21世纪高等学校规划教材 | 信息管理与信息系统

信息安全管理与风险评估

赵 刚 编著

清华大学出版社

信息安全管理与风险评估

赵 刚 编著

清华大学出版社

内 容 简 介

本书在系统归纳国内外信息安全管理与风险评估的最佳实践以及近年来研究成果的基础上，全面介绍了信息安全管理、信息安全管理体系、信息安全风险评估的基本知识、相关标准和各项内容，全书涵盖了信息安全管理体系建立流程、风险评估实施流程，以及信息系统安全等级保护、云计算安全管理与风险评估、IT 治理等内容。

本书既可作为高等院校信息安全专业、信息管理与信息系统专业、管理科学与工程专业及计算机相关专业的本科生和研究生的教材，也可作为从事信息化相关工作的管理人员、信息安全管理人员、网络与信息系统安全管理人员、IT 相关人员的参考书。

图书在版编目(CIP)数据

信息安全管理与风险评估/赵刚编著. --北京：清华大学出版社，2013
21 世纪高等学校规划教材 · 信息管理与信息系统
ISBN 978-7-302-33600-6

Ⅰ. ①信… Ⅱ. ①赵… Ⅲ. ①信息系统－安全管理－高等学校－教材 ②信息系统－安全技术－风险分析－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2013)第 203897 号

责任编辑：魏江江　薛　阳
封面设计：傅瑞学
责任校对：时翠兰
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：13.25　　**字　　数**：315 千字
版　　次：2014 年 1 月第 1 版　　**印　　次**：2014 年 1 月第1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：053926-01

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程”（简称“质量工程”），通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上。精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻性。教材由个人申报或各校推荐（通过所在高校的“编委会”成员推荐），经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前，针对计算机类和电子信息类相关专业成立了两个“编委会”，即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括：

(1) 21 世纪高等学校规划教材·计算机应用——高等学校各类专业，特别是非计算机专业的计算机应用类教材。

(2) 21 世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21 世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21 世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21 世纪高等学校规划教材·信息管理与信息系统。

(6) 21 世纪高等学校规划教材·财经管理与应用。

(7) 21 世纪高等学校规划教材·电子商务。

(8) 21 世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力，在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌，为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格，这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人：魏江江

E-mail：weijj@tup.tsinghua.edu.cn

前言

信息化已融入到人类社会的每一个角落，不断推动着社会的进步和发展。然而，无处不在的信息孕育着随时可能发生的风险，信息安全事件时有发生，信息安全问题也成为全社会共同关注的问题，信息系统的安全、管理、风险与控制日益成为突出的问题。信息安全研究所涉及的领域相当广泛，信息安全的建设是一个系统工程，正确的做法是遵循国内外相关信息安全标准与最佳实践，考虑组织对信息安全各个层面的需求，在风险评估的基础上引入合理的控制措施，建立信息安全管理体系以保证信息的安全属性。绝大多数信息安全问题是管理方面的缺陷，因此信息安全管理是十分重要的课题，在解决信息安全问题中占重要地位，其发展对信息安全人才的培养提出了更高的要求。风险评估是信息安全管理体系和信息安全风险管理的基础，是建立信息安全保障体系的必要前提，通过风险评估能够将信息安全活动的重点放在重要的问题上。本书旨在通过本课程的学习，帮助学生了解信息安全管理、信息安全风险评估的基本知识、相关标准，理解信息安全管理体系的建立过程以及风险评估的实施过程，进而在实际工作中得到应用，对组织的具体实践提供理论指导，帮助组织建立合理的信息安全管理体系。

