文件编码：CCRC-ISV-C01:2026

信息安全服务规范

版本：B/0

2026-11-02 发布　　2026-11-16 实施

中国网络安全审查认证和市场监管大数据中心发布

目录

1. 适用范围 1
2. 规范性引用文件 1
3. 术语与定义 1
3.1. 信息安全服务 1
3.2. 信息安全风险评估 1
3.3. 信息安全应急处理 1
3.4. 信息系统安全集成 1
3.5. 信息系统灾难备份与恢复 1
3.6. 软件安全开发 2
3.7. 信息系统安全运维 2
3.8. 网络安全审计 2
3.9. 渗透测试 2
4. 服务管理要求 2
4.1. 三级要求 2
4.1.1. 办公场所要求 2
4.1.2. 人员能力要求 2
4.1.3. 业绩要求 2
4.1.4. 管理制度要求 3
4.1.5. 技术工具要求 3
4.1.6. 服务技术要求 3
4.2. 二级要求 3
4.2.1. 办公场所要求 3
4.2.2. 人员能力要求 3
4.2.3. 业绩要求 3
4.2.4. 管理制度要求 3
4.2.5. 技术工具要求 4
4.2.6. 服务技术要求 4
4.3. 一级要求 4
4.3.1. 办公场所要求 4
4.3.2. 人员能力与要求 4
4.3.3. 业绩要求 4
4.3.4. 管理制度要求 4
4.3.5. 技术工具要求 4
4.3.6. 服务技术要求 5

5. 服务特性要求 5
5.1. 风险评估服务特性要求 5
5.2. 安全集成服务特性要求 5
5.3. 应急处理服务特性要求 5
5.4. 灾难备份与恢复服务特性要求 5
5.5. 软件安全开发服务特性要求 5
5.6. 安全运维服务特性要求 5
5.7. 网络安全审计服务特性要求 5
5.8. 渗透测试服务特性要求 5
6. 评价方法及判定规则 5
6.1. 评价方法 5
6.2. 判定规则 5
附录 A（规范性附录）： 信息安全风险评估服务特性要求 6
附录 B（规范性附录）： 信息系统安全集成服务特性要求 9
附录 C（规范性附录）： 信息安全应急处理服务特性要求 11
附录 D（规范性附录）： 信息系统灾难备份与恢复服务特性要求 13
附录 E（规范性附录）： 软件安全开发服务特性要求 16
附录 F（规范性附录）： 安全运维服务特性要求 18
附录 G（规范性附录）： 网络安全审计服务特性要求 20
附录 H（规范性附录）： 渗透测试服务特性要求 23
附录 I：信息安全服务人员能力要求 27
附录 J: 参考文献 49

1. 适用范围

本规范规定了信息安全服务提供者（以下简称服务提供者）在提供服务时应具备的服务管理要求和服务特性要求。

本规范可作为第三方认证机构对服务提供者的评价依据，也可作为服务提供者开展自我评价的依据，同时，可为政府及有关社会组织选择服务提供者提供参考。

2. 规范性引用文件

GB/T 25069-2022《信息安全技术　术语》

3. 术语与定义

3.1. 信息安全服务

面向组织或个人的各类信息安全需求和信息安全保障需求,由服务提供方按照服务协议所执行的信息安全过程或任务。

注1:信息安全服务通常是基于信息安全技术、产品或管理体系,通过外包的形式,由专业信息安全人员所提供的支持和帮助。

注2:信息安全服务通常以信息安全服务提供方和信息安全服务需求方之间的服务项目方式进行。

3.2. 信息安全风险评估

对特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害进行识别、分析和评价的过程。

3.3. 信息安全应急处理

为应对信息系统运行过程中突发/重大信息安全事件的发生所做的准备，在事件发生时，按照既定的程序对事件进行处理，以及在事件发生后所采取措施的过程。

3.4. 信息系统安全集成

按照信息系统建设的安全需求，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行为或活动。

3.5. 信息系统灾难备份与恢复

将信息系统的数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份，并在灾难发生时，将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态、将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态的过程。

注：信息系统灾难备份与恢复分为资源服务类（A 类）、技术服务类（B 类）两个类别。

资源服务类（A 类），指灾难备份资源服务提供方需具备灾备中心场地资源、基础设施、运维管理等能力。

技术服务类（B 类），指灾难备份技术服务提供方实施灾备技术服务时具备灾备方案设计、系统建设与管理、预案制定与演练等能力。

3.6. 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。

3.7. 信息系统安全运维

从面向业务的运维服务出发，依据安全需求对信息系统进行安全运维准备、安全运维实施，并对实施安全运维服务的有效性进行评审，从而进行持续性改进，全过程、全生命周期地为信息系统运行提供安全保障的过程。

3.8. 网络安全审计

网络安全审计是指网络安全审计服务机构对被审计方所属的计算机信息系统的安全性、可靠性和经济性进行检查、监督，通过获取审计证据并对其进行客观评价所开展的系统的、独立的、形成文件的活动。

3.9. 渗透测试

渗透测试是指以未经授权的动作绕过某一系统的安全机制来检查信息系统的安全功能,以发现信息系统安全问题的手段。

4. 服务管理要求

服务管理要求适用于风险评估、安全集成、应急处理、灾难备份与恢复、软件安全开发、安全运维、网络安全审计、渗透测试等类别的信息安全服务认证评价，均分为三个级别，其中一级最高。

4.1. 三级要求

4.1.1. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.1.2. 人员能力要求

技术负责人应具备与申报类别一致的信息安全服务管理能力；项目负责人、项目工程师应具备与申报类别一致的信息安全服务技术能力。能力评价要求参考附录 I。

4.1.3. 业绩要求

a) 从事信息安全服务（与申报类别一致）6个月以上。

b) 近3年内签订并完成至少1个信息安全服务（与申报类别一致）项目。

4.1.4. 管理制度要求

a) 建立并运行文档管理程序，包括组织管理、服务过程管理、质量管理等内容，明确项目产生、发布、保存、传输、使用（包括交付和内部使用）、废弃等环节的文档控制。

b) 建立并运行项目管理程序，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，提供项目风险管理记录。

c) 建立并运行保密管理程序，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

d) 建立与运行供应商管理程序，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维、灾难备份与恢复方向）。

4.1.5. 技术工具要求

应配备承担信息安全服务（与申报类别一致）所需的安全、可信的软硬件工具和设备。

4.1.6. 服务技术要求

建立和制定信息安全服务（与申报类别一致）所需的流程和规范，并遵照实施。

4.2. 二级要求

4.2.1. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.2.2. 人员能力要求

技术负责人应具备与申报类别一致的信息安全服务管理能力；项目负责人、项目工程师应具备与申报类别一致的信息安全服务技术能力。能力评价要求参考附录Ⅰ。

4.2.3. 业绩要求

a) 从事信息安全服务（与申报类别一致）3年以上，或取得信息安全服务（与申报类别一致）三级1年以上。

b) 近3年内签订并完成至少6个信息安全服务（与申报类别一致）项目。

4.2.4. 管理制度要求

a) 建立并运行文档管理程序，包括组织管理、服务过程管理、质量管理等内容，明确项目产生、发布、保存、传输、使用（包括交付和内部使用）、废弃等环节的文档控制。

b) 建立并运行项目管理程序，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，提供项目风险管理记录。

c) 建立并运行保密管理程序，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

d) 建立与运行供应商管理程序，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维、灾难备份与恢复方向）。

4.2.5. 技术工具要求

应配备承担信息安全服务（与申报类别一致）所需的安全、可信的软硬件工具和设备。

4.2.6. 服务技术要求

建立和制定信息安全服务（与申报类别一致）所需的流程和规范，并遵照实施。

4.3. 一级要求

4.3.1. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.3.2. 人员能力与要求

技术负责人应具备与申报类别一致的信息安全服务管理能力；项目负责人、项目工程师应具备与申报类别一致的信息安全服务技术能力。能力评价要求参考附录 I。

4.3.3. 业绩要求

a) 从事信息安全服务（与申报类别一致）5年以上，或取得信息安全服务（与申报类别一致）二级1年以上。

b) 近3年内签订并完成至少10个信息安全服务（与申报类别一致）项目。

4.3.4. 管理制度要求

a) 建立并运行文档管理程序，包括组织管理、服务过程管理、质量管理等内容，明确项目产生、发布、保存、传输、使用（包括交付和内部使用）、废弃等环节的文档控制。

b) 建立并运行项目管理程序，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，提供项目风险管理记录。

c) 建立并运行保密管理程序，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

d) 建立与运行供应商管理程序，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维、灾难备份与恢复方向）。

4.3.5. 技术工具要求

应配备承担信息安全服务（与申报类别一致）所需的安全、可信的软硬件工具和设备。关键软硬件工具和设备的安全性应获得第三方评价或者证明。

4.3.6. 服务技术要求

建立和制定信息安全服务（与申报类别一致）所需的流程和规范，并遵照实施。

5. 服务特性要求

5.1. 风险评估服务特性要求

风险评估服务特性要求参见附录A。

5.2. 安全集成服务特性要求

安全集成服务特性要求参见附录B。

5.3. 应急处理服务特性要求

应急处理服务特性要求参见附录C。

5.4. 灾难备份与恢复服务特性要求

灾难备份与恢复服务特性要求参见附录D。

5.5. 软件安全开发服务特性要求

软件安全开发服务特性要求参见附录E。

5.6. 安全运维服务特性要求

安全运维服务特性要求参见附录F。

5.7. 网络安全审计服务特性要求

网络安全审计服务特性要求参见附录G。

5.8. 渗透测试服务特性要求

渗透测试服务特性要求参见附录H。

6. 评价方法及判定规则

6.1. 评价方法

服务管理要求评价方法为查阅文件、人员访谈等。

服务特性要求的评价方法为现场观察、查阅文件、人员访谈、服务技术文档审查、演示等。

6.2. 判定规则

对于《信息安全服务规范》各项要求的评价结论分为符合、不符合和严重不符合。

当服务管理要求和服务特性要求的所有评价项均为符合或不符合已整改并通过验证时，该服务类别评价结论为推荐。

当服务管理要求和服务特性要求的评价项存在严重不符合、不符合未完成整改或整改验证未通过时，所有涉及的服务类别评价结论为不推荐。

附录A（规范性附录）： 信息安全风险评估服务特性要求

申请组织应满足申请级别和低于申请低级别的对应要求。

条款		三级要求	二级要求	一级要求
1.准备阶段	1.1. 服务方案制定	a)编制风险评估方案、风险评估模板，并在项目实施过程中按照模板实施。 b)应为风险评估实施活动提供总体计划或方案，方案应包含风险评价准则。	c)应进行充分的系统调研，形成调研报告。	
	1.2. 项目团队	a)应组建评估团队。风险评估实施团队应由管理层、相关业务骨干、IT技术人员等组成。		
2.风险识别阶段	2.1. 资产识别	a)参考国家或国际标准，对资产进行分类。 b)识别重要信息资产，形成资产清单。 c)对已识别的重要资产，分析资产的保密性、完整性和可用性等安全属性的等级要求。 d)对资产根据其在保密性、完整性和可用性上的等级分析结果，经过综合评定进行赋值。		e)识别信息系统处理的业务功能，重点识别出关键业务功能和关键业务流程。 f)根据业务特点和业务流程识别出关键数据和关键服务。 g)识别处理数据和提供服务所需的关键系统单元和关键系统组件。
	2.2. 脆弱性识别	a)应对已识别资产的安全管理或技术脆弱性利用适当的工具进行核查，并形成安全管理或技术脆弱性列表。 b)应对脆弱性进行赋值。		
	2.3. 威胁识别	a)应参考国家或国际标准，对威胁进行分类； b)应识别所评估信息资产存在的潜在威胁；		c)采用多种方法进行威胁调查。
	2.4. 已有安全措施确认	a)应识别组织已采取的安全措施； b)应评价已采取的安全措施的有效性。		
3.风险分	3.1. 风险分析模型建立	a)应构建风险分析模型。风险分析模型应将资产、威胁、脆弱性三个基本要素及每个要素各自的属性进行关联。		

