huang

发布

北京网络空间安全协会

广东省网络空间安全协会

2021-11-1实施

2021-10-12发布

**HCS**

中国标准文献分类号：

团体标准

**T**/**BJCSA** 1—2019

网络空间安全专业人员认证规范

Cyberspace SecurHty ProfessHonal CertHfHcatHon SpecHfHcatHon

（征求意见稿）

2021-8-12

目 录

[前 言 III](#_Toc3919)

[引 言 IV](#_Toc28064)

[1. 范围 1](#_Toc10657)

[2. 规范性引用文件 1](#_Toc29009)

[3. 术语和定义 1](#_Toc22517)

[4. 认证类别、专业方向及级别划分 3](#_Toc14298)

[4.1 认证类别 3](#_Toc10105)

[4.2 级别划分 3](#_Toc23963)

[5. 认证通用要求 4](#_Toc20007)

[5.1 基本要求 4](#_Toc7648)

[5.2 初次申请资格要求 5](#_Toc31755)

[5.3 再认证资格要求 7](#_Toc27551)

[5.4 认证升级资格要求 7](#_Toc1564)

[6. 认证评价 7](#_Toc27224)

[6.1 认证评价方式 7](#_Toc27264)

[6.2 书面考试 7](#_Toc19363)

[6.3 书面评价 7](#_Toc2777)

[6.5 认证批准 8](#_Toc20235)

[6.6 颁发证书与公告 8](#_Toc16361)

[6.7 年度确认 8](#_Toc11297)

[6.8 再注册 8](#_Toc1389)

[6.9 变更 8](#_Toc20573)

[6.10暂停、恢复、撤销和注销认证 8](#_Toc6406)

[附 录 A(资料性) 网络空间安全专业人员认证分类 10](#_Toc12037)

[附 录 B（规范性） 通用基础知识考试大纲 11](#_Toc11050)

[附 录 C（规范性） 网络安全风险管理考试大纲 14](#_Toc5417)

[附 录 D（规范性） 物联网安全考试大纲 18](#_Toc14801)

[附 录 E（规范性） 云计算安全考试大纲 21](#_Toc24981)

[附 录 F（规范性） 网络安全规划设计方向考试大纲 24](#_Toc17135)

[附 录 G（规范性） 信息系统安全运维人员考试大纲 27](#_Toc7828)

[附 录H（规范性） 软件安全开发方向考试大纲 30](#_Toc3638)

[附 录 I(规范性) 网络安全应急响应方向考试大纲 34](#_Toc32625)

[附 录 J(规范性) 信息系统安全集成方向考试大纲 38](#_Toc16238)

[参考文献 38](#_Toc16238)

前 言

本标准按GB/T 1.1-2020给出的规则起草。

本标准由广东省网络空间安全协会、北京网络空间安全协会提出并归口。

本标准起草单位：广东省网络空间安全协会、广东关键信息基础设施保护中心、网安联认证服务有限公司、广发证券股份有限公司、联通（广东）产业互联网有限公司、蓝盾信息安全技术有限公司 、 广州华南信息安全测评中心、深圳市计量质量检测研究院、广东计安信息网络培训中心、广东省东莞市凤岗医院、广东中证声像资料司法鉴定所。

本标准起草人：成珍苑、吴星火、林小博、陈彦彬、姚飞、周绍午、安创文、李炯彬、 覃晓宁 、杜守红、谭祥明、杨文玲、王欢、徐伟、陈宁、贺锋、叶婷、曾幸钦、曾炽强、袁毅鸣、曾灶烟、李树湖、刘泽楠、周贵招、麦世能、卢焕镇。

引 言

网络空间的竞争，归根结底是人才竞争，保障网络空间安全，维护网络空间主权和国家安全、社会公共利益，促进经济社会信息化健康发展，网络空间安全人才将发挥关键作用。我国《网络安全法》已对关键信息基础设施运营者“设置专门安全管理机构和安全管理负责人”做出了明确规定，同时鼓励其他网络运营者自愿参与关键信息基础设施保护体系。对网络空间安全从业人员专业知识、能力和行为准则进行标准化规范，有利于人才队伍的健康发展，但目前对从业人员如何分级分类、应具备何种专业知识和能力水平等问题尚未建立标准规范，各用人单位的网络空间安全岗位设置和能力要求各行其是，差别较大。

制定统一的标准，推进权威机构的网络空间安全专业人才资质能力考核、认证工作，能够有效证明从业人员具备了相应的专业知识和能力、工作经验和业绩、以及较高的职业道德水平，从而为网络空间安全人才评价考核、选拔任用、职业晋阶提供参考依据，推进网络空间安全人才的职业化和专业化发展。

本标准是针对网络空间安全从业人员资格认定：网络空间安全专业人员认证（Code for CertHfHcatHon of Cyberspace SecurHty ProfessHonl英文缩写CSP）, 这种认定通过考试和其它评价方式证明获证人员具备了从事网络空间安全工作的个人素质和相应的技术知识与应用能力，以供用人单位选用具备能力资格的网络空间安全专业人员。

本标准规定了网络空间安全专业人员等级认定的类别及级别划分，获证人员职业素养、资历、知识和能力要求。

通过CSP评定，表明获证人员：

1.在申请认定前成功完成了北京网络空间安全协会或其授权培训机构组织的网络空间安全专业人员培训课程相应资质所需的分类课程，并取得培训合格证书；

2.通过了《网络空间安全专业人员认证规范》要求的相应类别和级别的技术知识水平与应用能力考试，并符合本规范的其它要求；

3.达到了网络空间安全从业人员应具有的职业素养、教育经历、从业经历的要求；

4.履行了《网络空间安全专业人员认证规范》规定的义务；

5.所有获证人员除符合本标准要求之外，还应遵守本国家和/或地区的有关法律、法规。

网络空间安全专业人员认证规范

1. 范围

本标准规定了网络空间安全专业人员认证的级别及资格要求。

本标准适用于参与网络空间安全工作的所有从业人员。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。

凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3. 术语和定义

GB/T 27024《合格评定人员认证机构通用要求》界定的以及下列文件中的术语和定义并适用于本文件。

3. 1

网络空间安全专业人员

从事网络空间安全相关工作的所有人员，如组织的管理人员（包括CHO、CSO、科技管理部门和风险控制管理部门的人员）、HT 相关的技术人员（包括运维、开发和集成人员），从事网络空间服务组织的技术人员（包括网络空间产品研发人员、网络空间咨询人员、网络空间服务实施人员和外派服务人员等）。

**3. 2**

获证人员

通过网络空间专业人员考试和认证评价，获得或保持网络空间专业人员证书的人员。

**3. 3**

工作经历

取得相应学历后的所有工作历史，无论是有偿的还是无偿的，全职的还是兼职的，不包括实习经历。

**3. 4**

第三方认证机构

独立于网络空间服务相关方的专业认证机构。

**3.5**

网络安全风险

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响 。

**3.6**

网络安全风险管理

依据有关信息安全技术与管理标准 ，对信息系统及由其处理 、传输和存储的信息的保密性 、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性 ，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

**3.7**

网络安全规划设计

是指综合运用计算机软、硬件技术、网络通信技术、密码技术、信息安全技术，在企业、系统或项目的设计规划阶段，提出综合性的解决方案，以保障网络系统及其所承载的数据的保密性、完整性及可用性。

3.8

物联网安全

物联网安全指能够对物联网络的访问加以控制、确定用户（如抽象的有权限的账号、人、物联网络端、物联网端节点或物联网接入网关）身份真实有效以及私密性、保证用户行为不可抵赖、保证传输和存储数据的机密性、完整性、保证物联网的可用性、防止网络、业务遇到偶然的、被动的和主动的威胁以及病毒的扩散的技术和管理措施，以及对影响网络、业务的意外事故的应对措施。

3.9

物联网漏洞

设备在物理防护、软件质量、配置、通信协议选择与实现的适用性等方面的缺陷。

3.10

渗透测试

模拟黑客攻击的手法，进行的非破坏性的攻击性测试，以期发现可能被黑客利用对系统进行入侵的安全漏洞和隐患及攻击路径，并将入侵的过程和漏洞细节产生报告给服务对象，提出详细、合理的修复建议，指导其进行整改，清除安全隐患，降低安全风险，为服务对象信息系统的平稳运行提供安全保障。

3.11

云计算安全

云计算安全或云安全指一系列用于保护云计算数据、应用和相关结构的策略、技术和控制的集合，属于计算机安全、网络安全的子领域，或更广泛地说属于信息安全的子领域。

3.12

信息系统安全运维

为保障和提升服务对象的信息系统安全防护能力，及时解决出现的网络安全问题，由服务机构通过管理与技术手段提供的网络安全服务。主要包括安全巡检、病毒查杀、备份和恢复、安全审计、安全优化、渗透测试、风险评估等。

3.13

软件安全开发

为解决软件产品的漏洞问题，而将安全活动集成到系统开发和软件质量保证活动中， 在软件开发的每个关键点嵌入安全要素，通过安全需求分析、安全设计、安全编码、安全测试等专业手段，解决各阶段可能出现的安全问题，有效减少软件产品潜在的漏洞数量提高软件产品安全质量的活动。

