

CISSP认证考试指南



[CISSP认证考试指南_下载链接1](#)

著者:[美]Shon Harris

出版者:清华大学出版社

出版时间:2011-10

装帧:平装

isbn:9787302269809

《CISSP认证考试指南(第5版)》提供最新最全的资源，涵盖通过CISSP(Certified Information Systems Security Professional，信息系统安全专家认证)考试所需的全部信息，内容涉及(ISC)2(International Information Systems Security Certification Consortium，国际信息系统安全认证协会)规定的10个考试领域。本书在每一章开头都明确学习目标，随后提供考试提示、练习题和深入的解释。本书不仅能够帮助您通过CISSP考试，也是您工作中不可缺少的参考资料。

作者介绍:

Shon Harris是CISSP、Logical Security总裁、安全顾问、美国空军信息战部门的前任工程师、技术总监和作者。她是两本CISSP畅销书的作者，并且与其他人合著了Hacker's Challenge: Test Your

Incident Response Skills Using 20 Scenarios和Gray Hat Hacking: The Ethical Hacker's Handbook(均由McGraw-Hill出版社出版)。Shon曾为众多客户提供计算机和信息安全服务,包括RSA、美国国防部、美国能源部、美国国家安全局(NSA)、美国银行、美国国防信息系统局(DISA)、BMC、西点军校等。Information Security Magazine认为Shon是信息安全领域最杰出的25位女性之一。

