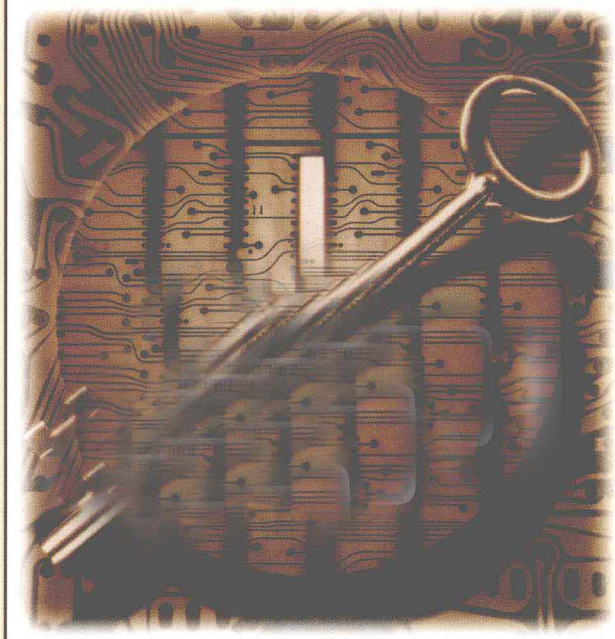
CISSP Practice Exams

Mc Graw Hill Education

CISSP
认证考试试题解析

- 数百个模拟题涵盖所有10个CISSP考试领域
- 详细解答现实问题



- 由顶级IT安全认证和培训专家亲笔撰著
- 提供在线模拟考试和音频讲座

(美) Shon Harris 著
杨金梅 译

清华大学出版社

CISSP 认证考试试题解析

(美) Shon Harris 著

杨金梅 译

清华大学出版社

北 京

Shon Harris
CISSP Practice Exams
EISBN：978-0-07-170139-6

北京市版权局著作权合同登记号　图字：01-2010-6806

图书在版编目(CIP)数据

CISSP 认证考试试题解析/(美) 哈里斯(Harris, S.) 著；杨金梅 译. —北京：清华大学出版社，2011.8
书名原文：CISSP Practice Exams

ISBN 978-7-302-25801-8

Ⅰ. C…　Ⅱ. ①哈…　②杨…　Ⅲ. 信息系统—安全技术—资格考试—题解　Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2011)第 113569 号

责任编辑：王　军　于　平
装帧设计：孔祥丰
责任校对：胡雁翎
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**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 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市兴旺装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：17.75　**字　数**：432 千字
版　　次：2011 年 8 月第 1 版　　**印　　次**：2011 年 8 月第1 次印刷
印　　数：1～3000
定　　价：48.00 元

产品编号：038394-01

作 者 简 介

Shon Harris，CISSP，Logical Security 公司创始人兼 CEO，计算机安全顾问，美国空军信息作战部前工程师，讲师兼作家。她迄今为止已经撰写了三本最畅销的 CISSP 书籍，参与编写了 *Hacker's challenge*(McGraw-Hill/Professional，2001)、*Gray Hat Hacking* 第 1 版和第 2 版(McGraw-Hill/Professional，2004 和 2007)和 *Security Information and Event Management(SIEM) Implementation*(McGraw-Hill/Professional，即将出版)。她目前正在从事 *Certified Ethical Hacker*(CEH)书籍的撰写工作。Harris 为 Pearson Education 开发了一套完整的数字信息安全产品系列，她同时还以一名信息安全专家证人的身份与多家律师事务所展开合作。

Harris 女士为美国多家财富 500 强企业提供咨询服务，其中包括美国运通公司、华纳兄弟公司、普利司通/费尔斯通、花旗银行、CitiFinancial、美国在线和 Cisco 等。她的专长涉及诸多方面，从建立风险管理方案和开发企业网络安全架构到以协同方式构建企业范围内的计算机安全和业务需求相结合的安全方案不等。

