<<信息安全管理体系审核指南>>

图书基本信息

书名：<<信息安全管理体系审核指南>>

13位ISBN编号：9787506670104

10位ISBN编号：7506670100

出版时间：2012-10

出版时间：中国标准出版社

作者：魏军，谢宗晓　编著

页数：118

字数：171000

<<信息安全管理体系审核指南>>

内容概要

本书分为七章，从审核基础、标准族介绍、认证流程介绍到审核实施等逐步展开。
其中，第2章“ ISMS标准族介绍 ”，将ISMS标准族所有标准的进展情况更新到今年3月份；第6章“ 信息安全控制措施审核 ”借鉴了ISO/IEC
27008的最新进展，较详细地介绍了控制恶意代码的技术检查，审计日志控制措施的技术检查，特殊权限管理控制措施的技术检查，备份控制措施的技术检查，网络安全管理控制措施的技术检查，用户职责管理控制措施的技术检查的检查内涵、检查方法和相关证据要求，为从业人员理解控制措施的有效性检查和审核点起到抛砖引玉的作用。
第7章“ ISMS结合审核 ”的内容也借鉴了ISO/IEC
27013的部分思想，从风险管理、有效性测量、信息安全事件管理、变更管理、容量管理、相关方管理和业务连续性管理7个方面，分析了两个标准的针对性要求和结合审核方法。

<<信息安全管理体系审核指南>>

书籍目录

章节摘录

版权页： 插图： 5.1.3 标准的附录部分 附录A列出许多详细的控制目标和控制措施，可供组织进行信息资产风险处理时选择使用。
这些可供选用的控制措施也称为控制要求（control requirements）。
组织在建立ISMS时，要选择“附录A”所列的控制目标和控制措施。
附录A属于规范性的附录，是ISO／IEC 27001：2005标准要求组织要使用的附录。
附录A的符合性审核也十分重要。
这将在第6章“控制目标和控制措施的符合性审核”再详细介绍。
附录B和附录C展示ISO／IEC 27001：2005标准与其他相关标准（或指南）之间的对应关系。
其内容十分简单，易读、易理解，读者只要花很少时间阅读后，就会明白和了解到相关信息。
由于这两个附录只起着提供信息的作用，属于信息性附录，不是标准的要求，与审核没有多大的关系。
5.2 审核方法 5.2.1 过程审核 ISO／IEC 27001：2005的要求是过程要求。
有些ISMS过程要通过形成文件的程序（documented procedures，通常称程序文件）加以控制，如“文件控制程序”、“记录控制程序”、“ISMS内部审核程序”和“纠正措施和预防措施控制程序”等。
有些过程不一定要用程序文件进行控制。
凡标准要求要有的过程，组织要有相应的过程。
审核人员应按标准要求进行过程审核。
对过程的审核可从两方面入手：（1）过程是否到位。
对于ISO／IEC 27001的相关条款的关键点上所要求的过程，组织实际建立的ISMS必须要有相应的过程。
（2）过程是否符合要求。
ISO／IEC 27001标准对每个ISMS过程，都有具体的和明确的要求（“shall”要求）。
组织的ISMS必须满足这些要求。
主要方法是将组织的ISMS与ISO／IEC 27001：2005的第4～8章规定的要求进行比较和分析。

媒体关注与评论

本丛书从ISMS的基础信息安全风险管理开始讨论，从不同领域、多个侧面，对ISMS相关知识进行了细致的介绍和阐述，有理论，更有实践，包括ISMS的审核指南、应用方法、业务连续性管理以及在重点行业的应用实例，很有特色。

——中国工程院院士 蔡吉人

信息安全是维护国家安全、保持社会稳定、关系长远利益的关键组成部分，本丛书中各种典型的案例、针对各种网络安全问题的应对措施，为组织提供一个完整的业务不间断计划，能为组织业务的正常运行起到保驾护航的作用。

——中国工程院院士 周仲义

编辑推荐

《信息安全管理体系审核指南》由中国标准出版社出版。

版权说明