ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31497—2015/ISO/IEC 27004:2009

信息技术　安全技术
信息安全管理　测量

**Information technology—Security techniques—
Information security management—Measurement**

(ISO/IEC 27004:2009,IDT)

2015-05-15 发布　　2016-01-01 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 27004:2009《信息技术　安全技术　信息安全管理　测量》(英文版)。

本标准做了以下编辑性修改：

——引言部分增加了有关信息安全管理体系标准族情况的介绍。

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、山东省计算中心、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、北京信息安全测评中心。

本标准主要起草人：上官晓丽、周鸣乐、李刚、许玉娜、顾卫东、闵京华、赵章界、董火民、李旺、史艳华、李敏、张建成、韩庆良。

引　言

0.1　总则

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)

——(本标准)　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

为了评估按照 GB/T 22080—2008 规定的已实施的信息安全管理体系(Information Security Management System,简称 ISMS)和控制措施或控制措施组的有效性,本标准提供了如何编制测度和测量以及如何使用的指南。

为了有助于决定 ISMS 过程或控制措施是否需要改变或改进,本标准涉及方针策略、信息安全风险管理、控制目标、控制措施、过程和规程,并且支持其校验过程。切记任何控制措施的测量都不能保证绝对安全。

本标准的实施形成了信息安全测量方案。信息安全测量方案将有助于管理者识别和评价不相容

的、无效的 ISMS 过程和控制措施，并优化改进或改变这些过程和(或)控制的活动。它也可有助于组织证明 GB/T 22080—2008 的符合性，并提供管理评审和信息安全风险管理过程的额外证据。

本标准假设：制定测度和测量的出发点是按照 GB/T 22080—2008 要求充分掌握了组织所面临的信息安全风险，并假设已经正确实施了组织的风险评估活动(即基于 GB/T 31722—2015)。信息安全测量方案将鼓励组织向利益相关者提供可靠的关于信息安全风险和管理这些风险已实施的 ISMS 的状况的信息。

通过有效地实施信息安全测量方案，将提高利益相关者对测量结果的信任，并能使其利用这些测度实现对信息安全和 ISMS 的持续改进。

累积的测量结果将允许把一段时间内实现信息安全目标的进展当作组织的 ISMS 持续改进过程的一部分。

0.2 管理概述

GB/T 22080—2008 要求组织“在考虑有效性测量结果的基础上，进行 ISMS 有效性的定期评审”，并且“测量控制措施的有效性，以验证安全要求是否得到满足”。GB/T 22080—2008 也要求组织“确定如何测量已选控制措施或控制措施组的有效性，并指明如何用这些测量措施来评估控制措施的有效性，以产生可比较的和可再现的结果。”

组织用以满足 GB/T 22080—2008 规定的测量要求所采用的方法，将基于一些重要因素而变化，包括组织所面临的信息安全风险、组织规模、可用的资源、适用的法律法规、规章和合同要求。为了防止过多的资源被用于 ISMS 的一些活动而损害其他活动，慎重选择和证明用于满足测量要求的方法是非常重要的。理想情况下，持续的测量活动将把组织的正常运作和最小的额外资源需求结合在一起。

为满足 GB/T 22080—2008 规定的测量要求，本标准建议基于以下活动：

a) 制定测度(即基本测度、导出测度和指标)；
b) 实施和运行信息安全测量方案；
c) 收集和分析数据；
d) 产生测量结果；
e) 与利益相关者沟通产生的测量结果；
f) 将测量结果作为 ISMS 相关决策的有利因素；
g) 用测量结果识别已实施的 ISMS 的改进需要，包括 ISMS 的范围、策略、目标、控制措施、过程和规程；
h) 促进信息安全测量方案的持续改进。

组织规模是影响组织完成测量的能力的因素之一。一般来说，业务的规模和复杂性以及信息安全的重要性，都会影响需要的测量程度，其中测量程度是针对已选的测度数量以及收集和分析数据的频率来说的。对于中小型企业来说，一个不太全面的信息安全测量方案就足够了。而对大型企业，则需要实施和运行多个信息安全测量方案。

单个信息安全测量方案可满足小型组织，而大型企业可能需要多个信息安全测量方案。

本标准产生的文件，有助于证明正在被测量和评估的控制措施的有效性。

信息技术　安全技术
信息安全管理　测量

1　范围

为了评估按照GB/T 22080—2008规定实施的信息安全管理体系(Information Security Management System,简称ISMS)和控制措施或控制措施组的有效性,本标准提供了如何编制测度和测量以及如何使用的指南。

本标准适用于各种类型和规模的组织。

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 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,IDT)

3　术语和定义

GB/T 29246—2012中界定的以及下列术语和定义适用于本文件。

3.1

分析模型　analytical model

将一个或多个基本和/或导出测度关联到决策准则的算法或计算。

[GB/T 20917—2007]

3.2

属性　attribute

可由人或自动化工具定量或定性辨别的对象特征或特性。

[GB/T 20917—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。

[GB/T 20917—2007]

注:一个基本测度在功能上独立于其他测度。

3.4

数据　data

赋予基本测度、导出测度和(或)指标的值的集合。

[GB/T 20917—2007]

3.5

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、目标性能或模式。

[GB/T 20917—2007]

3.6

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。

[GB/T 20917—2007]

3.7

指标　indicator

为由规定信息需要的相关分析模型导出的指定属性提供估算或评价的测度。

3.8

信息需要　information need

针对目标、目的、风险和问题的管理，所表达的必要见解。

[GB/T 20917—2007]

3.9

测度　measure

通过执行一次测量赋予对象属性的数或类别。

[GB/T 20917—2007]

注：术语“测度”是基本测度、导出测度和指标的统称。

示例：测量出的缺陷率与规划的缺陷率之间的比较，其差异就与指示一个问题的评估紧密联系在一起。

3.10

测量　measurement

使用测量方法、测量函数、分析模型和决策准则来获取有关 ISMS 和控制措施有效性信息的过程。

3.11

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。

[GB/T 20917—2007]

3.12

测量方法　measurement method

一般描述为，用于以指定的标度量化属性的逻辑操作序列。

[GB/T 20917—2007]

注：测量方法类型取决于用来量化属性的操作本质。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。

3.13

测量结果　measurement results

处理某信息需要的一个或多个指标及其相应的解释。

3.14

对象　object

通过对其属性的测量所表征出来的项。

3.15

标度　scale

值的一个有序集合，连续的或离散的；或由属性所映射的一个范畴集合。

[GB/T 20917—2007]

注：依赖标度值之间关系的本质，标度类型通常定义为以下四种：

标称型标度—测量值是范畴化的。

顺序型标度—测量值是序列化的。

间距型标度—对应该属性等同的量，测量值具有该等同量的距离。

比率型标度—对应该属性等同的量，测量值具有该等同量的百分比，其中若该值为零，则对应无该属性。

这些只是标度类型的示例。

3.16

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。

[GB/T 20917—2007]

3.17

确认　validation

通过提供客观证据对特定的预期用途或应用要求已得到满足的认定。

3.18

验证　verification

通过提供客观证据对规定要求已得到满足的认定。

[GB/T 19000—2008]

注：又称为“符合性测试”。

4　本标准的结构

为了按照 GB/T 22080—2008 的 4.2 要求管理充分和适当的安全控制措施，本标准提供了评估 ISMS 要求的有效性所需要的测度和测量活动的解释。

本标准由以下部分构成：

——信息安全测量方案和信息安全测量模型的概述(第 5 章)；

——信息安全测量的管理职责(第 6 章)；

——信息安全测量方案中实施的测量构造和过程(即计划和制定、实施和运行、改进测量、沟通测量结果)(第 7～10 章)。

此外，附录 A 提供了信息安全测量构造的一个示例模板，测量构造的组成部分是信息安全测量模型的元素(见第 7 章)。附录 B 使用附录 A 给出的模板，为特定的 ISMS 控制措施或过程提供了测量构造示例。

这些示例的目的是帮助组织实施信息安全测量，并记录测量活动和结果。

5　信息安全测量概述

5.1　信息安全测量目标

在信息安全管理体系的背景下，信息安全测量的目标包括如下几个方面：

a)　评价已实施的控制措施或控制措施组的有效性[见图 1 中的 4.2.2 d)]；

b)　评价已实施的 ISMS 的有效性[见图 1 中的 4.2.3 b)]；

c)　验证满足已识别的安全要求的程度[见图 1 中的 4.2.3 c)]；

d)　在组织的总体业务风险方面，促进信息安全执行情况的改进；

e)　为了便于做出 ISMS 相关的决策，并证明已实施的 ISMS 所需的改进，为管理评审提供输入。

针对GB/T 22080—2008规定的规划-实施-检查-处置(PDCA)循环,图1给出了相关的测量活动及其他周期性输入——输出之间的关系。图中每个数字代表GB/T 22080—2008中的相应章节。

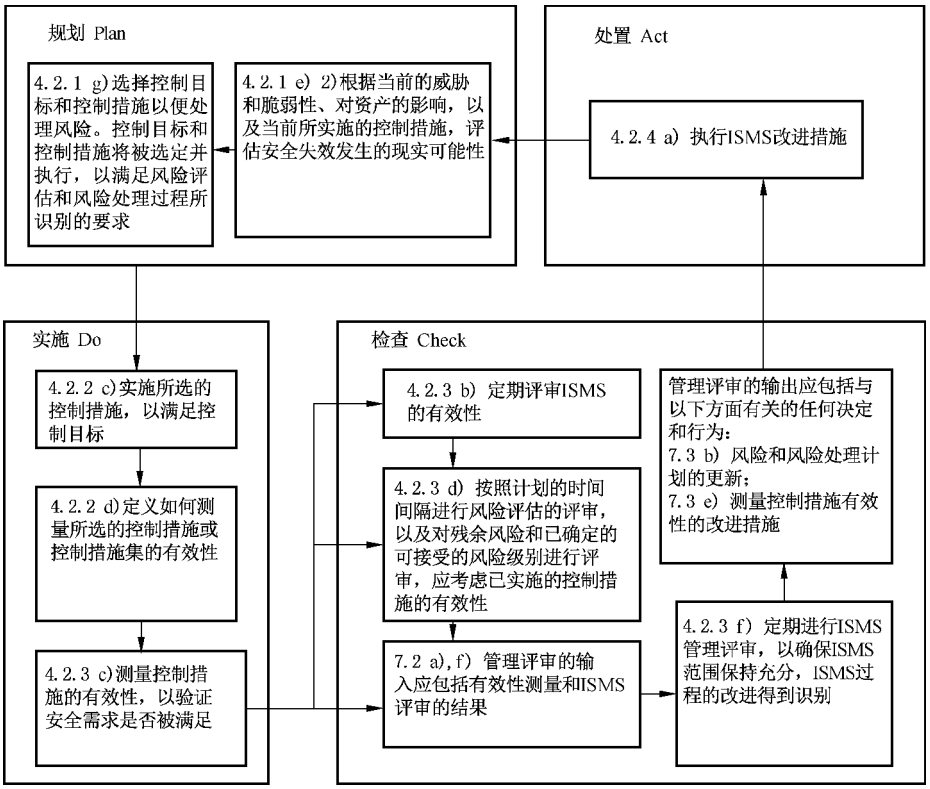


图1 信息安全管理的ISMS PDCA循环中的测量输入和输出

组织为了建立测量目标,宜考虑下列因素:

a) 在支持组织的总体业务活动中,信息安全的角色及其面临的风险;

b) 适用的法律法规、规章和合同要求;

c) 组织结构;

d) 实施信息安全测量的成本和效益;

e) 组织的风险接受准则;

f) 需要进行比较的同一组织的ISMS。

5.2 信息安全测量方案

为了便于实现既定的测量目标,组织宜建立并管理一个信息安全测量方案,并且在组织的整体测量活动中采用PDCA模型。为了便于获得可重复的、客观的和有用的测量结果,组织也宜基于信息安全测量模型(见5.4)制定和实施测量构造。

为了识别改进已实施的ISMS的需要,信息安全测量方案和已制定的测量构造宜确保组织有效地达到目标和可重复测量,并为利益相关者提供测量结果。这些改进需要包括ISMS的范围、策略、目标、控制措施、过程和规程。

一个信息安全测量方案宜包括以下过程:

a) 测度和测量的制定(见第7章);

b) 测量运行(见第8章);

c) 数据分析和测量结果报告(见第9章);

d) 信息安全测量方案的评价和改进(见第 10 章)。

宜通过考虑 ISMS 的规模和复杂性来确定信息安全测量方案的组织结构和运行结构。在任何情况下,信息安全测量方案的角色和职责宜明确赋予能胜任的人员(见 7.5.8)。

