信息安全保障人员认证考试大纲

ISCCC-COP-R02

中国信息安全认证中心

发布日期：2013 年 4 月 22 日　　实施日期：2012 年 2 月 10 日

信息安全保障人员认证考试大纲

1 目的

为使考生达到《信息安全保障人员认证准则》规定的各个方向和级别的能力要求，指导考生有效准备考试，特制定本考试大纲（以下简称大纲）。

2 适用范围

本大纲适用于所有参与信息安全保障人员认证的机构和个人。

3 术语与定义

本大纲采用下列术语定义。

3.1 信息安全保障人员（CISAW）

从事信息安全相关工作的所有人员，如组织的管理人员（包括 CIO、CSO、科技管理部门和风险控制管理部门的人员）、IT 相关的技术人员（包括运维、开发和集成人员）、信息安全服务组织的技术人员（包括信息安全产品研发人员、信息安全咨询人员、信息安全服务实施人员和外派服务人员）。

4 考试

4.1 考试机构

CISAW 考试机构为中国信息安全认证中心。

4.2 考试范围与要求

依据《信息安全保障人员认证准则》要求，制定考试范围，如表 1 所示。

表 1. 认证分类分级与考试范围结构图

专业方向		安全软件	安全集成	安全管理	安全运维	安全咨询	风险管理	应急服务	灾备服务	业务连续性
类别	级别	考试课程								
专业认证	III级(专业高级)	III 级专业课程①+附加课程②+II 级信息安全实验（适用时）③								
	II级（专业级）	II级通用课程④+II级专业课程								
资格认证	I 级（基础级）	基础课程⑤+I级通用课程								
预备认证	预备级	大专院校认定课程+基础课程								

注①参见 4.2.4，注②参见 4.2.5，注③参见 4.2.3，注④参见 4.2.3，注⑤参见 4.2.2。

4.2.1 各认证级别、专业方向相关要求

各认证级别和专业方向的范围与要求见表 2-20：

表 2：《基础级》范围与要求

课程名称	课程类型	选择范围	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%
风险管理基础	基础课程	全部	15%
项目管理基础（I 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	1、3、7 必选 2、4、5、6 任选 2 个以上	50%

表 3：《安全软件专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	2、5、6	10%
安全软件技术与测试（II 级）	专业课程	全部	80%
信息安全实验（I 级）	通用课程	任选 3 个以上	

表 4：《安全软件专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例
信息安全技术（II 级）	通用课程	2、5、6	20%
安全软件技术与测试（III 级）	专业课程	全部	80%
信息安全实验（II 级）	通用课程	任选 2 个以上	

表 5：《安全集成专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	全部	50%
安全集成（II 级）	专业课程	全部	30%
通信技术基础	附加课程	全部	10%
信息安全实验（I 级）	通用课程	任选 3 个以上	

表 6：《安全集成专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例

信息安全技术（II 级）	通用课程	全部	40%
安全集成（III 级）	专业课程	全部	50%
通信技术基础	附加课程	全部	10%
信息安全实验（II 级）	通用课程	任选 2 个以上	

表 7：《安全管理专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	1、3、4、7	10%
安全管理（II 级）	专业课程	全部	80%
安全管理实验（I 级）	通用课程	安全管理实验	

表 8：《安全管理专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例
信息安全技术（II 级）	通用课程	1、3、4、7	10%
安全管理（III 级）	专业课程	全部	70%
管理体系审核	附加课程	全部	20%
安全管理实验（II 级）	通用课程	安全管理实验	

表 9：《安全运维专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	1、3、4、7	20%
安全运维技术与应用（II 级）	专业课程	全部	70%
信息安全实验（I 级）	通用课程	任选 3 个以上	

表 10：《安全运维专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例
信息安全技术（II 级）	通用课程	1、3、4、7	20%
安全运维技术与应用（III 级）	专业课程	全部	80%
信息安全实验（II 级）	通用课程	任选 2 个以上	

表 11：《安全咨询专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%

信息安全技术（I 级）	通用课程	全部	20%
安全咨询（II 级）	专业课程	全部	60%
通信技术基础	附加课程	全部	10%

表 12：《安全咨询专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例
信息安全技术（II 级）	通用课程	全部	10%
安全咨询（III 级）	专业课程	全部	80%
通信技术基础	附加课程	全部	10%

表 13：《风险管理专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	3、4、5、6	10%
风险管理（II 级）	专业课程	全部	70%
通信技术基础	附加课程	全部	10%
信息安全实验（I 级）	通用课程	任选 3 个以上	

表 14：《风险管理专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例
信息安全技术（II 级）	通用课程	3、4、5、6	10%
风险管理（III 级）	专业课程	全部	80%
通信技术基础	附加课程	全部	10%
信息安全实验（II 级）	通用课程	任选 2 个以上	

表 15：《应急服务专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	3、4	10%
应急服务技术与应用（II 级）	专业课程	全部	60%
通信技术基础	附加课程	全部	10%
渗透测试技术与应用	附件课程	全部	10%
信息安全实验（I 级）	通用课程	任选 3 个以上	

表 16：《应急服务专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例

信息安全技术（II 级）	通用课程	3、4	10%
应急服务技术与应用（III 级）	专业课程	全部	70%
通信技术基础	附加课程	全部	10%
渗透测试技术与应用	附件课程	全部	10%
信息安全实验（II 级）	通用课程	任选 2 个以上	

表 17：《灾备服务专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	3、4、6、7	10%
灾备服务技术与应用（II 级）	专业课程	全部	80%
信息安全实验（I 级）	通用课程	任选 3 个以上	

表 18：《灾备服务专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例
信息安全技术（II 级）	通用课程	3、4、6、7	20%
灾备服务技术与应用（III 级）	专业课程	全部	80%
信息安全实验（II 级）	通用课程	任选 2 个以上	

