国家“十二五”重点规划图书
信息安全管理体系丛书

信息安全风险评估

（第2版）

- 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

赵战生　谢宗晓　主编

中国质检出版社
中国标准出版社

信息安全风险评估

（第2版）

赵战生　谢宗晓◉主编

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

信息安全风险评估 / 赵战生，谢宗晓主编．—2 版．—北京：中国标准出版社，2016.6

ISBN 978-7-5066-8272-5

Ⅰ.①信… Ⅱ.①赵… ②谢… Ⅲ.①信息系统—安全技术—风险评价 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2016）第 110662 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（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 787×1092　1/16　印张 22.75　字数 483 千字
2016 年 6 月第二版　2016 年 6 月第三次印刷

*

定价 98.00 元

国家“十二五”重点规划图书
信息安全管理体系丛书

丛书序

Series introduction

看到由北京知识安全工程中心编写的ISMS丛书，我很高兴，并十分乐意向广大读者推荐这套将信息安全知识和管理体系知识融合在一起的丛书！丛书的出版为中国读者了解ISMS知识打开了一扇窗户，必将促进ISMS在中国的推广和有效实施，为保障我国信息安全带来积极的作用！

ISMS（Information Security Management System，信息安全管理体系）是继质量管理体系、环境管理体系、职业健康安全管理体系、食品安全管理体系之后发展起来的一个新兴的管理体系，是管理体系家族中的一个新“成员”。通过建立和实施ISMS并取得ISMS认证，已经成为各种类型和规模的组织保障信息安全的一个科学、有效的方法。伴随着ISO/IEC 27001：2005和ISO/IEC 17799：2005等ISMS系列国际标准的发布，ISMS开始被全球越来越多的组织认识并接受。

近年来，我国高度重视信息安全保障工作。为指导信息安全保障工作的有效开展，党中央在总结以往信息安全保障经验的基础上，在《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发［2003］27号）中明确提出了“立足国情，以我为主，坚持管理与技术并重”的信息安全保障原则。同时还要求“各级党委和政府要充分认识加强信息安全保障工作的重要性和紧迫性，要抓紧建立健全信息安全管理体制”。

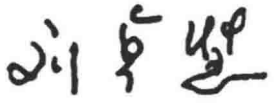
信息安全涉及国家安全，因此要“以我为主”，管理和技术都是实现信息安全目标的重要手段，因此要“坚持管理与技术并重”。建立和实施ISMS符合中央提出的信息安全保障原则，是落实中央精神、保障国家信息安全的要求。

我国认证认可、信息安全、标准化等有关部门对ISMS标准和认证的发展也进行了积极、深入的跟踪、探索和研究。2002年以来，全国信息安全标准化技术委员会就开始着手制定ISMS相关国家标准，并于2005年发布了国家标准GB/T 19716—2005《信息安全管理实用规则》。国家认证认可监督管理委员会开始研究建立ISMS认证认可制度，相继批准了一批ISMS试点认证机构和认证培训机构，中国认证认可协会和中国合格评定国家认可委员会也分别开展了ISMS人员培训注册和机构认可等相关工作。2006年11月国家成立了“中国信息安全认证中心”，专门负责在信息安全领域开展产品和管理体系认证等相关工作。这些探索和实践为ISMS在我国的推广和有效实施奠定了基础。

尽管我们对ISMS进行了一定的探索和实践，但是对于大部分读者来说，ISMS仍然是一个新领域、新事物，它涉及信息安全、管理体系、标准、认证等多个知识领域，是一门典型的交叉学科。北京知识安全工程中心组织力量编写的这套丛书，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。丛书中的每一本既相对独立，又相互联系，既可以单独使用，也可组合起来作为一套教材系统地学习。丛书可谓既专又广，是一套ISMS领域不可多得的优秀教科书，一定会为我国ISMS专业人才的培养起到积极的推动作用。

我在向广大读者推荐这套ISMS丛书的同时，也真诚地企盼能有更多的信息安全和管理体系相关工作者投入到ISMS的研究和推广工作中去，为更广大的读者不断提供更丰富、更新鲜的作品，为我国信息安全保障和ISMS认证认可工作做出贡献！

国家认证认可监督管理委员会副主任



2007年1月26日于北京

丛书前言

Series introduction

IT技术的快速发展和广泛应用掀起了全球信息化的大潮，使人类进入了继农业革命、工业革命后的第三次生产力的革命阶段。我国信息化的规模和速度全球瞩目，逐步渗透到各行各业。人们享用着信息化的成果，憧憬着信息化带来的前所未有的美好前景。

由于人们认识真理、实践真理的能力的局限性，IT产品存在安全性问题，信息系统存在着脆弱性。加之存在着意识形态的斗争、经济发展的竞争以及社会犯罪和恐怖主义活动，信息系统的正常功能受到制约，信息化带来的高效率、高效益受到限制，信息资源受到威胁，信息空间的安全形势严峻。