析阶段		b)应根据风险分析模型对已识别的重要资产的威胁、脆弱性及安全措施进行分析。 c)应识别威胁利用脆弱性的可能性，分析威胁利用脆弱性对组织可能造成的影响。 d)应根据风险分析模型确定的方法计算出风险值。		
	3.2. 风险评价	a)应根据风险评价准则确定风险等级。	b)应对不同等级的安全风险进行统计、评价，形成最终的总体安全评价。	
	3.3. 风险评估报告	a)应向客户提供风险评估报告，报告应包括但不限于评估过程、评估方法、评估结果、处置建议等内容。	b)风险评估报告中应对本次评估建立的风险分析模型进行说明，并应阐明本次评估采用的风险计算方法及风险评价方法。 c)风险评估报告中应对计算分析出的风险给予比较详细的说明。	
4.风险处置阶段	**4.1. 风险处置原则确定**		a)应协助被评估组织确定风险处置原则，以及风险处置原则适用的范围和例外情况。	
	4.2. 安全整改建议		a)对组织不可接受的风险提出风险处置措施。	

	4.3. 组织评审会			a)协助被评估组织召开评审会； 依据最终的评审意见进行相应的整改，形成最终的整改材料。
	4.4. 残余风险处置			a)对组织提出完整的风险处置方案。 b)必要时，对残余风险进行再评估。

附录 B（规范性附录）： 信息系统安全集成服务特性要求

申请组织应满足申请级别和低于申请低级别的对应要求。

条款		三级要求	二级要求	一级要求
1.集成准备阶段	1.1. 需求调研与分析	a) 调研客户背景信息，采集系统建设需求和建设目标，明确系统功能、性能及安全性要求。 b) 基于系统建设需求，提出产品选型方案和建设预算。	c)准确识别和综合分析系统在信息安全特性方面相适应的安全需求，并编制需求分析报告。	
2.方案设计阶段		a) 根据系统建设安全需求，编制安全集成技术方案。 b) 依据技术方案，编制安全集成实施方案，明确项目人员、进度、质量、沟通、风险等方面的要求。	c)结合需求分析和客户在保障系统安全方面的投入能力，提出系统建设安全设计说明书，明确系统架构、产品选型、产品功能、性能及配置等参数。	d)结合项目需要，编制安全集成项目施工手册和作业指导书。 e)基于安全集成项目需求和进度计划，编制信息安全产品和工具定制开发计划。
3.建设实施阶段	3.1. 实施集成	a)项目实施人员按时提交施工记录和工程日志，及时向项目经理汇报项目进度。	b)产品、设备安装调试过程中，应完整妥善记录相关信息。	c)制定项目应急处置方案和恢复策略，对项目过程中的应急事件及时进行响应。
	3.2. 监督管理			a)定期对项目实施情况进行评审，采取适当措施，控制项目风险。
4. 安全保障阶段	4.1. 系统测试	a) 依据项目技术方案和测试计划，对系统进行联调和系统测试，完整记录测试过程相关信息。 b) 对于新建系统重点测试系统的功能、性能和安全性等；对于系统改造或升级项目，还需进行兼容性测试。	c)系统测试完成后，制定系统测试报告，并提交客户。	d)基于建设系统的安全要求，制定系统安全性测试方案，模拟攻击场景，对系统安全性进行测试。
	4.2. 系统试运行	a) 为测试系统运行的可靠性和稳定性，系统初验后需进行试运行，并记录系统运行状况。	c)系统试运行周期至少一个月，项目组制定系统试运行报告，并提交客户。	d)综合分析系统运行状态，建立系统运行策略和安全指南，并对相关产品和设备设施进行配置管理。

		b） 基于系统运行相关记录，及时对系统设备进行调整和维护。		e)提供三个月以上的试运行记录和报告。
	4.3. 验收	a)根据合同约定，向客户提交完整的项目资料及交付物，并提出终验申请。 b)根据合同约定，配合组织项目验收，出具项目验收报告。		
	4.4. 运行维护	a)根据合同约定，向客户提供维保服务，并形成维保记录。		b)建立维保流程，制定维保方案，并按方案实施维保。

附录 C（规范性附录）： 信息安全应急处理服务特性要求

申请组织应满足申请级别和低于申请低级别的对应要求。

条款	三级要求	二级要求	一级要求
1. 准备阶段	具有处理一般信息安全事件的能力（注：参考国家标准 GB/Z 20986-2023《信息安全技术网络安全事件分类分级指南》，或参考组织所提供应急处理服务的对象所处的行业对信息安全事件的等级划分标准，主要考察有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件几类），具体见以下要求： a) 明确客户的应急需求。 b) 了解客户应急预案的内容。 c) 可提供本地2小时应急响应服务能力。 d) 对在应急处理服务过程中可能会采取的操作、处理等行为，获得用户的书面授权。	e) 在客户应急需求基础上制定应急服务方案，应急服务方案应涉及客户应急预案的启动与执行；若客户未建立应急预案，可协助客户建立；应急处理方案应包含实施方案失败的应变和回退措施。 f) 可提供本地1小时、外地8小时应急响应服务能力。	g) 可提供本地7*24小时、外地4小时应急响应服务能力。
2. 检测阶段	a) 确定检测对象及范围。 b) 对发生异常的系统进行信息的收集与分析，判断是否真正发生了安全事件。 c) 与客户共同确定应急处理方案，应急处理方案应明确检测范围与检测行为规范，其检测范围应仅限于客户已授权的与安全事件相关的数据，对客户的机密性数据信息未经授权不得访问。	d) 协助客户确定安全事件等级。	e) 对确认的安全事件启动安全事件管理程序。 f) 应急处理方案中应对可能造成的影响进行分析，包括社会影响。
3. 抑制阶段	a) 抑制措施应能够限制受攻击的范围，抑制潜在的或进一步的攻击和破坏行为。		b) 应使用可信的工具进行安全事件的抑制处理，不得使用受害系统已有的不可信文件。
4. 根除阶段	a) 协助客户检查所有受影响的系统，提出根除的方案建议，并协助客户进行具体实施。		b) 应使用可信的工具进行安全事件的根除处理，不得使

			用受害系统已有的不可信文件。
5. 恢复阶段	a) 告知客户网络或信息安全事件的恢复方法及可能存在的风险。 b) 对于不能彻底恢复配置和彻底清除系统上的恶意文件，或不能确定系统经过根除处理后是否可恢复正常时，应选择重建系统，具体要求如下：。 ● 应协助客户按照系统的初始化安全策略恢复系统。 ● 应协助客户验证恢复后的系统是否运行正常，并确认与原有系统配置保持一致。 ● 在帮助客户重建系统前需进行全面的数据备份，备份的数据要确保是没有被攻击者改变过的数据。	c) 与客户共同制定系统恢复方案，根据实际情况协助客户选择合理的恢复方法。 d)（如需重建系统时适用该条款）帮助客户为重建后的系统建立系统快照。	e)（如需重建系统时适用该条款）帮助客户对重建后的系统进行全面的安全加固。
6. 总结阶段	a) 应保存完整的网络或信息安全事件处理记录，并对事件处理过程进行总结和分析。 b) 提供网络或信息安全事件处理报告。 c) 提供网络或信息安全方面的建议和意见，必要时指导和协助客户实施。	d) 网络与信息安全事件处理记录应具备可追溯性。 e) 提供详实的网络与信息安全事件处理报告，完整展现应急处理服务的整个过程。	f) 对网络与信息安全事件进行总结和分析后，针对典型案例存入事件知识库。

附录 D（规范性附录）： 信息系统灾难备份与恢复服务特性要求

申请组织应满足申请级别和低于申请低级别的对应要求。

D1资源服务类（A类）要求

条款	三级要求	二级要求	一级要求
1.灾备中心场地资源要求	a)拥有至少1个可用于灾备中心的场地，位置避免处于地质沉降地带，交通便利、抗震等级按照国家规定的该地区抗震设防烈度执行，抗震设防类别为丙类及以上。 b)机房设置7×24小时门禁系统，所有进入机房的外部人员均需获得授权。 c)提供7×24小时闭路电视监控，其中公共区域的监控数据保留1个月以上，机房区域的监控数据保留2个月以上。 d)具备较高灵敏度的烟雾探测系统和消防系统，可实现分区灭火和定点报警。 e)灾备中心建筑耐火等级达到二级及以上。	f)拥有至少2个在不同地域的可用于灾备中心的场地资源，抗震设防烈度按照国家规定的该地区抗震设防烈度执行，抗震设防类别为乙类及以上。 g)灾备中心建设等级满足国标A级或国际T3以上机房要求。 h)具备气体灭火的消防系统，并具备早期报警系统/温感和烟感系统两级报警。	i)拥有至少2个在不同地域且处于不同的风险区域的灾备中心，满足异地灾备场地要求。 j)灾备中心应符合环保要求，采用高效新风换气系统，机房内正压，确保机房洁净度。 k)灾备中心的所有通道、机房内均设置CCTV 摄像头和7X24小时监控，并且可以按照客户的要求提供更长的保存期限。 l)灾备中心建筑耐火等级达到一级。
2.灾备中心基础设施要求	a)拥有灾备中心基础保障设施，包括但不限于供配电设施、空调暖通设施、给排水设施、监控设施、货运设施等，并定期检查。 b)拥有灾备中心基础配套设施，包括但不限于灾难恢复指挥中心、灾难恢复坐席、办公区、新闻发布中心、会议室、培训教室、模拟演练室等。 c)拥有灾备中心基础生活设施，包括但不限于日常运维人员生活所需宿舍、食堂、活动室等。 d)拥有灾备中心运行所需工作环境，包括但不限于计算机机房、主操作室、通讯机房、介质机房、信息系统设备测试维修机房等。	g)建立并运行基础设施日常巡检、监控、检查、维护、性能和容量管理、系统优化、应急与故障演练制度和流程。 h)具备双路高压供电和双路UPS供电，拥有后备发电机组，并能在UPS后备时间内提供电力供应，满足全部负荷连续运行48小时以上。 i)采用精密空调系统，机房温度应达到 22° C±2° C，湿度应达到45%-65%。	j)高压电来自两个独立的变电站的双路设计。 k)后备发电机组具有不停机补充燃料的能力，并且与燃料供应商签署燃料供应保障协议，保障燃料数量和质量要求，UPS和油机可自动切换。