本书从信息安全管理、风险评估的概念出发，全面、系统地介绍了信息安全管理体系、信息安全风险评估、信息系统安全等级保护、云计算安全管理与风险评估、IT 治理等内容。全书由基本知识、信息安全风险评估、信息安全管理三部分构成，共分为 11 章。第 1 章引论，着重介绍了信息安全管理和风险评估相关的基本概念及其发展过程、现状和发展趋势，初步介绍了信息安全管理与风险评估的关系；第 2 章信息安全管理的主要内容，主要介绍了信息安全管理体系模型、建立信息安全管理体系的基本过程，讨论了国内外信息安全管理相关标准以及主要的信息安全管理工具；第 3 章信息安全风险评估的主要内容，主要介绍了风险评估模型、实施风险评估的总体流程，讨论了国内外相关标准以及主要的风险评估工具；第 4 章 IT 治理概述，主要介绍了 IT 治理概念和基础内容，围绕国际上公认的 IT 治理标准，重点讨论了 IT 治理支持手段；第 5 章信息安全风险评估实施流程，充分讨论了风险评估准备、资产识别、威胁识别、脆弱性识别、已有安全措施确认、风险分析等实施风险评估的各阶段作业流程和各方面内容，介绍了风险处置计划和风险评估报告的内容；第 6 章信息系统生命周期各阶段的风险评估，介绍了信息系统生命周期中规划阶段、设计阶段、实施阶段、运维阶段和废弃阶段中风险评估的工作内容；第 7 章建立信息安全管理体系的工作流程，深入细致地讨论了信息安全管理体系的策划与准备、设计与建立、实施与运行、体系审核、改进与保持等各阶段的工作内容；第 8 章信息安全管理体系的认证，从信息安全管理体系认证概念出发，介绍了认证的目的、范围、认证机构，及认证过程等内容；第 9 章信息安全管理控制措施，详细阐述了选择控制措施的方法和过程，围绕国内外较为通用的标准、重点讨论了信息安全管理控制规范；第 10 章信息系统安全等级保护标准体系，从等级保护基本知识出发，详细讨论了等级保护实施方法和过程，着重分析了等级保护与信息安全管理体

系、等级保护与信息安全风险评估的关系；第 11 章云计算的安全管理与风险评估，介绍了云计算的模式与架构，着重分析了云计算的信息安全问题，重点讨论了云计算风险评估的特点和方式，深入阐述了云计算的风险控制措施。

全书结构合理、内容全面、概念清晰、深入浅出，符合教学特点和需求，业务实用性强，紧跟信息安全管理与风险评估研究以及 IT 应用的发展趋势，融入了最新的创新内容。

本书既可作为高等院校信息安全专业、信息管理与信息系统专业、管理科学与工程专业及计算机相关专业的本科生和研究生的教材，也可作为从事信息化相关工作的管理人员、信息安全管理人员、网络与信息系统安全管理人员、IT 相关人员的参考书。

本书是作者长期从事理论研究和科学实践以及教学经验和成果的归纳总结，作者精心设计安排全书的结构和内容，以适应不同层次和不同专业读者的需求。书中汲取了大量国内外本领域代表文献的精华，参考了大量的国内外有关研究成果，在此，谨向书中提到和参考文献列出的作者表示感谢。作者所指导的学生刘换、宋健豪等参与了编写本书的相关工作，在此一并表示感谢。同时感谢北京信息科技大学信息管理学院的领导、全体教师的大力支持和帮助。最后，衷心感谢清华大学出版社为本书出版付出的辛勤劳动。

信息技术在飞速发展，信息安全管理和风险评估也在不断创新和发展，其理念和技术等都在不断地更新。书稿虽经多次修改，但由于作者水平有限，书中难免存在不足和疏漏之处，诚望使用本教材的师生和读者不吝指教。

本书配套的教学电子课件，读者可登录清华大学出版社网站（http://www.tup.com.cn）下载。

编　者

2013 年 4 月于北京

参考文献

[1] 孙强，陈伟，王东红. 信息安全管理全球最佳实务与实施指南. 北京：清华大学出版社，2004.

[2] 范红，冯登国，吴亚非. 信息安全风险评估方法与应用. 北京：清华大学出版社，2006.

[3] 中国标准出版社第四编辑室. 信息安全标准汇编 信息安全管理卷. 北京：中国标准出版社，2008.

