信息安全
风险评估手册

Information Security Risk Assessment

郭鑫 编著

本书涵盖了信息安全风险评估的国家标准、评估实操方法、评估示例、分析模型、计算公式、评估工具、移动安全评估、云平台安全评估

机械工业出版社
CHINA MACHINE PRESS

信息安全风险评估手册

郭　鑫　编著

机 械 工 业 出 版 社

本书介绍了认识风险评估、信息安全风险评估的主要内容、实施流程、评估工具、评估案例、安全管理措施、手机客户端安全检测、云计算信息安全风险评估。

本书主要面向国家和地方政府部门、大型企事业单位的信息安全管理人员，以及信息安全专业人员，可作为培训教材和参考书使用。本书对进行信息安全风险评估、风险管理、ISMS（ISO/IEC27001）认证等具有较高的实用参考价值。

图书在版编目（CIP）数据

信息安全风险评估手册 / 郭鑫编著. —北京：机械工业出版社，2017.5
ISBN 978-7-111-56605-2

Ⅰ. ①信… Ⅱ. ①郭… Ⅲ. ①信息系统－安全技术－风险评价－手册
Ⅳ. ①TP309-62

中国版本图书馆 CIP 数据核字（2017）第 063437 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：杨 源 责任编辑：杨 源
责任校对：张艳霞 责任印制：李 昂
三河市宏达印刷有限公司印刷
2017 年 4 月第 1 版 · 第 1 次印刷
169mm × 239mm · 18 印张 · 301 千字
0001-3500 册
标准书号：ISBN 978-7-111-56605-2
定价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
服务咨询热线：(010)88361066	机 工 官 网：www. cmpbook. com
读者购书热线：(010)68326294	机 工 官 博：weibo. com/cmp1952
(010)88379203	教育服务网：www. cmpedu. com
封面无防伪标均为盗版	金 书 网：www. golden-book. com

推 荐 语

攻防是网络安全永恒的两面，安全看重的是全局，而非单点。本书参照国际相关标准，通过风险评估理论突出了网络安全整体把控，内容详尽且深入浅出。无论是对希望从事网络安全行业的人员，还是长期从事网络安全的专业人士，此书都大有裨益。

——公安部信息安全等级保护评估中心　副主任　张宇翔

这本书在原有风险评估基础上，又加入了移动安全评估、云平台安全评估两个热点行业，紧跟信息安全发展趋势，值得一读！

——信息产业信息安全测评中心　常务副主任　霍珊珊

目前国内的企业进行信息安全建设时，大多是进行单点建设，但安全是一个整体的过程，需要进行全局考虑。此书基于风险评估国际标准，对企业进行通盘安全评估，是一本难得的好书！

——中国信息安全认证中心体系与服务认证部　副主任　翟亚红

信息安全风险恒久存在，并不会因为信息技术的不断发展而消失。在云计算、物联网、移动互联网等技术日新月异的今天，更应该关注风险评估技术的发展，切实保障信息安全。此书详细解读了风险评估的全过程，值得所有对信息安全有兴趣的读者一读。

——中国信息安全测评中心资质评估处　副处长　王琰

前　言

随着信息化进程的深入和互联网产业的迅速发展，人们的工作、学习和生活方式正在发生巨大变化，效率大为提高，信息资源得到共享。但必须看到，紧随信息化发展而来的网络安全问题日渐凸出，如果不能很好地解决这个问题，必将阻碍信息化发展的进程。网络安全问题已成为信息时代人类共同面临的挑战，国内的网络安全问题也日益突出。

同时，各国围绕互联网关键资源和网络空间国际规则的角逐将更加激烈，工业控制系统、智能技术应用、云计算、移动支付领域面临的网络安全风险进一步加大，黑客组织和网络恐怖组织等发起的网络安全攻击将持续增加，影响力和破坏性显著增强，我国网络安全形势更加严峻。

个人、企业乃至国家的信息安全需要科学、系统地进行防护建设，信息安全风险评估基于 ISO27001 的国际标准，是信息系统安全的基础性工作。它是传统的风险理论和方法在信息系统中的运用，是科学地分析和理解信息与信息系统在保密性、完整性、可用性等方面所面临的风险，并在风险的减少、转移和规避等风险控制方法之间做出决策的过程。