信息安全测量方案所选取和实施的测度宜直接与一个 ISMS 的运行、其他测度以及组织的业务过程相关。测量应被纳入定期的运行活动或按照 ISMS 管理者所确定的时间间隔定期执行。

5.3 成功因素

a) 为了有助于 ISMS 的持续改进,信息安全测量方案成功的一些因素如下:
   1) 管理者有关适当资源的承诺;
   2) 现有的 ISMS 过程和规程;
   3) 为了提供一段时间内的相关趋势,一个能够获取和报告有意义数据的可重复过程;
   4) 基于 ISMS 目标的可量化的测度;
   5) 容易获取的、可用于测量的数据;
   6) 对信息安全测量方案的有效性评价,以及实现所识别的改进;
   7) 以一种有意义的方式,持续的定期收集、分析和报告测量数据;
   8) 利益相关者使用该测量结果来识别改进已实施的 ISMS 的需要,包括 ISMS 的范围、策略、目标、控制措施、过程和规程;
   9) 从利益相关者那里接受有关测量结果的反馈;
   10) 评价测量结果的有用性,并实现所识别的改进。
b) 一旦信息安全测量方案被成功实施,它就可以:
   1) 证明组织对适用法律或法规的要求和合同义务的符合性;
   2) 支持对以前未被发现的或未知的信息安全问题的识别;
   3) 当说明历史和当前活动的测度时,协助满足管理报告的需要;
   4) 用作信息安全风险管理过程、内部 ISMS 审核和管理评审的输入。

5.4 信息安全测量模型

注:本标准采用的信息安全测量模型和测量构造的概念都是基于 GB/T 20917—2007 中的概念。本标准中使用的术语"测量结果"是 GB/T 20917—2007 中"信息产品"的同义词,本标准中使用的"测量方案"是 GB/T 20917—2007 中"测量过程"的同义词。

5.4.1 概述

信息安全测量模型是将信息需要和相关测量对象及其属性关联的结构。测量对象可包括已计划的或已实施的过程、规程、项目和资源。

信息安全测量模型描述如何将相关属性进行量化并转换为指标,以提供决策依据。图 2 给出了信息安全测量模型。

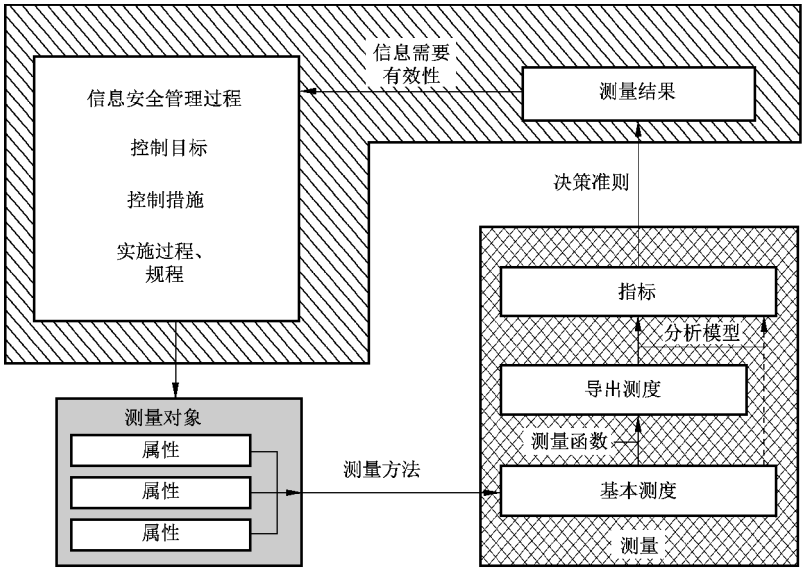


图 2　信息安全测量模型

注：第 7 章提供了关于信息安全测量模型的各个元素的详细信息。

本章接下来介绍模型的各个元素，并给出如何使用这些元素的示例。

表 1～表 4 的示例中使用的信息需要或测量意图，是用于评估相关人员符合组织安全策略的意识状态(GB/T 22080—2008 中控制目标 A.8.2、控制措施 A.8.2.1 和 A.8.2.2)。

5.4.2　基本测度和测量方法

基本测度是可获得的最简单的测度。基本测度是通过对一个测量对象所选择的属性应用一个测量方法而产生的。一个测量对象可能有许多属性，但只有部分属性可提供赋予基本测度的有用值。对于不同的基本测度，可使用一个给定的属性。

测量方法是一种逻辑操作序列，用于按指定标度量化属性。操作可能涉及例如统计出现次数或观测时间推移之类的活动。

一个测量方法能应用于一个测量对象的多个属性。例如，测量对象可以是：

——ISMS 中已实施的控制措施的执行情况；

——受控制措施保护的信息资产的状况；

——ISMS 中已实施的过程的执行情况；

——已实施的 ISMS 责任人的行为；

——信息安全责任部门的活动；

——感兴趣方的满意程度。

一个测量方法可以使用来自不同源测量和属性的测量对象，例如：

——风险分析和风险评估结果；

——问卷调查和人员访谈；

——内部和(或)外部审核报告；

——事件记录，如日志、报告统计和审计轨迹；

——事件报告，特别是那些产生影响的事件的报告；

——测试结果，如来自渗透试验、社会工程、符合性测试工具和安全审计工具的结果；

——与规程和方案相关的组织信息安全记录，如信息安全意识培训结果。

表 1～表 4 给出了在以下控制措施上信息安全模型的应用：

——“控制措施 2”是指 GB/T 22080—2008 的控制措施 A.8.2.1 管理职责(“管理者应要求雇员、承包方人员和第三方人员按照组织已建立的方针策略和规程对安全尽心尽力”)；被实施为“与 ISMS 相关的所有人员在被授权访问一个信息系统前必须签署用户协议”；

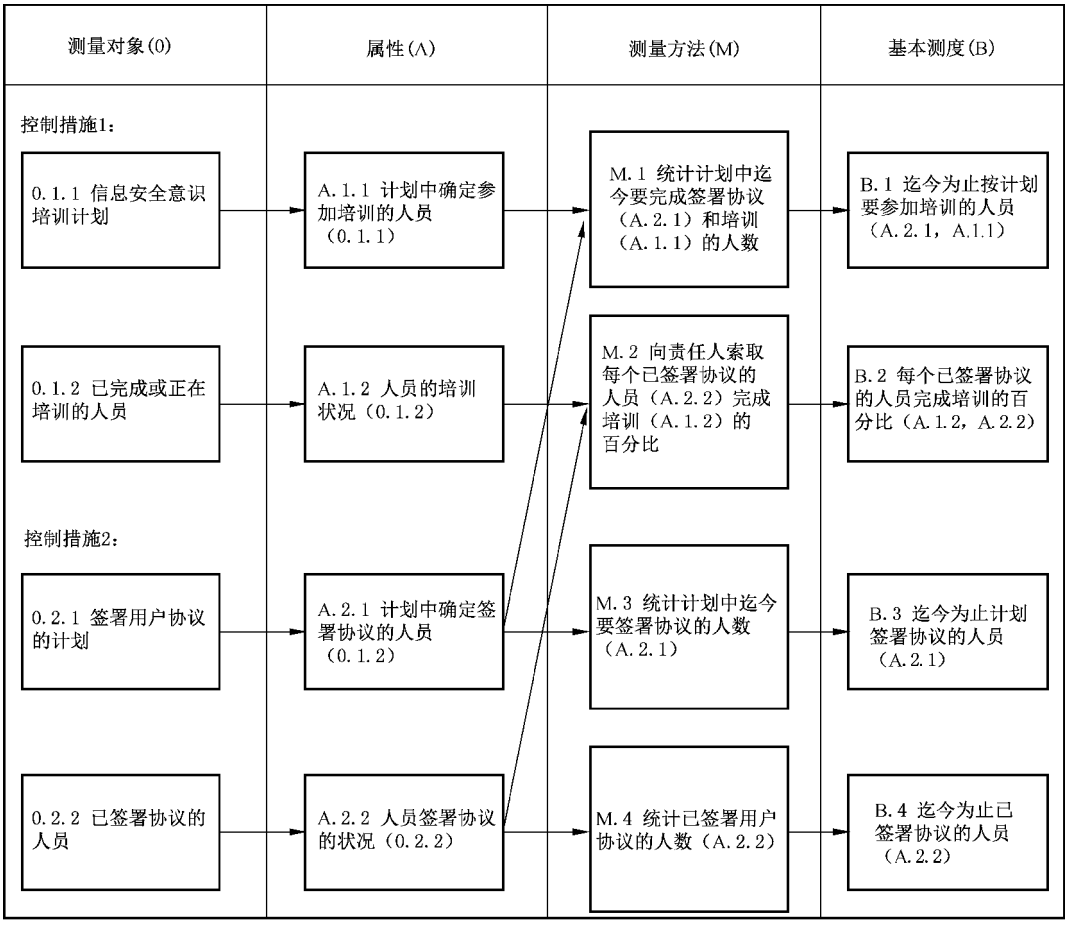
——“控制措施 1”是指 GB/T 22080—2008 的控制措施 A.8.2.2“信息安全意识、教育和培训”(“适当时，包括承包方人员和第三方人员在内的组织的所有雇员，应受到与其工作职能相关的适当的意识培训和组织方针策略及规程的定期更新培训”)；被实施为“所有 ISMS 相关人员在被授权访问一个信息系统前必须接受信息安全意识培训”。

相应的测量构造包含在 B.1 内。

注：表 1～表 4 由不同列组成(表 1 有 4 列，表 2～表 4 有 3 列)，其中各列被指定一个字母代号。每列中的方格被指定一个数字代号。字母和数字代号的组合被用于随后的方格，以便于参考之前的方格。箭头代表本示例中信息安全测量模型的个体元素之间的数据流。

为了测量以上描述的已实施控制措施所建立的对象，表 1 给出了测量对象、属性、测量方法以及基本测度之间关系的一个示例。

表 1　基本测度和测量方法示例



5.4.3　导出测度和测量函数

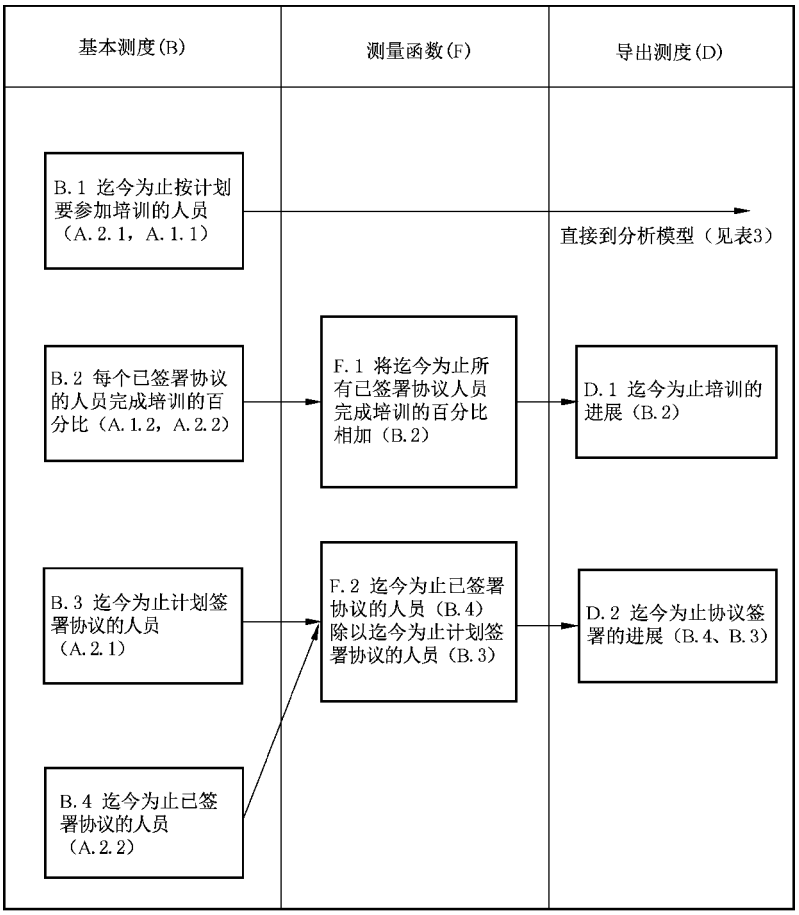
导出测度是两个或两个以上基本测度的聚集。一个给定的基本测度可作为多个导出测度的输入。测量函数是用于组合两个或两个以上基本测度，以生成一个导出测度的计算。

导出测度的标度和单位取决于组合的基本测度的标度和单位，以及测量函数组合这些基本测度的方法。

测量函数可涉及到多种技术，例如求基本测度的平均值、对基本测度进行加权、或给基本测度指定定性值。测量函数可使用不同的标度来组合基本测度，例如使用百分比和定性的评估结果。

