(ISC)² Official Study Guide

安全技术经典译丛

CISSP

官方学习指南(第8版)

CISSP: Certified Information Systems Security Professional Official Study Guide, Eighth Edition

迈克·查普尔(Mike Chapple), CISSP
[美] 詹姆斯·迈克尔·斯图尔特(James Michael Stewart), CISSP 著
达瑞尔·吉布森(Darril Gibson), CISSP
王连强 吴 萧 罗爱国 等译
北京爱思考科技有限公司 审

涵盖CISSP所有考试目标，全面讲解资产安全、软件开发安全、安全运营等重要主题！

清华大学出版社

安全技术经典译丛

CISSP 官方学习指南

(第 8 版)

迈克 • 查普尔(Mike Chapple)，CISSP
[美] 詹姆斯 • 迈克尔 • 斯图尔特(James Michael Stewart)，CISSP 著
达瑞尔 • 吉布森(Darril Gibson)，CISSP

王连强 吴 潇 罗爱国 等译

北京爱思考科技有限公司 审

清华大学出版社

北 京

Mike Chapple, James Michael Stewart, Darril Gibson
CISSP: Certified Information Systems Security Professional Official Study Guide, Eighth Edition
EISBN：978-1-119-47593-4

北京市版权局著作权合同登记号　图字：01-2018-4945

图书在版编目(CIP)数据

CISSP官方学习指南 / (美)迈克 • 查普尔(Mike Chapple)，(美)詹姆斯 • 迈克尔 • 斯图尔特(James Michael Stewart)，(美)达瑞尔 • 吉布森(Darril Gibson)著；王连强 等译. －8版. －北京：清华大学出版社，2019
(安全技术经典译丛)
书名原文：CISSP: Certified Information Systems Security Professional Official Study Guide, Eighth Edition
ISBN 978-7-302-53029-9

Ⅰ. ①C… Ⅱ. ①迈… ②詹… ③达… ④王… Ⅲ. ①信息系统－安全技术－资格考试－指南
Ⅳ. ①TP309-62

中国版本图书馆 CIP 数据核字(2019)第 093926 号

责任编辑：王　军
装帧设计：孔祥峰
责任校对：成凤进
责任印制：丛怀宇

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
印 装 者：三河市铭诚印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：46.75　　**字　　数**：1227 千字
版　　次：2019 年 10 月第 1 版　　**印　　次**：2019 年 10 月第 1 次印刷
定　　价：158.00 元

产品编号：080790-01

欢迎你，(ISC)^2 的未来成员：

祝贺你开启自己的 CISSP 认证之旅。赢得 CISSP 资质，是你的网络安全职业生涯的一个里程碑，既令人激动，又具有奖赏意义。它不仅表明，你已有能力开发和管理一个组织的网络安全运营，胜任几乎所有方面的工作，而且表明你向你的雇主作出承诺，你将活到老学到老，终身致力于实现(ISC)² 提出的“营造一个安全稳定网络世界”的愿景。

本学习指南包含的材料源自(ISC)² CISSP 通用知识体系。它将帮助你准备考试，评估你在以下 8 个域的能力：

- 安全与风险管理
- 资产安全
- 安全架构和工程
- 通信与网络安全
- 身份和访问管理
- 安全评估与测试
- 安全运营
- 软件开发安全

虽然本学习指南会为你的备考提供帮助，但能否通过 CISSP 考试，最终还取决于你掌握各域知识并借助自己的实践经验把这些概念适用于实际的能力。

祝你在继续追求成为一名 CISSP 及 (ISC)² 认证会员的道路上一帆风顺！

David Shearer, CISSP
(ISC)² CEO

译 者 序

信息技术已广泛应用于我国各行业，网络空间逐步兴起，这极大促进了我国经济社会的繁荣进步，但同时带来了新的安全风险和挑战。网络安全不仅牵涉公众个人，更涉及所有企业和社会机构，已逐步上升为信息时代国家安全的战略基石。2016 年 12 月，我国《国家网络空间安全战略》发布，着重强调“没有网络安全，就没有国家安全”，网络安全的重要性和意义更加凸显，我国信息安全产业也迎来了更大的发展机遇。2017 年 6 月，《中华人民共和国网络安全法》正式实施，这使得我国的网络安全工作有法可依，网络安全市场空间、产业投入与建设将步入持续稳定的发展阶段。

CISSP (Certified Information Systems Security Professional)——“(ISC)² 注册信息系统安全师”认证是信息安全领域被全球广泛认可的 IT 安全专业认证，一直以来被誉为业界的“金牌标准”。CISSP 认证确保了信息安全从业人员具有构建及管理组织信息安全必备的广泛知识、技能与经验。

(ISC)² 成立于 1989 年，是全球最大的网络、信息、软件与基础设施安全认证会员制非营利性组织，会员遍布超过 160 个国家和地区。CISSP 认证由(ISC)² 于 1994 年开始逐步推广，2013 年正式引入中国大陆，并启用了中文认证考试，它见证了国内信息安全行业的蓬勃发展，也见证了国内信息安全从业人员从兴趣爱好走向职业化的发展道路。如果你打算在信息安全这一当今最为瞩目的行业领域里成就一番事业，获得 CISSP 认证理应成为你的下一个职业目标。

本书的内容源自(ISC)² CISSP 通用知识体系，可为学员参加 CISSP 认证考试打下坚实基础。本书全面系统地讲述 CISSP 认证考试的八大知识域：安全与风险管理、资产安全、安全架构和工程、通信与网络安全、身份和访问管理、安全评估与测试、安全运营和软件开发安全，涵盖风险管理、云计算、移动安全、应用开发安全等热点信息安全议题，是全球最新信息行业最佳实践的总结与展现。本书旨在为任何对 CISSP 感兴趣且想通过认证的读者提供详细指导。尽管本书主要是为 CISSP 认证考试撰写的学习指南，但我们希望本书能在你通过认证考试后仍可作为一本有价值的专业参考书。

北京爱思考科技有限公司(Beijing Athink Co., Ltd)特意组织力量将该书翻译出版，希望书中介绍的有关 CISSP 认证考试的内容对读者理解和掌握通用知识体系，对 CISSP 考生进行学习和备考提供支持和帮助。

在这里衷心感谢本书的原作者和编辑们，是他们的支持和授权，才使这本书的中文版得以顺利出版；还要感谢(ISC)² 中国办公室和清华大学出版社将本书引入中国，以飨广大安全行业的读者；更要感谢为本书的出版和审校工作付出大量艰辛劳动的各位译者，是他们的辛勤工作，才能让更多读者更方便地学习 CISSP 知识体系；最后感谢清华大学出版社的编辑团队，是他们耐心细致的审校，确保了本书的专业性和准确性。

最后，预祝所有应试者顺利通过 CISSP 认证考试；衷心希望广大读者通过本书的阅读与学习，更好地掌握信息安全知识体系，提升自身信息安全水平和能力，为中国信息安全事业贡献自己的力量！

译者简介

王连强，现任北京时代新威信息技术有限公司技术负责人，博士、全国信安标委 WG7 成员，持有信息系统审计师、IPMP 等认证证书，负责统筹本书翻译各项工作事务，并承担本书第 6 章、第 7 章和第 17 章的翻译工作，以及全书的审校和定稿工作。

吴潇，现任北京天融信网络安全技术有限公司专家级安全顾问，持有 CISSP、CISA、PMP、ISO27001 等认证证书，负责本书第 1~4 章的翻译工作。

罗爱国，现就职于互联网公司，持有 CISSP 及 CSSLP 认证证书，参与本书第 18~21 章的翻译工作。

郭鹏程，现任北森云计算安全负责人，中国云安全联盟专家委员会专家、云安全讲师、C-Star 咨询师，持有 CISSP、CCSK 等认证证书，负责本书第 11 章、第 13 章和第 14 章的翻译工作。

刘北水，现任中国赛宝实验室信息安全研究中心工程师，持有 CISSP、PMP 等认证证书，负责本书第 15 章和第 16 章的翻译工作，并为本书撰写译者序。

孙书强，北京中科博安科技有限公司创始人，$(ISC)^2$ 北京分会秘书长、$(ISC)^2$ 官方授权讲师，持有 CISSP-ISSAP、ISSMP、CISA、PMP、系统分析师等认证证书，负责本书第 8 章和第 9 章的翻译工作。

顾广宇，现任国家电网安徽省电力科学研究院高级工程师，持有 CISSP 认证证书，负责本书第 10 章和第 12 章的翻译工作。

马多贺，现任中国科学院信息工程研究所副研究员，$(ISC)^2$ 北京分会会员主席、CISSP 认证讲师、博士、硕士生导师，持有 CISSP、PMP 等认证证书，参与了本书第 5 章的翻译工作。

最后，感谢顾伟在本书译校过程中提供的帮助。

献给我的导师、朋友和同事 Dewitt Latimer。深深怀念你。

——Mike Chapple

献给 Cathy，你对世界和生活的见解常令我震惊，令我敬畏，同时也加深了我对你的爱。

——James Michael Stewart

献给 Nimfa，感谢你 26 年来的陪伴，感谢你允许我把自己的生活与你共享。

——Darril Gibson

致　谢

我们要感谢 Sybex 对这个项目的持续支持。尤其感谢第 8 版的开发编辑 Kelly Talbot 以及技术编辑 Jeff Parker、Bob Sipes 和 David Seidl，他们的指导性意见对于本书的不断完善功不可没。还要感谢我们的代理人 Carole Jelen，正是他的持续帮助才使这些项目最终圆满完成。

——Mike、James 和 Darril

特别感谢圣母大学的信息安全团队，他们用大量时间就安全问题开展的有趣对话和辩论，激发了本书的创作灵感并提供了许多资料。

我要感谢 Wiley 团队，他们在本书的整个开发过程中都在提供宝贵帮助。还要感谢我的文稿代理人 Carole Jelen。James Michael Stewart 和 Darril Gibson 都是伟大的合作者。勤奋而博学的技术编辑 Jeff Parker、Bob Sipes 和 David Seidl 提出了许多宝贵意见。

我还要感谢参与本书制作，但我素未谋面的许多人：图形设计团队、制作人员以及为本书面世付出辛劳的所有人员。

——Mike Chapple

感谢 Mike Chapple 和 Darril Gibson 为本项目持续作出的贡献。同时感谢我的 CISSP 课程的所有学生，他们为我的培训课件以及最终形成的本书的完善提出了见解和意见。致我挚爱的妻子 Cathy：我们共同建立的美好生活和家庭远超我的想象。致 Slayde 和 Remi：你们在快速成长，学习上也进步惊人，你们每天都带给我无尽的欢乐。你们两个都会成长为了不起的人。致我的妈妈 Johnnie：有你在身边陪伴真好。致 Mark：无论时间过去多久，我们见面的次数有多少，我都始终并将永远是你的朋友。最后，一如既往地，致 Elvis：你从前喜欢鲜熏肉，后来又迷上花生酱/香蕉/熏肉三明治，我想这恰恰是你历经沧桑的证明！

——James Michael Stewart

感谢 Jim Minatel 和 Carole Jelen 在(ISC)^2 发布考试目标之前所做的及时更新。这帮助我们的这个新版本领先了一步，感谢你们付出的努力。与 James Michael Stewart 和 Mike Chapple 这样才华横溢的人一起工作是一件乐事。感谢你们俩为这个项目做的所有工作。技术编辑 Jeff Parker、Bob Sipes 和 David Seidl 为我们提供了许多很好的反馈意见，这本书因为他们的努力而变得更优秀。感谢 Sybex 团队(包括项目经理、编辑和图形设计专家)为帮助本书付梓所做的所有工作。最后，感谢我的妻子 Nimfa，在我写这本书的过程中，她容忍我用掉大量业余时间。

——Darril Gibson

作者简介

Mike Chapple，CISSP、博士、Security+、CISA、CySA+，圣母大学 IT、分析学和运营学副教授。曾任品牌研究所首席信息官、美国国家安全局和美国空军信息安全研究员。他主攻网络入侵检测和访问控制专业。Mike 经常为 TechTarget 所属的 SearchSecurity 网站撰稿，著书逾 25 本，其中包括《(ISC)：CISSP 官方习题集》《CompTIA CSA+学习指南》以及《网络战：互连世界中的信息战》。

James Michael Stewart，CISSP、CEH、ECSA、CHFI、Security+、Network+，从事写作和培训工作 20 多年，目前专注于安全领域。自 2002 年起一直讲授 CISSP 培训课程，互联网安全、道德黑客/渗透测试等内容更在他的授课范围之内。他是超过 75 部著作以及大量课件的作者和撰稿者，内容涉及安全认证、微软主题和网络管理，其中包括《Security+ (SY0-501) 复习指南》。

Darril Gibson，CISSP、Security+、CASP，YCDA 有限责任公司首席执行官，是 40 多部著作的作者或共同作者。Darril 持有多种专业证书，经常写作、提供咨询服务和开展教学，涉及各种技术和安全主题。

技术编辑简介

Jeff T. Parker，CISSP、技术编辑和审稿人，主攻信息安全的多个重点领域。Jeff 为作者服务，在需要的地方给作者的著作加上自己的经验和实用知识。Jeff 在波士顿为惠普公司做了 10 年咨询工作，又在捷克为《布拉格邮报》工作了 4 年，这些履历是他经验的来源。Jeff 现定居加拿大，教自己的孩子以及其他中学生如何建立(和毁掉)家庭实验室。他最近与人合著了《安全专业人员专用版 Wireshark》，目前正在撰写《CySA+实用考试指南》。他是活到老学到老的楷模！

Bob Sipes，CISSP、DXC Technology 公司的企业安全架构师和账户安全官，负责为 DXC 的客户提供战术和战略指导。他持有多种专业证书，积极参与包括 ISSA 和 Infragard 在内的安全专业组织的各项活动。他在网络安全、通信和领导力等领域具有丰富的演讲经验。Bob 把自己的业余时间花在收集古籍上，是一个狂热的古籍收藏家；他拥有一个庞大的图书馆，收藏了大量19世纪和20世纪初的儿童文学作品。你可以通过Twitter账户@bobsipes关注Bob。

David Seidl，CISSP、圣母大学校园技术服务部高级主管，并在该校门多萨商学院讲授网络安全和联网课程。David 著有多部网络安全认证和网络战著作，并担任《CISSP 官方学习指南》第 6 版、第 7 版和第 8 版的技术编辑。David 拥有东密歇根大学信息安全硕士学位和通信技术学士学位，同时持有 CISSP、GPEN、GCIH 和 CySA+认证证书。

前　言

本书可为你参加 CISSP(注册信息系统安全师)认证考试打下坚实基础。买下这本书，就表明你想学习并通过这一认证提高自己的专业技能。这里将对本书和 CISSP 考试做基本介绍。

本书为想以努力学习方式通过 CISSP 认证考试的读者和学生而设计。如果你的目标是成为一名持证安全专业人员，则 CISSP 认证和本学习指南是你的最佳选择。本书的目的就是帮助你为参加 CISSP 考试做好准备。

在深入阅读本书前，你首先要完成几项任务。你需要对 IT 和安全有一个大致了解。你应该在 CISSP 考试涵盖的 8 个知识域中的两个或多个拥有 5 年全职全薪工作经验(如果你有本科学历，则有 4 年工作经验即可)。如果根据$(ISC)^2$规定的条件你具备了参加 CISSP 考试的资格，则意味着你做好了充分准备可借助本书备考 CISSP。有关$(ISC)^2$的详细信息，稍后介绍。

如果你拥有$(ISC)^2$先决条件路径认可的其他认证，$(ISC)^2$也允许把 5 年工作经验的要求减掉一年。这些认证包括 CAP、CISM、CISA、CCNA Security、Security+、MCSA、MCSE 等，以及多种 GIAC 认证。有关资格认证的完整列表，可访问 https://www.isc2.org/certifications/CISSP/Prerequisite-pathway 查询。需要指出的是，你只能用一种方法减少工作经验年限，要么是本科学历，要么是认证证书，不能两者都用。

$(ISC)^2$

CISSP 考试由国际信息系统安全认证联盟(International Information Systems Security Certification Consortium)管理，该联盟的英文简称是$(ISC)^2$。$(ISC)^2$是一个全球性非营利组织，致力于实现 4 大任务目标：

- 为信息系统安全领域维护通用知识体系(CBK)。
- 为信息系统安全专业人员和从业者提供认证。
- 开展认证培训并管理认证考试。
- 通过继续教育，监察合格认证申请人的持续评审工作。

$(ISC)^2$由董事会管理，董事从持证从业人员中按级别选出。

$(ISC)^2$支持和提供多项专业认证，其中包括 CISSP、SSCP、CAP、CSSLP、CCFP、HCISPP 和 CCSP。这些认证旨在验证所有行业 IT 安全专业人员的知识和技术水平。有关$(ISC)^2$及其证书认证的详情，可访问$(ISC)^2$网站 www.isc2.org 查询。

CISSP 证书专为在组织内负责设计和维护安全基础设施的安全专业人员而设。

知识域

CISSP 认证涵盖 8 个知识域的内容，分别是：

- 安全与风险管理
- 资产安全
- 安全架构和工程
- 通信与网络安全
- 身份和访问管理
- 安全评估与测试
- 安全运营
- 软件开发安全

这 8 个知识域以独立于厂商的视角展现了一个通用安全框架。这个框架是支持在全球所有类型的组织中讨论安全实践的基础。

最新修订的主题域在 2018 年 4 月 15 日开始的考试中体现出来。若需要根据 8 个知识域的划分全面了解 CISSP 考试涵盖的主题范围，请访问$(ISC)^2$网站 www.isc2.org，索取“申请人信息公告”(Candidate Information Bulletin)。这份文件包含完整的考试大纲以及有关认证的其他相关信息。

资格预审

$(ISC)^2$规定了成为一名 CISSP 必须满足的资格要求。首先，你必须是一名有 5 年以上全职全薪工作经验或者有 4 年工作经验并具有 IT 或 IS 本科学历的安全专业从业人员。专业工作经验的定义是：在 8 个 CBK 域的两个或多个域内有工资或佣金收入的安全工作。

其次，你必须同意遵守道德规范。CISSP 道德规范是$(ISC)^2$希望所有 CISSP 申请人都严格遵守的一套行为准则，目的是在信息系统安全领域保持专业素养。你可在$(ISC)^2$网站 www.isc2.org 的信息栏下查询有关内容。

$(ISC)^2$还提供一个名为“$(ISC)^2$准会员”的入门方案。这个方案允许没有任何从业经验或经验不足的申请人参加 CISSP 考试，通过考试后再获得工作经验。准会员资格有 6 年有效期，申请人需要在这 6 年时间里获得 5 年安全工作经验。只有在提交 5 年工作经验证明(通常是有正式签名的文件和一份简历)之后，准会员才能得到 CISSP 证书。

CISSP 考试简介

CISSP 考试堪称从万米高空俯瞰安全，涉及更多的是理论和概念，而非执行方案和规程。它的涵盖面很广，但并不很深。若想通过这个考试，你需要熟知所有的域，但不必对每个域都那么精通。

2017 年 12 月 18 日后，CISSP 英语考试将以自适应形式呈现。$(ISC)^2$给新版考试定名为

CISSP-CAT(计算机化自适应考试)。有关这一新版考试呈现形式的详细信息，可访问 https://www.isc2.org/certifications/CISSP/CISSP-CAT 查询。

CISSP-CAT 考试将最少含 100 道考题，最多含 150 道考题。呈现给你的所有考项不会全部计入你的分数或考试通过状态。(ISC)^2 把这些不计分考项定名为*考前题*(pretest question)，而计分考项叫作*操作项*(operational item)。这些考题在考试中均不标明计入考分还是不计入考分。认证申请人会在考试中遇到 25 个不计分考项——无论他们只做 100 道考题就达到了通过等级还是看全了所有 150 道题。

CISSP-CAT 考试时间最长不超过 3 小时。如果你没等达到某个通过等级就用完了时间，将被自动判定失败。

CISSP-CAT 不允许返回前面的考题修改答案。你离开一道考题后，你选择的答案将是最终结果。

CISSP-CAT 没有公布或设置需要达到的分数。相反，你必须在最后的 75 个操作项(即考题)之内展示自己具有超过(ISC)^2 通过线(也叫*通过标准*)的答题能力。

如果计算机判断你达到通过标准的概率低于 5%，而且你已答过 75 个操作项，你的考试将自动以失败告终。一旦计算机评分系统根据必要数量考题以 95%的信心得出结论，判断你有能力达到或无法达到通过标准，将不保证有更多考题展示给你。

如果你第一次未能顺利通过 CISSP 考试，你可在以下条件下再次参加 CISSP 考试：

- 每 12 个月内你最多可以参加 3 次 CISSP 考试。
- 从第一次考试到第二次考试之间，你必须等待 30 天。
- 从第二次考试到第三次考试之间，你必须再等待 90 天。
- 从第三次考试到下次考试之间，你必须再等待 180 天，或者第一次考试之日后满 12 个月。