目录: 第1章 成为一名CISSP 1

1.1 成为CISSP的理由 1

1.2 CISSP考试 2

1.3 CISSP认证的发展简史 6

1.4 如何成为一名CISSP 6

1.5 本书概要 7

1.6 CISSP应试小贴士 7

1.7 本书使用指南 8

1.7.1 问题 9

1.7.2 答案 12

第2章 计算机安全的发展趋势 13

2.1 安全已成为一个难题 13

2.2 安全所涉及的领域 15

2.3 信息战 16

2.3.1 黑客活动的最新进展 17

2.3.2 信息安全对国家的影响 19

2.3.3 信息安全对公司的影响 20

2.3.4 美国政府的相关行动 22

2.4 政治和法律 24

2.5 黑客与攻击 26

2.6 管理 27

2.7 分层模式 29

2.7.1 结构化分析方法 30

2.7.2 遗漏的一层 30

2.7.3 将所有的层结合在一起 31

2.8 教育 31

2.9 小结 32

第3章 信息安全与风险管理 33

3.1 安全管理 33

3.1.1 安全管理职责 34

3.1.2 自顶而下的安全方式 35

3.2 安全管理与支持控制 35

3.2.1 安全的基本原则 37

3.2.2 可用性 37

3.2.3 完整性 38

3.2.4 机密性 38

3.2.5 安全定义 39

3.2.6 通过隐匿实现安全 40

3.3 组织化安全模型 41

3.4 信息风险管理 52

3.4.1 谁真正了解风险管理 52

3.4.2 信息风险管理策略 53

3.4.3 风险管理团队 53

3.5 风险分析 54

3.5.1 风险分析团队 55

3.5.2 信息和资产的价值 55

3.5.3 构成价值的成本 56

- 3.5.4 识别威胁 56
- 3.5.5 失效和故障分析 59
- 3.5.6 定量风险分析 61
- 3.5.7 定性风险分析 65
- 3.5.8 定量与定性的对比 66
- 3.5.9 保护机制 67
- 3.5.10 综合考虑 70
- 3.5.11 总风险与剩余风险 70
- 3.5.12 处理风险 71
- 3.6 策略、措施、标准、基准和指导原则 72
- 3.6.1 安全策略 73
- 3.6.2 标准 75
- 3.6.3 基准 75
- 3.6.4 指导原则 76
- 3.6.5 措施 76
- 3.6.6 实施 77
- 3.7 信息分类 77
- 3.7.1 私有企业与军事机构的分类比较 78
- 3.7.2 分类控制 80
- 3.8 责任分层 81
- 3.8.1 涉及的人员 81
- 3.8.2 数据所有者 87
- 3.8.3 数据看管员 87
- 3.8.4 系统所有者 87
- 3.8.5 安全管理员 88
- 3.8.6 安全分析员 88
- 3.8.7 应用程序所有者 88
- 3.8.8 监督员 88
- 3.8.9 变更控制分析员 88
- 3.8.10 数据分析员 88
- 3.8.11 过程所有者 89
- 3.8.12 解决方案提供商 89
- 3.8.13 用户 89
- 3.8.14 生产线经理 89
- 3.8.15 审计员 89
- 3.8.16 为何需要这么多角色 90
- 3.8.17 员工 90
- 3.8.18 结构 90
- 3.8.19 招聘实践 91
- 3.8.20 雇员控制 92
- 3.8.21 解雇 93
- 3.9 安全意识培训 93
- 3.9.1 各种类型的安全意识培训 93
- 3.9.2 计划评估 94
- 3.9.3 专门的安全培训 95
- 3.10 小结 95
- 3.11 快速提示 96
- 3.11.1 问题 98
- 3.11.2 答案 103
- 第4章 访问控制 107
- 4.1 访问控制概述 107
- 4.2 安全原则 108

- 4.2.1 可用性 108
- 4.2.2 完整性 109
- 4.2.3 机密性 109
- 4.3 身份标识、身份验证、授权与可问责性 109
 - 4.3.1 身份标识与身份验证 111
 - 4.3.2 密码管理 119
 - 4.3.3 授权 137
- 4.4 访问控制模型 148
 - 4.4.1 自主访问控制 149
 - 4.4.2 强制访问控制 149
 - 4.4.3 角色型访问控制 151
- 4.5 访问控制方法和技术 153
 - 4.5.1 规则型访问控制 153
 - 4.5.2 限制性用户接口 154
 - 4.5.3 访问控制矩阵 154
 - 4.5.4 内容相关访问控制 155
 - 4.5.5 上下文相关访问控制 156
- 4.6 访问控制管理 156
 - 4.6.1 集中式访问控制管理 157
 - 4.6.2 分散式访问控制管理 162
- 4.7 访问控制方法 162
 - 4.7.1 访问控制层 163
 - 4.7.2 行政管理性控制 163
 - 4.7.3 物理性控制 164
 - 4.7.4 技术性控制 165
- 4.8 访问控制类型 167
 - 4.8.1 预防：行政管理方面 169
 - 4.8.2 预防：物理方面 169
 - 4.8.3 预防：技术方面 169
- 4.9 可问责性 171
 - 4.9.1 审计信息的检查 172
 - 4.9.2 击键监控 173
 - 4.9.3 保护审计数据和日志信息 173
- 4.10 访问控制实践 173
- 4.11 访问控制监控 176
 - 4.11.1 入侵检测 176
 - 4.11.2 入侵防御系统 183
- 4.12 对访问控制的几种威胁 184
 - 4.12.1 字典攻击 185
 - 4.12.2 蛮力攻击 185
 - 4.12.3 登录欺骗 186
- 4.13 小结 189
- 4.14 快速提示 189
 - 4.14.1 问题 191
 - 4.14.2 答案 196
- 第5章 安全体系结构和设计 199
 - 5.1 计算机体系结构 200
 - 5.2 中央处理单元 201
 - 5.2.1 多重处理 204
 - 5.2.2 操作系统体系结构 205
 - 5.2.3 进程活动 210
 - 5.2.4 存储器管理 211