就信息安全测量模型的应用，进一步涉及基本测度、测量函数和导出测度等元素，表 2 给出了它们之间关系的一个示例。

表 2　导出测度和测量函数的示例

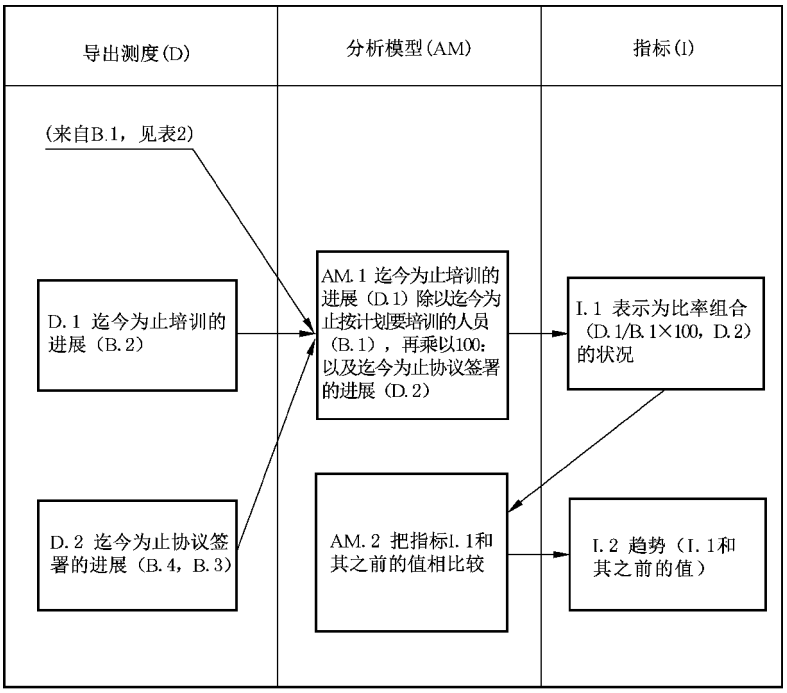


5.4.4　指标和分析模型

指标是一个测度，该测度依据一个分析模型，针对所定义的信息需要，提供所规约属性的一个估算和评价。指标是通过应用一个分析模型于一个基本和/或导出测度，并把它们与决策准则进行组合而获得的。标度和测量方法影响用于产生指标的分析技术的选择。

表 3 给出了信息安全测量模型应用的导出测度、分析模型和指标之间关系的一个示例。

表 3　指标和分析模型的示例



注：如果一个指标是以图形形式给出的，那么就要使之对残疾用户是可用的，或可用于单色拷贝。为此，宜尽可能使该指标包括颜色、暗影、铅字或其他可视化方法。

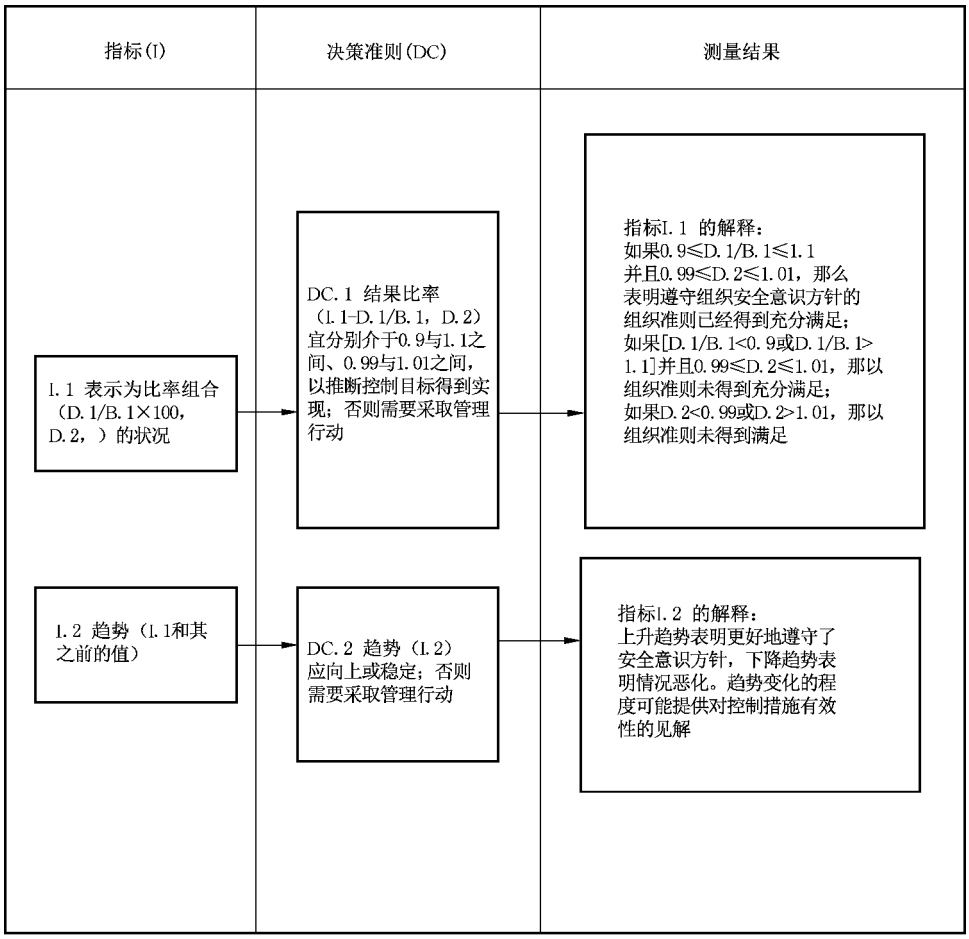
5.4.5　测量结果和决策准则

测量结果是基于确定的决策准则，通过解释适当的指标而产生的，并宜在评估 ISMS 有效性的整体测量目标的背景下来考虑。决策准则的目的是确定是否需要采取措施或进一步调查，同时用于描述给定测量结果的可信度。决策准则可适用于一系列的指标，例如基于在不同时间点获得的指标，进行趋势分析。

目标性能为组织或其部门提供了一种可用的、详细的性能规约。该目标性能来自信息安全目标（例如 ISMS 目标和控制目标），以及为了实现这些目标，需要建立和实现该目标性能。

表 4 给出了信息安全测量模型应用的指标、决策准则和测量结果之间关系的一个示例。

表 4　测量结果和决策准则的示例



6　管理职责

6.1　概述

管理者负责建立信息安全测量方案、吸纳利益相关者(见 7.5.8)参与测量活动、接受测量结果作为管理评审的输入以及在 ISMS 改进活动中使用测量结果。

为了完成上述职责，管理者宜：

a)　确定信息安全测量方案的目标；

b)　制定信息安全测量方案的策略；

c)　建立信息安全测量方案的角色和职责；

d)　提供足够的资源来执行测量，包括人员、资金、工具和基础设施；

e)　确保信息安全测量方案的目标得以实现；

f)　确保用于收集数据的工具和设备能够得到适当维护；

g)　为每一个测量构造建立测量意图；

h)　确保测量就 ISMS 有效性和已实施的 ISMS 的改进需求为利益相关者提供充足的信息，包括 ISMS 的范围、策略、目标、控制措施、过程和规程；

i)　确保测量就控制措施或控制措施组的有效性和改进已实施的控制措施的需求为利益相关者提供充足的信息。

通过适当分配测量角色和职责,管理者宜确保测量结果不受信息拥有者(见 7.5.8)的影响。这可通过职责分离来实现,或者可借助能够进行独立检查的详细文件来实现。

6.2 资源管理

为了支持测量必需的活动,例如数据收集、分析、存储、报告和发布,管理者宜分配和提供相应的资源。资源分配宜包括:

a) 负责信息安全测量方案的各个方面的人员支持;

b) 适当的资金支持;

c) 适当的基础设施支持,例如用于执行测量过程的物理基础设施和工具。

注:GB/T 22080—2008 中 5.2.1 规定了提供 ISMS 实施和运行所需资源的要求。

6.3 测量培训、意识和能力

管理者宜确保:

a) 对已实施的信息安全测量方案,利益相关者(见 7.5.8)在实现其角色和职责方面得到充分的培训,并且有能力执行其角色和职责;

b) 利益相关者了解其责任,包括为改进所实施的信息安全测量方案提出建议的责任。

7 测度和测量的制定

7.1 概述

为了评估已实施的 ISMS 和控制措施或控制措施组的有效性,并识别组织特定的测量构造集合,本章给出了如何编制测度和测量的指南。宜建立编制测度和测量所需的活动,并应建立相应的文件。活动包括:

a) 定义测量范围(见 7.2);

b) 识别信息需要(见 7.3);

c) 选择测量对象及其属性(见 7.4);

d) 制定测量构造(见 7.5);

e) 应用测量构造(见 7.6);

f) 确定数据收集和分析过程及报告(见 7.7);

g) 确定测量实施途经和相应的文件(见 7.8)。

在建立这些活动时,组织宜考虑资金、人力和基础设施(物理的和工具)资源。

7.2 测量范围的定义

由于组织能力和资源的缘故,测量活动的初始范围将受限于诸如特定的控制措施、受特定控制措施保护的信息资产、管理者给出最高优先级的特定信息安全活动等因素。随着时间的推移,考虑到利益相关者的优先级,为了处理已实施的 ISMS 和控制措施或控制措施组的深层要素,测量活动的范围还将可能扩大。

宜识别利益相关者,并宜使其参与到测量范围的定义之中。利益相关者可以是组织内部的或外部的,例如项目管理者、信息系统管理者或信息安全决策者。宜确定用于强调单个控制措施或控制措施组有效性的特定测量结果,并与利益相关者进行沟通。

为了确保决策者有能力根据报告的测量结果有效改进 ISMS,组织可考虑限制在给定时间间隔内向决策者报告的测量结果数量。因为报告的测量结果过多,会影响决策者集中精力和对未来改进活动进行优先级排序的能力。宜根据相应的信息需要及其相关 ISMS 目标的重要性来对测量结果进行优先

级排列。

注：测量范围是与根据 GB/T 22080—2008 中 4.2.1 a)确定的 ISMS 范围相关的。

7.3 信息需要的识别

每一个测量构造宜至少符合一个信息需要。附录 A 给出了一个信息需要的例子，该信息需要始于测量意图，终于相关的决策准则。

为了识别相关的信息需要，宜执行以下活动：

a) 检查 ISMS 及其过程，例如：

1) ISMS 策略和目标、控制目标和控制措施；

2) 法律法规、规章、合同和组织上的信息安全需要；

3) GB/T 22080—2008 中描述的信息安全风险管理过程结果。

b) 基于以下准则对已识别的信息需要进行优先级排序，例如：

1) 风险处置优先级；

2) 组织的能力和资源；

3) 利益相关者的利益；

4) 信息安全策略；

5) 满足法律法规、规章和合同所需的信息；

6) 相对于测量成本的信息价值。

c) 为优先级列表中所强调的测量活动，选择所需要的信息子集；

d) 建立所选的信息需要的文件，并与所有利益相关者进行沟通。

宜根据所选的信息需要实施所有相关测度，这些测度是应用于已实施的 ISMS、控制措施或控制措施组的。

7.4 对象及其属性的选择

宜在 ISMS 整体背景和范围内识别测量对象及其属性。宜注意一个测量对象可能有多个可用的属性。

测量用的对象及其属性宜根据相应信息需要的优先顺序来选择。

赋予相关基本测度的值是通过对所选属性应用适当的测量方法获得的。这一选择宜确保：

——能识别相关基本测度和适当的测量方法；

——基于获取值和已制定的测度，产生有意义的测量结果。

已选属性的特征决定了使用何种类型的测量方法(如定性或定量)，以获取赋予基本测度的值。

宜建立已选对象和属性的文件，并给出选择依据。

描述测量对象及其相应属性的数据宜用作赋予基本测度的值。测量对象的例子包括但不限于：

——产品和服务；

——过程；

——GB/T 22080—2008(A.7.1.1 资产清单)中已识别的可用资产，例如设施、应用和信息系统；

——业务单位；

——地理位置；

——第三方服务。

宜评审属性以确保：

a) 为测量选择了适当的属性；

b) 已确定了的收集数据能够为有效测量提供足够数量的属性。

宜选取仅与相应基本测度有关的属性。虽然属性的选择宜考虑在获取要测属性的难度，但不宜仅

选择那些容易获得的数据或容易测量的属性。

7.5 测量构造的制定

7.5.1 概述

从7.5.2(测度选择)～7.5.8(利益相关者)给出了测量构造的制定方法。

7.5.2 测度选择

宜识别可能满足已选信息需要的测度。为了实施所选择的测度,宜足够详细地定义已识别的测度。新识别的测度可涉及到现有测度的改变。

注:基本测度的识别是与测量对象及其属性的识别密切相关的。

宜选择可能满足已选信息需要的已识别的测度。也宜考虑解释或规范测度必需的背景信息。

注:可以选择许多不同的测度组合(即基本测度、导出测度和指标)用于处理特定的信息需要。

已选测度宜反映信息需要的优先顺序。更多可用于选择测度的示例准则包括:

