<<信息安全管理体系实施指南>>

图书基本信息

书名：<<信息安全管理体系实施指南>>

13位ISBN编号：9787506670012

10位ISBN编号：7506670011

出版时间：2012-10

出版时间：中国标准出版社

作者：谢宗晓

页数：245

字数：360000

前言

关于本书的写作目的及其与相关书籍之间的关系　　如何在组织内部署信息安全管理体系？
让所有的读者都去阅读晦涩难懂的英文标准肯定不现实，因此我们一直希望能以一本书来解决所有的问题，于是就有了2008年出版的《信息安全管理体系应用手册》。
根据这几年读者的反馈，发现这样简单的解读反倒有“夹生饭”的嫌疑。
这如同读经书，读“论”固然可以快速提高自己的理解水平，但读“经”才能更正确地理解经书原意。
于是，我决定着手写一本关于GB/T 22080-2008/ISO/IEC 27001：2005逐句解读的讲义，让读者在实施过程中“知其然，更知其所以然”。
讲义已经成稿并准备出版的时候，中国标准出版社张宁老师告诉我《信息安全管理体系丛书》已被列入新闻出版总署“‘十二五’时期（2011-2015年）国家重点图书、音像、电子出版物出版规划”。
为了使整套丛书内容更加完整，分册的原则也更加清晰，我们决定将准备出版的讲义纳入本丛书中，即这本《信息安全管理体系实施指南》。
本书较之《信息安全管理体系应用手册》，既是改版，又有互补。
对于《信息安全管理体系应用手册》中的“标准解析”以及“标准实施”等内容，我们根据最新的标准以及这几年的最新实践进行了修订，但是对于原书中大量信息安全技术的讨论，在本书中不再涉及，在信息安全管理体系丛书中也不再讨论，以更突出管理体系的文件化规程的特点。
此外，本书也不再介绍信息安全的基本内容，而是直接从解读GB/T 22080-2008/ISO/IEC 27001：2005开始。
……

内容概要

本书共有三篇：标准解读、标准落地及延伸阅读。

标准解读包括：正文解读、附录解读和参考文献解读。
正文解读的形式为左侧标准原文，右侧解读或注释。
在正文解读中，用了大量的图示，也列举了大量的示例，
力求通俗易懂，以帮助读者利用已有的经验来理解信息安全管理体系中晦涩的概念。

书籍目录

目录
第一篇
基础 标准解读
第1章 GB/T22080-2008 /
ISO/IEC27001:2005正文解读
引言
1
范围
2
规范性引用文件
3
术语和定义
4
信息安全管理体系（ISMS）
5
管理职责
6
内部ISMS审核
7
ISMS的管理评审
8
ISMS改进
第2章 GB/T22080-2008 /
ISO/IEC27001:2005附录解读
附录A
（规范性附录） 控制目标和控制措施
附录B
（资料性附录） OECD原则和本标准
附录C
（资料性附录） ISO
9001:2000, ISO 14001:2004 和本标准之间的对照
第3章 GB/T22080-2008 /
ISO/IEC27001:2005参考文献解读
第二篇
实施 标准落地
第4章 项目整体设计（Plan）
开始考虑实施ISMS
获得批准并启动项目
建立ISMS方针
建立组织安全要求
进行风险评估及处置
设计ISMS
确定正式的项目计划
第5章 文件体系设计及编写指南（Plan）
设计文件的架构

文件的过程控制
文件编写注意要点
确定文件目录
确定文件编写及发布计划
编写文件
第6章 体系运行管理（Do-Check-Act）
进行监视与评审
组织内部审核
组织管理评审
申请外部审核
第三篇
提高 延伸阅读
第7章 ISO/IEC27000标准族开发进展及概述
ISO/IEC
27000至ISO/IEC
27059标准的基本情况
第8章 几个重要的ISO/IEC27000标准介绍
ISO/IEC27000:2009基础与词汇
GB/T22080—2008/ISO/IEC27002:2005信息安全管理实用规则
ISO/IEC
27003:2010信息安全管理体系应用指南
ISO/IEC
27004:2009信息安全管理-测量
ISO/IEC
27005:2011信息安全风险管理
ISO/IEC
27006:2007信息安全管理体系认证审核机构要求
ISO/IEC 27007:2011信息安全管理体系审核指南
ISO/IEC TR 27008:2011控制措施审核指南
致谢
后记

章节摘录

版权页： 插图： （二）制度描述虽然明确，但是不切实际。
例如，风险评估的实施频率为每季度至少一次，必须覆盖所有的信息系统。
对于信息系统复杂的组织来说，这个要求很难实现，而且必要性也不大。
反倒是风险评估所带来的业务中断更值得关注。
在制度中尽量避免出现“有关部门”、“相关部门”、“相关人员”等模糊词汇，这种词汇一般是出于制度制定者的“免责”的心态，看似义正言辞，实则言之无物。
一个制度，一旦站在“立场正确”的角度对现象进行指责，并强烈呼吁“提高人的××素质”，唯独缺乏可操作性的措施，注定是失败的制度。
术语要规范，前后要统一 无论是否有专门的术语定义，术语的引用应该尽量与国家标准保持一致，但是有些术语本身没有统一的规范，或者还没有国家标准，因此在一篇文档里至少应该保持统一性。
例如，confidentiality，在中文里面有时翻译成“保密性”，有时翻译成“机密性”，在日常应用中，经常会发现一篇文档，“保密性”和“机密性”轮换使用，而作者却浑然不觉。
再如，在以往的翻译中，information security event译为“信息安全事件”，而informationsecurity incident译为“信息安全事故”但是在GB／Z 20985——2007中，将information security event译为“信息安全事态”，而information security incident译为“信息安全事件”。
虽然开始不习惯，但是也必须跟国家标准保持一致。
用词力求准确，避免产生可能的歧义明确是为了防止模棱两可，准确则是为了防止产生歧义。
例如，在GB／T 22080—2008／ISO／IEC 27001：2005部署之前，应分析组织目前情况与标准之间的差距。
“差距”一词，不够准确，这意味着组织实际的所有方面都没有标准要求的好，但实际上，某些方面，组织的控制措施可能已经超过了GB／T 22080 2008／ISO／IEC 27001：2005的要求，上句修正为“差异”则比较准确。
在GB／T 1.1—2009的6.3.1.3强调了规范性技术要素的可证实性原则：不论标准的目的如何，标准中应只列入那些能被证实的要求。
标准中的要求应定量并使用明确的数值表示，不应仅使用定性的表述，如“足够坚固”或“适当的强度”等。
当然，一个企业的制度不必一定达到GB／T 1.1——2009的要求。

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

《信息安全管理体系实施指南》由中国标准出版社出版。

名人推荐

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

版权说明