- 5.2.5 存储器类型 213
- 5.2.6 虚拟存储器 219
- 5.2.7 CPU模式和保护环 220
- 5.2.8 操作系统体系结构 221
- 5.2.9 域 222
- 5.2.10 分层和数据隐藏 223
- 5.2.11 术语的演变 224
- 5.2.12 虚拟机 225
- 5.2.13 其他存储设备 226
- 5.2.14 输入/输出设备管理 227
- 5.3 系统体系结构 229
 - 5.3.1 预定义的主体和客体子集 230
 - 5.3.2 可信计算基 231
 - 5.3.3 安全周边 233
 - 5.3.4 引用监控器和安全内核 233
 - 5.3.5 安全策略 234
 - 5.3.6 最小特权 235
- 5.4 安全模型 235
 - 5.4.1 状态机模型 236
 - 5.4.2 Bell-LaPadula模型 238
 - 5.4.3 Biba模型 240
 - 5.4.4 Clark-Wilson模型 241
 - 5.4.5 信息流模型 243
 - 5.4.6 无干扰模型 245
 - 5.4.7 格子模型 246
 - 5.4.8 Brewer and Nash模型 247
 - 5.4.9 Graham-Denning模型 248
 - 5.4.10 Harrison-Ruzzo-Ullman模型 248
- 5.5 运行安全模式 249
 - 5.5.1 专用安全模式 249
 - 5.5.2 系统高安全模式 250
 - 5.5.3 分隔安全模式 250
 - 5.5.4 多级安全模式 250
 - 5.5.5 信任与保证 251
- 5.6 系统评估方法 252
 - 5.6.1 对产品进行评估的原因 252
 - 5.6.2 橘皮书 253
- 5.7 橘皮书与彩虹系列 256
- 5.8 信息技术安全评估准则 258
- 5.9 通用准则 260
- 5.10 认证与鉴定 261
 - 5.10.1 认证 263
 - 5.10.2 鉴定 263
- 5.11 开放系统与封闭系统 264
 - 5.11.1 开放系统 264
 - 5.11.2 封闭系统 264
- 5.12 企业体系结构 264
- 5.13 一些对安全模型和体系结构的威胁 270
 - 5.13.1 维护陷阱 271
 - 5.13.2 检验时间/使用时间攻击 271

5.13.3 缓冲区溢出	272
5.14 小结	276
5.15 快速提示	276
5.15.1 问题	279
5.15.2 答案	282
第6章 物理和环境安全	285
6.1 物理安全简介	285
6.2 规划过程	287
6.2.1 通过环境设计来 预防犯罪	290
6.2.2 制订物理安全计划	294
6.3 保护资产	304
6.4 内部支持系统	305
6.4.1 电力	305
6.4.2 环境问题	309
6.4.3 通风	311
6.4.4 火灾的预防、检测 和扑灭	311
6.5 周边安全	317
6.5.1 设施访问控制	318
6.5.2 人员访问控制	325
6.5.3 外部边界保护机制	325
6.5.4 入侵检测系统	332
6.5.5 巡逻警卫和保安	334
6.5.6 安全狗	335
6.5.7 对物理访问进行审计	335
6.5.8 测试和演习	335
6.6 小结	336
6.7 快速提示	336
6.7.1 问题	338
6.7.2 答案	342
第7章 通信与网络安全	345
7.1 开放系统互连参考模型	346
7.1.1 协议	347
7.1.2 应用层	349
7.1.3 表示层	350
7.1.4 会话层	350
7.1.5 传输层	351
7.1.6 网络层	353
7.1.7 数据链路层	353
7.1.8 物理层	355
7.1.9 OSI模型中的功能 和协议	355
7.1.10 综合这些层	357
7.2 TCP/IP	357
7.2.1 TCP	358
7.2.2 IP寻址	362
7.2.3 IPv6	364
7.3 传输的类型	365
7.3.1 模拟和数字	365
7.3.2 异步和同步	366
7.3.3 宽带和基带	367
7.4 LAN网络互联	367
7.4.1 网络拓扑	368