每次考试都需要支付全额考试费。

从前的纸质或 CBT(基于计算机的考试)平面 250 题版考试已不可能重现。CISSP 现在只使用 CBT CISSP-CAT 格式。

更新后的 CISSP 考试将以英文、法文、德文、巴西葡萄牙文、西班牙文、日文、简体中文和韩文等版本提供。

自 2017 年 12 月 18 日起，CISSP(注册信息系统安全师)考试(仅英语考试)将通过(ISC)^2 授权的 Pearson VUE 考试中心在所授权地区以 CAT 形式进行。英文以外其他语言 CISSP 考试以及(ISC)^2 所有其他认证考试将继续以固定的线性考试(linear examination)方式进行。

CISSP 考试的考题类型

CISSP 考试的大多数考题都有 4 个选项，这种题目只有一个正确答案。有些考题很简单，比如要求你选一个定义。有些考题则复杂一些，要求你选出合适的概念或最佳实践规范。有些考题会向你呈现一个场景或一种情况，让你选出最佳答案。下面举一个例子：

1. 以下哪一项是安全解决方案的最重要目标并具有最高优先级？
   A. 防止泄露
   B. 保持完整性
   C. 保持人身安全

D. 保持可用性

你必须选出一个正确或最佳答案并把它标记出来。有时，正确答案一目了然。而在其他时候，几个答案似乎全都正确。遇到这种情况时，你必须为所问的问题选出最佳答案，你应该留意一般性、特定、通用、超集和子集答案选项。还有些时候，几个答案看起来全都不对。遇到这种情况时，你需要把最不正确的那个答案选出来。

注意：

顺便提一句，这道题的答案是 C。保持人身安全永远是重中之重。

除了标准多选题格式以外，(ISC)^2 还增加了一种高级考题格式，叫作高级创新题(advanced innovative question)。其中包括拖放题和热点题。这些类型考题要求你按操作顺序、优先级偏好或与所需解决方案的适当位置的关联来排列主题或概念。具体来说，拖放题要求参试者移动标签或图标，以在图像上把考项标记出来。热点题要求考生用十字记号笔在图像上标出一个位置。这些考题涉及的概念很容易处理和理解，但你要注意放置或标记操作的准确性。

有关考试的建议

CISSP 考试由两个关键元素组成。首先，你需要熟知 8 个知识域涉及的内容。其次，你必须掌握高超的考试技巧。你最多只有 3 小时时间，期间可能要回答多达 150 道题。如此算来，每道题的答题时间平均只有 1 分多钟。因此，快速答题至关重要，但也不必太过匆忙，只要不浪费时间就好。

(ISC)^2 对 CISSP-CAT 格式的描述并未讲明猜答案是不是适合每种情况的好办法，但是这似乎确实是比跳题答问更好的策略。我们建议你在猜一道题的答案之前尽量减少选项的数量；如果实在无法排除任何答案选项，可考虑跳过这道题，而不进行随机猜测。对减少了数量的选项作出有根据的猜测，可以提高答对考题的概率。

我们还要请大家注意，(ISC)^2 并没有说明，面对由多个部分组成的考题时，如果你只答对了部分内容，是否会得到部分考分。因此，你需要注意带复选框(而不是带单选按钮)的考题，并且确保按需要的数量选择考项，以适当解决问题。

你将被发给一块白板和一支记号笔，用来记下你的思路和想法。但是写在白板上的任何东西都不能改变你的考分。离开考场之前，你必须把这块白板还给考试管理员。

为帮助你在考试中取得最好成绩，这里提出几条一般性指南：

- 先读一遍考题，再把答案选项读一遍，之后再读一遍考题。
- 先排除错误答案，再选择正确答案。
- 注意双重否定。
- 确保自己明白考题在问什么。

掌控好自己的时间。尽管可在考试过程中歇一会儿，但这毕竟会把部分考试时间消耗掉。你可以考虑带些饮品和零食，但食物和饮料不可带进考场，而且休息所用的时间是要计入考试时间的。确保自己只随身携带药物或其他必需的物品，所有电子产品都要留在家里或汽车

里。你应该避免在手腕上戴任何东西，其中包括手表、健身跟踪器和首饰。你不可使用任何形式的防噪耳机或耳塞式耳机，不过你可使用泡沫耳塞。我们还建议你穿着舒适的衣服，并带上一件薄外套(一些考场有点儿凉)。

如果英语不是你的第一语言，你可注册其他语言版本的考试。或者，如果你选择使用英文版考试，你将被允许使用翻译词典(务必事先联系你的考场，以便提前做好安排)。你必须能够证明你确实需要这样一部词典，这通常需要你出示自己的出生证或护照。

注意：

考试或考试目标偶尔会发生一些小变化。每逢这种情况，Sybex 都会在自己网站上贴出更新的内容。参加考试前应访问 www.wiley.com/go/cissp8e，确保自己掌握最新信息。

学习和备考技巧

我们建议你为 CISSP 考试制定一个月左右的晚间强化学习计划。这里提几点建议，可以最大限度增加你的学习时间；你可根据自己的学习习惯做必要修改：

- 用一两个晚上细读本书的每一章并把它的复习材料做一遍。
- 回答所有复习题，并把本书和考试引擎中的练习考试做一遍。完成每章的书面实验，并利用每章的复习题来找到一些主题，投入更多时间对它们进行深入学习，掌握其中的关键概念和战略，或许能令你受益。
- 复习$(ISC)^2$的考试大纲：www.isc2.org。
- 利用学习工具附带的速记卡来强化自己对概念的理解。

提示：

我们建议你把一半的学习时间用来阅读和复习概念，把另一半时间用来做练习题。有学生报告说，花在练习题上的时间越多，考试主题记得越清楚。除了本学习指南的练习考试外，Sybex 还出版了《(ISC): CISSP 官方习题集》。这本书为每个域都设置了 100 多道练习题，还含 4 个完整的练习考试。与本学习指南一样，它还有在线版考题。

完成认证流程

你被通知成功通过 CISSP 认证考试后，你离真正获得 CISSP 证书还差最后一步。最后一步是背书(endorsement)。这基本上是让一个本身是 CISSP 或$(ISC)^2$其他证书持有者、有很高声望并熟悉你的职业履历的人为你提交一份举荐表。通知你通过考试的电子邮件会附带把这个举荐表发给你。举荐人必须审查你的履历，确保你在 8 个 CISSP 知识域有足够的工作经验，

然后以数字形式或通过传真或邮寄方式把举荐表提交给(ISC)² 。你必须在收到通知考试成绩的电子邮件后的 90 天内，向(ISC)² 递交举荐文件。(ISC)² 将在收到举荐表后结束整个认证流程，并将通过美国邮政(USPS)给你寄送欢迎包。

CISSP 考试后的专项加强认证

(ISC)² 为 CISSP 证书持有者设置了 3 个专项加强认证。(ISC)² 围绕 CISSP 考试介绍的概念设置专项加强认证，主要针对架构、管理和工程这 3 个具体方面。这 3 个专项加强认证如下。

信息系统安全架构师(ISSAP)　面向从事信息安全架构工作的人员。涉及的关键域包括：访问控制系统和方法，密码学，物理安全集成，需求分析和安全标准、指南及准则，业务连续性计划和灾难恢复计划中与技术相关的方面，以及电信和网络安全。这是专为设计安全系统或基础设施的人员，或审计和分析这些结构的人员设置的一种证书。

信息系统安全管理师(ISSMP)　面向从事信息安全策略、实践规范、原则和规程管理的人员，涉及的关键域包括：企业安全管理实践规范，企业系统开发安全，法律、调查、犯罪取证和职业操守，运营安全合规监督，以及了解业务连续性计划、灾难恢复计划和运行连续性计划。这是专为负责安全基础设施(特别是必须强制合规的安全基础设施)的人员设置的一种证书。

信息系统安全工程师(ISSEP)　面向设计安全软硬件信息系统、组件或应用程序的人员，涉及的关键域包括：认证和认可、系统安全工程、技术管理和美国政府信息保障法规。大多数 ISSEP 为美国政府部门或管理政府安全审查的政府承包商工作。

有关这些专项加强认证的详细信息，可访问(ISC)² 网站 www.isc2.org 查阅。

本书的组织结构

本书涵盖 CISSP 通用知识体系的 8 个域，其深度足以让你清晰掌握相关资料。本书的主体由 21 章构成。域和各章的关系说明如下。

第 1~4 章：安全与风险管理。

第 5 章：资产安全。

第 6~10 章：安全架构和工程。

第 11 章和第 12 章：通信与网络安全。

第 13 章和第 14 章：身份和访问管理(IAM)。

第 15 章：安全评估与测试。

第 16~19 章：安全运营。

第 20 章和第 21 章：软件开发安全。

每章包含的元素可帮助你归纳学习重点和检验你掌握的知识。有关每章所涵盖域主题的详情，请见本书目录和各章介绍。

本学习指南的元素

你在阅读本学习指南的过程中会见到许多反复出现的元素。下面将介绍其中的部分元素：

考试要点　考试要点突出了可能以某种形式出现在考试中的主题。虽然我们显然无从确切知道某次考试将包括哪些内容，但这个元素将强化对于掌握 CBK 特定方面知识及 CISSP 考试规范至关重要的概念。

复习题　每章都设有复习题，旨在衡量你对该章所述关键理念的掌握程度。你应该在读完每章内容后把这些题做一遍；如果你答错了一些题，说明你需要耗费更长时间来钻研相关主题。本书附录 B 给出复习题的答案。

书面实验　每章都设有书面实验，用以综述该章出现的各种概念和主题。书面实验提出的问题旨在帮助你把散布于该章各处的重要内容归纳到一起形成一个整体，使你能够提出或描述潜在安全战略或解决方案。

真实场景　在学习各章内容的过程中，你会发现对典型且真实可信的工作场景的描述，在这些情景下，你从该章学到的安全战略和方法可在解决问题或化解潜在困难的过程中发挥作用。这让你有机会了解如何把具体安全策略、指南或实践规范应用到实际工作中。

本章小结　这是对该章的简要回顾，归纳了该章涵盖的内容。

附加的学习工具

本书的读者可以得到一些附加的学习工具。我们努力提供一些必要工具，帮助你完成认证考试。请在准备考试时把下列所有工具都载入你的工作站。

注意：

访问 www.wiley.com/go/cissptestprep 可得到下面介绍的工具。

Sybex 备考软件

Sybex 专家开发的备考软件可帮助你为 CISSP 考试作好充分准备。你会在这个测验引擎中找到本书包含的所有复习题和评估题。你可进行评估测验，逐章检验自己的复习进展，也可选用练习考试或选用涵盖了所有方面问题的随机生成的考试。

电子速记卡

Sybex 开发的电子速记卡包含数百道考题，旨在进一步挑战你参加 CISSP 考试的能力。从复习题、练习考试和速记卡中，你总能找到足够的练习来应对考试！

PDF 格式词汇表

Sybex 提供了一个 PDF 格式的强大词汇表。这个可搜索的全面词汇表包含了你应该掌握的所有关键词语。

附加练习考试

Sybex 包含附加练习考试，每个考试的考题设置旨在了解你对 CISSP CBK 的关键元素掌握了多少。本书有 6 个附加练习考试，每个考试含 150 道考题，以与真实考试最长的时间长度匹配。访问 http://www.wiley.com/go/sybextestprep 便可得到这些考试。

如何使用本书的学习工具

本书设计的许多特性旨在辅导你准备 CISSP 认证考试。本书在每一章的开头列出该章涵盖的 CISSP 通用知识体系域主题，同时确保该章对每个主题进行充分论述，以此对你提供帮助。每章末尾的复习题和练习考试是为了检验你对学过的内容记住了多少，确保你清楚自己还需要在哪些方面多加努力。以下是使用本书和学习工具的几点建议(详见 www.wiley.com/go/cissptestprep)：

- 开始阅读本书之前先进行一次评估测验。这会让你了解哪些方面需要自己投入更多学习时间，以及哪些方面只需要简单复习一下即可。
- 读完每一章后回答复习题；每当你的答案有误时，都应回到该章重读相关主题，若还需要更多信息，则可从其他资源找出相关内容深入学习。
- 把速记卡下载到你的移动设备上，白天有空闲时间时就看几分钟。
- 抓住每个机会测试自己。除了评估测验和复习题以外，附带的学习工具还有附加练习考试。在不参考相关章节的情况下进行这些考试，看看自己做到什么程度，然后回头复习与丢分相关的主题，直到你完全掌握所有内容并能灵活应用这些概念为止。

最后，如果可能，找一个伙伴。有个人陪伴你一起复习备考，当你遇到有困难的主题时伸手帮你一把，这会使整个过程变得轻松愉快。你还可在伙伴的薄弱环节帮助他，以此来巩固自己学过的知识。

评估测验

1. 以下哪类访问控制寻求发现不良、未经授权、非法行为的证据？
   A. 预防
   B. 威慑
   C. 检测
   D. 纠正

2. 定义和详述口令挑选过程中可把良好口令选择与最终属于糟糕的口令选择区分开来的方面。

A. 难猜或无法预料
B. 符合最低长度要求
C. 符合特定复杂性要求
D. 以上所有

3. 以下哪一项最有可能检测出 DoS 攻击？

A. 基于主机的 IDS
B. 基于网络的 IDS
C. 漏洞扫描器
D. 渗透测试

4. 以下哪一项属于 DoS 攻击？

A. 在电话上假扮一名技术经理，要求接听者更改他们的口令
B. 上网向一台 Web 服务器发送一条畸形 URL，造成系统占用百分之百 CPU
C. 复制从某一特定子网流过的数据包，以此窃听通信流
D. 出于骚扰目的向没有提出请求的接收者发送消息包

5. 路由器在 OSI 模型的哪一层运行？

A. 网络层
B. 第 1 层
C. 传输层
D. 第 5 层

6. 哪种防火墙可以根据当前会话的通信流内容自动调整过滤规则？

A. 静态数据包过滤
B. 应用级网关
C. 电路级网关
D. 动态数据包过滤

7. VPN 可在以下哪种连接上建立？

A. 无线 LAN 连接
B. 远程访问拨号连接
C. WAN 链接
D. 以上所有

8. 哪种恶意软件利用社会工程伎俩诱骗受害者安装？

A. 病毒
B. 蠕虫
C. 木马
D. 逻辑炸弹

9. 构成 CIA 三部曲的是哪些元素？

A. 邻接、互操作、安全有序
B. 身份验证、授权和问责制

C. 胜任、可用、一体化
D. 可用性、保密性、完整性

10. 以下哪一项不是支持问责制所有要求的成分？
A. 审计
B. 隐私
C. 身份验证
D. 授权

11. 以下哪一项不属于防范串通的措施？
A. 职责分离
B. 受限岗位责任
C. 组用户账户
D. 岗位轮换

12. 数据托管员在_____为资源分配安全标签后负责确保资源安全。
A. 高管
B. 数据所有者
C. 审计员
D. 安全人员

13. 软件能力成熟度模型(SW-CMM)在哪个阶段用量化测量获得对软件开发过程的详细了解？
A. 可重复级
B. 定义级
C. 管理级
D. 优化级

14. 环保护方案通常不在以下哪一层实际执行？
A. 第 0 层
B. 第 1 层
C. 第 3 层
D. 第 4 层

15. TCP/IP 三次握手序列的最后阶段是什么？
A. SYN 包
B. ACK 包
C. NAK 包
D. SYN/ACK 包

16. 参数检查是解决以下哪种漏洞的最佳方式？
A. 对使用时间的时间检查
B. 缓冲区溢出
C. SYN 洪水
D. 分布式拒绝服务

17. 以下哪一项是下面所示逻辑运算的值？

```
X:          0 1 1 0 1 0
Y:          0 0 1 1 0 1
----------------------
X ∨ Y:      ?
```

A. 011111
B. 011010
C. 001000
D. 001101

18. 在哪类密码中，明文消息的字母被重新排列而形成密文？
A. 替换密码
B. 块密码
C. 移位密码
D. 单次密本

19. 以下哪一项是 MD5 算法生成的消息摘要的长度？
A. 64 位
B. 128 位
C. 256 位
D. 384 位

20. 如果 Renee 收到 Mike 发来的一条有数字签名的消息，她用哪个密钥来验证消息确实发自 Mike？
A. Renee 的公钥
B. Renee 的私钥
C. Mike 的公钥
D. Mike 的私钥

21. 以下哪一项不涉及安全模型的构成原理？
A. 级联
B. 反馈
C. 迭代
D. 连接

22. TCB 中共同执行引用监测功能的组件集是什么？
A. 安全边界
B. 安全内核
C. 访问矩阵
D. 受限界面

23. 以下哪个陈述是正确的？
A. 系统越不复杂，漏洞越多
B. 系统越复杂，提供的保障越少
C. 系统越简单，可信度越低
D. 系统越复杂，所形成的受攻击面越小

24. 从被称为保护环的设计架构安全机制的角度看，0 环还指以下四项中除哪一项外的其他三项？

A. 特权模式
B. 监管模式
C. 系统模式
D. 用户模式

25. 审计踪迹、日志、闭路电视监控系统(CCTV)、入侵检测系统、杀毒软件、渗透测试、口令破解器、性能监控和循环冗余校验(CRC)是以下哪一项的例子？

A. 指示控制
B. 预防控制
C. 检测控制
D. 纠正控制

26. 系统架构、系统完整性、隐蔽通道分析、可信设施管理和可信恢复是什么安全准则的元素？

A. 质量保障
B. 运行保障
C. 生命周期保障
D. 数量保障

27. 以下哪一项是专为测试并或许绕过系统安全控制而设计的一种规程？

A. 日志使用数据
B. 战争拨号
C. 渗透测试
D. 部署受保护台式机工作站

28. 审计是用来保持和执行什么的因素？

A. 问责制
B. 保密性
C. 可访问性
D. 冗余

29. 以下哪一项是用来计算 ALE 的公式？

A. ALE = AV * EF * ARO
B. ALE = ARO * EF
C. ALE = AV * ARO
D. ALE = EF * ARO

30. 以下哪一项是业务影响评估流程的第一步？

A. 确定优先级
B. 可能性评估
C. 风险识别
D. 资源优先级排序

31. 以下哪一项代表了可能会对组织构成威胁或风险的自然事件？
A. 地震
B. 洪水
C. 龙卷风
D. 以上所有
32. 哪种恢复设施可使组织在主设施发生事故后尽快恢复运行？
A. 热站点
B. 温站点
C. 冷站点
D. 以上所有
33. 以下哪种形式的知识产权可用来保护文字、口号和徽标？
A. 专利
B. 版权
C. 商标
D. 商业机密
34. 以下哪类证据是指可拿到法庭上证明某个事实的书面文件？
A. 最佳证据
B. 工资表证据
C. 文档证据
D. 言辞证据
35. 军事和情报攻击为什么被列在最严重计算机罪行之中？
A. 落入敌人之手的信息一旦被利用，有可能对国家利益产生深远的不利战略影响。
B. 军事信息保存在安全的机器里，一旦被成功攻击，会令人颜面尽失。
C. 机密信息被人长期用于政治目的，会影响一个国家的领导地位。
D. 军事和情报机构已确保保护他们的信息的法律是最严厉的法律。
36. 哪类被检测出来的事件可为调查提供最长时间？
A. 破坏
B. 拒绝服务
C. 恶意代码
D. 扫描
37. 如果你想限制一个设施的进出，你会选用以下哪一项？
A. 大门
B. 旋转门
C. 围栏
D. 捕人陷阱
38. 二级验证系统的意义是什么？
A. 验证用户的身份
B. 验证用户的活动
C. 验证系统的完整性
D. 验证系统的正确性

39. 当有大量不请自来的消息被发送给受害者时，就发生了垃圾邮件攻击。由于发送给受害者的数据多得足以阻止正常活动，这种攻击又叫什么？

A. 嗅探

B. 拒绝服务

C. 蛮力攻击

D. 缓冲区溢出攻击

40. 哪类入侵检测系统(IDS)可视为一种专家系统？

A. 基于主机的 IDS

B. 基于网络的 IDS

C. 基于知识的 IDS

D. 基于行为的 IDS

评估测验答案

1. C。检测访问控制用于发现(并记录)不良或未经授权活动。

2. D。强口令选择难猜、不可预料和且符合规定的最低长度要求，以确保口令条目不可能被自动确定。口令可随机生成，使用所有字母、数字和标点符号字符；它们绝不应被写下来或与人共享；它们不应保存在可公开访问或通常可读的位置；它们还不应被明文传送。

3. B。基于网络的 IDS 通常能检测攻击的发起或实施攻击的持续尝试(包括拒绝服务，即 DoS)。但它们不能提供信息说明攻击是否得逞或哪些具体系统、用户账号、文件或应用程序受到影响。基于主机的 IDS 在检测和跟踪 DoS 攻击方面有些困难。漏洞扫描器不检测 DoS 攻击，它们测试可能存在的漏洞。渗透测试可能会造成 DoS 攻击或用于测试 DoS 漏洞，但它不属于检测工具。