	e)具备单路高压供电和独立UPS不间断电源保障。 f)采用精密空调系统，并具备恒温恒湿要求。		
3.灾备中心运维管理要求	a) 拥有灾备中心运维组织架构和运行管理团队，建立灾备中心机房运行管理和信息安全管理制度，并有效运行。 b) 建立灾备中心信息系统运行监控平台，及时发现灾备系统运行的故障并进行故障定位、诊断和审计，保存相关记录。 c) 建立灾备中心与生产中心统一变更流程。 d) 定期开展数据验证工作，确保生产与灾备数据的一致性、完整性和可用性。	e)灾备中心建立与生产中心统一的运维管理流程，实现两个中心联动运维。 f)灾备中心建立完整的电子化IT资产管理系统，能动态跟踪灾备中心IT资产变更。 g)灾备中心提供统一的客户服务平台，集中受理客户服务请求。 h)妥善保管运维记录，所有文档应满足客户监管机构要求。 i)定期开展灾难恢复模拟切换演练工作，确保发生灾难时，灾备系统能够接替生产系统运行。	j)采用运维监控和流程管理工具，实现对多数据中心资源的统一监控和自动化管理。 k)针对特定的灾难场景进行灾难恢复真实切换演练，并能接替生产完成至少2个小时的真实交易，并能在规定时间内进行回切。 l)具备真实切换演练的方案设计、培训、实施管理和应急处置能力。 m)定期维护灾难恢复预案，及时更新和分发预案文档，确保预案体系持续有效。 n)建立灾备中心应急管理体系，确保灾备系统稳定运行。

D2技术服务类（B类）要求

条款	三级要求	二级要求	一级要求
1.方案设计要求	a)开展灾难恢复系统建设需求调研，并进行需求分析。 b)按照灾难恢复规划和客户的投入能力，制定灾难备份与恢复系统技术方案、实施方案。	c)按照不同灾难恢复等级对资源的要求，确定灾备中心基础设施、数据备份系统、备用数据处理系统和备用网络系统等方面的需求，形成调研报告。 d)对业务系统中断后的损失进行分析，制定业务系统的最大可容忍业务中断时间（RTO）、最大可容忍中断时间点（RPO）。 e)依据系统建设要求和技术方案，制定系统测试方案。	f)识别客户的信息资产及其脆弱性和威胁，对基础设施和信息系统进行风险评估，制定本地风险控制策略和灾难恢复策略。 g)分析业务系统与应用系统之间的关联关系，确定应用系统灾难恢复指标和恢复优先级别。
2.系统建设与管理要求	a)依据灾难备份与恢复实施方案，实施灾难备份与恢复系统建设。 b)妥善保存灾难备份与恢复系统建设过程记录文档。	c)依据测试方案，组织实施系统测试，并详细记录。 d)制定灾难备份与恢复系统试运行方案，并详细记录试运行过程情况。	
3.预案制定与演练要求	a)制定信息系统灾难恢复预案。 b)开展信息系统灾难恢复桌面推演，并详细记录。 c)结合项目需要，组织开展灾难恢复预案培训。	d)制定系统演练方案，明确演练范围、人员、场景、步骤等内容。 e)组织演练培训和动员，明确参演人员角色、职责和具体任务。 f)设计多种演练场景并组织推演，详细记录演练过程。	g)制定信息系统灾难恢复预案体系，包括应急预案和恢复预案。 h)基于特定的演练场景，制定详细的切换演练方案。 i)组织完成真实切换演练前的桌面推演和模拟测试工作。 j)详细记录演练过程并进行总结，及时修订应急和恢复预案体系。

附录 E（规范性附录）：软件安全开发服务特性要求

条款	三级要求	二级要求	一级要求
1. 准备阶段	a) 制定软件项目安全开发管理计划，明确开发过程管控措施。 b) 建立软件开发的配置管理计划，明确配置管理的安全要求。 c) 建立变更控制制度，明确软件项目变更控制的安全要求。	d) 建立软件安全开发项目风险管理机制，对软件项目进行风险评估。	
2. 需求阶段	a) 调研项目背景信息，收集项目需求，明确软件功能、性能及安全方面的要求。	b) 基于客户需求，开展需求分析，编制具有软件安全需求的分析报告，需求分析报告中明确项目开发中使用的安全技术标准、规范。	c) 应基于软件安全威胁开展需求分析。 d) 基于软件项目需求分析建立软件安全开发模型。
3. 设计阶段	a) 根据软件项目需求，编制软件设计说明书，软件设计说明书明确系统/子系统的功能和非功能设计要求。 b) 软件设计说明书明确包含安全功能要求，包括标识与鉴别、访问控制、安全审计和安全管理等。	c) 概要设计说明书应明确数据完整性和保密性、通信完整性和保密性、软件容错、资源控制等安全功能要求。 d) 详细设计说明书中应包含对数据产生、传输、存储、使用、处理和归档安全方面的详细设计。	e) 概要设计说明书中应明确基于软件安全威胁分析的安全要求。 f) 当开发场景适用时，概要设计说明书中应明确抗抵赖、安全标记、可信路径等安全功能要求。 g) 依据安全要求和概要设计说明书，明确基于软件安全威胁分析进行详细设计。
4. 编码阶段	a) 制定统一的代码安全编码规范，确保开发人员参照规范安全编码。 b) 软件代码要经过安全检查、评审，对于发现的漏洞能有效修复。	c) 软件代码的安全检查、评审工作应形成记录。	d) 采用自动化工具对代码安全漏洞进行审查，对于发现的漏洞能有效修复，并形成审查报告。
5. 测试阶段	a) 依据软件设计说明书对软件功能、安全功能进行测试。 b) 对测试发现的漏洞进行分析并有效修复。	c) 制定包括系统安全性测试在内的测试计划，并执行系统测试，形成测试记录。	e) 基于软件项目的安全要求，制定系统渗透性测试方案，模拟攻击场景，对系统安全性进行测试，并形成分析报告。

			d)基于软件安全功能的安全要求，制定脆弱性测试方案，对安全漏洞进行测试，形成测试记录。	
6.验收阶段	**6.1 系统试运行**	a)测试系统运行的可靠性、稳定性和安全性，进行试运行，并记录系统运行状况，试运行周期至少一个月。 b)基于系统试运行相关记录，及时对软件进行调整、维护。试运行结束后，制定系统试运行报告。		c)提供三个月以上的试运行记录和报告；综合软件系统试运行状态，建立软件系统运行策略和安全指南。
	6.2 验收交付	a)根据合同约定，进行项目验收，形成项目验收报告。		
7.维保阶段		a)对于影响软件系统安全、稳定运行的缺陷，及时有效采取打补丁、版本升级等方式予以消除，并提供远程技术支持服务。	b)制定系统运行计划、安全事件响应计划、安全事件应急预案，建立应急响应服务保障团队；及时应对突发安全事件，并向用户提供安全事件解决报告。	c)制定软件健康检查计划、方案，定期实施，提交相应的系统健康检查报告、巡检报告；根据健康检查报告进行分析，持续优化系统。

附录F（规范性附录）：安全运维服务特性要求

条款		三级要求	二级要求	一级要求
1.准备阶段	1.1.需求调研与分析	a)调研客户信息系统安全现状，采集客户安全服务需求与目标，明确客户对信息系统安全运维服务时间、服务期限、服务内容以及服务方式的需求。 b)进行信息系统运维预算，定义运维服务。	c)分析客户对信息系统安全服务的需求和类型。 d)收集与分析信息系统的可用性指标。	
	1.2.签订服务协议	a)与客户签订服务协议，明确范围、目标、时间、内容、金额、质量和输出等以及安全运维的方式。		
2.方案设计阶段		a)根据系统安全运维需求，编制安全运维服务方案，明确安全运维服务时间、服务内容、服务方式、服务期限、服务人员、服务交付物、服务质量管理、服务沟通机制、服务风险管理等方面要求。 b)提供安全设备、业务系统的健康检查服务，并约定服务方式、检查频次和检查内容。	c)编制信息系统的可用性计划，监控可用性事件，报告可用性执行，指导可用性的改进。 d)编制信息系统的安全基线。	e)建立应急响应和灾难恢复机制，形成业务连续性计划。
3.服务实施阶段		a)实施初始服务，根据合同约定服务范围完成信息系统资产识别。 b)采集信息系统重要资产的安全配置、流量信息等安全信息。 c)对安全设备进行日常维护及监控，并记录硬件故障。 d)收集与分析网络及安全设备、服务器、数据库、中间件、应用系统的日志。 e)实施日常巡检服务：对用户的安全设备、网络设备、服务器提供业务操作巡检、状态巡检、安全策略配置巡检服务。 f)实施日常安全运维服务：完成安全设备、网络设备、服务器、应用系统安全事件监控；病毒监测、查杀及网	i)收集与建立配置管理数据库，确保配置项目的机密性、完整性、可用性（专职管理）。 j)实施安全设备、网络设备、中间件、数据库、服务器等资产的安全配置管理，定期对配置项进行更新和维护。 k)根据制定的安全配置基线，定期进行安全配置核查工作。	l)实施应急响应服务：完成应急响应预案制定，对应急事件及时响应，并对应急预案进行演练，形成相关记录。 m)依据运维变更管理程序，对运维实施过程中方案、资源变更进行有效控制，完整记录变更过程。 n)依据风险评估方案与计划实施信息系统风险评估；依据渗透测试方案与计划实施信息系统渗透测试。

	络防病毒维护；漏洞扫描、安全加固、补丁安装；并有相关记录。 g)对信息安全事件进行统计与分析。 h)实施健康检查服务：完成安全设备、业务系统的健康检查服务。		
4.运维服务报告阶段	a)向客户提交服务报告，定期收集与报告安全运维实施情况。 b)汇总整理全年服务记录，形成年终安全运维服务总结报告。 c)根据合同约定，配合组织项目验收，出具项目验收报告。		d)对客户满意度进行趋势分析。 e)对客户系统的安全态势做出分析，并给出安全建议。