表 19：《业务连续性专业级》范围与要求

课程名称	课程类型	选择范围	所占比例
项目管理基础（II 级）	通用课程	全部	10%
信息安全技术（I 级）	通用课程	3、4、6、7	10%
业务连续性管理（II 级）	专业课程	全部	80%
信息安全实验（I 级）	通用课程	任选 3 个以上	

表 20：《业务连续性专业高级》范围与要求

课程名称	课程类型	选择范围	所占比例
信息安全技术（II 级）	通用课程	3、4、6、7	20%
业务连续性管理（III 级）	专业课程	全部	80%
信息安全实验（II 级）	通用课程	任选 2 个以上	

4.2.2 基础课程

目前设置的基础课程包括：《信息安全保障人员基本素质教育》、《信息安全意识教育》、《信息安全法律法规体系》和《风险管理基础》。具体范围与要求见

表 21-24：

表 21：《信息安全保障人员基本素质教育》范围与要求

章节号	章节名	内容与要求	参考文献
1	职业素养	1. 深刻理解从事信息安全保障工作必备的职业素养 2. 深刻理解从事信息安全保障工作的特殊责任	1.《信息安全保障人员认证考试辅导丛书》 2．各类信息安全报刊
2	知识结构	1. 理解从事信息安全保障工作所需的基础知识结构 2. 深刻理解信息安全保障的本质含义	
3	工作技能	1. 理解从事信息安全保障工作所需的基本技能 2. 理解信息安全保障工作的特殊困难	

表 22：《信息安全意识教育》范围与要求

章节号	章节名	内容与要求	参考文献
1	信息安全保障概念	1. 了解信息安全的发展足迹 2. 理解什么是通信保密 3. 理解什么是网络安全 4. 理解什么是信息安全 5. 理解什么是信息安全保障 6. 准确理解信息安全属性 7. 掌握什么时候需要分别考虑信息安全属性	1.《信息安全保障人员认证考试辅导丛书》 2．各类信息安全报刊与年鉴
2	信息安全形势	1. 了解国内外的信息安全形势 2. 了解最新的典型信息安全问题 3. 了解应对典型信息安全问题的手段	
3	信息安全需求识别	1. 了解形势发展的需要 2. 理解社会责任的需求 3. 理解组织业务保障的需要 4. 了解现实信息技术环境的需求 5. 指导如何提出实际需要 6. 了解法律法规的要求 7. 了解客户合同的要求 8. 了解强制标准的要求 9. 了解风险评估的要求 10. 了解日常保障的要求 11. 了解新技术和新措施应用的要求	

表 23：《信息安全法律法规体系》范围与要求

章节号	章节名	内容与要求	参考文献
1	法律法规结构体系	1. 了解我国信息安全法律法规结构 2. 了解我国信息安全法律法规的基本分类	1.《信息安全保障人员认证考试辅导丛书》 2．国内有
2	国内外信息安全法律法规建设概况	1. 了解我国信息安全相关法律法规建设情况 2. 了解美国信息安全相关法律法规建设情况 3. 了解其他国家信息安全相关法律法规建设情况	

3	国内外信息安全标准建设概况	1. 了解国外信息安全标准化相关机构以及相互关系，如国际标准化组织（ISO）、国际电工委员会（IEC）、即国际电信联盟（ITU）和国发达家的信息安全标准相关组织机构，如美国、英国等 2. 了解我国信息安全标准相关组织机构及其关系，如国家标准化管理委员会、全国信息安全标准化技术委员会（TC260）等 3. 了解 ISO、IEC 和 ITU 的信息安全相关标准建设情况 4. 了解美国特有的信息安全相关标准建设情况 5. 了解我国信息安全相关标准建设情况	关法律法规 3．各类信息安全报刊与年鉴
4	我国信息安全管理概况	1. 了解我国信息安全相关管理机构 2. 了解我国信息安全相关管理模式 3. 了解我国主要的信息安全管理手段	
5	典型信息安全法律法规	1. 了解刑法与信息安全相关条款 2. 了解《保守国家秘密法》 3. 了解《商用密码管理条例》 4. 了解互联网相关管理规定 5. 了解信息安全产品相关管理规定	

表 24：《风险管理基础》范围与要求

章节号	章节名	内容与要求	参考文献
1	基本概念	1. 理解风险的定义 2. 理解风险管理的基本思想	1.《信息安全保障人员认证考试辅导丛书》 2．各类风险管理正式出版书籍
2	常见风险评估方法	1. 了解各类风险评估方法的基本思路 2. 了解各类风险评估方法的应用场景	
3	典型的风险评估方法	1. 掌握 1 种风险评估方法	
4	风险处置方法	1. 了解各种风险处置方法 2. 了解各种风险处置方法的应用场景	
5	风险管理相关标准	1. 了解国际相关标准 2. 了解我国相关标准	

4.2.3 通用课程

按照《信息安全保障人员认证准则》的要求，目前设置的通用课程包括：《项目管理基础》、《信息安全技术》和《信息安全实验》。具体范围与要求见表 25-27：

表 25：《项目管理基础》范围与要求

章节号	章节名	内容与要求		参考文献
		I 级	II 级	
1	项目管理基本概念	1. 正确理解项目的本质 2. 正确理解管理的本质	1. 正确理解项目的本质 2. 正确理解管理的本质	1.《信息安全保障人员