4. B。并非 DoS 攻击的所有情况都是恶意动机的结果。在编写操作系统、服务和应用程序时出现的错误也曾导致出现 DoS 情况。这方面的例子包括一个进程未能释放对 CPU 的控制，或一项服务对系统资源的消耗与该服务正在处理的服务请求不成比例。社会工程和嗅探通常不属于 DoS 攻击。

5. A。网络硬件设备(包括路由器)在第 3 层(即网络层)运行。

6. D。动态包过滤服务器可根据通信流内容，实时修改过滤规则。

7. D。VPN 链接可在任何其他网络通信连接上建立。它们可能是典型的 LAN 电缆连接、无线 LAN 连接、远程访问拨号连接、WAN 连接，甚至可能是客户端为访问办公室 LAN 而使用的互联网连接。

8. C。木马是恶意软件的一种形式，借助社会工程伎俩诱使受害者安装——所用伎俩是使受害者相信，他们下载或得到的只是一个主机文件，而实际上，却是一个隐藏的恶意载荷。

9. D。CIA 三部曲的成分是保密性、可用性和完整性。

10. B。隐私不必支持问责制。

11. C。组用户账户允许多人以一个用户账户登录。由于它阻碍问责，因此使串通得以实现。

12. B。数据所有者在数据托管员可对资源实施适当保护之前，必须先给资源分配一个安全标签。

13. C。SW-CMM 的“管理级”阶段涉及使用量化开发测量指标。SEI 把这一层涉及关键流程的方面定义为量化流程管理和软件质量管理。

14. B。第 1 层和第 2 层含设备驱动，但通常不实际执行。第 0 层始终含安全内核。第 3 层含用户应用程序。第 4 层不存在。

15. B。SYN 包首先从发起主机发送给目的主机。目的主机随后用一个 SYN/ACK 包回应。发起主机这时发送一个 ACK 包，连接由此建立。

16. B。参数检查用于预防出现缓冲区溢出攻击的可能性。

17. A。~ OR 符号表示 OR 函数，当一个或两个输入位为真时为真。

18. C。移位密码通过一种加密算法重新排列明文消息的字母，形成密文消息。

19. B。MD5 算法可为任何输入生成 128 位消息摘要。

20. C。任何接收者都能用 Mike 的公钥验证数字签名的真实性。

21. C。迭代不属涉及安全模型的构成原理。级联、反馈和连接是三大构成原理。

22. B。TCB 中共同执行参考监测功能的组件集叫安全内核。

23. B。系统越复杂，提供的保障越低。更复杂意味着更多方面存在漏洞，更多方面必须在保护下抵御威胁。更多的漏洞和威胁意味着系统随之提供的安全保护可靠性较低。

24. D。0 环可直接访问大多数资源；因此，用户模式并不是合适的标签，因为用户模式要求通过限制条件来制约对资源的访问。

25. C。检测控制的例子包括审计踪迹、日志、CCTV、入侵检测系统、杀毒软件、渗透测试、口令破解器、性能监控和循环冗余校验(CRC)。

26. B。保障是指你在满足计算机、网络、解决方案等的安全需要时所能给予的可信程度。运行保障侧重于可帮助支持安全性的系统基本性能和架构。

27. C。渗透测试尝试绕过安全控制以检测系统的总体安全性。

28. A。审计是用来保持和执行问责制的因素。

29. A。年度损失期望(ALE)是资产价值(AV)乘以暴露因子(EF)后再乘以年度发生率(ARO)的积。这是公式 ALE = SLE * ARO 的加长形式。这里显示的其他公式不能准确反映这一计算。

30. A。确定优先级是业务影响评估流程的第一步。

31. D。会对组织构成威胁的自然事件包括地震、洪水、飓风、龙卷风、火灾以及其他自然灾害。因此，选项 A、B、C 都正确，因为它们是自然发生而非人为的。

32. A。热站点提供的备份设施始终保持一种工作状态，完全可接管业务运行。温站点为业务运行预先配置好了硬件和软件，但这些硬件和软件不含关键业务信息。冷站点是配备了电力和环境支持系统的简单设施，但不含经过配置的硬件、软件或服务。灾难恢复服务可代表一家公司推进并运行这些站点。

33. C。商标可用来保护代表一家公司及其产品或服务的文字、口号和徽标。

34. C。拿到法庭上证明某一案件的事实性的书面文件叫作文档证据。

35. A。军事和情报攻击的目的是获取机密信息。这些信息落入敌人之手一旦被利用，会造成近乎无限的不利影响。这类攻击由极其老练的攻击者发起，往往很难查明哪些文件被成功攫取。所以当这种破坏事件发生时，你经常无法搞清损失到底有多大。

36. D。扫描事件往往是侦察性攻击。而对系统真正造成损害的是后续攻击，因此，如果你早期检测出扫描攻击，你可能会有一些时间来作出反应。

37. B。旋转门是一种大门，可防止多人同时进入，并且往往把行进限制在一个方向上。它用于让人只进不出，或只出不进。

38. D。建立二级验证机制是为了形成验证检测系统和传感器正确性的手段。这往往意味着把多种类型传感器或系统(CCTV、热和运动传感器等)组合到一起，共同勾勒被测出事件的更完整图像。

39. B。垃圾邮件攻击(发送大量不请自来的电子邮件)可当作一种拒绝服务攻击手段使用。它不借助窃听方法，因此不属于嗅探。蛮力攻击旨在破解口令。缓冲区溢出攻击向系统发送数据串，旨在造成系统瘫痪。

40. D。基于行为的 IDS 可贴上专家系统或伪人工智能系统的标签，因为它能够学习并对事件作出假设。换句话说，这种 IDS 可像人类专家那样对照已知事件评估当前事件。基于知识的 IDS 通过“已知攻击方法”数据库来检测攻击。基于主机和基于网络的 IDS 可基于知识或行为，也可同时基于知识和行为。

目　录

第 1 章　实现安全治理的原则和策略……1
1.1　理解和应用保密性、完整性及可用性的概念……1
1.1.1　保密性……2
1.1.2　完整性……3
1.1.3　可用性……4
1.1.4　其他安全概念……6
1.1.5　保护机制……8
1.1.6　分层……9
1.1.7　抽象……9
1.1.8　数据隐藏……9
1.1.9　加密……10
1.2　评估和应用安全治理原则……10
1.2.1　与业务战略、目标、使命和宗旨相一致的安全功能……10
1.2.2　组织的流程……12
1.2.3　组织的角色与责任……16
1.2.4　安全控制框架……17
1.2.5　应尽关心和尽职审查……18
1.3　开发、记录和实施安全策略、标准、程序和指南……18
1.3.1　安全策略……18
1.3.2　标准、基线和指南……19
1.3.3　程序……20
1.4　理解与应用威胁建模的概念和方法……21
1.4.1　识别威胁……22
1.4.2　确定和绘制潜在的攻击……25
1.4.3　执行简化分析……26
1.4.4　优先级排序和响应……26
1.5　将基于风险的管理理念应用到供应链……27
1.6　本章小结……28
1.7　考试要点……29
1.8　书面实验……31
1.9　复习题……31

第 2 章　人员安全和风险管理的概念……35
2.1　人员安全策略和程序……36
2.1.1　候选人筛选及招聘……38
2.1.2　雇佣协议及策略……38
2.1.3　入职和离职程序……39
2.1.4　供应商、顾问和承包商的协议和控制……41
2.1.5　合规策略要求……42
2.1.6　隐私策略要求……42
2.2　安全治理……43
2.3　理解并应用风险管理理念……44
2.3.1　风险术语……45
2.3.2　识别威胁和脆弱性……46
2.3.3　风险评估/分析……47
2.3.4　风险响应……53
2.3.5　选择与实施控制措施……54
2.3.6　适用的控制类型……56
2.3.7　安全控制评估……57
2.3.8　监视和测量……57
2.3.9　资产估值与报告……57
2.3.10　持续改进……58
2.3.11　风险框架……59
2.4　建立和维护安全意识、教育和培训计划……60
2.5　管理安全功能……61
2.6　本章小结……62
2.7　考试要点……62
2.8　书面实验……64
2.9　复习题……64

第 3 章　业务连续性计划……68
3.1　业务连续性计划简介……68

3.2 项目范围和计划……69
3.2.1 业务组织分析……69
3.2.2 选择 BCP 团队……70
3.2.3 资源需求……71
3.2.4 法律和法规要求……72
3.3 业务影响评估……73
3.3.1 确定优先级……74
3.3.2 风险识别……74
3.3.3 可能性评估……75
3.3.4 影响评估……76
3.3.5 资源优先级排序……77
3.4 连续性计划……77
3.4.1 策略开发……77
3.4.2 预备和处理……78
3.5 计划批准和实施……79
3.5.1 计划批准……79
3.5.2 计划实施……79
3.5.3 培训和教育……80
3.5.4 BCP 文档化……80
3.6 本章小结……83
3.7 考试要点……83
3.8 书面实验……84
3.9 复习题……84

第 4 章 法律、法规和合规……88
4.1 法律的分类……88
4.1.1 刑法……89
4.1.2 民法……90
4.1.3 行政法……90
4.2 法律……90
4.2.1 计算机犯罪……91
4.2.2 知识产权……94
4.2.3 许可……97
4.2.4 进口/出口控制……98
4.2.5 隐私……98
4.3 合规……104
4.4 合同和采购……105
4.5 本章小结……105
4.6 考试要点……106
4.7 书面实验……106
4.8 复习题……107

第 5 章 保护资产安全……110
5.1 资产识别和分类……110
5.1.1 定义敏感数据……111
5.1.2 定义数据分类……112
5.1.3 定义资产分类……114
5.1.4 确定数据的安全控制……114
5.1.5 理解数据状态……115
5.1.6 管理信息和资产……116
5.1.7 数据保护方法……121
5.2 定义数据所有权……123
5.2.1 数据所有者……123
5.2.2 资产所有者……124
5.2.3 业务/任务所有者……124
5.2.4 数据使用者……125
5.2.5 管理员……127
5.2.6 托管员……127
5.2.7 用户……128
5.2.8 保护隐私……128
5.3 使用安全基线……128
5.3.1 范围界定和按需定制……129
5.3.2 选择标准……129
5.4 本章小结……130
5.5 考试要点……130
5.6 书面实验……131
5.7 复习题……131

第 6 章 密码学和对称密钥算法……135
6.1 密码学的历史里程碑……135
6.1.1 凯撒密码……136
6.1.2 美国南北战争……136
6.1.3 Ultra 与 Enigma……137
6.2 密码学基本知识……137
6.2.1 密码学的目标……137
6.2.2 密码学的概念……139
6.2.3 密码数学……140
6.2.4 密码……144
6.3 现代密码学……149
6.3.1 密码密钥……149
6.3.2 对称密钥算法……150

6.3.3 非对称密钥算法……151
6.3.4 散列算法……153
6.4 对称密码……154
6.4.1 数据加密标准……154
6.4.2 三重 DES……155
6.4.3 国际数据加密算法……156
6.4.4 Blowfish……157
6.4.5 Skipjack……157
6.4.6 高级加密标准……157
6.4.7 对称密钥管理……158
6.5 密码生命周期……160
6.6 本章小结……160
6.7 考试要点……161
6.8 书面实验……162
6.9 复习题……162

第 7 章 PKI 和密码应用……166
7.1 非对称密码……166
7.1.1 公钥和私钥……167
7.1.2 RSA……167
7.1.3 El Gamal……169
7.1.4 椭圆曲线……169
7.2 散列函数……170
7.2.1 SHA……171
7.2.2 MD2……171
7.2.3 MD4……171
7.2.4 MD5……172
7.3 数字签名……172
7.3.1 HMAC……173
7.3.2 数字签名标准……174
7.4 公钥基础设施……174
7.4.1 证书……174
7.4.2 发证机构……175
7.4.3 证书的生成和销毁……176
7.5 非对称密钥管理……177
7.6 应用密码学……178
7.6.1 便携设备……178
7.6.2 电子邮件……179
7.6.3 Web 应用程序……180
7.6.4 数字版权管理……182
7.6.5 联网……185
7.7 密码攻击……187
7.8 本章小结……189
7.9 考试要点……190
7.10 书面实验……191
7.11 复习题……191

第 8 章 安全模型、设计和能力的原则……195
8.1 使用安全设计原则实施和管理工程过程……195
8.1.1 客体和主体……196
8.1.2 封闭系统和开放系统……196
8.1.3 用于确保保密性、完整性和可用性的技术……197
8.1.4 控制……198
8.1.5 信任与保证……198
8.2 理解安全模型的基本概念……199
8.2.1 可信计算基……200
8.2.2 状态机模型……201
8.2.3 信息流模型……201
8.2.4 非干扰模型……202
8.2.5 Take-Grant 模型……202
8.2.6 访问控制矩阵……203
8.2.7 Bell-LaPadula 模型……204
8.2.8 Biba 模型……206
8.2.9 Clark-Wilson 模型……207
8.2.10 Brewer and Nash 模型……208
8.2.11 Goguen-Meseguer 模型……208
8.2.12 Sutherland 模型……209
8.2.13 Graham-Denning 模型……209
8.3 基于系统安全需求选择控制措施……209
8.3.1 彩虹系列……210
8.3.2 TCSEC 分类和所需功能……211
8.3.3 通用准则……214
8.3.4 行业和国际安全实施指南……217
8.3.5 认证和鉴定……217
8.4 理解信息系统的安全功能……219
8.4.1 内存保护……219
8.4.2 虚拟化……220

8.4.3 可信平台模块……220
8.4.4 接口……220
8.4.5 容错……221
8.5 本章小结……221
8.6 考试要点……221
8.7 书面实验……222
8.8 复习题……222

第 9 章 安全漏洞、威胁和对策……226
9.1 评估和缓解安全漏洞……227
9.1.1 硬件……227
9.1.2 固件……241
9.2 基于客户端的系统……242
9.2.1 applet……242
9.2.2 本地缓存……244
9.3 基于服务端的系统……245
9.4 数据库系统安全……246
9.4.1 聚合……246
9.4.2 推理……246
9.4.3 数据挖掘和数据仓库……247
9.4.4 数据分析……247
9.4.5 大规模并行数据系统……248
9.5 分布式系统和端点安全……248
9.5.1 基于云的系统和云计算……250
9.5.2 网格计算……253
9.5.3 对等网络……253
9.6 物联网……254
9.7 工业控制系统……255
9.8 评估和缓解基于 Web 系统的漏洞……255
9.9 评估和缓解移动系统的漏洞……259
9.9.1 设备安全……260
9.9.2 应用安全……263
9.9.3 BYOD 关注点……264
9.10 评估和缓解嵌入式设备和信息物理系统的漏洞……267
9.10.1 嵌入式系统和静态系统的示例……267
9.10.2 保护嵌入式和静态系统的方法……268
9.11 基本安全保护机制……270
9.11.1 技术机制……270
9.11.2 安全策略和计算机架构……272
9.11.3 策略机制……273
9.12 常见的架构缺陷和安全问题……273
9.12.1 隐蔽通道……274
9.12.2 基于设计或编码缺陷的攻击和安全问题……274
9.12.3 编程……276
9.12.4 计时、状态改变和通信中断……277
9.12.5 技术和过程集成……277
9.12.6 电磁辐射……277
9.13 本章小结……278
9.14 考试要点……278
9.15 书面实验……280
9.16 复习题……281

第 10 章 物理安全要求……284
10.1 站点与设施设计的安全原则……285
10.1.1 安全设施计划……285
10.1.2 站点选择……285
10.1.3 可见度……286
10.1.4 自然灾害……286
10.1.5 设施设计……286
10.2 实现站点与设施安全控制……287
10.2.1 设备故障……288
10.2.2 配线间……288
10.2.3 服务器间与数据中心……290
10.2.4 介质存储设施……293
10.2.5 证据存储……293
10.2.6 受限区与工作区安全……294
10.2.7 基础设施与 HVAC……295
10.2.8 火灾预防、探测与消防……297
10.3 物理安全的实现与管理……300
10.3.1 边界安全控制……300
10.3.2 内部安全控制……303
10.4 本章小结……306
10.5 考试要点……307
10.6 书面实验……309
10.7 复习题……309

第 11 章　安全网络架构和保护网络组件……312
11.1　OSI 模型……312
11.1.1　OSI 模型的历史……313
11.1.2　OSI 功能……313
11.1.3　封装/解封……314
11.1.4　OSI 模型层次……315
11.2　TCP/IP 模型……321
11.3　融合协议……334
11.4　无线网络……336
11.4.1　保护无线接入点……336
11.4.2　保护 SSID……338
11.4.3　进行现场调查……338
11.4.4　使用安全加密协议……339
11.4.5　天线放置……341
11.4.6　天线类型……342
11.4.7　调整功率电平控制……342
11.4.8　WPS……342
11.4.9　使用强制门户……343
11.4.10　一般 Wi-Fi 安全程序……343
11.4.11　无线攻击……344
11.5　安全网络组件……346
11.5.1　网络访问控制……347
11.5.2　防火墙……347
11.5.3　端点安全……350
11.5.4　硬件的安全操作……351
11.6　布线、无线、拓扑、通信和传输介质技术……353
11.6.1　传输介质……354
11.6.2　网络拓扑……357
11.6.3　无线通信与安全……359
11.6.4　局域网技术……363
11.7　本章小结……366
11.8　考试要点……367
11.9　书面实验……369
11.10　复习题……369

第 12 章　安全通信与网络攻击……373
12.1　网络与协议安全机制……373
12.1.1　安全通信协议……374
12.1.2　身份验证协议……374
12.2　语音通信的安全……375
12.2.1　VoIP……375
12.2.2　社会工程……376
12.2.3　欺骗与滥用……377
12.3　多媒体合作……378
12.3.1　远程会议……379
12.3.2　即时通信……379
12.4　管理邮件安全……379
12.4.1　邮件安全目标……380
12.4.2　理解邮件安全问题……381
12.4.3　邮件安全解决方案……381
12.5　远程访问安全管理……383
12.5.1　远程访问安全计划……385
12.5.2　拨号上网协议……386
12.5.3　中心化远程身份验证服务……386
12.6　虚拟专用网……387
12.6.1　隧道技术……387
12.6.2　VPN 的工作机理……388
12.6.3　常用的 VPN 协议……388
12.6.4　虚拟局域网……390
12.7　虚拟化……391
12.7.1　虚拟软件……391
12.7.2　虚拟化网络……392
12.8　网络地址转换……392
12.8.1　私有 IP 地址……393
12.8.2　有状态 NAT……394
12.8.3　静态与动态 NAT……395
12.8.4　自动私有 IP 分配……395
12.9　交换技术……396
12.9.1　电路交换……396
12.9.2　分组交换……397
12.9.3　虚电路……397
12.10　WAN 技术……398
12.10.1　WAN 连接技术……399
12.10.2　拨号封装协议……401
12.11　多种安全控制特征……401
12.11.1　透明性……402
12.11.2　验证完整性……402
12.11.3　传输机制……402
12.12　安全边界……403

12.13 防止或减轻网络攻击……403
12.13.1 DoS 与 DDoS……404
12.13.2 窃听……404
12.13.3 假冒/伪装……405
12.13.4 重放攻击……405
12.13.5 修改攻击……406
12.13.6 地址解析协议欺骗……406
12.13.7 DNS 毒化、欺骗及劫持……406
12.13.8 超链接欺骗……407
12.14 本章小结……407
12.15 考试要点……409
12.16 书面实验……410
12.17 复习题……410

第 13 章 管理身份和身份验证……414
13.1 控制对资产的访问……414
13.1.1 比较主体和客体……415
13.1.2 CIA 三性和访问控制……416
13.1.3 访问控制的类型……416
13.2 比较身份识别和身份验证……418
13.2.1 身份注册和证明……418
13.2.2 授权和问责……419
13.2.3 身份验证因素……420
13.2.4 密码……421
13.2.5 智能卡和令牌……423
13.2.6 生物识别技术……425
13.2.7 多因素身份验证……428
13.2.8 设备验证……429
13.2.9 服务身份验证……429
13.3 实施身份管理……430
13.3.1 单点登录……430
13.3.2 凭据管理系统……434
13.3.3 集成身份服务……434
13.3.4 管理会话……435
13.3.5 AAA 协议……435
13.4 管理身份和访问配置生命周期…437
13.4.1 访问配置……437
13.4.2 账户审核……438
13.4.3 账户撤消……439
13.5 本章小结……439
13.6 考试要点……440
13.7 书面实验……441
13.8 复习题……441

第 14 章 控制和监控访问……445
14.1 比较访问控制模型……445
14.1.1 比较权限、权利和特权……445
14.1.2 理解授权机制……446
14.1.3 使用安全策略定义需求……447
14.1.4 实施纵深防御……447
14.1.5 总结访问控制模型……448
14.1.6 自主访问控制……449
14.1.7 非自主访问控制……449
14.2 了解访问控制攻击……454
14.2.1 风险要素……454
14.2.2 识别资产……455
14.2.3 识别威胁……456
14.2.4 识别漏洞……457
14.2.5 常见的访问控制攻击……457
14.2.6 保护方法综述……465
14.3 本章小结……467
14.4 考试要点……467
14.5 书面实验……468
14.6 复习题……468