- 7.4.2 LAN介质访问技术 370
- 7.4.3 布线 375
- 7.4.4 传输方法 379
- 7.4.5 介质访问技术 380
- 7.4.6 LAN协议 382
- 7.5 路由协议 386
- 7.6 网络互联设备 389
 - 7.6.1 中继器 389
 - 7.6.2 网桥 389
 - 7.6.3 路由器 391
 - 7.6.4 交换机 392
 - 7.6.5 网关 396
 - 7.6.6 PBX 397
 - 7.6.7 防火墙 398
 - 7.6.8 蜜罐 411
 - 7.6.9 网络分隔与隔离 411
- 7.7 网络互联服务和协议 412
 - 7.7.1 域名服务 412
 - 7.7.2 目录服务 416
 - 7.7.3 轻量级目录访问协议 417
 - 7.7.4 网络地址转换 418
- 7.8 内联网与外联网 419
- 7.9 城域网 420
- 7.10 广域网 422
 - 7.10.1 通信的发展 422
 - 7.10.2 专用链路 424
 - 7.10.3 WAN技术 426
- 7.11 远程访问 440
 - 7.11.1 拨号和RAS 440
 - 7.11.2 ISDN 441
 - 7.11.3 DSL 442
 - 7.11.4 线缆调制解调器 443
 - 7.11.5 VPN 443
 - 7.11.6 身份验证协议 449
 - 7.11.7 远程访问指导原则 450
- 7.12 无线技术 451
 - 7.12.1 无线通信 451
 - 7.12.2 WLAN组件 453
 - 7.12.3 无线标准 455
 - 7.12.4 WAP 463
 - 7.12.5 i-Mode 464
 - 7.12.6 移动电话安全 464
 - 7.12.7 WLAN战争驾驶攻击 466
 - 7.12.8 卫星 466
 - 7.12.9 3G无线通信 467
- 7.13 rootkit 469
 - 7.13.1 间谍软件和广告软件 470
 - 7.13.2 即时通信 470
- 7.14 小结 471
- 7.15 快速提示 471
 - 7.15.1 问题 474
 - 7.15.2 答案 477
- 第8章 密码术 481
 - 8.1 密码术的历史 482

- 8.2 密码术定义与概念 486
 - 8.2.1 Kerckhoffs原则 488
 - 8.2.2 密码系统的强度 488
 - 8.2.3 密码系统的服务 488
 - 8.2.4 一次性密码本 490
 - 8.2.5 滚动密码与隐藏密码 491
 - 8.2.6 隐写术 492
- 8.3 密码的类型 494
 - 8.3.1 替代密码 494
 - 8.3.2 换位密码 495
- 8.4 加密的方法 496
 - 8.4.1 对称算法与非对称算法 497
 - 8.4.2 对称密码术 497
 - 8.4.3 分组密码与流密码 501
 - 8.4.4 混合加密方法 504
- 8.5 对称系统的类型 509
 - 8.5.1 数据加密标准 509
 - 8.5.2 三重DES 515
 - 8.5.3 高级加密标准 515
 - 8.5.4 国际数据加密算法 516
 - 8.5.5 Blowfish 516
 - 8.5.6 RC4 516
 - 8.5.7 RC5 516
 - 8.5.8 RC6 516
- 8.6 非对称系统的类型 517
 - 8.6.1 Diffie-Hellman算法 517
 - 8.6.2 RSA 519
 - 8.6.3 El Gamal 521
 - 8.6.4 椭圆曲线密码系统 521
 - 8.6.5 LUC 522
 - 8.6.6 背包算法 522
 - 8.6.7 零知识证明 522
- 8.7 消息完整性 523
 - 8.7.1 单向散列 523
 - 8.7.2 各种散列算法 527
 - 8.7.3 针对单向散列函数的攻击 529
 - 8.7.4 数字签名 530
 - 8.7.5 数字签名标准 532
- 8.8 公钥基础设施 532
 - 8.8.1 认证授权机构 533
 - 8.8.2 证书 535
 - 8.8.3 注册授权机构 535
 - 8.8.4 PKI步骤 535
- 8.9 密钥管理 537
 - 8.9.1 密钥管理原则 538
 - 8.9.2 密钥和密钥管理的规则 539
- 8.10 链路加密与端对端加密 539
- 8.11 电子邮件标准 541
 - 8.11.1 多用途Internet邮件扩展(MIME) 541
 - 8.11.2 保密增强邮件 542
 - 8.11.3 消息安全协议 542
 - 8.11.4 可靠加密 542