附录 G（规范性附录）： 网络安全审计服务特性要求

条款		三级要求	二级要求	一级要求
1.审计对象识别	1.1 了解被审计方业务和 IT 情况	a)编制业务情况和IT情况调研表，并按照调研表收集有效信息。	b)编制审计对象列表，包括审计对象的数量、容量、功用、版本等属性。	c)梳理被审计方业务逻辑、应用系统处理逻辑和IT基础设施架构。
	1.2 了解被审计方组织管理和 IT 管理情况	a)有效掌握被审计方组织结构、IT管理情况，以及被审计方IT支撑业务的对应关系。 b)对网络安全审计的风险进行初步评价。	c)梳理被审计方规章制度文件，形成审计项并编制对应检查表。 d)编制完整审计调研报告，并说明重点审计项。	e)制定审计风险评价准则，评价审计风险，为确定重点审计项和明确审计内容提供依据。 f)应建立审计调研报告分级复核制度，明确规定各级复核人员的要求和责任。
2.编制审计实施方案	2.1 确定网络安全审计目标	a)合理确定每个具体网络安全审计项目的目标，网络安全审计目标可以包括信息化政策合规性、网络安全建设和绩效、政务系统整合和数据共享、个人信息保护和数据保护、信息化项目建设绩效与合规、信息系统有效性和可靠性、信息系统应急响应能力等。		
	2.2 确定网络安全审计依据	a)应根据具体审计目标，准确确定审计依据，网络安全审计依据可以是国家和政策部门法律法规、国际国内相关标准、被审计方自己实行的有关规章制度，以及审计委托方指定的其它审计依据。	b)应建立并维护常用审计依据库，并确保审计依据是当前适用版本。	
	2.3 确定网络安全审计	a)应根据审计目标和审计依据，确定审计范围。审计范围应包括组织机构范围、业务范围、IT基础设施和应用系统范围等。	d)应建立审计范围、审计对象、审计依据要求项、审计程序（方法）、所需资源的对应关系。	

	范围和审计内容	b)应根据审计依据和范围，确定审计内容。审计内容应划分到具体审计事项，明确每一个审计事项的审计要点和审计方法及所需资源。 c)审计方法及所需资源应包括审计人员、计划时间安排、审计工具，以及可操作的审计方法和流程。		
	2.4 组建审计组	a)应考虑审计目标、审计内容、审计范围等组建审计组，选择审计组成员应满足通用评价要求的人员能力要求，同时应满足审计和网络安全审计基础流程中的人员能力要求。		b)对于特定行业领域的网络安全审计，应具备聘请外部行业技术专家作为审计组成员。
3.审计取证与评价	**3.1 审计取证**	a)应选择适当的方法，在现场审计或非现场审计活动中获取审计证据。审计取证的方法可以是访谈、文件和记录调阅、审计项检查表、系统操作验证、审计工具、函证等。 b)在获取审计证据过程中，应选择适当的抽样方式。 c)应采取必要措施，保证审计证据的相关性、可靠性和充分性。	d)应具备至少利用一种网络安全审计工具执行审计取证的能力。 e)对电子形式存在的审计证据，应做好取证记录；应采取必要的措施，保护取证过程中所采集的电子数据的安全。	f)应至少具备和使用数据分析类、漏洞和缺陷扫描类、系统配置和运行日志检查类等类型的审计工具取证的能力。 g)利用审计工具取证时，应采取措施确保对审计对象的风险最小化。
	3.2 编制审计工作底稿	a)应在审计取证完成后，编制审计工作底稿或审计取证单，审计工作底稿或审计取证单应内容完整、记录清晰、结论明确，客观地反映项目审计方案的编制及实施情况，以及与形成审计结论、意见和建议有关的所有重要事项。	b)应建立审计工作底稿的分级复核制度，明确规定各级复核人员的要求和责任，审计工作底稿的内容应包括但不限于被审计部门的名称，审计事项及其期间或者截止日期，审计程序的执行过程及结果记录，审计结论、意见及建议，审计人员姓名和审计日期，复核人员姓名、复核日期和复核意见，编号及页次，被审计方意见、附件等。	

	3.3 审计评价	a)应对审计证据与审计依据的符合性进行评价，以形成审计发现，审计发现应明确审计项符合或不符合审计依据的程度，该程度可以用不同级别来表示。	b)应编制审计发现列表。	
4.审计报告	**4.1 审计报告的内容**	a)审计报告应完整、准确地反映审计结果，内容应包括审计概况、审计依据、审计发现、审计结论、审计意见等。	b)应建立审计报告分级复核制度，明确规定各级复核人员的要求和责任，审计报告中应提出审计发现问题改进建议。应建立程序，对已经出具的审计报告可能存在的重要错误或者遗漏及时更正，并将更正后的审计报告提交给原审计报告接收者。	c)在审计的任何阶段，如果遇到或发现与审计目标和内容有关的重大问题，如违法违规问题、重大安全风险等，应出具审计专报。
	4.2 交付审计报告	a)应建立审计报告的批准和交付程序，保留交付记录。	b)应建立审计报告归档和保管制度。任何组织或者个人查阅和使用归档后的审计报告，必须经审计机构负责人批准，但国家有关部门依法进行查阅的除外。	
5.跟踪审计	**5.1 跟踪审计报告**	a)应安排对审计发现问题的整改措施和整改措施的效果进行跟踪审计。 b)应与被审计方约定在规定的时间内实施跟踪审计，一般自审计报告交付起不超过6个月。 c)应当根据跟踪审计的实施过程和结果编制跟踪审计报告。 d)跟踪审计报告的管理参照4审计报告。	e)应编制跟踪审计方案，对后续审计做出安排。 f)跟踪审计报告的管理参照4审计报告。	g)跟踪审计报告的管理参照4审计报告。
6.审计质量控制	**6.1 审计质量控制制度**	a)应建立审计质量控制制度，审计质量控制制度应覆盖审计质量责任、审计职业道德、审计人力资源、审计业务执行、审计质量监控等。	b)应建立网络安全审计工作手册，规范网络安全审计全生命周期内的所有活动，确保审计质量控制制度与网络安全审计工作手册相适应。	c)应监督网络安全审计实施的过程，定期开展网络安全审计质量检查。

附录 H（规范性附录）： 渗透测试服务特性要求

条款		三级要求	二级要求	一级要求
1.准备阶段	1.1 需求调研内容	a)目标系统范围、业务类型、支持业务运行的系统技术框架和组件类型； b)目标系统业务高峰、测试时间与周期； c)目标系统是否有登录功能，如需登录测试，能否提供不同权限的测试账号； d)渗透测试实施方式，如需远程测试，是否需要VPN，是否有防火墙、WAF设备，是否可加白名单； e)目标系统负责人、对接人、应急联系人的联系方式。	f)渗透测试限制条件和注意事项	
	1.2 需求调研记录	a)应形成覆盖全部调研内容的调研记录，包括但不限于系统名称、业务类型、功能介绍、联系人等	b)编制渗透测试调研报告	
	1.3 方案制定	应依据渗透测试作业指导书，编制渗透测试方案，内容包括但不限于： a) 项目概述、服务背景、测试范围、测试原则、组织架构等； b) 测试对象、测试时间、测试方式（黑盒、灰盒、白盒）、测试接入方式（互联网、内网、专网）、测试计划、签订保密协议、工具准备等； c) 实施流程、测试授权、信息收集、漏洞测试、测试收尾、项目验收等； d) 调研记录、渗透测试记录与报告等项目交付物；		

		e) 项目实施风险及规避措施。		
	1.4 方案确认	a)应获得委托方对渗透测试方案的确认，确认方式可选择通过邮件、会议纪要、签字等任意一种方式。		
	1.5 渗透测试授权	a)应获得委托方的书面授权，授权书应签字或加盖单位公章。授权书内容包括但不限于委托方名称、联系人姓名、联系电话、允许测试时间、渗透测试范围（URL/IP/系统）、双方声明。		
2.实施阶段	2.1 信息收集分析	a)应对目标系统所在服务器端口的开放情况进行探测； b)应对目标系统业务功能进行分析，识别出关键功能模块、关键功能接口以及业务流程等，并对识别的资产进行信息收集及分析，包括但不限于Web网站、APP客户端、小程序等资产。	c)通过对目标系统的信息收集，识别目标系统前端、后端、以及系统架构、通用组件、数据库类型、通信方式、加密特征等关键信息； d)通过结合目标系统特征，关联进行信息收集，包括关联源码信息、系统版本号、系统弱口令、网盘等； e)对收集到的资产、业务特征、系统架构、关联资产信息的整合分析。	f)利用第三方工具或威胁情报平台等方式方法，对目标系统进行全面的敏感信息收集； g)通过一定的自动化开发工作，编写自动化信息收集工具，对目标系统的暴露面进行信息收集。
	2.2 漏洞发现	a)应利用收集到的信息，使用漏洞扫描工具进行漏洞扫描； b)应利用收集到的信息，通过人工方式识别漏洞，并针对性的进行漏洞挖掘。	c)通过对系统输入不同的数据和命令，使用黑盒漏洞发现方法，发现潜在漏洞。	d)通过访问系统源代码、配置文件和文档等信息，使用白盒漏洞发现方法，发现潜在漏洞； e)通过对系统输入大量的随机、异常或非预期的数据，使用模糊测试方法，发现系统潜在漏洞。

	2.3 漏洞验证	a)应针对被测目标系统进行漏洞利用和验证,并结合业务情况描述漏洞影响； b)应在测试过程中，针对增加、删除、修改、查询等测试动作进行记录，并在测试结束后，协助委托方进行后门清理、痕迹清除等工作。	c)在测试过程中，确保测试范围完整和风险可控，并保留测试过程中能够证明漏洞存在的关键截图、记录漏洞发生的参数位置信息及功能模块、记录漏洞验证的详细条件及验证过程； d)通过自动化手段对目标系统存在漏洞进行验证和分析； e)尝试通过多个漏洞的关联利用验证漏洞的综合可利用性及可能造成的实质影响。	f)能够持续进行原创漏洞挖掘和验证，具备CNNVD、CNVD任意证书的相应证明材料。
	2.4 漏洞评价	a)应参考国家标准，并结合行业相关标准，确定漏洞评价准则； b)应对漏洞风险进行定级和统计。	c)对已定级漏洞，根据业务场景变化，再次评估影响范围、利用难度，修订漏洞等级； d)已发现的漏洞类型未在漏洞评价准则中给予说明的或漏洞等级与漏洞定级评价准则存在出入的，应给出漏洞级别修订的原因，并完善本项目的漏洞评价准则。	
3. 总结阶段	3.1 报告编制	应编写渗透测试报告，内容包括但不限于： a)摘要、正文、版本信息、商业秘密等级（根据系统属性确定）； b)渗透测试目标、范围、时间、工具、人员； c)漏洞评价准则； d)测试过程中发现所有漏洞及修复建议等。	e)详细记录测试的技术细节和发现的问题； f)测试目标的漏洞统计数据和整体风险情况总结及安全评价。	g)对未公开信息或未发布补丁的漏洞提出缓解措施； h)对潜在的业务影响进行分析，根据渗透测试的结果和发现的漏洞，评估潜在的业务影响，包括数据泄露、服务中断、信息篡改等，提供对业务的风险评估和建议。

