|  |  |
| --- | --- |
| **内部资料 注意保管** | |
| **项目编号** | — — |
| **合同编号** | — — |

**{{varPlatName}}**

**系统安全等级测评方案**

|  |  |
| --- | --- |
| **项目名称：** | {{varPlatName}}网络安全等级保护测评项目 |
| **测评单位：** | 内蒙古信元网络安全技术股份有限公司 |
| **编制时间：** | 2021年X月 |

|  |  |  |  |
| --- | --- | --- | --- |
| **测评文档基本信息** | | | |
| **文档名称** | {{varPlatName}}信息系统安全等级测评方案 | | |
| **编制单位** | 内蒙古信元网络安全技术股份有限公司 | | |
| **编 制 人** |  | | |
| **审 阅 人** |  | | |
| **提交日期** |  | | |
| **测评文档确认信息** | | | |
| **确 认 人** |  | **日期** |  |
| **单位/部门** |  | | |

目 录

[目 录 1](#_Toc26798786)

[1 概述 1](#_Toc26798787)

[1.1 项目简介 1](#_Toc26798788)

[1.2 测评依据 1](#_Toc26798789)

[2 被测信息系统情况 2](#_Toc26798790)

[2.1 定级情况 2](#_Toc26798791)

[2.2 承载的业务情况 2](#_Toc26798792)

[2.3 网络结构 2](#_Toc26798793)

[2.4 信息系统构成 2](#_Toc26798794)

[2.4.1 物理机房 2](#_Toc26798795)

[2.4.2 网络设备 2](#_Toc26798796)

[2.4.3 安全设备 2](#_Toc26798797)

[2.4.4 服务器或存储设备 3](#_Toc26798798)

[2.4.5 终端或现场设备 3](#_Toc26798799)

[2.4.6 系统管理软件或平台 3](#_Toc26798800)

[2.4.7 业务应用系统或平台 3](#_Toc26798801)

[2.4.8 关键数据类型 3](#_Toc26798802)

[2.4.9 安全相关人员 4](#_Toc26798803)

[2.4.10 安全管理文档 4](#_Toc26798804)

[3 测评范围与方法 5](#_Toc26798805)

[3.1 测评指标 5](#_Toc26798806)

[3.1.1 安全通用要求指标 5](#_Toc26798807)

[3.1.2 安全扩展要求指标 8](#_Toc26798808)

[3.2 测评对象 10](#_Toc26798809)

[3.2.1 测评对象选择方法 10](#_Toc26798810)

[3.2.2 测评对象选择结果 10](#_Toc26798811)

[3.3 测评方法 13](#_Toc26798812)

[3.3.1 访谈 13](#_Toc26798813)

[3.3.2 检查 13](#_Toc26798814)

[3.3.3 测试 14](#_Toc26798815)

[4 单项测评内容 15](#_Toc26798816)

[4.1 基础环境安全测评 15](#_Toc26798817)

[4.1.1 安全物理环境测评 15](#_Toc26798818)

[4.1.2 安全通信网络测评 16](#_Toc26798819)

[4.1.3 安全区域边界测评 16](#_Toc26798820)

[4.1.4 安全计算环境测评 17](#_Toc26798821)

[4.1.5 安全管理中心测评 18](#_Toc26798822)

[4.1.6 安全管理制度测评 18](#_Toc26798823)

[4.1.7 安全管理机构测评 19](#_Toc26798824)

[4.1.8 安全管理人员测评 19](#_Toc26798825)

[4.1.9 安全建设管理测评 20](#_Toc26798826)

[4.1.10 安全运维管理测评 20](#_Toc26798827)

[4.2 云计算安全测评 21](#_Toc26798828)

[4.2.1 安全物理环境 21](#_Toc26798829)

[4.2.2 安全通信网络 21](#_Toc26798830)

[4.2.3 安全区域边界 22](#_Toc26798831)

[4.2.4 安全计算环境 22](#_Toc26798832)

[4.2.5 安全管理中心 23](#_Toc26798833)

[4.2.6 安全建设管理 23](#_Toc26798834)

[4.2.7 安全运维管理 23](#_Toc26798835)

[4.3 移动互联安全测评 23](#_Toc26798836)

[4.3.1 安全物理环境 24](#_Toc26798837)

[4.3.2 安全区域边界 24](#_Toc26798838)

[4.3.3 安全计算环境 24](#_Toc26798839)

[4.3.4 安全建设管理 24](#_Toc26798840)

[4.3.5 安全运维管理 25](#_Toc26798841)

[4.4 工业控制系统安全测评 25](#_Toc26798842)

[4.4.1 安全物理环境 25](#_Toc26798843)

[4.4.2 安全通信网络 25](#_Toc26798844)

[4.4.3 安全区域边界 26](#_Toc26798845)

[4.4.4 安全计算环境 26](#_Toc26798846)

[4.4.5 安全建设管理 27](#_Toc26798847)

[4.5 大数据安全测评 27](#_Toc26798848)

[4.5.1 安全物理环境 27](#_Toc26798849)

[4.5.2 安全通信网络 27](#_Toc26798850)

[4.5.3 安全计算环境 28](#_Toc26798851)