作为新时代信息安全书籍，本书中加入了风险评估案例，理论与实践内容结合，相信可以让广大读者获取到更多的实践知识点。同时，也期待读者通过阅读、学习，可以用所学知识为国家做出更大的贡献！

欢迎广大读者与我邮件交流：g3eek@ hotmail. com

目　录

第1章　认识风险评估

1.1　信息安全风险评估的基本概念

1.1.1　风险评估介绍

风险评估（Risk Assessment）是指在风险事件发生之前或之后（但还没有结束），对该事件给人们的生活、生命和财产等各个方面造成的影响和损失的可能性进行量化评估的工作。即风险评估就是量化测评某一事件或事物带来的影响或损失的可能程度。

从信息安全的角度来讲，风险评估是对信息资产（即某事件或事物所具有的信息集）所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程。

1.1.2　风险评估的基本注意事项

在风险评估过程中，有下列几个关键的问题需要考虑。

- 要确定保护的对象（或者资产）是什么？它的直接和间接价值如何？
- 资产面临哪些潜在威胁？导致威胁的问题是什么？威胁发生的可能性有多大？

- 资产中存在哪些弱点可能会被威胁或利用？利用的容易程度又如何？
- 一旦发生威胁事件，组织会遭受怎样的损失或者面临怎样的负面影响？
- 组织应该采取怎样的安全措施才能将风险带来的损失降低到最低程度？

解决以上问题的过程，就是风险评估的过程。

进行风险评估时，有下列几个对应关系必须考虑。

- 每项资产可能面临多种威胁。
- 威胁源（威胁代理）可能不止一个。
- 每种威胁可能利用一个或多个弱点。

1.2 信息安全风险评估相关标准

在信息安全产业界，风险评估早已不是陌生话题。近几年来，众多信息安全公司完成的风险评估项目已不在少数，甚至在几乎所有的信息安全服务厂商中，风险评估都是其核心业务。

风险评估的核心不仅仅是理论，更是实践。风险评估的实践工作非常困难，据国外的统计数字显示，只有60%的风险评估是成功的。国内的风险评估工作面临的挑战更多，需要一定时间的积累和沉淀，要有一个学和练的过程。需要大家先掌握理论基础，了解风险评估的相关标准。下面就来认识这些国际标准。

1. ISO 27001 起源

随着信息化水平的不断发展，信息安全逐渐成为人们关注的焦点，世界范围内的各个机构、组织和个人都在探寻如何保障信息安全的问题。英国、美国、挪威、瑞典、芬兰和澳大利亚等国均制定了有关信息安全的本国标准，国际标准化组织（ISO）也发布了 ISO/IEC17799、ISO 13335 和 ISO 15408 等与信息安全相关的国际标准及技术报告。目前，在信息安全管理方面，ISO 27001:2005 已经成为世界上应用最广泛与典型的信息安全管理标准，它是在 BSI/DISC 的 BDD/2 信息安全管理委员会指导下制定完成的，最新版本为 ISO 27001:2013。

ISO 27001 标准于 1993 年由英国贸易工业部立项，于 1995 年在英国首次出版 BS 7799 - 1:1995《信息安全管理实施细则》，它提供了一套综合的、由信息安全最佳惯例组成的实施规则，其目的是作为确定工商业信息系统在大多数情况下所需控制范围的唯一参考基准，并且适用于大、中、

小组织。

1998 年，英国公布了标准的第二部分《信息安全管理体系规范》，它规定了信息安全管理体系要求与信息安全控制要求，是一个组织全面或部分信息安全管理体系评估的基础，可以作为一个正式认证方案的根据。BS 7799 - 1 与 BS 7799 - 2 经过修订于 1999 年重新予以发布，1999 年版考虑了信息处理技术，尤其是在网络和通信领域应用的近期发展，同时还特别强调了商务涉及的信息安全及信息安全的责任。

2000 年 12 月，BS 7799 - 1:1999《信息安全管理实施细则》通过了国际标准化组织（ISO）的认可，正式成为国际标准——ISO/IEC 17799:2000《信息技术——信息安全管理实施细则》。2002 年 9 月 5 日，BS 7799 - 2:2002 草案经过广泛的讨论之后，终于发布成为正式标准，同时 BS 7799 - 2:1999 被废止。2004 年 9 月 5 日，BS 7799 - 2:2002 正式发布。