Harris 女士在法律和法规遵循方面有着丰富的知识和实践经验。她曾致力于让美国最大的公司遵守 OCC 法规、SOX、GLBA、HIPAA、PCI 和 SAS70 等的规定。Harris 女士擅长风险管理、治理和安全指标的开发和实施。

Harris 女士向很多客户提供信息安全课程，其中包括微软公司、国防部、能源部、国家安全局、RSA、美国西点军校、美国银行和其他多家金融机构。

Harris 女士被 *Information Security* 杂志评为信息安全领域最杰出的 25 位女士之一。

开发编辑简介

Crystal Bedell 是 Bedell Communications 公司的总裁，这是一家专门从事提供全方位技术和 B2B 通信领域文案和编辑服务的公司。她拥有多达 15 年的联合编辑、写作和市场营销经验，其中 8 年在 TechTarget 公司，为它的 IT 专家开发 Web 内容。既从事出版工作又从事市场营销工作的经历使 Crystal 对于 IT 专家的需求拥有独到的见解，同时也使她非常了解他们的工作环境和典型的 IT 决策者所拥有的局限性。她知道如何用他们的语言阐述问题，也知道如何把市场营销语言转换为朴实无华的英语。

作为一名专业的文案人员，Crystal 为技术公司撰写案例研究、白皮书、Web 副本以及很多其他内容。她还是 Tech Marcom 博客的作者，网址是 http://bedellcommunications.com/。

技术编辑简介

Polisetty Veera Subrahmanya Kumar，CISSP、CISA、PMP、PMI-RMP、MCPM、ITIL，拥有 20 多年的信息技术领域的经验。他的专业领域包括信息安全、业务连续性、项目管理和风险管理。目前，他是项目管理协会的 PMI-RMP(PMI-风险管理专家)认证委员会主席。过去，他曾作为内容开发团队负责人从事了各种各样的 PMI 标准开发项目。他曾是 PMI PMBOK 审核研讨会的主要讲师。他现在还是 ISACA 的 India Growth Task Force 团队的一名成员。

序　言

出版这本书以及为您提供在线问题的目的是让您熟悉CISSP考试中的多选题部分那些困难而棘手的问题，从而做好备战 CISSP 考试的充分准备。这本书中的问题将带您进入CISSP考试中要面对的Common Body of Knowledge(CBK)更为复杂的主题。

我们撰著的这本书可以和《CISSP认证考试指南(第5版)》(清华大学出版社引进并出版)(McGraw-Hill/Professional，2010)以及在线问题(www.logicalsecurity.com/CISSPQuizBook.html)同时使用。现将准备这次考试所用到的全部资料总结如下。

1. 复习这本书中的问题和答案。

2. 如果需要这些问题的进一步解释，请查看《CISSP认证考试指南(第5版)》一书的相关资料。

3. 复习所有www.logicalsecurity.com/CISSPQuizBook.html上提供的问题。

4. 作为自学内容的一部分，请收听www.logicalsecurity.com/CISSPQuizBook.html上提供的MP3文件。

5. 每周，复习www.logicalsecurity.com/practice/ques_of_week.html上提供的CISSP每周问题。

我们出版这本书的主要目的是帮助您通过考试，所以我们向您提供了CISSP考试所涉及的方方面面，另外再请结合《CISSP认证考试指南(第5版)》、在线问题和在线MP3文件等材料。充分利用所有这些可用的工具对您成功通过认证考试至关重要。

这本书的所有问题都配有这个答案为什么是正确的、那些答案为什么是错误的详细解答，我们相信即使在您通过考试之后，这本书仍然会是您非常有价值的专业资源。

在书中

这本书的每个章节都包含一个CISSP考试领域的模拟题，既适合有经验的信息安全专家使用，也适合安全领域的初学者。每章覆盖考试的一个主要领域，其答案既解释了“为什么”又解释了“如何”使用和支持这些技术和概念。