	3.2 报告评审交付	a)应对渗透测试报告进行内部评审，并得到委托方确认； b)应向委托方交付加盖公章或其他具有法律效力的印章的渗透测试报告，并采取措施保证报告交付的机密性和完整性。		
	3.3 漏洞复测	a)应具备漏洞复测的能力； b)必要时，按照委托方要求进行漏洞复测。	c)提供漏洞复测报告。	

附录 I：信息安全服务人员能力要求

从事信息安全服务的相关人员，应具备技术和管理能力并通过考试，各服务类别的笔试科目及范围如下：

序号	风险评估方向考试科目和范围
1.	信息安全保障人员基本素质 （1）职业素养：深刻理解从事信息安全保障工作必备的职业素养、特殊责任。 （2）知识结构：理解信息安全保障工作所需基础知识结构，深刻理解信息安全保障本质含义。 （3）工作技能：理解从事信息安全保障工作所需的基本技能、信息安全保障工作的特殊困难。
2.	信息安全意识教育 （1）信息安全保障概念：了解信息安全发展历程，理解通信保密、网络安全、信息安全、信息安全保障等概念，准确理解信息安全属性，掌握什么时候需要分别考虑信息安全属性。 （2）信息安全形势：了解国内外信息安全形势、最新的典型信息安全问题、应对典型信息安全问题的方法。 （3）信息安全需求识别：了解形势发展的需要，理解社会责任的需求、组织业务保障的需要，了解现实信息技术环境的需求，指导如何提出实际需要，了解法律法规的要求、客户合同的要求、强制标准的要求、风险评估的要求、日常保障的要求、新技术和新措施应用的要求。
3.	信息安全法律法规体系 （1）法律法规结构体系：了解我国信息安全法律法规结构、基本分类。 （2）国内外信息安全法律法规建设概况：了解中国、美国及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：了解国外信息安全标准化相关机构以及相互关系，如 ISO、IEC、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，了解我国信息安全标准相关组织及其关系，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，了解 ISO、IEC 和 ITU 信息安全相关标准建设情况，了解美国特有的信息安全相关标准建设情况，了解我国信息安全相关标准建设情况。 （4）我国信息安全管理概况：了解我国信息安全相关管理机构、管理模式、主要的信息安全管理手段。 （5）典型信息安全法律法规：了解刑法中与信息安全相关的条款，了解《保守国家秘密法》、《商用密码管理条例》，了解我国互联网相关管理规定、信息安全产品相关管理规定。
4.	通信技术基础 （1）通信的基本概念：理解通信的本质含义及电信概念、通信网络形成过程，了解通信网络结构、通信网络中的安全属性、通信网络应用分类、“网络”习惯分类、通信网络安全问题本质成因。 （2）通信协议及应用：熟悉 OSI 七层模型、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、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。
5.	风险管理基础 （1）基本概念：理解风险的定义，风险管理的基本思想。 （2）常见风险评估方法：各类风险评估方法的基本思路、应用场景。 （3）典型风险评估方法：掌握 1 种风险评估方法。 （4）风险处置方法：了解各种风险处置方法及其应用场景。 （5）风险管理相关标准：了解风险管理相关国际标准、国家标准。
6.	风险管理 （1）风险管理的业界标准与实践：理解 GB/T 24353、GB/T 20984，了解各行业的信息安全风险管理指引。 （2）风险管理的实施过程：了解风险管理的全过程、风险管理准备工作（如组织与规划）的主要方法、风险评估主要方法与实施、风险评估的报告格式与形成报告的方法、风险处置主要方法与实施。 （3）风险管理工具使用：了解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：了解典型的风险具体处置措施。 （5）风险管理实例：了解主要行业的典型安全风险特性，了解 1-2 个行业的典型风险管理实例。
7.	项目管理基础 （1）项目管理基本概念：正确理解项目的本质、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。 （2）项目管理的发展历史与现状：了解项目管理的发展过程、国际项目管理发展现状、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：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、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，掌握并实践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、项目生命周期，正确掌握集成类项目九大管理知识领域特性，掌握并实践完整的集成类项目过程。
8.	信息安全技术 （1）信息安全技术发展：了解信息安全技术结构及相互关系、最新进展、应用基本方法。

	（2）密码学及其应用:了解密码学发展历史、密码学在信息安全中的特殊地位，基本理解密码学的基本原理，基本掌握典型密码算法（对称、非对称、HASH 函数）、典型密码算法的作用与应用方法、典型应用中如何采用密码技术，了解密钥管理方法。 （3）网络安全技术:了解网络安全技术的范畴、网络边界划分原则与方法、典型的网络安全问题、典型的网络攻击手段、网络边界防御原理与方法、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）、网络通讯安全原理与方法、了解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）。 （4）平台安全技术:了解常用系统平台（UNIX、Linux、Windows 等）的典型安全问题、常用的应用支撑平台（WEB、数据库等）的典型安全问题、各类安全漏洞的管理标准与方法、典型的对平台攻击手段、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、桌面系统的典型安全问题、桌面系统的安全保障方法与工具。 （5）应用安全技术: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、安全软件开发过程管理与控制、典型的应用安全漏洞、应用软件安全测试方法与工具。 （6）数据安全技术:了解数据安全的范畴、数据生命周期的各阶段安全需求、数据生命周期的各阶段安全保障技术与方法、灾难备份与恢复技术。 （7）物理安全技术：了解信息安全保障中物理安全的范畴、典型的物理安全问题、典型的物理安全防范技术与方法、支持性基础设施的物理安全问题及保护措施。

序号	安全集成方向考试科目和范围
1.	信息安全保障人员基本素质 （1）职业素养：深刻理解从事信息安全保障工作必备的职业素养、特殊责任。 （2）知识结构：理解信息安全保障工作所需基础知识结构，深刻理解信息安全保障本质含义。 （3）工作技能：理解从事信息安全保障工作所需的基本技能、信息安全保障工作的特殊困难。
2.	信息安全意识教育 （1）信息安全保障概念：了解信息安全发展历程，理解通信保密、网络安全、信息安全、信息安全保障等概念，准确理解信息安全属性，掌握什么时候需要分别考虑信息安全属性。 （2）信息安全形势：了解国内外信息安全形势、最新的典型信息安全问题、应对典型信息安全问题的方法。 （3）信息安全需求识别：了解形势发展的需要，理解社会责任的需求、组织业务保障的需要，了解现实信息技术环境的需求，指导如何提出实际需要，了解法律法规的要求、客户合同的要求、强制标准的要求、风险评估的要求、日常保障的要求、新技术和新措施应用的要求。
3.	信息安全法律法规体系 （1）法律法规结构体系：了解我国信息安全法律法规结构、基本分类。 （2）国内外信息安全法律法规建设概况：了解中国、美国及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：了解国外信息安全标准化相关机构以及相互关系，如 ISO、IEC、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，了解我国信息安全标准相关组织及其关系，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，了解 ISO、IEC 和 ITU 信息安全相关标准建设情况，了解美国特有的信息安全相关标准建设情况，了解我国信息安全相关标准建设情况。 （4）我国信息安全管理概况：了解我国信息安全相关管理机构、管理模式、主要的信息安全管理手段。 （5）典型信息安全法律法规：了解刑法中与信息安全相关的条款，了解《保守国家秘密法》、《商用密码管理条例》，了解我国互联网相关管理规定、信息安全产品相关管理规定。
4.	通信技术基础 （1）通信的基本概念：理解通信的本质含义及电信概念、通信网络形成过程，了解通信网络结构、通信网络中的安全属性、通信网络应用分类、“网络”习惯分类、通信网络安全问题本质成因。 （2）通信协议及应用：熟悉 OSI 七层模型、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、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。
5.	风险管理基础 （1）基本概念：理解风险的定义，风险管理的基本思想。

	（2）常见风险评估方法：各类风险评估方法的基本思路、应用场景。 （3）典型风险评估方法：掌握 1 种风险评估方法。 （4）风险处置方法：了解各种风险处置方法及其应用场景。 （5）风险管理相关标准：了解风险管理相关国际标准、国家标准。
6.	安全集成基础 （1）安全集成的业界标准与实践：了解 GB/T 20261、ISO/IEC 21827、SSE-CMM3.0 对安全集成的要求，了解信息系统安全集成服务服务认证实施规则对安全集成的要求，了解 CNCA/CTS 0052 信息安全服务服务认证技术规范。 （2）安全集成过程：了解安全软件集成管理的全过程、安全集成准备工作（如需求分析）的主要方法、安全集成设计的主要方法、安全集成实施的主要工作、安全集成保证的主要内容。 （3）安全集成工具使用：了解典型的安全集成工具，熟悉需求分析工具使用，了解安全集成设计工具使用、安全保证工具使用。 （4）典型安全保障手段：了解典型的信息安全保障手段、常用的信息安全技术应用、常用的信息安全产品。 （5）安全集成实例：了解安全集成方案的结构、主要行业的安全集成特性、1-2 个行业的典型安全集成实例。
7.	项目管理基础 （1）项目管理基本概念：正确理解项目的本质、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。 （2）项目管理的发展历史与现状：了解项目管理的发展过程、国际项目管理发展现状、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：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、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，掌握并实践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、项目生命周期，正确掌握集成类项目九大管理知识领域特性，掌握并实践完整的集成类项目过程。
8.	信息安全技术 （1）信息安全技术发展：了解信息安全技术结构及相互关系、最新进展、应用基本方法。 （2）密码学及其应用:了解密码学发展历史、密码学在信息安全中的特殊地位，基本理解密码学的基本原理，基本掌握典型密码算法（对称、非对称、HASH 函数）、典型密码算法的作用与应用方法、典型应用中如何采用密码技术，了解密钥管理方法。