[4.5.4 安全建设管理 28](#_Toc26798852)

[4.5.5 安全运维管理 29](#_Toc26798853)

[5 工具测试 30](#_Toc26798854)

[5.1 测评工具 30](#_Toc26798855)

[5.2 风险和规避措施 30](#_Toc26798856)

[5.2.1 操作系统和常见应用漏洞扫描 30](#_Toc26798857)

[5.2.2 WEB应用漏洞扫描 31](#_Toc26798858)

[5.3 工具测试接入点说明 32](#_Toc26798859)

[5.4 渗透测试说明 33](#_Toc26798861)

[6 系统整体测评内容 36](#_Toc26798862)

[6.1 层面间安全测评 36](#_Toc26798863)

[6.2 区域间安全测评 36](#_Toc26798864)

[6.3 系统结构安全测评 36](#_Toc26798865)

[7 配合资源需求 38](#_Toc26798866)

[7.1 办公场所 38](#_Toc26798867)

[7.2 配合人员 38](#_Toc26798868)

[7.3 文档资料 38](#_Toc26798869)

[7.4 办公用品 40](#_Toc26798870)

[7.5 网络接入 40](#_Toc26798871)

[7.6 安全权限 40](#_Toc26798872)

# 概述

## 项目简介

为落实相关文件要求，{{varorganName}}委托内蒙古信元网络安全技术股份有限公司对{{varPlatName}}系统实施安全等级测评。通过测评来评判目前该信息系统安全保护的程度或水平与国家信息系统安全等级保护要求之间的差距，用以指导开展信息系统安全方面的调整和改进。

## 测评依据

测评过程中主要依据的标准：

1) GB 17859-1999 《计算机信息系统 安全保护等级划分准则》

2) GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》

3) GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

4) GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

5) GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

# 被测信息系统情况

## 定级情况

表2‑1系统定级情况表

| **序号** | **系统名称** | **系统安全保护等级** | **业务信息安全等级** | **系统服务安全等级** |
| --- | --- | --- | --- | --- |
| 1 | {{varPlatName}} | {{G}} | {{S}} | {{A}} |

## 承载的业务情况

{{varDescribe}}

## 网络结构

该系统已托管{{cloudPlatName}}，网络安全由{{cloudPlatName}}负责。

## 信息系统构成

### 物理机房

表2‑2物理机房基本情况表

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
| 该系统已托管{{cloudPlatName}}，物理机房由{{cloudPlatName}}负责。 | | | |

### 网络设备

表 2‑3 网络设备基本情况表

| **序号** | **所属定级系统** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **IP地址** | **数量** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 该系统已托管{{cloudPlatName}}，网络设备由{{cloudPlatName}}负责。 | | | | | | | | | |

### 安全设备

表 2‑4 安全设备基本情况表

| **序号** | **所属定级系统** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **IP地址** | **数量** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 该系统已托管{{cloudPlatName}}，安全设备由{{cloudPlatName}}负责。 | | | | | | | | | |

### 服务器或存储设备

表 2‑5服务器或存储设备基本情况表

| **{{hosts}}序号** | **所属定级系统** | **设备名称** | **所属业务应用系统/平台名称** | **是否虚拟设备** | **物理/逻辑区域** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **数量** | **IP地址** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [index] | [platName] | [hostName] | [appSystemName] | [isVMhost] | [area] | [osName] | [dataOSname] | [bitName] | [amount] | [ipAddr] | [hostDegree] |

### 终端或现场设备

表 2‑6 终端或现场设备基本情况表

| **{{terminal}}序号** | **所属定级系统** | **设备名称** | **是否为虚拟设备** | **物理/逻辑区域** | **操作系统/控制软件及版本** | **设备类别/用途** | **数量** | **IP地址** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [tindex] | [tplatName] | [tdeviceName] | [tisVMhost] | [tosName] | [tmodel] | [tdescribe] | [tamount] | [tipAddr] | [tDegree] |

### 系统管理软件或平台

表 2‑7系统管理软件或平台基本情况表

| **序号** | **所属定级系统** | **系统软件软件/平台名称** | **主要功能** | **版本** | **所在设备名称** | **IP地址** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 无 |  |  |  |  |  |  |

### 业务应用系统或平台

表 2‑8业务应用系统或平台基本情况表

| **{{app}}序号** | **所属定级系统** | **业务应用系统/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- |
| [aindex] | [aplatName] | [appName] | [aFunction] | [aVersion] | [aDevelopName] | [aDegree] |

### 关键数据类型

表 2‑9 关键数据类型基本情况表

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** | **重要程度** |
| --- | --- | --- | --- | --- |
| 1 | 重要鉴别数据 | {{varPlatName}} | 完整性，保密性 | 关键 |
| 2 | 重要管理数据 | {{varPlatName}} | 完整性，保密性 | 关键 |
| 3 | 重要业务数据 | {{varPlatName}} | 完整性，保密性 | 关键 |

### 安全相关人员

表 2‑10 安全相关人员基本情况表

| **{{job}}序号** | **姓名** | **岗位角色** | **联系方式** |
| --- | --- | --- | --- |
| [jindex] | [jName] | [jobName] | [jphone] |