为了强化信息安全保障，各国都在制定方略，加强研究，采取措施，建设信息安全保障体系。人们逐步认识到，依靠信息安全技术产品只是解决信息安全问题的一个方面，大量的问题还需要通过管理来解决，而且技术和管理都需要通过人来使用和操作。为了规范信息安全产品的生产使用和信息安全管理操作，各国都加强了信息安全各类标准的制定工作。ISMS等信息安全管理标准成为当前的热点和重点。

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003] 27号）提出了“立足国情，以我为主，坚持技术管理并重”的要

求，并提出了“抓紧制定急需的信息安全管理和技术标准”的任务。国务院信息办常务副主任，全国信息安全标准化技术委员会主任曲维枝同志最近也指出：“没有信息安全的信息化是危险的信息化；没有完善的信息安全标准，信息化建设中的产品、系统、工程就不能实现安全的互联、互通、互操作，就不能形成我国自主的信息安全产业，就不能构造出一个自主可控的信息安全保障体系，就难以保证国家信息安全和国家利益。”根据以上要求和国务院信息办组织的信息安全管理标准应用试点工作的实践，全国信息安全标准化技术委员会确定了跟踪借鉴 ISMS 国际标准制定我国信息安全管理体系标准的任务。

北京知识安全工程中心作为我国第一个依据《中华人民共和国认证认可条例》授权进行 ISMS 认证培训服务的机构，为了规范自己的培训和咨询服务，根据国际和国家标准以及自己长期研究和实践的经验，编写了一套 ISMS 的丛书。该丛书由《信息安全管理体系教程》、《信息安全管理体系教程习题与案例分析》、《信息安全风险评估》、《信息安全管理体系控制措施实施和测量》、《信息安全管理体系审核指南》、《信息安全管理体系建立和实施》、《信息安全管理体系内部审核》等组成。丛书全面涉及了 ISMS 的概念，构建 ISMS 的程序、步骤和方法要求等各个方面，是一套深入浅出、系统介绍 ISMS 的实用教材，将为我国宣传贯彻 ISMS 标准，落实 ISMS 认证工作，加强 ISMS 人才培养发挥重要的作用。

建立和实施 ISMS 是一个组织有序提升信息安全管理能力的有效战略举措。不论是否以通过 ISMS 认证为目的，都具有重要的参考借鉴作用。只要组织存在信息安全问题，就需要根据组织自身的需要和特点，建立

起自己的ISMS。ISMS的建立和运行为我国的信息安全等级保护制度的执行提供有力支撑，是在一个组织范围内落实信息安全保障的各项基础性工作的科学指南。ISMS是一个持续的计划（P）、实施（D）、检查（C）、改进（A）的过程。为了加强ISMS的执行力，形成ISMS的常态化，形成体系文件是必要的，但是落实到人和信息系统是更为重要的。通过角色和责任的落实和数字化自动化支撑工具的运用才能把心里想的、纸上写的落实到信息安全工作的过程和活动中。

没有明白人，难办明白事。ISMS的人才培养是成功建立和实施ISMS的重中之重。让我们积极行动起来，加大信息安全专门人才培养的工作力度，不断创造适合我国国情的新经验、新手段，把建设我国信息安全保障体系的艰巨任务不断推进，落到实处。

2007年1月21日

第一版前言

虽然风险评估在信息安全中的应用是新生事物，但是目前书店里与此相关的书籍却并不少见。本书的目的，显然不是在混乱的局面中再增加一本。我们的目的是站在新的视角，结合 ISMS（Information Security Management System，信息安全管理体系），从概念、理论方法以及实践经验三个方面去阐述信息安全风险评估，并对其做一个阶段性的综述。

实质上，风险评估是关于实践的学问，也就是说，它不是建立在公理或者定理的基础上经过严格的证明得到的。我们所用的模型都是从实践中总结出来，然后应用到实践中去的。我们在本书中将向读者展示这些模型的来龙去脉和应用方法以及可能遇到的难点。实践应用是本书所强调的重点，因此我们用大量的篇幅去介绍应用的示例，而不是仅仅论述空洞的理论。

本书按照下面的顺序循序渐进地讨论风险评估。

首先从风险概念的来龙去脉说起，对风险的概念进行全面的剖析。以此为中心，介绍风险评估、风险管理、风险分析、风险评价和风险处理等相关概念。接着对目前关于风险评估的文献进行综述，对这些文献的内容和创新性做了大致的介绍。然后在这些文献的基础上介绍主流的风险评估方法。最后一部分给出一个详细的风险评估实践的例子，这个

示例完整地介绍了初次风险评估的全过程，甚至细致到开动员会时的讲话提纲，并给出近百个可以直接引用的问卷和调查表等。

此外，本书的附录A与附录B给出了资产分类表和威胁脆弱性对应表，组织可以裁剪使用；附录C、附录D给出了一个风险评估程序和风险处理程序的模板；附录E对其他行业成熟的风险分析方法做了逐一的介绍。

本书力求通俗易懂，对于书中出现的所有专业词汇均做了相应的注解。本书可以指导将要进行信息安全风险评估的组织，也可以作为其他管理体系的审核员（如质量管理体系审核员）进入信息安全领域的学习教材，或者供计算机工程师更好地理解体系方法时参考。