——数据容易收集;

——为收集和管理数据,人力资源具有可用性;

——具有可用的适当工具;

——基本测度支持的潜在相关指标的数量;

——容易解释;

——已制定的测量结果的用户数量;

——该测度适合意图或信息需要的证据;

——收集、管理和分析该数据的成本。

7.5.3 定义测量方法

宜为每个基本测度定义一种测量方法。测量方法通过把属性变成赋予基本测度的值来量化测量对象。

测量方法可以是主观或客观的。主观方法依赖于涉及人为判断的量化;而客观方法使用基于诸如计算的数值规则的量化,可通过人工或自动化手段予以实现。

测量方法通过应用适当的标度将属性量化为值。每个标度都有测量单位。只用同一测量单位表示的量可以直接进行比较。

对于每个测量方法,宜建立验证过程,并建立相应的文件。验证宜确保通过对测量对象的属性应用一个测量方法得到的、并赋给基本测度的值的可信度。需要确定有效值时,用来获取属性的工具宜被标准化,并在规定的时间间隔内对其进行验证。

宜考虑测量方法的精度,并宜记录相关的偏差或变化。

为了便于在不同时间赋给基本测度的值是可比较的,赋给导出测度和指标的值也是可比较的,测量方法宜在整个时间内是一致的。

7.5.4 定义测量函数

宜为每个导出测度定义一个测量函数,应用该函数对两个或两个以上基本测度进行赋值。通过测量函数把对一个或多个基本测度的赋值变成对一个导出测度的赋值。在某些情况下,除了导出测度外,基本测度可直接作为分析模型的输入。

测量函数(例如一个计算)可能涉及多种技术,例如计算所有基本测度的赋值的平均值、对基本测度的赋值进行加权,或在把基本测度聚合成导出测度之前,给基本测度的赋值指定定性值。测量函数可采用不同标度来组合基本测度的赋值,例如采用百分比和定性评估结果。

7.5.5 定义分析模型

宜为每个指标确定分析模型,以便将一个或多个赋给基本测度和(或)导出测度的值转换成对该指标的赋值。

分析模型以一种对利益相关者产生有意义输出的方式,对相关测度进行组合。

当定义分析模型时,也宜考虑应用于指标的决策准则。

有时,一个分析模型可能是相当简单的,只是把一个导出测度的值转换成赋予一个指标的值。

7.5.6 指标的生成

通过聚合赋予导出测度的值来产生赋予指标的值,并基于决策准则解释这些值。对于报告给用户的每个指标,宜定义指标表达格式,作为报告格式的一部分(见 7.7)。

指标表述格式将直观地描述测度,并提供指标的逐字说明。指标表述格式宜客户化,以便满足客户的信息需要。

7.5.7 定义决策准则

宜基于信息安全目的,对每一个指标,定义相应的决策准则,以便为利益相关者提供措施方面上的指南。这一指南宜基于指标,强调期望的进展以及初始改进措施的阈值。

决策准则建立了一个性能目的,通过这一性能目的来度量测量方案的成功(见 5.3),并提供有关解释该指标是否接近该目标的指导。

宜对 ISMS 过程和控制性能、达到的目的以及对该 ISMS 的有效性评估等每一项,建立相应的性能目的。

管理者在初始数据收集之前可以不建立有关指标的性能目标。一旦识别了基于初始数据的纠正措施,那么就可以为一个特定的 ISMS 定义实际可用的决策准则和实施里程碑。如果在一个点上没有建立决策准则,那么管理者就宜评价该测量对象及其对应的测度是否为组织提供了所期望的值。

如果历史数据就开发的或选择的测度是可用的话,那么建立决策准则就可能是服务性的。过去所观察的趋势将提供以前存在的性能程度的见解,并指导创建实际可用的决策准则。决策准则可以计算出来,或基于所期望行为的概念上的理解。决策准则可以从历史数据、计划和直觉中导出,或按统计上的控制限度或统计上的可信度限度计算出来。

7.5.8 识别利益相关者

宜为每个基本和/或导出测度识别适当的利益相关者,并建立相应的文件。利益相关者可包括:

a) 测量委托人:要求或需要关于 ISMS、控制措施或控制措施组的有效性的信息的管理者或其他相关方;
b) 测量评审人:确认已制定的测量构造是否适合于评估 ISMS、控制措施或控制措施组的有效性的人员或部门;
c) 信息拥有人:拥有关于测量对象及其属性的信息,并且负责该测量的人员或部门;
d) 信息收集人:负责收集、记录和存储数据的人员或部门;
e) 信息沟通人:负责分析数据并负责沟通测量结果的人员或部门。

7.6 测量构造的应用

在应用测量构造中,其规约至少宜包括如下信息:

a) 测量目的;
b) 要测量的控制措施、特定控制措施、一组控制措施以及要测量的 ISMS 过程所实现的控制

目的；

c) 测量对象；

d) 要收集、使用的数据；

e) 数据收集和分析的过程；

f) 测量结果报告过程，包括报告格式；

g) 利益相关者的角色和职责；

h) 评审测量的周期，以确保其对信息需要是有用的。

附录A给出了一个通用的测量构造实例，包含a)～h)。附录B给出了应用于测量ISMS过程和控制措施的测量构造实例。

7.7 数据收集、分析和报告的建立

宜建立数据收集和分析的规程，并报告已产生测量结果的过程。如有需要，也宜建立支持工具、测量设备和技术。这些规程、工具、测量设备和技术将关注以下活动：

a) 数据收集，包括数据存储和验证(见8.3)。规程宜识别在使用测量方法、测量函数和分析模型中，如何收集数据，以及在任何特定信息环境下如何存储数据。为了验证丢失的数据是否是最小的，并且赋给每个测度的值是否是有效的，通过对照构造的检查表，检查数据来完成数据验证。

注：赋予基本测度的值的验证是与测量方法(见7.5.3)的验证密切相关的。

b) 数据分析和已产生的测量结果的报告。规程宜规定数据分析技术(见9.2)以及报告测量结果的频率、格式和方法。宜识别执行数据分析可能需要的工具范围。

报告格式的例子包括：

——记分卡，通过整合高层次指标，提供战略信息；

——可执行和可运行的仪表，其极少注重于战略目标，更多地受特定的控制措施和过程的有效性的约束；

——报表，其形式可以是简单和静态的报表(例如给定时期内的测度列表)，也可以是相当复杂的交叉报表，具有嵌套分组、滚动总结、动态追溯或链接功能。当用户需要查看原始数据时，报表最好使用容易阅读的格式。

——表示一个动态值的测量仪器，包括警报、附加的图形元素和终点标记。

7.8 测量实施途径和相应文件的建立

在一个实施计划中，宜建立测量整个途径的文件。该实施计划至少宜包括以下信息：

a) 组织信息安全测量方案的实施情况；

b) 如下的测量规约：

1) 组织通用的测量构造；

2) 组织独有的测量构造；

3) 数据收集、分析的范围和规程的定义；

c) 执行测量活动的日程计划；

d) 通过执行测量活动产生的记录，包括已收集的数据和分析记录；

e) 向管理者或利益相关者报告的测量结果的报告格式(见GB/T 22080—2008第7章“管理评审”)。

8 测量运行

8.1 概述

为了确保已产生的测量结果能为已实施的 ISMS、控制措施或一组控制措施的有效性提供准确的信息，信息安全测量的运行涉及一些必不可少的活动。

活动包括：

a) 将测量规程整合到整个 ISMS 的运行中；

b) 收集、存储并验证数据。

8.2 规程的整合

信息安全测量方案宜完全整合到 ISMS 中，并由该 ISMS 所使用。测量规程宜与 ISMS 运行相协调，包括：

a) 针对信息安全测量的制定、实施和维护，定义角色、授权和职责，并建立相应的文件；

b) 收集数据，并在必要时，为了配合数据的产生和收集活动，修改当前 ISMS 的运行；

c) 与利益相关者沟通数据收集活动中的变更；

d) 保持信息收集人能力，及其对已需要的数据类型、数据收集工具和数据收集规程的理解；

e) 有关定义测量在组织内的使用、测量信息的发布、信息安全测量方案的审核和评审，制定方针策略和规程；

f) 把数据分析和报告与相关过程进行整合，以便确保它们的正常执行；

g) 监视、评审和评价测量结果；

h) 为了确保测度和组织一起发展，建立逐步淘汰测度和增加新测度的过程；

i) 为了进行趋势分析，建立一个确定历史数据使用寿命的过程。

8.3 数据收集、存储和验证

数据收集、存储和验证活动包括：

a) 定期使用指定的测量方法收集所需的数据；

b) 建立数据收集的文件，包括：

1) 数据收集的日期、时间和地点；

2) 信息收集人；

3) 信息拥有人；

4) 在数据收集期间发生的、所有可能有用的问题；

5) 有关数据验证和测量确认的信息。

c) 按照测度选择准则和测量构造确认准则，验证所收集的数据。

宜整合已收集的数据和所有必要的背景信息，并以有利于进行数据分析的记录格式进行存储。

9 数据分析和测量结果报告

9.1 概述

为了产生测量结果，宜分析已收集的数据。宜通报已产生的测量结果。

活动包括：

a) 分析数据并产生测量结果；

b） 与利益相关者沟通测量结果。

9.2 分析数据并产生测量结果

宜使用决策准则分析和解释已收集的数据。在分析之前，数据可被整合、转换或重新记录。在分析数据期间，为了产生指标，宜对数据进行相应的处理。可应用到许多分析技术。宜根据数据特点和信息需要，确定分析的深度。

注：执行统计分析的指南可在 ISO/TR 10017(统计技术在 ISO 9001 中的应用指南)中找到。

宜解释数据分析结果。分析结果的人员(沟通者)宜能够根据结果得出初步结论。然而，由于沟通者可能不直接参与技术和管理过程，因此这些结论需要由其他利益相关者予以评审。所有的解释宜考虑测度的背景。

数据分析宜识别已实施的 ISMS、控制措施或控制措施组的预期测量结果与实际测量结果之间的差距。已识别的差距将能够指出已实施的 ISMS 的改进需要，包括 ISMS 的范围、方针策略、目标、控制措施、过程和规程。

宜识别那些被证明不符合或者不良性能的指标，并可把它们归类如下：

a） 风险处置计划失效于实施，或失效于控制措施或失效于 ISMS 过程的不充分实施、运行和管理(例如，控制措施和 ISMS 过程可能被威胁绕过)；

b） 风险评估失效于：

1） 控制措施或 ISMS 过程是无效的，因为它们要么不足以应对已估计的威胁(如因为低估了威胁发生的可能性)，要么不足以应对新的威胁；

2） 没有实施控制措施或 ISMS 过程，因为忽视了威胁。

按照信息安全测量方案的实施计划，宜采用适当的报告格式(见 7.7)，编制用于跟利益相关者沟通测量结果的报告。

为了确保数据的合理解释，分析结论宜由利益相关者予以评审。为了与利益相关者沟通，宜对数据分析的结果，建立相应的文件。

9.3 沟通测量结果

信息沟通者宜确定如何沟通信息安全测量结果，例如：

——确定哪些测量结果要向内部和向外部报告；

——测度列表要与单个利益相关者或相关方对应；

——提供特定测量结果，根据各组需要裁剪表述类型；

——为了评价测量结果的有用性和信息安全测量方案的有效性的需要，获取利益相关者反馈信息的方式。

信息沟通者宜与不同类型的内部利益相关者沟通测量结果。内部利益相关者包括但不限于：

——测量委托人(见 7.5.8)；

——信息拥有人(见 7.5.8)；

——承担信息安全风险管理的人员，特别是那些风险评估失效的人员；

——负责那些被识别为需要进行改进领域的人员。

有些情况下，会要求组织向外部各方(包括监管部门、利益相关者、客户和提供方)分发测量结果报告。建议组织向外部分发的测量结果报告只包含适合外部发布的数据，并且在发布前得到管理者和利益相关者的批准。

10 信息安全测量方案的评价和改进

10.1 概述

组织宜按计划的时间间隔评价以下方面：

a) 已实施的信息安全测量方案的有效性，以确保它：

1) 以有效的方式产生测量结果；

2) 可按计划予以执行；

3) 关注了已实施的 ISMS 和(或)控制措施的变化；

4) 关注了环境(如要求、法律或技术)的变化。

b) 已产生的测量结果的有用性，以确保已产生的测量结果满足相关的信息需要。

管理者宜规定这种评价的频率，规划定期修订，并建立使修订成为可能的机制(见 GB/T 22080—2008 7.2)。

宜包括以下相关活动：

1) 识别信息安全测量方案的评价准则(见 10.2)；

2) 监视、评审和评价测量(见 10.3)；

3) 实施改进(见 10.4)

