**记录编号：P2021XXXXX-GF01**

**AAAAA**

**BBBBB**

**等级保护测评方案**

|  |  |
| --- | --- |
| **被测对象：** | **BBBBB** |
| **被测单位：** | **AAAAA** |
| **测评单位：** | **上海计算机软件技术开发中心** |
| **发布日期：** | **2021年　X　月　X日** |

**文档版本历史表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **作者** | **操作** | **日期** | **说明** |
| V1.0 | XXX | 新建 | 2021-X-X |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**文档审核记录表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **审核人** | **审核人签字** | **审核日期** | **说明** |
| V1.0 | XXX |  | 2021-X-X |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

[1. 概述 1](#_Toc78095376)

[1.1 项目简介 1](#_Toc78095377)

[1.2 测评依据 1](#_Toc78095378)

[2. 被测对象描述 1](#_Toc78095379)

[2.1 承载的业务情况 1](#_Toc78095380)

[2.2 定级情况 2](#_Toc78095381)

[2.3 网络结构 3](#_Toc78095382)

[2.4 系统构成 3](#_Toc78095383)

[2.4.1 物理机房 3](#_Toc78095384)

[2.4.2 网络设备 3](#_Toc78095385)

[2.4.3 安全设备 4](#_Toc78095386)

[2.4.4 服务器/存储设备 4](#_Toc78095387)

[2.4.5 终端/现场设备 4](#_Toc78095388)

[2.4.6 系统管理软件/平台 4](#_Toc78095389)

[2.4.7 业务应用系统/平台 4](#_Toc78095390)

[2.4.8 数据资源 5](#_Toc78095391)

[2.4.9 安全相关人员 5](#_Toc78095392)

[2.4.10 安全管理文档 5](#_Toc78095393)

[2.5 安全服务 6](#_Toc78095394)

[3. 测评对象与指标 6](#_Toc78095395)

[3.1 测评指标 6](#_Toc78095396)

[3.1.1 安全通用要求指标 7](#_Toc78095397)

[3.1.2 安全扩展要求指标 9](#_Toc78095398)

[3.1.3 其他安全要求指标 14](#_Toc78095399)

[3.2 测评对象 14](#_Toc78095400)

[3.2.1 测评对象选择方法 14](#_Toc78095401)

[3.2.2 测评对象选择结果 16](#_Toc78095402)

[3.3 现场测评时间安排 20](#_Toc78095403)

[4. 测评方法与工具 22](#_Toc78095404)

[4.1 测评方法 22](#_Toc78095405)

[4.2 主要测评工具 22](#_Toc78095406)

[5. 测评内容与实施 23](#_Toc78095407)

[5.1 通用安全要求 23](#_Toc78095408)

[5.1.1 安全物理环境测评 23](#_Toc78095409)

[5.1.2 安全通信网络测评 26](#_Toc78095410)

[5.1.3 安全区域边界测评 28](#_Toc78095411)

[5.1.4 安全计算环境测评 30](#_Toc78095412)

[5.1.5 安全管理中心测评 34](#_Toc78095413)

[5.1.6 安全管理制度测评 36](#_Toc78095414)

[5.1.7 安全管理机构测评 38](#_Toc78095415)

[5.1.8 安全管理人员测评 40](#_Toc78095416)

[5.1.9 安全建设管理测评 42](#_Toc78095417)

[5.1.10 安全运维管理测评 45](#_Toc78095418)

[5.2 云计算安全测评扩展要求 50](#_Toc78095419)

[5.2.1 安全物理环境测评 50](#_Toc78095420)

[5.2.2 安全通信网络测评 51](#_Toc78095421)

[5.2.3 安全区域边界测评 52](#_Toc78095422)

[5.2.4 安全计算环境测评 53](#_Toc78095423)

[5.2.5 安全管理中心测评 56](#_Toc78095424)

[5.2.6 安全建设管理测评 56](#_Toc78095425)

[5.2.7 安全运维管理测评 58](#_Toc78095426)

[5.3 移动互联安全测评扩展要求 58](#_Toc78095427)

[5.3.1 安全物理环境测评 58](#_Toc78095428)

[5.3.2 安全区域边界测评 59](#_Toc78095429)

[5.3.3 安全计算环境测评 60](#_Toc78095430)

[5.3.4 安全建设管理测评 61](#_Toc78095431)

[5.3.5 安全运维管理测评 62](#_Toc78095432)

[5.4 物联网安全测评扩展要求 62](#_Toc78095433)

[5.4.1 安全物理环境测评 62](#_Toc78095434)

[5.4.2 安全区域边界测评 63](#_Toc78095435)

[5.4.3 安全计算环境测评 64](#_Toc78095436)

[5.4.4 安全运维管理测评 65](#_Toc78095437)

[5.5 工业控制系统安全测评扩展要求 66](#_Toc78095438)

[5.5.1 安全物理环境测评 66](#_Toc78095439)

[5.5.2 安全通信网络测评 66](#_Toc78095440)

[5.5.3 安全区域边界测评 67](#_Toc78095441)

[5.5.4 安全计算环境测评 68](#_Toc78095442)

[5.5.5 安全建设管理测评 70](#_Toc78095443)

[5.6 大数据可参考安全评估方法 70](#_Toc78095444)

