地，根据多种因素，包括风险暴露、规模、资源可用性、能力、行为和部门需求的不同，被组织采用来测量控制措施有效性的方法也有所不同。仔细地选择和证明所使用的方法是很重要的，这可以保证过多的资源不被投入到信息安全管理体系中某个方面，从而损害到其它必要的领域。明智地，应该将控制措施有效性测量纳入到组织的日常运作中，包括最小的附加资源需求，以满足对测量的持续需求。

对所有组织来说，基本规程的要求已概括在0.1（指南列表）中。然而，某个因素（如系统规模）可能影响组织测量控制措施有效性。一般而言，业务的规模和复杂度，及其与信息安全重要性的组合，将影响所需测量的扩展程度，无论是测度数量还是测量频度。中小企业可以实施基本理解意义上的信息安全测量项目，而大企业则可能多个信息安全测量项目。

在初始实施和适当改进措施被实施后，整个测量过程应该被评审。

本国际标准的使用将提供适当的文档和支持，这将有助于展示控制措施有效性正在被测量和评估。

1 范围

本国际标准为开发和使用测量提供了指南，以评估ISO/IEC 27001中所描述的信息安全管理体系（ISMS）过程、控制目标以及控制措施的有效性。

本国际标准适用于任何类型和规模的组织。

2 规范性引用

以下的引用文档对本文的应用是不可缺少的。对那些标有日期的引用，只有该引用的版本才适用。对于没有标日期的引用，应使用最新版本（包括任何修正文档）。

- ISO/IEC 27001，信息技术——安全技术——信息安全管理体系－－要求

3 术语和定义

以下术语和定义适用于本标准：

3.1

测量分析模型 analytical model for measurement

分析模型 analytical model

将一个或多个基本测度和/或导出测度与相关决策准则组合在一起的算法或计算。

3.2

属性 attribute

可由人或自动化工具定量或定性辨别的实体特征或特性。[ISO/IEC 15939:2007]

3.3

基本测度 base measure

用某个属性及其量化方法定义的测度。[ISO/IEC 15939:2007]

注1：一个基本测度在功能上独立于其它测度。

3.4

控制措施 control

管理风险的方法，包括策略、规程、指南、惯例或组织结构。它们可以是行政、技术、管理、法律等方面的。[ISO/IEC 27002:2005]

注：控制措施也用于防护措施或对策的同义词。

3.5

数据 data

赋予基本测度、导出测度和（或）指标的值的集合。[ISO/IEC 15939:2007]

3.6

决策准则 decision criteria

用于确定是否需要行动或进一步调查的，或者用于描述给定结果置信度的阈值、目标或模式。[ISO/IEC 15939:2007]

3.7

导出测度 derived measure

定义为两个或两个以上基本测度的函数的测度。[ISO/IEC 15939:2007]

3.8

指标 indicator

对由规定信息需要的相关模型导出的指定属性提供估算或评价的测度。[ISO/IEC 15939:2007]

3.9

信息需要 information need

为管理目标、目的、风险和问题所必需的见解。[ISO/IEC 15939:2007]

3.10

信息安全管理体系 information security management system (ISMS)

整体管理体系的一部分，基于业务风险方法，建立、实施、运行、监控、核查、维持和改进信息安全[ISO/IEC 27001: 2005]。

注：管理系统包括组织结构，策略，计划活动，责任，实践，规程，过程和资源。

3.11

ISMS有效性 ISMS effectiveness

信息安全活动满足组织目标的程度。

注：在本标准中，效率仅关注于控制措施的有效性。

3.12

测度 Measure

一个变量，该变量被赋值，作为执行一次测量的结果。[ISO/IEC 15939:2007]

注：术语”measures” 用来指基本测度、导出测度，以及指标。

3.13

测量 measurement

一个过程，包括信息安全管理体系和用以实现控制目标的控制措施的有效性，以及信息安全管理体系各过程性能相关信息的获取，以及测量方法、测量函数、测量模型及测量准则的使用。

3.14

测量函数 measurement function

为组合两个或两个以上基本测度而执行的算法或计算。[ISO/IEC 15939:2007]

3.15

测量方法 measurement method

一般地描述为，用于以指定的标度量化属性的逻辑操作序列。[ISO/IEC 15939:2007]

注：测量方法类型取决于用来量化属性的操作的性质。可分为两种类型：

主观类－－涉及人为判断的量化；

客观类－－基于数字规则的量化。

3.16

测量结果 measurement results

针对信息安全需求的一个或多个指标及其相关的解释。

3.17

对象 object

一个对象通过对其属性的测量得以识别

3.18

标度 scale

一组有序的连续或离散值，或与属性映射的类目。[ISO/IEC 15939:2007]

注：标度类型取决于标度值间关系的性质，通常定义四种类型的标度：

标称标度－－测量值是类目；

顺序标度－－测量值是队列；

间隔标度－－测量值的等距与属性的等量对应；

比率标度－－测量值的等距与属性的等量对应，其中零值对应于无属性。

3.19

测量单位 unit of measurement

按约定定义和采用的具体量，其他同类量与这个量进行比较，用以表示它们相对于这个量的大小。[ISO/IEC 15939:2007]

3.20

确认~~证实~~ validation

通过提供客观证据，证实对某个有意使用或应用的需求已经得到满足。

3.21

验证 verification

通过提供客观证据，证实特定的要求已经得到满足。

注：也称为符合性测试

4 本标准的结构

除了为开发和使用测量提供了指南，以评估ISO/IEC 27001中所描述的信息安全管理体系（ISMS）过程、控制目标以及控制措施的有效性外，本国际标准还提供了对测量过程及其活动的描述。