10.2 识别信息安全测量方案的评价准则

组织宜为评价信息安全测量方案的有效性以及评价已产生的测量结果的有用性，定义相应的评价准则。该评价准则宜在开始实施信息安全测量方案时，通过考虑技术和组织业务目标予以定义。

在组织评价和改进已实施的信息安全测量方案时，最可能的准则包括：

——组织业务目标的变更；

——信息安全法律法规或规章的要求和合同义务的变更；

——组织信息安全要求的变更；

——组织信息安全风险的变更；

——为测量意图，增强更精细或更适宜数据的可用性，或增强数据收集方法的可用性；

——测量对象和(或)其属性的变更。

以下准则可应用于评价已产生的测量结果：

a) 测量结果是：

1) 易于理解的；

2) 以及时的方式进行沟通的；

3) 客观的、可比较的和可重新生成的。

b) 为了产生测量结果而建立的过程：

1) 被很好地定义；

2) 易于运行；

3) 被正确遵循。

c) 测量结果对改进信息安全有帮助。

d) 测量结果满足相应的信息需要。

10.3 监视、评审和评价信息安全测量方案

组织宜按照已确立的准则(见 10.2)，监视、评审和评价信息安全测量方案。

组织宜识别改进信息安全测量方案的潜在需求，包括：

a) 修订或删除已采用的、不再适用的测量构造；

b) 重新分配资源，以支持信息安全测量方案。

组织也宜识别改进已实施的 ISMS 的潜在需求，包括 ISMS 的范围、策略、目标、控制措施、过程和规程；为了便于在随后的评审期间进行比较和趋势分析，组织宜建立管理决策的文件。

组织宜与利益相关者沟通评价结果和已识别的潜在改进需求，方便其对必要的改进做出相应的决策。

组织宜确保获取利益相关者对评价结果和已识别的潜在改进需要的反馈。组织宜了解该反馈是对信息安全测量方案有效性的输入之一。

10.4 实施改进

组织宜确保利益相关者识别出信息安全测量方案所需要的改进[见 GB/T 22080—2008 中 7.3 e)]。已识别的改进宜得到管理者的批准。宜为已批准的计划建立相应的文件，并与适当的利益相关者进行沟通。

组织宜确保已批准的信息安全测量方案的改进能够按计划予以实施。

组织可应用项目管理技术来完成这些改进。

附 录 A
（资料性附录）
信息安全测量构造模板

附录 A 给出了一个信息安全测量构造的示例模板，根据 5.4 的描述，该模板包括 7.5 中所识别的所有成分。组织可根据自己的要求，对该模板进行适当的修改。

测量构造识别	
测量构造名称	测量名称
数字标识符	组织特定的唯一的数字标识符
测量构造的意图	描述引入该测量的理由
控制/过程目标	(已计划或实施的)测量的控制/过程的目标
控制措施(1)/过程(1)	要测量的控制措施/过程
控制措施(2)/过程(2)	可选：如适用(已计划或实施的)，在同一测度的控制措施/过程集内进一步要测的控制措施/过程
测量对象及其属性	
测量对象	对象(实体)是通过测量其属性来表征其特征的。对象可能包含过程、计划、项目、资源、系统或系统组件
属性	测量对象的特征或特性，可以通过人为的或自动的手段定量或定性方法予以区分
基本测度说明(对每一个基本测度[1…n])	
基本测度	利用一个属性及量化该属性所规约的测量方法来定义一个基本测度(例如受训人员数量、场所数量、迄今为止的累计成本)。当数据收集后，一个值被赋予给一个基本测度
测量方法	一种逻辑操作序列，用于按指定标度量化属性
测量方法类型	取决于用来量化属性的操作本质。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(例如统计)的量化
标度	值的一个有序集合；或由该基本测度的属性所映射的范畴
标度类型	取决于标度值间关系的本质。通常定义四种类型的标度：标称型标度、顺序型标度、间距型标度和比率型标度
测量单位	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，以便把两者的比率表示为一个数

导出测度说明	
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	为组合两个或两个以上基本测度而执行的算法或计算。导出测度的标度和单位取决于所组合的基本测度的标度和单位，以及组合这些基本测度的测量函数
指标说明	
指标	依据一个分析模型所导出的测度，该测度就所定义的一个信息需要，针对所规约的属性，提供了一个估算或评价。指标是分析和决策制定的基础
分析模型	按照相关的决策准则，组合一个或多个基本测度和(或)导出测度的算法或计算。分析模型基于基本测度和(或)导出测度和(或)它们在整个测量期间行为的理解或假设。模型产生与已确定的信息需要相关的评估或评价
决策准则说明	
决策准则	用于确定有关行动或进一步调查的需要，或者用于描述给定结果可信度的阈值、目标性能或模式。决策准则有助于解释测量结果
测量结果	
指标解释	样例指标(见指标描述中的样例图)宜如何解释的一个描述
报告格式	宜识别报告格式，并建立相应的文件。描述组织或信息责任人可能想记录的评论。报告格式将真实地描述测度，并提供指标的书面说明。报告格式宜针对该信息客户予以客户化
利益相关者	
测量委托人	要求或需要关于 ISMS、控制措施或控制措施组的有效性信息的管理者或其他相关方
测量评审人	确认已制定的测量构造是否适合于评估 ISMS、控制措施或控制措施组的有效性的人员或部门
信息责任人	拥有关于测量对象及其属性的信息，并且负责测量的人员或部门
信息收集人	负责收集、记录和存储数据的人员或部门
信息沟通人	负责分析数据并沟通测量结果的人员或组织部门
频率/周期	
数据收集频率	多久收集一次数据
数据分析频率	多久分析一次数据
测量结果报告频率	测量结果多久报告一次(可能比数据收集频率低)
测量修订	测量修订的日期(测量有效期满或更新)
测量周期	定义测量的周期

附 录 B
（资料性附录）
测量构造示例

以下给出了测量构造的示例。这些示例是为了说明如何使用附录 A 中提供的模板来应用本标准。

目次

相关的过程和控制措施(GB/T 22080—2008 中的章条或附录 A 中的控制措施编号)	相关的测量构造示例（本附录引用）	测量构造示例名称
4.2.2 h)	B.4.1	信息安全事件管理的有效性
5.2.2 d)	B.1.1	已完成 ISMS 培训的人员
8.2	B.4.2	纠正措施的执行情况
控制措施 A.6.1.8	B.3	ISMS 评审过程
控制措施 A.6.1.1 和 A.6.1.2	B.5	管理承诺
控制措施 A.6.2.3	B.10	第三方协议中的安全
控制措施 A.8.2. 和 A.8.2.2	B.1.2	信息安全培训
控制措施 A.8.2. 和 A.8.2.2	B.1.3	信息安全意识符合性
控制措施 A.9.1.2	B.7	物理入口控制
控制措施 A.9.2.4	B.9	定期维护管理
控制措施 A.10.4.1	B.6	防范恶意代码
控制措施 A.10.10.1 和 A.10.10.2	B.8	日志审查
控制措施 A.11.3.1	B.2.1	口令质量——手册
控制措施 A.11.3.1	B.2.2	口令质量——自动化

B.1 ISMS 培训

B.1.1 已完成 ISMS 培训的人员

测量构造识别	
测量构造名称	已完成 ISMS 培训的人员
数字标识符	组织特定的
测量构造的目的	确定控制措施,符合组织信息安全策略
控制/过程目标	5.2.2 (GB/T 22080—2008) 培训、意识和能力
控制措施(1)/过程(1)	5.2.2.d) (GB/T 22080—2008) 培训、意识和能力 组织应通过 d)保持教育、培训、技能、经历和资格的记录,确保所有被赋予 ISMS 职责的人员具有执行所要求任务的能力
控制措施(2)/过程(2)	可选:如适用(已计划或实施的),在同一测度的控制措施/过程集内进一步的控制措施/过程
测量对象及其属性	
测量对象	员工数据库
属性	培训记录
基本测度说明(1)	
基本测度	根据 ISMS 年度培训计划,已接受 ISMS 培训的员工数量。 必须接受 ISMS 培训的员工数量
测量方法	统计 ISMS 培训日志/登记簿上写为“已接受”的员工数量
测量方法类型	客观类
标度	个数
标度类型	比率标度
测量单位	员工
导出测度说明	
导出测度	已完成 ISMS 培训的人员百分比
测量函数	已接受 ISMS 培训的员工数量除以必须接受 ISMS 培训的员工数量×100
指标说明	
指标	用颜色标识的颜色代码。描绘与分析模型定义的阈值(红、黄、绿)有关的多个报告周期的符合性的柱状图。图表使用的报告周期的数量宜由组织定义
分析模型	0～60%——红色;60%～90%——黄色;90%～100% ——绿色。对于黄色,如果每季度没有达到至少 10%的进展,等级自动变为红色

决策准则说明	
决策准则	红色——要求干预,必须进行原因分析,以确定不符合和执行情况较差的原因。 黄色——可能变为红色,宜密切关注指标。 绿色——不需要采取行动
测量结果	
指标解释	组织特定的
报告格式	基于决策准则的有颜色代码条的柱状图。简短总结哪些测量工具和可能的管理活动宜附在柱状图上
利益相关者	
测量委托人	负责 ISMS 的管理者
测量评审人	负责 ISMS 的管理者
信息责任人	培训管理者——人力资源
信息收集人	培训管理者——人力资源部门
信息沟通人	负责 ISMS 的管理者
频率/周期	
数据收集频率	每月,当月的第一个工作日
数据分析频率	每季度
测量结果报告频率	每季度
测量修订	每年评审一次
测量周期	每年

B.1.2 信息安全培训

测量构造识别	
测量构造名称	信息安全培训
数字标识符	组织特定的
测量构造的目的	评价年度信息安全意识培训要求的符合性
控制/过程目标	A.8.2 任用中 目标:确保所有的雇员、承包方人员和第三方人员知悉信息安全威胁和利害关系、他们的职责和义务,并准备好在其正常工作过程中支持组织的安全策略,以减少人为出错的风险
控制措施(1)/过程(1)	A.8.2.2 (GB/T 22080—2008)信息安全意识、教育和培训 组织的所有雇员,适当时,包括承包方人员和第三方人员,应受到与其工作职能相关的适当的意识培训和组织方针策略及规程的定期更新培训

测量对象及其属性	
测量对象	员工数据库
属性	培训记录
基本测度说明(1)	
基本测度	已接受年度信息安全意识培训的员工数量。 需要接受年度信息安全意识培训的员工数量
测量方法	统计年度信息安全意识培训日志/登记簿上写为“已接受”的员工数量
测量方法类型	客观类
标度	个数
标度类型	比率标度
测量单位	员工
导出测度说明	
导出测度	已接受年度信息安全意识培训的人员百分比
测量函数	已接受年度信息安全意识培训的员工数量 / 必须接受年度信息安全意识培训的员工数量×100
指标说明	
指标	描绘与分析模型定义的阈值(红、黄、绿)有关的多个报告周期的符合性的柱状图。图表使用的报告周期的数量宜由组织定义
分析模型	0～60% ——红色；60%～90%——黄色；90%～100% ——绿色。对于黄色,如果每季度没有达到至少 10%的进展,等级自动变为红色
决策准则说明	
决策准则	红色——要求干预,必须进行原因分析,以确定不符合和执行情况较差的原因。 黄色——可能变为红色,宜密切关注指标。 绿色——不需要采取行动
测量结果	
指标解释	组织特定的
报告格式	基于决策准则的有颜色代码条的柱状图。简短总结哪些测量工具和可能的管理活动宜附在柱状图上
利益相关者	
测量委托人	负责 ISMS 的管理者、安全管理者、培训管理者
测量评审人	安全管理者
信息责任人	信息安全部门人员和培训管理者
信息收集人	培训管理者——人力资源部门
信息沟通人	负责 ISMS 的管理者