		3. 掌握项目管理的基本分类 4. 理解项目管理的生命周期与流程 5. 了解项目管理相对其他管理的特性	3. 掌握项目管理的基本分类 4. **熟练掌握**项目管理的生命周期与流程 5. **掌握**项目管理相对其他管理的特性	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	1. 了解项目管理的发展过程 2. 了解国际项目管理发展现状 3. 了解国际国内项目管理人员认证情况	1. 了解项目管理的发展过程 2. 了解国际项目管理发展现状 3. 了解国际国内项目管理人员认证情况	
3	九大项目管理知识领域	1. 理解项目综合管理、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 2. 了解项目综合管理、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	1. **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 2. **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	1. 了解开发类项目管理的特点 2. 了解开发类项目生命周期 3. 了解开发类项目九大管理知识领域特性 4. 了解一个完整的开发类项目过程	1. **掌握**开发类项目管理的特点 2. **掌握**开发类项目生命周期 3. **正确掌握**开发类项目九大管理知识领域特性 4. **实践**一个完整的开发类项目过程	
5	集成类项目管理技巧	1. 了解集成类项目管理的特点 2. 了解集成类项目生命周期 3. 了解集成类项目九大管理知识领域特性 4. 了解一个完整的集成	1. **掌握**集成类项目管理的特点 2. **掌握**集成类项目生命周期 3. **掌握**集成类项目九大管理知识领域特性 4. **实践**一个完整的集成	

		类项目过程	类项目过程	

表 26：《信息安全技术》范围与要求

章节号	章节名	内容与要求		参考文献
		I 级	II 级	
1	信息安全技术发展	1. 了解信息安全技术结构及相互关系 2. 了解信息安全技术最新进展 3. 了解信息安全技术应用基本方法	1. **理解**信息安全技术结构及相互关系 2. **掌握**信息安全技术最新进展 3. **掌握**信息安全技术应用基本方法	1.《信息安全保障人员认证考试辅导丛书》 2. 各类信息安全期刊 3. 各类信息安全正式出版文献
2	密码学及其应用	1. 了解密码学的发展历史 2. 了解密码学在信息安全中的特殊地位 3. 基本理解密码学的基本原理 4. 基本掌握典型密码算法（对称、非对称、HASH 函数） 5. 基本掌握典型密码算法的作用与应用方法 6. 基本掌握典型应用中如何采用密码技术 7. 了解密钥管理方法	1. **掌握**密码学的发展历史 2. **掌握**密码学在信息安全中的特殊地位 3. **理解**密码学的基本原理 4. **掌握**典型密码算法（对称、非对称、HASH 函数） 5. **掌握**典型密码算法的作用与应用方法 6. **掌握**典型应用中如何采用密码技术 7. **正确掌握**密钥管理方法	
3	网络安全技术	1. 了解网络安全技术的范畴 2. 了解网络边界划分原则与方法 3. 了解典型的网络安全问题 4. 了解典型的网络攻击手段 5. 了解网络边界防御原理与方法 6. 了解典型的网络边界防御设备的系统原理与应用方法（网关防御、网络监控、网络交换） 7. 了解网络通讯安全原理与方法 8. 了解典型的网络通讯	1. **正确理解**网络安全技术的范畴 2. **理解**网络边界划分原则与方法 3. **熟悉**典型的网络安全问题 4. **熟知**典型的网络攻击手段 5. **理解**网络边界防御原理与方法 6. **掌握**典型的网络边界防御设备的系统原理与应用方法（网关防御、网络监控、网络交换） 7. **理解**网络通讯安全原理与方法 8. **掌握**典型的网络通讯	

		安全设备的系统原理与应用方法（访问控制、通讯加密）	安全设备的系统原理与应用方法（访问控制、通讯加密）	
4	平台安全技术	1. 了解常用系统平台（UNIX、Linux、Windows 等)的典型安全问题 2. 了解常用的应用支撑平台(WEB、数据库等）的典型安全问题 3. 了解各类安全漏洞的管理标准与方法 4. 了解典型的对平台攻击手段 5. 了解主机安全防护的主要手段（安全加固、安全监控、安全审计、主机保护等）的原理与实施方法及其工具 6. 了解桌面系统的典型安全问题 7. 了解桌面系统的安全保障方法与工具	1. **熟悉**常用系统平台（UNIX、Linux、Windows 等）的典型安全问题 2. **熟悉**常用的应用支撑平台(WEB、数据库等）的典型安全问题 3. **掌握**各类安全漏洞的管理标准与方法 4. **熟知**典型的对平台攻击手段 5. **掌握**主机安全防护的主要手段（安全加固、安全监控、安全审计、主机保护等）的原理与实施方法及其工具 6. **熟悉**桌面系统的典型安全问题 7. **掌握**桌面系统的安全保障方法与工具	
5	应用安全技术	1. 了解各类常用应用系统（通用应用系统、专业应用系统、特殊业务系统等）的典型安全问题 2. 了解安全软件开发过程管理与控制 3. 了解典型的应用安全漏洞 4. 了解应用软件安全测试方法与工具	1. **熟悉**各类常用应用系统（通用应用系统、专业应用系统、特殊业务系统等）的典型安全问题 2. 了解安全软件开发过程管理与控制 3. 了解典型的应用安全漏洞 4. 了解应用软件安全测试方法与工具	
6	数据安全技术	1. 了解数据安全的范畴 2. 了解数据生命周期的各阶段安全需求 3. 了解数据生命周期的各阶段安全保障技术与方法 4. 了解灾难备份与恢复技术	1. **理解**数据安全的范畴 2. **理解**数据生命周期的各阶段安全需求 3. **基本掌握**数据生命周期的各阶段安全保障技术与方法 4. **熟悉**灾难备份与恢复技术**应用和系统设计**	
7	物理安全技术	1. 了解信息安全保障中物理安全的范畴	1. **熟知**信息安全保障中物理安全的范畴	

		2. 了解典型的物理安全问题 3. 了解典型的物理安全防范技术与方法 4. 了解支持性基础设施的物理安全问题及保护措施	2. **熟悉**典型的物理安全问题 3. **掌握**典型的物理安全防范技术与方法 4. **掌握**支持性基础设施的物理安全问题及保护措施	