对信息安全测量项目及其模型的概述和背景信息见第5节。管理职责见第6节。第7节到第10节描述了测量项目中的各过程（详见5.2）。

如何开发和记录测量的附加信息见附录。附录A提供了测量模板的范例，附录B提供了使用附录A中模板的测量范例。

5 信息安全测量概述

5.1 信息安全目标

在信息安全管理体系背景下，测量项目的目标可以包括：

a) 评价所实施信息安全控制目标和控制措施的有效性；

b) 评价信息安全管理体系有效性，包括持续改进循环；

c) 基于组织整体业务风险，促进信息安全的性能改进；

d) 提供客观数据和分析，来帮助管理评审、辅助决策，以及向管理层证明控制措施的改进；

e) 为安全审核提供输入；

f) 向相关的利益相关方沟通信息安全的有效性；

g) 作为风险管理过程的输入；

h) 为对有效性的内部比较和内部打分提供信息；以及

i) 支持对所识别安全需求满足到何种程度的验证。

一个特定组织的测量项目应当基于大量的考虑，包括：

a) 在支持组织整体业务活动和所面临的风险方面，信息安全所扮演的角色；

b) 基于客观测量的持续改进；

c) 适用的法律、规章，以及合同要求；

d) 组织的架构；

e) 实施信息安全测量的成本和收益；以及

f) 组织对风险的接受态度。

图1 解释了与ISO/IEC 27001中描述的PDCA循环相比，测量活动的输入－输入循环关系。

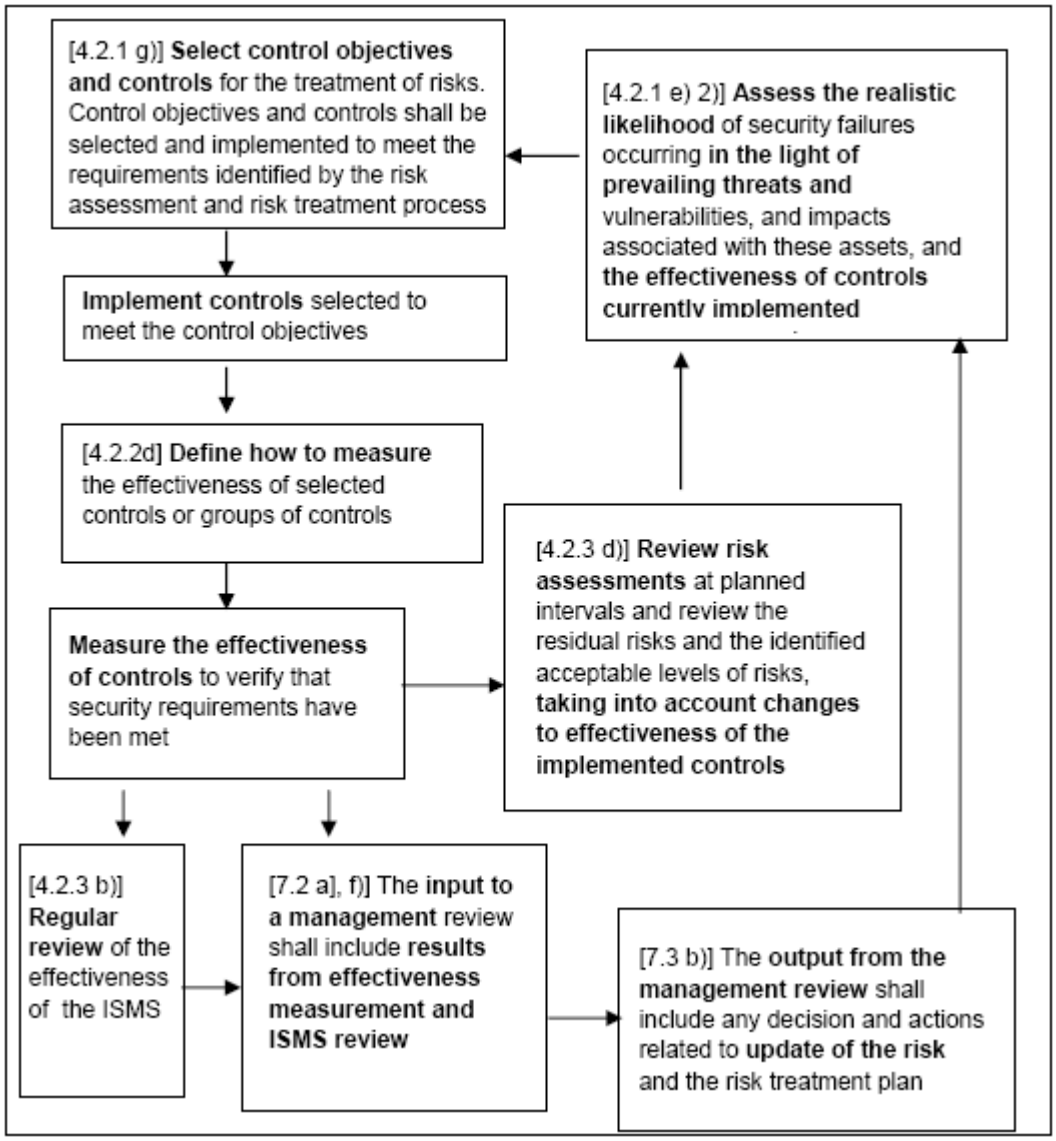

图1 PDCA循环中的测量输入与输出

为了达到信息安全测量所建立的目标，并在所有测量活动中实施PDCA循环，组织应该建立并管理一个信息安全测项目（见5.2）。为获得基于信息安全测量模型（见5.3）的可重复的、客观的和有用的结果，组织还应建立一个测量活动框架。

5.2 信息安全测量项目

一个信息安全测量项目通过使用测度，识别和评价信息安全管理体系的充分性和有效性，并对改进现有控制措施和整体信息安全管理体系的需求进行识别。

为了策划和组织多种和大量的测量，并为在一个指定的时间段和/或时期内有效和高效地执行测量提供资源，一个测量项目包括了所有必要的活动。组织可以建立一个以上的测量项目。