### 安全相关人员

表 2‑11 安全管理文档基本情况表

| **{{doc}}序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| [dindex] | [documenName] | [details] |

# 测评范围与方法

《基本要求》中对不同等级信息系统的安全功能和措施作出具体要求，信息安全等级测评要根据信息系统的等级从中选取相应等级的安全测评指标，并根据《测评要求》的要求，对信息系统实施安全现状测评。因此，本次测评将根据信息系统的等级选取相应级别的测评指标。

## 测评指标

### 安全通用要求指标

依据定级结果，{{varPlatName}}系统的安全测评指标应包括《基本要求》第7节“第{{G}}级基本要求”中的{{G}}级通用指标类（G{{G}}），{{S}}级业务信息安全性指标类（S{{S}}）和{{A}}级业务服务保证类（A{{A}}）。所包括的安全控制指标类型情况具体如下表：

表3‑1系统测评指标统计列表

| **安全类** | **安全控制点** | **测评项数** |
| --- | --- | --- |
| 安全计算环境 | 身份鉴别 | 4 |
| 访问控制 | 7 |
| 安全审计 | 4 |
| 入侵防范 | 6 |
| 恶意代码防范 | 1 |
| 可信验证 | 1 |
| 数据完整性 | 2 |
| 数据保密性 | 2 |
| 数据备份恢复 | 3 |
| 剩余信息保护 | 2 |
| 个人信息保护 | 2 |
| 安全管理中心 | 系统管理 | 2 |
| 审计管理 | 2 |
| 安全管理 | 2 |
| 集中管控 | 6 |
| 安全管理制度 | 安全策略 | 1 |
| 管理制度 | 3 |
| 制定和发布 | 2 |
| 评审和修订 | 1 |
| 安全管理机构 | 岗位设置 | 3 |
| 人员配备 | 2 |
| 授权和审批 | 3 |
| 沟通和合作 | 3 |
| 审核和检查 | 3 |
| 安全管理人员 | 人员录用 | 3 |
| 人员离岗 | 2 |
| 安全意识教育和培训 | 3 |
| 外部人员访问管理 | 4 |
| 安全建设管理 | 定级和备案 | 4 |
| 安全方案设计 | 3 |
| 产品采购和使用 | 3 |
| 自行软件开发 | 7 |
| 外包软件开发 | 3 |
| 工程实施 | 3 |
| 测试验收 | 2 |
| 系统交付 | 3 |
| 等级测评 | 3 |
| 服务供应商选择 | 3 |
| 安全运维管理 | 环境管理 | 3 |
| 资产管理 | 3 |
| 介质管理 | 2 |
| 设备维护管理 | 4 |
| 漏洞和风险管理 | 2 |
| 网络和系统安全管理 | 10 |
| 恶意代码防范管理 | 2 |
| 配置管理 | 2 |
| 密码管理 | 2 |
| 变更管理 | 3 |
| 备份与恢复管理 | 3 |
| 安全事件处置 | 4 |
| 应急预案管理 | 4 |
| 外包运维管理 | 4 |

### 安全扩展要求指标

表3‑2安全扩展要求指标列表

| **扩展类型** | **安全类** | **安全控制点** | **测评项数** |
| --- | --- | --- | --- |
| 云计算安全扩展要求 | 安全计算环境 | 剩余信息保护 | 2 |
| 访问控制 | 2 |
| 数据完整性和保密性 | 4 |
| 入侵防范 | 3 |
| 镜像和快照保护 | 3 |
| 身份鉴别 | 1 |
| 数据备份恢复 | 4 |
| 云计算安全扩展要求 | 安全管理中心 | 集中管控 | 4 |
| 云计算安全扩展要求 | 安全建设管理 | 云服务商选择 | 5 |
| 供应链管理 | 3 |
| 云计算安全扩展要求 | 安全运维管理 | 云计算环境管理 | 1 |

## 测评对象

### 测评对象选择方法

测评对象包括网络互联与安全设备操作系统、应用软件系统、主机操作系统、数据库管理系统、安全相关人员、机房、介质以及管理文档。选择过程中综合考虑了信息系统的安全保护等级、业务应用特点和对象所在具体设备的重要情况等要素，并兼顾了工作投入与结果产出两者的平衡关系。

### 测评对象选择结果

#### 物理机房

表3‑3测评对象-物理机房列表

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
| 该系统已托管{{cloudPlatName}}，物理机房由{{cloudPlatName}}负责，本次测评不涉及。 | | | |

#### 网络设备

表3‑4测评对象-网络设备列表

| **序号** | **所属定级系统** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **IP地址** | **数量** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 该系统已托管{{cloudPlatName}}，网络设备由{{cloudPlatName}}负责，本次测评不涉及。 | | | | | | | | | |

#### 安全设备

表3‑5测评对象-安全设备列表

| **序号** | **所属定级系统** | **设备名称** | **是否虚拟设备** | **系统及版本** | **品牌及型号** | **用途** | **IP地址** | **数量** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 该系统已托管{{cloudPlatName}}，安全设备由{{cloudPlatName}}负责，本次测评不涉及。 | | | | | | | | | |

