

<<CISSP认证考试指南(第6版)>>

图书基本信息

书名：<<CISSP认证考试指南(第6版)>>

13位ISBN编号：9787302344407

10位ISBN编号：730234440X

出版时间：2014-1

出版时间：清华大学出版社

作者：哈里斯(Shon Harris)

译者：张胜生,张博,付业辉

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<CISSP认证考试指南(第6版)>>

内容概要

《cissp认证考试指南(第6版)》针对最新发布的信息系统安全专家考试做了全面修订,它全面、最新地覆盖了(isc)2开发的cissp考试的所有10个专业领域。

这本权威的考试指南在每一章的开始都给出了学习目标、考试技巧、实践问题和深入的解释。

《cissp认证考试指南(第6版)》由it安全认证和培训的首席专家撰写,将帮助您轻松地通过考试,也可以作为工作的一本重要参考书。

<<CISSP认证考试指南(第6版)>>

作者简介

hon harris , cissp, logical security有限责任公司的创始人兼首席执行官、安全咨询顾问、美国空军信息作战部门的前工程师、讲师和畅销书作者。

她为财富100强公司和政府机构提供广泛安全问题的咨询服务。

她也是本书先前版本的作者。

<<CISSP认证考试指南(第6版)>>

书籍目录

《cissp认证考试指南(第6版)》

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	5
1.4 如何注册考试	6
1.5 本书概要	6
1.6 cissp应试小贴士	6
1.7 本书使用指南	8
1.7.1 问题	8
1.7.2 答案	16
第2章 信息安全治理与风险管理	17
2.1 安全基本原则	18
2.1.1 可用性	18
2.1.2 完整性	19
2.1.3 机密性	19
2.1.4 平衡安全	20
2.2 安全定义	21
2.3 控制类型	22
2.4 安全框架	26
2.4.1 iso/iec 27000系列	28
2.4.2 企业架构开发	32
2.4.3 安全控制开发	41
2.4.4 coso	44
2.4.5 流程管理开发	45
2.4.6 功能与安全性	51
2.5 安全管理	52
2.6 风险管理	52
2.6.1 谁真正了解风险管理	53
2.6.2 信息风险管理策略	53
2.6.3 风险管理团队	54
2.7 风险评估和分析	55
2.7.1 风险分析团队	56
2.7.2 信息和资产的价值	56
2.7.3 构成价值的成本	56
2.7.4 识别脆弱性和威胁	57
2.7.5 风险评估方法	58
2.7.6 风险分析方法	63
2.7.7 定性风险分析	66
2.7.8 保护机制	69
2.7.9 综合考虑	71
2.7.10 总风险与剩余风险	71
2.7.11 处理风险	72
2.7.12 外包	74
2.8 策略、标准、基准、指南和	

<<CISSP认证考试指南(第6版)>>

过程	75
2.8.1 安全策略	75
2.8.2 标准	78
2.8.3 基准	78
2.8.4 指南	79
2.8.5 措施	79
2.8.6 实施	80
2.9 信息分类	80
2.9.1 分类级别	81
2.9.2 分类控制	83
2.10 责任分层	84
2.10.1 董事会	84
2.10.2 执行管理层	85
2.10.3 cio	86
2.10.4 cpo	87
2.10.5 cso	87
2.11 安全指导委员会	88
2.11.1 审计委员会	89
2.11.2 数据所有者	89
2.11.3 数据看管员	89
2.11.4 系统所有者	89
2.11.5 安全管理员	90
2.11.6 安全分析员	90
2.11.7 应用程序所有者	90
2.11.8 监督员	90
2.11.9 变更控制分析员	91
2.11.10 数据分析员	91
2.11.11 过程所有者	91
2.11.12 解决方案提供商	91
2.11.13 用户	91
2.11.14 生产线经理	92
2.11.15 审计员	92
2.11.16 为何需要这么多角色	92
2.11.17 人员安全	92
2.11.18 招聘实践	93
2.11.19 解雇	94
2.11.20 安全意识培训	95
2.11.21 学位或证书	96
2.12 安全治理	96
2.13 小结	100
2.14 快速提示	101
2.14.1 问题	103
2.14.2 答案	110
第3章 访问控制	115
3.1 访问控制概述	115
3.2 安全原则	116
3.2.1 可用性	116