第 15 章 安全评估与测试……472
15.1 构建安全评估和测试方案……473
15.1.1 安全测试……473
15.1.2 安全评估……474
15.1.3 安全审计……474
15.2 开展漏洞评估……476
15.2.1 漏洞描述……477
15.2.2 漏洞扫描……477
15.2.3 渗透测试……484
15.3 测试软件……486
15.3.1 代码审查与测试……486
15.3.2 接口测试……489
15.3.3 误用例测试……489
15.3.4 测试覆盖率分析……490
15.3.5 网站监测……490

15.4 实施安全管理流程……491
15.4.1 日志审查……491
15.4.2 账户管理……491
15.4.3 备份验证……492
15.4.4 关键绩效和风险指标……492
15.5 本章小结……492
15.6 考试要点……493
15.7 书面实验……494
15.8 复习题……494

第 16 章 安全运营管理……498
16.1 应用安全运营概念……498
16.1.1 知其所需和最小特权……499
16.1.2 职责分离……500
16.1.3 岗位轮换……502
16.1.4 强制休假……503
16.1.5 特权账户管理……503
16.1.6 管理信息生命周期……504
16.1.7 服务水平协议……505
16.1.8 关注人员安全……506
16.2 安全配置资源……507
16.2.1 管理硬件和软件资产……507
16.2.2 保护物理资产……508
16.2.3 管理虚拟资产……509
16.2.4 管理云资产……509
16.2.5 介质管理……510
16.3 配置管理……513
16.3.1 基线……513
16.3.2 使用镜像技术创建基线……513
16.4 变更管理……514
16.4.1 安全影响分析……516
16.4.2 版本控制……516
16.4.3 配置文档……517
16.5 补丁管理和漏洞减少……517
16.5.1 系统管理……517
16.5.2 补丁管理……518
16.5.3 漏洞管理……519
16.5.4 常见的漏洞和风险……520
16.6 本章小结……521
16.7 考试要点……521
16.8 书面实验……522
16.9 复习题……523

第 17 章 事件的预防和响应……526
17.1 事件响应管理……527
17.1.1 事件的定义……527
17.1.2 事件响应步骤……527
17.2 落实检测和预防措施……532
17.2.1 基本预防措施……532
17.2.2 了解攻击……533
17.2.3 入侵检测和预防系统……540
17.2.4 具体预防措施……545
17.3 日志记录、监测和审计……553
17.3.1 日志记录和监测……553
17.3.2 出口监测……559
17.3.3 效果评价审计……561
17.3.4 安全审计和审查……564
17.3.5 报告审计结果……564
17.4 本章小结……566
17.5 考试要点……567
17.6 书面实验……569
17.7 复习题……570

第 18 章 灾难恢复计划……573
18.1 灾难的本质……574
18.1.1 自然灾难……574
18.1.2 人为灾难……577
18.2 理解系统恢复和容错能力……580
18.2.1 保护硬盘驱动器……581
18.2.2 保护服务器……582
18.2.3 保护电源……583
18.2.4 受信恢复……583
18.2.5 服务质量……584
18.3 恢复策略……585
18.3.1 确定业务单元的优先顺序……585
18.3.2 危机管理……586
18.3.3 应急通信……586
18.3.4 工作组恢复……586
18.3.5 可替代的工作站点……587
18.3.6 相互援助协议……590
18.3.7 数据库恢复……590

18.4 恢复计划开发……592
18.4.1 紧急事件响应……592
18.4.2 人员通知……593
18.4.3 评估……593
18.4.4 备份和离站存储……593
18.4.5 软件托管协议……596
18.4.6 外部通信……597
18.4.7 公用设施……597
18.4.8 物流和供应……597
18.4.9 恢复与还原的比较……597
18.5 培训、意识与文档记录……598
18.6 测试与维护……599
18.6.1 通读测试……599
18.6.2 结构化演练……599
18.6.3 模拟测试……599
18.6.4 并行测试……599
18.6.5 完全中断测试……599
18.6.6 维护……600
18.7 本章小结……600
18.8 考试要点……600
18.9 书面实验……601
18.10 复习题……601

第 19 章 调查和道德……605
19.1 调查……605
19.1.1 调查的类型……606
19.1.2 证据……607
19.1.3 调查过程……610
19.2 计算机犯罪的主要类别……613
19.2.1 军事和情报攻击……613
19.2.2 商业攻击……614
19.2.3 财务攻击……614
19.2.4 恐怖攻击……614
19.2.5 恶意攻击……615
19.2.6 兴奋攻击……616
19.3 道德规范……616
19.3.1 (ISC)² 的道德规范……616
19.3.2 道德规范和互联网……617
19.4 本章小结……618
19.5 考试要点……618
19.6 书面实验……619
19.7 复习题……619

第 20 章 软件开发安全……623
20.1 系统开发控制概述……623
20.1.1 软件开发……624
20.1.2 系统开发生命周期……628
20.1.3 生命周期模型……630
20.1.4 甘特图与 PERT……635
20.1.5 变更和配置管理……635
20.1.6 DevOps 方法……636
20.1.7 应用编程接口……637
20.1.8 软件测试……638
20.1.9 代码仓库……639
20.1.10 服务水平协议……639
20.1.11 软件采购……640
20.2 创建数据库和数据仓储……640
20.2.1 数据库管理系统的体系结构……641
20.2.2 数据库事务……643
20.2.3 多级数据库的安全性……644
20.2.4 ODBC……646
20.2.5 NoSQL……646
20.3 存储数据和信息……647
20.3.1 存储器的类型……647
20.3.2 存储器威胁……647
20.4 理解基于知识的系统……648
20.4.1 专家系统……648
20.4.2 机器学习……649
20.4.3 神经网络……649
20.4.4 安全性应用……649
20.5 本章小结……650
20.6 考试要点……650
20.7 书面实验……651
20.8 复习题……651

第 21 章 恶意代码和应用攻击……654
21.1 恶意代码……654
21.1.1 恶意代码的来源……654
21.1.2 病毒……655
21.1.3 逻辑炸弹……659
21.1.4 特洛伊木马……660

21.1.5　蠕虫……661
21.1.6　间谍软件与广告软件……662
21.1.7　零日(Zero-Day)攻击……663
21.2　密码攻击……663
21.2.1　密码猜测攻击……663
21.2.2　字典攻击……664
21.2.3　社会工程学……665
21.2.4　对策……666
21.3　应用程序攻击……666
21.3.1　缓冲区溢出……666
21.3.2　检验时间到使用时间……667
21.3.3　后门……667
21.3.4　权限提升和 rootkit……667
21.4　Web 应用的安全性……668
21.4.1　跨站脚本……668
21.4.2　跨站请求伪造……669
21.4.3　SQL 注入攻击……669
21.5　侦察攻击……671
21.5.1　IP 探测……672
21.5.2　端口扫描……672
21.5.3　漏洞扫描……672
21.6　伪装攻击……673
21.6.1　IP 欺骗……673
21.6.2　会话劫持……673
21.7　本章小结……673
21.8　考试要点……674
21.9　书面实验……674
21.10　复习题……675
附录 A　书面实验答案……678
附录 B　复习题答案……687

第 1 章

实现安全治理的原则和策略

本章涵盖的 CISSP 认证考试主题包括：

✓域 1：安全与风险管理

- 1.1 理解和应用保密性、完整性及可用性的概念
- 1.2 评估和应用安全治理原则
  - 1.2.1 与业务战略、目标、使命和宗旨相一致的安全功能
  - 1.2.2 组织的流程
  - 1.2.3 组织的角色与责任
  - 1.2.4 安全控制框架
  - 1.2.5 应尽关心和尽职审查
- 1.6 开发、记录和实施安全策略、标准、程序和指南
- 1.10 理解与应用威胁建模的概念和方法
  - 1.10.1 威胁建模的方法
  - 1.10.2 威胁建模的概念
- 1.11 将基于风险的管理理念应用到供应链
  - 1.11.1 与硬件、软件和服务相关的风险
  - 1.11.2 第三方评估与监测
  - 1.11.3 最低安全需求
  - 1.11.4 服务水平要求

CISSP 认证考试通用知识体系(CBK)的“安全与风险管理”域涉及安全解决方案中的许多基础性概念，包括设计、实现和管理安全机制需要了解的原理。“安全与风险管理”域的内容在第 1~4 章以及第 19 章中讨论，请务必阅读所有这些章节以全面认识“安全与风险管理”域的考试主题。

1.1 理解和应用保密性、完整性及可用性的概念

安全管理的概念与原则是实施安全策略和安全解决方案的核心内容。安全管理的概念与原则定义了安全环境中必需的基本参数，也定义了安全策略设计人员和系统实施人员为创建安全解决方案必须实现的目标。对于现实世界中的安全专业人员及 CISSP 考生来说，透彻理解这些内容是非常重要的。本章包含一系列对全球性大企业和小公司安全都适用的安全治理主题。

安全必须要有起点。通常这个起点是最重要的安全原则列表。在这个列表中，保密性、完整性和可用性(Confidentiality, Integrity and Availability，CIA)始终存在，因为它们经常被视为安全基础架构中主要的安全目标和宗旨。它们作为安全基础要素频频出现，以至于被简称为 CIA 三元组(见图 1.1)。

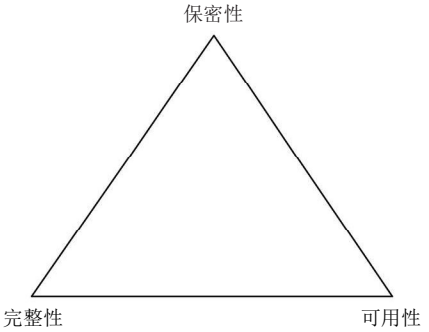

图 1.1　CIA 三元组

安全控制评估通常用来评价这三个核心信息安全原则的符合情况。总的来说，一个完整的安全解决方案应该充分满足这些原则。对脆弱性和风险的评估也基于它们对一个或多个 CIA 三元组原则的威胁。因此，有必要熟悉这些原则并将其作为判断所有安全相关事项的准则。

这三个信息安全原则被视为安全领域最重要的原则。每个原则对特定组织有多重要取决于该组织的安全目标和需求以及组织安全受到威胁的程度。

1.1.1　保密性

CIA 三元组的第一个原则是“保密性”。保密性指为保障数据、客体或资源保密状态而采取的措施。保密性保护的目标是阻止或最小化未经授权的数据访问。保密性关注的安全措施重点在于确保除预期收件人外的任何人都不会接收到或读取到信息。保密性保护为授权用户提供了访问资源以及与资源交互的方法，同时主动阻止未经授权的用户对资源的访问。许多安全控制措施可提供保密性保护，包括但不限于加密、访问控制和隐写术。

如果安全机制提供保密性，那它就对阻止未经授权的主体访问数据、客体或资源提供了高度保障。如果保密性受到威胁，就会出现未经授权的信息泄露。客体(object)是安全关系中的被动元素，如文件、计算机、网络连接和应用程序。主体(subject)是安全关系中的主动元素，如用户、程序和计算机。主体作用于客体或对抗客体。主体与客体之间的关系管理称为访问控制。

总的来说，要维护网络中的保密性，必须保护数据避免在存储、处理和传输过程中遭受未经授权的访问、使用或泄露。对于数据、资源和对象的每种状态，都需要独特的安全控制来保持保密性。

许多攻击都聚焦在违反保密性上。这些攻击包括抓包网络流量与窃取密码文件，以及社会工程、端口扫描、肩窥、窃听、嗅探、特权升级等。

违反保密性的行为不仅包括直接的故意攻击，也包括许多由人为错误、疏忽或不称职造成的未经授权的敏感或机密信息泄露。致使违反保密性的事件包括：未正确实现的加密传输，在传输数据前未对远程系统充分进行身份验证，开放的非安全访问点，访问恶意代码打开的后门，错误路由传真，文件遗留在打印机上，甚至在访问终端仍显示数据时走开。

违反保密性可能是因为最终用户或系统管理员的不当行为，也可能是因为安全策略中的疏漏或配置有误的安全控制。

许多控制措施有利于保障保密性以抵御潜在的威胁。这些控制措施包括加密、填充网络流量、严格的访问控制、严格的身份验证程序、数据分类和充分的人员培训。

保密性和完整性相互依赖。没有客体完整性(换句话说，没能力保证客体不受未经授权的修改)，就无法维持客体保密性。保密性的其他相关概念、条件和特征包括：

敏感性　敏感性指信息的特性，这种特性的数据一旦泄露会导致伤害或损失。维持敏感信息的保密性有助于预防伤害或损失。

判断力　判断力是一种操作者可影响或控制信息泄露，以将伤害或损失程度降至最低的决策行为。

关键性　信息的关键程度是其关键性的衡量标准，关键级别越高，越需要保持信息的保密性。高级别的关键性对一个组织的运营和功能必不可少。

隐藏　隐藏(Concealment)指藏匿或防止泄露的行为。通常，隐藏被看成一种掩盖、混淆和干扰注意力的手段。与隐藏相关的一个概念是通过晦涩获得安全，即试图通过隐藏、沉默或保密获得保护。虽然通过晦涩保持安全的有效性未得到公认，但有些情况下它仍然有价值。

保密　保密是指对某事保密或防止信息泄露的行为。

隐私　隐私指对个人身份或可能对他人造成伤害、令他人感到尴尬的信息保密。

隔绝　隔绝(Seclusion)就是把东西放在不可到达的地方。这个位置还可提供严格的访问控制。隔绝有助于实施保密性保护。

隔离　隔离(Isolation)是保持把某些事物与其他事物分离的行为。隔离可用于防止信息混合或信息泄露。

每个组织都需要评估他们想要实施的具体保密性措施。用于实现某种形式保密性的工具和技术可能不支持或不允许其他形式的保密性。

1.1.2　完整性

CIA 三元组的第二个原则是完整性。完整性是保护数据可靠性和正确性的概念。完整性保护措施防止了未经授权的数据更改。它确保数据保持准确、未被替换。恰当实施的完整性保护措施允许合法修改数据，同时可预防故意和恶意的未经授权的活动(如病毒和入侵)以及授权用户的误操作(如错误或疏忽)。

为保持完整性，客体必须保持其准确性，并仅由授权的主体按预期方式修改。如果安全机制提供了完整性，它就高度保证数据、客体和资源不会由最初的受保护状态转变到非保护状态。客体在存储、传输或过程中都不应遭受未经授权的更改。因此，保持完整性意味着客体本身不被未经授权地更改，且管理和操作客体的操作系统和程序实体不被破坏。

可从以下三个方面检验完整性：

- 防止未经授权的主体进行修改。
- 防止授权主体进行未经授权的修改，如引入错误。
- 保持客体内外一致以使客体的数据能够真实反映现实世界，而且与任何子客体、对等客体或父客体的关系都是有效的、一致的和可验证的。

为在系统中维持完整性，必须对数据、客体和资源的访问设置严格的控制措施。此外，应

该使用活动记录日志来确保只有经过授权的用户才能访问各自的资源。在存储、传输和处理中维护和验证客体的完整性需要多种控制和监督措施。

许多攻击聚焦在破坏完整性上。这些攻击包括病毒、逻辑炸弹、未经授权的访问、编码和应用程序中的错误、恶意修改、故意替换及系统后门。

与保密性一样，能破坏完整性的不仅有蓄意攻击。人为错误、疏忽或不称职造成了很多未经授权修改敏感信息的案例。导致完整性破坏的事件包括：修改或删除文件，输入无效的数据，修改配置时在命令、代码和脚本中引入错误，引入的病毒，执行恶意代码(如特洛伊木马)。导致完整性破坏的原因可能是任何用户(包括管理员)的操作，也可能是安全策略中的疏漏或配置有误的安全控制。

许多控制措施可预防对完整性的威胁。这些控制措施包括严格的访问控制、严格的身份验证流程、入侵检测系统、客体/数据加密、散列值验证(见第 6 章)、接口限制、输入/功能检查和充分的人员培训。

完整性依赖于保密性。完整性相关的其他概念、条件和特征如下。

- **准确性**：正确且精确无误。
- **真实性**：真实地反映现实。
- **可信性**：可信的或非伪造的。
- **有效性**：实际上(或逻辑上)是正确的。
- **不可否认性**：不能否认执行过某个动作或活动，或能证明通过了某个通信或事件的初始验证。
- **问责制**：对行为和结果负有责任或义务。
- **职责**：负责或控制某人或某事。
- **完整性**：拥有全部需要和必要的组件或部件。
- **全面性**：完整的范围，充分包含所有需要的元素。

不可否认性

不可否认性(Nonrepudiation)确保事件的主体或引发事件的人不能否认事件的发生。不可否认性可预防主体否认发送过消息、执行过动作或导致某个事件的发生。通过标识、身份验证、授权、问责制和审计使不可否认性成为可能。可使用数字证书、会话标识符、事务日志以及其他许多事务性机制和访问控制机制来实施不可否认性。在构建的系统中，如果没有正确实现不可否认性，就不能证明某个特定实体执行了某个操作。不可否认性是问责制的重要组成部分。如果嫌疑人能够证明起诉不成立，他就不会被追究责任。

1.1.3 可用性

CIA 三元组的第三个原则是可用性，这意味着授权主体被授予实时的、不间断的客体访问权限。通常，可用性保护控制措施提供组织所需的充足带宽和实时的处理能力。如果安全机制提供了可用性，它就提供了对数据、客体和资源可被授权主体访问的高度保障。

可用性包括对客体的有效的持续访问及抵御拒绝服务(DoS)攻击。可用性还意味着支撑性基础设施(包括网络服务、通信和访问控制机制)是可用的，并允许授权用户获得授权的访问。

要在系统上维护可用性，必须有适当的控制措施以确保授权的访问和可接受的性能水平，能快速处理终端，能提供冗余，能维护可靠的备份，能防止数据丢失或受损。

有很多针对可用性的威胁。这些威胁包括设备故障、软件错误和环境问题(过热、静电、洪水、断电等)。还有一些聚焦于破坏可用性的攻击形式，包括 DoS 攻击、客体破坏和通信中断。

与保密性和完整性一样，对可用性的侵犯不仅限于蓄意攻击。许多未经授权修改敏感信息的实例都是由人为错误、疏忽或不称职造成的。导致可用性破坏的一些事件包括意外删除文件、滥用硬件或软件组件、资源分配不足、错误标记或错误的客体分类。

破坏可用性的原因可能是任意用户(包括管理员)的操作。安全策略中的疏漏或配置有误的安全控制也会破坏可用性。

大量控制措施可防御潜在的可用性威胁。这包括正确设计中转传递系统、有效使用访问控制、监控性能和网络流量、使用防火墙和路由器防止 DoS 攻击、对关键系统实施冗余机制以及维护和测试备份系统。大多数安全策略以及业务连续性计划(BCP)关注不同级别的访问/存储/安全(即磁盘、服务器或站点)上的容错特性，目标是消除单点故障，保障关键系统的可用性。

可用性依赖于完整性和保密性。没有完整性和相互信任，就无法维持可用性。与可用性相关的其他一些相关概念、条件和特征如下。

- **可用性**：能够容易被主体使用或学习的状态，或能被主体理解和控制。
- **可访问性**：保证全部授权主体可与资源交互而不考虑主体的能力或限制。
- **及时性**：及时、准时，在合理的时间内响应，或提供低时延的响应。

真实场景

CIA 优先级排序

每个组织都有独特的安全需求。在 CISSP 考试中，大多数安全概念都用通用术语来说明，但在真实世界中，只有通用概念和最佳实践还不够。管理团队和安全团队必须协力确定组织安全需求的优先级别。这包括制定预算和支出计划，分配专业人员和工作时间，关注信息技术(IT)和安全人员的工作成果。这项工作中的一个关键任务是对组织的安全需求进行优先级排序。清楚在创建安全的环境及最后部署安全解决方案时哪个原则或资产更重要。通常，进行优先级排序是一个难题。解决这个难题的一个可行做法是首先确定保密性、完整性和可用性这三个主要安全原则的优先级。定义这些原则中的哪个对组织制定充分的安全解决方案是最重要的。这就建立了一个从概念到设计、架构、部署，最后到维护的可复用模式。

你知晓 CIA 三元组中每个原则对组织的优先级别吗？如果不知道，那就去寻找答案。CIA 三元组的优先级别中一个普遍存在的情况是军方和政府机构很多时候倾向于优先考虑保密性而不是完整性和可用性，而私营企业倾向于优先考虑可用性而不是保密性和完整性。尽管这些优先级别侧重于 CIA 三元组的某个原则，但这并不意味着会忽略或不恰当处理排在第二或第三优先级别的原则。OT(操作技术)系统的例子有 PLC(可编程逻辑控制器)、SCADA(监控和数据采集)以及制造车间使用的 MES(制造执行系统)设备和系统。将标准 IT 系统与 OT 系统进行比较时，发现了另一种观点。IT 系统(甚至在私营企业)倾向于满足 CIA 三元组；而 OT 系统虽然倾向于满足 CIA 三元组，但其中可用性的优先级别最高，完整性又优先于保密性。再次强调，这只是一个概述，但它可能有助于你在 CISSP 考试中回答问题。每个独立组织都会决定自身的安全优先级别。