频率/周期	
数据收集频率	每月,当月的第一个工作日
数据分析频率	每季度
测量结果报告频率	每季度
测量修订	每年评审一次
测量周期	每年

B.1.3 信息安全意识符合性

测量构造识别	
测量构造名称	信息安全意识策略符合性
数字标识符	组织特定的
测量构造的目的	评估相关人员对组织安全意识策略的符合状况
控制/过程目标	A.8.2 任用中 确保所有的雇员、承包方人员和第三方人员知悉信息安全威胁和利害关系、他们的职责和义务,并准备好在其正常工作过程中支持组织的安全策略,以减少人为出错的风险
控制措施(1)/过程(1)	A.8.2.2 组织的所有雇员,适当时,包括承包方人员和第三方人员,应受到与其工作职能相关的适当的意识培训和组织方针策略及规程的定期更新培训。 (实施)所有 ISMS 相关人员在被授权访问一个信息系统前必须接受信息安全意识培训。 培训包括……
控制措施(2)/过程(2)	A.8.2.1 管理者应要求雇员、承包方人员和第三方人员按照组织已建立的方针策略和规程对安全尽心尽力。 (实施)与 ISMS 相关的所有人员在被授权访问一个信息系统前必须签署用户协议
测量对象及其属性	
测量对象	1.信息安全意识培训计划/时间表; 2.已完成或正在培训的人员; 3.签署用户协议的计划/时间表; 4.已签署协议的人员
属性	1.计划中确定参加培训的人员; 2.人员的培训状况; 3.计划中确定签署协议人员; 4.人员签署协议的状况

基本测度说明	
基本测度	1.迄今为止按计划要参加培训的人数； 2.已签署协议的人数； 3.迄今为止计划签署协议的人数； 4.迄今为止已签署协议的人数
测量方法	1.统计计划中迄今为止要完成签署协议和培训的人数； 2.向责任人索取已完成培训和签署协议人员的百分比； 3.统计计划中迄今要签署协议的人数； 4.统计已签署用户协议的人数
测量方法类型	1.客观类； 2.主观类； 3.客观类； 4.客观类
标度	1.从 0 到无穷大的整数； 2.从 0 到 100 的整数； 3.从 0 到无穷大的整数； 4.从 0 到无穷大的整数
标度类型	1.顺序标度； 2.比率标度； 3.顺序标度； 4.顺序标度
测量单位	1.人员； 2.百分率； 3.人员； 4.人员
导出测度说明	
导出测度	1.迄今为止培训的进展； 2.迄今为止协议签署的进展
测量函数	1.将迄今为止所有已签署协议人员完成培训的百分比相加； 2.迄今为止已签署协议的人员除以迄今为止计划签署协议的人员
指标说明	
指标	1.表示为比率组合的状况； 2.趋势
分析模型	1.迄今为止培训的进展除以迄今为止按计划要培训的人员，再乘以 100；以及迄今为止协议签署的进展； 2.把现状和之前的状况相比较

决策准则说明	
决策准则	1.结果比率宜分别在 0.9 与 1.1 之间、0.99 与 1.01 之间，以推断控制目标得以实现及不需要采取行动； 2.趋势宜向上或稳定
测量结果	
指标解释	指标 a）的解释宜包括以下方面： 当 0.9≤第一个比率≤1.1 且 0.99≤第二个比率≤1.01 时，表明符合组织安全意识策略的组织准则已得到充分满足；对应标准字体； 当[第一个比率＜0.9 或第一个比率＞1.1] 且 0.99≤第二个比率≤1.01时，组织准则未得到充分满足；对应斜体； 当第二个比率＜0.99 或第二个比率＞1.01 时，组织准则未得到满足；对应黑体。 指标 b）的解释宜包括以下方面： 上升趋势表明安全意识策略符合情况已改善，下降趋势表明情况恶化。趋势变化的程度可提供对控制措施实施有效性的深入了解。各趋势的明显变化指明控制措施实施要求进一步考察以确定原因。消极趋势可要求管理干预。积极趋势宜进行考察，以识别潜在的最佳实践
报告格式	标准字体＝准则已得到充分满足； 斜体＝准则未得到充分满足； 黑体＝准则未得到满足
利益相关者	
测量委托人	负责 ISMS 的管理者、安全管理者、培训管理者
测量评审人	安全管理者
信息责任人	信息安全部门人员和培训管理者
信息收集人	培训管理者—人力资源部门
信息沟通人	负责 ISMS 的管理者
频率/周期	
数据收集频率	每月，当月的第一个工作日
数据分析频率	每季度
测量结果报告频率	每季度
测量修订	每年评审一次
测量周期	每年

B.2 口令策略

B.2.1 口令质量——手册

测量构造识别	
测量构造名称	口令质量
数字标识符	组织特定的
测量构造的目的	评估用户用来访问组织的 IT 系统的口令质量
控制/过程目标	防止用户选择不安全的口令
控制措施(1)/过程(1)	A.11.3.1 应要求用户在选择和使用口令时,遵循良好的安全习惯。 实施。 所有用户必须为每个系统选择强口令,这些口令: 1.长度大于 8; 2.不是基于任何他人能轻易猜测或获取使用人的相关信息,如姓名、电话号码和出生日期等; 3.不是由词典内的词组成; 4.不是连贯相同的、全数字或全字母的字符。 组织的 IT 系统的所有用户账号和口令必须由员工系统控制
测量对象及其属性	
测量对象	用户口令数据库
属性	个人口令
基本测度说明	
基本测度	1.已注册口令的数量; 2.每个用户满足组织的口令策略的口令数量
测量方法	1.统计用户口令数据库中的口令数量; 2.求每个用户满足组织的口令策略的口令数量
测量方法类型	1.客观类; 2.主观类
标度	1.从 0 到无穷大的整数; 2.从 0 到无穷大的整数
标度类型	1.顺序标度; 2.顺序标度
测量单位	1.口令; 2.口令
导出测度说明	
导出测度	符合组织的口令质量策略的口令总数

测量函数	每个用户符合组织的口令质量策略的口令总数之和
指标说明	
指标	1.满足组织的口令质量策略的口令比率； 2.关于口令质量策略的符合状况趋势
分析模型	1.(符合组织的口令质量策略的口令总数)除以(已注册的口令数量)； 2.把比率与之前的比率相比较
决策准则说明	
决策准则	如果结果比率大于0.9,已实现控制目标,并不需要采取任何行动。如果结果比率在0.8～0.9之间,未实现控制目标,但向上趋势表明有改进。如果结果比率小于0.8,宜立即采取行动
测量结果	
指标解释	指标a)的解释宜包括以下方面： 比率＞0.9时,符合组织口令策略的组织准则得到充分满足。 0.8≤比率≤0.9时,符合组织口令策略的组织准则未得到充分满足。 比率＜0.8时,符合组织口令策略的组织准则未得到满足。 指标b)的解释宜包括以下方面： 上升趋势表明符合情况已改善,下降趋势表明符合情况恶化。 趋势变化的程度可提供对已实施的控制措施的有效性的深入了解。 消极趋势可要求进一步的控制措施,例如意识,或选择强口令或修改之前的口令的技术工具。 积极趋势宜进行考察,以从当前比率估计满足口令策略的必要条件。不满足准则的影响是增加了泄密的风险。 偏差的潜在原因包括安全意识的缺乏、技术实施的缺陷,以及实施所有IT系统所需时间的缺乏
报告格式	把描绘符合组织的口令质量策略的口令数量的趋势线,与前一报告提交时间段期间产生的趋势线进行叠加
利益相关者	
测量委托人	负责ISMS的管理者、安全管理者
测量评审人	安全管理者
信息责任人	系统管理员
信息收集人	安全人员
信息沟通人	安全人员
频率/周期	
数据收集频率	每年
数据分析频率	每年
测量结果报告频率	每年

测量修订	每年评审、更新一次
测量周期	每年

B.2.2 口令质量——自动化

测量构造识别	
测量构造名称	口令质量
数字标识符	组织特定的
测量构造的目的	评估用户用来访问组织的 IT 系统的口令质量
控制/过程目标	防止用户选择不安全的口令
控制措施(1)/过程(1)	A.11.3.1 应要求用户在选择和使用口令时,遵循良好的安全习惯。 实施。 所有用户必须为每个系统选择强口令,这些口令: 1.长度大于 8; 2.不是基于任何他人能轻易猜测或获取使用人的相关信息,如姓名、电话号码和出生日期等。 3.不是由词典内的词组成; 4.不是连贯相同的、全数字或全字母的字符。 组织的 IT 系统的所有用户账号和口令必须由员工系统控制。 必须使用口令破解软件检查口令的强韧性
测量对象及其属性	
测量对象	员工系统账户数据库
属性	存储在员工系统账户记录中的个人口令
基本测度说明(1)	
基本测度	1.口令总数; 2.不能破译的口令总数
测量方法	1.运行查询员工账户记录; 2.采用混合攻击的方式,对员工系统账户记录进行口令破解
测量方法类型	1.客观类; 2.客观类
标度	1.从 0 到无穷大的整数; 2.从 0 到无穷大的整数
标度类型	1.顺序标度; 2.顺序标度
测量单位	1.口令 2.口令

导出测度说明	
导出测度	无
测量函数	无
指标说明	
指标	1.在 4 小时内可破译口令的比率； 2.比率 1 的趋势
分析模型	1.不能破译的口令总数除以口令总数； 2.把比率与之前的比率进行比较
决策准则说明	
决策准则	如果结果比率大于 0.9，已实现控制目标，并不需要采取任何行动。如果结果比率在 0.8 和 0.9 之间，未实现控制目标，但向上趋势表明有改进。如果结果比率小于 0.8，宜立即采取行动
测量结果	
指标解释	指标 1 的解释宜包括以下方面： 比率＞0.9 时，符合组织口令策略的组织准则得到充分满足。 0.8≤比率≤0.9 时，符合组织口令策略的组织准则未得到充分满足。 比率＜0.8 时，符合组织口令策略的组织准则未得到满足。 指标 2 的解释宜包括以下方面： 上升趋势表明符合情况已改善，下降趋势表明符合情况恶化。 趋势变化的程度可提供已实施的控制措施的有效性的深入了解。 消极趋势可要求进一步的控制措施，例如意识，或选择强口令或修改之前的口令的技术工具。 积极趋势宜进行考察，以从当前比率估计满足口令策略的必要条件。不满足准则的影响是增加了口令妥协的风险，可导致未授权的系统访问。偏差的潜在原因包括安全意识的缺乏、技术实施的缺陷，以及实施所有 IT 系统所需时间的缺乏
报告格式	把描绘已测试的所有记录的口令可破解性的趋势线，与前一测试期间产生的趋势线进行叠加
利益相关者	
测量委托人	负责 ISMS 的管理者、安全管理者
测量评审人	安全管理者
信息责任人	系统管理员
信息收集人	安全人员
信息沟通人	安全人员
频率/周期	
数据收集频率	每周

数据分析频率	每周
测量结果报告频率	每周
测量修订	每年评审、更新一次
测量周期	适用 3 年

B.3 ISMS 评审过程

测量构造识别	
测量构造名称	ISMS 评审过程
数字标识符	组织特定的
测量构造的目的	评估信息安全的独立评审的完成程度
控制/过程目标	在组织内管理信息安全
控制措施(1)/过程(1)	A.6.1.8 组织管理信息安全的方法及其实施(即信息安全的控制目标、控制措施、策略、过程和规程)应按计划的时间间隔进行独立评审。当安全实施发生重大变化时,也要进行独立评审。 (实施) 组织管理信息安全的方法及其实施由第三方安全顾问每季度评审
测量对象及其属性	
测量对象	1.第三方评审报告; 2.第三方评审计划
属性	1.已报告的第三方评审; 2.已计划的第三方评审
基本测度说明	
基本测度	1.第三方已组织评审的数量; 2.已计划第三方评审的总数
测量方法	1.统计第三方已组织定期评审的报告数量; 2.统计已计划第三方评审的数量
测量方法类型	1.客观类; 2.客观类
标度	1.从 0 到无穷大的整数; 2.从 0 到无穷大的整数
标度类型	1.顺序标度; 2.顺序标度
测量单位	1.评审; 2.评审

导出测度说明	
导出测度	无
测量函数	无
指标说明	
指标	已完成独立评审的进度比率
分析模型	第三方已组织评审的数量除以已计划第三方评审的总数
决策准则说明	
决策准则	指标的结果比率宜在 0.8～1.1 之间，以推断控制目标的成效和不需要采取行动。如果不满足之前的条件，比率宜大于 0.6
测量结果	
指标解释	指标的解释宜包括以下方面： 0.8≤比率≤ 1.1 时，第三方评审的组织内管理信息安全的组织准则已得到充分满足。 0.6≤比率＜0.8 或 比率＞1.1 时，组织准则未得到充分满足。要求进行监视，以确保取得适当进展。 0≤比率＜0.6 时，组织准则未得到满足。要求立即干预，以确保取得适当进展。 如果在第二季度结束时指标不令人满意，需要采取纠正措施，并宜与负责 ISMS 的管理者沟通纠正措施。 如果在年终时指标不令人满意，必须告知高级管理者，并请求他们的支持。 不满足准则的影响是无效的管理评审过程。 偏差的可能原因包括低预算、不正确的规划，以及关键人员/管理者承诺的缺乏
报告格式	描绘与决策准则定义的阈值有关的、多个报告周期符合情况的柱状图
利益相关者	
测量委托人	负责 ISMS 的管理者、质量系统管理者
测量评审人	负责 ISMS 的管理者
信息责任人	负责 ISMS 的管理者
信息收集人	内部审计、质量管理者
信息沟通人	内部审计、质量管理者、负责 ISMS 的管理者
频率/周期	
数据收集频率	每季度
数据分析频率	每季度
测量结果报告频率	每季度
测量修订	每 2 年评审、更新一次
测量周期	适用 2 年

