

				(2)设备监测数据分析
		3-3 网络安全事件响应	10	(1)常见网络安全事件响应
				(2)常见网络攻击溯源和上报
				(3)留存网络安全事件相关证据记录
4. 培训指导	10	4-1 培训实施	5	(1)制订培训工作计划
				(2)编制和实施培训方案
				(3)编写培训教材、讲义、课件
				(4)培训宣讲
		4-2 技术指导	5	(1)技能指导
			(2)技能水平考核	

2.3.7 二级/技师职业技能培训操作技能考核规范（网络安全管理员）

考核范围	考核比重 (%)	考核内容	考核比重 (%)	考核形式	选考方法	考核时间 (分钟)	重要程度
1. 网络与信息安全防护	40	1-1 网络安全防护	15	操作	必考	15	X
		1-2 系统安全防护	15	操作	必考	15	X
		1-3 应用安全防护	10	操作	必考	15	X
2. 网络与信息安全管理	30	2-1 网络安全等级保护	15	操作	必考	15	X
		2-2 应用安全评估	15	操作	必考	15	X
3. 网络与信息安全处置	30	3-1 网络安全事件监测	10	操作	必考	15	X
		3-2 网络安全事件分析	10	操作	必考	15	X
		3-3 网络安全事件	10	操作	必考	15	X

		响应					
合计	100	-	100	-	-	120	-

2.3.8 二级/技师职业技能培训理论知识考核规范（信息安全管理员）

模块	考核比重(%)	考核内容	考核比重 (%)	考核单元
1. 网络与信息安全防护	30	1-1 信息资产安全防护	10	(1)信息资产分类分级
				(2)安全域资源防护策略制定
		1-2 数据安全防护	10	(1) 数据安全存储策略、数据加密策略配置
				(2)制定数据容灾策略
		1-3 互联网信息安全防护	10	(1)重要信息脆弱性评估及防护
				(2)员工个人信息安全策略配置
2. 网络与信息安全管理	30	2-1 数据安全 管理	15	(1) 数据在存储、通信中的公私钥和证书管理
				(2) 数据高可用管理
				(3) 重要数据保护
		2-2 互联网信息安全管理	15	(1)履行信息安全管理义务
				(2)编制个人敏感信息安全保护技术方案
				(3)个人敏感信息脆弱性评估及防护
3. 网络与信息 安全处置	30	3-1 信息安全事件监测	10	(1)监测信息破坏事件
				(2)监测信息内容安全事件
				(3)监测其他信息安全事件
		3-2 信息安全事件分析	10	(1)信息安全监测数据清洗、汇总
				(2)信息安全监测数据分析
		3-3 信息安全事件响应	10	(1)常见信息安全事件响应
(2)常见信息安全事件溯源和上报				
(3)留存信息安全事件相关证据记录				

4. 培训指导	10	4-1 培训实施	5	(1)制订培训工作计划
				(2)编制和实施培训方案
				(3)编写培训教材、讲义、课件
				(4)培训宣讲
	4-2 技术指导	5	(1)技能指导	
			(2)技能水平考核	

2.3.9 二级/技师职业技能培训操作技能考核规范（信息安全管理员）

考核范围	考核比重 (%)	考核内容	考核比重 (%)	考核形式	选考方法	考核时间 (分钟)	重要程度
1. 网络与信息安全防护	40	1-1 信息资产安全防护	15	操作	必考	15	X
		1-2 数据安全防护	15	操作	必考	15	X
		1-3 互联网信息安全防护	10	操作	必考	15	X
2. 网络与信息安全 管理	30	2-1 数据安全 管理	15	操作	必考	15	X
		2-2 互联网信息 安全管理	15	操作	必考	15	X
3. 网络与信息安全 处置	30	3-1 信息安全事件 监测	10	操作	必考	15	X
		3-2 信息安全事件 分析	10	操作	必考	15	X
		3-3 信息安全事件 响应	10	操作	必考	15	X
合计	100	-	100	-	-	120	-

2.3.10 一级/高级技师职业技能培训理论知识考核规范（网络安全管理员）

模块	考核比重(%)	考核内容	考核比重 (%)	考核单元
1. 网络与信息安全防护	30	1-1 网络安全风险评估	15	(1)组织整体业务系统安全风险评估
				(2)网络和应用系统渗透测试及漏洞验证和修补
		1-2 新技术、新应用安全防护	15	(1)云计算应用安全防护策略
				(2)物联网应用安全防护策略
				(3)移动互联应用安全防护策略
				(4)工业控制系统安全防护策略
2. 网络与信息安全管理	30	2-1 网络安全风险管理	10	(1)网络安全风险管理
				(2)漏洞评估及制定安全管理措施
2-2 网络安全等级保护	10	2-2 网络安全等级保护	10	(1)网络安全等级保护定级
				(2)网络安全等级保护备案
				(3)网络安全等级保护建设整改
				(4)网络安全自我监督检查
2-3 关键信息基础设施保护	10	2-3 关键信息基础设施保护	10	(1)关键信息基础设施安全检查
				(2)制定关键信息基础设施安全加固方案
				(3)网络安全事件应急预案编制
3. 网络与信息安全处置	30	3-1 网络安全事件预警	10	(1)建立安全事件威胁预警机制
				(2)网络安全事件风险定级、设计响应级别和

