# 2018-CISSP考纲变革及备考重点解析



北京谷安天下科技有限公司
方乐，CISSP, CISA, CISM, CRISC, CGEIT, ITIL Expert

 

## 新版大纲章节和考试权重

| 知识领域 | 权重 | 老版权重 |
|---|---|---|
| 1. 安全与风险管理 | 15% | 16% |
| 2. 资产安全 | 10% | 10% |
| 3. 安全工程 | 13% | 12% |
| 4. 通信与网络安全 | 14% | 12% |
| 5. 身份与访问管理 | 13% | 13% |
| 6. 安全评估与测试 | 12% | 11% |
| 7. 安全运营 | **13%** | 16% |
| 8. 软件开发安全 | 10% | 10% |
| 累计 | 100% | 100% |

 

## 1.安全与风险管理 - 概述

- 本知识域包括信息安全和风险管理的普遍性议题。
- 本知识域以信息安全的基本要素即保密性、可用性、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。
- 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。
- 本知识域还涵盖业务连续性计划(BCP)的各个方面，包括信息和需求收集、业务影响分析(BIA)以及恢复点目标(RPO)。
- CISSP 考生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。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 考生在人员安全政策方面的知识，期望 CISSP 考生有能力建立并维护安全教育、培训和意识方案。




## 2.资产安全 - 概述

- 本知识域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。
- 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。

## 3.安全工程 - 概述

- 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。包含将安全控制措施、行为与能力合并及整合到信息系统和企业架构中。
- 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需求，并能够选取满足那些设计需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。包括客户端和服务器端脆弱性、数据库安全、分布式系统和云安全、密码系统和工业控制，还包括Web应用程序脆弱性、移动设备和嵌入式系统。
- 密码学涉及确保信息的完整性、保密性和真实性。考生需要掌握密码学一般性概念、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。




## 4. 通信与网络安全 - 概述

- 本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。

## 5.身份与访问控制 - 概述

- 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。
- 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。




## 6. 安全评估和测试 - 概述

- 该知识域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、合成交易、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(DR)和业务连续性计划(BCP)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。

## 7. 安全运营 - 概述

- 该知识域是包含单个议题最多的知识域。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。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。
- 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(DLP)。
- 安全运营还涉及资源配置以及为资源的整个生命周期提供管理和保护。CISSP 考试将测试考生操作和维护保护性控制措施的能力，包括防火墙、入侵防御系统、应用程序白名单、反恶意软件、蜜罐、蜜网和沙箱技术，以及管理第三方安全合同和服务的能力，还包括补丁、漏洞和变更管理。
- 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。




## 8.软件开发安全 - 概述

- 本知识域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考生进行测试。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。

# 神奇的广告页

【CISSP保障班简介】

CISSP培训是谷安最先推出的认证课程之一，时至今日我们的CISSP学员数量早已过千，我们对CISSP认证持有者在国内数量的不断增加，各行业、各单位信息安全岗对CISSP的迫切需要不断提升而欣慰；

与此同时，2013年官方推出的CISSP中文考试，使更多的信息安全员有了考取认证的胆量，部分学员也有了明确的学习目的：获取认证!

为此，谷安在原有经典班基础上，结合众多CISSP讲师和顾问的学习与考试经验，组织核心讲师精心翻译CISSP官方模拟试题，面向需要获取认证的学员，2014年隆重推出CISSP认证培训保障班。保障班承诺：参加谷安CISSP保障班，万一首次考试没有通过，我们出考试费让您考第二次，再不过我们赔您考试费。

谷安天下CISSP培训保障班的真正含义：并不是与ISC2有特殊关系，而是在学员参加完经典班课程之后，谷安帮助大家制定学习计划、督促学习过程、详解考试知识点、组织习题练习与模拟考试、深入习题解析、考前强化训练等一系列服务，让学员真正掌握CISSP考试大纲内容，以不变应万变，争取一次通过CISSP考试。