3.14

网络安全应急响应

是指在突发重大网络安全事件后对包括计算机运行在内的业务运行进行维持或恢复的各种技术和管理策略与规程。

3.15

信息系统安全集成

按照信息系统的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成的统一和协调的系统之中，使资源达到充分共享，实现集中、高效、便利的管理，从而使建设完成后的信息系统满足建设方或使用方的安全需求而开展的活动。

4. 认证类别、专业方向及级别划分

4.1 认证类别

网络空间安全专业人员共分3个类别，包括管理类、运营类、技术类，共18个专业方向。管理类包括网络安全审计、网络安全风险管理、个人信息安全保护、舆情监测等4个方向，运营类包括监测预警、网络安全规划设计、信息系统安全运维、网络安全应急相应等4个方向，技术类包括云计算安全、软件安全开发、工业互联网安全、信息安全集成、渗透测试、大数据安全、密码技术、人工智能安全、物联网安全等9个方向；认证方向具体描述见附录A。

4.2 级别划分

网络空间安全专业人员共设置五个级别，一至五级，其中一级最低、五级最高，一、二级不分专业方向，三、四、五级分专业方向。

表1-1

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 类别 | 管理类 | | | | 运营类 | | | | |
| 方向  级别 | 网络安全审计 | 网络安全风险管理 | 个人信息安全保护 | 舆情监测 | 监测预警 | 网络安全规划设计 | 信息系统安全运维 | 网络安全风险评估 | 网络安全  应急响应 |
| 五级 | 资历评定，在各类别的某个方向领域资质符合条款5.2.1.5的要求即可申请 | | | | | | | | |
| 四级 | 需掌握各类别的专业方向所要求的知识，并通过相应的考试，根据资历条件颁发三级或四级认证证书 | | | | | | | | |
| 三级 |
| 二级 | 需掌握通用基础知识，并通过相应的考试，根据资历条件颁发一级或二级认证证书 | | | | | | | | |
| 一级 |

表1-2

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 类别 | 技术类 | | | | | | | | |
| 方向  级别 | 云计算安全 | 软件安全开发 | 工业互联网安全 | 信息系统安全集成 | 渗透测试 | 大数据安全 | 密码技术 | 人工智能安全 | 物联网安全 |
| 五级 | 资历评定，在各类别的某个方向领域资质符合条款5.2.1.5要求即可申请 | | | | | | | | |
| 四级 | 需掌握各类别的专业方向所要求的知识，并通过相应的考试，根据资历条件颁发三级或四级认证证书 | | | | | | | | |
| 三级 |
| 二级 | 需掌握通用基础知识，并通过相应的考试，根据资历条件颁发一级或二级认证证书 | | | | | | | | |
| 一级 |

5. 认证通用要求

5.1 基本要求

获证人员应满足如下基本要求；

a) 具有独立的民事行为能力，具备承担法律责任的能力；

b) 近三年内未受过刑事处罚；

c) 不存在法律法规禁止从业的情形；

d) 自愿遵守颁布的网络空间专业人员认证相关文件的有关规定，履行相关义务；

e) 符合有关法律法规的规定。

5.2 初次申请资格要求

5.2.1 教育及工作经历

5.2.1.1 一级认证人员（预备级）认证资格要求

获证人员应满足下面要求：

教育部发布的“具有普通高等学历教育招生资格的高等学校名单”中的院校的在校生、应届毕业生或全国研究生招生计划中研究生招生单位在校研究生、应届毕业生等；

5.2.1.2 二级认证人员（基础级）教育及工作经历要求

专业要求：无专业要求限制。

获证人员工作经历应至少满足下面一项要求：

a) 本科（含）以上学历， 1年以上从事网络空间安全有关工作经历；

b) 专科毕业，2年以上从事网络空间安全有关的工作经历；

c) 中等专科毕业，4年以上从事网络空间有关的工作经历；

e) 具有丰富的项目经验，5年以上从事网络空间安全有关的工作经历；

5.2.1.3 三级认证人员（专业级）教育及工作经历要求

专业要求：网络空间、信息安全、计算机相关或相近专业，非以上专业的人员需先通过二级人员认证。

获证人员工作经历应至少满足下面一项要求：

a) 硕士研究生（含）以上学历，1年以上从事网络空间有关工作经历；

b) 本科毕业，3年以上从事网络空间有关工作经历；

c) 专科毕业，5年以上从事网络空间有关工作经历；

d) 中等专科毕业， 7年以上从事网络空间有关工作经历；

5.2.1.4 四级认证人员（高级专业级）教育及工作经历要求

专业要求：网络空间、信息安全、通讯、计算机相关或相近专业，非以上专业的人员，需首先通过二级人员认证。

获证人员工作经历应至少满足下面一项要求：

a) 硕士研究生（含）以上学历， 3年以上从事网络空间有关工作经历，其中至少1年以上项目经理经验；

b) 本科毕业，5年以上从事网络空间相关工作经历，其中至少2年以上项目经理经验；

c) 专科毕业，7年以上从事网络空间有关工作经历，其中至少2年以上项目经理经验；

d) 8年以上从事网络空间有关工作经历，其中至少2年以上项目经理经验；

5.2.1.5 五级认证人员（专家级）教育与工作经历要求

专业要求：网络空间、信息安全、计算机相关或相近专业；

获证人员工作经历应至少满足下面一项要求：

a) 硕士研究生（含）以上学历， 5年以上从事网络空间有关工作经历，其中至少2年项目经理经验；

b) 本科毕业，7年以上从事网络空间相关工作经历，其中3年项目经理经验；

c) 专科毕业，9年以上从事网络空间有关工作经历，其中至少3年项目经理经验；

d) 10年以上从事网络空间有关工作经历，其中至少3年项目经理经验。

职称要求：

具有信息技术相关专业的高级技术职称（含副高）；

5.2.1.6 其他要求

除5.2.1.1-5.2.1.5外的其他要求：

1. 满足评定要求的工作经历应在取得相应学历后获得。
2. 申请人应提交工作经历的书面证明，证明中应提供申请人从事的工作职责、岗位、级别和主要工作内容。

c) 实习经历不能包括在工作经历内。

5.2.2 考试要求

获证人员应满足下面要求：

a) 通过其申请的相应认证类别和级别的考试，包括笔试和实操（必要时）；

b) 必要时，通过由第三方认证或评估机构组织的专家面试；

c) 必要时，通过由第三方认证或评估机构组织的工作现场见证。

d）一、二级认证人员需要掌握附录B网络空间安全专业人员认证通用知识要求”中所要求的知识，且通过相应的考试。

e）三、四级认证人员分类别和专业方向，各类别专业方向人员须掌握附录(C~J)中对应方向要求的知识，且通过相应的考试。

f）五级认证人员为资历评定，学历、工作经历、职称符合条款5.2.1.5的条件即可申请，无考试要求。

5.3 再认证资格要求

1）已通过网络空间专业人员认证，且在认证有效期内；

2）获证后3年内至少有2年的网络空间工作经历；

3）每年不少于16课时的网络空间相关专业的继续教育课程学习。

5.4 认证升级资格要求

获证人员应满足下面要求：

a) 已通过网络空间专业人员认证，且在认证有效期内；

b) 满足网络网络空间专业人员高一级别认证要求，包括工作经历、培训和考试要求。

6. 认证评价

6.1 认证评价方式

书面考试 + 书面评价 + 面试（需要时）  
6.2 书面考试

培训合格后，人员可参加第三方认证机构组织的相应级别的书面考试，考试大纲见附件(C-J)要求。

6.3 书面评价

6.3.1 满足一级认证要求的网络空间安全从业人员，提交认证的申请材料，包括但不限于学籍注册证明、身份证明(身份证、军官证等复印件)、考试合格证明、工作经历等资格证明材料;

6.3.2 满足认证其他级别和类别要求的的网络空间安全人员提交的认证申请材料，包括身份证明(身份证、军官证等复印件)、学历、工作经历、书面考试合格等证明材料;

6.3.3 收到申请材料后，第三方认证机构的申请评审人员负责审查申请人提交的申请资料，若申请人提交的资料齐全、填写清楚、正确，且资料表明符合认证准则基本要求的则予以正式受理;

6.3.4 在资料审查过程中，申请评审人员应将所发现的与认证条件不符合之处通知申请人;

6.3.5 认证审核人员对申请人提交认证申请材料进行审查，并给出符合性评价结论论;

6.3.6 认证审核人员对申请人的考试成绩进行核实，并给出其在所申请的专业方向和对应级别的知识水平和应用能力的评价结论;

6.3.7 认证审核人员对申请人进行综合评价，以决定直接推荐认证评定或 需进一步面试评价。  
6.4 面试评价(需要时)

6.4.1 面试评价人员依据认证审核人员的建议对申请人综合素质、所申请的专业方向和级别要求的知识和能力通过面谈的方式进行考核或核实，并给出其在所申请的专业方向和对应级别的知识水平和应用能力的评价结论。  
6.4.2 面试评价人员对申请人进行综合评价，以决定是否推荐认证批准。