表 27:《信息安全实验》范围与要求

章节号	章节名	内容与要求		参考文献
		I 级	II 级	
1	实验平台构建	实验 1 桌面虚拟机的安装、配置、使用和基本操作 实验 2 使用虚拟机构建信息安全实验平台	实验 1 基于服务器的信息安全实验平台安装、配置及实验实例构建	1.《信息安全保障人员认证考试辅导丛书》
2	网络基础实验	实验 1 常用网络命令 实验 2 地址转换协议（APR） 实验 3 网际协议（IP） 实验 4 用户数据报协议（UDP） 实验 5 传输控制协议（TCP） 实验 6 动态主机配置协议（DHCP） 实验 7 域名服务协议（DNS） 实验 8 超文本传输协议（HTTP）	实验 1 网络地址转换 NAT 实验 2 数据包捕获与分析实验 实验 3 路由信息协议(RIP) 实验 4 生成树协议（STP） 实验 5 简单网络管理协议（SNMP） 实验 6 TELNET 和 FTP 实验 7 邮件协议(SMTP、POP3、IMAP） 实验 8 NetBIOS 应用协议	
3	主机安全实验	实验 1 IE 安全设置 实验 2 帐号和口令的安全设置 实验 3 EFS 文件系统安全设置 实验 4 端口安全设置 实验 5 注册表编辑器的使用 实验 6 安全补丁更新	实验 1 注册表的使用技巧和安全配置 实验 2 Linux 口令破解 实验 3 Unix 操作系统的常用操作 实验 4 Unix 操作系统的安全设置	
4	数据库安全实验	实验 1 SQL Server 数据库的安全配置 实验 2 SQL Server 数据库安全扫描	实验 1 Oracle 数据库的安全配置 实验 2 Oracle 数据库安全扫描	

5	密码学与加解密实验	实验 1 DES 加密演示实验 实验 2 RSA 加密演示实验 实验 3 哈希算法实验 实验 4 BIOS 的密码设置与清除 实验 5 Windows 的密码设置与破解实验 实验 6 使用 LC5 破解账户口令 实验 7 Office 办公软件密码的设置与破解 实验 8 用压缩软件加密文件及破解密码	实验 1 PGP 的安装及密钥的生成实验 实验 2 使用 PGP 对邮件、文件进行加密和解密和粉碎等	
6	访问控制实验	实验 1 典型计算机病毒演示实验 实验 2 防病毒实验 实验 3 Windows 个人防火墙的配置 实验 4 灰鸽子木马的种植和清除 实验 5 基于 Snort 的 IDS 安装	实验 1 硬件防火墙的配置 实验 2 嗅探器技术及 Sniffer 的使用 实验 3 硬件入侵检测设备的配置与使用	
7	攻击技术实验	实验 1 ARP 地址欺骗 实验 2 ICMP 重定向 实验 3 路由欺骗 实验 4 IPC$入侵 实验 5 远程管理计算机 实验 6 Telnet 入侵 实验 7 远程综合入侵 实验 8 基于木马的入侵	实验 1 口令破解 实验 2 Land 攻击 实验 3 UDP Flood 攻击 实验 4 DDoS 攻击 实验 5 CC 攻击 实验 6 DameWare 入侵	
8	主动防御技术实验	实验 1 端口扫描软件 实验 2 IIS 的安全配置 实验 3 使用 Windows 系统备份工具对文件进行备份、还原及设置 实验 4 Norton Ghost 数据备份与恢复 实验 5 使用 Easy Recovery 恢复已删除的文件 实验 6 使用 FinalData 还原文件及硬盘数据	实验 1 WWW 服务器和 FTP 服务器的安全配置 实验 2 计算机取证过程演示实验 实验 3 取证设备的演示实验	

9	安全管理实验	实验 1 使用 Microsoft 基准安全分析器 实验 2 风险评估工具的使用	实验 1 撰写应急响应计划 实验 2 撰写灾难恢复应急预案	

4.2.4 专业课程

按照《信息安全保障人员认证准则》的要求，目前的专业课程是完全根据从业方向设置的，包括：《安全软件技术与测试》、《信息系统安全集成》、《信息安全管理》、《安全运维技术与应用》、《安全咨询》、《风险管理》、《应急服务技术与应用》、《灾难备份技术与应用》、《业务连续性管理》。具体范围与要求见表 28-36：

表 28：《安全软件技术与测试》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	安全软件的业界标准与实践	1. 了解信息安全管理体系对安全软件的要求 2. 了解 CC 对安全软件的要求 3. 了解 FIPS 140-2 对安全软件的要求 4. 了解 PCI DSS 对安全软件的要求 5. 了解安全弱点管理相关规范，如 SCAP	1. **理解**信息安全管理体系对安全软件的要求 **2. 理解** CC 对安全软件的要求 **3. 理解** FIPS 140-2 对安全软件的要求 **4. 理解** PCI DSS 对安全软件的要求 5. **理解**安全弱点管理相关规范，如 SCAP	1.《信息安全保障人员认证考试辅导丛书》 2. 各类安全软件正式出版文献
2	安全开发生命周期	1. 了解安全软件开发管理的全过程，如 SDL 2. 了解安全需求分析的主要方法 3. 了解安全设计的主要方法 4. 了解安全编码的主要工作 5. 了解安全测试的主要内容 6. 了解安全生产的主要内容	1. **熟悉**安全软件开发管理的全过程，如 SDL 2. **掌握**安全需求分析的主要方法 3. **掌握**安全设计的主要方法 4. **掌握**安全编码的主要工作 5. **理解**安全测试的主要内容 6. **理解**安全生产的主要内容	
3	安全软件开发环境管理	1. 熟悉物理环境控制 2. 了解逻辑访问控制 3. 了解开发工具与配置项管理 4. 熟悉人员与角色管理	1. 熟悉物理环境控制 2. **熟悉**逻辑访问控制 3. **熟悉**开发工具与配置项管理 4. 熟悉人员与角色管理	