在网上

如果您购买了这本书，便可免费享用Shon Harris编写的1000多个CISSP问题和30多个小时的讲座。您应该充分利用这些工具和这本书中所提供的材料，从而充分备考CISSP

考试。在线问题和 MP3 视频文件，可以在 www.logicalsecurity.com/CISSPQuizBook.html 网址上找到。

Shon Harris 还每周至少发布一次新的 CISSP 问题，从而您可以不间断地做模拟题。这些问题可以在 www.logicalsecurity.com/practice/ques_of_week.html 上找到。

更多有关免费在线模拟题的信息，请参阅这本书后面的附录“免费在线模拟考试和 MP3 文件的使用说明”。

在每章中

我们所创建的每个章节都可以帮助您把注意力集中在测试和复习过程的每个主要环节，并且向您提供了有帮助的考试提示。在每章中，您可以找到以下内容：

- 每章都包括一个认证目标领域的模拟试题。钻研每个领域的各类问题，您将知道如何在考试中回答这些问题。
- 这些模拟题都类似于认证考试中的题，都是您在真正考试时所遇到的最常见和最容易混淆的题目。这些问题将有助于了解考试重点，练习这些模拟题将有助于确保您掌握考试需要掌握的内容。
- 每个问题后面都有深入的答案解析——既提供了正确答案的解析，也提供了错误答案的解析。通过阅读这些答案解析，您能巩固该章所学的内容，并熟悉考试题的结构。
- 每章后面都附有答案列表，仅提供正确答案所选字母。这使您可以在复习之前快速给自己打分。
- 一旦您完成了每章的测试，便可以参加在线考试。在线考试是一种现场考试形式，旨在按领域模拟各种题型，帮助您找到现场考试的感觉。

前　言

计算机、信息和物理安全日益重要。在过去几年中，随着 Web 站点的被损毁、拒绝服务式攻击的增多、信用卡信息的被盗、公开可用黑客工具的升级以及今天病毒和蠕虫持续造成的前所未有的损坏，人们对计算机和信息安全的需求已经迅速增长。

公司必须花费数百万美元之巨来消除这些问题所带来的影响，花费甚至更多的金钱来安装设备和软件、聘请顾问和实施教育培训以保证他们周边及内部网络的安全。特别是在 2001 年 9 月 11 日之后，对于这种安全的必要性和紧要性已经上升到了一个新的高度。政府、国家和社会易遭受通过网络和电波进行的许多不同类型的攻击的趋势已经逐渐明晰。社会严重依赖于各种类型的计算能力和功能，而这种能力和功能大多是由公共部门和私有部门所提供。这意味着尽管政府有责任保护他们的公民，但很明显，公民以及他们的企业也必须保证安全以保护整个国家。

这种保护实际上可以从适当的教育和了解开始，并且必须坚定不移地传授这种知识。本书为大家了解构成有效安全的众多不同领域奠定了基础。我们需要了解常见的所有威胁和危险，了解为减少这些漏洞必须采取的步骤。

除了阅读这本书外，您还可以在 www.logicalsecurity.com 上免费进行在线模拟考试。详细信息，请参阅本书后面的附录“免费在线模拟考试和 MP3 文件的使用说明”。

目　录

第 1 章

信息安全与风险管理

该领域包含的问题与下列主题有关：

- 安全管理责任
- 行政、技术和物理控制的区别
- 三大安全原则
- 风险管理与风险分析
- 安全策略
- 数据分类
- 安全意识培训

安全专业人士的责任远不止应对病毒和应对成为媒体头版头条的黑客消息那么简单。从表面上看，他们的日常工作很枯燥，但是却对保护公司免受入侵以避免其成为下一个头版头条至关重要。组织内部安全这一职责很复杂，因为它与每一个员工都息息相关，所以必须在全公司范围内对其进行管理。您要从管理的角度和业务的角度来理解安全问题，而不只是拘泥于技术细节，这无论是对参加 CISSP 考试还是履行你的本职工作都很重要。