6.5 认证批准

6.5.1第三方认证机构认证决定人员负责审核认证书面评价和面试评价（需要时）的意见，并最终决定是否批准认证。

6.5.2 认证决定人员和审核人员不应为同一人员。

6.5.3 最终决定结果是以下三种类型之一:

a) 通过认证;  
b) 不予通过认证;  
c) 补充证据或信息，再行认证评定。

6.6 颁发证书与公告

第三方认证机构应发布公告，公告通过认证的人员名单，并发放认证证书，认证证书有效期3年。

6.7 年度确认

获证人员在证书有效期内每年完成相应的再继续培训16个学时以上来维持认证资质的持续有效。

6.8 再注册

获证人员在证书过期前90天内应向第三方认证机构提交资料申请再注册申请，再注册评价需提交近三年的网络空间安全相关工作经历，应至少包括2年以上认证方向相关的经历或2个认证方向的完成项目。

6.9 变更

获证人员在证书有效期内提出级别、方向、类别方向的变更，如升级、降级、变更到其他方向、类别，或增加其他方向、类别的证书，均可提交变更申请，以及提供标准中要求的符合性证明材料以供评价。

6.10暂停、恢复、撤销和注销认证

6.10.1 暂停认证  
6.10.1.1 获证人员如不能持续地符合认证条件和要求，包括不提交专业持续发展课程学习的证明、不提供相关认证专业方向的工作经历证明和不按时缴纳费用，第三方认证机构可以暂停部分或全部认证资格。  
6.10.1.2 暂停期不小于 60 天，但不大于 180 天，获证人员在暂停期间不再享有相应权利，不得使用被暂停的证书，也不得以任何明示或隐含的方式向外界表示被暂停认证的范围仍然有效。

6.10.2 恢复认证

被暂停认证的，在规定的暂停期限内达到认证要求后，申请并经确认符合，可以恢复认证资格。

6.10.3 撤销认证

在下列情况下，第三方认证机构应撤销认证:  
a) 被暂停认证的，超过暂停期仍不能恢复认证(部分暂停的则部分撤销);

b) 当认证规则、认证准则变更时，在规定时间内不能满足新要求的;  
c) 获证人员不能履行第三方认证机构的相关认证规则中规定的义务;  
d) 获证人员被证实不再符合认证准则所规定的要求。

6.10.4 注销认证

在下列情况下，第三方认证机构应注销认证:

a) 获证人员自愿申请撤销认证;

b) 认证有效期满未申请再认证。

6.10.5 暂停、恢复、撤销和注销认证公告

在暂停、恢复、撤销和注销认证决定后，第三方认证机构将发布认证公告。部分撤销认证的同时更新原有发布的电子证书。

附 录 A

（资料性）

网络空间安全专业人员认证分类

表1 网络空间安全专业人员认证分类

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类别** | **方向** | **适合人员** |
| 1 | 管理类 | 网络安全审计 | 网络安全审计的人员 |
| 2 | 网络安全风险管理 | 网络安全风险管理人员 |
| 3 | 个人信息保护 | 接触到公众或个人信息的各类政企工作人员 |
| 4 | 舆情监控 | 需要随时综合监测网络上传递的与本单位相关的舆情,各类政企工作人员 |
| 5 | 运营类 | 监测预警 | 各级各类网络安全管理人员 |
| 6 | 网络安全规划设计 | 从事各类网络空间相关的软硬件开发、系统设计与分析、网络空间安全规划管理等工作的人员 |
| 7 | 信息系统安全运维 | 从事信息系统运维的技术人员以及数据库操作人员 |
| 9 | 网络安全应急响应 | 针对网络安全事件做应急准备、和事件发生后采取处置措施的人员 |
| 10 | 技术类 | 云计算安全 | 提供云计算服务的企事业单位安全管理人员、安全技术人员等 |
| 11 | 软件安全开发 | 软件开发相关管理与技术人员 |
| 12 | 工业互联网安全 | 企事业单位工业互联网管理和技术人员、提供工业互联网服务的企事业单位的管理和技术人员 |
| 13 | 信息安全集成 | 系统集成相关管理与技术人员 |
| 14 | 渗透测试 | 信息测评单位或其他单位的渗透测试人员 |
| 15 | 大数据安全 | 从事大数据安全的管理和技术人员 |
| 16 | 密码技术 | 对信息数据进行加密、分析、识别和确认以及对密钥进行管理的技术和管理人员 |
| 17 | 人工智能安全 | 人工智能领域的安全管理和技术人员 |
| 18 | 物联网安全 | 物联网安全领域的管理和技术人员 |

附 录 B

（规范性）

通用基础知识考试大纲

B.1 目的

为使考生达到本认证规范中规定网络空间安全专业人员一、二级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证一、二级的人员。

B.2 考试内容

B.2.1课程要求和考试比例

表B.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 网络安全管理实践 | 基础课程 | 全部 | 30% |
| 信息安全技术 | 基础课程 | 全部 | 30% |
| 网络安全合规指引 | 基础课程 | 全部 | 40% |

B.3 各课程知识点要求

B.3.1 网络安全管理实践

表B.2 网络安全管理实践课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 基本概念 | 理解网络安全基本概念和信息安全模型 | 《网络安全管理实践》 |
| 2 | 安全管理策略 | 了解各国网络安全管理策略 |
| 3 | 安全机构和人员管理 | 掌握安全机构和人员管理的职责、管理方法 |
| 4 | 安全技术管理 | 掌握密码学、物理和通讯链路安全、网络安全管理、系统安全管理等基本概念和方法 |
| 5 | 系统建设和安全管理 | 掌握信息安全风险评估、信息安全工程知识  掌握信息系统获取、开发和维护管理 |
| 6 | 安全事件管理和应急响应 | 掌握信息安全事件分类分级  掌握信息安全事件处置方法、流程  掌握网络安全通报预警和应急处置知识、应急预案编制管理知识 |
| 7 | 连续性管理 | 掌握业务连续性管理知识  掌握备份技术和恢复管理知识 |
| 8 | 法规和标准 | 了解网络信息安全相关法律法规  了解网络信息安全管理标准 |
| 9 | 网络安全等级保护 | 了解网络安全等级保护制度和标准  了解信息安全等级保护实施过程  理解安全等级保护定级和备案知识  理解安全等级保护建设知识  掌握安全等级保护测评知识  了解网络安全自查和监督检查知识 |

B.3.2 信息安全技术

表B.3 信息安全技术课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 密码学基础 | 了解密码学发展简史和基本概念  掌握密码学算法知识，如对称密码算法、非对称密码算法、哈希函数和数字签名算法 | 《信息安全技术》 |
| 2 | 密码学应用 | 了解密码学应用基础  了解公钥基础设施  了解虚拟专用网络知识  了解特权管理基础设施  了解其他密码应用知识 |
| 3 | 鉴别和访问控制 | 掌握鉴别的类型、访问控制模型、访问控制技术 |
| 4 | 操作系统安全 | 掌握wHndows系统安全机制相关知识  掌握LHnux系统安全机制相关知识  掌握安全操作系统设计原则 |
| 5 | 网络安全 | 掌握网络安全协议、网络安全设备、网络架构安全知识 |
| 6 | 数据库安全 | 了解数据库系统概念  了解数据库安全知识  理解数据库安全防护方法 |
| 7 | 应用安全 | 了解应用安全概念  掌握web应用安全、互联网服务安全、办公软件安全等知识 |
| 8 | 安全漏洞和恶意代码 | 了解安全漏洞的产生和发展  掌握安全漏洞发现和修复知识  掌握恶意代码的产生和发展、实现技术、防御技术 |
| 9 | 安全攻击和防护 | 了解信息收集和分析的作用、方法和防范  了解常见攻击和防范  了解后门设置与防范、痕迹清除和防范 |
| 10 | 软件安全开发 | 了解软件安全开发背景  掌握软件开发模型知识  掌握软件安全需求和设计  掌握软件安全测试方法 |
| 11 | 新技术安全 | 了解云计算安全、物联网安全、工业控制安全等知识 |

B.3.3 网络安全合规指引

表B.4 网络安全合规指引课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 安全义务 | 了解一般安全义务、网络运营者的安全义务、网络产品和服务提供者的安全义务、涉恐及安全义务 | 《网络安全管理实践》 |
| 2 | 执法程序 | 了解网络安全和信息安全的执法程序 |

B.4 考试说明

B.4.1 题型和分值比例

表B.5 题型和分值比例

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 30 | 1 | 30 |
| 多项选择 | 30 | 1.5 | 45 |
| 判断题 | 10 | 1 | 10 |
| 问答题 | 1 | 15 | 15 |

B.4.2考试时间

总考试时间为60分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

B.4.3 考试合格标准

考试满分为100分，考试成绩60分以上为合格。

附 录 C

（规范性）

网络安全风险管理考试大纲

C.1 目的

为使考生达到本认证规范中规定网络空间安全专业人员管理类网络安全风险管理（Network securHty rHsk management）方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证管理类网络安全风险管理方向三、四级的人员。