4	安全功能架构与设计	1. 了解典型的安全功能 2. 了解安全功能的实现模型	1. **熟悉**典型安全功能 2. **熟悉**安全功能的实现模型	
5	安全漏洞分析	1. 了解 SCAP 2. 了解 CVSS 3. 了解典型的安全漏洞机理	1. 了解 SCAP 2. **熟悉** CVSS 3. **熟悉**典型的安全漏洞机理	
6	安全编码	1. 了解典型的安全编码规则 2. 了解典型问题的修复方法	1. **熟悉**典型的安全编码规则 2. **熟悉**典型问题的修复方法	
7	密码安全模块	1. 了解典型的加密算法和应用方法 2. 了解典型的密码应用方式 3. 熟悉 FIPS 140-2 的要求	1. **熟悉**典型的加密算法和应用方法 2. **熟悉**典型的密码应用方式 3. **熟悉** FIPS 140-2 的要求	
8	安全测试与实验	1. 了解软件测试的基本方法 2. 了解软件安全功能测试的基本手段 3. 能够使用软件安全性测试工具（如扫描工具、压力测试工具等）	**1. 基本掌握**软件测试的基本方法 **2. 掌握**软件安全功能测试的基本手段 **3. 熟练使用**软件安全性测试工具（如扫描工具、压力测试工具等）	

表 29：《信息系统安全集成》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	安全集成的业界标准与实践	1. 了解 GB/T 20261 对安全集成的要求 2. 了解 ISO/IEC 21827 对安全集成的要求 3. 了解 SSE-CMM3.0 对安全集成的要求 4. 了解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 5. 了解 CNCA/CTS 0052 信息安全服务资质认证技术规范	1. **掌握** GB/T 20261 对安全集成的要求 2. **掌握** ISO/IEC 21827 对安全集成的要求 3. **掌握** SSE-CMM3.0 对安全集成的要求 4. **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 5. **掌握** CNCA/CTS 0052 信息安全服务资质认证技术规范	1.《信息安全保障人员认证考试辅导丛书》 2. 各类安全集成正式出版文献
2	安全集成过程	1. 了解安全软件集成管理的全过程 2. 了解安全集成准备工	1. **掌握**安全软件集成管理的全过程 2. **掌握**安全集成准备工	

		作（如需求分析）的主要方法 3. 了解安全集成设计的主要方法 4. 了解安全集成实施的主要工作 5. 了解安全集成保证的主要内容	作（如需求分析）的主要方法 3. **掌握**安全集成设计的主要方法 4. **掌握**安全集成实施的主要工作 5. **掌握**安全集成保证的主要内容	
3	安全集成工具使用	1. 了解典型的安全集成工具 2. 熟悉需求分析工具使用 3. 了解安全集成设计工具使用 4. 了解安全保证工具使用	1. **熟悉**典型的安全集成工具； 2. 熟悉需求分析工具使用 3. **熟悉**安全集成设计工具使用 4. **熟悉**安全保证工具使用	
4	典型安全保障手段	1. 了解典型的信息安全保障手段 2. 了解常用的信息安全技术应用 3. 了解常用的信息安全产品	1. **熟悉**典型的信息安全保障手段 2. **熟悉**常用的信息安全技术应用 3. **熟悉**常用的信息安全产品	
5	安全集成实例	1. 了解安全集成方案的结构 2. 了解主要行业的安全集成特性 3. 了解 1-2 个行业的典型安全集成实例	1. **熟悉**安全集成方案的结构 2. **熟悉**主要行业的安全集成特性 3. **理解** 1-2 个行业的典型安全集成实例	

表 30：《信息安全管理》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	安全管理的业界标准与实践	1. 理解 GB/T 22080（ISO/IEC 27001） 2. 理解 GB/T22081（ISO/IEC 27002） 3. 了解 ISO/IEC 27000 系列其他标准	1. **深刻理解** GB/T 22080（ISO/IEC 27001） 2. **深刻理解** GB/T 22081（ISO/IEC 27002） 3. **初步理解** ISO/IEC 27000 系列其他标准	1.《信息安全保障人员认证考试辅导丛书》 2. 各类安全管理正式出版文献
2	安全管理的实施过程	1. 了解安全管理的全过程 2. 了解安全管理准备工作（如安全需求分析）的主要方法 3. 了解安全管理设计的	1. **理解**安全管理的全过程 2. **理解**安全管理准备工作（如安全需求分析）的主要方法 3. **理解**安全管理设计的	

		主要方法 4. 了解安全管理实施与运行的主要工作 5. 了解安全管理的检查与评审主要内容 6. 了解安全管理的保持与持续改进主要内容	主要方法 4. **理解**安全管理实施与运行的主要工作 5. **理解**安全管理的检查与评审主要内容 6. **理解**安全管理的保持与持续改进主要内容	
3	安全管理工具使用	1. 了解典型的安全管理工具	1. **熟悉**典型的安全管理工具；	
4	典型安全保障手段	1. 了解典型的安全保障手段 2. 了解常用的信息安全技术应用 3. 了解常用的信息安全产品	1. **熟悉**典型的安全保障手段 2. **熟悉**常用的信息安全技术应用 3. **熟悉**常用的信息安全产品	
5	安全管理实例	1. 了解安全管理的结构 2. 了解主要行业的安全管理特性 3. 了解 1-2 个行业的典型安全管理实例	1. **熟悉**安全管理的结构 2. **熟悉**主要行业的安全管理特性 3. **理解** 1-2 个行业的典型安全管理实例	
6	风险管理	1. 理解风险的定义 2. 理解风险管理的基本思想 3. 了解各类风险评估方法的基本思路 4. 了解各类风险评估方法、处置方法的应用场景 5. 掌握 1 种风险评估方法和风险处置方法 6. 了解国际相关标准 7. 了解我国相关标准	1. **熟悉**风险的定义 2. 理解风险管理的基本思想 3. **熟悉**各类风险评估方法的思路 4. **熟悉**各类风险评估方法、处置方法的应用场景 5. **掌握多种**风险评估方法和处置方法 6. **熟悉**国际相关标准 7. **熟悉**我国相关标准	

