国家“十二五”重点规划图书
信息安全管理体系丛书

信息安全管理体系实施案例

- 丛书顾问：蔡吉人　周仲义
- 丛书主编：吕述望　赵战生　陈华平
- 执行主编：谢宗晓　吕茂强

谢宗晓　编著

中国质检出版社
中国标准出版社

信息安全管理体系实施案例

谢宗晓 ◉ 编著

中国质检出版社
中国标准出版社

北 京

图书在版编目（CIP）数据

信息安全管理体系实施案例/谢宗晓编著．
—北京：中国标准出版社，2012.10
（信息安全管理体系丛书）
ISBN 978-7-5066-7000-5

Ⅰ.①信… Ⅱ.①谢… Ⅲ.①信息系统—安全管理—体系—案例—中国 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2012）第 227314 号

中国质检出版社
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（100013）
北京市西城区三里河北街 16 号（100045）
网址：www.spc.net.cn
总编室：（010）64275323 发行中心：（010）51780235
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 787×960 1/16 印张 20.25 字数 436 千字
2012 年 10 月第一版 2012 年 10 月第一次印刷
*
定价 54.00 元

序言

prologue

中国工程院院士 蔡吉人 推荐序

党中央、国务院高度重视信息安全工作。在中办发〔2006〕11号《2006—2020年国家信息化发展战略》中明确指出："坚持积极防御、综合防范，探索和把握信息化与信息安全的内在规律，主动应对信息安全挑战，实现信息化与信息安全协调发展"，"积极跟踪、研究和掌握国际信息安全领域的先进理论、前沿技术和发展动态"。

虽然信息安全技术和信息安全管理得到了前所未有的重视，但是信息安全事件却一直处于有增无减的状态。只有信息安全技术和管理并重，在宏观层次上实施了良好的信息安全管理，才能使微观层次上的安全，如物理措施等，实现其恰当的作用。采用信息安全管理体系并得到认证无疑是组织应该考虑的方案之一。事实上，也只有这样才能真正站在组织的高度上来对待信息安全问题。

信息安全管理体系（ISMS）是基于组织业务风险方法来建立、实施、运行、监视、评审、保持和改进信息安全，它跳出了"为安全信息而信息安全"的传统概念，强调站在组织业务的角度来管理信息安全活动。ISMS相关标准不仅为一个组织提供从框架到细节的全面指导，而且为ISMS的整个产业链提供指南。

基于此，中国质检出版社组织了国内的信息安全专家及标准的起草

者编写了《信息安全管理体系丛书》。本丛书是我国第一套全面系统的信息安全管理体系丛书，它从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，可谓既专又广，是一套充分展示ISMS领域当前成果并将其推广的优秀图书，一定会为我国ISMS专业人才的培养起到重要的推动作用。

2012年9月

序言

prologue

中国工程院院士 周仲义 推荐序

当前，国际上围绕信息的获取、分析、利用和控制的竞争越来越激烈，信息安全已成为维护国家安全、保持社会稳定、关系长远利益的关键组成部分，备受各国政府的关注和重视。如何确保信息安全已是各国政府及各种组织改进其竞争能力的一个新的具有挑战性的任务。

入选国家“十二五”重点图书规划的出版项目《信息安全管理体系丛书》，融入了作者多年来在信息安全、信息安全管理体系领域的研究和实践成果，包括多项具有自主知识产权的创新成果，是面向现代信息安全从业人员普及国家信息安全政策和信息安全知识，强化组织信息安全意识和信息安全保障能力建设，展示信息安全领域最新成果和信息安全管理体系建设、实施、运行、审核成就的高水平通俗读物。

该套丛书共有13个分册，主要内容涉及信息安全风险管理和风险评估、信息安全管理体系实施、信息安全管理体系审核、业务连续性管理、信息安全管理体系与ISO/IEC 20000的整合、信息安全管理体系与信息系统安全等级保护的整合以及信息安全管理体系在重点行业和领域的应用。书中各种典型的案例，针对各种网络安全问题的应对措施，为组织提供了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。

该套丛书主要作者长期从事信息安全领域的科学研究与实践，曾参与多项信息安全国家标准的制修订，经验丰富，成果丰硕。他们编著的这套《信息安全管理体系丛书》，可代表现阶段我国信息安全管理体系领域最高研究水平，在服务于国家或组织，提升国家安全战略方面将起到非常重要的作用，必将产生显著的社会效益。该套丛书的出版，在我国工程技术领域是具有重要意义的大事，将为我国信息安全保障能力建设提供有力的支撑，让信息安全管理体系真正成为对抗信息霸权主义、抵御信息侵略的重要保障。

