信息安全管理
先锋论坛

跟我学信息安全管理

09、CISSP课程内容介绍　郑路赛

信息安全管理专家委员会发布
2016年4月

信息安全管理论坛（http://www.iso27001cn.com）成立于2014年9月，为国内目前最专业的信息安全管理学习和实践交流平台。是学习信息安全管理方法、分享实战经验、提升实践水平的好地方！

关于我们

我们提供

- 最全的信息安全管理资料
- 信安经理高薪工作机会推荐
- 每周专家讲堂（ 每周四晚上8点半YY频道89519382 ）
- 物美价廉的ISO27001课程团购

- 信息安全管理学习实践QQ群 207723402
- 微信 IT管理精英圈 itilxf_(记得有下划线)

欢迎关注

授课老师

郑路赛

9年的IT管理和信息安全的工作经验，目前就职于一家美资软件公司，担任信息安全经理，负责公司信息安全体系建设和运维。拥有CISSP，ITIL，CCNP从业资格认证，曾经多次参加ISO27001的内外部审计，参与过信息安全书籍的翻译工作。

(ISC)²的简介

International Information Systems Security Certification Consortium

- 国际信息系统安全认证协会(ISC)²成立于1989年，总部设在美国弗罗里达州Palm Harbor，在伦敦、香港、东京、北京等地设有办事处，是一个独立的、全球性的、非盈利的组织。

致力于：

- 维护信息系统安全领域的通用知识体系
- 为信息系统安全专业人士和从业者提供认证
- 从事认证考试的培训和对认证考试进行的管理
- 通过连续教育培训,对有资格的认证候选人的授权工作进行管理.
- (ISC)2同时也向公众提供信息安全方面的教育和咨询服务。

CISSP的简介

Certified Information Systems Security Professional

CISSP认证考试由 (ISC)² 组织与管理，参加CISSP认证的人员需要遵守CISSP 道德规范（Code of Ethics），同时要有在信息系统安全通用知识框架（CBK）的8个领域之中拥有最少2个领域的专业经验5年;若考生持有任何一项(ISC)² 认可的有效认证 ，可享有减免一年工作经验的权利。或者， 考生如拥有四年制大学学士学位或区域性同等学历， 同样可以减免一年工作经验。 总体可减免的工作经验要求最多不超过一年。此外，CISSP应考者还需要得到另外一位持有有效认证的专业人士推荐确认（Endorsement)。

CISSP的简介

Certified Information Systems Security Professional

- 考试形式：250题单项选择题，其中25题用于调查目的，不计分
- 考试时间：6小时
- 通过分数：700
- 考试费用：599美金

CISSP的证书维护

Certified Information Systems Security Professional

CISSP认证有效期为三年，必须通过继续教育学分维护它，3 年总共 120 个 CPE 学分，每年最少 20 个 CPE 学分。

AMF 85$每年

CISSP的CBK

Common Body of Knowledge

CISSP CBK涵盖的八个知识域提供了一个厂商中立并受全球认可的通用知识框架。基于该框 架， 信息安全专业人员可以跨越地理和政治地理边界， 探讨、讲授、甚至促进信息安全实践。

CISSP CBK 所涵盖的议题可谓包罗万象， 确保了其与信息安全领域所有学科的关联度。 每个知识域 所包含内容的极尽详细， 也确保了 CISSP 持证者在专业知识与技能的广度和深度上， 达到了一名经验丰富的信息安全专业人员所应具备的水平。

CISSP新旧版本CBK对比

新版

- 1.安全与风险管理
- 2.资产安全
- 3.安全工程
- 4.通信与网络安全
- 5.身份与访问管理
- 6.安全评估与测试
- 7.安全运营
- 8.软件开发安全

老版

- 1. 信息安全治理和风险管理
- 2. 访问控制
- 3. 安全架构和设计
- 4. 物理和环境安全
- 5. 通信和网络安全
- 6.密码学
- 7. 业务连续性和灾难恢复
- 8. 法律，法规，合规和调查
- 9. 软件开发安全
- 10. 安全运营