	（3）网络安全技术:了解网络安全技术的范畴、网络边界划分原则与方法、典型的网络安全问题、典型的网络攻击手段、网络边界防御原理与方法、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）、网络通讯安全原理与方法、了解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）。 （4）平台安全技术:了解常用系统平台（UNIX、Linux、Windows 等）的典型安全问题、常用的应用支撑平台（WEB、数据库等）的典型安全问题、各类安全漏洞的管理标准与方法、典型的对平台攻击手段、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、桌面系统的典型安全问题、桌面系统的安全保障方法与工具。 （5）应用安全技术: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、安全软件开发过程管理与控制、典型的应用安全漏洞、应用软件安全测试方法与工具。 （6）数据安全技术:了解数据安全的范畴、数据生命周期的各阶段安全需求、数据生命周期的各阶段安全保障技术与方法、灾难备份与恢复技术。 （7）物理安全技术：了解信息安全保障中物理安全的范畴、典型的物理安全问题、典型的物理安全防范技术与方法、支持性基础设施的物理安全问题及保护措施。

序号	应急处理方向考试科目和范围
1.	信息安全保障人员基本素质 （1）职业素养：深刻理解从事信息安全保障工作必备的职业素养、特殊责任。 （2）知识结构：理解信息安全保障工作所需基础知识结构，深刻理解信息安全保障本质含义。 （3）工作技能：理解从事信息安全保障工作所需的基本技能、信息安全保障工作的特殊困难。
2.	信息安全意识教育 （1）信息安全保障概念：了解信息安全发展历程，理解通信保密、网络安全、信息安全、信息安全保障等概念，准确理解信息安全属性，掌握什么时候需要分别考虑信息安全属性。 （2）信息安全形势：了解国内外信息安全形势、最新的典型信息安全问题、应对典型信息安全问题的方法。 （3）信息安全需求识别：了解形势发展的需要，理解社会责任的需求、组织业务保障的需要，了解现实信息技术环境的需求，指导如何提出实际需要，了解法律法规的要求、客户合同的要求、强制标准的要求、风险评估的要求、日常保障的要求、新技术和新措施应用的要求。
3.	渗透测试技术与应用 （1）渗透测试的基本概念：熟悉信息安全威胁、设备渗透测试、渗透测试流程、渗透测试的目标、渗透测试的分类、渗透测试的限制。 （2）渗透测试法律问题：熟悉渗透测试的法律依据、渗透测试的法律框架、与客户签订渗透测试协议。 （3）渗透测试方法论：熟悉组织、个人、技术和道德的相关要求，掌握渗透测试的方法论、渗透测试五个步骤。 （4）实施渗透测试与报告撰写：熟悉渗透测试的准备，掌握对渗透目标的预查，熟悉信息及风险的分析方法，熟知启动渗透测试，熟悉最后分析及消除影响、渗透测试报告的撰写。 （5）Unix 渗透测试方法与工具使用：熟知 Unix 缓冲区溢出渗透、Unix Shell 渗透技术、Unix 系统提权、Apache 安全渗透、Unix 后门技术。 （6）Windows 系统渗透测试方法与工具使用：熟悉网络协议安全、网络端口扫描与漏洞扫描、嗅探技术与密码截获及破解、缓冲区溢出渗透、病毒与木马技术。 （7）Web 应用系统渗透测试方法与工具使用：熟悉 HTTP 协议基本概念、SQL 注入渗透技术与工具、XSS 跨站脚本技术、CSRF 渗透技术、Web Service 渗透技术，了解 Web 安全编程。 （8）数据库渗透测试与工具使用：熟悉数据库系统的威胁、Oracle 渗透测试、各种 PL/SQL Injection 漏洞利用、Lateral SQL Injection，了解其他数据库渗透测试。
4.	信息安全法律法规体系 （1）法律法规结构体系：了解我国信息安全法律法规结构、基本分类。 （2）国内外信息安全法律法规建设概况：了解中国、美国及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：了解国外信息安全标准化相关机构以及相互关系，如 ISO、IEC、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，了解我国信息安全标准相关组织及其关系，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，了解 ISO、IEC 和 ITU 信息安全相关标准建设情况，了解美国特有的信息安全相关标准建设情况，了解我国信息安全相关标准建设情况。 （4）我国信息安全管理概况：了解我国信息安全相关管理机构、管理模式、主要的信息安全管理手段。 （5）典型信息安全法律法规：了解刑法中与信息安全相关的条款，了解《保守国家秘密法》、《商用密码管理条例》，了解我国互联网相关管理规定、信息安全产品相关管理规定。
5.	通信技术基础 （1）通信的基本概念：理解通信的本质含义及电信概念、通信网络形成过程，了解通信网络结构、通信网络中的安全属性、通信网络应用分类、“网络”习惯分类、通信网络安全问题本质成因。 （2）通信协议及应用：熟悉 OSI 七层模型、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、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。
6.	风险管理基础 （1）基本概念：理解风险的定义，风险管理的基本思想。 （2）常见风险评估方法：各类风险评估方法的基本思路、应用场景。 （3）典型风险评估方法：掌握 1 种风险评估方法。 （4）风险处置方法：了解各种风险处置方法及其应用场景。 （5）风险管理相关标准：了解风险管理相关国际标准、国家标准。
7.	应急服务技术与应用 （1）应急服务的相关规范：了解 YD/T 1799、业务连续性标准 ISO/IEC 22301、应急服务的相关安全要求。 （2）应急服务过程管理：了解应急服务的全过程、应急服务准备工作（如组织与规划）的主要方法、应急服务的回退过程、应急服务的风险评估、应急服务的资源协调、应急服务的升级机制、应急服务的现场保护与取证方法。 （3）安全技术工具的使用：了解典型的安全监测工具、典型的安全检测工具（渗透工具）、典型的安全分析工具、典型的安全管理工具。 （4）典型应急案例分析：了解 1-2 个行业的典型管理实例。
8.	项目管理基础 （1）项目管理基本概念：正确理解项目的本质、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。 （2）项目管理的发展历史与现状：了解项目管理的发展过程、国际项目管理发展现状、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：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、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，掌握并实践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、项目生命周期，正确掌握集成类项目九大管理知识领域特性，掌握并实践完整的集成类项目过程。
9.	信息安全技术 （1）信息安全技术发展：了解信息安全技术结构及相互关系、最新进展、应用基本方法。 （2）密码学及其应用:了解密码学发展历史、密码学在信息安全中的特殊地位，基本理解密码学的基本原理，基本掌握典型密码算法（对称、非对称、HASH 函数）、典型密码算法的作用与应用方法、典型应用中如何采用密码技术，了解密钥管理方法。 （3）网络安全技术:了解网络安全技术的范畴、网络边界划分原则与方法、典型的网络安全问题、典型的网络攻击手段、网络边界防御原理与方法、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）、网络通讯安全原理与方法、了解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）。 （4）平台安全技术:了解常用系统平台（UNIX、Linux、Windows 等）的典型安全问题、常用的应用支撑平台（WEB、数据库等）的典型安全问题、各类安全漏洞的管理标准与方法、典型的对平台攻击手段、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、桌面系统的典型安全问题、桌面系统的安全保障方法与工具。 （5）应用安全技术: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、安全软件开发过程管理与控制、典型的应用安全漏洞、应用软件安全测试方法与工具。 （6）数据安全技术:了解数据安全的范畴、数据生命周期的各阶段安全需求、数据生命周期的各阶段安全保障技术与方法、灾难备份与恢复技术。 （7）物理安全技术：了解信息安全保障中物理安全的范畴、典型的物理安全问题、典型的物理安全防范技术与方法、支持性基础设施的物理安全问题及保护措施。

序号	灾难备份与恢复方向考试科目和范围
1.	信息安全保障人员基本素质 （1）职业素养：深刻理解从事信息安全保障工作必备的职业素养、特殊责任。 （2）知识结构：理解信息安全保障工作所需基础知识结构，深刻理解信息安全保障本质含义。 （3）工作技能：理解从事信息安全保障工作所需的基本技能、信息安全保障工作的特殊困难。
2.	信息安全意识教育 （1）信息安全保障概念：了解信息安全发展历程，理解通信保密、网络安全、信息安全、信息安全保障等概念，准确理解信息安全属性，掌握什么时候需要分别考虑信息安全属性。 （2）信息安全形势：了解国内外信息安全形势、最新的典型信息安全问题、应对典型信息安全问题的方法。 （3）信息安全需求识别：了解形势发展的需要，理解社会责任的需求、组织业务保障的需要，了解现实信息技术环境的需求，指导如何提出实际需要，了解法律法规的要求、客户合同的要求、强制标准的要求、风险评估的要求、日常保障的要求、新技术和新措施应用的要求。
3.	信息安全法律法规体系 （1）法律法规结构体系：了解我国信息安全法律法规结构、基本分类。 （2）国内外信息安全法律法规建设概况：了解中国、美国及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：了解国外信息安全标准化相关机构以及相互关系，如 ISO、IEC、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，了解我国信息安全标准相关组织及其关系，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，了解 ISO、IEC 和 ITU 信息安全相关标准建设情况，了解美国特有的信息安全相关标准建设情况，了解我国信息安全相关标准建设情况。 （4）我国信息安全管理概况：了解我国信息安全相关管理机构、管理模式、主要的信息安全管理手段。 （5）典型信息安全法律法规：了解刑法中与信息安全相关的条款，了解《保守国家秘密法》、《商用密码管理条例》，了解我国互联网相关管理规定、信息安全产品相关管理规定。
4.	风险管理基础 （1）基本概念：理解风险的定义，风险管理的基本思想。 （2）常见风险评估方法：各类风险评估方法的基本思路、应用场景。 （3）典型风险评估方法：掌握 1 种风险评估方法。 （4）风险处置方法：了解各种风险处置方法及其应用场景。 （5）风险管理相关标准：了解风险管理相关国际标准、国家标准。
5.	灾备服务技术与应用 （1）灾备服务的业界标准与实践：了解国内外灾备相关技术和标准情况、GB/T 20988。

	（2）灾备恢复技术：了解数据存储技术、数据复制技术和数据管理技术的原理，了解灾难检测技术、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：了解灾备服务的全过程、灾备服务准备工作（如组织与规划）的主要方法、灾备服务的资源协调、备份管理机制、恢复测试管理、恢复实施管理、灾备服务的现场保护与取证方法。 （4）灾备工具使用与管理：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，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。 （5）灾备实例分析：了解主要行业的典型灾难备份系统管理特性，了解 1-2 个行业的典型灾难备份系统管理实例。
6.	项目管理基础 （1）项目管理基本概念：正确理解项目的本质、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。 （2）项目管理的发展历史与现状：了解项目管理的发展过程、国际项目管理发展现状、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：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、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，掌握并实践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、项目生命周期，正确掌握集成类项目九大管理知识领域特性，掌握并实践完整的集成类项目过程。
7.	信息安全技术 （1）信息安全技术发展：了解信息安全技术结构及相互关系、最新进展、应用基本方法。 （2）密码学及其应用:了解密码学发展历史、密码学在信息安全中的特殊地位，基本理解密码学的基本原理，基本掌握典型密码算法（对称、非对称、HASH 函数）、典型密码算法的作用与应用方法、典型应用中如何采用密码技术，了解密钥管理方法。 （3）网络安全技术:了解网络安全技术的范畴、网络边界划分原则与方法、典型的网络安全问题、典型的网络攻击手段、网络边界防御原理与方法、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）、网络通讯安全原理与方法、了解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）。 （4）平台安全技术:了解常用系统平台（UNIX、Linux、Windows 等）的典型安全问题、常用的应用支撑平台（WEB、数据库等）的典型安全问题、各类安全漏洞的管理标准与方法、典型的对平台攻击手段、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、桌面系统的典型安全问题、桌面系统的安全保障方法与工具。