#### 服务器或存储设备

表3‑6测评对象-服务器或存储设备列表

| **{{hostsb}}序号** | **所属定级系统** | **设备名称** | **所属业务应用系统/平台名称** | **是否虚拟设备** | **物理/逻辑区域** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **数量** | **IP地址** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [index] | [platName] | [hostName] | [appSystemName] | [isVMhost] | [area] | [osName] | [dataOSname] | [bitName] | [amount] | [ipAddr] | [hostDegree] |

#### 终端或现场设备

表3‑7测评对象-终端或现场设备列表

| **{{terminalb}}序号** | **所属定级系统** | **设备名称** | **是否为虚拟设备** | **物理/逻辑区域** | **操作系统/控制软件及版本** | **设备类别/用途** | **数量** | **IP地址** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [tindex] | [tplatName] | [tdeviceName] | [tisVMhost] | [tosName] | [tmodel] | [tdescribe] | [tamount] | [tipAddr] | [tDegree] |

#### 系统管理软件或平台

表3‑8测评对象-系统管理软件或平台列表

| **序号** | **所属定级系统** | **系统软件软件/平台名称** | **主要功能** | **版本** | **所在设备名称** | **IP地址** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 无 |  |  |  |  |  |  |

#### 业务应用系统或平台

表3‑9测评对象-业务应用系统或平台列表

| **{{app}}序号** | **所属定级系统** | **业务应用系统/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- |
| [aindex] | [aplatName] | [appName] | [aFunction] | [aVersion] | [aDevelopName] | [aDegree] |

#### 关键数据类型

表3‑10测评对象-关键数据类型列表

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** | **重要程度** |
| --- | --- | --- | --- | --- |
| 1 | 重要鉴别数据 | {{varPlatName}} | 完整性，保密性 | 关键 |
| 2 | 重要管理数据 | {{varPlatName}} | 完整性，保密性 | 关键 |
| 3 | 重要业务数据 | {{varPlatName}} | 完整性，保密性 | 关键 |

#### 安全相关人员

表3‑11测评对象-安全相关人员列表

| **{{job}}序号** | **姓名** | **岗位角色** | **联系方式** |
| --- | --- | --- | --- |
| [jindex] | [jName] | [jobName] | [jphone] |

#### 安全管理文档

表3‑12测评对象-安全管理文档列表

| **{{doc}}序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| [dindex] | [documenName] | [details] |

## 测评方法

本次等级测评现场实施过程中将综合采用访谈、检查和测试等测评方法。

### 访谈

访谈是指测评人员通过与被测系统有关人员（个人/群体）进行交流、询问等活动，获取证据以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，访谈方法主要应用于安全管理机构测评、人员安全管理测评、系统建设管理测评和系统运维管理测评等安全管理类测评任务中。

在安全管理类测评任务中，测评人员依据定制的测评指导书（访谈问题列表）对相关人员进行访谈，获取与安全管理有关的评估证据用于判断特定的安全管理措施是否符合国家相关标准以及委托方的实际需求。

### 核查

核查是指测评人员通过对评估对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，检查方法的应用范围覆盖了物理、主机、网络、应用和数据等技术类测评任务，以及安全管理类测评任务。

在物理安全测评任务中，测评人员采用文档查阅与分析和现场观察等检查方法来获取测评证据（如机房的温湿度情况），用于判断目标系统在机房安全方面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。

在主机、网络、应用和数据等测评任务中，测评人员综合采用文档查阅与分析、安全配置核查和网络监听与分析等检查方法来获取测评证据（如相关措施的部署和配置情况，特定设备的端口开放情况等），用于判断目标系统在主机、网络和应用层面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。

在安全管理类测评任务中，测评人员主要采用文档查阅与分析的检查方法来获取测评证据（如制度文件的编制情况），用于判断特定的安全管理措施是否符合国家、行业相关标准的要求以及委托方的实际需求。

### 测试

测试是指评估人员使用预定的方法/工具使评估对象产生特定的行为，通过查看、分析这些行为的结果，获取证据以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，测试方法主要应用在手工验证、漏洞扫描、渗透测试等测评任务中。

在网络安全、主机安全和应用安全等测评任务中，测评人员将综合采用手工验证和工具测试（如漏洞扫描、渗透测试等）方法对特定安全技术措施的有效性进行测试，测试结果用于判断目标系统在网络、主机或应用层面采用的特定技术措施是否符合国家相关标准以及委托方的实际需求，并进一步应用于对目标系统进行安全性整体分析。

# 单项测评内容

## 基础环境安全测评

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。具体分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

### 安全物理环境测评

安全物理环境测评中，测评人员将以文档查阅与分析和现场观测等检查方法为主，访谈为辅来获取测评证据（如机房的温湿度情况），用于评测机房的安全保护能力。

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

安全物理环境测评实施过程涉及10个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-1安全物理环境测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 物理位置选择 | 通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
|  | 物理访问控制 | 通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
|  | 防盗窃和防破坏 | 通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
|  | 防雷击 | 通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
|  | 防火 | 通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
|  | 防水和防潮 | 通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
|  | 防静电 | 通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。 |
|  | 温湿度控制 | 通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。 |
|  | 电力供应 | 通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。 |
|  | 电磁防护 | 通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |

### 安全通信网络测评

安全通信网络测评中，测评人员将以配置核查和文档查阅为主，访谈和分析为辅来获取证据（如相关措施的部署和配置情况），用于测评信息系统的网络安全保护。

安全通信网络测评涉及的测评对象主要为网络设备和安全。

安全通信网络测评实施过程涉及3个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-2安全通信网络测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 网络架构 | 测评分析网络架构与网段划分、隔离等情况的合理性和有效性。 |
|  | 通信传输 | 测评通信过程中的完整性、保密性等。。 |
|  | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |

### 安全区域边界测评

安全区域边界测评主要涉及边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证6个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-3安全通信网络测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 边界防护 | 测评分析信息系统网络边界安全防护的状况。 |
|  | 访问控制 | 测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。 |
|  | 入侵防范 | 测评分析信息系统对攻击行为的识别和处理情况。 |
|  | 恶意代码和垃圾邮件防范 | 测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮件的防护情况。 |
|  | 安全审计 | 测评分析信息系统审计配置和审计记录保护情况。 |
|  | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |

### 安全计算环境测评

安全计算环境测评主要涉及身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护11个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-4安全计算环境测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 身份鉴别 | 检查服务器的身份标识与鉴别和用户登录的配置情况。 |
|  | 访问控制 | 检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。 |
|  | 安全审计 | 检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。 |
|  | 入侵防范 | 检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 |
|  | 恶意代码防范 | 检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。 |
|  | 可信验证 | 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。 |
|  | 数据完整性 | 测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。 |
|  | 数据保密性 | 测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。 |
|  | 数据备份恢复 | 测评信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。 |
|  | 剩余信息保护 | 测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。 |
|  | 个人信息保护 | 测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。 |

### 安全管理中心测评

安全管理中心测评主要涉及系统管理、审计管理、安全管理、集中管控4个方

面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-5安全管理中心测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 系统管理 | 测评信息系统的系统管理员对系统的管理情况。 |
|  | 审计管理 | 测评信息系统的安全审计员对系统的审计情况。 |
|  | 安全管理 | 测评信息系统的安全管理员对系统的安全策略的配置情况。 |
|  | 集中管控 | 测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。 |

### 安全管理制度测评

安全管理制度测评主要涉及安全策略、管理制度、制定和发布、评审和修订4个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-6安全管理制度测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 安全策略 | 测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。 |
|  | 管理制度 | 测评信息系统管理制度在内容覆盖上是否全面、完善。 |
|  | 制定和发布 | 测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 |
|  | 评审和修订 | 测评信息系统管理制度定期评审和修订情况。 |

### 安全管理机构测评

安全管理机构测评主要涉及岗位设置、人员配备、授权和审批、沟通与合作、审核和检查5个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-7安全管理机构测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 岗位设置 | 测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。 |
|  | 人员配备 | 测评信息系统各个岗位人员配备情况。 |
|  | 授权和审批 | 测评信息系统对关键活动的授权和审批情况。 |
|  | 沟通与合作 | 测评信息系统内部部门间、与外部单位间的沟通与合作情况。 |
|  | 审核和检查 | 检查信息系统安全工作的审核和测评情况。 |

### 安全管理人员测评

安全管理人员测评主要涉及人员录用、人员离岗、安全意识教育和培训、外部人员访问管理4个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-8安全管理人员测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 人员录用 | 测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
|  | 人员离岗 | 测评信息系统人员离岗时是否按照一定的手续办理。 |
|  | 安全意识教育和培训 | 测评是否对人员进行安全方面的教育和培训。 |
|  | 外部人员访问管理 | 测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |

### 安全建设管理测评

安全建设管理测评主要涉及定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择10个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-9安全建设管理测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 定级和备案 | 测评是否按照一定要求确定系统的安全等级并完成备案工作。 |
|  | 安全方案设计 | 测评系统整体的安全规划设计是否按照一定流程进行。 |
|  | 产品采购和使用 | 测评是否按照一定的要求进行系统的产品采购。 |
|  | 自行软件开发 | 测评自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
|  | 外包软件开发 | 测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。 |
|  | 工程实施 | 测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
|  | 测试验收 | 测评系统运行前是否对其进行测试验收工作。 |
|  | 系统交付 | 测评是否采取必要的措施对系统交付过程进行有效控制。 |
|  | 等级测评 | 测评是否依据国家要求完成等级测评和整改工作。 |
|  | 服务供应商选择 | 测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

### 安全运维管理测评

安全运维管理测评主要涉及环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理14个方面的安全保护能力，具体测评指标描述如下表所示：