<<CISSP认证考试指南(第6版)>>

- 3.2.2 完整性 117
- 3.2.3 机密性 117
- 3.3 身份标识、身份验证、授权与可问责性 117
 - 3.3.1 身份标识与身份验证 119
 - 3.3.2 密码管理 127
 - 3.3.3 授权 149
- 3.4 访问控制模型 161
 - 3.4.1 自主访问控制 161
 - 3.4.2 强制访问控制 162
 - 3.4.3 角色型访问控制 164
- 3.5 访问控制方法和技术 166
 - 3.5.1 规则型访问控制 167
 - 3.5.2 限制性用户接口 167
 - 3.5.3 访问控制矩阵 168
 - 3.5.4 内容相关访问控制 169
 - 3.5.5 上下文相关访问控制 169
- 3.6 访问控制管理 170
 - 3.6.1 集中式访问控制管理 171
 - 3.6.2 分散式访问控制管理 176
- 3.7 访问控制方法 176
 - 3.7.1 访问控制层 177
 - 3.7.2 行政管理性控制 177
 - 3.7.3 物理性控制 178
 - 4.7.4 技术性控制 179
- 3.8 可问责性 181
 - 3.8.1 审计信息的检查 183
 - 3.8.2 保护审计数据和日志信息 184
 - 3.8.3 击键监控 184
- 3.9 访问控制实践 185
- 3.10 访问控制监控 187
 - 3.10.1 入侵检测 187
 - 3.10.2 入侵防御系统 194
- 3.11 对访问控制的几种威胁 196
 - 3.11.1 字典攻击 196
 - 3.11.2 蛮力攻击 197
 - 3.11.3 登录欺骗 198
 - 3.11.4 网络钓鱼 198
 - 3.11.5 威胁建模 200
- 3.12 小结 202
- 3.13 快速提示 202
 - 3.13.1 问题 204
 - 3.13.2 答案 211
- 第4章 安全架构和设计 215
 - 4.1 计算机安全 216
 - 4.2 系统架构 217
 - 4.3 计算机架构 220
 - 4.3.1 中央处理单元 220

<<CISSP认证考试指南(第6版)>>

4.3.2 多重处理	224
4.3.3 操作系统架构	226
4.3.4 存储器类型	235
4.3.5 虚拟存储器	245
4.3.6 输入/输出设备管理	246
4.3.7 cpu架构	248
4.4 操作系统架构	251
4.5 系统安全架构	260
4.5.1 安全策略	260
4.5.2 安全架构要求	261
4.6 安全模型	265
4.6.1 状态机模型	266
4.6.2 bell-lapadula模型	268
4.6.3 biba模型	270
4.6.4 clark-wilson模型	271
4.6.5 信息流模型	274
4.6.6 无干扰模型	276
4.6.7 格子模型	276
4.6.8 brewer and nash模型	278
4.6.9 graham-denning模型	279
4.6.10 harrison-ruzzo-ullman模型	279
4.7 运行安全模式	280
4.7.1 专用安全模式	280
4.7.2 系统高安全模式	281
4.7.3 分隔安全模式	281
4.7.4 多级安全模式	281
4.7.5 信任与保证	283
4.8 系统评估方法	283
4.8.1 对产品进行评估的原因	284
4.8.2 橘皮书	284
4.9 橘皮书与彩虹系列	288
4.10 信息技术安全评估准则	289
4.11 通用准则	291
4.12 认证与认可	295
4.12.1 认证	295
4.12.2 认可	295
4.13 开放系统与封闭系统	296
4.13.1 开放系统	296
4.13.2 封闭系统	297
4.14 一些对安全模型和架构的威胁	297
4.14.1 维护陷阱	297
4.14.2 检验时间/使用时间攻击	298
4.15 小结	299
4.16 快速提示	300
4.16.1 问题	302
4.16.2 答案	307
第5章 物理和环境安全	311