管理层应该为测量项目建立角色和职责。

一个测量项目应包括以下过程：

a) 测度和测量的开发（见第7节）；

b) 测量的运行（见第8节）；

c) 测度的分析和报告（见第9节）；以及

d) 测量项目改进（见第10节）。

图2展示了测量项目管理的过程流。

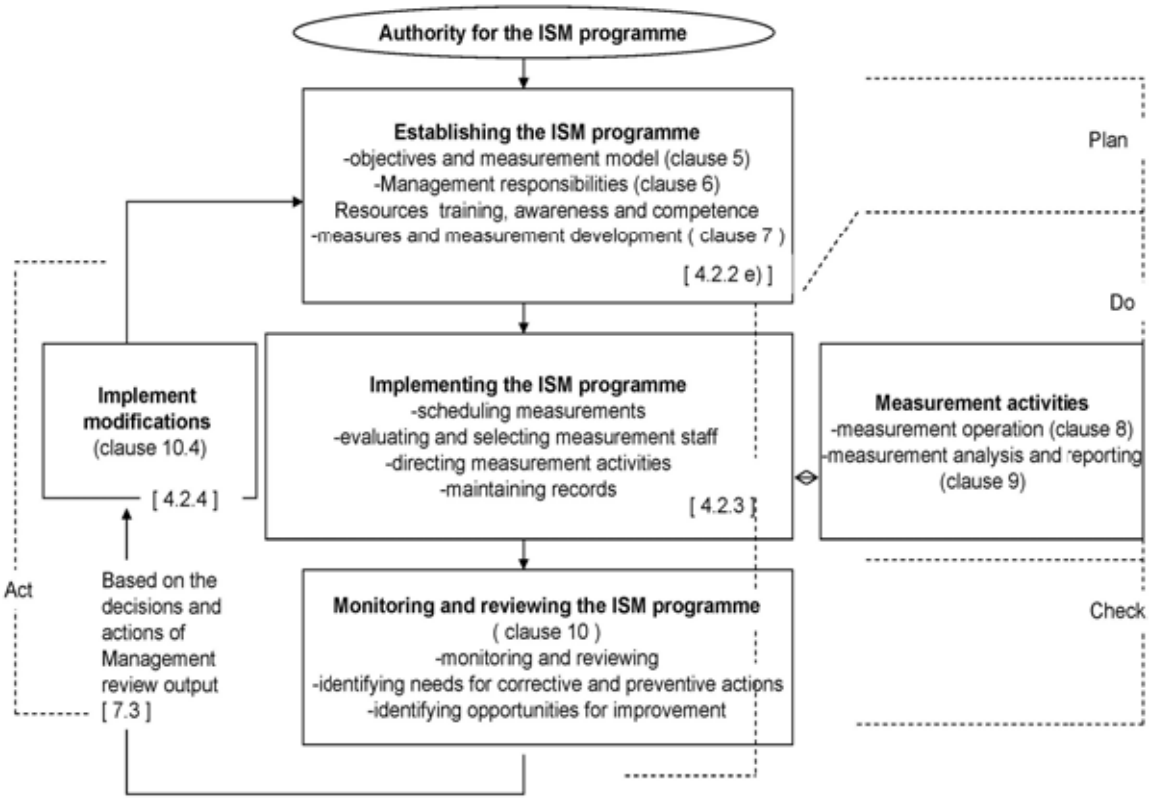

图2 测量项目管理过程流示意图

通过测量的使用——信息安全测量项目的一个关键元素，可以对现有控制措施和过程进行评价来确定这些控制措施和过程是否充分和有效，或是这些控制措施和过程是否需要被改进或变更，从而改进整个信息安全管理体系。

为了成功达成信息安全管理体系的持续改进，信息安全测量项目应当考虑，例如，以下要素的适当组合：

a) 管理层的承诺并有适当资源支持；

b) 信息安全管理体系各过程和规程的存在；

c) 能够捕获和报告有意义数据的过程；

d) 基于信息安全管理体系目标的定量安全测度；

e) 易于获取和测量的定量安全测度；

f) 一个可重复的过程，以提供一段时间的相关趋势；

g) 一个有用的追踪过程，以支持有效地调配资源；

h) 以一种有意义的方式，一致、定期地收集、分析和报告测量数据；

i) 利益相关方使用信息安全管理体系测量结果，来改进现有信息安全管理体系过程和控制措施的有效性；

j) 一个反馈环，以支持整体改进；

k) 对所产生结果有用性的评价；以及

l) 风险管理过程的输入机制，来辅助对控制措施选择、实施以及资源分配的优先顺序。

一旦成功实施，信息安全测量项目能：

a) 展示组织与适用法律、法规、规章的符合性；

b) 支持对以前未检测到的未知信息安全因素的识别；

c) 当描述历史和当前活动的测量时，有助于满足向管理层的报告需求；以及

d) 被用作信息安全管理体系内审和管理评审的输入。

5.3 信息安全测量模型

信息安全测量模型将单个的简单测度纳入更复杂的组合测度，从而提供全面的和一致的测量结果，可以不断重复地用于基准测试和比较。图3中描述了一个信息安全测量模型。通过应用该模型所开发的测量范例见附录B。

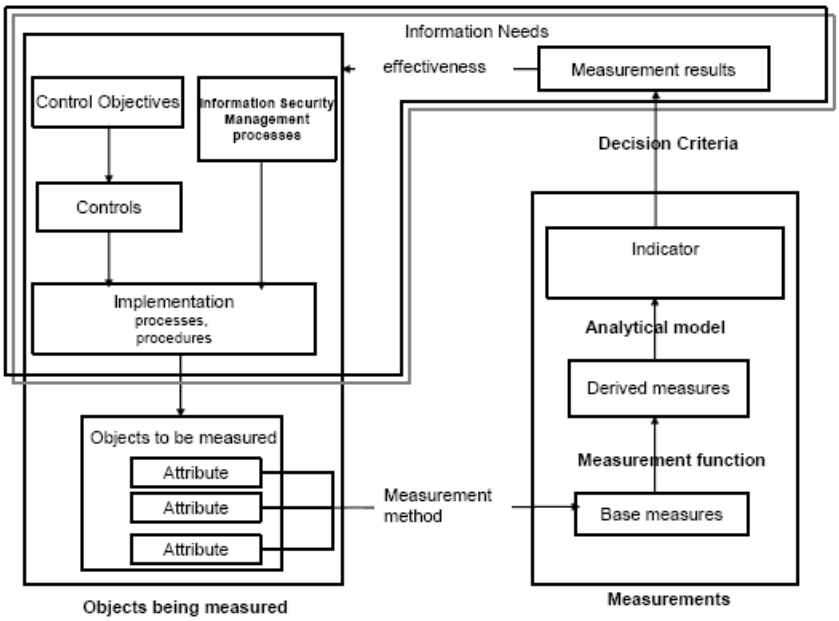

图3 信息安全测量模型

以下各子节将使用这样一个范例来描述模型中的各元素：策略要求所有员工在被授权访问信息系统前，应被适当告知信息处理的规则。两个控制措施被定义来实施该策略：

a) 所有员工在被授权访问信息系统前，必须签署用户协议；以及

b) 所有员工在被授权访问信息系统前，必须接受信息安全意识培训。

5.3.1 基本测度和测量方法

一个测量对象可能会有多个属性，只有这些属性中的一些为基本测度提供输入是有用的。对测量对象的各种属性应用测量方法，得到基本测度。一个给定的属性可被用在多个不同的测量上。