Domain 1:安全与风险管理

Security and Risk Management

- 保密性、完整性和可用性（CIA）的概念
- 安全治理（安全功能与组织战略、目标和使命相一致）
- 合规
- 制定并实施文档化的安全策略、标准、程序和方针
- 人员安全策略
- 风险管理
- 威胁建模
- 信息安全教育、安全培训与安全意识

Domain 1:安全与风险管理

Security and Risk Management

CISSP 考试的第一个知识域是安全与风险管理，包括信息安全和风险管理的普遍性议题， 所涉及的范围甚广。安全和风险管理以信息安全的基本要素即保密性、可用性和完整性为开 始， 这也是所有信息安全功能得以实现的基础。 然后， 本知识域在这些概念的基础上，延伸到 安全治理与合规领域。
CISSP 考试将测试职业道德有关的一般性知识，尤其是对(ISC)² 职业道德规范的理解。 公众信任是信息安全专业人员应用其知识与技能的基础和前提， 必须植根于一套合乎道德伦理且可持续遵循的道德规范。
没有精心构建并统一实施的安全策略和程序， 就无法成功实现信息安全功能。因此，考试将测 试考生在信息安全环境下制定并实施策略和程序的能力。
风险管理是本知识域不可分割的一部分， 应对风险管理的概念有全面而透彻的了解。其中所涵盖的单个风险管理议题，包括风险分析、对策选择和实施、风险监视、报告和风险框 架。本知识域在风险管理概念的基础上进一步展开，介绍了威胁建模、如何将风险管理整合到 硬件、软件和服务合同的采购和管理之中。
考试还将考察 CISSP 考生在人员安全策略方面的知识，期望 CISSP 考生有能力建立并维护安全教 育、培训和意识方案。

Domain 2:资产安全

Asset Security

- 数据管理
- 确定并维护所有权
- 信息分类
- 适当的数据保留
- 资产管理
- 保护隐私
- 确定数据安全控制措施

Domain 2:资产安全

Asset Security

CISSP 考试的第二个知识域是“资产安全”，涉及贯穿整个信息生命周期的信息收集、处理及保护。信息与支持资产的分类形成本知识域所涵盖全部议题的基础，CISSP 考试要求考生十分熟悉这方面的知识。 涉及信息、系统、业务过程的所有权与信息分类密切相关， 是资产安全知识域的第二个议题。
随着数字化个人信息收集和存储的迅速膨胀， 隐私问题的重要性也相应增加，隐私保护构成资 产安全知识域的重要组成部分。 CISSP考试涉及的隐私保护相关议题包括数据所有者、数据处理 者、数据残留的概念以及信息收集和存储的限制。任何有关信息收集和存储的讨论都离不开数 据保留的议题， 而数据保留必须考虑组织、法律和法规的要求。测试内容将包含各个方面的知识。
经过考虑以上讨论的所有要素后，选择恰当数据安全控制措施的责任则落在了信息安全专业人员 身上。 CISSP考试将对考生在这方面的知识进行较为详细的测试。在这一知识领域涵盖的议题包 括基准、范围界定和裁剪、 标准选用和密码学。
资产安全知识域的最后一个议题涉及数据处理要求，包括数据存储、数据标记和数据销毁。期望 CISSP 考生具备评估数据处理要求，并基于该评估结果制定适当策略和程序的能力。

Domain 3:安全工程

Security Engineering

- 安全模型的基本概念
- 理解信息系统的安全能力
- 访问控制方法
- 密码学的应用
- DRM（数字版权管理）
- 站点安全和设计
- 设计和实施物理安全

Domain 3:安全工程

Security Engineering

“安全工程”是CISSP考试的第三个知识域。安全工程可定义为构建能够在面对由恶意行为、人员失误、硬件故障和自然灾难导致的威胁时仍继续交付所需功能的信息系统和相关架构的实践活动。
CISSP考生采用安全设计原则来实施和管理安全工程过程的能力将被测试。考生必须理解安全模 型的基础概念，有能力基于组织要求和安全策略制定出设计要求能够选取满足那，并些设计要 求的控制措施和对策。
信息安全专业人员必须持续地评估和缓解安全架构、设计和解决方案要素中的脆弱性。 在这个方 面，将对CISSP考生进行较为详细的测试。
CISSP测试内容包括密码 学一般性概念、密码生命周期、密码系统、公钥基础设施、密钥管理实践、数字签名和数字版权 管理等方面。 考生还必须全面理解密码攻击向量，包括社会工程学攻击、暴力破解攻击、唯密文攻击、已知明文攻击、频率分析攻击、选择密文攻击以及实施攻击。
安全工程不仅限于信息系统开发，本知识域涵盖的其它议题还包括将安全设计原则应用于场地 与设施设计， 以及物理安全之中。

