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指南

- 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指南

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指南/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 978-7-5066-7001-2

Ⅰ.①信… Ⅱ.①谢… Ⅲ.①信息系统—安全管理—体系—中国—指南 Ⅳ.①TP309-62

中国版本图书馆 CIP 数据核字（2012）第 227311 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 16.75 字数 360 千字
2012 年 10 月第一版 2012 年 10 月第一次印刷
*
定价 45.00 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。

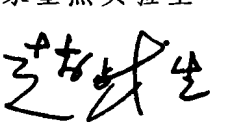
信息安全已经从关注技术平台发展到关注业务使命和组织治理。信息安全保障也提升到了依赖信息化手段的使命保障。我们需要跟上这个提升，研究思考和部署更高层次的安全保障。

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

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。

关于本书的主要内容以及如何阅读本书的指导

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。

正文解读的形式如下：

0.1 总则

本标准用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系（Information Security Management System，简称 ISMS）提供模型[1]。采用 ISMS 应当是一个组织的一项战略性决策[2]。一个组织的 ISMS 的设计和实施受其需要[一]和目标[二]、安全要求[三]、所采用的过程[四]以及组织的规模[五]和结构[六]的影响，上述因素及其支持系统会不断发生变化。按照组织的需要实施 ISMS 是本标准所期望的，例如，简单的情况可采用简单的 ISMS 解决方案[3]。

本标准可被内部和外部相关方用于一致性评估[4]。

（1）标准开门见山地说明了 GB/T 22080—2008/ISO/IEC 27001：2005 的主要用途，即“提供模型”。也就是说，GB/T 22080—2008/ISO/IEC 27001：2005 仅仅是提供解决信息安全问题的模型，而不是方法。所以，应用本标准的主要目的是建立信息安全模型、框架，而不是解决所有的具体问题。因此，在部署 GB/T 22080—2008/ISO/IEC 27001：2005 的过程中，首先要把握一点，就是应该着重于整个框架的搭建，而不是纠缠于具体的细节。

（2）战略是宏观的、全局的、长远的，是指导性的方针、政策，具有普遍的意义，如经济发展战略、国防战略等；而战术则是微观的、局部的、针对具体问题的。例如，军事上的战略战术，前者指对高层次问题的筹划及指导，而后者则是指具体的方法。采用 ISMS 是组织的一项战略性决策（strategic decision），再次表明了 ISMS 不是针对具体方法的。

（3）在 1.1 总则中讨论标准的适用范围时特别指明“本标准适用于所有类型的组织”，因此在采用 ISMS 时，必须具体情况具体对待，而不能过于教条。

对于不易理解的条款，在本书中还对照原文进行了更为细致的解读，示例如下：

为了满足风险接受准则必要

（27）风险接受准则（risk acceptance criteria）。

的进行的任何控制措施的删减[27]，必须证明是合理的(一)，且需要提供证据证明相关风险已被负责人员接受(二)。除非删减不影响组织满足由风险评估和适用法律法规要求所确定的安全要求的能力和/或责任，否则不能声称符合本标准[28]。

这句话从另一方面强调了控制措施与风险的关系。

(28) 这两句话应该认为是同义的。原文如下：

[第一句] Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria (主语) needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons (宾语从句).

[第二句] Where any controls are excluded (定语从句，修饰主语), claims of conformity to this International Standard (主语) are not acceptable unless (条件状语从句)

由于标准附录编排的特殊形式，因此附录解读的形式与正文不同，上侧为标准原文，下侧为解读或注释。附录A的解读参考了GB/T 22081—2008 / ISO/IEC 27002：2005，而又有显著的不同，GB/T 22081—2008 / ISO/IEC 27002：2005是为了提供实用的方法，而本书则是为了理解概念。附录解读的形式如下：

A.7 资产管理		
A.7.1 对资产负责 *目标*：实现和保持对组织资产的适当保护。		
A.7.1.1	资产清单[142]	*控制措施* 应清晰地识别所有资产，编制并维护所有重要资产的清单[143]。