C.2 考试内容

C.2.1课程要求和考试比例

表C.1课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 网络安全风险管理人员基本素质 | 基础课程 | 全部 | 5% |
| 网络安全风险管理意识教育 | 基础课程 | 全部 | 5% |
| 网络安全法律法规体系 | 基础课程 | 全部 | 5% |
| 网络安全风险管理基础 | 专业课程 | 全部 | 5% |
| 网络安全风险管理基础（H级） | 专业课程 | 全部 | 10% |
| 网络安全风险管理基础（HH级） | 专业课程 | 全部 | 30% |
| 信息安全风险评估实施方法  （脆弱性、威胁、风险措施） | 专业课程 | 全部 | 30% |
| 信息安全风险评估案例分析 | 专业课程 | 全部 | 10% |

C.3 各课程知识点要求

C.3.1 网络安全风险管理基础

表C.2 网络安全风险管理基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 职业素养 | 了解从事网络安全风险管理工作必备的职业素养 | 《中华人民共和国网络安全法》  《信息安全评测与风险评估》 |
| 2 | 知识结构 | 理解从事网络安全风险管理工作的基础知识 |
| 3 | 工作技能 | 理解从事网络安全风险管理工作的基础技能 |

C.3.2 信息安全风险评估的基础理念

表C.3信息安全风险评估的基础理念课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 信息安全风险评估的基本概念 | 风险评估的的介绍、基本注意事项 | 《信息安全风险评估手册》（[机械工业出版社](https://book.jd.com/publish/%E6%9C%BA%E6%A2%B0%E5%B7%A5%E4%B8%9A%E5%87%BA%E7%89%88%E7%A4%BE_1.html" \t "https://item.jd.com/_blank" \o "机械工业出版社)，HSBN：9787111566052） |
| 2 | 信息安全风险评估相关标准 | 了解国际上通用的信息安全风险评估标准以及国内的风险评估标准 |
| 3 | 信息安全风险评估的发展与现状 | 了解国内信息安全风险评估的发展、现状 |

C.3.3 信息安全风险评估框架及流程

表C.4 信息安全风险评估框架及流程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 信息安全风险评估的主要内容 | 掌握风险评估的的依据、原则；风险评估基础模型、风险分析原理、风险评估方法介绍 | 《信息安全风险评估手册》（[机械工业出版社](https://book.jd.com/publish/%E6%9C%BA%E6%A2%B0%E5%B7%A5%E4%B8%9A%E5%87%BA%E7%89%88%E7%A4%BE_1.html" \t "https://item.jd.com/_blank" \o "机械工业出版社)，HSBN：9787111566052） |
| 2 | 信息系统生命周期各阶段的风险评估 | 掌握信息系统规划、设计、实施、运维、废弃阶段的信息安全风险评估 |
| 3 | 风险评估管理工具及评估工具介绍 | 掌握风险评估管理工具（MBSA、COBRA）、评估工具（极光远程安全评估系统、天镜脆弱性扫描与管理系统、KALH渗透测试工具）使用方法。 |

C.3.4 信息安全风险评估实施方法

表C.4 信息安全风险评估实施方法内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 信息安全风险实施1 | 资产识别（资产分类、资产赋值）、威胁识别（威胁分类、威胁赋值）、脆弱性识别（脆弱性识别、脆弱性赋值） | 《信息安全风险评估手册》（[机械工业出版社](https://book.jd.com/publish/%E6%9C%BA%E6%A2%B0%E5%B7%A5%E4%B8%9A%E5%87%BA%E7%89%88%E7%A4%BE_1.html" \t "https://item.jd.com/_blank" \o "机械工业出版社)，HSBN：9787111566052） |
| 2 | 信息安全风险实施2 | 确认已有安全措施，对识别的风险进行分析，风险计算原理，风险结果判定，制定风险处置计划。 |
| 3 | 信息安全风险报告编制 | 掌握风险评估记录方法，风险评估工作形式（自评估、检查评估），风险计算方法（矩阵法计算风险、相乘法计算风险） |
| 4 | 风险评估辅助工具使用 | 风险评估资产调研表、人员访谈模板、基线检查模板、风险评估工作申请单、项目计划及会议纪要 |
| 5 | 风险评估脆弱性识别工具使用 | 掌握极光远程安全评估系统、天镜脆弱性扫描与管理系统、KALH渗透测试等工具使用方法。 |

C.3.5 网络安全风险防范

表C.5网络安全风险防范内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 信息系统安全风险说明 | 掌握信息系统的安全属性，安全风险要素，风险评估与控制模型。 | 《网络安全风险估计与控制理论》、《网络安全与管理》、 《信息安全管理与风险评估》（网络空间安全技术丛书）、《网络安全意识导论》（网络安全攻防技术》《网络安全管理常用技术》 《网络安全风险识别》 《网络安全测试系统》 《网络空间安全内网攻击防御》 |
| 2 | 信息系统资源分布模型及基于信息资产的风险识别与分析 | 掌握信息网络安全风险识别过程，信息网络系统的威胁识别，信息系统的脆弱性识别，信息系统的风险分析。 |
| 3 | 网络安全机制设计 | 掌握网络安全攻防，安全等设计方法。 |
| 4 | 网络安全访问控制策略设计 | 掌握网络安全访问控制策略的特点，理解当前网络安全访问控制策略的设计。 |
| 5 | 网络云端安全设计 | 掌握网络安全云端安全机制，理解云计算云服务上的安全策略设计。 |
| 6 | 网络安全系统实现 | 掌握网络安全系统设计流程，理解安全平台使用的各种安全机制及其实施。 |

C.3.5 网络安全风险管理

表C.6 网络安全风险管理内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 网络安全系统风险评估 | 掌握信息保护设计原则，风险属性等 | 《网络安全风险估计与控制理论》、《网络安全与管理》、 《信息安全管理与风险评估》（网络空间安全技术丛书）、《网络安全意识导论》（网络安全攻防技术》《网络安全管理常用技术》 《网络安全风险识别》 《网络安全测试系统》 《网络空间安全内网攻击防御》 |
| 2 | 网络安全系统统合规性监管 | 掌握网络安全设备合规性监管及制定网络安全合规程度的方法，掌握构建或调整网络合规性监管方法。 |
| 3 | 网络安全风险事件管理与取证 | 掌握网络安全事件管理内容，理解网络安全事件响应方法的制定、规划与实施，检测与分析以及取证等解决办法。 |
| 4 | 网络安全风险运维 | 掌握网络安全系统生命周期，理解网络安全与风险管理规划、部署、管理、监控与检测、修复与处置等方面的运维方法。 |

C.3.6 信息安全风险评估案例分析

表C.6 信息安全风险评估案例分析内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 信息安全风险评估概述 | 确定评估的内容、评估的依据 | 《信息安全风险评估手册》（[机械工业出版社](https://book.jd.com/publish/%E6%9C%BA%E6%A2%B0%E5%B7%A5%E4%B8%9A%E5%87%BA%E7%89%88%E7%A4%BE_1.html" \t "https://item.jd.com/_blank" \o "机械工业出版社)，HSBN：9787111566052） |
| 2 | 安全现状分析 | 对系统进行介绍、编制资产调查列表、描述网络现状 |
| 3 | 风险评估内容 | 进行安全评估综合分析，具体包括：威胁评估、网络设备安全评估、主机人工安全评估、应用安全评估、网络架构安全评估、无线网络安全评估、工具扫描、管理安全评估 |
| 4 | 风险分析和处理 | 进行综合风险分析，具体包括：综合风险评估方法、综合风险评估分析； 进行风险处置，具体包括：风险处置方式、风险处置计划 |

C.4 考试说明

C.4.1 题型

表 C.7 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 30 | 1 | 30 |
| 多项选择 | 20 | 2 | 40 |
| 判断题 | 10 | 1 | 10 |
| 问答题 | 20 | 10 | 20 |

C.4.2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

C.4.3考试合格标准

考试满分为100分，考试成绩60分以上为合格。

附 录 D

（规范性）

物联网安全考试大纲

D.1目的

为使考生达到本认证规范中规定网络空间安全专业人员技术类物联网安全方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证技术类物联网安全方向三、四级的人员。

D.2考试内容

D.2.1课程要求和考试比例

表D.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 物联网安全基础 | 基础课程 | 全部 | 10% |
| 物联网安全系统规划与实现 | 专业课程 | 全部 | 50% |
| 物联网安全管理与运维 | 专业课程 | 全部 | 15% |
| 物联网渗透测试 | 专业课程 | 全部 | 20% |
| 物联网安全职业素养 | 基础课程 | 全部 | 5% |

D.3 各课程知识点要求

D.3.1 物联网安全基础

表D.2 物联网安全基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 物联网安全概述 | 了解物联网发展过程，理解物联网生态，物联网安全模型以及安全特性。 | 《物联网安全》（网络空间安全技术丛书）、《物联网渗透测试》（网络空间安全技术丛书）、《物联网安全技术》（物联网工程规划教材） |
| 2 | 物联网密码学基础 | 掌握密钥学、密钥管理等相关知识，理解几种典型的密钥管理方案，评估方案优缺点。 |
| 3 | 物联网设备安全开发方法 | 理解物联网设备安全设计和部署采用的各种工程方法。 |
| 4 | 物联网漏洞、攻击及其应对措施 | 理解物联网面临的各种威胁以及应对措施。 |