- 8.11.5 量子密码术 543
- 8.12 Internet安全 545
- 8.13 攻击 553
 - 8.13.1 唯密文攻击 554
 - 8.13.2 已知明文攻击 554
 - 8.13.3 选定明文攻击 554
 - 8.13.4 选定密文攻击 554
 - 8.13.5 差分密码分析 555
 - 8.13.6 线性密码分析 555
 - 8.13.7 旁路攻击 555
 - 8.13.8 重放攻击 556
 - 8.13.9 代数攻击 556
 - 8.13.10 分析式攻击 556
 - 8.13.11 统计式攻击 556
- 8.14 小结 556
- 8.15 快速提示 557
 - 8.15.1 问题 559
 - 8.15.2 答案 563
- 第9章 业务连续性与灾难恢复 565
 - 9.1 业务连续性与灾难恢复 565
 - 9.1.1 业务连续性步骤 567
 - 9.1.2 将业务连续性计划作为安全策略和纲要的一部分 568
 - 9.1.3 项目起始阶段 569
 - 9.2 业务连续性规划要求 571
 - 9.2.1 业务影响分析 571
 - 9.2.2 预防性措施 576
 - 9.2.3 恢复战略 577
 - 9.2.4 业务流程恢复 578
 - 9.2.5 设施恢复 578
 - 9.2.6 供给和技术恢复 583
 - 9.2.7 终端用户环境 587
 - 9.2.8 数据备份选择方案 587
 - 9.2.9 电子备份解决方案 589
 - 9.2.10 选择软件备份设施 591
 - 9.2.11 保险 593
 - 9.2.12 恢复与还原 594
 - 9.2.13 为计划制定目标 597
 - 9.2.14 实现战略 598
 - 9.2.15 测试和审查计划 599
 - 9.2.16 维护计划 602
 - 9.3 小结 604
 - 9.4 快速提示 605
 - 9.4.1 问题 606
 - 9.4.2 答案 611
- 第10章 法律、法规、遵从和调查 613
 - 10.1 计算机法律的方方面面 613
 - 10.2 计算机犯罪法律的关键点 614
 - 10.3 网络犯罪的复杂性 616
 - 10.3.1 电子资产 617
 - 10.3.2 攻击的演变 617
 - 10.3.3 发生在不同国家的

- 计算机犯罪 619
- 10.3.4 法律的类型 620
- 10.4 知识产权法 624
 - 10.4.1 商业秘密 624
 - 10.4.2 版权 624
 - 10.4.3 商标 625
 - 10.4.4 专利 625
 - 10.4.5 知识产权的内部保护 626
 - 10.4.6 软件盗版 626
- 10.5 隐私 627
- 10.6 义务及其后果 633
 - 10.6.1 个人信息 636
 - 10.6.2 黑客入侵 636
- 10.7 调查 637
 - 10.7.1 事故响应 637
 - 10.7.2 事故响应措施 640
 - 10.7.3 计算机取证和适当的证据收集 643
 - 10.7.4 国际计算机证据组织 643
 - 10.7.5 动机、机会和方式 644
 - 10.7.6 计算机犯罪行为 644
 - 10.7.7 事故调查员 645
 - 10.7.8 取证调查过程 646
 - 10.7.9 法庭上可接受的证据 650
 - 10.7.10 监视、搜索和查封 652
 - 10.7.11 访谈和审讯 653
 - 10.7.12 几种不同类型的攻击 653
- 10.8 道德 655
 - 10.8.1 计算机道德协会 656
 - 10.8.2 Internet体系结构研究委员会 657
 - 10.8.3 企业道德计划 658
- 10.9 总结 658
- 10.10 快速提示 659
 - 10.10.1 问题 661
 - 10.10.2 答案 664
- 第11章 应用程序安全 667
 - 11.1 软件的重要性 667
 - 11.2 何处需要安全 668
 - 11.3 不同的环境需要不同的安全 669
 - 11.4 环境与应用程序 670
 - 11.5 功能的复杂性 670
 - 11.6 数据的类型、格式与长度 670
 - 11.7 实现和默认配置问题 671
 - 11.8 故障状态 672
 - 11.9 数据库管理 672
 - 11.9.1 数据库管理软件 673
 - 11.9.2 数据库模型 674
 - 11.9.3 数据库编程接口 678
 - 11.9.4 关系数据库组件 679
 - 11.9.5 完整性 682
 - 11.9.6 数据库安全问题 683
 - 11.9.7 数据仓库与数据挖掘 687