B.4 ISMS 持续改进

B.4.1 信息安全事件管理的有效性

测量构造识别	
测量构造名称	信息安全事件管理的有效性
数字标识符	组织特定的
测量构造的目的	评估信息安全事件管理的有效性
控制/过程目标	能够及时发觉安全事故并响应安全事件
控制措施(1)/过程(1)	4.2.2 h)(GB/T 22080—2008)
测量对象及其属性	
测量对象	ISMS
属性	单个事件
基本测度说明	
基本测度	之前规定的阈值数量
测量方法	统计数据报告的信息安全事件的发生率
测量方法类型	客观类
标度	个数
标度类型	顺序标度
测量单位	事件
导出测度说明	
导出测度	超过阈值的事件
测量函数	把所有事件的数量与阈值相比较
指标说明	
指标	描绘说明在多个报告提交时间段上违反事件总数的阈值数的不断的水平线的折线图
分析模型	当事件总数超过阈值(过了线)时,为红色; 当事件总数在阈值的 10%以内时,为黄色; 当事件总数低于阈值的 10%或 10%以上时,为绿色
决策准则说明	
决策准则	红色——要求立即调查增加事件数量的原因。 黄色——需要密切监视数量,如果数量没有改进,宜开始调查。 绿色——不需要采取行动

测量结果	
指标解释	如果在两个报告周期内看到红色,要求进行事件管理规程评审,以纠正现行规程或确定附加规程。如果在接下来两个报告提交时间段内不能扭转趋势,要求采取纠正措施,例如建议扩大 ISMS 范围
报告格式	折线图
利益相关者	
测量委托人	ISMS 管理委员会、负责 ISMS 的管理者、安全管理者、事件管理者
测量评审人	负责 ISMS 的管理者
信息责任人	负责 ISMS 的管理者
信息收集人	事件管理的管理者
信息沟通人	ISMS 管理委员会
频率/周期	
数据收集频率	每月
数据分析频率	每月
测量结果报告频率	每月
测量修订	6 个月
测量周期	每月

B.4.2 纠正措施的实施

测量构造识别	
测量构造名称	纠正措施的实施
数字标识符	组织特定的
测量构造的目的	评估纠正措施实施的执行情况
控制/过程目标	8.2 (GB/T 22080—2008)纠正措施 组织应采取措施,消除与 ISMS 要求不符合的原因,以防止再发生
控制措施(1)/过程(1)	形成文件的纠正措施规程,应规定以下方面的要求: 1.识别不符合; 2.确定不符合的原因; 3.评价确保不符合不再发生的措施需求; 4.确定和实施所需要的纠正措施;

控制措施(1)/过程(1)	5.记录所采取措施的结果(见 4.3.3)； 6.评审所采取的纠正措施。 (已实施) …… 组织确定要求的纠正措施,并发布记载有关不符合的信息的纠正措施报告、其原因,以及采取的纠正措施到期日。 收到报告后,负责检测不符合方面的管理者被要求确保没有不合理的延迟所采取的措施,以消除不符合及其原因。 如果按要求不实施纠正措施,必须识别不实施的原因,同时确定适当地替代原来的纠正措施。 所采取的带有相应日期和结果的措施宜形成文件。如果不按计划实施纠正措施,原因和替代措施必须形成文件。宜向信息安全管理者提供报告
测量对象及其属性	
测量对象	纠正措施报告
属性	报告内纠正措施到期日； 报告记录内已采取纠正措施的日期； 延迟和不采取措施的原因
基本测度说明	
基本测度	1.迄今为止已计划的纠正措施数量； 2.迄今为止按计划已实施的纠正措施数量； 3.迄今为止有原因不实施的纠正措施数量
测量方法	1.统计迄今为止按计划已实施的纠正措施数量； 2.统计到截止日期为止按已实施记录的纠正措施数量； 3.统计有原因已计划不采取的纠正措施数量
测量方法类型	1～3 客观类
标度	1～3 从 0 到无穷大的整数
标度类型	1～3 顺序标度
测量单位	1～3 纠正措施
导出测度说明	
导出测度	1.迄今为止不实施的纠正措施； 2.没有合理原因不实施的纠正措施

测量函数	1.(迄今为止已计划的纠正措施)减去(迄今为止按计划采取的纠正措施); 2.(迄今为止有原因已计划不采取的纠正措施)减去(迄今为止不实施的纠正措施)
指标说明	
指标	1.表示不实施的纠正措施的比率的状况; 2.表示没有原因不实施的纠正措施的比率 状况的趋势
分析模型	1.(迄今为止不实施的纠正措施)除以(迄今为止已计划的纠正措施); 2.(没有原因不实施的纠正措施)除以(迄今为止已计划的纠正措施); 3.把状况与之前的状况相比较
决策准则说明	
决策准则	为了推断出目标完成、不采取措施,指标 a)和 b)宜分别在 0.4～0.0、0.2～0.0 之间,而且指标 c)的趋势宜在最后 2 个报告时间段下降。指标 c)宜与之前的指标进行比较。以便能调查纠正措施实施的趋势
测量结果	
指标解释	指标 a)和 b)的解释宜包括以下方面: 必须实施已计划的纠正措施,除非组织的优先事项已经改变,导致需要实施不同的纠正措施或分配给纠正措施实施的资源重定向。如果不管原因,纠正措施 40%以上没有被实施,要求采取管理措施。如果没有很好的理由,20%以上纠正措施未被实施,要求采取管理措施。宜调查没有实施的纠正措施,以识别不实施的原因。根据不实施的总百分比和原因,可要求采取进一步的措施。 指标 c)的解释宜包括以下方面: 因为任何表现的整体恶化或表现显著改善,宜调查纠正措施实施的趋势。如果在最后 2 个报告时间段已实施的纠正措施的比例已稳步下降,不管不符合的原因荡然无存,要求采取管理措施。 不满足准则的影响是 IMS 持续改进的潜在缺乏。 潜在原因可包括资源缺乏、不正确的计划,以及关键人员和管理承诺的缺乏
报告格式	用测量结果的陈述堆积的条形图,包括调查结果的执行概要和可能的管理措施,描述纠正措施的总数,分成已实施的、无合理的理由不实施的,以及有合理的理由不实施的
利益相关者	
测量委托人	负责 ISMS 的管理者、信息安全管理者
测量评审人	负责 ISMS 的管理者
信息责任人	负责 ISMS 的管理者
信息收集人	负责 ISMS 的管理者

信息沟通人	负责 ISMS 的管理者
频率/周期	
数据收集频率	每季度
数据分析频率	每季度
测量结果报告频率	每季度
测量修订	每年评审一次
测量周期	适用 1 年

B.5 管理承诺

测量构造识别	
测量构造名称	管理评审频率
数字标识符	组织特定的
测量构造的目的	评价与管理评审活动有关的管理承诺和信息安全评审活动
控制/过程目标	A.6.1 管理(已计划的)组织范围内的信息安全 管理组织范围内的信息安全,通过规范地执行管理评审
控制措施(1)/过程(1)	A.6.1.1 信息安全管理的管理承诺应通过清晰的说明、可证实的承诺、明确的分配及(已实施的)信息安全确认,积极支持组织内的安全。 组织必须每月召开管理评审会,通过清晰的说明、可证实的承诺、明确的分配及信息安全确认,以支持组织内的安全。 ISMS 管理评审宜结合 QMS 管理评审
控制措施(2)/过程(2)	A.6.1.2 信息安全活动应由组织不同部门并具备相关角色和工作职责的代表进行协调。 (已实施的) 具备相关角色的不同部门的代表宜协调和参加管理评审
测量对象及其属性	
测量对象	1.信息安全管理评审计划/时间表; 2.管理评审会议记录
属性	1.定于本计划内的管理评审会日期; 2.计划参加管理评审会的管理者; 3.记录在会议纪要的管理评审会日期; 4.作为已参加过管理评审会而被记录的管理者

基本测度说明	
基本测度	1.迄今为止已计划的管理评审会的数量； 2.计划参加管理评审会的管理者数量； 3.迄今为止按计划已召开的管理评审会的数量； 4.迄今为止计划外已召开的管理评审会的数量； 5.迄今为止已重新安排、召开的管理评审会的数量； 6.迄今为止已参加过管理评审会的管理者数量
测量方法	1.统计迄今为止已安排的管理评审会； 2.迄今为止每个管理评审会，统计计划出席的管理人，并增加通过特别的方式完成计划外会议的默认值的新入口； 3.统计到目前为止按计划召开的管理评审会； 4.统计到目前为止计划外召开的管理评审会； 5.到目前为止重新安排召开的管理评审会； 6.统计所有已召开的管理评审会出席的管理人的数量
测量方法类型	1.客观类； 2.客观类或主观类； 3.客观类； 4.客观类； 5.客观类； 6.客观类
标度	1.从 0 到无穷大的整数； 2.从 0 到无穷大的整数； 3.从 0 到无穷大的整数； 4.从 0 到无穷大的整数； 5.从 0 到无穷大的整数； 6.从 0 到无穷大的整数
标度类型	1.顺序标度； 2.顺序标度； 3.顺序标度； 4.顺序标度； 5.顺序标度； 6.顺序标度
测量单位	1.会议； 2.人员； 3.会议； 4.会议； 5.会议； 6.人员
导出测度说明	
导出测度	1.到目前为止已召开的管理评审会的数量； 2.到目前为止已召开的管理评审会的参与率

测量函数	1.把(到目前为止已计划的管理评审会的数量)、(到目前为止计划外的管理评审会的数量)和(到目前为止已重新安排的管理评审会的数量)相加； 2.对于每次管理评审会,(已参加过管理评审会的管理人的数量)除以(已安排参加管理评审会的管理人的数量)
指标说明	
指标	1.到目前为止已结束的管理评审会； 2.到目前为止管理评审会的平均参与率
分析模型	1.已完成的管理评审会除以已安排的管理评审会； 2.计算管理评审会的所有参与率的平均值和标准偏差
决策准则说明	
决策准则	指标 a)的结果比率宜在 0.7 和 1.1 之间,以推断控制目标的成效和不需要采取行动。即使不满足,比率宜大于 0.5,以推断最小成效。 关于指标 b),基于标准偏差计算的置信界限表明接近平均参与率的实际结果将会被实现的可能性。很宽的置信界限暗示一个潜在地巨大背离和对处理这个结果的应急计划的需要
测量结果	
指标解释	指标 a) 的解释宜包括以下方面： 当 0.7≤比率≤1.1 时,在组织彻底的管理评审内管理信息安全的组织准则已得到充分满足； 当 0.5≤比率＜0.7 或比率＞1.1 时,组织准则未得到充分满足。这个结果可表明可能缺乏管理承诺,并可要求纠正措施。随后的测量结果宜被监视和评价。 0≤比率＜0.5 时,组织准则未得到满足。这个结果表明缺少管理承诺,并要求立即干预,以实施一个适当的纠正措施。高层管理者宜被告知结果。比率接近 0,可表明缺少高层管理承诺。如果 ISMS 管理者不优先考虑 ISMS 管理评审,他们可被高层管理者影响。 不满足准则的影响是持续和有效的管理评审过程的潜在缺乏。 在指标 b)内偏差的潜在原因可能包括不正确的计划、负责 ISMS 的管理者不足的承诺、优先级冲突和(或)劳累过度影响 ISMS 管理者
报告格式	折线图,描绘与关于几个数据收集的准则一起的指标和与测量结果声明一起的报告提交时间段。数据收集数量和报告提交时间段宜被组织限定
利益相关者	
测量委托人	负责 ISMS 的管理者、质量系统管理者
测量评审人	ISMS 内部审核方案的专家
信息责任人	质量系统管理者 承担 QMS 和 ISMS 综合管理系统者
信息收集人	质量管理者、信息安全管理者

信息沟通人	信息安全管理者、质量管理者
频率/周期	
数据收集频率	每月
数据分析频率	每季度
测量结果报告频率	每季度
测量修订	每 2 年评审、更新一次
测量周期	适用 2 年