D.3.2 物联网安全系统规划与实现

表D.3 物联网安全系统规划与实现

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 物联网安全设计方法 | 掌握物联网设备的安全设计方法，理解物联网安全的设计目标。 | 《物联网安全》（网络空间安全技术丛书）、《物联网渗透测试》（网络空间安全技术丛书）、《物联网安全技术》（物联网工程规划教材） |
| 2 | 物联网接入安全设计 | 理解物联网身份识别和访问控制管理机制，理解物联网设备授权和访问控制的设计方法。 |
| 3 | 物联网安全机制设计 | 掌握物联网安全路由、物联网安全时间同步、物联网安全数据融合等设计方法。 |
| 4 | 物联网安全访问控制策略设计 | 掌握物联网访问控制策略的特点，理解当前物联网安全访问控制策略的设计。 |
| 5 | 物联网云端安全设计 | 掌握物联网云端安全机制，理解云计算、雾计算以及物联网云服务上的安全策略设计。 |
| 6 | 物联网安全系统实现 | 掌握物联网安全系统设计流程，理解物联网安全平台使用的各种安全机制及其实施。 |

D.3.3 物联网安全管理与运维

表 D.4 物联网安全管理与运维课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 物联网系统风险评估 | 了解物联网隐私相应评估指南，隐私保护设计原则等 | 《物联网安全》（网络空间安全技术丛书）、《物联网渗透测试》（网络空间安全技术丛书）、《物联网安全技术》（物联网工程规划教材） |
| 2 | 物联网系统合规性监管 | 掌握物联网设备合规性监管及制定物联网合规程度的方法，掌握构建或调整物联网合规性监管方法。 |
| 3 | 物联网安全事件管理与取证 | 掌握物联网安全事件管理内容，理解物联网事件响应方法的制定、规划与实施，检测与分析以及取证等解决办法。 |
| 4 | 物联网安全运维 | 了解物联网系统安全生命周期，理解物联网安全规划、部署、管理、监控与检测、修复与处置等方面的运维方法。 |

D.3.4 物联网渗透测试

表D.5 物联网渗透测试课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | HoT渗透测试基础 | 掌握开展HoT渗透测试的基础知识，掌握HoT渗透测试环境的部署。 | 《物联网安全》（网络空间安全技术丛书）、《物联网渗透测试》（网络空间安全技术丛书）、《物联网安全技术》（物联网工程规划教材） |
| 2 | HoT威胁建模 | 掌握HoT威胁建模概念及方法，掌握HoT Web应用、移动应用、设备硬件以及无线电通信的威胁建模。 |
| 3 | 固件分析与漏洞利用 | 理解固件分析方法、固件提取、固件分析文件系统分析等内容。重点掌握握HoT Web应用、移动应用漏洞利用。 |
| 4 | HoT设备攻击技术 | 理解HoT设备硬件攻击方法以及分析技术、无线电攻击技术等，理解HoT设备中漏洞挖掘与利用。 |
| 5 | HoT自动化防护 | 理解HoT设备中高级漏洞利用技术，掌握采用自动化方法避免HoT设备出现漏洞。 |

D.3.5 物联网安全职业素养

表D.6 物联网安全职业素养课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 网络安全法律法规 | 理解国家网络、信息安全相法律法规。 | 《中华人民共和国网络安全法》 |
| 2 | 物联网安全职业素养 | 了解从事物联网安全保障工作必备的职业素养 |

D.4 考试说明

D.4.1 题型

表D.7 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 30 | 1 | 30 |
| 多项选择 | 20 | 2 | 40 |
| 判断题 | 10 | 1 | 10 |
| 问答题 | 2 | 10 | 20 |

D.4.2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

D.4.3 考试合格标准

考试满分为100分，考试成绩60分以上为合格。

附 录 E

（规范性）

云计算安全考试大纲

E.1 目的

为使考生达到本认证规范中规定网络空间安全专业人员技术类的云计算方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证技术类的云计算方向三、四级的人员。

E.2考试内容

E.2.1课程要求和考试比例

表E.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 云计算基础 | 基础课程 | 全部 | 15% |
| 云计算信息安全及产品 | 基础课程 | 全部 | 10% |
| 云计算信息安全管理及标准 | 专业课程 | 全部 | 25% |
| 访问控制及身份鉴别 | 专业课程 | 全部 | 25% |
| 基础设施和虚拟化安全 | 专业课程 | 全部 | 25% |

E.3 各课程知识点要求

E.3.1 云计算基础

表E.2 云计算基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 云计算的定义、特点及发展历史 | 了解云计算的定义及基本概念、发展历史和主要特点，掌握云计算与传统HT的区别。 | 《云计算：概念、技术与架构》、《云计算数据中心规划与设计》《大规模分布式存储系统-原理解析与架构实战》 |
| 2 | 云计算数据中心的组成 | 了解云计算数据中心分类和建设标准，掌握云计算数据中心的基本架构，云计算系统的组成、安全体系架构。 |
| 3 | 云计算服务的分类 | 了解云计算服务的分类，各类服务包含的具体产品类别及相互关系。 |
| 4 | 主流云计算厂商及技术 | 了解云计算行业内主流国内和国外厂商产品、服务及特点。了解各云计算厂商的主要技术及发展趋势。 |
| 5 | 云存储技术及产品 | 了解云存储技术的种类及特点，掌握云存储产品和服务所使用的技术和特点。 |
| 6 | 虚拟化技术及发展 | 了解不同层次的虚拟化技术及分类，掌握典型虚拟化方案的具体实现，了解虚拟化发展的方向。 |

E.3.2云计算信息安全及产品

表 E.3 云计算信息安全及产品课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 云计算安全与传统信息安全的特点比较 | 了解云计算环境与传统HT信息安全方面的面临问题的差异。 | 《云安全原理与实践》、《云计算信息安全管理—CSA C-STAR实施指南》 |
| 2 | 云计算主要的安全问题及分类 | 了解云计算面临在主要安全问题及分类，掌握安全威胁的种类、基本原理和防御手段。 |
| 3 | 云计算网络安全及产品 | 了解云计算安全产品和服务的分类，掌握各厂商特色安全产品及特点。熟悉安全等级保护对应的安全产品。 |

E.3.2云计算信息安全管理及标准

表E.4 云计算信息安全管理及标准课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 云计算相关国际、国内标准及规定 | 了解云计算安全管理标准化工作概况，掌握HSO27001、HSO27018等主要安全管理标准及对应的国家标准。 | 《云计算信息安全管理—CSAC-STAR实施指南》、《云计算安全体系/信息安全国家重点实验室信息安全丛书》 |
| 2 | 云计算安全管理的规定和要求 | 掌握《网络安全法》、《计算机信息系统安全保护条例》等主要法律法规对云计算的要求。 |
| 3 | 信息安全管理体系、方法及安全评估模型 | 了解云计算安全管理体系及管理方法，了解云计算信息安全评估模型。 |

E.3.3 访问控制及身份鉴别

表E.5 访问控制及身份鉴别课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 主机的访问控制 | 了解云计算虚拟主机的访问控制相关技术，了解访问控制模型及实现机制，掌握常用的访问控制手段和控制策略。 | 《访问控制/全国网络安全与执法专业丛书》、《GM/Y5002-2018云计算身份鉴别服务密码标准体系》 |
| 2 | SSL、VPN及堡垒机 | 了解SSL、VPN及堡垒机涉及的相关安全技术，了解主流厂商产品及特点，掌握SSL、VPN及堡垒机在云资源的安全使用和运维方面的作用。 |
| 3 | 身份鉴别及密码技术 | 了解云计算环境身份鉴别面临的挑战，熟悉鉴别与授权、身份管理、公钥密码体系等技术及应用，了解国家相关标准在身份鉴别方面的要求。 |

E.3.4基础设施和虚拟化安全

表E.6 基础设施和虚拟化安全课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 云数据中心的安全 | 了解云计算数据中心面临的安全问题，掌握云技术数据中心相关的安全设计及防护方法。 | 《云计算数据中心规划与设计》、《网络攻防技术与实战》、《云计算安全/网络空间安全系列丛书》、《云虚拟化安全攻防实践》、《虚拟化安全解决方案》 |
| 2 | 主机虚拟化安全 | 了解虚拟化架构及安全挑战、熟悉主流虚拟化管理软件及技术特点，了解虚拟化安全相关技术及解决方案。 |

E.4考试说明

E.4.1 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择题 | 30 | 1 | 30 |
| 不定项选择题 | 30 | 2 | 60 |
| 判断题 | 10 | 1 | 10 |

E.4.2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

E.4.3考试合格标准

考试满分为100分，考试成绩60分以上为合格。

附 录 F

（规范性）

网络安全规划设计方向考试大纲

F.1 目的

为使考生达到本认证规范中规定网络空间安全专业人员运营类网络安全规划设计方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲)，本大纲适用于所有申请网络空间安全专业人员认证运营类网络安全规划设计方向三、四级的人员。