- 11.10 系统开发 689
 - 11.10.1 开发管理 690
 - 11.10.2 生命周期的不同阶段 690
 - 11.10.3 软件开发方法 700
 - 11.10.4 计算机辅助软件工程 702
 - 11.10.5 原型开发 702
 - 11.10.6 安全设计方法 702
 - 11.10.7 安全开发方法 703
 - 11.10.8 安全测试 703
 - 11.10.9 变更控制 704
 - 11.10.10 能力成熟度模型 705
 - 11.10.11 软件托管 706
- 11.11 应用程序开发方法学 706
- 11.12 面向对象概念 708
 - 11.12.1 多态 713
 - 11.12.2 数据建模 714
 - 11.12.3 软件体系结构 714
 - 11.12.4 数据结构 715
 - 11.12.5 内聚和耦合 715
- 11.13 分布式计算 716
 - 11.13.1 CORBA与ORB 716
 - 11.13.2 COM与DCOM 718
 - 11.13.3 企业JavaBeans 719
 - 11.13.4 对象链接和嵌入 720
 - 11.13.5 分布式计算环境 720
- 11.14 专家系统和知识性系统 721
- 11.15 人工神经网络 723
- 11.16 Web安全 724
 - 11.16.1 故意破坏 725
 - 11.16.2 金融欺诈 725
 - 11.16.3 特权访问 725
 - 11.16.4 窃取交易信息 725
 - 11.16.5 窃取知识产权 725
 - 11.16.6 拒绝服务(DoS)攻击 726
 - 11.16.7 建立质量保证流程 726
 - 11.16.8 安装Web应用程序防火墙 726
 - 11.16.9 安装入侵防御系统 726
 - 11.16.10 在防火墙上实现SYN代理 726
 - 11.16.11 针对Web环境的特定威胁 727
- 11.17 移动代码 734
 - 11.17.1 Java applet 734
 - 11.17.2 ActiveX控件 736
 - 11.17.3 恶意软件 737
 - 11.17.4 防病毒软件 741
 - 11.17.5 垃圾邮件检测 744
 - 11.17.6 防恶意软件程序 744
- 11.18 补丁管理 745
 - 11.18.1 步骤1: 基础设施 745
 - 11.18.2 步骤2: 研究 746