一个测量方法是用于以指定的标度量化属性的逻辑操作序列。

测量方法可以通过各类资源使用测量对象的数据，例如：

a)风险评估和风险分析结果；

b)调查表和个人面谈；

c)内部或外部审计报告；

d)事件记录，如日志、报表统计、审计轨迹等；

e)事故报告，尤其是那些造成影响发生的事故；

f)测试结果，如渗透性测试、社交工程、符合性工具和安全审计工具；以及

g)信息安全意识培训结果。

表1包含一个范例，说明测量对象、属性、测量方法和基本测度之间的关系。

测量对象	属性	测量方法	基本测度
员工安全意识过程	员工数据库中的员工记录中的个人字段	1) 数据库查询，获取已接受意识培训的员工数。 2) 数据库查询，获取已签署用户协议的员工数。 3) 数据库查询，获取已接受意识培训并已签署用户协议的员工数。 4) 数据库查询，获取全体员工数。	1) 接受安全意识培训的员工数。 2) 签署用户协议的员工数。 3) 接受安全意识培训并签署用户协议的员工数。 4) 员工总数。

5.3.2 导出测度和测量函数

导出测度通过对一个或多个基本测度应用测量函数来定义。一个给定的基本测度可能被用

作多个导出测度的输入。

一个测量函数是为组合两个或两个以上基本测度而执行的算法或计算，定义了这些基本测度如何被聚合到一个导出测度。

导出测度的标度和单位依赖于其各组成基本测度的标度和单位，以及组合函数。

测量函数可能会包括多种不同的技术，如对所有基本测度取平均值，对基本测度应用权重，或将它们赋予定性值。测量函数可能会使用不同标度来组合各基本测度，如百分比和定性评估结果。

表2包含一个范例，说明基本测度、测量函数和导出测度之间的关系。

基本测度	测量函数	导出测度
1) 接受安全意识培训，并签署用户协议的员工数。 2) 签署用户协议的员工数。 3) 员工总数。	1) 将接受安全意识培训，并签署用户协议的员工数除以员工总数，乘以100%。 2) 将签署用户协议的员工数除以员工总数，乘以100%。	1) 接受安全意识和培训，并签署用户协议的员工百分比。 2) 签署用户协议的员工百分比。

5.3.3 指标和分析模型

通过对导出测度应用分析模型，获得指标。分析模型是将一个或多个基本测度和/或导出测度与相关决策准则组合在一起的算法或计算（见表3）。

指标是对由规定信息需要的相关模型导出的指定属性提供估算或评价的测度。标度和测量方法会影响产生指标的分析技术的选择。

表3包含一个范例，说明导出测度、分析模型和指标之间的关系。

导出测度	分析模型	指标
1) 接受安全意识培训，并签署用户协议的员工百分比。 2) 签署用户协议的员工百分比。	X＝已定义的组织可接受的策略符合性阈值。 指标值假设为“粗体”。 如果X%的用户签署了用户协议，指标值变为“斜体”。 如果X%的用户接受了安全意识培训并签署了用户协议，指标值变为“标准体”。	组织安全意识策略的符合性，在图形上用粗体、斜体和标准体重新表示。

注：如果使用颜色编码，必须增强对颜色的描述，使用不同的阴影或不同的字体。目的为了保障视障用户的使用，或者黑白打印的场合。以下章节同样应用。

5.3.4 测量结果和决策准则

基于已定义的决策准则，对适用的指标进行解释，可以得到测量结果的评价。测量结果应当考虑评估信息安全管理体系过程、控制目标、控制措施有效性的整体测量目标。

决策准则是用于确定是否需要行动或进一步调查的，或者用于描述给定结果置信度的阈值、目标或模式。

目标是可应用于组织整体或部分的详细的性能规格，来自于信息安全目标并需要被设置及达到，如信息安全管理体系目标和控制目标。

表4包含一个范例，说明指标、决策准则和测量结果之间的关系。

指标	决策准则	测量结果
组织安全意识策略的符合性，在图形上用粗体、斜体和标准体重新表示。	标准体——符合策略。 斜体和粗体——不符合策略。 向上趋势显示符合性得到改进，向下趋势显示符合性的恶化。倾斜角度可能提供了控制措施实施有效性的见解。任何方向的陡峭斜线显示对控制措施的实施需要做仔细的检查，来判断这种情况的原因。消极趋势可能需要管理层的干预。积极趋势应该进行检查，来识别潜在的最佳实践。	符合策略－－不需要变更。 不符合策略－－应该考虑修订（策略）。

6. 管理职责

6.1 概述

在信息安全管理体系范围内，管理层负责建立信息安全测量项目，引入不同的利益相关方（见7.4.3），并使用测量结果来作为监控和改进信息安全的输入。

为此，管理层应：

a) 为信息安全项目建立一个策略；

b) 建立信息安全项目的角色和职责；

c) 确保信息安全项目目标的达成（见5.1）；

d) 提供充足的资源来执行信息安全测量项目；

e) 确保适当的基础设施到位；

f) 确保使用适当的工具执行测量过程；

g) 建立测量结果的目标；

h) 确保测量向组织内各利益相关方提供了充足的信息（正如7.4.3节所定义的），以有效监控各控制措施的有效性，并/或识别整体控制措施架构的缺陷；

管理层应通过适当分配测量相关的角色和责任，保证测量结果不受到被测量对象所有者的影响。这可能是通过职责分割，或如果这不可能，通过使用允许独立检查的详细记录来实现。

6.2 资源管理

管理层应该分配和提供资源来支持信息安全测量的必要功能，例如数据收集、分析、存储、报告和分发。资源分配应包括以下方面的分配：

a) 负责信息安全测量项目所有方面的人员；

b) 适当的财务支持；以及

c) 适当的基础设施支持，例如用于测量过程的物理基础设施和工具。

6.3 测量培训，意识和能力

管理层应保证:

a) 参与测量设计和使用的所有职员在模型和项目上被充分培训，并且有适当的能力来履行他们的角色；以及

b) 使用测量的所有职员理解他们职责中有一部分是要为过程改进提供建议，这可能包括建议不同的测量。

7. 测度和测量开发

7.1 概述

本节描述了为了量化信息安全管理体系、控制目标和控制措施的有效性，并识别针对特定利益相关方的一套测量，怎样来开发测量。这些测量将通过提供评估信息安全管理体系有效性的多种手段，以及支持组织内信息安全的持续改进，进一步加强信息安全管理体系的性能。