Domain 4:通信与网络安全

Communication and Network Security

- 安全网络设计和架构
- 设计与建立安全通信信道
- 预防和减缓网络攻击
- 无线安全
- 网络硬件安全配置

Domain 4:通信与网络安全

Communication and Network Security

“通信与网络安全”知识域包括网络架构、传输方式、传输协议、控制设备以及为维护在私有 与公共通信网络中所传输信息的保密性、完整性和可用性而使用的安全措施。CISSP考生应彻底理解网络基础知识，包括网络拓扑、 IP寻址、网络分段、交换和路由、无线网 络、 OSI和TCP模型以及TCP/IP协议族。 由于与安全网络通信有关， CISSP考试也会在密码学方面 对考生进行测试。 通信与网络安全知识域还包括保护网络设备安全领域的一系列广泛议题。 CISSP考试将考察考生在安全操作和维护网络控制设备方面的专业知识与能力，包括交换机、路 由器和无线接入点等。考生必须熟悉各种形式传输媒介所固有的安全考虑因素，还包括网络访问控制、 端点安全以及内容分发网络。

CISSP 考生应有能力利用广泛的技术手段来设计并实施安全通信信道，以方便大量应用，包括数 据、语音、远程访问、多媒体协作以及虚拟化网络。 考试还将测试考生对于网络攻击向量方面的 知识，以及预防或减缓这些攻击的能力。

Domain 5:身份与访问管理

Identity and Access Management

- 控制资产的物理与逻辑访问
- 管理人员与设备的身份和验证
- 整合身份即服务
- 整合第三方身份服务
- 实施和管理授权机制
- 预防与减缓访问控制攻击
- 管理身份与访问供给生命周期

Domain 5:身份与访问管理

Identity and Access Management

从总体上看，“身份与访问管理”是信息安全的一个重要组成部分，尤其是对 CISSP 认证考试来 说更是如此。 该知识域涉及供给和管理人与信息系统之间、不同的信息系统之间、甚至是信息 系统各个部件之间相互交互所使用的身份和访问权限。 通过入侵身份或访问控制系统，获得系 统和信息的非授权访问也恰好是几乎所有涉及数据保密性攻击的目标。 因此，信息安全专业人员应当在这一知识领域投入大量的学习时间。

该知识域涉及不同用户、系统和服务的身份认证与授权管理，将考核 CISSP 考生对身份管理系统、 单一和多因素身份认证、可追溯性、会话管理， 身份注册与证明、联合身份管理和凭证管理系统 等知识的掌握情况。

考核内容还包括整合基于云的身份认证和第三方就地部署身份服务。 CISSP 考生应有能力实施 和管理授权机制，包括基于角色、 基于规则的访问控制，强制访问控制和自主访问控制。本知识 域涵盖的其它议题还包括预防和缓解针对访问控制系统和身份管理生命周期的攻击。

Domain 6:安全评估与测试

Security Assessment and Testing

- 漏洞评估和渗透测试
- 日志管理
- 内部和第三方审计
- 模拟攻击场景
- 用户培训和意识

Domain 6:安全评估与测试

Security Assessment and Testing

“安全评估与测试”涉及利用各种工具和技术对信息资产和相关基础设施进行评估，从而识别和 缓解由于架构问题、设计缺陷、配置错误、硬件和软件漏洞、编码错误， 以及任何影响信息系统 安全地交付其预期功能的其它缺陷所引起的风险。从 CISSP 认证考试角度出发，还包括持续验证 组织信息安全计划、政策、流程和程序的应用。