	（5）应用安全技术: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、安全软件开发过程管理与控制、典型的应用安全漏洞、应用软件安全测试方法与工具。 （6）数据安全技术:了解数据安全的范畴、数据生命周期的各阶段安全需求、数据生命周期的各阶段安全保障技术与方法、灾难备份与恢复技术。 （7）物理安全技术：了解信息安全保障中物理安全的范畴、典型的物理安全问题、典型的物理安全防范技术与方法、支持性基础设施的物理安全问题及保护措施。

序号	软件安全开发方向考试科目和范围
1.	信息安全保障人员基本素质 （1）职业素养：深刻理解从事信息安全保障工作必备的职业素养、特殊责任。 （2）知识结构：理解信息安全保障工作所需基础知识结构，深刻理解信息安全保障本质含义。 （3）工作技能：理解从事信息安全保障工作所需的基本技能、信息安全保障工作的特殊困难。
2.	信息安全意识教育 （1）信息安全保障概念：了解信息安全发展历程，理解通信保密、网络安全、信息安全、信息安全保障等概念，准确理解信息安全属性，掌握什么时候需要分别考虑信息安全属性。 （2）信息安全形势：了解国内外信息安全形势、最新的典型信息安全问题、应对典型信息安全问题的方法。 （3）信息安全需求识别：了解形势发展的需要，理解社会责任的需求、组织业务保障的需要，了解现实信息技术环境的需求，指导如何提出实际需要，了解法律法规的要求、客户合同的要求、强制标准的要求、风险评估的要求、日常保障的要求、新技术和新措施应用的要求。
3.	信息安全法律法规体系 （1）法律法规结构体系：了解我国信息安全法律法规结构、基本分类。 （2）国内外信息安全法律法规建设概况：了解中国、美国及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：了解国外信息安全标准化相关机构以及相互关系，如 ISO、IEC、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，了解我国信息安全标准相关组织及其关系，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，了解 ISO、IEC 和 ITU 信息安全相关标准建设情况，了解美国特有的信息安全相关标准建设情况，了解我国信息安全相关标准建设情况。 （4）我国信息安全管理概况：了解我国信息安全相关管理机构、管理模式、主要的信息安全管理手段。 （5）典型信息安全法律法规：了解刑法中与信息安全相关的条款，了解《保守国家秘密法》、《商用密码管理条例》，了解我国互联网相关管理规定、信息安全产品相关管理规定。
4.	通信技术基础 （1）通信的基本概念：理解通信的本质含义及电信概念、通信网络形成过程，了解通信网络结构、通信网络中的安全属性、通信网络应用分类、“网络”习惯分类、通信网络安全问题本质成因。 （2）通信协议及应用：熟悉 OSI 七层模型、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、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。
5.	风险管理基础 （1）基本概念：理解风险的定义，风险管理的基本思想。

	（2）常见风险评估方法：各类风险评估方法的基本思路、应用场景。 （3）典型风险评估方法：掌握 1 种风险评估方法。 （4）风险处置方法：了解各种风险处置方法及其应用场景。 （5）风险管理相关标准：了解风险管理相关国际标准、国家标准。
6.	安全软件技术与测试 （1）安全软件的业界标准与实践：了解信息安全管理体系对安全软件的要求、CC 对安全软件的要求、FIPS 140-2 对安全软件的要求、PCI DSS 对安全软件的要求、安全弱点管理相关规范，如 SCAP。 （2）安全开发生命周期：了解安全软件开发管理的全过程，如 SDL、安全需求分析的主要方法、安全设计的主要方法、安全编码的主要工作、安全测试的主要内容、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，了解逻辑访问控制、开发工具与配置项管理，熟悉人员与角色管理。 （4）安全功能架构与设计：了解典型的安全功能、安全功能的实现模型。 （5）安全漏洞分析：了解 SCAP、 CVSS、典型的安全漏洞机理。 （6）安全编码：了解典型的安全编码规则、典型问题的修复方法。 （7）密码安全模块：了解典型的加密算法和应用方法、典型的密码应用方式，熟悉 FIPS 140-2 的要求。 （8）安全测试与实验：了解软件测试的基本方法、软件安全功能测试的基本手段，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）。
7.	项目管理基础 （1）项目管理基本概念：正确理解项目的本质、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。 （2）项目管理的发展历史与现状：了解项目管理的发展过程、国际项目管理发展现状、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：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、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，掌握并实践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、项目生命周期，正确掌握集成类项目九大管理知识领域特性，掌握并实践完整的集成类项目过程。
8.	信息安全技术

	（1）信息安全技术发展：了解信息安全技术结构及相互关系、最新进展、应用基本方法。 （2）密码学及其应用:了解密码学发展历史、密码学在信息安全中的特殊地位，基本理解密码学的基本原理，基本掌握典型密码算法（对称、非对称、HASH 函数）、典型密码算法的作用与应用方法、典型应用中如何采用密码技术，了解密钥管理方法。 （3）网络安全技术:了解网络安全技术的范畴、网络边界划分原则与方法、典型的网络安全问题、典型的网络攻击手段、网络边界防御原理与方法、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）、网络通讯安全原理与方法、了解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）。 （4）平台安全技术:了解常用系统平台（UNIX、Linux、Windows 等）的典型安全问题、常用的应用支撑平台（WEB、数据库等）的典型安全问题、各类安全漏洞的管理标准与方法、典型的对平台攻击手段、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、桌面系统的典型安全问题、桌面系统的安全保障方法与工具。 （5）应用安全技术: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、安全软件开发过程管理与控制、典型的应用安全漏洞、应用软件安全测试方法与工具。 （6）数据安全技术:了解数据安全的范畴、数据生命周期的各阶段安全需求、数据生命周期的各阶段安全保障技术与方法、灾难备份与恢复技术。 （7）物理安全技术：了解信息安全保障中物理安全的范畴、典型的物理安全问题、典型的物理安全防范技术与方法、支持性基础设施的物理安全问题及保护措施。

序号	安全运维方向考试科目和范围
1.	信息安全保障人员基本素质 （1）职业素养：深刻理解从事信息安全保障工作必备的职业素养、特殊责任。 （2）知识结构：理解信息安全保障工作所需基础知识结构，深刻理解信息安全保障本质含义。 （3）工作技能：理解从事信息安全保障工作所需的基本技能、信息安全保障工作的特殊困难。
2.	信息安全意识教育 （1）信息安全保障概念：了解信息安全发展历程，理解通信保密、网络安全、信息安全、信息安全保障等概念，准确理解信息安全属性，掌握什么时候需要分别考虑信息安全属性。 （2）信息安全形势：了解国内外信息安全形势、最新的典型信息安全问题、应对典型信息安全问题的方法。 （3）信息安全需求识别：了解形势发展的需要，理解社会责任的需求、组织业务保障的需要，了解现实信息技术环境的需求，指导如何提出实际需要，了解法律法规的要求、客户合同的要求、强制标准的要求、风险评估的要求、日常保障的要求、新技术和新措施应用的要求。
3.	信息安全法律法规体系 （1）法律法规结构体系：了解我国信息安全法律法规结构、基本分类。 （2）国内外信息安全法律法规建设概况：了解中国、美国及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：了解国外信息安全标准化相关机构以及相互关系，如 ISO、IEC、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，了解我国信息安全标准相关组织及其关系，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，了解 ISO、IEC 和 ITU 信息安全相关标准建设情况，了解美国特有的信息安全相关标准建设情况，了解我国信息安全相关标准建设情况。 （4）我国信息安全管理概况：了解我国信息安全相关管理机构、管理模式、主要的信息安全管理手段。 （5）典型信息安全法律法规：了解刑法中与信息安全相关的条款，了解《保守国家秘密法》、《商用密码管理条例》，了解我国互联网相关管理规定、信息安全产品相关管理规定。
4.	通信技术基础 （1）通信的基本概念：理解通信的本质含义及电信概念、通信网络形成过程，了解通信网络结构、通信网络中的安全属性、通信网络应用分类、“网络”习惯分类、通信网络安全问题本质成因。 （2）通信协议及应用：熟悉 OSI 七层模型、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、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。
5.	风险管理基础 （1）基本概念：理解风险的定义，风险管理的基本思想。

	（2）常见风险评估方法：各类风险评估方法的基本思路、应用场景。 （3）典型风险评估方法：掌握 1 种风险评估方法。 （4）风险处置方法：了解各种风险处置方法及其应用场景。 （5）风险管理相关标准：了解风险管理相关国际标准、国家标准。
6.	安全运维技术与应用 （1）业界标准与实践：了解信息安全管理体系对安全运维的要求、服务管理体系对安全运维的要求、安全弱点管理相关规范。 （2）安全运维结构与思想：了解安全运维的核心思想、安全运维的管理关系结构。 （3）安全运维工具使用：了解典型的安全运维工具、典型的安全运维为手段。 （4）安全运维实例：了解主要行业的安全运维特性，了解 1-2 个行业的典型安全运维实例。
7.	项目管理基础 （1）项目管理基本概念：正确理解项目的本质、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。 （2）项目管理的发展历史与现状：了解项目管理的发展过程、国际项目管理发展现状、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：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、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，掌握并实践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、项目生命周期，正确掌握集成类项目九大管理知识领域特性，掌握并实践完整的集成类项目过程。

8.	信息安全技术 （1）信息安全技术发展：了解信息安全技术结构及相互关系、最新进展、应用基本方法。 （2）密码学及其应用:了解密码学发展历史、密码学在信息安全中的特殊地位，基本理解密码学的基本原理，基本掌握典型密码算法（对称、非对称、HASH 函数）、典型密码算法的作用与应用方法、典型应用中如何采用密码技术，了解密钥管理方法。 （3）网络安全技术:了解网络安全技术的范畴、网络边界划分原则与方法、典型的网络安全问题、典型的网络攻击手段、网络边界防御原理与方法、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）、网络通讯安全原理与方法、了解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）。 （4）平台安全技术:了解常用系统平台（UNIX、Linux、Windows 等）的典型安全问题、常用的应用支撑平台（WEB、数据库等）的典型安全问题、各类安全漏洞的管理标准与方法、典型的对平台攻击手段、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、桌面系统的典型安全问题、桌面系统的安全保障方法与工具。 （5）应用安全技术: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、安全软件开发过程管理与控制、典型的应用安全漏洞、应用软件安全测试方法与工具。 （6）数据安全技术:了解数据安全的范畴、数据生命周期的各阶段安全需求、数据生命周期的各阶段安全保障技术与方法、灾难备份与恢复技术。 （7）物理安全技术：了解信息安全保障中物理安全的范畴、典型的物理安全问题、典型的物理安全防范技术与方法、支持性基础设施的物理安全问题及保护措施。