7.2 测量范围识别

测量开发的过程应该被建立和记录，包括选择用于测量的具体控制措施和控制目标，识别这些对象的各种测量属性，明确测量，并且建立数据收集、分析、报告的各种过程与工具。计划过程应包括识别财力、人力，以及基础设施（物理的和工具的）资源。管理层有责任来提供

这些资源，以保证信息安全测量的成功实施。

取决于组织的能力和资源，组织信息安全测量活动的最初范围可能会被限制在管理层给予最高优先级的活动、产品和服务上。随着时间的推移，测量活动的最初范围可以扩大来包括信息安全管理体系的更多元素。

测量的利益相关方应该被识别并参与定义测量范围。测量的利益相关方可能是组织单位内部或外部的，例如项目经理、信息系统经理或信息安全决策者。关于每个控制措施有效性的具体信息被收集、聚合、分析，并向利益相关方进行展示。

组织应考虑在一段给定时间段内，对供一个决策者使用的测量数量进行限制，以保证基于所收集信息进行有效改变的能力。过多的测量可能会削弱有效集中力量和未来活动优先排序的能力。将被使用测量的优先顺序应基于特定组织的准则，并包括基于风险的考虑。

7.3 信息需要识别

每个测量应对应于一个信息需要。信息需要是对于哪些需要被测量的表述，关于 ISMS 过程、控制目标、控制措施，以及这些过程、控制目标、控制措施的实施。

应该通过执行下列活动来识别信息需要：

a) 检查信息安全管理体系及其过程，例如：
   1) 组织的信息安全管理体系策略、目标、风险和安全要求；
   2) 法律、法规和合同的要求；
   3) ISO/IEC 27001 标准中所描述的风险评估和处置过程的结果；
   4) 信息安全管理体系的有效性要求；
b) 基于准则对所识别的信息需要，排列优先次序，例如：
   1) 风险处置优先次序；
   2) 组织的能力和资源；
   3) 利害相关方的利益；
   4) 信息安全策略；
   5) 为满足法律、法规和合同要求所需要的信息；
   6) 与测量成本相关的信息的价值；
c) 根据已建立的准则，选择经过优先排序的信息需要；以及
d) 向所有相关的利害相关方，记录和沟通已选择的信息需要。

所有适用于信息安全管理体系过程、控制目标和控制措施或成组的控制措施的测度，应该基于已选择的信息需要来实施。

7.4 对象识别

信息安全测量能在整个背景和信息安全管理体系范围内，被用在不同的业务对象上。识别用于测量的对象包括：

a) 考虑已建立的测量目标；以及

b) 明确这些对象的关键属性，这些属性可能会提供关于控制措施和控制目标有效性及其实施的相关信息。

描述测量对象和相应属性的数据将被用来作为单个基本测度的输入。测量对象包括但不限于：

a) 产品和服务；

b) 过程；

c) 适用的资产，如ISO/IEC 27001 中所识别的各种设施、应用程序，以及信息系统；

d) 业务单元；

e) 地理位置。

测量对象应该要仔细地选择，以确保测量的结果是有意义的。所选择的对象应该和选择的理由一起被记录。

7.5 测量开发和选择

组织应该使用已有的各种资源，来识别和剪裁信息安全测度。

每个测量应该被详细地开发，适合每个组织的需求，并应至少包括：

a） 测度识别；

b） 测量对象和属性；

c） 基本测度；

d） 导出测度；

e） 指标；

f） 数据收集规程；以及

g） 数据分析规程。

信息安全测量的详细模板范例在附录 A 中提供。ISO/IEC 27001 控制措施子集的测量范例参见附录 B。

7.5.1 测量方法

对每个基本测度应识别其测量方法。通过将属性转换为基本测度，测量方法被用来量化测量对象。

测量方法可能是主观的或客观的。主观方法含有对人的判断的量化，而客观方法是基于数字规则的量化，如可能通过手工或自动化手段实施的计算。

通过应用适当的标度，测量方法将属性量化成数值。每个标度使用一个测量单位。只有以同种测量单位表达的量才能直接进行比较。

不管是手工（例如，问询、观察、自评估）还是自动化测量方法都需要独立的验证，以建立每个属性值的置信度。对每个测量方法，验证准则应被定义和记录。

应考虑测量方法的精度，相关的错误应记录。

测量方法应在一段时间保持一致，这样在不同时间采取的基本测度是可比较的，并且基于这些基本测度的导出测度和指标也同样是可比较的。

7.5.2 测量函数

对每个导出测度，应该定义一个使用两个或两个以上基本测度的测量函数。在某些情况下，基本测度能与导出测度一起作为分析模型的输入。

测量函数（如，公式）可能会包括多种不同的技术，如对所有基本测度取平均值，对基本测度应用权重，或是在将基本测度聚合成导出测度前，将它们赋予定性值。测量函数可能会使用不同标度来组合各基本测度，如百分比和定性评估结果。

应该定义一个计算每个测度的公式并记录。应考虑由于基本测度的组合而导致的累积性错误。

7.5.3 利益相关方

对于每个测量，适当的利益相关方都应被识别和记录。利益相关方可能包括：

a) 所有者——人员或组织单位，它们拥有被用来创建基本测度的测量对象和属性的相关信息，并负责测量；
b) 顾客——人员或组织单位，为了开展他们的业务功能而申请和需要测量；
c) 收集者——人员或组织单位，负责收集、记录和存储数据；
d) 沟通者——人员或组织单位，负责分析数据和报告结果；以及
e) 评审者——人员或组织单位，负责对测量评价准则是否适当作评审，以验证控制措施和信息安全管理体系过程的有效性。