1.1.4 其他安全概念

除了 CIA 三元组外，在设计安全策略和部署安全解决方案时，还需要考虑其他许多与安全相关的概念和原则。

你也许听说过 AAA 服务的概念。这 3 个字母 A 分别代表身份验证(Authentication)、授权(Authorization)和记账(Accounting)；最后一个 A 有时也指审计(Auditing)。尽管缩写中只有三个字母，但实际上代表了五项内容：标识(Identification)、身份验证、授权、审计和记账，如图 1.2 所示。

这五项内容代表以下安全程序。

- 标识：当试图访问受保护的区域或系统时声明自己的身份。
- 身份验证：证实身份。
- 授权：对一个具体身份定义其对资源和客体的访问许可(如：允许/授予和/或拒绝)。
- 审计：记录与系统和主体相关的事件与活动日志。
- 记账(又名问责制)：通过审查日志文件来核查合规和违规情况，以便让主体对自身行为负责。

虽然经常讲 AAA 与身份验证系统关联在一起，但实际上，AAA 是一个安全基础概念。缺少这五个要素之一，安全机制就是不完整的。下面将分别讨论这五个要素。

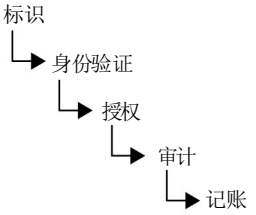

图 1.2 AAA 服务的五个要素

1. 标识

标识是主体声明身份和责任的过程。主体必须为系统提供身份标识来启动身份验证、授权和记账过程。提供身份标识可能需要：输入用户名，刷卡，摇动一台近场通信设备，说出一个短语，或将你的脸、手掌或手指放入摄像机或扫描设备。提供流程 ID 号也是一种标识过程。如果没有身份标识，系统就无法将身份验证因素与主体相关联。

一旦主体被标识(即，一旦主体的身份被标识和验证)，该主体要对其接下来的所有行为负责。IT 系统通过身份标识来跟踪活动，而不是通过主体本身。计算机并不知道一个人与另一个人的区别，但它知道你的用户账户与其他所有用户账户是不同的。主体的身份通常被标记为或被认为是公开信息。然而，简单地声明身份并不意味着访问或授权。在允许访问受控资源(验证授权)之前，必须证明身份(验证)或验证身份(确保不可否认性)。这个过程就是身份验证。

2. 身份验证

验证或测试声明的身份是否有效的过程称为身份验证。身份验证要求主体提供与所要求的身份对应的附加信息。最常见的身份验证形式是使用密码(这包括个人身份识别码和密码短语)。

身份验证通过将一个或多个因子与有效的身份数据库(即用户账户)进行比较来验证主体的身份。用于身份验证的身份验证因子通常被标记为或被认为是私有信息。主体和系统对身份验证因子的保密能力直接反映了系统的安全性水平。如果非法获取和使用目标用户身份验证因子的过程比较容易，那身份验证系统就不安全。如果这个过程比较困难，那么身份验证系统是相当安全的。

通常在一个流程中完成标识和身份验证两个步骤。提供身份标识是第一步，提供身份验证因子是第二步。如果不能同时提供，主体就不能访问系统——就安全性而言，单独使用任一身份验证因子都不是有效的。在某些系统中，看起来好像只提供了一个身份验证因子，但也获得了访问权限，例如在输入 ID 代码或 PIN 时。其实在此类情况下，标识是通过另一种方式处理的，比如物理位置，或者以物理形式访问系统的能力。标识和身份验证都会进行，但你可能不会像手动输入用户名和密码时那样意识到它们的存在。

一个主体可提供多种类型的身份验证因子——例如，你知道的东西(如密码、PIN)、你拥有的东西(如密钥、令牌、智能卡)、你具备的东西(即生物特征识别，如指纹、虹膜或语音识别)等。每种身份验证技术或身份验证因子都有优缺点。因此，重要的是根据环境来评估每种身份验证机制的部署可行性。

3. 授权

一旦主体通过身份验证，就必须进行访问授权。授权过程确保对已通过验证的身份所请求的活动或对客体的访问是可以被赋予的权利和特权。大多数情况下，系统评估一个访问控制矩阵来对比主体、客体与预期的活动。如果特定行为是允许的，则对主体进行授权。如果特定行为不被允许，就不对主体进行授权。

请记住，仅因为主体已通过标识和身份验证过程，并不意味着主体已被授权执行任意功能或访问受控环境中的所有资源。主体或许可登录到网络(即经过标识和身份验证)，但会被禁止访问文件或将其打印(即未授权执行该活动)。大多数网络用户仅被授权对特定资源集执行有限的活动。

标识和身份验证体现了访问控制的全有或全无特性。对于环境中的每个主体，授权在全部允许或全部拒绝之间有广泛的变化。用户可读取文件但不能删除，可打印文档但不更改打印队列，或者可登录到系统但不访问任何资源。通常使用访问控制模型来定义授权，例如自主访问控制(Discretionary Access Control，DAC)、强制访问控制(Mandatory Access Control，MAC)或基于角色的访问控制(Role Based Access Control，RBAC 或角色 BAC)；详见第 14 章。

4. 审计

审计或监控是追踪和记录主体的操作，以便在验证过的系统中让主体为其行为负责的程序化过程。审计也是对系统中未经授权的或异常的活动进行检测的过程。审计不仅记录主体及其客体的活动，还会记录维护操作环境和安全机制的核心系统功能的活动。通过将系统事件记录到日志中而创建的审计踪迹可用于评估系统的健康状况和性能。系统崩溃可能表明存在程序错误、驱动器错误或入侵企图。记录系统崩溃起因的事件日志常用于发现系统出现故障的原因。日志文件为重构事件、入侵或系统故障的历史记录提供了审计踪迹。

我们需要通过审计来检测主体的恶意行为、入侵企图和系统故障，以及重构事件，为起诉提供证据，生成问题报告和分析结果。审计通常是操作系统、大多数应用程序和服务的内置功能。因此，配置系统功能来记录特定类型事件的审计信息非常简单。

监控是审计的组成部分，而审计日志是监控系统的组成部分，但监控和审计这两个术语具有不同含义。监控是一种观测或监督，而审计是把信息记录到档案或文件。可在没有审计的情况下进行监控。不过如果没有某种形式的监控，则无法进行审计。虽然有此差异，但在不太严谨的讨论中，这两个术语常被互换使用。

5. 记账(或问责制)

组织的安全策略只有在有问责制的情况下才能得到适当实施。换句话说，只有在主体对他们的行为负责时，才能保持安全性。有效的问责制依赖于检验主体身份及追踪其活动的能力。通过安全服务和审计、身份验证、授权和身份标识等机制，将人员与在线身份的活动联系起来，进而建立问责制。因此，人员的问责制最终取决于身份验证过程的强度。如果没有强大的身份验证过程，那么在发生不可接受的活动时，我们就无法确定与特定用户账户相关联的人员就是实际控制该用户账户的实体。

为了获得切实可行的问责制，你可能需要能够在法庭上支持你的安全决策及实施。如果不能在法律上支持安全方面的努力，就不太可能让某人对与用户账户有关的行为负责。只使用密码进行身份验证，这显然值得怀疑。密码是最不安全的身份验证形式，有数十种不同类型的攻击可破坏这种身份验证形式。不过，使用多因素身份验证，例如组合使用密码、智能卡和指纹扫描，那么其他人几乎不可能通过攻击身份验证过程来假冒代表特定用户账户的人员。

法律上可防卫的安全

安全的要点是在防止坏事发生的同时支持好事的出现。坏事发生时，组织常希望借助法律实施和法律系统的援助来获得补偿。为获得法律赔偿，就必须证明存在犯罪行为或嫌疑人实施了犯罪，以及组织已尽力阻止罪行的发生，这意味着组织的安全需要是合法防御的。如果无法使法庭相信日志文件是准确的，以及只有主体才会实施特定的罪行，就无法获得赔偿。最终，这需要一个完整的安全解决方案，其中应当使用强大的多因素身份验证技术、可靠的授权机制和无可挑剔的审计系统。此外，还必须证明组织机构遵守了所有适用的法律和规则；发布了适当的警告和通知；逻辑和物理安全性没有受到其他危害；以及电子证据没有其他可能的合理解释。这是一个相当有挑战性的标准。因此，一个组织应该对其安全基础设施进行评估，并再次考虑如何设计和实现合法防御的安全。

1.1.5 保护机制

理解和应用保密性、完整性和可用性概念的另一个方面是保护机制或保护控制。保护机制是安全控制的共同特征。并不是所有安全控制都必须具有这些机制，但许多保护控制通过使用这些机制提供了保密性、完整性和可用性。这些机制的常见示例包括使用多层或分层访问、利用抽象、隐藏数据和使用加密技术。

1.1.6　分层

分层(layering)也被称为纵深防御，指简单使用一系列控制中的多个控制。没有哪个控制能防范所有可能的威胁。使用多层防护解决方案允许使用许多不同的控制措施来抵御随时出现的威胁。在设计分层防护安全解决方案时，一个控制失效不会导致系统或数据暴露。

使用串行层而不是并行层是很重要的。在串行层中执行安全控制意味着以线性方式连续执行一个又一个控制。只有通过串行层的配置，安全控制才能扫描、评估或减轻每个攻击。在串行层的配置中，单个安全控制的失败并不会导致整个解决方案失效。如果安全控制是并行实现的，威胁就可通过一个没有处理其特定恶意活动的检查点而导致整个解决方案失效。

串行配置的范围很窄，但层级很深；而并行配置的范围很宽，但层级很浅。并行系统在分布式计算应用程序中很有用，但在安全领域中，并行机制往往不是一个有用的概念。

想想通向建筑物的物理入口。购物中心采用并行配置。商场周边的多个地方都有出入口。串行配置最可能用于银行或机场。这些地方只提供单一入口，这个入口实际上是为了进入建筑物活动区而必须按顺序通过的多个关口或检查点。

分层还包括网络由许多独立实体组成的概念，每个实体都有自己独特的安全控制和脆弱性。在有效的安全解决方案中，所有联网系统之间存在协同作用，从而构建了统一的安全防线。使用独立的安全系统可创建分层的安全解决方案。

1.1.7　抽象

抽象(abstraction)是为了提高效率。相似的元素被放入组、类或角色中作为一个集合被指派安全控制、限制或许可。因此，可将抽象的概念应用到对客体进行分类或向主体分配角色。抽象概念还包括对客体和主体类型的定义或客体自身的定义(即，用于定义实体类的模板的数据结构)。抽象用于定义客体可包含哪些类型的数据、可在该客体上或由该客体执行哪些类型的功能以及该客体具有哪些功能。抽象使你可将安全控制分配给按类型或功能归类的客体集，由此简化安全。

1.1.8　数据隐藏

顾名思义，数据隐藏是将数据存放在主体无法访问或读取的逻辑存储空间以防止数据被泄露或访问。数据隐藏的形式包括防止未经授权的访问者访问数据库，以及限制安全级别较低的主体访问安全级别较高的数据。阻止应用程序直接访问存储硬件也是一种数据隐藏形式。数据隐藏通常是安全控制和编程中的关键元素。

通过隐匿(obscurity)保持安全与数据隐藏是类似的，不过通过隐匿保持安全是另一种概念。数据隐藏是指故意将数据存放在未授权的主体无法查看或访问的位置，而通过隐匿保持安全是指不告知主体有客体存在，从而希望主体不发现该客体。通过隐匿保持安全实际上并没有提供任何形式的保护。它只是寄希望通过保持重要事物的保密性进而不让其泄露。通过隐匿保持安全的一个实例是：虽然程序员知道软件代码存在缺陷，但他们还是发布了产品，并希望没人会发现和利用代码中存在的缺陷。

1.1.9 加密

加密(encryption)是关于对非预期的接收者隐藏通信的真实含义和意图的艺术与科学，它能将信息传递的意义或意图隐藏起来。加密有多种形式并适用于各种类型的电子通信，包括文本、音频和视频文件及应用程序。加密是安全控制中的重要内容，特别在系统间传输数据时。有多种强度的加密技术，每种加密都被设计为适用于特定用途。较弱或较差的加密可被认为类似于隐匿或通过隐匿保持安全。加密将在第 6 章和第 7 章中详细讨论。

1.2 评估和应用安全治理原则

安全治理是与支持、定义和指导组织安全工作相关的实践集合。安全治理原则通常与公司和 IT 治理密切相关，并常常交织在一起。这三类治理的工作目标一般是相同的或相互关联的。例如，组织治理的共同目标是确保组织能持续存在并随着时间不断成长或扩张。因此，治理的共同目标是维护业务流程，同时努力实现增长和弹性。

组织迫于法律和法规的要求必须实施治理，也被要求遵守行业指南或许可证要求。所有形式的治理(包括安全治理)都必须不时进行评估和验证。由于政府法规或行业最佳实践，可能存在各种审计和验证要求。通常不同的行业与国家面临的治理合规性问题也有所不同。随着多个组织的扩展和走向全球市场，治理问题变得更复杂。当不同国家的法律不一致或实际上存在冲突时，这个难题更难解决。组织作为一个整体应该具备方向、指导和工具以提供有效的监督和管理能力，解决威胁和风险；重点是缩短停机时间，并将潜在的损失或损害降至最低。

正如你看到的，安全治理通常是较严格和高层次的内容。最终，安全治理指实施安全解决方案以及与之紧密关联的管理方法。安全治理直接监督并涉及所有级别的安全。安全不完全是 IT 事务，也不应该仅被视为 IT 事务。相反，安全会影响组织的方方面面，不是仅靠 IT 人员自身能力就能处理好的事情。安全是业务运营事务，是组织流程，而不仅是 IT 极客在后台实施的事情。使用术语“安全治理”指出安全需要在整个组织中进行管理和治理，而不仅是在 IT 部门，就是为了强调这一点。

安全治理通常由治理委员会或至少由董事会管理。这是一群有影响力的专家，他们的主要任务是监督和指导组织安全与运营行动。安全是一项复杂任务。组织通常是庞大的，并很难从单一角度去理解。为实现可靠的安全治理，让一组专家协同工作是一项可靠战略。

有许多安全框架和治理指南，包括 NIST 800-53 或 NIST 800-100。虽然 NIST 主要应用在政府和军事行业，但也能调整它，供其他类型的组织采用。许多组织采用安全框架，以标准化和有序方式组织那些复杂且混乱的活动，即努力实现可接受的安全治理。

1.2.1 与业务战略、目标、使命和宗旨相一致的安全功能

安全管理计划确保正确地创建、执行和实施安全策略。安全管理计划使安全功能与业务战略、目标、使命和宗旨相一致。这包括基于业务场景、预算限制或资源稀缺来设计和实现安全。业务场景通常是文档化的参数或声明的立场，用来定义作出决策或采取某类行为的需求。创建

新的业务场景是指：对于特定业务需求，要修改现有流程或选择完成业务任务的方法。业务场景常用来证明新项目的启动是合理的，特别是与安全相关的项目。考虑可分配给基于业务需求的安全项目的预算也很重要。安全可能很昂贵，但通常比没有安全的代价更低。因此，安全是可靠和长期经营的基本要素。在大多数组织中，资金和资源(如人员、技术和空间)都是有限的。由于这些资源的限制，任何努力都需要获得最大利益。

最能有效处理安全管理计划的一个方法是自上而下。上层、高级或管理部门负责启动和定义组织的策略。安全策略为组织架构内的各个级别提供指导。中层管理人员负责将安全策略落实到标准、基线、指导方针和程序。然后，操作管理人员或安全专业人员必须实现安全管理文档中规定的配置。最后，最终用户必须遵守组织的所有安全策略。

注意：

与自上而下方法相反的是自下而上方法。在采用自下而上方法的环境中，IT 人员直接做出安全决策，而不需要高级管理人员的参与。组织中很少使用自下而上方法，在 IT 行业中，该方法被认为是有问题的。

安全管理是上层管理人员的责任，而不是IT人员的责任，它也被认为是业务操作问题，而不是IT管理问题。在组织中负责安全的团队或部门应该是独立的。信息安全(InfoSec)团队应由指定的首席信息安全官(CISO)领导，CISO必须直接向高级管理层汇报。将CISO和CISO团队赋予组织典型架构之外的自主权可改进整个组织的安全管理。这还有助于避免跨部门和内部问题。首席安全官(CSO)有时等同于CISO，不过在很多组织中，CSO是CISO的下属职位，主要关注物理安全。另一个可能替代CISO的术语是信息安全官(ISO)，但ISO也可以是CISO下属职位。

安全管理计划的内容包括：定义安全角色，规定如何管理安全、由谁负责安全以及如何检验安全的有效性，制定安全策略，执行风险分析，要求对员工进行安全教育。这些工作都通过制定管理计划来完成。

如果没有高级管理人员批准这个关键过程，即使最好的安全计划也毫无用处。没有高级管理层的批准和承诺，安全策略就不会取得成功。策略开发团队的责任是充分培训高级管理人员，使其了解即使在部署了策略中规定的安全措施后仍然存在的风险和责任。制定和执行安全策略体现了高级管理人员的应尽关心(due care)与尽职审查(due diligence)。如果一家公司的管理层在安全方面没有给予应尽关心或没有实施尽职审查，管理者就要对疏忽负责，并应对资产和财务损失负责。

安全管理计划团队应该开发三种类型的计划，如图 1.3 所示。

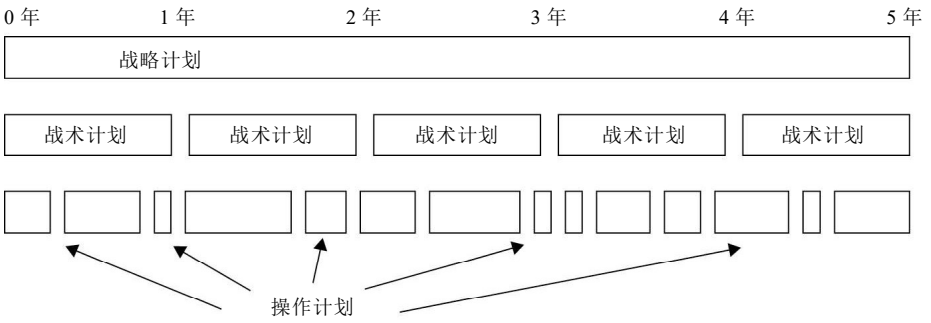

图 1.3　战略计划、战术计划和操作计划的时间跨度比较

战略计划 战略计划(strategic plan)是一个相对稳定的长期计划。它定义了组织的安全目的，还有助于理解安全功能，并使其与组织的目标、使命和宗旨相一致。如果每年进行维护和更新，战略计划的有效期大约是 5 年。战略计划也可作为计划范围。战略计划中讨论了未来的长期目标和远景。战略计划还应包括风险评估。

战术计划 战术计划(tactical plan)是为实现战略计划中设定的目标提供更多细节而制定的中期计划，或可根据不可预测的事件临时制定。战术计划通常在一年左右的时间内有用，通常规定和安排实现组织目标所需的任务。战术计划的一些示例包括项目计划、收购计划、招聘计划、预算计划、维护计划、支持计划和系统开发计划。

操作计划 操作计划(operational plan)是在战略计划和战术计划的基础上，制定的短期、高度详细的计划。操作计划只在短时间内有效或有用。操作计划必须经常更新(如每月或每季)，以保持符合战术计划。操作计划阐明了如何实现组织的各种目标，包括资源分配、预算需求、人员分配、进度安排与细化或执行程序。操作计划包括如何符合组织安全策略的实施细节。操作计划的示例包括：培训计划、系统部署计划和产品设计计划。

安全是一个持续的过程。因此，安全管理计划的活动可能有一个确定的起点，但它的任务和工作从来没有完成或实现过。有效的安全计划重点集中在具体和可实现的目标、预测变化和潜在问题上，并作为整个组织决策的基础。安全文档应该是具体的、定义完善的和明确说明的。为使安全计划有效，必须开发、维护和实际使用安全计划。

1.2.2 组织的流程

安全治理需要关注组织的方方面面，包括收购、剥离和治理委员会的流程。收购与兼并会增加组织的风险等级。这些风险包括不恰当的信息泄露、数据丢失、停机或未能获得足够的投资回报率(Return On Investment，ROI)。除了所有兼并与收购中的典型业务和财务方面外，对于降低在转型期间发生损失的可能性，良好的安全监督和加强的审查通常也是极其重要的。