2005 年，BS 7799 - 2:2002 终于被 ISO 组织所采纳，于同年 10 月推出 ISO/IEC 27001:2005。

2005 年 6 月，ISO/IEC 17799:2000 经过改版，形成了新的 ISO/IEC 17799:2005，新版本较老版本，无论是组织编排还是内容完整性上都有了很大的增强和提升。ISO/IEC 17799:2005 已更新，并在 2007 年 7 月 1 日正式发布为 ISO/IEC 27002:2005，这次更新的只是在标准上的号码，内容并没有改变。

2. ISO 27001 发展

2000 年，国际标准化组织（ISO）在 BS 7799 - 1 的基础上制定通过了 ISO 17799 标准。BS 7799 - 2 在 2002 年也由 BSI 进行了重新修订。ISO 组织在 2005 年对 ISO 17799 再次进行修订，BS 7799 - 2 也于 2005 年被采用为 ISO27001:2005。

信息安全管理体系标准（ISO 27001）可有效保护信息资源，保护信息化进程健康、有序、可持续发展。ISO 27001 是信息安全领域的管理体系标准，类似于质量管理体系认证的 ISO 9000 标准。一旦某组织通过了 ISO 27001 的认证，就相当于通过 ISO 9000 的质量认证一般，表示该组织信息安全管理已建立了一套科学有效的管理体系作为保障。根据 ISO 27001 对信息安全管理体系进行认证，可以带来以下几点好处。

1）引入信息安全管理体系，就可以协调各个方面的信息管理，从而使管理更为有效。保证信息安全不是仅有一个防火墙，或找一个 24 h 提供信息安全服务的公司就可以达到的。它需要全面的综合管理。

2）通过进行 ISO 27001 信息安全管理体系认证，可以增进组织间电子

商务往来的信用度，能够使网站和贸易伙伴之间互相信任，随着组织间电子交流的增加，通过信息安全管理的记录可以明显看到信息安全管理的利益，并为广大用户和服务提供商提供一个基础的设备管理。同时，把组织的干扰因素降到最小，创造出更大的收益。

3）通过认证能保证和证明组织所有的部门对信息安全的承诺。

4）通过认证可改善全体的业绩，消除不信任感。

5）获得国际认可的机构的认证证书，可得到国际上的承认，从而拓展业务。

6）建立信息安全管理体系能降低这种风险，通过第三方的认证能增强投资者及其他利益相关方的投资信心。

7）组织按照 ISO 27001 标准建立信息安全管理体系，会有一定的投入，但是若能通过认证机关的审核，获得认证，将会获得有价值的回报。企业通过认证将可以向其客户、竞争对手、供应商、员工和投资方展示其在同行内的领导地位；定期的监督审核将确保组织的信息系统不断地被监督和改善，并以此作为增强信息安全性的依据，增强信任、信用及信心，使客户及利益相关方感受到组织对信息安全的承诺。

8）通过认证能够向政府及行业主管部门证明组织对相关法律法规的符合性。

3. ISO 27001 标准修订

自 2005 年国际标准化组织（简称 ISO）将 BS7799 转化为 ISO 27001：2005 发布以来，此标准在国际上获得了空前的认可，相当数量的组织采纳并进行了信息安全管理体系的认证。

ISO 对标准的更新一般是以 3 年为一个周期，但因为 ISO 27001：2005 标准发布后的巨大成功，以及 ICT 行业的飞速发展，使得这个标准的更新变得非常谨慎。从 ISO 发布的最新信息可以看到，ISO 27001 标准的更新筹备实际上已经在 2008 年开始，任命了工作组（JTC 1/SC 27 WG 1）；2009 年正式启动更新。

从 ISO 27001 标准新版更新的一些说明材料中，可以看出这次 ISO 27001 标准改版将会具有以下几个特征：采用 ISO 导则 83，规范了今后 ISO 管理体系认证标准的基本框架；采用导则 83 颁布的第一个标准是 2012 年 5 月发布的业务连续管理体系标准——ISO 22301：2012。