<<CISSP认证考试指南(第6版)>>

5.1 物理安全简介	311
5.2 规划过程	313
5.2.1 通过环境设计来预防犯罪	316
5.2.2 制订物理安全计划	320
5.3 保护资产	331
5.4 内部支持系统	332
5.4.1 电力	333
5.4.2 环境问题	337
5.4.3 通风	339
5.4.4 火灾的预防、检测和扑灭	339
5.5 周边安全	345
5.5.1 设施访问控制	346
5.5.2 人员访问控制	352
5.5.3 外部边界保护机制	353
5.5.4 入侵检测系统	360
5.5.5 巡逻警卫和保安	362
5.5.6 安全狗	363
5.5.7 对物理访问进行审计	363
5.5.8 测试和演习	363
5.6 小结	364
5.7 快速提示	364
5.7.1 问题	366
5.7.2 答案	371
第6章 通信与网络安全	375
6.1 通信	376
6.2 开放系统互连参考模型	377
6.2.1 协议	378
6.2.2 应用层	379
6.2.3 表示层	380
6.2.4 会话层	381
6.2.5 传输层	383
6.2.6 网络层	384
6.2.7 数据链路层	385
6.2.8 物理层	386
6.2.9 osi模型中的功能和协议	387
6.2.10 综合这些层	389
6.3 tcp/ip模型	390
6.3.1 tcp	391
6.3.2 ip寻址	395
6.3.3 ipv6	397
6.3.4 第2层安全标准	400
6.4 传输的类型	402
6.4.1 模拟和数字	402
6.4.2 异步和同步	404
6.4.3 宽带和基带	405
6.5 布线	406
6.5.1 同轴电缆	407

<<CISSP认证考试指南(第6版)>>

- 6.5.2 双绞线 407
- 6.5.3 光缆 408
- 6.5.4 布线问题 409
- 6.6 网络互联基础 411
 - 6.6.1 网络拓扑 412
 - 6.6.2 介质访问技术 414
 - 6.6.3 网络协议和服务 425
 - 6.6.4 域名服务 433
 - 6.6.5 电子邮件服务 440
 - 6.6.6 网络地址转换 444
 - 6.6.7 路由协议 446
- 6.7 网络互联设备 449
 - 6.7.1 中继器 449
 - 6.7.2 网桥 450
 - 6.7.3 路由器 451
 - 6.7.4 交换机 453
 - 6.7.5 网关 457
 - 6.7.6 pbx 459
 - 6.7.7 防火墙 462
 - 6.7.8 代理服务器 480
 - 6.7.9 蜜罐 482
 - 6.7.10 统一威胁管理 482
 - 6.7.11 云计算 483
- 6.8 内联网与外联网 486
- 6.9 城域网 487
- 6.10 广域网 489
 - 6.10.1 通信的发展 490
 - 6.10.2 专用链路 492
 - 6.10.3 wan技术 495
- 6.11 远程连接 513
 - 6.11.1 拨号连接 513
 - 6.11.2 isdn 514
 - 6.11.3 dsl 515
 - 6.11.4 线缆调制解调器 516
 - 6.11.5 vpn 518
 - 6.11.6 身份验证协议 523
- 6.12 无线技术 525
 - 6.12.1 无线通信 526
 - 6.12.2 wlan组件 528
 - 6.12.3 无线标准 534
 - 6.12.4 wlan战争驾驶攻击 538
 - 6.12.5 卫星 538
 - 6.12.6 移动无线通信 539
 - 6.12.7 移动电话安全 543
- 6.13 小结 545
- 6.14 快速提示 546
 - 6.14.1 问题 549