B.6 防范恶意代码

测量构造识别	
测量构造名称	防范恶意软件
数字标识符	组织特定的
测量构造的目的	评估防范恶意软件攻击的系统的有效性
控制/过程目标	控制目标 A.10.4(GB/T 22080—2008)保护软件和信息的完整性。 (已计划的) 保护软件和信息的完整性,使其不受恶意软件攻击
控制措施(1)/过程(1)	控制措施 10.4.1(GB/T 22080—2008) 控制恶意代码 应实施恶意代码的检测、预防和恢复的控制措施,以及适当的提高用户安全意识的规程
测量对象及其属性	
测量对象	1.事件报告; 2.恶意软件的对策软件的日志
属性	恶意软件产生的事件
基本测度说明	
基本测度	1.恶意软件造成的安全事件数量; 2.恶意软件造成的阻止攻击
测量方法	1.统计事件报告中恶意软件造成的安全事件数量; 2.统计阻止攻击的记录数量
测量方法类型	1.客观类; 2.客观类
标度	1.从 0 到无穷大的整数; 2.从 0 到无穷大的整数
标度类型	1.顺序标度; 2.顺序标度

测量单位	1.安全事件； 2.记录
导出测度说明	
导出测度	恶意软件防范力度
测量函数	恶意软件造成的安全事件数量/恶意软件造成的检测和阻止攻击的数量
指标说明	
指标	在多个报告提交时间段没有被阻止的已检测到的攻击的趋势
分析模型	把比率与之前的百分比相比较
决策准则说明	
决策准则	趋势线宜保持在规定数量下面。结果趋势宜向下或保持不变
测量结果	
指标解释	向上趋势表明符合性恶化，向下趋势表明符合性得到改进；并且当趋势明显上升时，宜需要调查原因和进一步的对策空间
报告格式	描绘恶意软件检测和预防的比率的趋势线，以及前一报告提交时间段期间生成的线
利益相关者	
测量委托人	安全管理者
测量评审人	安全管理者
信息责任人	系统管理员
信息收集人	安全管理者、系统管理员、网络管理者
信息沟通人	服务协调
频率/周期	
数据收集频率	每日
数据分析频率	每月
测量结果报告频率	每月
测量修订	每年评审一次
测量周期	适用 1 年

B.7 物理入口控制

测量构造识别	
测量构造名称	有准入卡的物理入口控制
数字标识符	组织特定的

测量构造的目的	显示用于访问控制的系统的存在、程度和质量
控制/过程目标	控制目标 A.9.1(GB/T 22080—2008)防止对组织场所和信息的未授权物理访问、损坏和干扰
控制措施(1)/过程(1)	控制措施 A.9.1.2(GB/T 22080—2008)物理入口控制 安全区域应由适合的入口控制进行保护,以确保只有授权的人员才允许访问
测量对象及其属性	
测量对象	安全领域
属性	身份管理记录
基本测度说明	
基本测度	有准入卡的物理入口控制
测量方法	一种相对测量方法,这种方法中每个低级别是高级别的子集。从以下方面控制和检查入口控制系统的类型: ——门禁一卡通系统的存在; ——PIN 口令使用; ——日志功能; ——生物特征鉴别
测量方法类型	主观类
标度	0～5 0 没有门禁系统。 1 有一个门禁系统,使用 PIN 口令(一个要素系统)来进行入口控制。 2 有一个门禁一卡通系统,使用通行卡(一个要素系统)来进行入口控制。 3 有一个门禁一卡通系统,使用通行卡和 PIN 口令来进行入口控制。 4 之前的+已激活的日志功能。 5 之前的+被生物特征鉴别(指纹、声音识别、视网膜扫描等)取代的 PIN 口令
标度类型	顺序标度
测量单位	—
导出测度说明	
导出测度	无
测量函数	无
指标说明	
指标	进度条。红色一直到 0.8,绿色在 0.8 和 1 之间
分析模型	测度分析

决策准则说明	
决策准则	值＝3 令人满意的
测量结果	
指标解释	低于 3,令人不满意(3－实际等级＝安全差距),基于安全差距程度采取行动。 超过 3,令人满意的、优秀的,级别可表明关于已测量的问题超过投资
报告格式	图表
利益相关者	
测量委托人	管理委员会
测量评审人	内部审核人/外部审核人
信息责任人	设备管理者
信息收集人	内部审核人/外部审核人
信息沟通人	内部审核人和安全管理者
频率/周期	
数据收集频率	每年
数据分析频率	每年
测量结果报告频率	每年
测量修订	12 个月
测量周期	适用 12 个月

B.8 日志文件评审

测量构造识别	
测量构造名称	日志文件评审
数字标识符	唯一的组织特定的数字标识符
测量构造的目的	评估决定性的系统日志文件的定期评审的符合状况
控制目标	控制目标 A.10.10(GB/T 22080—2008)检测未经授权的信息处理活动(已计划的) 从系统日志检测决定性的系统的未经授权的信息处理活动
控制措施(1)	控制目标 A.10.10.2(GB/T 22080—2008)。应建立信息处理设施的监视使用规程,并经常评审监视活动的结果
测量对象及其属性	
测量对象	系统
属性	单个日志文件

基本测度说明(1)	
基本测度	日志文件数量
测量方法	把评审日志清单中列出的日志文件总数相加
测量方法类型	客观类
标度	从 0 到无穷大的整数
标度类型	顺序标度
测量单位	日志文件
基本测度说明(2)	
基本测度	已评审的日志文件数量
测量方法	把 ISMS 范围内的所有系统上的日志文件总数相加
测量方法类型	客观类
标度	个数
标度类型	比率标度
测量单位	日志文件
基本测度说明(3)	
基本测度	ISMS 范围内的系统数量
测量方法	识别已评审的日志文件的数量
测量方法类型	客观类
标度	个数
标度类型	比率标度
测量单位	日志文件
导出测度说明	
导出测度	每个时间段要求的已评审的审核日志文件的百分比
测量函数	规定时间段内已评审的日志文件的数量除以日志文件的总数×100
指标说明	
指标	贯穿审核日志评审进度内的时间段的趋势线图
分析模型	上升趋势接近 100%是可取的
决策准则说明	
决策准则	结果低于 20%,宜检查表现较差的原因

测量结果	
指标解释	低于组织指定值的值是令人不满意的(组织指定值－实际值＝安全差距)。根据安全差距程度,要求采取管理措施。大于组织指定值的值可表明超出投资,除非这些访问控制机制是按每个风险评估要求的
报告格式	折线图,描绘调查结果总结和任何已建议的管理措施的趋势。
利益相关者	
测量委托人	负责 ISMS 的管理者、安全管理者
测量评审人	安全管理者
信息责任人	安全管理者
信息收集人	安全人员
信息沟通人	安全人员
频率/周期	
数据收集频率	每月
数据分析频率	每月
测量结果报告频率	每季度
测量修订	每 2 年评审、更新一次
测量周期	适用 2 年

B.9 定期维护管理

测量构造识别	
测量构造名称	定期维护管理
数字标识符	组织特定的
测量构造的目的	评价时间表内维护活动的及时性
控制目标	控制目标 A.9.2(GB/T 22080—2008)防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。 (已计划的) 通过定期系统维护,防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断
控制措施(1)	控制目标 A.9.2.4(GB/T 22080—2008)设备应予以正确地维护,以确保其持续的可用性和完整性
测量对象及其属性	
测量对象	1.系统维护计划/时间表; 2.系统维护记录

属性	1.已计划/安排的系统维护日期； 2.已完成的系统维护日期
基本测度说明(1～4)	
基本测度	1.已安排的维护日期； 2.已完成维护的日期； 3.已计划的维护事件的总数； 4.已完成的维护事件的总数
测量方法	1.从系统维护计划中获取已安排日期； 2.从系统维护记录中获取已完成日期； 3.统计系统维护计划内已计划的维护事件的数量； 4.统计维护记录
测量方法类型	客观类
标度	1. 时间； 2. 时间； 3. 从 0 到无穷大的整数； 4. 从 0 到无穷大的整数
标度类型	1.表； 2.表； 3.顺序标度； 4.顺序标度
测量单位	1. 区间； 2. 区间； 3. 维护事件； 4. 维护事件
导出测度说明	
导出测度	每个已完成的维护事件的维护延迟
测量函数	对于每个已完成的事件,已安排的维护日期减去实际维护日期
指标说明	
指标	1.平均维护延迟； 2.已完成的维护事件的比率； 3.平均维护延迟的趋势； 4.已完成的维护事件的比率的趋势
分析模型	1.每个已完成的维护事件的维护延迟的总和除以已完成的维护事件的数量； 2.已完成的维护事件的数量除以已计划的维护事件的数量； 3.比较在多个时间段内的指标 1； 4.比较在多个时间段内的指标 2

决策准则说明	
决策准则	1.组织特定的,例如,如果超过 3 天平均延迟始终显示,需要调查原因; 2.已完成的维护事件的比率宜大于 0.9; 3.趋势宜稳定或接近 0; 4.趋势宜稳定或向上
测量结果	
指标解释	指标有助于衡量设备维护过程的质量
报告格式	折线图,描绘维护延迟的平均偏差,与前一报告提交时间段产生的线、在范围内的系统数量进行叠加。 对潜在管理措施的调查结果和建议的解释
利益相关者	
测量委托人	负责 ISMS 的管理者、安全管理者
测量评审人	安全管理者
信息责任人	系统管理员
信息收集人	安全人员
信息沟通人	安全人员
频率/周期	
数据收集频率	每年
数据分析频率	每年
测量结果报告频率	每年
测量修订	每年
测量周期	每年

B.10 第三方协议中的安全

测量构造识别	
测量构造名称	第三方协议中的安全
数字标识符	组织特定的
测量构造的目的	评价处理个人信息处理的第三方协议的安全程度
控制/过程目标	控制目标 A.6.2(GB/T 22080—2008)保持组织被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全
控制措施(1)/过程(1)	控制目标 A.6.2.3(GB/T 22080—2008)涉及访问、处理或管理组织的信息或信息处理设施以及与之通信的第三方协议,或在信息处理设施中增加产品或服务的第三方协议,应涵盖所有相关的安全要求

测量对象及其属性	
测量对象	第三方协议
属性	每个第三方协议内的安全条款或要求
基本测度说明(1)	
基本测度	第三方协议的数量
测量方法	评审第三方协议,统计协议数量
测量方法类型	客观类
Scale 标度	从 0 到无穷大的整数
标度类型	顺序标度
测量单位	第三方协议
基本测度说明(2)	
基本测度	第三方协议所要求的标准安全要求的数量
测量方法	识别必须在每个协议策略内处理的安全要求的数量
测量方法类型	客观类
标度	从 0 到无穷大的整数
标度类型	顺序标度
测量单位	要求
基本测度说明(3)	
基本测度	在每个第三方协议内已处理的安全要求的数量
测量方法	评审第三方协议,统计每个协议内已处理的安全要求数量
测量方法类型	客观类
标度	从 0 到无穷大的整数
标度类型	顺序标度
测量单位	要求
导出测度说明	
导出测度	在第三方协议中已处理的相关安全要求的平均百分比
测量函数	每个协议(已要求的要求数量－已处理的要求数量)的总和除以协议数量
指标说明	
指标	1.已处理要求的不同标准要求的平均比率; 2.比率的趋势

分析模型	1.每个协议(已处理的安全要求总数)—(标准安全要求总数)的总和除以第三方协议的数量 2.与前一指标 1 相比较
决策准则说明	
决策准则	1.指标 1 宜大于 0.9; 2.指标 2 宜保持不变或向上
测量结果	
指标解释	本指标提供了对处理安全要求的外包功能的能力的深刻见解
报告格式	描绘在多个报告提交时间段的趋势的折线图。调查结果的简短总结和可能的管理措施
利益相关者	
测量委托人	负责 ISMS 的管理者、安全管理者
测量评审人	安全管理者
信息责任人	合同管理办公室
信息收集人	安全人员
信息沟通人	安全人员
频率/周期	
数据收集频率	每月
数据分析频率	每季度
测量结果报告频率	每季度
测量修订	2 年
测量周期	适用 2 年

参 考 文 献

[1] GB/T 19000—2008 质量管理体系 基础和术语
[2] GB/Z 19027—2005 GB/T 19001—2000 的统计技术指南
[3] GB/T 20917—2007 软件工程 软件测量过程
[4] GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理
[5] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则
[6] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
[7] ISO/IEC 15504-3:2004 信息技术 过程评定 第三部分:评定执行指南
[8] ISO Guide 99:2007 国际计量学词汇 基本和通用概念及相关术语(VIM)
[9] NIST SP 800-55 信息安全执行测量指南,2008 年 7 月

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术
信息安全管理 测量
GB/T 31497—2015/ISO/IEC 27004:2009
*
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:155066·1-51117

GB/T 31497-2015