1.1 问题

1. Which of the following best describes the relationship between CobiT and ITIL?
   A. CobiT is a model for IT governance, whereas ITIL is a model for corporate governance.
   B. CobiT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.
   C. CobiT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them.
   D. CobiT provides a framework for achieving business goals, whereas ITIL defines a framework for achieving IT service-level goals.
2. Jane has been charged with ensuring that clients' personal health information is adequately protected before it is exchanged with a new European partner. What data security requirements must she adhere to?
   A. HIPAA
   B. NIST SP 800-66
   C. Safe Harbor
   D. European Union Principles on Privacy
3. Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?
   A. Committee of Sponsoring Organizations of the Treadway Commission
   B. The Organisation for Economic Co-operation and Development
   C. CobiT
   D. International Organization for Standardization
4. Steve, a department manager, has been asked to join a committee that is responsible for defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What committee is he joining?
   A. Security policy committee
   B. Audit committee
   C. Risk management committee
   D. Security steering committee
5. As head of sales, Jim is the information owner for the sales department. Which of the following is not Jim's responsibility as information owner?
   A. Assigning information classifications
   B. Dictating how data should be protected
   C. Verifying the availability of data
   D. Determining how long to retain data

6. Assigning data classification levels can help with all of the following except:
   A. The grouping of classified information with hierarchical and restrictive security
   B. Ensuring that nonsensitive data is not being protected by unnecessary controls
   C. Extracting data from a database
   D. Lowering the costs of protecting data
7. Which of the following is not included in a risk assessment?
   A. Discontinuing activities that introduce risk
   B. Identifying assets
   C. Identifying threats
   D. Analyzing risk in order of cost or criticality
8. Sue has been tasked with implementing a number of security controls, including antivirus and antispam software, to protect the company's e-mail system. What type of approach is her company taking to handle the risk posed by the system?
   A. Risk mitigation
   B. Risk acceptance
   C. Risk avoidance
   D. Risk transference
9. The integrity of data is not related to which of the following?
   A. Unauthorized manipulation or changes to data
   B. The modification of data without authorization
   C. The intentional or accidental substitution of data
   D. The extraction of data to share with unauthorized entities
10. There are several methods an intruder can use to gain access to company assets. Which of the following best describes masquerading?
    A. Changing an IP packet's source address
    B. Elevating privileges to gain access
    C. An attempt to gain unauthorized access as another user
    D. Creating a new authorized user with hacking tools
11. A number of factors should be considered when assigning values to assets. Which of the following is not used to determine the value of an asset?
    A. The asset's value in the external marketplace
    B. The level of insurance required to cover the asset
    C. The initial and outgoing costs of purchasing, licensing, and supporting the asset
    D. The asset's value to the organization's production operations
12. Jill is establishing a companywide sales program that will require different user groups with different privileges to access information on a centralized database. How should the security manager secure the database?
    A. Increase the database's security controls and provide more granularity.

B. Implement access controls that display each user's permissions each time they access the database.

C. Change the database's classification label to a higher security status.

D. Decrease the security so that all users can access the information as needed.

13. As his company's CISO, George needs to demonstrate to the Board of Directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?

A. threats × vulnerability × asset value = residual risk

B. SLE × frequency = ALE, which is equal to residual risk

C. (threats × asset value × vulnerability) × control gap = residual risk

D. (total risk – asset value) × countermeasures = residual risk

14. Authorization creep is to access controls what scope creep is to software development. Which of the following is not true of authorization creep?

A. Users have a tendency to request additional permissions without asking for others to be taken away.

B. It is a violation of "least privilege."

C. It enforces the "need-to-know" concept.

D. It commonly occurs when users transfer to other departments or change positions.

15. For what purpose was the COSO framework developed?

A. To address fraudulent financial activities and reporting

B. To help organizations install, implement, and maintain CobiT controls

C. To serve as a guideline for IT security auditors to use when verifying compliance

D. To address regulatory requirements related to protecting private health information

16. Susan, an attorney, has been hired to fill a new position at Widgets Inc. The position is Chief Privacy Officer (CPO). What is the primary function of her new role?