[4] 谢宗晓，郭立生. 信息安全管理体系应用手册——ISO/IEC 27001 标准解读及应用模板. 北京：中国标准出版社，2008.

[5] 范红. 信息安全风险评估规范国家标准理解与实施. 北京：中国标准出版社，2007.

[6] 吴亚非，李新友，禄凯. 信息安全风险评估. 北京：清华大学出版社，2007.

[7] 于军. 信息安全管理的体系化管理——ISMS 在电子政务中的应用. 北京：国防工业出版社，2008.

[8] 张红旗，王新昌，杨英杰等. 信息安全管理. 北京：人民邮电出版社，2007.

[9] 张泽虹，赵冬梅. 信息安全管理与风险评估. 北京：电子工业出版社，2010.

[10] 王春东，杨宏，赵俊阁. 信息安全管理. 武汉：武汉大学出版社，2008.

[11] 吴晓平，付钰. 信息系统安全风险评估理论与方法. 北京：科学出版社，2011.

[12] 刘换，赵刚. 人工智能在信息安全风险评估中的应用. 北京信息科技大学学报(自然科学版)，2012，27(4)：59-63.

[13] 李艳杰. GB/T 22080—2008《信息安全管理体系 要求》解析. 中国标准导报，2012，10：6-9.

[14] 许玉娜，罗锋盈，陈星. SP 800-39：2011 信息安全风险管理研究. 信息技术与标准化，2012，4：41-44.

[15] 胡灵娟. 大型数据中心 ISO 27001 信息安全管理体系贯标认证实践. 中国金融电脑，2012，5：32-37.

[16] 赵战生. 完善信息安全管理标准 落实信息安全等级保护制度. 信息网络安全，2008，1：15-18.

[17] 陈清明，张俊彦. 信息安全风险评估工具及其应用分析. 信息安全与通信保密，2010，1：93-95.

[18] 王亚东，吕丽萍，汤永利等. 信息安全管理体系与等级保护的关系研究. 北京电子科技学院学报，2012，20(2)：26-31.

[19] 赵刚，刘换. 基于多层次模糊综合评判及熵权理论的实用风险评估. 清华大学学报(自然科学版)，2012，52(10)：1382-1387.

[20] 马遥，黄俊强. 信息安全管理体系与等级保护管理要求. 信息技术，2012，6：140-142.

[21] 周佑源，张晓梅. 信息安全管理在等级保护实施过程中的要点分析. 信息安全与通信保密，2009，9：66-68.

[22] 黄成哲. 信息安全风险评估工具综述. 黑龙江工程学院学报，2006，20(1)：45-48.

[23] 蔡盈芳. 基于云计算的信息系统安全风险评估模型. 中国管理信息化，2010，13(12)：75-77.

[24] 汪兆成. 基于云计算模式的信息安全风险评估研究. 信息网络安全，2011，9：56-59.

[25] 薄明霞，陈军，王渭清等. 浅谈云计算的安全隐患及防护策略. 信息安全与技术，2011，9：62-64.

[26] 刘波. 云计算的安全风险评估及其应对措施探讨. 移动通信，2011，9：34-37.

[27] 董建锋，裴立军，王兰英. 云计算环境下信息安全分级防护研究. 信息网络安全，2011，6：38-40.