同样，资产剥离或任何形式的资产减少或员工裁减都会增加风险，进而增加对集中安全治理的需求。需要对资产进行消磁以防止数据泄露。应该删除和销毁存储介质，因为介质净化处理技术不能保证残留数据不被恢复。需要对不再负责相关事宜的员工询问工作完成情况，该过程通常被称为离职面谈。这一过程通常包括审查所有保密协议及其他任何在雇佣关系终止后仍继续生效的约束合同或协议。

加强安全治理的另外两个组织流程示例是变更控制/变更管理和数据分类。

1. 变更控制/变更管理

变更控制或变更管理是安全管理的另一重要内容。安全环境的变更可能引入漏洞、重叠、客体丢失和疏忽进而导致出现新脆弱性。面对变更，维护安全的唯一途径就是系统性的变更管理。这通常涉及与安全控制和安全机制相关的活动，包括广泛的计划、测试、日志记录、审计和监控。然后对环境变化进行记录来识别变更发起者，无论变更发起者是客体、主体、程序、通信路径还是网络本身。

变更管理的目标是确保变更不会消减或损坏安全。变更管理还负责让变更能回滚到变更前的安全状态。变更管理可在任意系统上实现而不考虑安全级别。最终，变更管理通过保护已实现的安全，使安全不受无意的、间接的或负面的影响，从而提升环境的安全性。尽管变更管理

的重要目标是防止非预期的安全降低，但它的首要目标是使所有变更被详细记录和审计，从而使变更能被管理层检查和审核。

变更管理应该用于监督系统的所有变更，包括硬件配置和操作系统(OS)以及应用软件。应该在设计、开发、测试、评估、实现、分发、演进、发展、持续操作和修改中都进行变更管理。变更管理需要每个组件和配置的详细清单。它还需要收集和维护每个系统组件(包括硬件、软件)的全部文档，从配置到安全特性。

配置管理或变更管理的变更控制过程有以下几个目标或要求：

- 在受监控的环境中有序实施更改。
- 包含正式的测试过程，验证变更能实现预期效果。
- 所有变更都能够撤消(也称为回退或回滚计划/程序)。
- 在变更实施前通知用户，以防止影响生产效率。
- 对变更影响进行系统性分析，以确定变更是否会对安全或业务流程产生负面影响。
- 最小化变更对能力、功能和性能方面的负面影响。
- 变更顾问委员会(Change Advisory Board，CAB)需要评审和批准变更。

变更管理过程的一个示例是并行运行，在这种新的系统部署测试中，新系统和旧系统并行运行。在新旧系统中同时执行所有主要的或重要的用户流程，以确保新系统能支持旧系统提供的所有业务功能。

2. 数据分类

数据分类(data classification，也称数据分级)是基于数据的保密性、敏感性或秘密性需求而对其进行保护的主要手段。在设计和实现安全系统时，以相同方式处理所有数据是低效的，因为有些数据项比其他数据项需要更多安全性。用低级别安全保护所有内容意味着敏感数据很容易被访问。用高级别安全保护所有内容又过于昂贵，并且限制了对未分类的、非关键数据的访问。数据分类用于确定为保护数据和控制对数据的访问而分配多少精力、金钱和资源。数据分类或分级是将条目、主体、客体等组织成具有相似性的组、类别或集合的过程。这些相似性可能是价值、成本、敏感性、风险、脆弱性、权利、特权、可能的损失程度或“知其所需”。

数据分类方案的主要目标是基于指定的重要性与敏感性标签，对数据进行正式化和分层化的安全防护过程。数据分类为数据存储、处理和传输提供安全机制，还确定了该如何从系统中删除和销毁数据。

以下是使用数据分类方案的好处：

- 数据分类证实了组织对有价值的资源和资产的保护承诺。
- 数据分类帮助组织确定最重要的或最有价值的资产。
- 数据分类给保护机制的选择提供了凭据。
- 数据分类通常是法规或法律限制的要求。
- 数据分类有助于定义访问级别、使用的授权类型，以及定义不再具有价值的资源的销毁和/或降级的参数。
- 数据分类有助于在数据的生命周期管理中确定数据存储时间(保留时间)，并确定数据使用和数据销毁方式。

数据分类标准因实施数据分类的组织而异。不过，可从通用的或标准化的分类系统总结出很多通用特征：

- 数据的有用性
- 数据的时效性
- 数据的价值或成本
- 数据的成熟度或年龄
- 数据的生命周期(或何时过期)
- 与人员的关联
- 数据泄露损失评估(即数据泄露将如何影响组织)
- 数据修改损失评估(即数据修改将如何影响组织)
- 数据对国家安全的影响
- 对数据的已授权访问(即谁有权访问数据)
- 对数据的访问限制(即谁对数据的访问受到限制)
- 维护和监测数据(即谁应该维护和监控数据)
- 数据存储

使用任何适合组织的数据分类标准，都要对数据进行评估，并为其分配适当的数据分类标签。某些情况下，数据分类标签会被添加到数据对象中。在其他情况下，在数据存储或对数据实施安全保护机制后，会自动进行数据分类标记。

要实现数据分类方案，必须执行七个主要的步骤或阶段：

(1) 确定管理人员，并定义其职责。

(2) 指定信息如何分类和标记的评估标准。

(3) 对每个资源进行数据分类和增加标签(数据所有者会执行此步骤，监督者应予以审核)。

(4) 记录数据分类策略中发现的任何异常，并集成到评估标准中。

(5) 选择将应用于每个分类级别的安全控制措施，以提供必要的保护级别。

(6) 指定解除资源分类的流程，以及将资源保管权转移给外部实体的流程。

(7) 建立组织范围的培训程序来指导所有人员使用分类系统。

解除分类常在设计分类系统和编写使用程序时被忽略。一旦资产不再被授权保护其当前指定的分类或敏感级别，就需要解除分类。换句话说，如果新增资产，它将被分配一个比当前指定的敏感级别更低的标签。如果资产未按照需要解除分类，安全资源会被浪费。

两种常用的数据分类方案是政府/军事分类(图 1.4)和商业/私营部门分类。政府/军事分类方案分为五个分类级别。

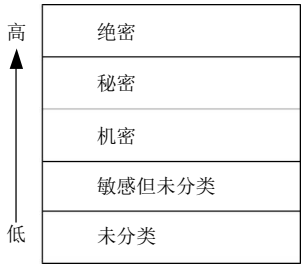

图 1.4　政府/军事分类方案

绝密(Top Secret)　绝密是最高级别的分类。未经授权泄露绝密数据，将对国家安全造成严重影响和严重损害。最高机密数据是基于“知其所需”划分的，这样用户就可以拥有最高机

密权限，并在“知其所需”前不访问任何数据。

秘密(Secret)　秘密用于描述具备限制性质的数据。未经授权泄露被列为秘密的数据，将对国家安全造成重大影响和重大损害。

机密(Confidential)　机密用于敏感的、专有的或高度有价值的数据。未经授权泄露机密信息，将对国家安全造成明显的影响和严重损害。这个级别适用于“秘密”和“敏感但非分类”之间的所有数据。

敏感但未分类　敏感但未分类(Sensitive But Unclassified，SBU)用于内部使用或仅用于办公室使用(For Office Use Only，FOUO)的数据。SBU 常用来保护可能侵犯个人隐私权的信息。这不是严格意义上的分类标签，而是表示使用或管理的标记或标签。

未分类　未分类(Unclassified)描述既不敏感也不需要分级的数据。泄露未分类数据不会损害保密性或造成任何明显的损害。这不是严格意义上的分类标签，而是表示使用或管理的标记或标签。

提示：

采用首字母记忆法按从最低安全到最高安全的顺序可轻易记住政府/军事分类方案中的 5 个名称：美国可停止恐怖主义(U.S. Can Stop Terrorism)。请注意，五个大写字母分别代表五个分类级别，从左边的最低安全级别到右边的最高安全级别(或按图 1.4 中自下向上的顺序)。

带有秘密、机密和绝密的标签统称为分类的级别。通常，向未经授权的个人透露数据的分类级别是一种侵犯行为。因此，术语“分类”通常指分类的级别在非分类级别之上的全部数据。所有分类的数据都不受《信息自由法案》以及许多其他法律法规的约束。美国军事分类方案最关心数据的敏感性，重点是保密性(即防止泄露)。可根据危害保密性事件发生时造成损害的严重程度粗略定义每个分类级别或分类标签。绝密数据将对国家安全造成严重损害，未分类数据不会对国家或地方安全造成任何严重损害。

商业公司和私营机构的分类系统差别很大，因为一般来说他们不需要遵守相同的标准或规定。CISSP 考试侧重于四个常见的或可能的商业分类级别，如图 1.5 所示。

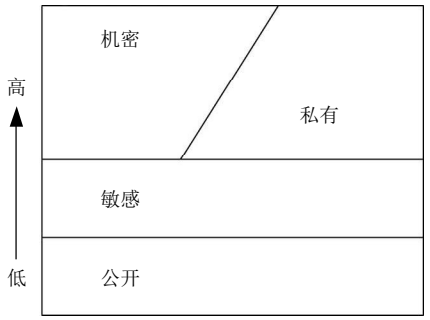

图 1.5　商业/私营部门分类方案

机密(Confidential)　机密是最高级别的分类。用于极度敏感的和只在内部使用的数据。如果机密数据被泄露，将对公司产生重大的负面影响。有时会用专有(proprietary)代替机密标签。有时专有数据被认为是一种特定形式的机密信息。如果泄露了专有数据，会给组织的竞争优势

带来极大的负面影响。

私有(Private) 私有指私有的或个人特有的及仅供内部使用的数据。如果公司或个人的私有数据被泄露，将产生重大的负面影响。

注意：

商业/私营部门分类方案中，对机密数据和私有数据的安全保护大致上都是相同的级别。这两个标签的真正区别在于，机密数据是公司数据，而私有数据是与个人相关的数据，如医疗数据。

敏感(Sensitive) 敏感用于比公开数据分类级别更高的数据。如果敏感数据被泄露，会给公司带来负面影响。

公开(Public) 公开是分类级别的最低层级。用于所有不适合较高分类级别的数据。泄露公开数据不会给组织带来严重的负面影响。

与数据分类或分级相关的另一相关因素是所有权。所有权将职责正式分配到个人或团体。文件或其他类型的客体可被指定所有者，这清晰而明确地体现了操作系统中的所有权。通常，所有者对其拥有的客体具有全部功能和权限。一般将所有权授予操作系统中最强大的账户，如 Windows 中的管理员账户、UNIX 中的 root 账户或 Linux 中的 root 账户。大多数情况下，创建新客体的主体默认为该客体的所有者。在某些环境中，安全策略要求在创建新客体时，必须将所有权从最终用户正式更改为管理员或管理用户。这种情况下，管理员账户可简单地获得新客体的所有权。

在正规的 IT 架构之外，客体的所有权通常不那么明显。在公司文档中可为设施、业务任务、流程、资产等定义所有者。不过，这样的文档在现实世界中并不总能“实现”所有权。文件客体的所有权由操作系统和文件系统强制执行，而物理客体、无形资产或组织概念(如研究部门或开发项目)的所有权仅在文档中定义，所以很容易遭到破坏。必须对现实世界中的所有权实施其他安全治理。

1.2.3 组织的角色与责任

安全角色是个人在组织内安全实施和管理总体方案中扮演的角色。安全角色不是固定或静止的，所以并不需要预先在工作内容中说明。熟悉安全角色对在组织内建立通信和支持结构是很有帮助的。这种结构能够支持安全策略的部署和执行。根据在安全环境中出现的逻辑顺序介绍如下六个角色。

高级管理者 组织所有者(高级管理者)角色被分配给最终对组织安全的维护负责及最关心资产保护的人员。高级管理者必须在所有策略问题上签字。事实上，执行所有活动前都必须经过高级管理者的认可和批准。如果缺少高级管理者的授权和支持，就没有有效的安全策略。高级管理者对安全策略的认可表明组织内已实现的、安全的可接受所有权。高级管理者将对安全解决方案的总体成功或失败负责，并负责在为组织建立安全方面给予应尽关心和实施尽职审查。

尽管高级管理者最终负责安全，但他们很少直接实施安全解决方案。大多数情况下，这种责任被分配给组织内的安全专业人员。

安全专业人员 安全专业人员角色或计算机事件响应小组(Incident Response Team，IRT)角色被分配给受过培训和经验丰富的网络、系统和安全工程师们，他们负责落实高级管理者下达

的指示。安全专业人员的职责是保证安全性，包括编写和执行安全策略。安全专业人员可被称为 IS/IT 功能角色。安全专业人员角色通常由一支团队完成，该团队负责根据已批准的安全策略设计和实现安全解决方案。安全专业人员不是决策者，而是实施者。所有决策都必须由高级管理者决定。

数据所有者　数据所有者(data owner)角色将被分配给在安全解决方案中负责布置和保护信息分类的人员。数据所有者通常是高级管理人员，他们最终对数据保护负责。然而，数据所有者通常将实际数据管理任务的责任委托给数据托管员。

数据托管员　数据托管员(data custodian)角色被分配给负责执行安全策略与高级管理者规定的保护任务的人员。数据托管员执行所有必要的活动，为实现数据的 CIA 三元组(保密性、完整性和可用性)提供充分的数据支持，并履行上级管理部门委派的要求和职责。这些活动包括执行和测试备份、验证数据完整性、部署安全解决方案以及基于分类管理数据存储。

用户　用户(最终用户或操作者)角色被分配给任何能访问安全系统的人员。用户的访问权限与他们的工作任务相关并受限，因此他们只有足够的访问权限来执行工作岗位所需的任务(最小特权原则)。用户有责任通过遵守规定的操作程序和在规定的安全参数内进行操作来理解和维护组织的安全策略。

审计人员　审计人员(auditor)负责审查和验证安全策略是否正确执行，以及相关的安全解决方案是否完备。审计人员角色可分配给安全专业人员或受过培训的用户。审计人员出具由高级管理者审核的审计报告。高级管理者将在这些报告中发现的问题作为新的工作内容分配给安全专业人员或数据托管员。不过，因为审计人员需要对活动发起者(即在环境中工作的用户或操作人员)进行审计或监控，所以审计人员被列为最后一个角色。

所有这些角色都在安全环境中发挥着重要作用。这些角色有助于确定义务和责任以及确定分级管理和授权方案。

1.2.4　安全控制框架

为组织制定安全声明通常涉及很多事项，并非只是写下几条远大理想。多数情况下，需要很多规划才能制定出可靠的安全策略。许多读者可能认为召开会议为未来的会议制定计划是一种荒谬的做法。但实际上，安全规划必须首先制定计划，然后规划标准和合规，最后实际开发和设计计划。跳过这些“规划-计划”步骤中的任何一个，都可能在组织的安全解决方案实施之前就破坏它。

安全规划步骤中的第一步最重要，就是考虑组织所希望的安全解决方案的总体安全控制框架或结构。可从几个相关的安全控制框架中进行选择，不过被应用广泛的安全控制框架之一是信息和相关技术控制目标(COBIT)。COBIT 是由信息系统审计和控制协会(ISACA)编制的一套记录最佳 IT 安全实践的文档。它规定了安全控制的目标和需求，并鼓励将 IT 安全思路映射到业务目标。COBIT 5 的基础是企业 IT 治理和管理的如下五个关键原则。

- 原则 1：满足利益相关方的需求
- 原则 2：从端到端覆盖整个企业
- 原则 3：使用单一的集成框架
- 原则 4：采用整体分析法
- 原则 5：把治理从管理中分离出来

COBIT 不仅可用于计划组织的 IT 安全，还可作为审计人员的工作指南。COBIT 是一个得到广泛认可与重视的安全控制框架。

幸运的是，在考试中只引用了 COBIT 的大体内容，不需要了解进一步的细节。不过如果你对这个概念感兴趣，请访问 ISACA 网站(www.isaca.org)；或者如果需要总体概述，请阅读 Wikipedia 上的 COBIT 条目。

IT 安全还有其他许多标准和指南，包括：

- **开源安全测试方法手册(Open Source Security Testing Methodology Manual，OSSTMM)** 安全基础设施测试和分析的同行评议指南，参见 www.isecom.org/research/。
- **ISO/IEC 27002(取代了 ISO 17799)** 一个国际标准，可作为实施组织信息安全及相关管理实践的基础，参见 www.iso.org/standard/54533.html。
- **信息技术基础设施库(Information Technology Infrastructure Library，ITIL)** ITIL 最初由英国政府精心设计，它是一套推荐的核心 IT 安全和操作流程的最佳实践，经常用作定制 IT 安全解决方案的起点。

1.2.5 应尽关心和尽职审查

为什么计划安全如此重要？原因之一是需要应尽关心(due care)和尽职审查(due diligence)。“应尽关心”指使用合理的关注来保护组织的利益，“尽职审查”指的是具体的实践活动。对于考试，应尽关心是指制定一种正式的安全框架，包含安全策略、标准、基线、指南和程序。尽职审查是指将这种安全框架持续应用到组织的 IT 基础设施上。操作性安全指组织内的所有责任相关方持续给予应尽关心和实施尽职审查。

在当今的商业环境中，谨慎是必需的。在安全事故发生时，拿出应尽关心和尽职审查的证据是证明没有疏忽的唯一方法。高级管理人员必须在安全事故发生时出示应尽关心和尽职审查的记录以减少对他们的处罚和承担的罪责。

1.3 开发、记录和实施安全策略、标准、程序和指南

对大多数组织来说，维护安全是业务发展的重要内容。如果安全受到严重破坏，许多组织都将无法正常运转。为降低安全故障出现的可能性，实施安全的流程在某种程度上就是按照组织架构确定的文档。每个级别都聚焦于信息和问题的一个特定类别。开发和实现文档化的安全策略、标准、程序和指南可以生成可靠的、可依赖的安全基础设施。这种规范化过程极大地减少了 IT 基础设施设计和实现的安全解决方案中的混乱和复杂性。

1.3.1 安全策略

规范化的最高层级文件是安全策略。安全策略定义了组织所需的安全范围，讨论需要保护的资产以及安全解决方案需要提供的必要保护程度。安全策略是对组织安全需求的概述或归纳，它定义了主要的安全目标，并概述了组织的安全框架。安全策略还确定了数据处理的主要功能

领域，并澄清和定义了所有相关术语。安全策略应该清楚地定义为什么安全性是重要的，以及哪些资产是有价值的。安全策略是安全实施的战略计划。安全策略应概述为保护组织利益而应采取的安全目标和做法。安全策略讨论了安全对日常业务运营的各个方面的重要性，以及高级管理者支持安全实施的重要性。安全策略用于分配职责、定义角色、指定审计需求、概述实施过程、确定合规性需求和定义可接受的风险级别。安全策略常用来证明高级管理者在保护组织免受入侵、攻击和灾难时已经给予了应尽关心。安全策略是强制性的。

很多组织使用多种类型的安全策略来定义或概述其总体安全策略。组织安全策略重点关注与整个组织相关的问题。特定问题的安全策略集中在特定的网络工作服务、部门、功能或有别于组织整体的其他不同方面。特定系统的安全策略关注于单个系统或系统类型，并规定了经过批准的硬件和软件，概述了锁定系统的方法，甚至强制要求采用防火墙或其他特定的安全控制。

除了这些针对特定类型的安全策略外，还有三大类综合的安全策略：监管性策略、建议性策略和信息性策略。当组织有需要遵守的行业或法律标准时，就需要监管性策略。该策略讨论了必须遵守的法规，并概述了用于促进满足监管要求的程序。建议性策略讨论可接受的行为和活动，并定义违规的后果。它说明了高级管理者对组织内安全性和合规性的期望，大多数策略都是建议性的。信息性策略旨在提供关于特定主体的信息或知识，如公司目标、任务声明或组织如何与合作伙伴和客户交流。信息性策略提供与整体策略特定要素相关的支持、研究或背景信息。

从安全策略可引出完整安全解决方案所需的其他很多文档或子元素。策略是宽泛的概述，而标准、基线、指南和程序包括关于实际安全解决方案的更具体、更详细的信息。标准是安全策略的下一级别。

安全策略与人员

作为一条经验法则，安全策略(以及标准、程序和指南)不应该针对特定的个人。安全策略应该为特定角色定义任务和职责，而不是为某个人定义任务和职责。这种角色可具备行政控制或人事管理职能。因此，安全策略不是定义谁要做什么，而是定义在安全基础结构内的各个角色必须做什么。然后将这些定义好的安全角色作为工作描述或工作任务分配给个人。

可接受的使用策略

可接受的使用策略是一个常规生成的文档，它是整个安全文档基础结构的一个组成部分。可接受的使用策略专门用来分配组织内的安全角色，并确保职责与这些角色相关联。该策略定义了可接受的性能级别及期望的行为和活动。不遵守该策略可能导致工作行为警告、处罚或解聘。

1.3.2　标准、基线和指南

一旦完成主要的安全策略，就可在这些策略的指导下编制其他安全文档。标准对硬件、软件、技术和安全控制方法的一致性定义了强制性要求。标准提供了在整个组织中统一实施技术和程序的操作过程。标准是战术计划文档，规定了达到安全策略定义的目标和总体方向的步骤或方法。