A. Ensuring the protection of partner data

B. Ensuring the accuracy and protection of company financial information

C. Ensuring that security policies are defined and enforced

D. Ensuring the protection of customer, company, and employee data

17. Jared plays a role in his company's data classification system. In this role, he must practice due care when accessing data and ensure that the data is used only in accordance with allowed policy while abiding by the rules set for the classification of the data. He does not determine, maintain, or evaluate controls, so what is Jared's role?

A. Data owner

B. Data custodian

C. Data user

D. Information systems auditor

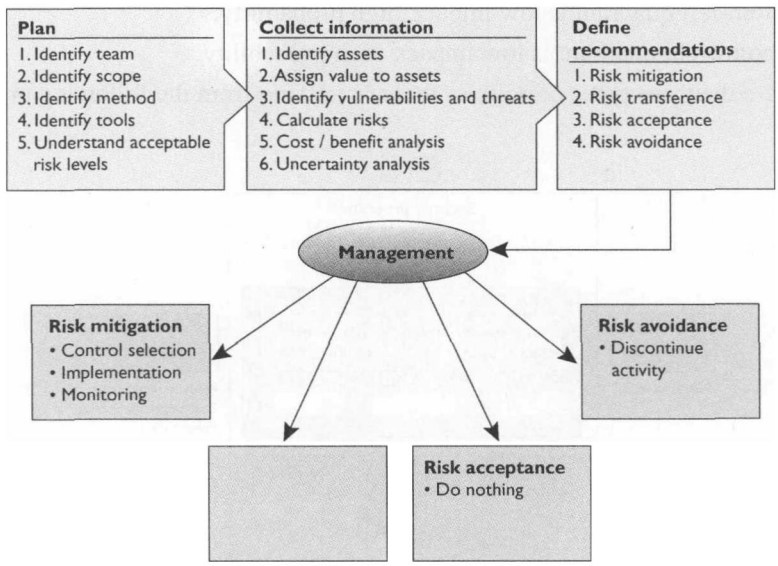
18. Risk assessment has several different methodologies. Which of the following official risk methodologies was not created for the purpose of analyzing security risks?

A. FAP
B. OCTAVE
C. ANZ 4360
D. NIST SP 800-30

19. Which of the following is not a characteristic of a company with a security governance program in place?
A. Board members are updated quarterly on the company's state of security.
B. All security activity takes place within the security department.
C. Security products, services, and consultants are deployed in an informed manner.
D. The organization has established metrics and goals for improving security.

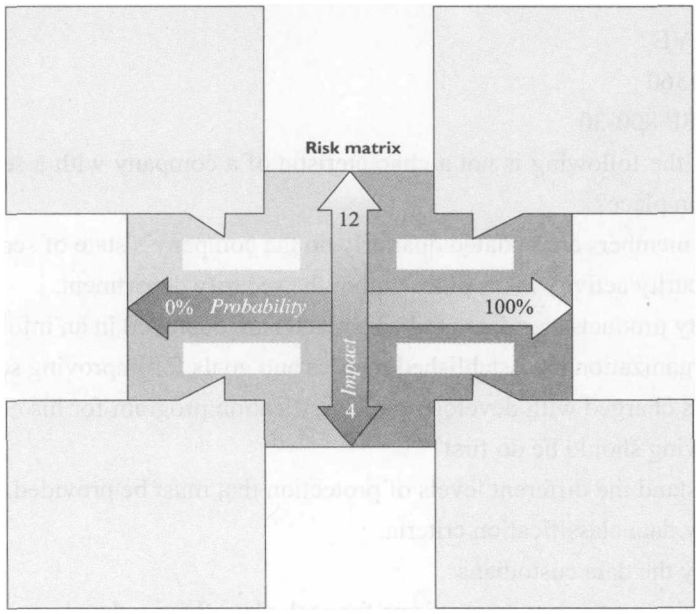
20. Michael is charged with developing a classification program for his company. Which of the following should he do first?
A. Understand the different levels of protection that must be provided.
B. Specify data classification criteria.
C. Identify the data custodians.
D. Determine protection mechanisms for each classification level.