序号	网络安全审计方向考试科目和范围
1.	网络安全审计人员基本素质 （1）职业素养：深刻理解从事网络安全审计工作必备的职业素养、特殊责任。 （2）知识结构：理解网络安全审计工作所需基础知识结构，深刻理解网络安全审计的本质含义。 （3）工作技能：理解从事网络安全审计工作所需的基本技能、网络安全审计工作的特殊困难。
2.	网络安全审计基础知识 （1）网络安全审计概念：理解审计、审计依据、审计计划、审计实施、审计报告、跟踪审计、审计证据、审计发现、审计工作底稿等概念，准确理解审计的含义、对象、分类等内容。 （2）网络安全审计内容：了解网络安全审计所涵盖的内容范围。 （3）网络安全审计的历史和发展：了解网络安全审计提出的必要性、与风险评估、测评、检查、审核等的关系，了解网络安全审计的发展历程。 （4）网络安全审计的发展形势：了解国内外网络安全审计发展形势、了解国内各行业和监管部门对网络安全审计的认识及最新动态。
3.	网络安全审计依据 （1）我国法律法规体系：了解我国信息系统法律法规架构、基本分类。 （2）国内外信息系统标准：了解国外信息标准化相关机构以及相互关系，如 ISO、IEC、ITU 和发达国家的信息标准相关组织机构，了解我国信息标准相关组织及其关系，如国家标准化管理委员会、全国信息化标准技术委员会、全国信息安全标准化技术委员会等，了解 ISO、IEC 和 ITU 信息相关标准建设情况，了解美国特有的信息相关标准建设情况，了解我国信息相关标准建设情况。 （3）我国相关行业标准：了解我国各行业信息相关标准管理机构、以及主要的信息管理标准，例如金融行业、通信行业、能力行业等。 （4）我国相关监管文件：了解我国监管部门制定及发布的信息化文件，例如银保监会、证监会、工信部、能源局等。 （5）国内外 IT 相关的最佳实践文档。
4.	网络安全审计方法 （1）网络安全审计流程：了解传统审计的流程，了解网络安全审计的流程。 （2）网络安全审计常用方法：了解网络安全审计中的访谈、检查、观察等常见方法，了解信息系统测试的常用方法。 （3）网络安全审计项目管理：了解网络安全审计计划管理的方法，了解网络安全审计质量管理的方法，了解网络安全审计风险管理的方法，了解网络安全审计档案管理的方法。
5.	网络安全审计实务

	（1）现场审计：了解网络安全审计计划的准备及编制方法，了解网络安全审计证据的获取方法，了解网络安全审计工作底稿的要求及编制方法。 （2）审计报告及后续审计：了解网络安全审计报告的编制方法，了解网络安全审计建议及跟踪验证的方式。 （3）网络安全审计实例：了解不同专项审计的要点和特性，理解 1-2 个专项审计的典型审计实例。
6.	信息系统一般控制审计 （1）信息系统总体控制审计：了解信息系统总体控制审计的目的，了解信息系统总体控制审计事项评价指标，包括战略规划、组织架构、制度体系、岗位职责、内部监督等。 （2）信息安全管理控制审计：了解信息安全管理控制审计的目的，了解信息安全管理控制审计事项评价指标，包括安全管理机构、安全管理制度、人员安全管理、系统建设安全管理、系统运维安全管理等。 （3）信息安全技术控制审计：了解信息安全技术控制审计的目的，了解信息安全技术控制审计事项评价指标，包括物理安全、网络安全、主机安全、应用安全、数据安全、信息化装备自主可控等。 （4）上机测试：了解一般控制的相关工具，掌握工具的使用方法。
7.	信息系统应用控制审计 （1）信息系统业务流程控制审计：了解信息系统业务流程控制审计的目的，了解信息系统业务流程控制审计事项评价指标，包括业务流程设计、业务流程处理、业务流程功能等。 （2）数据输入、处理和输出控制审计：了解数据输入、处理和输出控制审计的目的，了解数据输入、处理和输出控制审计事项评价指标，包括数据录入和导入控制、数据修改和删除控制、数据校验控制、数据入库控制、数据共享与交换控制、备份与恢复数据接收控制、数据转换控制、数据整理控制、数据计算控制、数据汇总控制、数据外设输出控制、数据检索输出控制、数据共享输出控制、备份与恢复输出控制等。 （3）信息共享和业务协同审计：了解信息共享和业务协同审计的目的，了解信息共享和业务协同审计事项评价指标，包括信息资源目录体系、信息资源交换体系、元数据和主数据、数据元素和数据库表、内部数据和外部数据、信息资源标准化等。
8.	信息化项目管理审计 （1）信息系统建设经济性审计：了解信息系统建设经济性审计的目的，了解信息系统建设经济性审计事项评价指标，包括信息系统规划经济性、信息系统建设经济性、信息系统应用经济性、信息系统运维经济性等。 （2）信息系统建设管理审计：了解信息系统建设管理审计的目的，了解信息系统建设管理审计事项评价指标，包括项目审批管理、项目建设管理、项目资金管理、项目监督管理、项目验收管理、项目运行管理等。 （3）信息系统绩效审计：了解信息系统绩效审计的目的，了解信息系统绩效审计事项评价指标，包括信息系统总体绩效、管理决策支持能力的绩效、信息资源共享能力的绩效、经济业务协同能力的绩效、系统建设发展能力的绩效、信息系统贡献能力的绩效等。

序号	渗透测试方向考试科目和范围
1.	信息安全保障人员基本素质 （1）职业素养：深刻理解从事信息安全保障工作必备的职业素养、特殊责任。 （2）知识结构：理解信息安全保障工作所需基础知识结构，深刻理解信息安全保障本质含义。 （3）工作技能：理解从事信息安全保障工作所需的基本技能、信息安全保障工作的特殊困难。
2.	信息安全意识教育 （1）信息安全保障概念：了解信息安全发展历程，理解通信保密、网络安全、信息安全、信息安全保障等概念，准确理解信息安全属性，掌握什么时候需要分别考虑信息安全属性。 （2）信息安全形势：了解国内外信息安全形势、最新的典型信息安全问题、应对典型信息安全问题的方法。 （3）信息安全需求识别：了解形势发展的需要，理解社会责任的需求、组织业务保障的需要，了解现实信息技术环境的需求，指导如何提出实际需要，了解法律法规的要求、客户合同的要求、强制标准的要求、风险评估的要求、日常保障的要求、新技术和新措施应用的要求。
3.	信息安全法律法规体系 （1）法律法规结构体系：了解我国信息安全法律法规结构、基本分类。 （2）国内外信息安全法律法规建设概况：了解中国、美国及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：了解国外信息安全标准化相关机构以及相互关系，如 ISO、IEC、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，了解我国信息安全标准相关组织及其关系，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，了解 ISO、IEC 和 ITU 信息安全相关标准建设情况，了解美国特有的信息安全相关标准建设情况，了解我国信息安全相关标准建设情况。 （4）我国信息安全管理概况：了解我国信息安全相关管理机构、管理模式、主要的信息安全管理手段。 （5）典型信息安全法律法规：了解刑法中与信息安全相关的条款，了解《保守国家秘密法》、《商用密码管理条例》，了解我国互联网相关管理规定、信息安全产品相关管理规定。
4.	通信技术基础 （1）通信的基本概念：理解通信的本质含义及电信概念、通信网络形成过程，了解通信网络结构、通信网络中的安全属性、通信网络应用分类、“网络”习惯分类、通信网络安全问题本质成因。 （2）通信协议及应用：熟悉 OSI 七层模型、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、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。
5.	渗透测试基础 （1）渗透测试基本概念：了解渗透测试的具体定义、流程、测试思路。

	（2）掌握《网络安全法》《数据安全法》等法规与渗透测试职业道德规范，掌握渗透测试授权书必须包含的条款，掌握测试过程中发现敏感数据时的处理流程； （3）了解 web 服务器运作原理及 web 应用常见的编码方式； （4）了解 HTTP 等常见的网络协议及其报文结构、请求、状态码等。
6.	信息收集 （1）掌握常见信息收集方法和工具的使用，例如 Nmap、搜索引擎、Github 等； （2）掌握域名信息收集的方法、工具和手段等； （3）了解协议栈指纹识别原理、内外网 IP 划分等；
7.	漏洞原理 （1）掌握常见漏洞扫描及漏洞利用工具的使用，了解工具所针对的漏洞类型、能够写出 payload 构造逻辑； （2）掌握注入类漏洞基本原理：例如从回显注入、报错注入到布尔盲注和时间盲注的逐字节猜解逻辑。管道符（|）、逻辑符（&&）在不同操作系统（Windows/Linux）下的闭合绕过技巧； （3）掌握跨站脚本（XSS）漏洞基本原理：反射型、存储型、DOM 型的区别；针对现代浏览器 SameSite Cookie 属性的绕过思路；内容安全策略（CSP）的防护原理等； （4）掌握认证与会话管理漏洞基本原理：JWT（JSON Web Token）篡改攻击；验证码的重放攻击与识别码爆破防御逻辑； （5）掌握业务逻辑漏洞基本原理：越权（水平/垂直越权）、支付金额篡改（负值交易）、竞争条件（并发抢购）、密码找回流程的步骤绕过等； （6）掌握文件上传漏洞基本原理：前端与后端校验的区别；图片马原理；.htaccess 和 user.ini 的利用场景等。
8.	内网渗透与横向移动 （1）了解权限提升常用方法及原理：Windows 系统的 UAC（用户账户控制）绕过机制；Linux 的 SUID 提权（如 find 命令）和脏牛（Dirty Cow）漏洞原理； （2）了解横向移动常用方法及原理：哈希传递攻击（Pass The Hash）的原理；如何通过 NTLM Relay 攻击域控；内网中如何通过 ARP 欺骗或 DNS 投毒进行流量劫持； （3）了解隧道技术原理：DNS 隧道和 ICMP 隧道用于出网通信的原理；正向代理与反向代理的区别及适用场景。

附录 J：参考文献

[1] GB/T 20261-2020 信息安全技术 系统安全工程 能力成熟度模型

[2] GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

[3] YD/T 1621-2007 网络与信息安全服务资质评价准则

[4] YD/T 2252-2011 网络与信息安全风险评估服务能力评价方法

[5] RB/T 201-2013 信息系统安全集成服务资质认证评价要求