周仲义

2012 年 9 月

丛书前言

Series introduction

信息通信技术（ICT）的快速发展和广泛应用，为人类开拓出继陆、海、空、天之外的第五维生存空间——赛博空间（Cyberspace）。ICT 的潜能不但使赛博空间展现出前所未有的美好前景，也为人类在陆、海、空、天的生产活动、科学研究以及知识学习、文化传承与交流和社会管理带来了高效率、高效益。信息化成为当今社会发展的巨大推动力。

但是，在新技术的应用中，风险和机遇并存。技术的不成熟，使得社会犯罪分子利用这些技术的漏洞谋取利益；霸权国家为其核心利益展现的把赛博空间作为新的战争空间的国策，使赛博空间显现出不和谐、不安宁的不良态势。

探究当代各国的信息安全战略和实践可知，提升信息安全保障能力是应对危机的对策，技术与管理并重是保障能力提升的出路，风险管理是指导保障能力形成的思想。

保障能力体现于预警能力、保护能力、检测能力、响应能力、恢复能力和反制能力。

技管并重要求，信息安全保障能力建设不但需要运用技术手段，还要运用管理手段，并且要运用技术手段支持管理手段，运用管理手段提升技术手段应有作用的有效发挥。

风险管理的思想使我们清醒地认识到，面对信息系统的应用，我们实际上是面对一个人机结合的、智能化的、非线性的时变复杂大系统。我们所做的防护努力，只能减少信息安全事件发生的可能性和发生事件

的损失及影响。绝对杜绝事件的发生是不可能的，我们必须积极应对处置可能发生的事件，保障依赖信息系统要完成的使命。

信息安全已经从关注技术平台发展到关注业务使命和组织治理。信息安全保障也提升到了依赖信息化手段的使命保障。我们需要跟上这个提升，研究思考和部署更高层次的安全保障。

信息安全管理的理论和实践，已经从依据长官意志的人治型管理，经由制度化建设的规章型管理，发展到了根据管理理论和成功实践经验加以规范化、标准化的体系化管理。ISO/IEC SC 27 的 27000 系列标准将不断丰富和完善的信息安全管理体系（ISMS）展现在我们面前。发达国家结合国情，也各自拥有与 27000 系列指导思想相一致的相关标准（例如美国国家技术标准研究所开发颁布的风险管理框架 NIST 特别出版物 SP 800 的相关系列标准）。我国信息安全标准化技术委员会已经把 27000 系列定为国家标准，同时结合国情颁布了若干为等级保护所需要的信息安全管理标准和风险评估、风险管理、事件分级分类、处置、灾难备份恢复等国家标准。

本系列丛书的目的在于跟踪国际和国家标准的发展，分析解析标准的内涵要义，试图帮助读者加深理解标准，也试图以总结作者的实践案例来宣贯标准，帮助读者正确地实施标准，执行标准。

信息安全保障能力是信息化条件下的综合国力的体现，能力低下必定吃亏挨打。我们不能满足我国信息化的发展速度和规模。我们必须依靠自己和世界上平等待我的朋友一起共建赛博家园，保障赛博家园的安康。

中国科学院信息安全国家重点实验室

2012 年 8 月

丛书主编吕述望教授的话

在 Internet 上搞中国的信息安全是不可控的，事实上，对于 Internet 而言，美国以外的国家都只是安全利用的问题。为什么这么说呢？这要从以下几点说起。

1. 互联网定义：**互联网是两个以上的具有一个主根的网络的平等连接。其上层不再有根。**

2. Internet 网是人类的重要建树，其中文译名为因特网。它是美国的国际网，可记作 USA-i-Net 。

3. 中国公众使用的网络实际上也是 USA-i-Net，中国用户域名 .cn。我们使用 IP 地址是要给美国人付钱的，而且，.cn 受 Internet 主根的控制，毫无安全保证。

4. 目前中国网络语言“互联网”指的是美国的国际网。“中国是互联网大国”指的是“Internet（因特网）用户大国”，“中国互联网协会”指的是“Internet 中国用户协会”。

5. 党和国家的领导人已经认识到了这一问题的严重性。2010 年 6 月 7 日，胡锦涛总书记在中国科学院、中国工程院两院院士大会上发表了“要积极研发和建设新一代互联网”，“改变核心技术受制于人”的讲话。“新一代互联网”的概念显然不是对现在 Internet 的改造，因为从前面的讲述可知，在 Internet 上实现中国的信息安全无异于缘木求鱼。