21. There are four ways of dealing with risk. In the graphic that follows, which method is missing and what is the purpose of this method?



A. Risk transference. Share the risk with other entities.
B. Risk reduction. Reduce the risk to an acceptable level.
C. Risk rejection. Accept the current risk.
D. Risk assignment. Assign risk to a specific owner.

22. The following graphic contains a commonly used risk management scorecard. Identify the proper quadrant and its description.



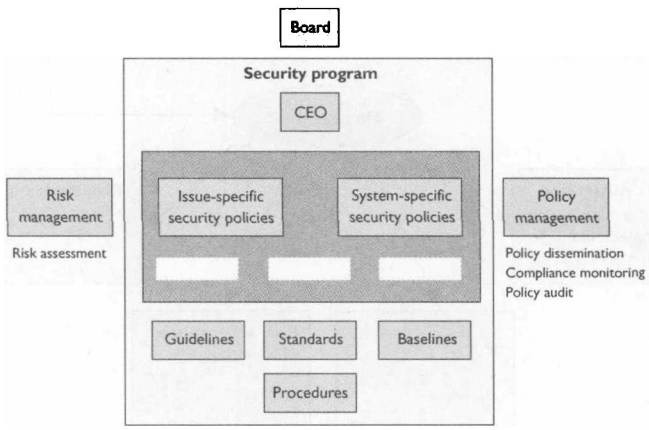
A. Top-right quadrant is high impact, low probability.

B. Top-left quadrant is high impact, medium probability.

C. Bottom-left quadrant is low impact, high probability.

D. Bottom-right quadrant is low impact, high probability.

23. What are the three types of policies that are missing from the following graphic?



A. Regulatory, Informative, Advisory

B. Regulatory, Mandatory, Advisory

C. Regulatory, Informative, Public

D. Regulatory, Informative, Internal Use

24. List in the proper order from the table on the top of the next page the learning objectives that are missing and their proper definitions.

A. Understanding, recognition and retention, skill
B. Skill, recognition and retention, skill
C. Recognition and retention, skill, understanding
D. Skill, recognition and retention, understanding

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning objective:			
Example teaching method:	**Media** • Videos • Newsletters • Posters	**Practical instruction** • Lecture and/or demo • Case study • Hands-on practice	**Theoretical instruction** • Seminar and discussion • Reading and study • Research
Test measure:	True/False Mutiple choice (Identify learning)	Problem solving, i.e., recognition and resolution (Apply learning)	Essay (Interpret learning)
Impact timeframe:	Short-term	Intermediate	Long-term

25. What type of risk analysis approach does the following graphic provide?

High	7–10	7–10
Medium	4–6	4–6
Low	0–3	0–3

0	10	20	30	40	50	60	70	80	90	100
0	9	18	27	36	45	54	63	72	81	90
0	8	16	24	32	40	48	56	64	72	80
0	7	14	21	28	35	42	49	56	63	70
0	6	12	18	24	30	36	42	48	54	60
0	5	10	15	20	25	30	35	40	45	50
0	4	8	12	16	20	24	28	32	36	40
0	3	6	9	12	15	18	21	24	27	30
0	2	4	6	8	10	12	14	16	18	20
0	1	2	3	4	5	6	7	8	9	10

41–100	High
20–40	Medium
0–19	Low

A. Quantitative
B. Qualitative
C. Operationally Correct
D. Operationally Critical