在新版标准中明确了以下要求：①信息安全风险评估。组织应确定如何确定其信息安全风险评估和处置过程的可靠性。②信息安全风险处理。适用时，组织应调整信息安全风险评估和处置过程，以及采用的方法，以

改善过程的可靠性。保留附录 A 控制措施与控制目标。新版 ISO 27001 依然会保留 SOA 和附录 A 控制目标、控制措施的架构；因此，毫无疑问，ISO 27001 的新版修订一定会与 ISO 27002 的修订同步进行。

事实上，关于控制措施和控制目标的修订，也是应对新的变化的信息安全威胁和风险的必要选择；这部分的更新，在修订项目中接受了大量的修改建议，争论也相当大，目前还没有最终结论。

古希腊哲学家赫拉克利特因其作为辩证法的奠基人之一而闻名于世，他曾经写道“一切皆流，无物常驻”。过去几年中，国际上几乎所有行业和组织面临的信息安全风险的局势无不体现了赫氏的这一学说。变化和发展是永恒的，信息安全风险总是处在持续演进中，攻击者的手段依然会层出不穷。因此，信息安全管理的实践和标准都在不断发展，唯一要做的就是保持警惕，随时准备抵御风险。

4. ISO 27001 认证机构

颁发 ISO 27001 信息安全管理体系证书的认证机构必须是经过 CNCA（中国国家认证认可监督管理委员会，简称国家认监委）授权的认证机构方可在国内进行审核发证，所有通过认证且合法的证书均可在 CNCA 的网站上进行查询。国外的认证机构如果没有在国内 CNCA 备案，即使认证机构得到了 UKAS 或者 ANAB 等的认可，也不符合中国的法律法规，将被视为违规操作，一旦被发现将会被 CNCA 处罚并公示证书在国内无效。经 CNCA 授权的认证机构可以在 CNCA 网站上查询。

认证是指由认证机构证明产品、服务和管理体系符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动。所谓认证机构，是指经中国国家认证认可监督管理委员会（CNCA）批准，可以在中国合法开展管理体系认证和产品认证的专业机构。也就是说，取得此项认证资质的企业或单位才可以进行审核活动。比如 BSI、DNV、北京新世纪认证有限公司和华夏认证中心有限公司等，他们都属于认证机构。认证机构是经 CNCA 授权的，认可机构管理认证机构。

认可是正式表明合格评定机构，具备实施特定合格评定工作能力的第三方证明。通俗地讲，认可是指认可机构按照相关国际标准或国家标准，对从事认证、检测和检查等活动的合格评定机构实施评审，证实其满足相关标准要求，进一步证明其具有从事认证、检测和检查等活动的技术能力和管理能力，并颁发认可证书。中国的认可机构是 CNAS（中国合格评定国家认可委员会），英国的认可机构是 UKAS，美国的认可机构是 ANAB。

一般来说，证书是由认证机构颁发的，认证机构要得到认可机构的授

权，认可机构要得到国家认监委（CNCA）的授权，因此在中国，认证的最高管理单位是CNCA。但是有些认证机构经CNCA备案授权，并没有获得CNAS的认可，这样在国内开展被授权的审核业务也是可以的。

1.3 信息安全标准化组织

1.3.1 国际标准化组织介绍

1.3.1.1 国际标准化组织简介

国际标准化组织（International Organization for Standardization，ISO）简称ISO，是一个全球性的非政府组织，是国际标准化领域中一个十分重要的组织。ISO一词来源于希腊语“ISOS”，即“EQUAL”——平等之意。ISO（国际标准化组织）成立于1946年，中国是ISO的正式成员，代表中国参加ISO的国家机构是中国国家技术监督局（CSBTS）。

ISO负责目前绝大部分领域（包括军工、石油和船舶等垄断行业）的标准化活动。ISO现有117个成员，包括117个国家和地区。ISO的最高权利机构是每年一次的“全体大会”，其日常办事机构是中央秘书处，设在瑞士日内瓦。中央秘书处现有170名职员，由秘书长领导。ISO的宗旨是“在世界上促进标准化及其相关活动的发展，以便于商品和服务的国际交换，在智力、科学、技术和经济领域开展合作。”ISO通过它的2856个技术结构开展技术活动，其中技术委员会（简称SC）共611个，工作组（WG）共2022个，特别工作组共38个。中国于1978年加入ISO，在2008年10月的第31届国际标准化组织大会上，中国正式成为ISO的常任理事国。