<<CISSP认证考试指南(第6版)>>

- 6.14.2 答案 556
- 第7章 密码术 561
 - 7.1 密码学的历史 562
 - 7.2 密码学定义与概念 566
 - 7.2.1 kerckhoffs原则 568
 - 7.2.2 密码系统的强度 568
 - 7.2.3 密码系统的服务 569
 - 7.2.4 一次性密码本 570
 - 7.2.5 滚动密码与隐藏密码 572
 - 7.2.6 隐写术 573
 - 7.3 密码的类型 575
 - 7.3.1 替代密码 575
 - 7.3.2 换位密码 575
 - 7.4 加密的方法 577
 - 7.4.1 对称算法与非对称算法 577
 - 7.4.2 对称密码学 577
 - 7.4.3 非对称密码学 579
 - 7.4.4 分组密码与流密码 581
 - 7.4.5 混合加密方法 586
 - 7.5 对称系统的类型 591
 - 7.5.1 数据加密标准 591
 - 7.5.2 三重des 597
 - 7.5.3 高级加密标准 597
 - 7.5.4 国际数据加密算法 598
 - 7.5.5 blowfish 598
 - 7.5.6 rc4 598
 - 7.5.7 rc5 599
 - 7.5.8 rc6 599
 - 7.6 非对称系统的类型 600
 - 7.6.1 diffie-hellman算法 600
 - 7.6.2 rsa 602
 - 7.6.3 el gamal 604
 - 7.6.4 椭圆曲线密码系统 604
 - 7.6.5 背包算法 605
 - 7.6.6 零知识证明 605
 - 7.7 消息完整性 606
 - 7.7.1 单向散列 606
 - 7.7.2 各种散列算法 610
 - 7.7.3 md2 611
 - 7.7.4 md4 611
 - 7.7.5 md5 611
 - 7.7.6 针对单向散列函数的攻击 612
 - 7.7.7 数字签名 613
 - 7.7.8 数字签名标准 615
 - 7.8 公钥基础设施 616
 - 7.8.1 认证授权机构 616
 - 7.8.2 证书 619

<<CISSP认证考试指南(第6版)>>

- 7.8.3 注册授权机构 619
- 7.8.4 pki步骤 620
- 7.9 密钥管理 621
 - 7.9.1 密钥管理原则 622
 - 7.9.2 密钥和密钥管理的规则 623
- 7.10 可信平台模块 623
- 7.11 链路加密与端对端加密 625
- 7.12 电子邮件标准 627
 - 7.12.1 多用途internet邮件扩展(mime) 627
 - 7.12.2 可靠加密 628
 - 7.12.3 量子密码学 629
- 7.13 internet安全 630
- 7.14 攻击 640
 - 7.14.1 唯密文攻击 640
 - 7.14.2 已知明文攻击 640
 - 7.14.3 选定明文攻击 640
 - 7.14.4 选定密文攻击 640
 - 7.14.5 差分密码分析 641
 - 7.14.6 线性密码分析 641
 - 7.14.7 旁路攻击 641
 - 7.14.8 重放攻击 642
 - 7.14.9 代数攻击 642
 - 7.14.10 分析式攻击 642
 - 7.14.11 统计式攻击 642
 - 7.14.12 社会工程攻击 643
 - 7.14.13 中间相遇攻击 643
- 7.15 小结 644
- 7.16 快速提示 644
 - 7.16.1 问题 646
 - 7.16.2 答案 651
- 第8章 业务连续性与灾难恢复 655
 - 8.1 业务连续性和灾难恢复 656
 - 8.1.1 标准和最佳实践 659
 - 8.1.2 使bcm成为企业安全计划的一部分 661
 - 8.2 bcp项目的组成 664
 - 8.2.1 项目范围 665
 - 8.2.2 bcp策略 666
 - 8.2.3 项目管理 666
 - 8.2.4 业务连续性规划要求 668
 - 8.2.5 业务影响分析(bia) 669
 - 8.2.6 相互依存性 675
 - 8.3 预防性措施 676
 - 8.4 恢复战略 676
 - 8.4.1 业务流程恢复 680
 - 8.4.2 设施恢复 680
 - 8.4.3 供给和技术恢复 685
 - 8.4.4 选择软件备份设施 689