7.5.4 属性选择和评审

一个测量对象可能有多个信息安全属性。一个基本测度可能会选择使用一个或多个属性。

应该对属性进行证实，以确保：

a) 合适的属性被选择用来测量；以及

b) 适当数量的属性已经被选择，以保证提供一个充分的集合来支持一个有效的测量。

所选择属性的特征决定着何种测量方法将被使用来确定基本测度（例如，定量或定性的）。

应仅有那些与相应基本测度有关的属性被选择。尽管属性选择应考虑获取测量属性的困难程度，它不应该只从那些易于获取的数据，或是易于测量的属性中选择。

7.5.5 分析模型

对每个测度来说，应该定义一个分析模型，目的是将一个或多个导出测度转换为一个指标。

分析模型以某种方式组合各测度并产生输出，这个输出与信息安全管理体系策略有关，并对信息安全管理体系利益相关方有意义。

注意，当定义分析模型时，应用在指标上的决策准则也应该被考虑。

有时分析模型可以简单到只是将单个导出测度转换为一个指标。

7.5.6 指标和报告格式

通过聚合各导出测度并基于决策准则对它们进行解释，将产生指标。对将向顾客报告的每个指标，应该定义并记录一个报告格式。

报告格式将可视地描述测度并提供一个指标的言语解释。报告格式应该被定制，以满足顾客的信息需要。

7.5.7 决策准则

每个指标对应的决策准则，应该基于信息安全目标来定义和记录，从而为客户提供可行动的指南。该指南应给出对测量进展的期望以及基于指标的启动改进措施的阈值。决策准则建立了一个目的，由此成功可以被测量，决策准则也为解释指标与目的的接近程度提供了指导。建立决策准则和目的的机制与从测度得到的指标是有区别的。

需要对与信息安全管理体系过程和控制措施性能相关的各项目设立目的，以及目标的达成情况，并最终对评价信息安全管理体系和控制措施的有效性。

组织可能会决定等到初始数据收集到后，再为指标设置目的。一旦基于初始数据的纠正措施被识别，就能定义适当的决策准则和实施里程碑，它们对特定的信息安全管理体系是现实的。如果不能建立决策准则，管理层应评价被测量的对象和相应的测度是否为组织提供了所期望的价值。

如果与这些测度开发或选择相关的历史数据存在，将有助于决策准则的建立。过去所观察到的趋势将提供对以前存在的性能范围的见解，并为创建现实的决策准则提供指导。决策准则

可以被计算或基于一个对期望行为的概念性理解。决策准则可以从历史数据、计划和启发式方法导出，或者从统计控制界限或统计置信界限计算得到。

7.6 测度证实

管理层应对所开发的测度进行证实，以保证所开发测度是有用并有成本效益的。下面这些准则可能与决定测度是否有用并有成本效益相关：

a) 战略的：与组织的业务目标和利益相关方的需求一致；

b) 定量的：提供客观和经验数据；

c) 解释性的：能容纳主观输入来帮助对数据的解释；

d) 具有成本效益：数据收集的成本应与被测量价值相关的潜在损失相平衡；

e) 可验证：第三方评审者应能评估数据，并能重现结果；

f) 有意义：数据应提供与一段时间内所应用控制措施和控制目标相关的有意义信息，使得能够对变更影响或结果一致性进行评估；

g) 实用：结果应支持使命、财务和运行的决策；

h) 不可分： 数据应该在可能的最细、不可分解的级别下被收集；

i) 良好定义：在7.5中所描述的详细模板中记录；以及

j) 可重复：测量应产生可比较和可再生的结果。

7.7 数据收集、分析和报告

应该建立或剪裁测量数据收集、分析和报告的过程，如果存在这样的过程。如果需要，还应该建立提供支持的工具和技术。这些过程、工具和技术可以满足以下测量相关的活动：

a) 数据收集，包括存储和验证。规程应详细说明数据是如何被收集和区分的，以及这些数据将怎样和在哪里被存储。数据验证可能会通过审计来完成。自动化工具能被用来支持这些规程；

b) 数据分析，以及测量的报告。规程应详细说明数据收集方法、频率、格式，以及报告信息产品的方法。应该识别哪些工具可以被用来执行数据分析。

报告格式的范例包括：

a) 通过整合高级别指标提供战略信息的记分卡；

b) 执行和运行的仪表板，不是集中在战略目标，而更关注特定控制措施和过程的有效性。仪表板可能会使用一系列的颜色来沟通结果——例如，从黑色（0%）到浅绿色（100%），但是请注意5.3.3中表3有关使用颜色的说明；

c) 报告，从简单和统计性的，比如一个给定时间段的测度列表，到更为复杂的交叉表，

这种交叉表包括内嵌组、滚动总结、动态透视或链接。报告最好被用在用户需要以一种易读的格式看原始数据时；以及

d) 量表来表示动态的数据值包括警报、附加的图形元素，以及端点的标记。

7.8 记录

测量的完整方法应被记录在一个实施计划中。实施计划应至少包括以下信息：

a) 测量的意图；

b) 将被测量的控制措施和控制目标；

c) 测量对象；

d) 将被收集和使用的测度；

e) 数据收集过程；

f) 数据分析和报告过程，包括报告格式；

g) 利益相关方的角色和责任；以及

h) 测度评审的周期，以确保测量与信息安全管理体系和业务目标保持同步。

8. 测量运行

8.1 概述

信息安全测量的运行包括收集、存储和验证被用来创建信息安全测度的数据。它也包括一些必要的活动，这些活动保证所收集的测量被用来获得对信息安全管理体系有效性的理解，以及识别适当的改进措施。本阶段包括以下活动：

a) 将测量规程整合进整个信息安全管理体系的运行；以及

b) 收集、存储和验证数据。

8.2 规程整合

信息安全测量项目应被信息安全管理体系充分地整合和使用，包括：

a) 在信息安全管理体系背景下，定义和记录关于开发、实施和维护信息安全测量的角色和职责；

b) 数据生成与收集，包括变更现有过程以容纳数据生成与收集活动；

c) 向利益相关方沟通数据收集活动的改变，以保证数据收集人的能力，包括他们对所要求数据类型、数据收集工具、数据收集规程的理解。增强信息收集人的能力将有助于提高数据收集质量，以及测量对组织的用处；