(142) 在正文的4.2.1 d) 中已经出现过“识别ISMS范围内的资产及其责任人”，这也就意味着这两个条款的实施应该尽量重复工作。在实际的部署过程中，一般在风险评估的过程中满足本条款的要求。

(143) 保证所有的资产是可核查的，毫无疑问是管理资产的前提。编制一份资产清单的过程也是风险管理的一个重要的先决条件。这里明确提出的是“编制并维护所有重要资产的清单”。

资产清单的编制过程并没有特殊的要求，可以用软件实现，也可以人工统计为EXCEL的形式，甚至可以统计为纸质的形式。这个清单宜包括所有为从灾难中恢复而必要的信息，包括资产类型、格式、位置、备份信息、许可证信息和业务价值。

既然是“重要资产清单”，因此必须对统计的资产按照重要度进行排序，重要度的判定也是风险管理的一个必须步骤。这时候的重要度不是针对其“财务价值”，更重要的是该资产对组织的“业务重要度”。

参考文献虽然不属于标准正文或附录内容，但是通过阅读参考文献，可以“按图索骥”，更好地理解作者的编写意图以及其中讨论问题的来龙去脉。因此，在本书中也予以解读，形式如下：

[2] NIST SP 800－30 信息技术系统的风险管理指南.

NIST 全称为 National Institue of Standards and Technology（国家标准与技术研究院），隶属于美国商业部。NIST 制定的标准，主要目的是为了保证计算机系统中敏感但非涉密的信息的安全（涉密信息归属 NSA（National Seurity Agency，美国国家安全局）管辖）。NIST 的官方标准以 FIPS（Federal Information Processing Standards）序列公布，SP 则是 Specail Publishment 系列。

信息技术系统的风险管理指南，英文为 Risk Management Guide for Information Technology Systems，在国内文献中多翻译为 IT 系统风险管理指南。

该指南共分为六章：

第 1 章给出了指南的法律依据、目的、目标读者和相关参考等。

标准落地部分主要介绍标准如何实施，本部分内容参考了 ISO/IEC 27003：2010，但又有显著的不同：尽量考虑国内部署信息安全管理体系的特殊情况，不但介绍标准实施的基本步骤，而且将文件体系设计及编写单独作为一章进行讨论，给出了从标准条款到文件目录，从文件目录到单个文件的概要和大纲，直至组织针对这些概要和大纲所选择的具体控制措施，最后成文的整个过程，力争达到“授人以鱼，不如授人以渔”的目的。在本部分中还介绍了如何管理信息安全管理体系的运行，如监视、评审、内部审核和管理评审等内容。

延伸阅读主要为想深入研究信息安全管理体系的读者准备，一部分是信息安全管理体系标准族的概述，以表格的形式给出了已经出版的和正在编写的标准的名称及简要介绍。另一部分是除了 GB/T 22080—2008 / ISO/IEC 27001：2005 之外的已经出版的重要标准的综述，其中重点介绍了 ISO/IEC 27000：2009、GB/T 22081—2008 / ISO/IEC 27002：2005 与 ISO/IEC 27004：2009，对 ISO/IEC 27003：2010、ISO/IEC 27005：2011、ISO/IEC 27007：2011 和 ISO/IEC TR 27008：2011 仅作概述，这

几个标准将会在信息安全管理体系丛书的其他分册中详细论述，而 ISO/IEC 27006：2007 对大部分读者意义不大，因此也不作为重点。对标准族中的其他标准，根据 ISO/IEC 27000：2009 的分类原则，在本书中也没有更深入地介绍。

关于本书的写作风格及其他

由于 GB/T 22080—2008 / ISO/IEC 27001：2005 标准条文晦涩难懂，因此本书成文力求深入浅出，通俗易懂，尽量避免“以理论解释理论”的惯常套路，而是用生活化的例子来对其中概念进行类比，以加强读者的直观理解。

当然由于我学识有限，谬误之处难免，恳请读者批评指正。关于书中的谬误或讨论，可直接发至我的信箱：xiezongxiao@vip.163.com。

谢宗晓

2012 年 5 月 8 日

信息安全管理体系丛书阅读指南