<<CISSP认证考试指南(第6版)>>

8.4.5 终端用户环境	691
8.4.6 数据备份选择方案	691
8.4.7 电子备份解决方案	694
8.4.8 高可用性	697
8.5 保险	699
8.6 恢复与还原	700
8.6.1 为计划制定目标	703
8.6.2 实现战略	704
8.7 测试和审查计划	706
8.7.1 核查性测试	707
8.7.2 结构化的排练性测试	707
8.7.3 模拟测试	707
8.7.4 并行测试	708
8.7.5 全中断测试	708
8.7.6 其他类型的培训	708
8.7.7 应急响应	708
8.7.8 维护计划	709
8.8 小结	712
8.9 快速提示	712
8.9.1 问题	714
8.9.2 答案	720
第9章 法律、法规、合规和调查	725
9.1 计算机法律的方方面面	725
9.2 计算机犯罪法律的关键点	726
9.3 网络犯罪的复杂性	728
9.3.1 电子资产	730
9.3.2 攻击的演变	730
9.3.3 国际问题	733
9.3.4 法律的类型	736
9.4 知识产权法	739
9.4.1 商业秘密	739
9.4.2 版权	740
9.4.3 商标	740
9.4.4 专利	741
9.4.5 知识产权的内部保护	742
9.4.6 软件盗版	743
9.5 隐私	745
9.5.1 对隐私法不断增长的需求	746
9.5.2 法律、指令和法规	747
9.6 义务及其后果	756
9.6.1 个人信息	759
9.6.2 黑客入侵	759
9.6.3 第三方风险	760
9.6.4 合同协议	760
9.6.5 采购和供应商流程	761
9.7 合规性	762
9.8 调查	763

<<CISSP认证考试指南(第6版)>>

- 9.8.1 事故管理 763
- 9.8.2 事故响应措施 766
- 9.8.3 计算机取证和适当的证据收集 769
- 9.8.4 国际计算机证据组织 770
- 9.8.5 动机、机会和方式 771
- 9.8.6 计算机犯罪行为 771
- 9.8.7 事故调查员 772
- 9.8.8 取证调查过程 772
- 9.8.9 法庭上可接受的证据 777
- 9.8.10 监视、搜索和查封 780
- 9.8.11 访谈和审讯 781
- 9.8.12 几种不同类型的攻击 781
- 9.8.13 域名抢注 783
- 9.9 道德 783
 - 9.9.1 计算机道德协会 784
 - 9.9.2 internet架构研究委员会 785
 - 9.9.3 企业道德计划 786
- 9.10 小结 786
- 9.11 快速提示 787
 - 9.11.1 问题 789
 - 9.11.2 答案 794
- 第10章 软件开发安全 797
 - 10.1 软件的重要性 797
 - 10.2 何处需要安全 798
 - 10.2.1 不同的环境需要不同的安全 799
 - 10.2.2 环境与应用程序 799
 - 10.2.3 功能与安全 800
 - 10.2.4 实现和默认配置问题 800
 - 10.3 系统开发生命周期 801
 - 10.3.1 启动 803
 - 10.3.2 购买/开发 804
 - 10.3.3 实现 805
 - 10.3.4 操作/维护 805
 - 10.3.5 处理 805
 - 10.4 软件开发生命周期 807
 - 10.4.1 项目管理 807
 - 10.4.2 需求收集阶段 808
 - 10.4.3 设计阶段 809
 - 10.4.4 开发阶段 811
 - 10.4.5 测试/验证阶段 813
 - 10.4.6 发布/维护阶段 815
 - 10.5 安全软件开发最佳实践 816
 - 10.6 软件开发模型 818
 - 10.6.1 边做边改模型 818
 - 10.6.2 瀑布模型 819
 - 10.6.3 v形模型(v模型) 819
 - 10.6.4 原型模型 820