F.2 考试内容

F.2 .1课程要求和考试比例

表F.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 信息安全保障人员基本素质 | 基础课程 | 全部 | 5% |
| 信息安全意识教育 | 基础课程 | 全部 | 10% |
| 信息安全法律法规体系 | 基础课程 | 全部 | 10% |
| 密码学基础 | 专业课程 | 全部 | 10% |
| 计算机网络 | 专业课程 | 全部 | 15% |
| 计算机网络安全 | 专业课程 | 全部 | 30% |

F.3 各课程知识点要求

F.3.1 信息安全法律法规体系

表 F.2课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 信息安全法律、行政法规 | 掌握网络安全法、数据安全法等法律、法规主要内容 | 《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国密码法》、《中华人民共和国网络安全审查办法》、《GB/T 22239-2019信息安全技术网络安全等级保护基本要求》等 |
| 2 | 网络安全标准 | 掌握网络安全相关的国家标准、行业标准 |
| 3 | 其他政策性文件 | 了解其他配套的政策性文件、法律法规解读等 |

F.3.2 密码学基础

表 F.3 密码学基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 网络安全基本概念 | 掌握安全三性，密码学基本算法 | 《密码编码学与网络安全-原理与实践》 |
| 2 | 数论基础 | 掌握除法、模运算、素数、相关定理的应用 |
| 3 | 对称密码 | 掌握对称密码的概念、经典技术及应用 |
| 4 | 非对称密码 | 掌握非对称密码的概念、经典技术及应用 |
| 5 | 互信 | 掌握密钥分发、证书、签名、用户认证等经典应用场景 |
| 6 | 网络和因特网安全 | 掌握密码技术在网络层、互联网应用、无线、邮件、云计算、物联网等领域的经典应用场景。 |

F.3.3 计算机网络

表F.4 计算机网络课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 网络体系结构概述 | 掌握TCP/HP的核心目标和体系结构概念 | 《TCP/HP详解》 |
| 2 | 网络协议 | 掌握链路层、网络层、传输层、应用层等协议内容与经典应用场景。 |
| 3 | 网络安全基础知识 | 掌握EAP、HPsec、TLS、DNSSEC等网络安全基础知识。 |

F.3.4 计算机网络安全

表F.5 计算机网络课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 网络安全概论 | 介绍网络安全基本概念，掌握网络安全概念与目标，安全技术发展等 | 《计算机网络安全原理》 |
| 2 | 网络安全基础内容 | 掌握密码学基础、数字认证、数字签名、身份认证、数字证书、PKH等内容 |
| 3 | 网络层协议安全 | 掌握各网络层协议内容、脆弱性与安全协议 |
| 4 | 常见网络安全攻防内容 | 包括web安全、邮件安全、DDOS、防火墙、恶意代码、入侵监测等内容 |
| 5 | 网络安全新技术 | 包括SDN、零信任等 |

F.4 考试说明

F.4 .1 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 20 | 2 | 40 |
| 多项选择 | 20 | 2 | 40 |
| 判断题 | 10 | 2 | 20 |

F.4 .2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

F.4 .3考试合格标准

考试满分为100分，考试成绩60分以上为合格。

附 录 G

（规范性）

信息系统安全运维人员考试大纲

G.1目的

为使考生达到本认证规范中规定网络空间安全专业人员信息系统安全运维方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证技术类信息系统安全运维方向三、四级的人员。

G.2 考试内容

G.2 .1课程要求和考试比例

表G.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 信息安全技术 | 专业课程 | 全部 | 10% |
| 信息系统安全运维 | 专业课程 | 全部 | 50% |
| 网络安全等保2.0技术产品 | 基础课程 | 全部 | 15% |
| 渗透测试与攻防实战 | 专业课程 | 全部 | 20% |
| 信息安全法律法规 | 基础课程 | 全部 | 5% |

G.3 各课程知识点要求

G.3.1 信息安全技术课程内容与要求

表G.2 信息安全技术课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 信息安全概论 | 介绍了信息安全的基本概 念、原理和知识体系 | 《物理安全》  《密码学基础与安全应用》  《网络安全技术》  《信息安全原理与实践（第2版）》 |
| 2 | 物理安全 | 包括物理安全概述、物理安全需要注意哪些方面以及相关的法律、法规等内容 |
| 3 | 通讯和网络安全工程 | 包括网络结构安全分析技术及其它的安全服务和安全机制策略等。 |
| 4 | 密码学及其应用 | 包括密码学基础知识、对称加密算法、非对称加密算法、散列算法及其应用、数字签名、PKH技术、SSL、SSH、HPSec、PGP加密文件系统等。 |

G.3.2 信息系统安全运维

表G.3 信息系统安全运维课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 操作系统安全原理与实践 | 掌握LHnux系统操作、文件管理、权限管理、常见漏洞、安全加固等。 | 《操作系统安全设计》、《软件安全分析与应用》、《[数据库安全技术](http://product.dangdang.com/1901054800.html" \o " 数据库安全技术" \t "http://search.dangdang.com/_blank)》、《[Web安全攻防：渗透测试实战指南](http://product.dangdang.com/25315023.html" \o " Web安全攻防：渗透测试实战指南 " \t "http://search.dangdang.com/_blank)》 |
| 2 | 常用数据库安全原理与实践 | 掌握包括数据库安全性控制概述，用户管理和角色管理，SQL Server的安全机制 |
| 3 | 应用开发安全 | 了解二进制程序分析、恶意代码分析、软件漏洞挖掘分析、网络协议逆向分析、应用软件安全分析等。 |
| 4 | Web安全渗透实战 | Web服务中常见安全漏洞，包括SQLH/XSS/CSRF/XXE/反序列化/上传/包含/业务逻辑等漏洞。 |

G.3.3 网络安全等保2.0技术产品

表G.4 网络安全等保2.0技术产品课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | VPN原理与实践 | 掌握HPsec VPN、GRE Over HPsec、DMVPN、SSL VPN等网络安全技术。 | 《防火墙与VPN原理与实践》  《入侵检与入侵防御》  《漏洞扫描与防护》 |
| 2 | 防火墙原理与实践 | 掌握[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99" \t "https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99%E4%B8%8EVPN%E5%8E%9F%E7%90%86%E4%B8%8E%E5%AE%9E%E8%B7%B5/_blank)安装和配置实践，特定的[防火墙技术](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99%E6%8A%80%E6%9C%AF" \t "https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99%E4%B8%8EVPN%E5%8E%9F%E7%90%86%E4%B8%8E%E5%AE%9E%E8%B7%B5/_blank)、工具和技巧 |
| 3 | 入侵防御原理与实践 | 掌握入侵防御系统的功能、原理与部署、关键技术 |
| 4 | 漏洞扫描原理与实践 | 掌握漏洞扫描与防护相关理论与技术 |
| 5 | 信息安全审计 | 掌握如何根据相关标准、法规进行合规性安全审计，以及如何对计算机信息系统中的所有网络资源（包括数据库、主机、操作系统、网络设备、安全设备等）进行安全审计，记录所有发生的事件，为系统管理员提供系统维护以及安全防范的依据。 | 《信息安全审计》 |
| 6 | 安全设备 | 了解HPS、上网行为管理，WAF主流产品 |  |

G.3.4 渗透测试与攻防实战

表G.5 渗透测试与攻防实战课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | web安全渗透测试与安全防御 | 了解渗透测试的基础知识，掌握渗透测试环境的部署，重点掌握Web应用、移动应用漏洞利用。 | 《Web安全攻防：渗透测试实战指南 》  《KalHLHnux高级渗透测试(第2版)》  《无线网络安全攻防实战》 |
| 2 | KalH LHnux渗透测试攻防实战 | 掌握KalH LHnux渗透测试的各种核心技术，涵盖从安装配置，到信息收集和漏洞扫描及利用，再到权限提升及各种渗透测试等技术。 |
| 3 | WHFH无线安全攻防 | 掌握设备硬件以及无线电通信的威胁。 |
| 4 | 攻防实战 | 掌握攻防实战技术 |

G.3.4 网络安全法律法规

表G.6 网络安全法律法规课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 网络安全法律法规 | 掌握网络安全法、数据安全法等法律、法规主要内容。 |  |

G.4 考试说明

G.4.1题型

表G.7 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 30 | 1 | 30 |
| 多项选择 | 20 | 2 | 40 |
| 判断题 | 10 | 1 | 10 |
| 问答题 | 2 | 10 | 20 |

G.4.2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

G.4.3 考试合格标准

考试满分为100分，考试成绩70分以上为合格。

附 录H

（规范性）

软件安全开发方向考试大纲

H.1 目的

为使考生达到本认证规范中规定网络空间安全专业人员技术类软件安全开发方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证技术类软件安全开发三、四级的人员。

H.2 考试内容

H.2.1 课程要求和考试比例

表H.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 项目管理基础 | 基础课程 | 全部 | 15% |
| 信息安全技术 | 专业课程 | 全部 | 35% |
| 软件安全开发 | 专业课程 | 全部 | 50% |