6. **中国应该建设中国国际网（CHINA-i-Net）。中国国际网的协议如**

果与美国国际网（Internet）一致也可，使用IPv9可能容量会大，权利纷争会小。问题的关键是中国有了主根，且有了与国际平等连接的物质基础与思想准备。

7. CHINA-i-Net，USA-i-Net等多个网络平等连接，自然形成互联网，世界未来网络是不会依附任何一个国家的。未来网络中的认证，识别，安全保密会有全新的概念与技术出现。数字世界是由数字序列、知识包、知识阅读器三部分组成的，人类将在数字世界里平等、自由、负责地畅游知识的海洋！

8. 有关互联网的项目要立足中国国际网（CHINA-i-Net）。我国北斗卫星导航系统与美国全球定位系统GPS是个好例子。

9. 除了加强Internet的安全利用，全面的信息安全管理也非常重要。

为此我们组织编写了《信息安全管理体系丛书》，并有幸被列入了国家“十二五”重点图书规划，这也表明了国家对信息安全问题的高度重视。

我深切期望，《信息安全管理体系丛书》的出版能为Internet的安全利用，为国内信息安全管理现状的提升尽绵薄之力。

中国科学院信息安全国家重点实验室
北京知识安全工程中心
吕述望

2012年8月

前言

preface

关于本书的写作目的及其与相关书籍之间的关系

广义的信息安全管理体系（Information Security Management System，ISMS）标准族从 ISO/IEC 27000 一直到 ISO/IEC 27059，共 60 个标准，架构非常复杂，针对如何阅读和理解标准，我们编写了《信息安全管理体系实施指南》。但是，无论步骤描述得如何清晰，ISMS 的概念及其部署都是抽象的、模糊的，这如同开车，无论我们对原理多么了解，步骤多么熟悉，这与真正上路还是两码事。

《信息安全管理体系实施案例》虽然不是真正的开车上路，但是提供了一个很好的模拟，至少可以让读者体会这些步骤在一个组织内部是如何落地的，接下来只需要了解路况了。当然，因为每个组织的情境各不相同，甚至大相径庭，最后的实战虽然我们爱莫能助，但每个组织的 ISMS 实施在本质上都是相同的，只要领悟了其精髓之处，自然能够以不变应万变。

在《信息安全管理体系实施案例》出版之前，我和刘琦博士在 2010 年已经在中国标准出版社出版了《信息安全管理体系案例及文件集》，为了节省篇幅，在《信息安全管理体系案例及文件集》中已经给出的文件，在本书中就不再赘述，有些需要改版的，在本书中重新进行了修订，当

然，本书中最关注的还是在《信息安全管理体系案例及文件集》中未讨论或讨论不足的那些文件。

同时，在我和郭立生主编的2008年版《信息安全管理体系应用手册》中对GB/T 22081—2008/ISO/IEC 27002：2005进行了大致的解读，限于篇幅，就只针对标题，而没有针对正文，但是，既然是讨论ISMS的落地，便不免要采纳GB/T 22081—2008/ISO/IEC 27002：2005中的指导意见。因此，在本书中，对我认为重要的、编写文件要涉及的GB/T 22081—2008/ISO/IEC 27002：2005正文内容进行了解读，虽然没有《信息安全管理体系应用手册》中全面，但是较《信息安全管理体系应用手册》要深入。

关于本书的主要内容以及如何阅读本书的指导

本书按照时间顺序描述了大都商业银行的ISMS项目实施过程，给出了主要的体系文件，并对这些文件所涉及的GB/T 22081—2008/ISO/IEC 27002：2005正文内容进行了详细的解读。为了使其中的逻辑清晰，本书给出了三种不同的目录：

目录一：时间顺序　目录

○项目开始一年前
□事件（－2）：开始考虑ISMS
□事件（－1）：了解ISMS并申请项目
○项目开始第1周
□事件（0）：ISMS项目启动大会
□事件（1）：确定项目推进组并初步制定推进计划
□事件（2）：调研/分析现状