				应急预案
		3-2 网络安全事件证据保存	10	(1)静态数据提取及固定 (2)动态易失数据提取及固定
		3-3 网络安全事件应急响应	10	(1)复杂网络安全事件应急响应 (2)恢复网络安全事件造成的网络或系统损坏
4. 培训指导	10	4-1 培训实施	5	(1) 培训需求分析
				(2) 编制培训规划
				(3) 组织编写培训教材、讲义、教案
				(4) 进行培训宣讲
		4-2 技术指导	5	(1) 技能指导
				(2) 技能水平考核
(3) 组织开展技术改造、技术革新活动				

2.3.11 一级/高级技师职业技能培训操作技能考核规范（网络安全管理员）

考核范围	考核比重 (%)	考核内容	考核比重 (%)	考核形式	选考方法	考核时间 (分钟)	重要程度
1. 网络与信息安全防护	40	1-1 网络安全风险评估	20	操作	必考	15	X
		1-2 新技术、新应用安全防护	20	操作	必考	15	X
2. 网络与信息安全 管理	30	2-1 网络安全风险管理	10	操作	必考	15	X
		2-2 网络安全等级保护	10	操作	必考	15	X
		2-3 关键信息基础设施保护	10	操作	必考	15	X

3. 网络与信息安全处置	30	3-1 网络安全事件预警	10	操作	必考	15	X
		3-2 网络安全事件证据保存	10	操作	必考	15	X
		3-3 网络安全事件应急响应	10	操作	必考	15	X
合计	100	-	100	-	-	120	-

2.3.12 一级/高级技师职业技能培训理论知识考核规范（信息安全管理员）

模块	考核比重(%)	考核内容	考核比重 (%)	考核单元
1. 网络与信息安全防护	30	1-1 信息安全风险评估	15	(1)组织关键业务系统风险评估
				(2)出具信息安全风险评估报告
				(3)制定信息安全风险整改措施
		1-2 新技术、新应用安全防护	15	(1)云计算应用安全防护策略
				(2)物联网应用安全防护策略
				(3)移动互联应用安全防护策略
2. 网络与信息安全风险管理	30	2-1 信息安全风险管理	10	(4)工业控制系统安全防护策略
				(5)大数据应用安全防护策略
				(6)区块链等其他新技术新应用安全防护策略
2-2 网络安全等级保护	10	10	(1)制定信息安全风险管理制度	
			(2)制定风险评估方案	
2-2 网络安全等级保护	10	10	10	(3)业务系统安全风险处置方案编制
				(1)网络安全等级保护定级
				(2)网络安全等级保护备案

				(3)设计和制定安全管理制度
		2-3 关键信息基础设施保护	10	(1)关键信息基础设施相关数据安全保护要求 (2)关键信息基础设施安全检查支持
3. 网络与信息安全处置	30	3-1 信息安全事件预警	10	(1)信息安全事件威胁预警
				(2)信息安全事件风险定级
		3-2 信息安全事件证据保存	10	(1)静态数据提取及固定
				(2)动态易失数据提取及固定
3-3 信息安全事件应急响应	10	(1)响应并处理复杂信息安全事件		
		(2)恢复信息安全事件造成的信息损坏		
4. 培训指导	10	4-1 培训实施	5	(1)对培训需求进行分析
				(2)编制培训规划
				(3)组织编写培训教材、讲义、教案
				(4)进行培训宣讲
		4-2 技术指导	5	(1)技能指导
				(2)技能水平考核
(3)组织开展技术改造、技术革新活动				

2.3.13 一级/高级技师职业技能培训操作技能考核规范（信息安全管理员）

考核范围	考核比重 (%)	考核内容	考核比重 (%)	考核形式	选考方法	考核时间 (分钟)	重要程度
1. 网络与信息安全防护	40	1-1 信息安全风险评估	20	操作	必考	15	X
		1-2 新技术、新应用安全防护	20	操作	必考	15	X
2. 网络与	30	2-1 信息	10	操作	必考	15	X

信息安全 管理		安全风险 管理					
		2-2 网络 安全等级 保护	10	操作	必考	15	X
		2-3 关键 信息基础 设施保护	10	操作	必考	15	X
3. 网络与 信息安全 处置	30	3-1 信息 安全事件 预警	10	操作	必考	15	X
		3-2 信息 安全事件 证据保存	10	操作	必考	15	X
		3-3 信息 安全事件 应急响应	10	操作	必考	15	X
合计	100	-	100	-	-	120	-