表4‑1-10安全运维管理测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 环境管理 | 测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。 |
|  | 资产管理 | 测评是否采取必要的措施对系统的资产进行分类标识管理。 |
|  | 介质管理 | 测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
|  | 设备维护管理 | 测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
|  | 漏洞和风险管理 | 测评是否采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补。测评是否定期开展安全测评。 |
|  | 网络和系统安全管理 | 测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。 |
|  | 恶意代码防范管理 | 测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。 |
|  | 配置管理 | 测评是否记录和保存系统的基本配置信息。 |
|  | 密码管理 | 测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
|  | 变更管理 | 测评是否采取必要的措施对系统发生的变更进行有效管理。 |
|  | 备份与恢复管理 | 测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
|  | 安全事件处置 | 测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。 |
|  | 应急预案管理 | 测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |
|  | 外包运维管理 | 测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。 |

## 云计算安全测评

### 安全计算环境

安全计算环境测评主要关注身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份和恢复、剩余信息保护,具体测评指标描述如下表所示:

表4‑2-4安全计算环境测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 身份鉴别 | 测评虚拟机、数据系统、网络设备和安全设备的身份鉴别能力。包括口令安全策略、身份鉴别机机制等。 |
|  | 访问控制 | 测评虚拟机、数据库系统、网络设备和安全设备的访问控制设置情况，包括安全策略、控制粒度以及权限设置情况等。 |
|  | 入侵防范 | 测评分析对虚拟机在运行过程中的隔离失效、异常访问的检测、告警能力，对虚拟机的迁移范围进行限制。 |
|  | 镜像和快照保护 | 测评虚拟机镜像和快照完整性、保密性和安全性。 |
|  | 数据完整性和保密性 | 测评虚拟机迁移过程的鉴别信息和用户数据在传输过程中的完整性保护情况。 |
|  | 数据备份和恢复 | 测评云租户重要数据的本地备份、存储位置，应用系统的可移植性等。 |
|  | 剩余信息保护 | 测评虚拟机的存储空间，被释放或再分配给其他用户前得到完全清除。 |

### 安全管理中心

安全管理中心测评主要关注集中管控,具体测评指标描述如下表所示:

表4‑2-5安全管理中心测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 集中管控 | 测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。 |

### 安全建设管理

安全建设管理测评主要关注云服务商选择、供应链选择,具体测评指标描述如下表所示:

表4‑2-6安全建设管理测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 云服务商选择 | 测评是否选择符合有关规定的云服务商。 |
|  | 供应链管理 | 测评供应链安全事件信息、重要变更或威胁信息是否及时传达到云租户。 |

### 安全运维管理

安全建设运维管理测评主要关注云计算环境管理,具体测评指标描述如下表所示:

表4‑2-7安全运维管理测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 云计算环境管理 | 云计算平台的运维地点位于中国境内，境外对境内云计算平台实施运维操作应遵循国家有关规定。 |

## 移动互联安全测评

### 安全物理环境

安全物理环境测评主要关注无线接入点的物理位置,具体测评指标描述如下表所示:

表4‑2-1安全物理环境测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 无线接入点的物理位置 | 测评无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。 |

### 安全区域边界

安全区域边界测评主要关注边界防护、访问控制、入侵防范,具体测评指标描述如下表所示:

表4‑3-2安全区域边界测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 边界防护 | 测评有线网络与无线网络边界之间的访问和数据流是否是通过无线接入网关设备。 |
|  | 访问控制 | 测评无线接入设备是否开启接入认证功能，并支持采用认证服务器认证或国家密码管理局批准的密码模块进行认证。 |
|  | 入侵防范 | 测评分析无线接入设备对攻击行为的识别和处理情况。 |

### 安全计算环境

安全计算环境测评主要关注移动终端管控、移动应用管控,具体测评指标描述如下表所示:

表4‑3-3安全计算环境测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 移动终端管控 | 测评移动终端安装、注册并运行终端管理客户端软件,移动终端并接受管理服务端的设备生命周期及设备远程控制。 |
|  | 移动应用管控 | 测评应用软件安装是否只允许指定证书签名的应用软件安装和运行,是否具有白名单功能。 |

### 安全建设管理

安全建设管理测评主要关注移动应用软件采购、移动应用软件开发,具体测评指标描述如下表所示:

表4‑3-4安全建设管理测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 移动应用软件采购 | 测评移动终端软件是否来自可靠分发渠道或者使用可靠证书签名,应用软件是否由指定开发者开发。 |
|  | 移动应用软件开发 | 测评是否对业务应用软件开发者进行资格审查,签名证书的合法性。 |

### 安全运维管理

安全运维管理测评主要配置管理,具体测评指标描述如下表所示:

表4‑3-5安全运维管理测评指标描述

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 配置管理 | 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。 |

# 工具测试

## 测评工具

主要使用到的测评工具有：漏洞扫描工具、渗透测试工具集。具体描述如下表：

表5‑1测试工具列表

| **序号** | **工具用途分类** | **具体描述** |
| --- | --- | --- |
| 1 | 系统层漏洞检测 | 绿盟远程安全评估系统。 |
| 2 | 应用层漏洞检测 | 绿盟远程安全评估系统。 |
| 3 | 渗透测试工具集 | 包含缓冲区溢出利用、口令破解、注入验证等。 |