d) 数据分析和报告应被整合进相关过程，以保证这些过程的常规性能；

e) 策略和规程，它们定义了组织内测量的使用，测量信息的发布，以及信息安全测量项目的审计和评审；

f) 一个监控测量的过程，以评价测量的使用情况；

g) 一个去除测量和增加新测量的过程，以确保测量随组织不断演进；以及

h) 一个确定用于趋势分析的历史数据有用期的过程。

8.3 数据收集和处理

数据收集过程包括：

a) 所需要的数据应根据实施计划中定义的过程，使用指定的测量方法按照常规间隔来收集；

b) 记录数据收集，包括：

1) 数据收集的日期、时间、地点；

2) 信息收集者；

3) 信息所有者；

4) 数据收据过程中发生的任何问题；以及

5) 数据验证和测量证实的信息；以及

c) 根据属性证实准则，验证所收集的数据

应对所收集数据进行整理，并以有助于数据分析和报告的格式来存储。所存储的数据应带有必要的背景信息。

9. 测量分析和报告

9.1 概述

测量应该被分析和报告。这个阶段包括以下活动：

a) 分析数据和产生测量结果；以及

b) 向利益相关方沟通测量结果。

9.2 分析数据和产生测量结果

收集的数据应该基于决策准则被分析和解释。数据在分析之前可以被聚合、转换或再次编码，在数据处理期间将产生计划中的指标。很多种分析技术能被应用。分析的深度应该根据数据的自身特性和信息需要来确定。执行统计分析的指南参见ISO TR 10017:2003。

数据分析的结果应该被解释。分析结果的人（沟通者）应该能基于结果给出一些初始结论。但是沟通者可能不会直接涉及技术和管理过程，这些结论需要由其他利益相关方进行评审。所

有的解释都应该考虑测度的背景。

数据分析应识别实际性能和期望性能间的差距。这种分析将指出可能需要改进的相关测量对象、控制目标及控制措施，以改进信息安全性能。对那些显示出不符合或性能差的指标，应该识别其原因，可能包括以下几类：

a) 实施失败造成的不符合——被期望实施的控制措施或信息安全管理体系过程，或者没有被实施，或者在实施、运行和管理上不充分；

b) 无效控制措施或信息安全管理体系过程

1) 控制措施或信息安全管理体系过程已被正常实施、运行和管理，但不能应对所预计的威胁；

2) 控制措施或信息安全管理体系过程已被实施，但没有被正常运行和管理。

c) 风险处置失败：控制措施或信息安全管理体系过程已被正常实施、运行和管理，但可以被威胁绕过；以及

d) 风险评估失败：

1) 控制措施或信息安全管理体系过程已被正常实施、运行和管理，但不能应对实际威胁，因为威胁范围太大；

2) 控制措施或信息安全管理体系过程未被实施，因为风险评估过程中忽视了一些威胁；以及

3) 控制措施或信息安全管理体系过程已被实施但无效，因为风险评估过程中忽视了一些威胁。

数据分析结果、指标、与决策准则相关的解释，以及相关的支持信息构成了测量结果。

总结测量结果的报告，应根据实施计划，使用适当的报告格式（见7.7）来准备。

分析的结论应被利益相关方评审，以保证对数据的适当解释。数据分析的结果应被记录，以便向各利益相关方进行沟通。

9.3 沟通结果

负责分析数据和报告结果的人员或组织单位（沟通者）应该决定如何沟通信息安全测量结果，包括：

a) 哪些测度在内部和外部报告；

b) 针对各利益相关方和兴趣相关方的测度列表；

c) 报告结构，被提供的特定测度，以及展示类型都应被剪裁以适合各个组的需求；以及

d) 各利益相关方之间交换反馈意见的方式，用来评价信息产品和测量过程；

测量结果应该与一系列的内部利益相关方沟通，包括但不限于：

a) 负责风险管理过程的人员，特别是在发现风险评估或风险处置失败之处；

b) 管理层，为了识别有待改进之处；

c) 提供任何反馈的信息拥有者。

测量可能需要发布给外部利益相关方，包括上级单位、股东、顾客和供应商。外部报告不应像内部报告那样详细，应仅包含适合外部使用的数据。外部报告在发布之前，应由组织内的管理层和其他适当方进行评审。

10. 测量项目评价和改进

10.1 概述

测量项目应该被评价和改进，以确保测量项目：

a) 以一种有用和有效的方式，持续满足组织对信息安全测量的要求；

b) 是否按计划执行；

c) 符合对威胁和脆弱性的变更；以及

d) 符合对环境的变更（例如：需求、法律和技术）。

证实的结果应能提供清晰的指示，关于对当前信息安全测量项目满足组织要求的程度，以及是否需要对测量项目作改进。

结果的实用性和获取它们的成本应依据测量项目的目标进行评价。评价的结果应该有助于决定是否当前信息安全测量项目满足组织要求的程度，或者是否需要作改进。

组织应明确评价的频率，计划周期性修订的时间段，并建立做这些可能修订的机制。

下面的步骤应被遵循：

a) 识别测量项目的评价准则（见10.2）；

b) 监控、评审和评价测量（见10.3）；以及

c) 实施改进（见10.4）。

10.2 识别测量项目的评价准则

在初步实施后，组织评价测量结果的实用性和有效性，以及获取测量结果所需要的投入。测量结果能被评价前就应该建立评价准则。评价的目的是评估修改或改进测量项目的必要性。除了内部信息安全管理体系审计外，还可以进行外部审计来提供独立的第三方评估。组织应为审计确定适当的时间，以保证它们不会严重地干扰运行。