由于风险评估的很多理论本身就颇有争议，因此书中的观点可能受到批评甚至是严厉批评。当然对于试图对信息安全风险评估做阶段性的综述，这种情况在所难免，尤其是有些相关领域进展的评价并不是我们所擅长的。我们尽量用客观的观点去描述目前流行的方法或标准，但由于行文仓促，加上水平有限，书中谬误之处肯定颇多，欢迎提出您的宝贵意见。

本书的成稿很大程度上得益于在讲课过程中的问题讨论，自然首先要感谢这些审核员们活跃的思维和全新的视角。

中国标准出版社张宁主任对本书的组织结构数次进行了改进，才使得本书在成书后更加符合读者的阅读逻辑。

对于书中的很多观点，我们都吸取了张剑博士的意见。

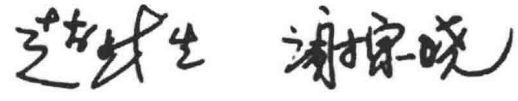
贵州文史馆训诂学专家顾久教授，认真阅读了本书对风险历史的论

述后给出了自己的观点，在没有公开文献的情况下，我们把他的意见已经吸收进本书中。

王连强博士对于风险分析部分提供了大量的资料，并给出了很多建议。

感谢王新杰经理，他对本书的结构安排提出了很多建议，尤其是对书中的案例部分。没有他的热心，不可能有本书的顺利出版。

最后再次真诚地感谢中国标准出版社的审稿者，他们的认真大大提高了本书的质量。

中国科学院研究生院
信息安全国家重点实验室 

2007 年 6 月 4 日

第二版前言

在《信息安全风险评估》的这一新版本中，我们大致保留了第一版的框架，但是自2007年初版至今，已接近10年，这期间诸多标准都进行了改版，人们对信息安全风险评估以及风险管理都有了新的认识，我们也是。

首先，我们根据GB/T23694—2013 / ISO/IEC Guide 73: 2009对风险管理的相关术语进行了重新定义和解读，这其中包括了很多细节的变化，例如，“风险估计”的过程被并入了“风险分析”[1]。更多的内容，请参见本书的第2章。

其次，相关的标准/方法综述，我们将其挪到了“深入阅读”部分。信息安全风险评估流程虽然依赖于一系列的标准，但是实践中也没有了解这么多，重点是能结合本书给出的完整实例并理解基本方法就够了。

当然，为了照顾想深入研究的读者，我们在附录中给出了已经发布的相关国家标准，其中包括：GB/T 23694—2013 / ISO Guide 73: 2009 风险管理　术语、GB/T 31722—2015 / ISO/IEC 27005: 2008 信息安全风险管理指南、GB/T 20984—2007 信息安全风险评估规范和GB/T 31509—2015 信息安全风险评估实施指南。

最后，我们修正了第一版中的某些理解偏差。例如，本书的2. 3. 1

[1] GB/T 23694—2013 / ISO Guide 73：2009中“风险分析”的定义，注2：风险分析包括风险估计。

信息安全及其几个词汇的界定，在新版中就进行了大篇幅的修改，因为第一版中的理解在现在看来是错的，或者说是不准确的。因此，如果读者发现问题，请不吝批评指正，联系方式为：xiezongxiao @ vip. 163. com。

谢宗晓

2015 年 12 月 17 日

目 录

contents

第一篇 概念

第 1 章 风险及其概念 …… 2

1.1 为什么是“风”险? …… 2

1.2 风险的定义 …… 4

1.3 风险与信息安全 …… 10

第 2 章 风险评估与风险管理 …… 12

2.1 区分风险评估/管理 …… 12

2.2 有关的术语解析 …… 13

2.3 信息安全风险评估/管理（ISRA/ISRM） …… 24

第二篇 方法

第 3 章 风险评估（Risk Assessment） …… 30

3.1 风险评估准备 …… 30

3.2 识别并评价资产 …… 36

3.3 识别威胁和脆弱性 …… 47

3.4 识别和评价控制措施 …… 62

3.5 分析可能性和影响 …… 65

3.6 更详细的方法（可选） …… 67

3.7 分析风险的大小 …… 71

3.8 编写风险评估报告 …… 72

第4章 风险应对（Risk Treatment） …… 76

4.1 应对选项 …… 76

4.2 基本流程 …… 77

第三篇 实践

第5章 一个完整的案例 …… 80

5.1 案例描述 …… 80

5.2 风险评估准备工作 …… 82

5.3 识别和评价资产 …… 88

5.4 识别威胁和脆弱性 …… 98

5.5 分析暴露和影响 …… 118

5.6 分析发生容易度和可能性 …… 118

5.7 分析风险大小 …… 118

5.8 编写风险评估报告 …… 122

第6章 几个需要讨论的问题 …… 125

6.1 实践中难点分析 …… 125

6.2 风险评估工具 …… 127

第四篇 深入阅读

第7章 相关的标准/方法综述 …… 132

7.1 可以参考的风险管理通用标准 …… 132

7.2 现行可参考的 ISRA/ISRM 标准 …… 136

7.3 已经废弃的 ISRA/ISRM 标准 …… 148