目录

第一部分 基本知识

第 1 章 引论 …… 3

1.1 信息安全管理概述 …… 3

1.1.1 信息安全管理的内涵 …… 3

1.1.2 信息安全管理发展状况 …… 5

1.2 信息安全风险评估概述 …… 7

1.2.1 信息安全风险评估的内涵 …… 7

1.2.2 风险评估的意义 …… 8

1.2.3 信息安全风险评估发展状况 …… 8

1.3 信息安全管理与风险评估的关系 …… 13

思考题 …… 14

第 2 章 信息安全管理的主要内容 …… 15

2.1 信息安全管理体系模型 …… 15

2.1.1 信息安全管理体系及其产业链 …… 15

2.1.2 PDCA 模型 …… 16

2.1.3 建立信息安全管理体系的流程概述 …… 20

2.1.4 信息安全管理体系与 PDCA 循环 …… 21

2.2 信息安全管理相关标准 …… 22

2.2.1 国外信息安全管理相关标准 …… 22

2.2.2 国内信息安全管理相关标准 …… 27

2.3 信息安全管理工具 …… 28

思考题 …… 29

第 3 章 信息安全风险评估的主要内容 …… 30

3.1 信息安全风险评估工作概述 …… 30

3.1.1 风险评估依据 …… 30

3.1.2 风险评估原则 …… 30

3.1.3 风险评估组织管理 …… 31

3.2 风险评估基础模型 …… 32

3.2.1 风险要素关系模型 …… 32

3.2.2 风险分析原理 …… 34
3.2.3 风险评估方法 …… 34
3.2.4 风险评估实施流程概述 …… 35
3.3 风险评估相关标准 …… 36
3.3.1 国外信息安全风险评估相关标准 …… 36
3.3.2 国内信息安全风险评估相关标准 …… 42
3.4 风险评估工具 …… 43
思考题 …… 44

第 4 章 IT 治理概述 …… 45

4.1 IT 治理 …… 45
4.2 IT 治理支持手段 …… 46
思考题 …… 54

第二部分 信息安全风险评估

第 5 章 信息安全风险评估实施流程 …… 57

5.1 风险评估准备 …… 57
5.2 资产识别 …… 58
5.2.1 工作内容 …… 59
5.2.2 参与人员 …… 59
5.2.3 工作方式 …… 60
5.2.4 工具及资料 …… 63
5.2.5 输出结果 …… 64
5.3 威胁识别 …… 65
5.3.1 工作内容 …… 65
5.3.2 参与人员 …… 65
5.3.3 工作方式 …… 66
5.3.4 工具及资料 …… 70
5.3.5 输出结果 …… 70
5.4 脆弱性识别 …… 70
5.4.1 工作内容 …… 70
5.4.2 参与人员 …… 70
5.4.3 工作方式 …… 71
5.4.4 工具及资料 …… 73
5.4.5 输出结果 …… 74
5.5 已有安全措施确认 …… 74
5.5.1 工作内容 …… 74
5.5.2 参与人员 …… 75

5.5.3 工作方式 …… 75
5.5.4 工具及资料 …… 76
5.5.5 输出结果 …… 76
5.6 风险分析 …… 77
5.7 风险处理计划 …… 83
5.7.1 现存风险判断 …… 84
5.7.2 控制目标确定 …… 84
5.7.3 控制措施选择 …… 85
5.8 风险评估报告 …… 87
思考题 …… 88

第 6 章 信息系统生命周期各阶段的风险评估 …… 89

6.1 规划阶段的信息安全风险评估 …… 89
6.2 设计阶段的信息安全风险评估 …… 89
6.3 实施阶段的信息安全风险评估 …… 90
6.4 运维阶段的信息安全风险评估 …… 91
6.5 废弃阶段的信息安全风险评估 …… 92
思考题 …… 92

第三部分 信息安全管理

第 7 章 建立信息安全管理体系的工作流程 …… 95

7.1 信息安全管理体系的策划与准备 …… 95
7.1.1 信息安全管理体系 …… 95
7.1.2 信息安全管理体系的准备 …… 96
7.2 信息安全管理体系的设计与建立 …… 100
7.2.1 编写信息安全管理体系文件 …… 100
7.2.2 建立信息安全管理框架 …… 103
7.3 信息安全管理体系的实施与运行 …… 106
7.3.1 信息安全管理体系的试运行 …… 106
7.3.2 实施和运行 ISMS 工作 …… 107
7.3.3 管理信息安全事件 …… 108
7.3.4 保持 ISMS 持续有效 …… 111
7.4 信息安全管理体系的审核 …… 112
7.4.1 审核的概念 …… 112
7.4.2 ISMS 内部审核 …… 113
7.4.3 信息安全管理体系管理评审 …… 116
7.5 信息安全管理体系的改进与保持 …… 119
7.5.1 持续改进 …… 119