## 风险和规避措施

### 操作系统和常见应用漏洞扫描

在使用扫描器对目标系统扫描的过程中，可能会出现以下的风险：

1. 占用带宽（风险不高）。
2. 进程、系统崩溃。由于目标系统的多样性及脆弱性，或是目标系统上某些特殊服务本身存在的缺陷，对扫描器发送的探测包或者渗透测试工具发出的测试数据不能正常响应，可能会出现系统崩溃或程序进程的崩溃。
3. 登录界面锁死。扫描器可以对某些常用应用程序（系统登录、FTP，Telnet，SNMP，SSH，WebLogic）的登录口令进行弱口令猜测验证，如果目标系统对登录失败次数进行了限制，尝试登录次数超过限定次数系统可能会锁死登录界面。

风险规避方法：

1. 根据目标系统的网络、应用状况，调整扫描测试时间段，采取避峰扫描。
2. 对扫描器扫描策略进行配置，适当调整扫描器的并发任务数和扫描的强度，可使减少扫描器工作时占用的带宽，降低对目标系统影响。
3. 根据目标系统及目标系统上运行的应用程序，通过与测评委托方相关人员协商，定制针对本系统测试的扫描插件、端口等配置，尽量合理设置扫描强度，降低目标系统或进程崩溃的风险。
4. 如目标系统对登录某些相关程序的尝试次数进行了限制，在进行扫描时，可屏蔽暴力猜解功能，以避免登录界面锁死的情况发生。

### WEB应用漏洞扫描

在使用WEB应用漏洞扫描器对目标系统扫描的过程中，可能会存在以下的风险：

1. 占用带宽（风险不高）。
2. 登录界面锁死。WEB应用漏洞扫描会对登录页面进行弱口令猜测，猜测过程可能会造成应用系统某些帐号锁死。

风险规避方法：

1. 根据目标系统的网络、应用状况，调整扫描测试时间段，采取避峰扫描。
2. 如目标系统对登录某些相关程序的尝试次数进行了限制，在进行扫描时，可屏蔽暴力猜解功能，以避免登录界面锁死的情况发生。

### 渗透测试

为保障客户系统在渗透测试过程中稳定、安全的运转，我们将从以下多种方式来进行风险规避:

1）对象选择

为更大程度的避免风险的产生，渗透测试还可选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

2）时间控制

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

3）技术手段

信元网安的渗透测试人员具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

4）监控措施

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

5）工具使用

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

## 工具测试接入点说明

### 漏洞扫描工具接入点

为了发挥测评工具的作用，达到测评的目的，各种测评工具需要接入到被测评的信息系统网络多处，并需要配置恰当的网络IP地址。测试工具接入到网络不同接入点后，在该点需要执行的具体操作详见工具测试作业指导书。

针对{{varPlatName}}信息系统的网络结构情况 ，需要在系统及其边界中设置1个测试工具接入点--接入点至接入点，如图所示。“接入点”标注表示进行工具测试时，需要从该网络设备上接入，对应的箭头路线表示工具测试数据的主要流向示意：

工具接入点拓扑图

### 漏洞扫描对象

| **{{ScanHost}}序号** | **接入点** | **设备名称** | **类型/OS** |
| --- | --- | --- | --- |
| [index] | 互联网 | [hostName] | [osName] |

## 渗透测试说明

渗透性测试安全工程师完全处于对系统一无所知的状态，通常这类测试最初信息来自于DNS、Web、Email及各种公开对外的服务器，主要是模拟来自互联网的攻击者。

### 渗透测试流程

1）信息收集：此阶段中，信元网安测试人员进行必要的信息收集，如 IP 地址、DNS 记录、软件版本信息、IP 段、Google中的公开信息等。

2）渗透测试：此阶段中，信元网安测试人员根据第一阶段获得的信息对网络、系统进行渗透测试。此阶段如果成功的话，可能获得普通权限。

3）缺陷利用：此阶段中，信元网安测试人员尝试由普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行。

4）成果收集：此阶段中，信元网安测试人员对前期收集的各类弱点、漏洞等问题进行分类整理，集中展示。

5）威胁分析：此阶段中，信元网安测试人员对发现的上述问题进行威胁分类和分析其影响。

6）输出报告：此阶段中，信元网安测试人员根据测试和分析的结果编写直观的渗透测试服务报告。

### 渗透测试工具接入点

为了发挥测评工具的作用，达到测评的目的，渗透测试工具需要接入到被测评的信息系统网络中，并需要配置恰当的网络IP地址。

针对{{varPlatName}}信息系统 的网络结构情况 ，需要在系统及其边界中设置0个测试工具接入点--接入点至接入点，如图所示。“接入点”标注表示进行工具测试时，需要从该网络设备上接入，对应的箭头路线表示工具测试数据的主要流向示意：

渗透工具接入点拓扑图

### 渗透测试对象

| **{{PenetraApp}}序号** | **接入点** | **设备名称** | **类型/OS** |
| --- | --- | --- | --- |
| [aindex] | 互联网 | [appName] | [architecture] |

# 系统整体测评内容

信息系统的安全控制集成到信息系统后，会在层面内、层面间和区域间产生连接、交互、依赖、协同等相互关联关系，使信息系统的整体安全功能与信息系统的结构密切相关，在整体上呈现出一种集成特性。这些集成特性在安全控制的工作单元中是没有完全体现。因此，在安全控制测评的基础上，有必要对集成系统和运行环境进行整体测评。

