参 考 文 献

[17] ISO/IEC 18045:2008 信息技术 安全技术 IT 安全评估方法学(Information technology—Security techniques—Methodology for IT security evaluation)

[18] ISO/IEC TR 19791:2006 信息技术 安全技术 操作系统的安全评估(Information technology—Security techniques—Security assessment of operational systems)

[19] ISO/IEC 20000-1:2005 信息技术 服务管理 第1部分:规范(Information technology—Service management—Part 1: Specification)

[20] ISO/IEC 27001:2005 信息技术 安全技术 信息安全管理体系 要求(Information technology—Security techniques—Information security management systems—Requirements)

[21] ISO 21500:2012 项目管理 项目管理操作(Project management—Guide to project management)

GB/T 31496—2015/ISO/IEC 27003:2010

GB/T 31496-2015

*

书号:155066·1-51118

定价: 48.00 元

ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31496—2015/ISO/IEC 27003:2010

信息技术 安全技术 信息安全管理体系实施指南

Information technology—Security techniques—Information securitymanagement system implementation guidance

(ISO/IEC 27003:2010,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

参 考 文 献

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

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

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

[4] 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要求(IDT ISO/IEC 27006:2007)

[5] ISO 9001:2008 质量管理体系 要求(Quality management systems—Requirements)

[6] ISO 14001:2004 环境管理体系要求及使用指南(Environmental management systems—Requirements with guidance for use)

[7] ISO/IEC 15026(所有部分) 系统和软件工程 系统和软件保证[1)](Systems and software engineering—Systems and software assurance)

[8] ISO/IEC 15408-1:2009 信息技术 安全技术 IT 安全评估准则 第 1 部分:介绍和一般模型(Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model)

[9] ISO/IEC 15408-2:2008 信息技术 安全技术 IT 安全评估准则 第 2 部分:安全功能组件(Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional components)

[10] ISO/IEC 15408-3:2008 信息技术 安全技术 IT 安全评估准则 第 3 部分:安全保证组件(Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance components)

[11] ISO/IEC TR 15443-1:2005 信息技术 安全技术 IT 安全保证框架 第 1 部分:概述和框架(Information technology—Security techniques—A framework for IT security assurance—Part 1: Overview and framework)

[12] ISO/IEC TR 15443-2:2005 信息技术 安全技术 IT 安全保证框架 第 2 部分:保证方法(Information technology—Security techniques—A framework for IT security assurance—Part 2: Assurance methods)

[13] ISO/IEC TR 15443-3:2007 信息技术 安全技术 IT 安全保证框架 第 3 部分:保证方法分析(Information technology—Security techniques—A framework for IT security assurance—Part 3: Analysis of assurance methods)

[14] ISO/IEC 15939:2007 系统和软件工程 测量过程(Systems and software engineering—Measurement process)

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

[16] ISO/IEC 16326:2009 系统和软件工程 生存周期过程 项目管理(Systems and software engineering—Life cycle processes—Project management)

1) 部分已发布。

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术
信息安全管理体系实施指南
GB/T 31496—2015/ISO/IEC 27003:2010
*
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.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.5 字数 100 千字
2015 年 6 月第一版 2015 年 6 月第一次印刷
*
书号:155066·1-51118 定价 48.00 元

如果组织开发其自己的测量要点，那么这些要点必须作为设计阶段的一部分被文件化（详情见GB/T 31497—2015）。这个文件可以非常全面，并可不必由管理者签署，因为细节可能在实施时发生变化。

ISMS 有效性的测量

在设置宜被实施的信息安全测量方案的范围时，要注意对象不要太多。如果对象太多，那么可将方案划分成不同的部分。这些部分的范围可看作独立的测量以便比较，但其主要目的是：将这些测量组合起来，就可提供一个评价 ISMS 有效性的指标。这些子范围通常是一个具有清晰边界定义的组织部门。在这些子范围内，作为对象的许多组织过程和测量的众多对象，组合在一起，就可形成一个信息安全测量方案的适当范围。这也可看作一系列具有两个以上过程/对象构造的 ISMS 活动。因此，整个 ISMS 的有效性可根据这些具有两个以上过程/对象的测量结果，进行测量。图 E.2 给出了一个示例：两方面有效性的测量：ISMS 的 PDCA 过程和组织内过程的示例。

由于目标是测量 ISMS 的有效性，因此对控制目标和控制措施进行测量是重要的。足够数量的控制措施是一方面，另一方面则是这些控制措施对于评价 ISMS 的有效性来讲是充分的。（可能还有限制信息安全测量方案范围的其他理由，这在 GB/T 31497—2015 中提到）。

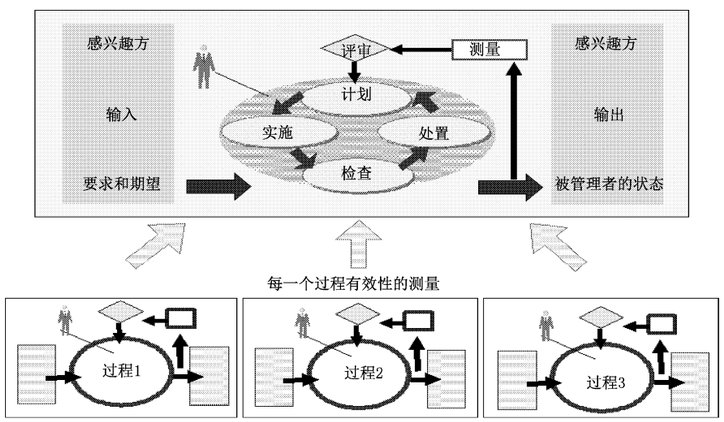

图 E.2　两方面的有效性的测量：ISMS 的 PDCA 过程和组织内过程的示例

在使用测量结果来评价 ISMS、控制目标和控制措施的有效性时，管理者了解信息安全测量方案的范围，这一点是最根本的。测量方案的负责人在信息安全测量方案发布之前，宜获得管理者对该范围的批准。

注 1：GB/T 22080—2008 中有关有效性测量的要求是："测量控制措施或控制措施集"（见 GB/T 22080—2008 的 4.2.2 d）。

注 2：GB/T 22080—2008 中有关 ISMS 有效性的要求仅是"整个 ISMS 有效性的评审"，而对"整个 ISMS 的测量"没有要求（见 GB/T 22080—2008 的 0.2.2）。

实际执行测量时，可使用内部人员或外部人员，或两者相结合。在评价内部或外部资源时，组织的规模、结构和文化都是要考虑的因素。小型和中等规模的公司相比大型组织而言，在使用外部支持时会得到更多的益处。使用外部资源的结果也可能提供一个更有效的结果，这取决于组织文化。如果组织习惯于内部审核，那么内部资源同样有效。

目　　次