7.5.2 纠正措施…… 119
7.5.3 预防措施…… 119
思考题…… 120

第 8 章 信息安全管理体系的认证…… 121

8.1 信息安全管理认证 …… 121
8.1.1 认证的定义…… 121
8.1.2 认证的目的和作用…… 121
8.1.3 认证范围…… 122
8.2 认证的基本条件与认证机构的选择 …… 122
8.2.1 认证条件…… 122
8.2.2 认证机构…… 122
8.3 信息安全管理体系的认证过程 …… 123
8.3.1 认证的准备…… 123
8.3.2 认证的实施…… 124
8.3.3 证书与标志…… 127
8.3.4 维持认证…… 127
思考题…… 128

第 9 章 信息安全管理控制措施…… 129

9.1 选择控制措施的方法 …… 129
9.2 选择控制措施的过程 …… 131
9.3 风险管理 …… 133
9.4 信息安全管理控制规范 …… 135
9.4.1 从需求解析信息安全管理控制措施…… 135
9.4.2 从安全问题解析信息安全管理控制措施…… 136
9.4.3 控制目标与控制措施详述…… 137
思考题…… 166

第 10 章 信息系统安全等级保护标准体系 …… 167

10.1 信息系统安全等级保护…… 167
10.1.1 等级保护概述…… 167
10.1.2 等级保护实施方法与过程…… 169
10.2 ISMS 与等级保护 …… 171
10.3 等级保护与风险评估…… 175
10.3.1 风险评估是等级保护制度建设的基础…… 175
10.3.2 等级保护和风险评估的宏观联系…… 176
10.3.3 风险评估是信息系统安全等级保护的技术支撑…… 176
10.3.4 风险评估在等级保护周期中的作用…… 177

10.3.5 风险评估在等级保护层次中的应用…… 179
思考题…… 179

第 11 章 云计算的安全管理与风险评估 …… 180

11.1 云计算概述…… 180
11.2 云计算的信息安全问题…… 182
11.3 云计算的风险评估与控制措施…… 183
11.3.1 云计算的风险评估…… 183
11.3.2 云计算的安全措施…… 185
思考题…… 187

附录 信息安全管理与风险评估相关表格(参考示例)…… 188

参考文献 …… 197

第一部分 基本知识

- 第1章 引论
- 第2章 信息安全管理的主要内容
- 第3章 信息安全风险评估的主要内容
- 第4章 IT治理概述

第1章 引论

1.1 信息安全管理概述

人类社会已经进入了信息时代，当今社会的发展对信息资源依赖的程度越来越大，从人们日常生活、组织运作，到国家管理，信息资源都已成为不可或缺的重要资源，信息已经渗透到了人类社会的每一个角落，融入了人们生活的每一个细节，没有各种信息的支持，现代社会将不能继续生存和发展下去。信息已经成为人类的重要资产，在政治、经济、军事、教育、科技、生活等方面发挥着重要作用。然而，信息在成为人类重要资产、为人们所用、给人们带来巨大价值的同时，也受到了各种各样来自于组织内部与外部威胁的冲击，信息安全事件在全球范围内屡屡发生，由于计算机技术的迅猛发展而带来的信息安全问题正变得日益突出，给人类社会的发展带来了巨大损失。

信息安全管理是随着信息和信息安全的发展而发展的。由于信息具有易传播、易扩散、易损毁的特点，信息资产比传统的实物资产更加脆弱，更容易受到损害，这样将使组织在业务运作过程中面临巨大的风险。这种风险主要来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节和漏洞，以及大量存在于组织内外的各种威胁。因此，对信息系统需要加以严格管理和妥善保护，信息安全管理也随之产生。