国际标准化组织总部设于瑞士日内瓦，成员包括162个会员国。该组织自我定义为非政府组织，官方语言是英语、法语和俄语。参加者包括各会员国的国家标准机构和主要公司。ISO是世界上最大的非政府性标准化专门机构，是国际标准化领域中一个十分重要的组织。

1.3.1.2 国际标准化组织内容

ISO的内容涉及广泛，从基础的紧固件、轴承各种原材料到半成品和成品，其技术领域涉及信息技术、交通运输、农业、保健和环境等。每个工作机构都有自己的工作计划，该计划列出了需要制定的标准项目（试验方法、术语、规格和性能要求等）。

ISO的主要功能是为人们制定国际标准达成一致意见提供一种机制。

其主要机构及运作规则都在一本名为 ISO/IEC 技术工作导则的文件中予以规定，其技术结构在 ISO 中是有 800 个技术委员会和分委员会，它们各有一个主席和一个秘书处，秘书处由各成员国分别担任，承担秘书国工作的成员团体有 30 个，各秘书处与位于日内瓦的 ISO 中央秘书处保持直接联系。

通过这些工作机构，ISO 已经发布了 17000 多个国际标准，如 ISO 公制螺纹、ISO 的 A4 纸张尺寸、ISO 的集装箱系列（世界上 95% 的海运集装箱都符合 ISO 标准）、ISO 的胶片速度代码、ISO 的开放系统互联（OSI）系列（广泛用于信息技术领域）和有名的 ISO 9000 质量管理系列标准。

此外，ISO 还与 450 个国际和区域的组织在标准方面有联络关系，特别与国际电信联盟（ITU）有密切联系。在 ISO/IEC 系统之外的国际标准机构共有 28 个。每个机构都在某一领域制定一些国际标准，通常它们处于联合国控制之下。一个典型的例子就是世界卫生组织（WHO）。ISO/IEC 制定了 85% 的国际标准，剩下的 15% 由这 28 个其他国际标准机构制定。

1.3.1.3　国际标准化组织标准分类

ISO 质量体系标准包括 ISO 9000、ISO 9001 和 ISO 9004。ISO 9000 标准明确了质量管理和质量保证体系，适用于生产型及服务型企业。ISO 9001 标准为从事和审核质量管理和质量保证体系提供了指导方针。

ISO 9000 质量体系标准包括了 3 个体系标准和 8 条指导方针。3 个体系标准分别是 ISO 9001、ISO 9002 和 ISO 9003；8 个指导方针是 ISO 9000 -1 ～ ISO 9000 -4 和 ISO 9004 - 1 ～ ISO 9004 - 4。其中首要标准是 ISO 9001，它为设计、制造产品及提供服务的组织明确指出了一套完整质量体系中的 20 条要素。ISO 9002 为只制造产品但不设计产品及提供服务的组织明确指出了 19 条要素。ISO 9003 为只进行检验的组织明确指出了 16 条要素。ISO 9000 标准每 5 ～ 7 年修订一次。第一批标准已于 1987 年公布，第一次修订则于 1994 年公布，第二次修订于 2000 年公布，现已有 2015 版。

ISO 9001 的新修订本包括一个单一质量体系标准。其指明了 ISO 9001 将适用于一切组织。它将涉及以下几个部分：管理职责、资源管理、工序管理、测量、分析及改进。资源管理这部分是全新的，其他部分包含了新项目。新修订本将包含所有旧的要求，并增加了附加管理要求、工序管理要求、工序测量及改进要求。

ISO/IEC 对于标准检验实验室的承认及其被规定的权限标准包括 ISO 指导 25、58、61、62 及 65。ISO/IEC 指导 58 明确了对认可标准和检验实验室的要求。ISO/IEC 指导 61 明确了对认可产品认证及质量体系注册团体的要求。ISO/IEC 指导 62 明确了对质量体系的要求。ISO/IEC 指导 65 明确