<<CISSP认证考试指南(第6版)>>

- 10.6.5 增量模型 821
- 10.6.6 螺旋模型 822
- 10.6.7 快速应用开发 823
- 10.6.8 敏捷模型 824
- 10.7 能力成熟度模型 825
- 10.8 变更控制 827
- 10.9 编程语言和概念 829
 - 10.9.1 汇编程序、编译器和解释器 831
 - 10.9.2 面向对象概念 832
- 10.10 分布式计算 841
 - 10.10.1 分布式计算环境 841
 - 10.10.2 corba与orb 842
 - 10.10.3 com与dcom 844
 - 10.10.4 java 平台, 企业版本 845
 - 10.10.5 面向服务架构 846
- 10.11 移动代码 849
 - 10.11.1 java applet 849
 - 10.11.2 activex控件 851
- 10.12 web安全 852
 - 10.12.1 针对web环境的特定威胁 852
 - 10.12.2 web应用安全原则 859
- 10.13 数据库管理 860
 - 10.13.1 数据库管理软件 861
 - 10.13.2 数据库模型 862
 - 10.13.3 数据库编程接口 866
 - 10.13.4 关系数据库组件 867
 - 10.13.5 完整性 869
 - 10.13.6 数据库安全问题 871
 - 10.13.7 数据仓库与数据挖掘 875
- 10.14 专家系统和知识性系统 878
- 10.15 人工神经网络 880
- 10.16 恶意软件 882
 - 10.16.1 病毒 883
 - 10.16.2 蠕虫 885
 - 10.16.3 rootkit 885
 - 10.16.4 间谍软件和广告软件 886
 - 10.16.5 僵尸网络 886
 - 10.16.6 逻辑炸弹 888
 - 10.16.7 特洛伊木马 888
 - 10.16.8 防病毒软件 889
 - 10.16.9 垃圾邮件检测 892
 - 10.16.10 防恶意软件程序 892
- 10.17 小结 894
- 10.18 快速提示 894
 - 10.18.1 问题 897
 - 10.18.2 答案 903
- 第11章 安全运营 909

<<CISSP认证考试指南(第6版)>>

- 11.1 运营部门的角色 909
- 11.2 行政管理 910
 - 11.2.1 安全和网络人员 912
 - 11.2.2 可问责性 913
 - 11.2.3 阈值级别 913
- 11.3 保证级别 914
- 11.4 运营责任 914
 - 11.4.1 不寻常或无法解释的事件 915
 - 11.4.2 偏离标准 915
 - 11.4.3 不定期的初始程序加载(也称为重启) 915
 - 11.4.4 资产标识和管理 915
 - 11.4.5 系统控制 916
 - 11.4.6 可信恢复 917
 - 11.4.7 输入与输出控制 918
 - 11.4.8 系统强化 919
 - 11.4.9 远程访问安全 921
- 11.5 配置管理 921
 - 11.5.1 变更控制过程 922
 - 11.5.2 变更控制文档化 923
- 11.6 介质控制 924
- 11.7 数据泄漏 928
- 11.8 网络和资源可用性 929
 - 11.8.1 平均故障间隔时间(mtbf) 930
 - 11.8.2 平均修复时间(mttr) 930
 - 11.8.3 单点失败 931
 - 11.8.4 备份 937
 - 11.8.5 应急计划 939
- 11.9 大型机 940
- 11.10 电子邮件安全 942
 - 11.10.1 电子邮件的工作原理 943
 - 11.10.2 传真安全 945
 - 11.10.3 黑客和攻击方法 946
- 11.11 脆弱性测试 953
 - 11.11.1 渗透测试 956
 - 11.11.2 战争拨号攻击 958
 - 11.11.3 其他脆弱性类型 958
 - 11.11.4 事后检查 959
- 11.12 小结 960
- 11.13 快速提示 961
 - 11.13.1 问题 962
 - 11.13.2 答案 967
- 附录a 完整的问题 969
- 附录b 配套光盘使用指南 1013

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>