表 31：《安全运维技术与应用》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	业界标准与实践	1. 了解信息安全管理体系对安全运维的要求 2. 了解服务管理体系对安全运维的要求 3. 了解安全弱点管理相关规范	1. **理解**信息安全管理体系对安全软件的要求 2. **理解**服务管理体系对安全运维的要求 3. **理解**安全弱点管理相关规范	1.《信息安全保障人员认证考试辅导丛书》 2. 各类安全运维正式出版文
2	安全运维结构与思	1. 了解安全运维的核心思想	1. **理解**安全运维的核心思想	

	想	2. 了解安全运维的管理关系结构	2. **理解**安全运维管理的关系结构	献
3	安全运维工具使用	1. 了解典型的安全运维工具 2. 了解典型的安全运维为手段	1. **熟悉**典型的安全运维工具； 2. **熟悉**典型的安全运维为手段	
4	安全运维实例	1. 了解主要行业的安全运维特性 2. 了解 1-2 个行业的典型安全运维实例	1. **熟悉**主要行业的安全运维特性 2. **熟悉** 1-2 个行业的典型安全运维实例	

表 32:《安全咨询》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	安全相关标准	1. 了解国际国内主要信息安全标准组织 2. 了解国际国内主要信息安全标准框架和核心标准	1. **熟悉**国际国内主要信息安全标准组织 2. **熟悉**国际国内主要信息安全标准框架和核心标准	1.《信息安全保障人员认证考试辅导丛书》 2. 各类信息安全咨询正式出版文献
2	咨询的过程管理	1. 了解安全咨询集成管理的全过程 2. 了解安全咨询准备工作（如客户需求分析）的主要方法 3. 了解安全框架与安全保障方案设计 4. 了解安全咨询实施的管理方法 5. 了解安全咨询质量保证的主要内容	1. **掌握**安全咨询集成管理的全过程 2. **掌握**安全咨询准备工作（如客户需求分析）的主要方法 3. **掌握**安全框架与安全保障方案的设计 4. **掌握**安全咨询实施的管理方法 5. **掌握**安全咨询质量保证的主要内容	
3	安全方案设计	1. 了解典型信息安全保障框架 2. 熟悉典型信息安全技术方案和产品 3. 了解常见管理体系相关标准和实施过程 4. 熟悉信息安全管理体系的建立、实施和运行、监视和评审、持续改进等	1. **掌握**典型信息安全保障框架 2. 熟悉典型信息安全技术方案和产品 3. **熟悉**常见管理体系相关标准和实施过程 4. **熟练掌握**信息安全管理体系的建立、实施和运行、监视和评审、持续改进等	
4	安全咨询工具的使用	1. 了解典型的安全监测工具 2. 了解典型的安全检测工具	1. **熟悉**典型的安全监测工具 2. **熟悉**典型的安全检测工具	

		3. 了解典型的安全分析工具 4. 了解典型的安全管理工具	3. **熟悉**典型的安全分析工具 4. **熟悉**典型的安全管理工具	
5	安全咨询知识库管理	1. 了解安全知识库的构建方法 2. 了解安全知识库的使用方法	1. **熟悉**安全知识库的构建方法 2. **掌握**安全知识库的使用方法	
6	典型咨询案例分析	1. 了解 1-2 个行业的典型管理实例	1. **理解** 1-2 个行业的典型管理实例	

表 33：《风险管理》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	风险管理的业界标准与实践	1. 理解 GB/T 24353 2. 理解 GB/T 20984 3. 了解各行业的信息安全风险管理指引	1. **深刻理解**GB/T 24353 2. **深刻理解**GB/T 20984 3. 了解各行业的信息安全风险管理指引	1.《信息安全保障人员认证考试辅导丛书》 2. 各类风险管理正式出版文献
2	风险管理的实施过程	1. 了解风险管理的全过程 2. 了解风险管理准备工作（如组织与规划）的主要方法 3. 了解风险评估主要方法与实施 4. 了解风险评估的报告格式与形成报告的方法 5. 了解风险处置主要方法与实施	1. **理解**风险管理的全过程 2. **理解**风险管理准备工作（如组织与规划）的主要方法 3. **理解**风险评估主要方法与实施 4. **理解**风险评估的报告格式与形成报告的方法 5. **理解**风险处置主要方法与实施	
3	风险管理工具使用	1. 了解典型的风险管理工具（技术、管理两类工具）	1. **熟悉**典型的风险管理工具（技术、管理两类工具）	
4	典型风险处置措施	1. 了解典型的风险具体处置措施	1. 了解典型的风险具体处置措施	
5	风险管理实例	1. 了解主要行业的典型安全风险特性 2. 了解 1-2 个行业的典型风险管理实例	1. **熟悉**主要行业的典型安全风险特性 2. **理解** 1-2 个行业的典型风险管理实例	

表 34：《应急服务技术与应用》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	应急服务	1. 了解 YD/T 1799	1. **熟悉** YD/T 1799	1.《信息安