目录二：GB/T 22081—2008/ISO/IEC 27002：2005 原文及解读　目录

（按照标准原序和讲解先后顺序分别排列）

目录三：信息安全管理体系（ISMS）文件　目录

对 GB/T 22081—2008/ISO/IEC 27002：2005 正文内容的解读为了让读者体会从标准到大都商业银行的完整落地过程，更详细的过程如下：

解读标准的条文 →

9.1.5 在安全区域工作

控制措施

宜设计和应用用于安全区域工作的物理保护和指南。

实施指南

宜考虑下列指南：

a）只在有必要知道的基础上，员工才应知道安全区域的存在或其中的活动；

b）为了安全原因和减少恶意活动的机会，均应避免在安全（safety）区域内进行不受监督的工作KS；

c）未使用的安全区域在物理上要上锁并定期地予以核查KS；

d）除非授权，不允许携带摄影、视频、声频或其他记录设备KS例如移动设备中的照相机。

在安全区域工作的安排包括对工作在安全区域内的雇员、承包方人员和第三方人员的控制，以及对其他发生在安全域的第三方活动的控制。

安全区域（secure areas）。

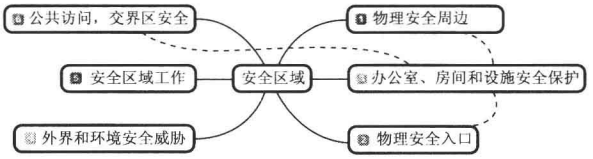
从实施指南看，安全区域最好要分出等级来，否则可能导致不易实施或者没有必要。

原文：unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

这种一般需要根据安全要求来确定。

第三方人员的控制在9.1中屡次提出。

分析总结条文 →

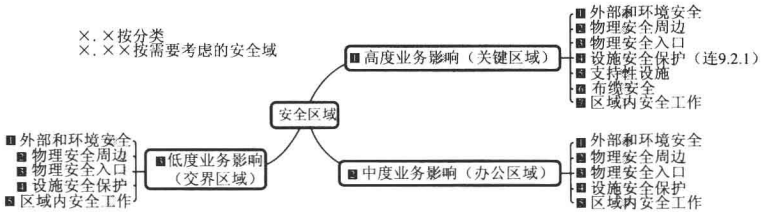


对条文进行应答 →

表13：介质的管理与处置要点

27002 KS（指南）	应答
10.7.1 可移动介质的管理	二级文件 作为特殊的一类介质
10.7.4 系统文件安全	《信息资产分类/分级规范》 二级文件的规范性附录 作为特殊的一类敏感信息
包含敏感信息的设备在物理上宜予以摧毁，或者采用使原始信息不可获取的技术破坏、删除或写覆盖，而不能采用标准的删除或格式化功能	二级文件 先判断信息，后处置介质的规程
包含有敏感信息的介质宜秘密和安全地存储和处置，例如，利用焚化或切碎的方法，或者将数据删除供组织内其他应用使用	二级文件 同上
宜有规程识别可能需要安全处置的项目	二级文件 销毁之前，必须判断存储信息

设计文件结构 →



编写相关文件 →

1 范围（略）

2 规范性引用文件（略）

3 术语与定义

需要定义移动介质包括范围，以区分普通的设备。

4 信息标识

4.1 高度业务影响/三级（High Business Impact,HBI）

4.1.1 标识

高度业务影响信息一旦生成，责任人必须根据《信息资产分类/分级规范》确定恰当的级别，并根据附录A进行标识。

该类信息资产载体无需标识，介质根据《物理设备安全管理规范》或《环境安全管理规范》进行恰当地安放。

4.1.2 存储

如果高度业务影响信息存储在数据库中，存储介质可根据该类据库的应用选择具有合适的可靠性的介质，选择依据为《存储设备选型安全指南》，并根据其安全要求进行恰当的设备选型。

关于本书的写作风格及其他

正如上所述，我们追求的是真实准确地描述一个ISMS项目的过程，让读者去体会如何让《信息安全管理体系实施指南》中描述的步骤、GB/T 22080—2008/ISO/IEC 27001：2005中的要求条款和GB/T 22081—2008/ISO/IEC 27002：2005的指导意见在大都商业银行落地。我们甚至希望案例中所涉及的人物形象都是鲜活的，能让读者不但理解“怎么做”，也能理解“为什么这么做”。

当然我并不是作家或编剧，描述过程未免顾此失彼，场景化并不能做到完全明显，人与事之间的关系也不能做到完全明确，这就使得读者在标准落地过程中不能与本单位的情境有效地一一对应。再加上本人学识也有限，疏、误之处难免，恳请读者批评指正。对于书中的疏、误或讨论，可直接发至我的信箱：xiezongxiao@vip.163.com。

谢宗晓

2012年7月6日

信息安全管理体系丛书阅读指南