下一层级是基线。基线定义了整个组织中每个系统必须满足的最低安全级别。所有不符合

基线要求的系统在满足基线要求之前都不能上线生产。基线建立了通用的基础安全状态，在此之上可实施所有额外的、更严格的安全措施。基线通常是系统特定的，一般参考行业或政府标准，如 TCSEC(可信计算机系统评估标准)或 ITSEC(信息技术安全评估和标准)或 NIST(美国国家标准与技术研究院)标准。

指南是规范化安全策略结构中基线的下一个元素。指南提供了关于如何实现标准和基线的建议，并作为安全专业人员和用户的操作指南。指南具有灵活性，所以可针对每个特定的系统或条件分别制定指南，并可在新程序的创建中使用指南。指南说明应该部署哪些安全机制，而不是规定特定的产品或控制措施，并详细说明配置。指南概述了方法(包括建议的行动)，但并非强制性的。

1.3.3 程序

程序是规范化安全策略结构的最后一个元素。标准操作程序(Standard Operating Procedure，SOP)是详细的分步实施文档，描述了实现特定安全机制、控制或解决方案所需的具体操作。程序可讨论整个系统部署操作，或关注单个产品或方面，如部署防火墙或更新病毒定义。大多数情况下，程序是针对特定系统和软件的。程序必须随着系统硬件与软件的发展而不断更新。程序的目的是确保业务流程的完整性。如果一切都是通过遵循详细的程序来完成的，那么所有活动都应该遵守策略、标准和指南。程序有助于在所有系统之间确保安全的标准化。

通常，安全策略、标准、基线、指南和程序的制定只是在顾问或审计人员的敦促下才会加以考虑。如果这些文档没有被使用和更新，安全环境的管理将无法把它们当成指南使用。如果没有这些文件提供的规划、设计、结构和监督，就无法维护环境的安全，也无法表示已经尽责地给予了应尽关心。

制定一个包含上述所有元素内容的文档也是常见的做法。不过应该避免这种做法。这些结构中的每个都必须作为独立实体存在，因为每个结构都实现了不同的特殊功能。在规范化安全策略文档结构中，顶层的文档较少，因为它们一般是对观点和目标的广泛讨论。在规范化安全策略文档结构的下层有很多文档(即指南和程序)，因为它们包含了数量有限的系统、网络、部门和区域的特定详细信息。

将这些文档作为独立实体保存有几个好处：

- 并非所有用户都需要知道所有安全分类级别的安全标准、基线、指南和程序。
- 当发生更改时，可以较方便地只更新和重新分发受影响的策略，而不是更新全部策略并在整个组织中重新分发。

制定整个安全策略和所有支持文档是一项艰巨任务。许多组织只是致力于定义基本的安全参数，对日常活动每个方面的详细描述较少。然而在理论上，详细和完整的安全策略能以针对性的、高效的和特定的方式支持现实世界的安全。如果安全策略文档相当完整，就可以用于指导决策、培训新用户、响应问题以及预测未来的发展趋势。安全策略不应该是一种事后的想法，而应是组织建立中的关键部分。

对于包含完整安全策略的文档的理解还有其他一些看法。图 1.6 显示了这些组件的依赖性：策略、标准、指南和程序。安全策略定义组织安全文档的总体结构。然后，标准是基于策略及法规和合同的约束。从中推演得到指南。最后，程序基于其他三个组件。使用金字塔可以传达每种文档的大小。完整安全策略中的程序通常远远超过任何单个元素的程序。相比之下，指南

比程序少，标准也比程序少，整体或组织范围内的安全策略通常更比程序少。

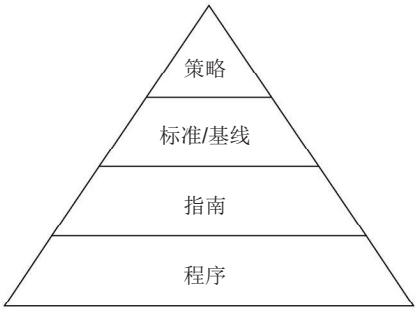

图 1.6　安全策略组件的比较关系

1.4　理解与应用威胁建模的概念和方法

威胁建模是识别、分类和分析潜在威胁的安全过程。威胁建模可当作设计和开发期间的一种主动措施被执行，也可作为产品部署后的一种被动措施被执行。这两种情况下，威胁建模过程都识别了潜在危害、发生的可能性、关注的优先级以及消除或减少威胁的手段。本节将介绍威胁建模概念的多个应用实例以及几种威胁建模方法。

威胁建模不是一个独立事件。组织通常在进行系统设计过程早期就开始进行威胁建模，并持续贯穿于系统整个生命周期中。例如，微软使用安全开发生命周期(SDL)过程在产品开发的每个阶段考虑和实现安全。这种做法支持“设计安全，默认安全，部署和通信安全”(也称为SD3+C)的座右铭。这一过程有两个目标：

- 降低与安全相关设计和编码的缺陷数量。
- 降低剩余缺陷的严重程度。

换句话说，尽力减少脆弱性与降低任何现存脆弱性的影响。总体结果也就降低了风险。

主动式威胁建模发生在系统开发的早期阶段，特别是在初始设计和规范建立阶段。这种类型的威胁建模也被称为防御方法。这种方法基于在编码和制作过程中预测威胁和设计特定防御，而不是依赖于部署后更新和打补丁。大多数情况下，集成的安全解决方案成本效益更高，比后期追加的解决方案更有效。遗憾的是，并非所有威胁都能在设计阶段被预测到，所以仍然需要被动式威胁建模来解决不可预见的问题。

被动式威胁建模发生在产品创建与部署后。这种部署可在测试或实验室环境中进行，或在通用市场中进行。此类威胁建模也称为对抗性方法。这种威胁建模技术是道德黑客、渗透测试、源代码审查和模糊测试背后的核心概念。尽管这些过程在发现需要解决的缺陷和威胁方面通常很有用，但遗憾的是，它们导致需要在编码中添加新对策的工作。从长远看，回到设计阶段可能生产出更好的产品，但从头开始会耗费大量时间，并导致产品发布时间的延迟。因此，最简单的方法是在部署后向产品中增加更新或补丁。但这样做的结果是在可能降低功能和用户友好性的前提下，并没有带来更有效的安全改进(过度主动的威胁建模)。

注意：

模糊(Fuzz)测试是一种专用的动态测试技术，它向软件提供许多不同类型的输入，以强调其局限性并发现以前未发现的缺陷。模糊测试软件向软件提供无效的输入，这些输入可以是随机生成的，也可以是专门为触发已知的软件漏洞而设计的。然后，模糊测试人员会监控应用程序的性能，观察软件崩溃、缓冲区溢出或其他不期望的和/或不可预测的结果。有关模糊测试的更多信息，请参阅第 15 章。

1.4.1 识别威胁

可能的威胁几乎是无限的，所以使用结构化的方法来准确地识别相关的威胁是很重要的。例如，有些组织使用以下三种方法中的一种或多种：

关注资产 该方法以资产为中心，利用资产评估结果，试图识别对有价值资产的威胁。例如，可对特定资产进行评估，以确定它是否容易受到攻击。如果资产中承载数据，则可通过评估访问控制来识别能绕过身份验证或授权机制的威胁。

关注攻击者 有些组织能识别潜在攻击者，并能根据攻击者的目标识别代表的威胁。例如，政府通常能识别潜在的攻击者以及攻击者想要达到的目标。然后，可利用这些数据来识别和保护相关资产。这种方法面临的一个挑战是，可能会出现之前未视为威胁的新攻击者。

关注软件 如果组织开发了软件，就需要考虑针对软件的潜在威胁。虽然前几年组织一般不自己开发软件，但现今这样做已经非常普遍。具体来说，大多数组织都存在 Web 应用，许多组织都创建自己的 Web 页面。精美的网页会带来更多流量，但也需要更复杂的编程，并会带来更多威胁。

如果威胁被确定为攻击者(而不是自然威胁)，威胁建模将尝试识别攻击者可能想要达到的目标。有些攻击者可能想要禁用系统，而其他攻击者可能想要窃取数据。一旦这些威胁被识别出来，就可根据目标或动机进行分类。此外，通常将威胁与脆弱性结合起来，以识别能够利用脆弱性并对组织带来重大风险的威胁。威胁建模的最终目标是对危害组织有价值资产的潜在威胁进行优先级排序。

当尝试对威胁进行盘点和分类时，使用指南或参考通常很有帮助。微软开发了一种被称为 STRIDE 的威胁分类方案。STRIDE 通常用于评估对应用程序或操作系统的威胁。但是，它也可以在其他情况下应用。STRIDE 是以下单词的首字母缩写。

- **欺骗(Spoofing)：** 通过使用伪造的身份获得对目标系统访问权限的攻击行为。欺骗可用于 IP 地址、MAC 地址、用户名、系统名、无线网络服务集标识符(SSID)、电子邮件地址和其他许多类型的逻辑标识。当攻击者将他们的身份伪造成合法的或授权的实体时，他们通常能够绕过针对未经授访问的过滤器和封锁。一旦攻击者利用欺骗攻击成功获得对目标系统的访问权，就可以在随后发起攻击，包括滥用、数据窃取或权限升级。
- **篡改(Tampering)：** 对传输或存储中的数据进行任何未经授权的更改或操纵。篡改被用来伪造通信或改变静态信息。这种攻击破坏了完整性和可用性。

- **否认(Repudiation)**：用户或攻击者否认执行动作或活动的能力。通常，攻击者会否认攻击以保持合理的辩解，从而不对自己的行为负责。否认攻击还可能导致无辜的第三方因安全违规而受到指责。
- **信息泄露(Information Disclosure)**：将私有、机密或受控信息泄露或发送给外部或未经授权的实体。这些信息可能包括客户身份信息、财务信息或专有业务操作细节。信息泄露可利用系统设计和实现上的错误，如未删除的调试代码，遗留的示例应用程序和账户，未删除客户端可见内容的编程注释(如 HTML 文档中的注释)或将过于详细的错误信息展示给用户。
- **拒绝服务(DoS)**：该攻击试图阻止对资源的授权使用。这类攻击可通过利用缺陷、过载连接或爆发流量来进行。DoS 攻击不一定导致资源完全无法访问，而是会减低吞吐量或提高延迟，阻碍对资源的有效使用。虽然大多数 DoS 攻击带来的危害是临时性的，只有在攻击者实施攻击时存在，但也有一些 DoS 攻击带来的危害是长久性的。长久性 DoS 攻击可能包括对数据集的破坏，用恶意软件替换原有软件，或劫持可能被中断的固件闪存操作或安装有问题的固件。这些 DoS 攻击中的任何一种都会导致系统永久受损，无法通过简单的重启或通过等待攻击者结束攻击而恢复到正常操作。要从永久性 DoS 攻击中恢复，需要完整的系统修复和备份恢复。
- **特权提升(Elevation of Privilege)**：该攻击是将权限有限的用户账户转换为具有更大特权、权利和访问权限的账户。这类攻击可能通过窃取或利用高级账户的凭据来实现，例如管理员(administrator)或根用户(root)。特权提升攻击也包括攻击系统或应用程序，使权限有限的其他账户临时或永久地获得额外权限。

虽然 STRIDE 通常针对应用程序威胁，但也适用于其他情况，比如网络威胁和主机威胁。其他攻击可能比网络攻击和主机攻击更特别，例如嗅探和劫持网络、恶意软件以及主机的任意代码执行，不过 STRIDE 的六个威胁概念有相当广泛的应用。

攻击模拟和威胁分析(Process for Attack Simulation and Threat Analysis，PASTA)过程是一种由七个阶段构成(见图 1.7)的威胁建模方法。PASTA 方法是以风险为核心，旨在选择或开发与要保护的资产价值相关的防护措施。PASTA 的七个阶段如下。

- 阶段 1：为风险分析定义目标
- 阶段 2：定义技术范围(Definition of the Technical Scope，DTS)
- 阶段 3：分解和分析应用程序(Application Decomposition and Analysis，ADA)
- 阶段 4：威胁分析(Threat Analysis，TA)
- 阶段 5：弱点和脆弱性分析(Weakness and Vulnerability Analysis，WVA)
- 阶段 6：攻击建模与仿真(Attack Modeling & Simulation，AMS)
- 阶段 7：风险分析和管理(Risk Analysis & Management，RAM)

PASTA 的每个阶段都有该阶段需要完成的目标和交付物的特别目标清单。有关 PASTA 的更多信息，请参阅 Tony UcedaVelez 和 Marco M. Morana 撰写的书籍《以风险为中心的威胁建模：攻击模拟和威胁分析的过程》。你可在线阅读该书附录，可在 http://www.isaca.org/chapters5/Ireland/Documents/2013%20Presentations/PASTA%20Methodology%20Appendix%20-%20November%202013.pdf 上找到对 PASTA 的介绍。

Trike 是另一种基于风险的威胁建模方法，侧重于基于风险，而不是依赖于 STRIDE 和 DREAD(Disaster, Reproducibility, Exploitability, Affected Users and Discoverability，潜在破坏、可

再现性、可利用性、受影响用户和可发现性)中使用的聚合威胁模型。有关 DREAD 的讨论，见后面的“优先级排序和响应”一节)。Trike 提供了一种可靠的、可重复的安全审核方法。它还为安全工作人员之间的通信和协作提供了一致的框架。Trike 对每种资产的可接受风险水平进行评估，然后确定适当的风险响应行动。

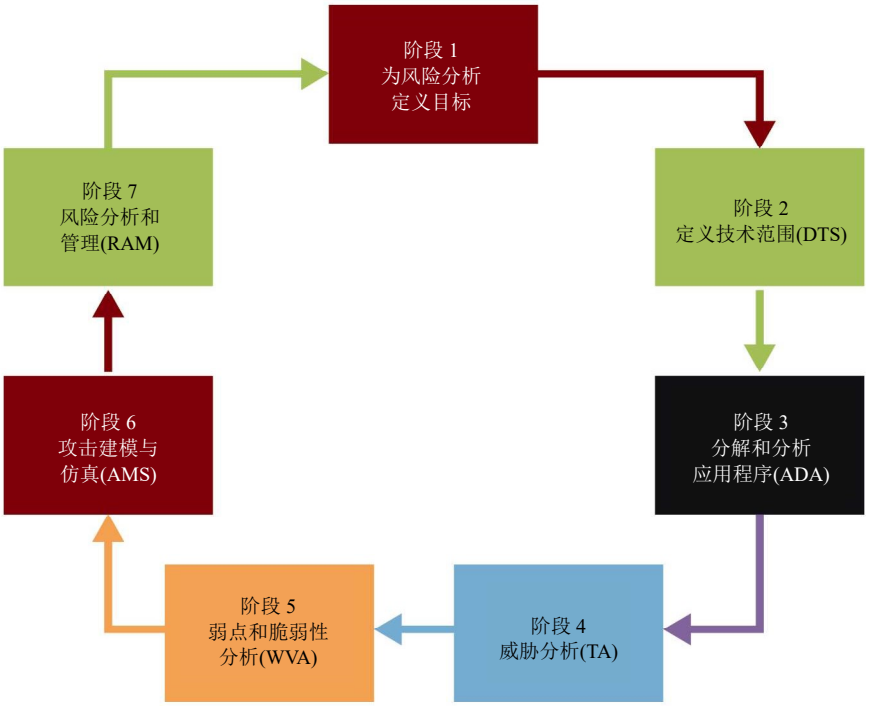

图 1.7　揭露威胁问题的图表示例

VAST(Visual, Agile, and Simple Threat，视觉、敏捷和简单威胁)是一种基于敏捷项目管理和编程原则的威胁建模概念。VAST 的目标是在可伸缩的基础上将威胁和风险管理集成到敏捷编程环境中。

上述这些只是由社区团体、商业组织、政府机构和国际协会提供的多种威胁建模概念和方法中的一小部分。

通常 STRIDE 和其他威胁建模方法的目的是考虑危害问题的范围，并关注攻击的目标或最终结果。尝试识别出每一种特定的攻击方法和技术是不可能完成的任务——因为新攻击不断出现。虽然仅能对攻击的目标或目的进行粗略分类和分组，但分类和分组保持相对稳定。

警惕个人威胁

竞争通常是企业成长的一个关键因素，但过度竞争会增加来自个人的威胁程度。除了恶意黑客和心怀不满的雇员，对手、承包商、员工甚至是值得信赖的合作伙伴都可能因为关系恶化而成为组织的威胁。

- 永远不要认为顾问或承包商对公司的忠诚度与长期员工一样高。承包商和顾问实际上就是雇佣兵，他们只为出价最高的人工作。也不要把员工的忠诚看成理所应当。如果对工作环境不满或觉得受到不公正待遇，员工可能试图进行报复。经济困难的雇员可能为自身利益考虑进行不道德和非法的活动，从而对企业造成威胁。

- 可信的合作伙伴仅仅是值得信赖的合作伙伴，只要你们彼此友好合作。如果最后的合作关系恶化或成为竞争对手，那么之前的合作伙伴可能会采取对组织业务构成威胁的行动。

组织的潜在威胁是多种多样的。公司面临着源于自然环境、技术和人员的威胁。大多数企业在防御威胁上关注了自然灾害和 IT 攻击，但考虑来自个人的潜在威胁同样重要。始终考虑组织的活动、决策和交互行为可能带来的最佳结果与最糟结果。识别威胁是设计防御以帮助减少或消除停机、危害和损失的第一步。

1.4.2　确定和绘制潜在的攻击

一旦对开发项目或部署的基础设施面临的威胁有所了解，威胁建模的下一步就是确定可能发生的潜在攻击。这通常通过创建事务中的元素图表及数据流和权限边界来完成(见图 1.8)。这是一个数据流的示意图，显示了系统的每个主要组件、安全区域之间的边界以及信息和数据的潜在流动或传输。通过为每个环境或系统制作这样的图表，可以更仔细地检查可能发生危害的每个关键点。

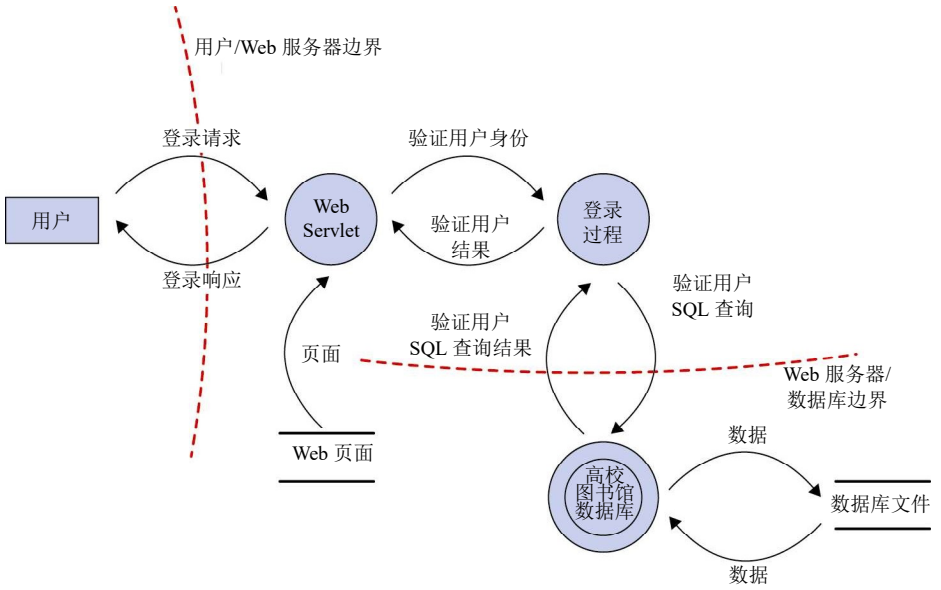

图 1.8　一个用图表来揭示威胁的例子

这种数据流图通过可视化表示，有助于更好地理解资源和数据流动之间的关系。绘制图表的过程也称为绘制架构图。创建图表有助于详细描述业务任务、开发过程或工作活动中的每个元素的功能和目的。重要的是要包括用户、处理器、应用程序、数据存储以及执行特定任务或操作需要的其他所有基本元素。这是高层次的概述而不是对编码逻辑的详细评估。但对于较复杂的系统，可能需要创建多个图表，关注不同的焦点并把细节进行不同层级的放大。

一旦绘制出图表，就要确定涉及的所有技术，包括操作系统、应用程序(基于网络服务和客户端)和协议。需要具体到使用的版本号和更新/补丁级别。

接下来，要确定针对图表中每个元素的攻击。请记住，要考虑到各种攻击类型，包括逻辑/

技术、物理和社会。例如，确保包括欺骗、篡改和社会工程。这个过程将引导你进入威胁建模的下一阶段：执行简化分析。

1.4.3 执行简化分析

威胁建模的下一步是执行简化分析。简化分析也称为分解应用程序、系统或环境。这项任务的目的是更好地理解产品的逻辑及其与外部元素的交互。无论应用程序、系统或整个环境，都需要划分为更小的容器或单元。如果关注的是软件、计算机或操作系统，那么这些可能是子程序、模块或客体；如果关注的是系统或网络，这些可能是协议。如果关注的是整个业务基础结构，这些可能是部门、任务和网络。为理解输入、处理、信息安全、数据管理、存储和输出，应该对每个已识别的子元素进行评估。

在分解过程中，必须确定五个关键概念：

信任边界 信任级别或安全级别发生变化的位置。

数据流路径 数据在两个位置之间的流动。

输入点 接收外部输入的位置。

特权操作 需要比标准用户账户或流程拥有更大特权的任何活动，通常需要修改系统或更改安全性。

安全声明和方法的细节 关于安全策略、安全基础和安全假设的声明。

将系统分解成各个组成部分能够更容易地识别每个元素的关键组件，并注意到脆弱性和攻击点。对程序、系统或环境的操作的了解越清楚，就越容易识别出针对它们的威胁。

1.4.4 优先级排序和响应

因为通过威胁建模过程识别出威胁，所以需要规定额外的活动来完成整个过程。下一步是全面记录这些威胁。在这个文档中，应该说明威胁的手段、目标和后果。要考虑完成开发所需的技术以及列出可能的控制措施和防护措施。

编制文档后，要对威胁进行排序或定级。可使用多种技术来完成这个过程，如“概率×潜在损失”排序、高/中/低评级或 DREAD 系统。

“概率×潜在损失”排序技术会生成一个代表风险严重性的编号。编号范围为 1~100，100 代表可能发生的最严重风险；初始值范围为 1~10，1 最低，10 最高。这些排名从某些程度上看有些武断和主观，但如果由同一个人或团队为组织指定数字，仍会产生相对准确的评估结果。

高/中/低评级过程更简单。从这三个优先级标签中为每个威胁指定一个优先级标签。被指定高优先级标签的威胁需要立即解决。被指定中优先级标签的威胁最终也要得到解决，但不需要立即采取行动。被指定低优先级的威胁可能会被解决，但若解决这类威胁对整个项目来说需要付出太多努力或费用，那么是否解决它们是可以选择的。

DREAD 评级系统旨在提供一种灵活的评级解决方案，它基于对每个威胁的五个主要问题的回答。

- **潜在破坏**：如果威胁成真，可能造成的伤害有多严重？
- **可再现性**：攻击者复现攻击有多复杂？
- **可利用性**：实施攻击的难度有多大？

- **受影响用户**：有多少用户可能受到攻击的影响(按百分比)?
- **可发现性**：攻击者发现弱点有多难?