	的相关规范	2. 了解业务连续性标准 ISO/IEC 22301 3. 了解应急服务的相关安全要求	2. **熟悉**业务连续性标准 ISO/IEC 22301 3. **熟悉**应急服务的相关安全要求	全保障人员认证考试辅导丛书》 2. 各类应急服务正式出版文献
2	应急服务过程管理	1. 了解应急服务的全过程 2. 了解应急服务准备工作（如组织与规划）的主要方法 3. 了解应急服务的回退过程 4. 了解应急服务的风险评估 5. 了解应急服务的资源协调 6. 了解应急服务的升级机制 7. 了解应急服务的现场保护与取证方法	1. **熟悉**应急服务的全过程 2. **熟悉**应急服务准备工作（如组织与规划）的主要方法 3. **熟悉**应急服务的回退过程 4. **熟悉**应急服务的风险评估 5. **熟悉**应急服务的资源协调 6. **熟悉**应急服务的升级机制 7. **熟悉**应急服务的现场保护与取证方法	
3	安全技术工具的使用	1. 了解典型的安全监测工具 2. 了解典型的安全检测工具（渗透工具） 3. 了解典型的安全分析工具 4. 了解典型的安全管理工具	1. **熟悉**典型的安全监测工具 2. **熟悉**典型的安全检测工具（渗透工具） 3. **熟悉**典型的安全分析工具 4. **熟悉**典型的安全管理工具	
4	典型应急案例分析	1. 了解 1-2 个行业的典型管理实例	1. **理解** 1-2 个行业的典型管理实例	

表 35：《灾备服务技术与应用》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	灾备服务的业界标准与实践	1. 了解国内外灾备相关技术和标准情况 2. 了解 GB/T 20988	1. **熟悉**国内外灾备相关技术和标准情况 2. **熟悉** GB/T 20988	1.《信息安全保障人员认证考试辅导丛书》 2. 各类灾备服务技术正式出版文献
2	灾备恢复技术	1. 了解数据存储技术、数据复制技术和数据管理技术的原理 2. 了解灾难检测技术、系统迁移技术和系统恢复技术的原理	1. **掌握**数据存储技术、数据复制技术和数据管理技术的原理 2. **掌握**灾难检测技术、系统迁移技术和系统恢复技术的原理	
3	灾备服务过程管理	1. 了解灾备服务的全过程	1. **熟悉**灾备服务的全过程	

		2. 了解灾备服务准备工作（如组织与规划）的主要方法 3. 了解灾备服务的资源协调 4. 了解备份管理机制 5. 了解恢复测试管理 6. 了解恢复实施管理 7. 了解灾备服务的现场保护与取证方法	2. **熟悉**灾备服务准备工作（如组织与规划）的主要方法 3. **熟悉**灾备服务的资源协调 4. **熟悉**备份管理机制 5. **熟悉**恢复测试管理 6. **熟悉**恢复实施管理 7. **熟悉**灾备服务的现场保护与取证方法	
4	灾备工具使用与管理	1. 了解数据存储、数据复制和数据管理典型工具的使用和管理 2. 了解灾难检测、系统迁移和系统恢复典型工具的使用和管理	1. **掌握**数据存储、数据复制和数据管理典型工具的使用和管理 2. **掌握**灾难检测、系统迁移和系统恢复典型工具的使用和管理	
5	灾备实例分析	1. 了解主要行业的典型灾难备份系统管理特性 2. 了解 1-2 个行业的典型灾难备份系统管理实例	1. **理解**主要行业的典型灾难备份系统管理特性 2. **熟悉** 1-2 个行业的典型灾难备份系统管理实例	

表 36：《业务连续性管理》

章节号	章节名	内容与要求		参考文献
		II 级	III 级	
1	业务连续性的业界标准与实践	1. 了解 ISO/IEC 22301 的要求 2. 了解 ISO/IEC 27031 的要求 3. 了解 BCI 业务连续性管理最佳实践 4. 了解 GB/T 20988	1. **理解** ISO/IEC 22301 的要求 2. **理解** ISO/IEC 27031 的要求 3. **理解** BCI 业务连续性管理最佳实践 4. **理解** GB/T 20988	1.《信息安全保障人员认证考试辅导丛书》 2．各类业务连续性技术正式出版文献
2	业务连续性管理结构与思想	1. 了解业务连续性管理的核心思想 2. 了解业务连续性管理的关系结构	1. **理解**业务连续性管理的核心思想 2. **理解**业务连续性管理的关系结构	
3	业务连续性管理环节	1. 了解业务连续性管理的应急响应 2. 了解业务连续性管理的事件管理（危机管理） 3. 了解业务连续性的恢复	1. **理解**业务连续性管理的应急响应 2. **理解**业务连续性管理的事件管理（危机管理） 3. **理解**业务连续性的恢复	

		4. 了解业务连续性的演练	4. **理解**业务连续性的演练	
4	业务连续性管理程序与计划	1. 了解程序与计划的典型结构 2. 了解程序与计划的编制方法 3. 了解程序与计划的维护方法	1. **理解**程序与计划的典型结构 2. **理解**程序与计划的编制方法 3. **理解**程序与计划的维护方法	
5	业务连续性管理实例	1. 了解主要行业的典型业务连续性管理特性 2. 了解 1-2 个行业的典型业务连续性管理实例	1. 理解主要行业的典型业务连续性管理特性 2. 熟悉 1-2 个行业的典型业务连续性管理实例	

4.2.5 附加课程

目前设置的附加课程包括：《通信技术基础》、《管理体系审核》和《渗透测试技术与应用》。具体范围与要求见表 37-39：

表 37：《通信技术基础》范围与要求

章节号	章节名	内容与要求	参考文献
1	通信的基本概念	1．理解通信的本质含义及电信概念 2．理解通信网络形成过程 3．了解通信网络结构 4．了解通信网络中的安全属性 5．了解通信网络应用分类 6．了解“网络”习惯分类 7．了解通信网络安全问题本质成因	1．《信息安全保障人员认证考试辅导丛书》 2．各类通信原理相关书籍
2	通信协议及应用	1． 熟悉 OSI 七层模型 2． 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 3． 熟悉 IPv6、移动互联网等技术及应用 4． 了解典型的通信网络及设备	
3	安全通信协议	1．了解典型的安全通信协议 2．了解典型的安全通信协议在通信过程中的应用	