CISSP 考生应当有能力对评估与测试策略进行验证，以及能够利用各种技术实施这些策略。考 核知识点包括脆弱性评估、渗透测试、综合事务、代码审查和测试、误用例、接口测试等。

信息安全专业人员必须确保应用安全政策和程序的连续性与统一性， 还必须确保灾难恢复和业 务连续性计划得以维护、更新，并在发生灾难的情况下实现预期的功能。为此，安全评估和测试 知识域还包括收集安全过程数据的议题。考生知识点包括账户管理、管理评审、 关键绩效与风险 指标、验证备份、培训与意识、灾难恢复和业务连续性。

如果缺少对评估结果的缜密分析和汇报，以此制定和实施适当的风险缓解策略，安全评估和测试 就毫无价值。因此， CISSP 认证考试将考核考生分析、报告测试结果的能力，以及开展或促进内 部和第三方审计的能力。

Domain 7:安全运营

Security Operations

- 安全运营的基本概念
- 理解与支持调查
- 理解调查类型的要求
- 保护资源的供给安全
- 入侵检测/防御
- 数据渗漏
- 灾难恢复
- 业务连续性

Domain 7:安全运营

Security Operations

安全运营”知识域所涵盖的议题非常广泛，涉及将信息安全概念与最佳实践应用于企业计算系统的运营。安全运营本质上重在实践操作，旨在涵盖该信息安全专业人员在日常工作中预期执行或每天需要面对的任务和情况。

该知识域包含旨在评估 CISSP 考生取证调查知识，以及有能力开展和支持取证调查的议题。因此，各种调查的概念将是考核知识点，包括证据收集、处理、文档化并形成报告、调查技术和电子取证。考生还必须从运营、刑事、民事、法规角度理解调查的要求。

有效的日志和监测机制是重要的安全功能。除了为取证调查提供支持，日志和监测还为信息技术基础设施的日常运营提供可视化展示。此知识领域涵盖的议题包括入侵检测和防御、 安全信息与事件监控系统和数据泄漏保护。

安全运营还涉及资源的配置以及在资源的整个生命周期为其提供管理和保护。只有在保护这些资源的基础上，安全运营才可预期。 安全运营这一知识域涉及的其他议题还包括事件响应和恢复、灾难恢复和业务连续性。因此， CISSP 考试将测试考生进行全方面事件管理、实施和测试灾难恢复流程、参与业务连续性规划的能力。本知识域以物理安全和人员安全的相关议题为结尾。

Domain 8:软件开发安全

Software Development Security

- 理解安全并将其应用于软件开发生命周期
- 在开发环境中执行安全控制
- 评估软件安全的有效性
- 评估采购软件的安全影响

Domain 8:软件开发安全

Software Development Security

CISSP考试的最后一个知识域是“软件开发安全”，涉及将安全概念与最佳实践应用到软件的生产环境和开发环境。一般而言，CISSP持证人员不是软件开发人员或软件安全工程师，然而，他们对运行在工作环境中的软件进行评估并执行安全控制措施有义不容辞的责任。

为到达这一目的，信息安全专业人员必须在软件开发生命周期的背景下理解和应用安全。CISSP考生在下列方面将被测试：软件开发方法论、成熟度模型、运行与维护和变更管理，以及理解对于一支综合性产品开发团队的需要。

信息安全专业人员还必须有能力在软件开发环境中执行安全控制措施。CISSP考试将对考生在这个领域的多个议题进行测试，包括软件开发工具的安全、源代码弱点和脆弱性、配置管理（因其涉及源代码开发）、代码仓库的安全、应用程序编程接口的安全。

CISSP 考试还将在软件安全控制评估方面对 CISS 进行测试。本领域涵盖的议题包括审计与日志（因其涉及变更管理）、风险分析和风险减缓（因其涉及软件安全）以及外购软件的安全影响。

看的都会，蒙的都对

Thank you

作者　郑路赛

2016.8.6

特别鸣谢

小标题

北宙咨询 North Universe

Trendsetting Consulting

艾拓咨询 AituoXianfeng Consulting

特别鸣谢