通过询问上述问题及潜在的附加定制化问题，并为答案指定 H/M/L 或 3/2/1 值，就可以建立详细的威胁优先级表。

一旦确定了威胁优先级，就需要确定对这些威胁的响应。

要考虑解决威胁的技术和过程，并对成本与收益进行权衡。响应选项应该包括对软件体系结构进行调整、更改操作和流程以及实现防御性与探测性组件。

1.5　将基于风险的管理理念应用到供应链

将基于风险的管理理念应用到供应链是一种确保安全策略更加可靠与成功的手段，适合在所有规模的组织中运用。供应链的概念并非指单个实体，而是包括大多数计算机、设备、网络和系统。事实上，我们所知道的大多数电脑和设备制造公司——如 Dell、Cisco、Extreme Networks、Juniper、Asus、Acer 和 Apple——一般都是按每台电脑的组装形式生产，而不是生产所有单个部件。通常 CPU、内存、驱动控制器、硬盘驱动器、SSD 卡和显卡都由其他第三方供应商生产。即便是这些大型销售商，也不太可能自行开采金属、加工石油制成塑料或生产蚀刻芯片的硅。因此，任何已完成的系统都有一段漫长而复杂的历史，这也使得供应链得以存在。

安全供应链指的是供应链中的所有供应商或链接都是可靠的、值得信赖的、信誉良好的组织，他们向业务伙伴(尽管不一定向公众)披露他们的实践和安全需求。供应链中的每个环节都是可靠的，并对下一个环节负责。从原材料到精炼产品，从电子部件到计算机部件，再到成品的每一次交接都经过适当的组织、记录、管理和审核。安全供应链的目标是确保成品质量，满足性能和操作目标，并提供规定的安全机制。在这个过程中，没有任何伪造或遭受未经授权或恶意操纵或破坏的节点。有关供应链风险的其他观点，请参阅 NIST 的一个案例研究，位于 https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf。

如果在未考虑安全性的情况下进行收购和兼并，那么所收购产品的固有风险将在整个部署生命周期中一直存在。将收购元素的固有威胁最小化能减少安全管理成本，并可能减少安全违规。

评估与硬件、软件和服务相关的风险很重要。具有弹性集成安全性的产品和解决方案通常比那些没有安全基础的产品和解决方案更昂贵。然而，与满足不良设计产品安全需求的费用相比，这种额外的初始费用通常更具有成本效益。因此在考虑兼并/收购成本时，重要的是考虑产品部署的整个生命周期内的总成本，而不只是考虑初始购买和实施费用。

收购不仅涉及硬件和软件，也包括外包、与供应商签订合同、聘请顾问等内容。与外部实体协同工作时，集成的安全性评估与确保在产品设计时考虑了安全性同等重要。

许多情况下，可能需要持续的安全监控、管理和评估。这可能是行业最佳实践或监管要求。这种评估和共同监督可能在组织内部进行，也可由外部审计人员完成。当使用第三方评估和监控服务时，请记住，外部实体需要在其业务操作中体现出安全意识。如果外部组织无法在安全的基础上管理自身的内部操作，他们又将如何为你提供可靠的安全管理功能呢？

在为安全集成而评估第三方时，请考虑以下过程：

现场评估　到组织现场进行访谈，并观察工作人员的操作习惯。

文件交换和审查 调查数据和文件记录交换的方式，以及执行评估和审查的正式过程。

过程/策略审查 要求提供安全策略、过程/程序，以及事件和响应文件的副本以供审查。

第三方审计 根据美国注册会计师协会(AICPA)的定义，拥有独立的第三方审计机构可根据 SOC 报告，对实体的安全基础设施进行公正的审查。认证业务标准声明(SSAE)是一项规定，定义了服务组织如何使用各种 SOC 报告来报告合规性。自 2011 年 6 月 15 日起生效的 SSAE 16 版本在 2017 年 5 月 1 日被 SSAE 18 取代。为进行安全性评估，需要考虑 SOC 1 和 SOC 2 审计框架。SOC 1 审计侧重于根据安全机制的描述来评估其适用性。SOC 2 审计侧重于实现与可用性、安全性、完整性、隐私性和保密性相关的安全控制。有关 SOC 审计的更多信息，请参见 https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socguidesandpublications.html。

为所有收购设立最低限度的安全要求。这些要求应以现有安全策略为模板。新的硬件、软件或服务的安全需求应该始终满足或超过现有基础设施的安全性。在使用外部服务时，一定要检查服务水平协议(SLA)，确保服务合同中有关于安全的规定。这可能包括针对特定需求制定服务级别的细则。

以下是一些与并购整合的安全相关的优秀资源：

- “通过收购提高网络安全和弹性”。源于美国国防部和总务管理局的最终报告，发表于 2013 年 11 月(www.gsa.gov/portal/getMediaData?mediaId=185371)。
- NIST 的特别出版物 800-64 版本 2：“系统开发生命周期中的安全考虑”(http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf)。

1.6 本章小结

安全治理、安全管理和安全原则是安全策略和解决方案部署中的核心内容。它们定义了安全环境所需的基本参数及安全策略设计人员和系统实施人员为创建安全的解决方案必须实现的目标和宗旨。

安全的宗旨包含在 CIA 三元组中：保密性、完整性和可用性。这三项原则被认为是安全领域最重要的原则。它们对组织的重要性取决于组织的安全目标和需求以及环境中安全受到的威胁程度。

CIA 三元组的第一个原则是保密性，即不向未经授权的主体泄露客体信息。安全机制提供了保密性，即对防御未经授权的主体访问数据、客体或资源提供了高度保障。如果存在对保密性的威胁，就可能发生未经授权的泄露。

CIA 三元组的第二个原则是完整性，即客体保持真实性且只被授权的主体进行有目的的修改。如果安全机制提供了完整性，那么它就高度保证数据、客体和资源不会由最初的受保护状态转变到非保护状态。客体在存储、传输或过程中都不应遭受未经授权的更改。因此，保持完整性意味着客体本身不被未经授权地更改，且管理和操作客体的操作系统和程序实体不受破坏。

CIA 三元组的第三个原则是可用性，这意味着授权主体被授予了实时与不间断地访问客体的权限。安全机制提供了可用性，即提供了对数据、客体和资源可被授权主体访问的高度保障。可用性包括对客体的有效持续访问及抵御拒绝服务(DoS)攻击。可用性还意味着支撑性基础设施是可用的，并允许授权用户获得授权的访问。

在设计安全策略和部署安全解决方案时应该考虑和处理的其他与安全相关的概念和原则是

隐私、标识、身份验证、授权、问责制、不可否认性和审计。

安全解决方案概念和原则的另一块内容是保护机制：分层、抽象、数据隐藏和加密。保护机制是安全控制的共同特征。并不是所有的安全控制都必须具有这些机制，但是许多保护控制通过使用这些机制提供了保密性、完整性和可用性。

安全角色决定谁对组织资产的安全负责。担任高级管理者角色的人员对任何资产损失负有最终的职责和义务，并定义安全策略。安全专业人员负责实现安全策略，用户负责遵守安全策略。担任数据所有者角色的人员负责对信息进行分类，数据托管员负责维护安全环境和备份数据。审计人员负责确认安全环境是否恰当地保护资产。

规范化的安全策略结构由策略、标准/基线、指南和程序组成。这些独立文档是任何环境中安全设计和实现安全的基本元素。

变更控制或变更管理是安全管理的另一项重要内容。安全环境的变更可能引入漏洞、重叠、客体丢失和疏忽，进而导致出现新的脆弱性。不过，可通过系统的变更管理来维护安全。这通常涉及与安全控制和安全机制相关的活动，包括广泛的计划、测试、日志记录、审计和监控。然后对环境变化进行记录来识别变更发起者，无论变更发起者是客体、主体、程序、通信路径还是网络本身。

数据分类是基于数据的保密性、敏感性或秘密性需求而对其进行保护的主要手段。在设计和实现安全系统时，以相同的方式处理所有数据是低效的，因为有些数据项比其他数据项需要更高的安全性。用低级别安全保护所有内容意味着敏感数据很容易被访问。用高级别安全保护所有内容又过于昂贵，并且限制了对未分类的、非关键数据的访问。数据分类用于确定为保护数据和控制对数据的访问而分配多少精力、金钱和资源。

安全管理计划的一个重要方面是正确实施安全策略。为保证效果，安全管理必须采用自上而下方法，上层或高级管理者负责启动和定义组织的策略。安全策略为组织架构内的较低级别提供指导。中层管理人员负责将安全策略落实到标准、基线、指南和程序。操作管理人员或安全专业人员实现安全管理文档中规定的配置。最后，最终用户遵守组织的所有安全策略。

安全管理计划包括定义安全角色、制定安全策略、执行风险分析以及要求员工接受安全教育。这些职责以制定的管理计划为指导。安全管理团队应制定战略计划、战术计划和操作计划。

威胁建模是识别、分类和分析潜在威胁的安全过程。威胁建模可当作设计和开发期间的一种主动措施被执行，也可作为产品部署后的一种被动措施被执行。这两种情况下，威胁建模过程都识别了潜在危害、发生的可能性、关注的优先级以及消除(或减少)威胁的手段。

将基于风险的管理理念应用到供应链是一种确保安全策略更加可靠与成功的手段，适合在所有规模的组织中运用。如果在没有考虑安全性的情况下进行收购和兼并，那么所收购产品的固有风险将在整个部署生命周期中一直存在。

1.7　考试要点

理解由保密性、完整性和可用性组成的 CIA 三元组。保密性原则是指客体不会被泄露给未经授权的主体。完整性原则是指客体保持真实性且只被经过授权的主体进行有目的的修改。可用性原则指被授权的主体能实时和不间断地访问客体。了解这些原则为什么很重要，并了解支持它们的机制，以及针对每种原则的攻击和有效的控制措施。

能够解释身份标识是如何工作的。身份标识是下属部门承认身份和责任的过程。主体必须为系统提供标识，以便启动身份验证、授权和问责制的过程。

理解身份验证过程。身份验证是验证或测试声称的身份是否有效的过程。身份验证需要来自主体的信息，这些信息必须与指示的身份完全一致。

了解授权如何用于安全计划。一旦对主体进行了身份验证，就必须对其访问进行授权。授权过程确保所请求的活动或对象访问是可能的，前提是赋予已验证身份的权利和特权。

理解安全治理。安全治理是与支持、定义和指导组织安全工作相关的实践集合。

能够解释审计过程。审计(或监控追踪和记录)主体的操作，以便在验证过的系统中让主体为其行为负责。审计也对系统中未经授权的或异常的活动进行检测。需要实施审计来检测主体的恶意行为、尝试的入侵和系统故障，以及重构事件、提供起诉证据、生成问题报告和分析结果。

理解问责制的重要性。组织安全策略只有在有问责制的情况下才能得到适当实施。换句话说，只有在主体对他们的行为负责时，才能保持安全性。有效的问责制依赖于检验主体身份及追踪其活动的能力。

能够解释不可否认性。不可否认性确保活动或事件的主体不能否认事件的发生。它防止主体声称没有发送过消息、没有执行过动作或没有导致事件的发生。

理解安全管理计划。安全管理基于三种类型的计划：战略计划、战术计划和操作计划。战略计划是相对稳定的长期计划，它定义了组织的目的、任务和目标。战术计划是中期计划，为实现战略计划中设定的目标提供更多细节。操作计划是基于战略和战术计划的短期和高度详细的计划。

了解规范化安全策略结构的组成要素。要创建一个全面的安全计划，需要具备以下内容：安全策略、标准/基线、指南和程序。这些文件清楚地说明安全要求，并促使责任各方实施尽职审查。

了解关键的安全角色。主要的安全角色有高级管理者、组织所有者、上层管理人员、安全专业人员、用户、数据所有者、数据托管员和审计人员。通过创建安全角色的层次结构，可以全面限制风险。

了解如何实施安全意识培训。在进行实际培训前，必须使用户树立安全意识，此后就可以开始培训或教育员工去执行工作任务并遵守安全策略。所有新员工都需要一定程度的培训，以便他们遵守安全策略中规定的所有标准、指南和程序。教育是一项更细致的工作，学生/用户学习的内容远远超过他们完成实际工作所需要了解的内容。教育最常与身份验证考试或寻求工作晋升的用户关联。

了解分层防御如何简化安全。分层防御使用一系列控制中的多个控制。使用多层防御解决方案允许使用许多不同的控制措施来抵御威胁。

能够解释抽象的概念。抽象用于将相似的元素放入组、类或角色中，作为集合被指派安全控制、限制或许可。抽象增加了安全计划的实施效率。

理解数据隐藏。顾名思义，数据隐藏指将数据存放在主体无法访问或读取的逻辑存储空间以防数据被泄露或访问。数据隐藏通常是安全控制和编程中的关键元素。

理解加密的必要性。加密是对非预期的接收者隐藏通信的真实含义和意图的艺术与科学。加密有多种形式，适用于各种类型的电子通信，包括文本、音频和视频文件及应用程序。加密是安全控制中的重要内容，特别是在系统间传输数据时。

能够解释变更控制和变更管理的概念。安全环境的变更可能引入漏洞、重叠、客体丢失和疏忽，进而导致出现新的脆弱性。面对变更，维护安全的唯一途径就是系统性的变更管理。

了解为什么以及如何对数据进行分类。对数据进行分类是为将安全控制分配过程简化成分配给一组客体而不是单个客体。两个常见的分类方案是政府/军事分类和商业/私营部门分类。了解政府/军事分类方案的五个级别和商业/私营部门分类方案的四个分类级别。

理解解除分类的重要性。一旦资产不再被授权保护其当前指定的分类或敏感级别，就需要解除分类。

了解 COBIT 的基础知识。COBIT 是一种安全控制基础架构，用于为企业制定复合的安全解决方案。

了解威胁建模的基础知识。威胁建模是识别、分类和分析潜在威胁的安全过程。威胁建模可当成设计和开发期间的一种主动措施执行，也可作为产品部署后的一种被动措施执行。关键概念包括资产/攻击者/软件、STRIDE、PASTA、Trike、VAST、图表、简化/分解和 DREAD。

理解将基于风险的管理理念应用于供应链的必要性。将基于风险的管理理念应用到供应链中，可确保所有规模的组织都具有更加可靠和成功的安全策略。若收购时未考虑安全因素，这些产品的固有风险在整个部署生命周期中都存在。

1.8　书面实验

1. 讨论和描述 CIA 三元组。
2. 要求某人对其用户账户的行为负责的要求是什么？
3. 描述变更控制管理的好处。
4. 实施分类计划的七个主要步骤或阶段是什么？
5. 请说出$(ISC)^2$为 CISSP 定义的六个主要安全角色名称。
6. 完整的组织安全策略由哪四个组成部分？其基本目的是什么？

1.9　复习题

1. 下列哪一项是安全的主要目标？
   A. 网络的边界范围
   B. CIA 三元组
   C. 独立系统
   D. 互联网
2. 对脆弱性和风险的评估基于以下哪种威胁？
   A. CIA 三元组的一个或多个原则
   B. 数据有效性
   C. 应尽关心
   D. 尽责程度

3. 下列哪一项是 CIA 三元组中的原则，代表授权主体被授予及时和不间断地访问客体的权限？

A. 标识
B. 可用性
C. 加密
D. 分层防御

4. 下列哪一项不被视为违反保密性？

A. 窃取密码
B. 窃听
C. 破坏硬件
D. 社会工程

5. 下列哪一项是不正确的？

A. 保密性的违反包括人为错误。
B. 保密性的违反包括管理监督。
C. 保密性的违反仅限于直接的故意攻击。
D. 当传输没有正确加密时可能发生违反保密性的情况。

6. STRIDE 常用于评估对应用程序或操作系统的威胁。下列哪一项不是 STRIDE 的元素？

A. 欺骗
B. 特权提升
C. 否认
D. 泄露

7. 如果安全机制提供了可用性，它就提供了高度保障，授权的主体可以 _____数据、客体和资源。

A. 控制
B. 审计
C. 访问
D. 否认

8. _____指对个人身份信息或可能对他人造成伤害、令他人感到尴尬的信息加以保密。

A. 隔绝
B. 隐藏
C. 隐私
D. 关键性

9. 对于所有受影响的个人，除了下列哪一项之外，个人都有知情权？

A. 限制个人电子邮件
B. 录音电话交谈
C. 收集有关上网习惯的信息
D. 用于保存电子邮件的备份机制

10. 数据分类管理的什么元素可覆盖所有其他形式的访问控制？
    A. 分类
    B. 物理访问
    C. 管理员职责
    D. 获得所有权
11. 以下哪一项确保活动或事件的主体不能否认事件的发生？
    A. CIA 三元组
    B. 抽象
    C. 不可否认性
    D. 散列值
12. 以下哪个概念相对于分层安全是最重要和最特别的？
    A. 多层
    B. 串行
    C. 并行
    D. 过滤
13. 下列哪一项不是数据隐藏的例子？
    A. 防止授权的客体阅读者删除客体
    B. 防止未经授权的访问者访问数据库
    C. 限制较低分类级别的主体访问较高分类级别的数据
    D. 阻止应用程序直接访问硬件
14. 变更管理的主要目标是什么？
    A. 维护文档
    B. 使用户得到变更通知
    C. 允许失败的变更进行回滚
    D. 防止安全危害
15. 数据分类方案的主要目标是什么？
    A. 控制授权主体对客体的访问。
    B. 根据指定的重要性和敏感性标签，对数据进行程序化和分层的保护过程。
    C. 为问责制建立事务跟踪。
    D. 为操作访问控制提供最有效的方法来授予或限制功能。
16. 对数据进行分类时，通常不考虑下列哪一项特征？
    A. 价值
    B. 客体的大小
    C. 可用的生命周期
    D. 对国家安全的影响
17. 两种常见的数据分类方案是什么？
    A. 政府/军事分类方案和商业/私营部门分类方案
    B. 个人和政府
    C. 私营部门和非限制性部门
    D. 已分类和未分类

18. 对于已分类的数据，下列哪一项是最低的军事数据分类级别？
   A. 敏感
   B. 机密
   C. 专有
   D. 私有
19. 商业/私营部门的哪个数据分类级别用于控制组织内的个人信息？
   A. 机密
   B. 私有
   C. 敏感
   D. 专有
20. 数据分类可用在除哪一项之外的所有安全控制中？
   A. 存储
   B. 处理
   C. 分层
   D. 传输