表 38：《管理体系审核》范围与要求

章节号	章节名	内容与要求	参考文献
1	审核的基本概念	1． 深刻理解审核的基本定义 2． 理解审核员的基本素质要求 3． 了解认证认可管理结构	1.《信息安全保障人员认证考试辅导丛书》
2	审核的基本流程	1． 了解审核的类型 2． 了解审核的基本流程	

		3. 了解审核关键环节的主要工作 4. 了解审核人日数计算方法	2. 管理体系相关标准、准则、规则
3	审核的基本方法	1. 掌握审核金三角 2. 掌握开会技巧 3. 掌握访谈技巧 4. 掌握观察技巧 5. 掌握抽样方法 6. 掌握审核点与审核思路设计技巧	
4	审核员的管理与能力要求	1. 了解对审核员的管理机构和管理方式 2. 了解审核具备的通用能力要求 3. 了解各专业对审核员能力的要求，以信息安全管理体系审核员为例	

表 39:《渗透测试技术与应用》

章节号	章节名	内容与要求	参考文献
1	渗透测试的基本概念	1. 熟悉信息安全威胁 2. 熟悉设备渗透测试 3. 熟悉渗透测试流程 4. 熟悉渗透测试的目标 5. 熟悉渗透测试的分类 6. 熟悉渗透测试的限制	1.《信息安全保障人员认证考试辅导丛书》 2. 各类渗透测试正式出版文献
2	渗透测试法律问题	1. 熟悉渗透测试的法律依据 2. 熟悉渗透测试的法律框架 3. 熟知与客户签订渗透测试协议	
3	渗透测试方法论	1. 熟悉组织、个人、技术和道德的相关要求 2. 掌握渗透测试的方法论 3. 掌握渗透测试五个步骤	
4	实施渗透测试与报告撰写	1. 熟悉渗透测试的准备 2. 掌握对渗透目标的预查 3. 熟悉信息及风险的分析方法 4. 熟知启动渗透测试 5. 熟悉最后分析及消除影响 6. 熟悉渗透测试报告的撰写	
5	Unix 渗透测试方法与工具使用	1. 熟知 Unix 缓冲区溢出渗透 2. 熟知 Unix Shell 渗透技术 3. 熟知 Unix 系统提权 4. 熟知 Apache 安全渗透 5. 熟知 Unix 后门技术	
6	Windows 系统渗透测试方法与工具使用	1. 熟悉网络协议安全 2. 熟悉网络端口扫描与漏洞扫描 3. 熟悉嗅探技术与密码截获及破解 4. 熟悉缓冲区溢出渗透 5. 熟悉病毒与木马技术	

7	Web 应用系统渗透测试方法与工具使用	1. 熟悉 HTTP 协议基本概念 2. 熟悉 SQL 注入渗透技术与工具 3. 熟悉 XSS 跨站脚本技术 4. 熟悉 CSRF 渗透技术 5. 熟悉 Web Service 渗透技术 6. 了解 Web 安全编程	
8	数据库渗透测试与工具使用	1. 熟悉数据库系统的威胁 2. 熟悉 Oracle 渗透测试 3. 熟悉各种 PL/SQL Injection 漏洞利用 4. 熟悉 Lateral SQL Injection 5. 了解其他数据库渗透测试	

4.2.6 考试时间

笔试：基础级（I 级） 2 小时；（120 道单选题）

专业级（II 级） 3 小时；（80 道单选题，20 道多选题，1 道综合题）

专业高级（III 级）（专业论文和实验）

实验：专业级（II 级） 2 小时（适用时）

专业高级（III 级）3 小时（适用时）

4.2.7 题型说明

1 单项选择题：给出问题描述，要求从给出的四个答案中选择其中最为恰当的一个；

例：过程是指 （ ）。

a） 有输入和输出的任意活动

b） 通过使用资源和管理，将输入转化为输出的任意活动

c） 所有业务活动的集合

d） 以上都不对

2 多项选择题：给出问题描述，要求从给出的四个答案中选择所有合适的选项，选项可以为 1-4 个；

例：防火墙的基本类型有 （ ）。

a） 包过滤防火墙

b） 应用层网关

c） 电路网关

d） 混合器型防火墙

3 综合题

例：某物流公司（上百名员工）在年初发生一起严重泄密事件：某员工因对公司不满，在离职半年后将其在职期间窃取的员工工资表（该表以 excel 文档保存在人事经理主机上）

以匿名邮件的形式发给公司里每个人，公司内部震动很大，一些不满薪金制度的员工还递上了辞呈。IT 主管于是从网上下载一个文档加密软件提交予人事部，要求其将相关重要文档加密存放。

请就上述事件指出该物流公司在信息安全防护措施方面具有哪些问题(至少列出四点)，并为防止类似事件发生给出一个整体安全集成解决方案。

4 实验题

例：一台 Windows XP 个人主机，初步判断被植入了木马程序，该木马程序可能持续向受控主机发起连接命令，请根据经验，利用 Windows 系统自身安全工具以及任何其他第三方的基本嗅探工具，检测、分析这台主机遭受木马侵害情况。

5 专业论文

例：论构建信息系统的安全应急响应策略。

计算机技术的迅速发展史 20 世纪后半叶和 21 世纪初最为显著的特征之一。计算机及计算机网络的普及和应用，给我们带来了极大的价值和便利，但计算机及计算机网络是一把双刃剑。设计、建设、部署及运营，都可能存在潜在问题，尤其是在运营过程中，如不能建立合适的应急响应策略，将可能给组织带来难以控制的损失。请以“论构建信息系统的安全应急响应策略”为题，分别从以下 3 个方面进行论述：

1.概要叙述你参与过的项目（项目的背景、规模、发起单位、目的、项目内容、组织结构、项目周期、项目安全需求、最终交付的安全产品等）；

2.结合项目实际论述构建信息安全应急响应策略的核心内容和设计原则；

3.结合实际的信息安全事件应急处理过程，简要论述信息安全应急响应策略在事件处理过程中所起的作用。