H.3 各课程知识点要求

H.3.1 项目管理基础

表H.2 项目管理基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 项 目 管 理 基本概念 | 正确理解项目的本质  正确理解管理的本质  掌握项目管理的基本分类  熟练掌握项目管理的生命周期与流程  掌握项目管理相对其 他管理的特性 | 1.《信息安 全保障人员认证考试辅 导丛书》  2.各类项目管理期刊  3.各类项目管理正式出 版文献  4.PM相关书籍5.PrHnce2 相关书籍 |
| 2 | 项目管理的发展历史与现状 | 了解项目管理的发展过程  了解国际项目管理发展现状  了解国际国内项目管理人员认证情 |
| 3 | 九大项目管理知识领域 | 熟练掌握项目综合管理、项目范围管理、 项目时间管理、项目成本管理、项目质量管理、项目人力资源管理、项目沟通管理、 项目风险管理和项目采购管理思想与方法  掌握项目综合管理、 项目范围管理、项目 时间管理、项目成本管理、项目质量管理、 项目人力资源管理、 项目沟通管理、项目风险管理和项目采购管理工具和实施技巧 |
| 4 | 开发类项目管理技巧 | 掌握开发类项目管理的特点  掌握开发类项目生命周期  正确掌握开发类项目九大管理知识领域特性  实践一个完整的开发类项目过程 |
| 5 | 集成类项目管理技巧 | 掌握集成类项目管理的特点  掌握集成类项目生命周期  掌握集成类项目九大管理知识领域特性  实践一个完整的集成 |

H.3.2 信息安全技术

表H.3 信息安全技术课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 密码学基础 | 了解密码学发展简史和基本概念  掌握密码学算法知识，如对称密码算法、非对称密码算法、哈希函数和数字签名算法 | 《信息安全技术》 |
| 2 | 密码学应用 | 了解密码学应用基础  了解公钥基础设施  掌握虚拟专用网络知识  了解特权管理基础设施  掌握其他密码应用知识 |
| 3 | 鉴别和访问控制 | 掌握鉴别的类型、访问控制模型、访问控制技术 |
| 4 | 操作系统安全 | 掌握wHndows系统安全机制相关知识  掌握LHnux系统安全机制相关知识  掌握安全操作系统设计原则 |
| 5 | 网络安全 | 掌握网络安全协议、网络安全设备、网络架构安全知识 |
| 6 | 数据库安全 | 了解数据库系统概念  掌握数据库安全知识  掌握数据库安全防护方法 |
| 7 | 应用安全 | 了解应用安全概念  掌握web应用安全、互联网服务安全、办公软件安全等知识 |
| 8 | 安全漏洞和恶意代码 | 了解安全漏洞的产生和发展  掌握安全漏洞发现和修复知识  掌握恶意代码的产生和发展、实现技术、防御技术 |
| 9 | 安全攻击和防护 | 了解信息收集和分析的作用、方法和防范  了解常见攻击和防范  掌握后门设置与防范、痕迹清除和防范 |
| 10 | 软件安全开发 | 熟悉软件安全开发背景  掌握软件开发模型知识  掌握软件安全需求和设计  掌握软件安全测试方法 |
| 11 | 新技术安全 | 掌握云计算安全、物联网安全、工业控制安全等知识 |

H.3.3 软件安全开发

表H.4 软件安全开发课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 软件安全开发基础 | 了解软件安全开发背景  了解软件安全开发概念  了解软件安全开发方法  了解软件安全开发风险管理、信息系统安全工程、CC标准等 | 《软件安全开发》 |
| 2 | 软件安全需求分析 | 了解软件安全需求的定义和分类、安全需求工程  熟练掌握安全需求分析方法 |
| 3 | 软件安全设计 | 了解软件设计主要工作  熟悉软件安全设计原则和减少受攻击面知识  掌握软件安全设计方法  掌握软件架构安全性分析方法  熟练掌握威胁建模知识 |
| 4 | 安全编码 | 了解软件漏洞含义及分类  掌握软件安全编码原则和安全编程基础知识  掌握Web应用安全编程方法  掌握数据安全编码知识 |
| 5 | 软件安全测试 | 掌握软件安全测试基础知识  熟练掌握代码分析知识  熟练掌握模糊测试和渗透测试知识 |
| 6 | 软件部署和项目管理安全 | 掌握软件部署安全知识  掌握软件项目管理安全知识  了解软件安全编码规范检查列表、安全测试工具、测试文档模版等 |

H.4 考试说明

H.4.1 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 30 | 1 | 30 |
| 多项选择 | 20 | 2 | 40 |
| 判断题 | 10 | 1 | 10 |
| 问答题 | 20 | 10 | 20 |

H.4.2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

H.4.3 考试合格标准

考试满分为100分，考试成绩60分以上为合格。

附 录 I

(规范性)

网络安全应急响应方向考试大纲

I.1 目的

为使考生达到本认证规范中规定网络空间安全专业人员运营类网络安全应急响应方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证运营类网络安全应急响应方向三、四级的人员。

I.2考试内容

I.2.1课程要求和考试比例

表I.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 项目管理基础 | 基础课程 | 全部 | 15% |
| 信息安全技术 | 基础课程 | 全部 | 25% |
| 通信技术基础 | 基础课程 | 全部 | 10% |
| 网络安全应急响应 | 专业课程 | 全部 | 50% |

I.3 各课程知识点要求

1.3.1 项目管理基础

表I.2 项目管理基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 项目管理基本概念 | 正确理解项目的本质  正确理解管理的本质  掌握项目管理的基本分类  熟练掌握项目管理的生命周期与流程  掌握项目管理相对其他管理的特性 | 《信息安全保障人员认证考试辅 导丛书》  2.各类项目管理期刊  3.各类项目管理正式出 版文献 4.PMP 相关书籍 5.PrHnce2 相关书籍 |
| 2 | 项目管理的发展历 史与现状 | 了解项目管理的发展过程  了解国际项目管理发展现状  了解国际国内项目管理人员认证情 |
| 3 | 九大项目管理知识领域 | 熟练掌握项目综合管理、项目范围管理、 项目时间管理、项目成本管理、项目质量 管理、项目人力资源 管理、项目沟通管理、 项目风险管理和项目 采购管理思想与方法  掌握项目综合管理、 项目范围管理、项目 时间管理、项目成本管理、项目质量管理、 项目人力资源管理、 项目沟通管理、项目风险管理和项目采购管理工具和实施技巧 |
| 4 | 开发类项目管理技巧 | 掌握开发类项目管理的特点  掌握开发类项目生命周期  正确掌握开发类项目九大管理知识领域特性  实践一个完整的开发类项目过程 |
| 5 | 集成类项目管理技巧 | 掌握集成类项目管理的特点  掌握集成类项目生命周期  掌握集成类项目九大管理知识领域特性  实践一个完整的集成 |

1.3.2 信息安全技术

表I.3 信息安全技术课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 密码学基础 | 了解密码学发展简史和基本概念  掌握密码学算法知识，如对称密码算法、非对称密码算法、哈希函数和数字签名算法 | 《信息安全技术》 |
| 2 | 密码学应用 | 了解密码学应用基础  了解公钥基础设施  掌握虚拟专用网络知识  了解特权管理基础设施  掌握其他密码应用知识 |
| 3 | 鉴别和访问控制 | 掌握鉴别的类型、访问控制模型、访问控制技术 |
| 4 | 操作系统安全 | 掌握wHndows系统安全机制相关知识  掌握LHnux系统安全机制相关知识  掌握安全操作系统设计原则 |
| 5 | 网络安全 | 掌握网络安全协议、网络安全设备、网络架构安全知识 |
| 6 | 数据库安全 | 了解数据库系统概念  掌握数据库安全知识  掌握数据库安全防护方法 |
| 7 | 应用安全 | 了解应用安全概念  掌握web应用安全、互联网服务安全、办公软件安全等知识 |
| 8 | 安全漏洞和恶意代码 | 了解安全漏洞的产生和发展  掌握安全漏洞发现和修复知识  掌握恶意代码的产生和发展、实现技术、防御技术 |
| 9 | 安全攻击和防护 | 了解信息收集和分析的作用、方法和防范  了解常见攻击和防范  掌握后门设置与防范、痕迹清除和防范 |
| 10 | 软件安全开发 | 熟悉软件安全开发背景  掌握软件开发模型知识  掌握软件安全需求和设计  掌握软件安全测试方法 |
| 11 | 新技术安全 | 掌握云计算安全、物联网安全、工业控制安全等知识 |

1.3.3 通讯技术基础

表I.4 通讯技术基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 通信的基本概念 | 理解通信的本质含义及电信概念  理解通信网络形成过程  了解通信网络结构  了解通信网络中的安全属性  了解通信网络应用分类  了解“网络”习惯分类  了解通信网络安全问题本质成因 | 《通信技术基础》  各类通信原理相关书籍 |
| 2 | 通信协议及应用 | 熟悉 OSH 七层模型  熟悉 TCP/HP 协议族的基本协议及  TCP/HP 协议族存在的固有安全问题  熟悉 HPv6、移动互联网等技术及应用  了解典型的通信网络及设备 |
| 3 | 安全通信协议 | 了解典型的安全通信协议  了解典型的安全通信协议在通信过程中的应用 |