当有如下最有可能的条件出现时，组织应该再次评价并改进当前的信息安全测量项目：

a) 业务目标和要求的变更；

b) 威胁环境的变更；

c) 风险的变更；

d) 用于测量的更完善或合适数据的增多；

e) 在组织的背景下，被用来测量的测量对象和属性的变更；以及

f) 法律、法规和其它外部要求的变更。

以下准则可以用来评价测量结果：

a) 测量结果对于改进信息安全是有用的；

b) 测量结果符合信息需要。

如果收集的测量结果在整体上对于改进组织的信息安全是有用的，那么测量项目是有效的。

10.3 监控、评审与评价测量项目

在依据10.2的准则初步实施后，以及在基础系统或相应业务目标发生重大变更时，包括所有的测度、指标、决策准则和测量结果在内的测量项目，应该被监控、评审和评价。潜在的改进可以被识别，包括：

a) 按照已建立的准则修正测度；

b) 去除或替换不再适合的测度、指标和决策准则；

c) 确保分配充足的资源来支持测量项目；

d) 识别测量项目所需的改进，并计划实施；

e) 记录管理层的决策，以允许以后各测量的比较和趋势分析。

监控、评审和评价测量项目的结果应该向管理层沟通，以便对必要的改进和测度今后的使用做出决策。管理层的决策和测量项目改进的结果应该向合适的利益相关者沟通。

利益相关者应该根据测度对其的有用性给出反馈，这种反馈将为信息安全测量项目的评价提供输入。

10.4 实施改进

已识别的改进应被管理层正式记录和批准。管理层应保证按计划实施改进。

组织可以使用项目管理技术来完成改进。

附录A（资料性附录）

信息安全测量模板

附录A提供了信息安全测量的模板，包含了5.3节描述的需要在7.5节识别的所有组件。组织可以根据自己的需求修改该模板。

测度识别	
测度名	测度名
数字识别码	特定组织的唯一识别码。
控制目标	待测量的控制目标（计划的或实施的）。
控制措施（1）	可选的：待测量的控制措施（计划的或实施的）。
控制措施（2）…	可选的：按相同测度分组的进一步控制措施（计划的或实施的）。
测量目的	描述引入测度的原因。
评审者	人员或组织单位，评审测量评价准则是否适合于证实控制措施和信息安全管理体系的有效性。
测量对象和属性	
测量对象	待测量的并可通过属性的可测量性给出特征的对象。对象可以包括过程、系统或系统组件。
属性	测量对象的属性或特征，能通过手工或自动化手段被定性或定量地区分。
基本测度规范（对每个基本测度[2…n]）	
基本测度	基本测度是用某个属性及其量化方法定义的测度（如，被培训人员的数量，场地数量，当前累计花费）。当数据被采集时，对基本测度赋予一个值。
测量方法	操作的逻辑序列，定义计数规则来计算每个基本测度。对基本测度来说，通过测量方法将获取到测量数据，包括精度、标度和测量单位。
标度	被用在基本测度上的值或类别的有序集合。
导出测度规范	
导出测度	由两个或两个以上基本测度的函数导出的测度。
测量函数	被用来计算导出测度的逻辑操作序列。对导出测度来说，通过测量函数相应基本测度得到聚合，导致累计的精确性。
标度	被用在基本测度上的值或类别的有序集合。
指标规范	
指标描述和范例	一个或多个测度（基础和导出）的显示，提供对由规定信息需要的相关模型导出的指定属性的估算或评价。 指标常显示为图或图表。包括指标的梗概。
分析模型	将一个或多个基本测度和/或导出测度与相关决策准则组合在一起的算法或计算。
决策准则	用于确定是否需要行动或进一步调查的，或者用于描述给定结果置信度的阈值、目标或模式。
指标解释	描述指标范例应该如何被解释。
效果/影响	指标所获得的结果带来的效果和影响的定义
偏离原因	在所获得结果中可能导致偏离的原因的定义
正向值	指定了值的升高是否会带来正向的价值（好的结果），或者是值

	的降低是否会带来正向的价值
报告格式	报告格式应被识别和记录。描述组织或信息所有者希望记录的观察。报告格式将可视地描述测度并提供对指标的言语解释。报告格式应根据信息顾客来定制。
数据收集规程	
收集频率	数据多久收集一次。
信息所有者	拥有关于能被用来创建基本测度的测量对象和属性相关信息的人员或组织单位，以及负责测量的人员
信息收集者	负责采集、记录、存储数据的人员或组织单位
数据收集工具	列出被用来收集数据的任何工具（如，脆弱性扫描器）
数据收集库	列出数据收集后存储的任何工具（如，数据库）
收集日期	应该获取数据的日期
数据记录规程	定义数据记录的规程（规程链接）
测量值有效期	修订日期（失效或需要重新验证）
分析周期	定义测量的周期
数据分析规程	
数据报告频率	数据多久报告一次（可能不如数据收集频繁）。
信息沟通者	负责分析数据和报告结果的人员或组织单位
分析数据源	列出分析所用的数据源
分析工具	列出被用来分析的任何工具（如，统计工具）
信息客户	提出请求并需要测度来支持其业务功能的个人或组织单位
附加信息	
附加分析指南	提供关于测度变化的其他指南。
实施考虑	列出对成功实施必要的过程或实施要求。

附录B（资料性附录）

测度范例

以下条文提供了测度的范例。这些例子是用来演示如何使用附件A提供的模板应用此国际标准。

目录

（略）

对应的过程和控制措施 （ISO/IEC 27001:2005中的条款或附录A的控制措施数量）	对应的测度 （本附录的引用）	测度名称
条款 4.2.2h	B.5.1	ISMS事件和有效性
条款 4.2.3b	B.1	ISMS整体有效性
条款 5.2.2d	B.2.1	ISMS个人培训
条款 7.2.b和7.2.i	B.4	ISMS评审过程
条款 7.3	B.6	管理承诺
条款 8.2	B.5.2	纠正措施实施
控制措施 A.6.2.3	B.11	第三方协议安全
控制措施 A.8.2.2	B.2.2	信息安全培训
控制措施 A.9.1.2	B.8	物理入口控制
控制措施 A.9.2.4	B.10	周期性维护管理
控制措施 A.10.4.1	B.7	恶意代码防护
控制措施 A.10.10.2	B.9	日志文件评审
控制措施 A.11.3.1	B.3.1	口令质量－手工
控制措施 A.11.3.1	B.3.2	口令质量－自动

B.1 ISMS整体有效性

（略）

B.2 ISMS培训

B.2.1 ISMS个人培训

（略）

B.2.2 信息安全培训

（略）

B.3. 口令策略

B.3.1 口令质量－手工

（略）

B.3.2 口令质量－自动

（略）

B.4. ISMS评审过程

（略）

B.5. ISMS持续改进

B.5.1 ISMS事件和有效性

（略）

B.5.2 纠正措施实施

（略）

B.6. 管理承诺

（略）

B.7. 恶意代码防护

（略）

B.8. 物理入口控制

（略）

B.9. 日志文件评审

（略）

B.10. 周期性维护管理

（略）

B.11. 第三方协议安全

（略）

参考文献

（略）