1.1.1 信息安全管理的内涵

1. 信息

信息(Information)的定义多种多样。国际公认的 ISO/IEC 信息技术安全管理指南(GMITS)对信息给出如下解释：信息是通过施加于数据上的某些约定而赋予这些数据的特定含义。信息可以简单地定义为经过加工的数据或消息，是对决策者有价值的数据。一般意义上的信息是指事物运动的状态和方式，是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。通常情况下，可以把信息理解为消息、信号、数据、情报、知识，可以是信息设施中存储与处理的数据、程序，可以是打印或书写出来的论文、电子邮件、设计图纸、业务方案，也可以是显示在胶片等载体或表达在会话中的消息。

2. 信息系统的定义

GB 17859—1999《计算机信息系统安全保护等级划分准则》定义：计算机信息系统是由

计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。毫无疑问,计算机及各类通信网络的出现与蓬勃发展使信息技术出现了前所未有的革命,也使信息量急剧膨胀。

3. 信息安全的定义

信息安全是一个广泛而抽象的概念,不同领域的不同方面对其概念的阐述都会有所不同,建立在网络基础之上的现代信息系统,其安全定义较为明确,其定义为:保护信息系统的硬件、软件及相关数据,使之不因为偶然或恶意侵犯而遭到破坏、更改及泄漏,保证信息系统能够连续、可靠、正常地运行。在商业和经济领域,资产是任何对组织有价值的事物,像其他重要的业务资产一样,信息是一种资产。对于一个组织的业务,信息资产是其中的关键,随着业务互联的增加,造成信息暴露出更多数量、更广范围的威胁和脆弱性,需要得到适当的保护。因此,信息安全主要强调的是保障信息不受威胁的侵扰,消减并控制风险,保持业务操作的连续性,将风险造成的损失和影响降到最低,并且获得最大化的投资回报和商业机会。

信息安全通过实施一套控制措施,包括方针、过程、程序、组织结构和软件硬件功能来实现。这些控制措施需要建立、实施、评审以及改进,以保障组织特定的安全和业务目标。

在信息保障的概念中,信息安全一般包括实体安全、运行安全、信息安全和管理安全4个方面的内容。实体安全包括环境安全、设备安全、媒体安全3个方面。运行安全包括风险分析、审计跟踪、备份和恢复、应急4个方面。信息安全包括操作系统安全、数据库安全、网络安全、病毒保护、访问控制、加密与鉴别7个方面。管理安全是指通过信息安全相关的法令和规章制度以及安全管理手段,确保信息安全生存与运营。

4. 信息安全属性

从信息安全属性出发,将信息安全的主要目标定义为信息的机密性、完整性和可用性的保持。ISO/IEC 13335-1:2004以及ISO/IEC 27002:2005中将信息安全定义为:保护信息的保密性(Confidentiality)、完整性(Integrity)、可用性(Availability)及其他属性,包括真实性(Authenticity)、可审核性(Accountability)、不可否认性(non-repudiation)和可靠性(Reliability)等。可用性是指已授权实体一旦需要就可访问和使用的特性;保密性是指使信息不泄漏给未授权的个人、实体、过程或不使信息为其利用的特性;完整性是指数据未经授权不可修改或破坏的特性,如图1-1所示。

5. 信息安全管理及其内容

信息安全管理是通过维护信息的机密性、完整性和可用性等来管理和保护信息资产的一项体制,是对信息安全保障进行指导、规范和管理的一系列活动和过程。管理体系包括组织机构、策略、策划、活动、职责、惯例、程序、过程和资源。

6. 信息安全管理体系

信息安全管理体系(Information Security

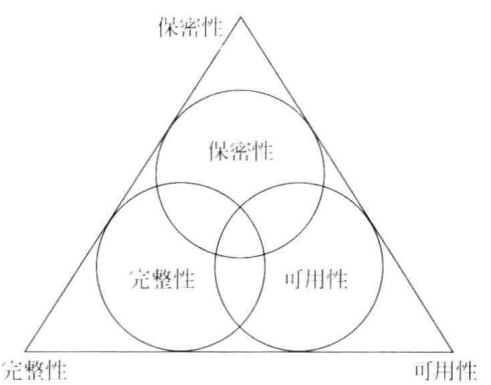

图1-1 安全属性