## 层面间安全测评

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。例如，网络层面、主机系统层面与安全管理的系统运维管理之间关系密切，应关注他们之间的关联互补作用。

## 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域

## 系统结构安全测评

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。从信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等基础上，结合不同位置上可能面临的威胁、可能暴露的脆弱性等，综合判定信息系统的整体布局是否合理、整体是否安全有效等。

在检查信息系统安全保护措施的具体实现方式和部署情况后，结合其业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范是否恰当合理。

# 配合资源需求

测评组分为网络、主机、应用、管理、扫描等工作小组。测评现场需要被测单位提供办公场所、配合人员、文档资料、办公用品、网络接入、安全权限等相关资源。

## 办公场所

测评组需要相对独立的办公环境，可以容纳5-10人。

## 配合人员

表7‑1人员配合需求表

| **序号** | **配合人员** | **配合需求** | **人员数量（人）** |
| --- | --- | --- | --- |
| 1 | 总体协调人员 | 协调网络、主机、应用、安全管理、机房管理等方面的相关人员配合测评。 | 1 |
| 2 | 网络管理人员 | 熟悉系统的网络架构、网络设备、安全设备、网络管理平台部署等情况，配合网络测评人员完成网络测评，在漏洞扫描期间监控系统网络的运行状态。 | 2 |
| 3 | 系统管理人员 | 熟悉系统中各类主机的操作系统、数据库系统、数据备份等情况，配合主机和数据库测评人员完成主机和数据库的测评，在漏洞扫描期间监控相关主机和数据库的运行状态。 | 2 |
| 4 | 应用开发或系统运维人员 | 熟悉各类应用部署、配置和管理等情况，配合应用测评人员完成应用测评，在漏洞扫描期间监控相关业务应用的运行状态。 | 1 |
| 5 | 机房管理人员 | 负责机房管理，现场配合物理环境测评人员完成物理安全测评。 | 1 |
| 6 | 安全文档管理人员 | 配合安全管测评人员完成管理测评工作。 | 1 |

## 文档资料

表7‑2文档资料需求表

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
| 1 | 机构总体安全方针和政策方面的管理制度 |  |
| 2 | 部门设置、岗位设置及工作职责定义方面的管理制度 |  |
| 3 | 授权审批、审批流程等方面的管理制度 |  |
| 4 | 安全审核和安全检查方面的管理制度 |  |
| 5 | 管理制度、操作规程修订、维护方面的管理制度 |  |
| 6 | 人员录用、离岗、考核等方面的管理制度 |  |
| 7 | 人员安全教育和培训方面的管理制度 |  |
| 8 | 第三方人员访问控制方面的管理制度 |  |
| 9 | 工程实施过程管理方面的管理制度 |  |
| 10 | 产品选型、采购方面的管理制度 |  |
| 11 | 软件外包开发或自我开发方面的管理制度 |  |
| 12 | 测试、验收方面的管理制度 |  |
| 13 | 机房安全管理方面的管理制度 |  |
| 14 | 办公环境安全管理方面的管理制度 |  |
| 15 | 资产、设备、介质安全管理方面的管理制度 |  |
| 16 | 信息分类、标识、发布、使用方面的管理制度 |  |
| 17 | 配套设施、软硬件维护方面的管理制度 |  |
| 18 | 网络安全管理（网络配置、帐号管理等）方面的管理制度 |  |
| 19 | 系统安全管理（系统配置、帐号管理等）方面的管理制度 |  |
| 20 | 系统监控、风险评估、漏洞扫描方面的管理制度 |  |
| 21 | 病毒防范方面的管理制度 |  |
| 22 | 系统变更控制方面的管理制度 |  |
| 23 | 密码管理方面的管理制度 |  |
| 24 | 备份和恢复方面的管理制度 |  |
| 25 | 安全事件报告和处置方面的管理制度 |  |
| 26 | 应急响应方法、应急响应计划等方面的文件 |  |
| 27 | 各类相关记录、表单 |  |

## 办公用品

表7‑3办公用品需求表

| **序号** | **用品名称** | **用品数量** |
| --- | --- | --- |
| 1 | 打印机 | 一台 |
| 2 | 打印纸 | 一包 |
| 3 | 带锁的文件柜 | 一个 |
| 4 | 电源接线插座 | 若干 |

## 网络接入

表7‑4网络接入需求表

| **序号** | **接入类别** | **接入位置** | **具体需求** |
| --- | --- | --- | --- |
| 1 | 工具测试接入 | 被测系统网络范围内，具体接入点参见5.3 工具测试接入点说明 | 对于每个接入点可用以太网电口方式接入，并分配合规的IP地址。 |
| 2 | 互联网接入 | 测评组所在办公场所 | 无 |

## 安全权限

表7‑5安全权限需求表

| **序号** | **安全权限需求** |
| --- | --- |
| 1 | 机房访问权限用于物理环境测评、网络测评、主机测评、数据库测评、工具测试。 |
| 2 | 应用访问权限用于应用测评、工具测试。 |
| 3 | 设备接入权限用于工具测试。 |

【全文结束】