1.3.4 网络安全应急响应

表I.5 网络安全应急响应课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 网络安全应急响应技术概念 | 了解网络安全应急响应的含义和相关法规  了解网络安全应急响应技术的发展趋势  了解网络安全应急响应技术框架  了解网络安全应急响应新发展 | 《网络安全应急响应》 |
| 2 | 网络安全应急响应技术基础知识 | 掌握风险评估相关概念、流程  了解风险评估与应急响应的关系  了解安全事件分级分类 |
| 3 | 网络安全应急响应技术流程与方法 | 熟练掌握应急响应准备阶段、抑制阶段、保护阶段、事件检测阶段、取证阶段、根除阶段、恢复阶段、总结报告等各阶段知识 |
| 4 | 应急演练 | 了解应急演练定义、目的、原则  了解应急演练分类及方法  了解应急演练的组织架构  了解应急演练流程和规划  掌握应急演练的实施和总结 |
| 5 | 网络安全事件应急处置实战 | 掌握常见Web 攻击应急处置实战知识  掌握信息泄露类攻击应急处置实战知识  掌握主机类攻击应急处置实战知识  掌握有害事件应急处置实战知识 |
| 6 | 分析排查 | 掌握wHndows/LHnux的分析排查知识 |

1.4 考试说明

I.4.1 题型

表I.6 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 30 | 1 | 30 |
| 多项选择 | 20 | 2 | 40 |
| 判断题 | 10 | 1 | 10 |
| 问答题 | 20 | 10 | 20 |

I.4.2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

I.4.3 考试合格标准

考试满分为100分，考试成绩60分以上为合格。

附 录 J

(规范性)

信息系统安全集成方向考试大纲

J.1 目的

为使考生达到本认证规范中规定网络空间安全专业人员技术类信息安全集成方向三、四级能力要求，指导考生有效准备考试，特制定本考试大纲(以下简称大纲),本大纲适用于所有申请网络空间安全专业人员认证技术类信息安全集成方向三、四级的人员。

J.2考试内容

J.2.1课程要求和考试比例

表J.1 课程要求和考试比例

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 课程类型 | 选择范围 | 考试所占比例 |
| 项目管理基础 | 基础课程 | 全部 | 20% |
| 信息安全技术 | 基础课程 | 全部 | 30% |
| 安全集成 | 基础课程 | 全部 | 30% |
| 通信技术基础 | 基础课程 | 全部 | 20% |

J.3 各课程知识点要求

J.3 .1项目管理基础

表J.2 项目管理基础课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 项 目 管 理 基本概念 | 正确理解项目的本质  正确理解管理的本质  掌握项目管理的基本分类  熟练掌握项目管理的生命周期与流程  掌握项目管理相对其 他管理的特性 | 《信息安 全保障人员认证考试辅 导丛书》  2.各类项目 管理期刊  3.各类项目 管理正式出 版文献  4.PMP 相关 书籍 5.Prince2 相关书籍 |
| 2 | 项目管理 的发展历 史与现状 | 了解项目管理的发展过程  了解国际项目管理发展现状  了解国际国内项目管理人员认证情 |
| 3 | 九大项目管理知识领域 | 熟练掌握项目综合管 理、项目范围管理、 项目时间管理、项目 成本管理、项目质量 管理、项目人力资源 管理、项目沟通管理、 项目风险管理和项目 采购管理思想与方法  掌握项目综合管理、 项目范围管理、项目 时间管理、项目成本管理、项目质量管理、 项目人力资源管理、 项目沟通管理、项目风险管理和项目采购 管理工具和实施技巧 |
| 4 | 开发类项目管理技巧 | 掌握开发类项目管理的特点  掌握开发类项目生命周期  正确掌握开发类项目九大管理知识领域特性  实践一个完整的开发类项目过程 |
| 5 | 集成类项目管理技巧 | 掌握集成类项目管理的特点  掌握集成类项目生命周期  掌握集成类项目九大管理知识领域特性  实践一个完整的集成 |

J.3 .2 信息安全技术

表J.3 信息安全技术课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 密码学基础 | 了解密码学发展简史和基本概念  掌握密码学算法知识，如对称密码算法、非对称密码算法、哈希函数和数字签名算法 | 《信息安全技术》 |
| 2 | 密码学应用 | 了解密码学应用基础  了解公钥基础设施  掌握虚拟专用网络知识  了解特权管理基础设施  掌握其他密码应用知识 |
| 3 | 鉴别和访问控制 | 掌握鉴别的类型、访问控制模型、访问控制技术 |
| 4 | 操作系统安全 | 掌握windows系统安全机制相关知识  掌握Linux系统安全机制相关知识  掌握安全操作系统设计原则 |
| 5 | 网络安全 | 掌握网络安全协议、网络安全设备、网络架构安全知识 |
| 6 | 数据库安全 | 了解数据库系统概念  掌握数据库安全知识  掌握数据库安全防护方法 |
| 7 | 应用安全 | 了解应用安全概念  掌握web应用安全、互联网服务安全、办公软件安全等知识 |
| 8 | 安全漏洞和恶意代码 | 了解安全漏洞的产生和发展  掌握安全漏洞发现和修复知识  掌握恶意代码的产生和发展、实现技术、防御技术 |
| 9 | 安全攻击和防护 | 了解信息收集和分析的作用、方法和防范  了解常见攻击和防范  掌握后门设置与防范、痕迹清除和防范 |
| 10 | 软件安全开发 | 熟悉软件安全开发背景  掌握软件开发模型知识  掌握软件安全需求和设计  掌握软件安全测试方法 |
| 11 | 新技术安全 | 掌握云计算安全、物联网安全、工业控制安全等知识 |

J.3.3 信息安全集成

表J.4 信息安全集成课程内容与要求

|  |  |  |  |
| --- | --- | --- | --- |
| 章节号 | 章节名 | 内容与要求 | 参考文献 |
| 1 | 安全集成的业界标准与实践 | 掌握 GB/T 20261 对安全集成的要求  掌握 ISO/IEC 21827对安全集成的要求  掌握 SSE-CMM3.0 对安全集成的要求  掌握信息系统安全集成服务资质认证实施规则对安全集成的要求  掌握 CNCA/CTS 0052 信息安全服务资质认证技术规范 | 《信息安全集成》 |
| 2 | 安全集成过程 | 掌握安全软件集成管 理的全过程  掌握安全集成准备工作(如需求分析)的主要方法 掌握安全集成设计的主要方法 掌握安全集成实施的主要工作 掌握安全集成保证的主要内容 |
| 3 | 安全集成 工具使用 | 熟悉典型的安全集成工具;  熟悉需求分析工具使用；  熟悉安全集成设计工具使用 ；  熟悉安全保证工具使用 ； |
| 4 | 典型安全保障手段 | 熟悉典型的信息安全保障手段  熟悉常用的信息安全技术应用  熟悉常用的信息安全产品 |
| 5 | 安全集成实例 | 熟悉安全集成方案的结构  熟悉主要行业的安全集成特性  理解 1-2 个行业的典型安全集成实例 |

J.3.4 通信技术基础

表J.5 通信技术基础课程内容与要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 章节号 | | 章节名 | 内容与要求 | 参考文献 |
| 1 | 通信的基本概念 | | 理解通信的本质含义及电信概念  理解通信网络形成过程  了解通信网络结构  了解通信网络中的安全属性  .了解通信网络应用分类  了解“网络”习惯分类  了解通信网络安全问题本质成因 | 《通信技术基础》  各类通信原理相 关书籍 |
| 2 | 通信协议及应用 | | 熟悉 OSI 七层模型   熟悉 TCP/IP 协议族的基本协议及  TCP/IP 协议族存在的固有安全问题   熟悉 IPv6、移动互联网等技术及应用   了解典型的通信网络及设备 |
| 3 | 安全通信协议 | | 了解典型的安全通信协议  了解典型的安全通信协议在通信过程中的应用 |

J.4 考试说明

J.4.1 题型

表J.6 题型

|  |  |  |  |
| --- | --- | --- | --- |
| 题型 | 数量 | 单题分值（分） | 小计分值（分） |
| 单项选择 | 30 | 1 | 30 |
| 多项选择 | 20 | 2 | 40 |
| 判断题 | 10 | 1 | 10 |
| 问答题 | 20 | 10 | 20 |

J.4.2 考试时间

总考试时间为120分钟，提前15分钟进入考场，迟到30分钟以上的视为放弃考试，考试开始后30分钟内离场的成绩无效。

J.4.3 考试合格标准

考试满分为100分，考试成绩60分以上为合格。

参 考 文 献

[l] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1 部分：简介和 一般模型

[2] GB/T 27203-2016 合格评定 用于人员认证的人员能力词汇

[3] GB/T 27024-2014 合格评定 人员认证机构通用要求