- 11.18.3 步骤3: 评估和测试 746
- 11.18.4 步骤4: 缓解(“回滚”) 746
- 11.18.5 步骤5: 部署(“首次展示”) 746
- 11.18.6 步骤6: 确证、报告和日志记录 746
- 11.18.7 补丁管理的限制 747
- 11.18.8 最佳实践 747
- 11.18.9 其他注意事项 747
- 11.18.10 攻击 747
- 11.19 小结 751
- 11.20 快速提示 751
- 11.20.1 问题 754
- 11.20.2 答案 757
- 第12章 操作安全 759
- 12.1 操作部门的角色 759
- 12.2 行政管理 760
- 12.2.1 安全和网络人员 762
- 12.2.2 可问责性 763
- 12.2.3 阈值级别 763
- 12.3 保证级别 764
- 12.4 操作责任 764
- 12.4.1 不寻常或无法解释的事件 765
- 12.4.2 偏离标准 765
- 12.4.3 不定期的初始程序加载(也称为重启) 765
- 12.4.4 资产标识和管理 765
- 12.4.5 系统控制 766
- 12.4.6 可信恢复 766
- 12.4.7 输入与输出控制 768
- 12.4.8 系统强化 769
- 12.4.9 远程访问安全 770
- 12.5 配置管理 771
- 12.5.1 变更控制过程 772
- 12.5.2 变更控制文档化 773
- 12.6 介质控制 774
- 12.7 数据泄漏 778
- 12.8 网络和资源可用性 779
- 12.8.1 平均故障间隔时间(MTBF) 780
- 12.8.2 平均修复时间(MTTR) 781
- 12.8.3 单点失败 781
- 12.8.4 备份 788
- 12.8.5 应急计划 790
- 12.9 大型机 791
- 12.10 电子邮件安全 792
- 12.10.1 电子邮件的工作原理 793
- 12.10.2 传真安全 796
- 12.10.3 黑客和攻击方法 797
- 12.11 脆弱性测试 803

12.11.1 渗透测试 806
12.11.2 战争拨号攻击 808
12.11.3 其他脆弱性类型 809
12.11.4 事后检查 811
12.12 小结 812
12.13 快速提示 812
12.13.1 问题 813
12.13.2 答案 818
附录A 安全内容自动化协议综述 821
附录B 配套光盘使用指南 827
术语表 831
· · · · · (收起)

[CISSP认证考试指南_下载链接1_](#)

标签

信息安全

CISSP认证

cissp

认证考试

计算机

网络安全

互联网

it.m.cissp

评论

读的第七版第一遍，试题翻译的很烂。内容还不错，穿插着各种比喻，示例，非常易懂

o

大半年时间，终于啃完了。感觉像用信息安全的观点重读了一遍大学。是所有企业IT人员必读的一本书，收获非常大！

原版很赞，但是翻译的像一坨……，

[CISSP认证考试指南_下载链接1](#)

书评

由IT安全认证和培训方面的顶级专家Shon Harris执笔，是亚马孙畅销书《CISSP认证考试指南(第4版)》的又一升级版，它对上一版做了全面更新，可以帮助读者顺利通过CISSP考试 附光盘： 数百道练习题及答案 作者的培训视频教程 完整的原版电子书

由IT安全认证和培训方面的顶级专家Shon Harris执笔，是亚马孙畅销书《CISSP认证考试指南(第4版)》的又一升级版，它对上一版做了全面更新，可以帮助读者顺利通过CISSP考试 附光盘： 数百道练习题及答案 作者的培训视频教程 完整的原版电子书

由IT安全认证和培训方面的顶级专家Shon Harris执笔，是亚马孙畅销书《CISSP认证考试指南(第4版)》的又一升级版，它对上一版做了全面更新，可以帮助读者顺利通过CISSP考试 附光盘： 数百道练习题及答案 作者的培训视频教程 完整的原版电子书

由IT安全认证和培训方面的顶级专家Shon Harris执笔，是亚马孙畅销书《CISSP认证考试指南(第4版)》的又一升级版，它对上一版做了全面更新，可以帮助读者顺利通过CISSP考试 附光盘： 数百道练习题及答案 作者的培训视频教程 完整的原版电子书

由IT安全认证和培训方面的顶级专家Shon Harris执笔，是亚马孙畅销书《CISSP认证考试指南(第4版)》的又一升级版，它对上一版做了全面更新，可以帮助读者顺利通过CISSP考试 附光盘： 数百道练习题及答案 作者的培训视频教程 完整的原版电子书

由IT安全认证和培训方面的顶级专家Shon Harris执笔，是亚马孙畅销书《CISSP认证考试指南(第4版)》的又一升级版，它对上一版做了全面更新，可以帮助读者顺利通过CISSP考试 附光盘： 数百道练习题及答案 作者的培训视频教程 完整的原版电子书

[CISSP认证考试指南_下载链接1](#)