[5.6.1 安全物理环境测评 70](#_Toc78095445)

[5.6.2 安全通信网络测评 71](#_Toc78095446)

[5.6.3 安全计算环境测评 71](#_Toc78095447)

[5.6.4 安全建设管理测评 73](#_Toc78095448)

[5.6.5 安全运维管理测评 74](#_Toc78095449)

[5.7 工具测试 75](#_Toc78095450)

[5.8 测评风险及应对措施 76](#_Toc78095451)

[5.9 整体测评 77](#_Toc78095452)

[等级保护测评方案用户确认 81](#_Toc78095453)

# 概述

## 项目简介

被测对象情况描述（必须包括被测对象责任主体、业务描述、网络拓扑描述）。

上海计算机软件技术开发中心受AAAAA委托，对BBBBB进行网络安全等级保护测评。本项目参照国家GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》标准，对BBBBB进行网络安全等级保护测评，以验证其是否满足GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》（第三级）S3A3G3的要求。

## 测评依据

以下标准为本次测评的主要依据标准：

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

以下标准为本次测评的参考标准：

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

GB/T 20984-2007《信息安全技术 信息安全风险评估规范》

GB 17859—1999 《计算机信息系统 安全保护等级划分准则》

# 被测对象描述

## 承载的业务情况

系统提供的服务介绍；系统存储的主要业务数据。

系统功能截图。

图2.1 xxxxx截图

图2.2 xxxxx截图

## 定级情况

系统业务信息遭到破坏后，对社会秩序和公共利益造成严重损害，即会出现：工作职能受到严重影响，业务能力严重下降且或功能无法执行，对社会秩序造成较大范围的社会不良影响，或对其他组织和个人造成较严重损害。定级为S3。

系统服务遭到破坏中断后，对社会秩序和公共利益造成严重损害，即会出现：工作职能受到严重影响，业务能力严重下降且或功能无法执行，对社会秩序造成较大范围的社会不良影响，对其他组织和个人造成较严重损害。定级为A3。

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定BBBBB安全保护等级为第三级（S3A3G3）。

## 网络结构

添加系统网络架构图

图2.5 网络拓扑

网络架构图说明。

## 系统构成

### 物理机房

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
|  |  |  |  |

### 网络设备

| **序号** | **设备名称** | **虚拟设备** | **系统及版本** | **品牌**  **型号** | **用途** | **重要**  **程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### 安全设备

| **序号** | **设备名称** | **虚拟设备** | **系统及版本** | **品牌型号** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### 服务器/存储设备

| **序号** | **设备名称** | **所属业务应用系统/平台名称** | **虚拟设备** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

### 终端/现场设备

| **序号** | **设备名称** | **虚拟设备** | **操作系统/控制软件及版本** | **设备类别/用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 系统管理软件/平台

| **序号** | **管理软件/平台名称** | **所在设备名称** | **版本** | **主要功能** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 业务应用系统/平台

| **序号** | **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** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### 数据资源

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| --- | --- | --- | --- |
|  | 鉴别数据 |  | 保密性、完整性 |
|  | 重要业务数据 |  | 保密性、完整性 |
|  | 重要审计数据 |  | 保密性、完整性 |
|  | 重要配置数据 |  | 保密性、完整性 |
|  | 重要个人信息 |  | 保密性、完整性 |

### 安全相关人员

| **序号** | **姓名** | **岗位/角色** | **联系方式** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 安全管理文档

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
|  |  | 机构总体安全方针和政策方面的管理制度 |
|  |  | 部门设置、岗位设置及工作职责定义方面的管理制度 |
|  |  | 授权审批、审批流程等方面的管理制度 |
|  |  | 安全审批和安全检查方面的管理制度 |
|  |  | 管理制度、操作规程修订、维护方面的管理制度 |
|  |  | 人员录用、离岗、考核等方面的管理制度 |
|  |  | 人员安全教育和培训方面的管理制度 |
|  |  | 人员沟通合作方面的管理制度 |
|  |  | 第三方人员访问控制方面的管理制度 |
|  |  | 工程实施过程管理方面的管理制度 |
|  |  | 产品选型、采购方面的管理制度 |
|  |  | 软件外包开发或自我开发方面的管理制度 |
|  |  | 测试、验收、交付方面的管理制度 |
|  |  | 机房安全管理方面的管理制度 |
|  |  | 办公环境安全管理方面的管理制度 |
|  |  | 资产、设备、介质安全管理方面的管理制度 |
|  |  | 配置设施、软硬件维护方面的管理制度 |
|  |  | 网络安全管理（网络配置、帐号管理等）方面的管理制度 |
|  |  | 系统安全管理（系统配置、帐号管理等）方面的管理制度 |
|  |  | 系统监控、风险评估、漏洞扫描方面的管理制度 |
|  |  | 病毒防范方面的管理制度 |
|  |  | 系统变更控制方面的管理制度 |
|  |  | 备份和恢复方面的管理制度 |
|  |  | 安全事件报告和处置方面的管理制度 |

## 安全服务

| **序号** | **安全服务名称[[1]](#footnote-1)** | **安全服务商** |
| --- | --- | --- |
|  | 安全测评 | 上海计算机软件技术开发中心 |

# 测评对象与指标

## 测评指标

根据被测对象定级情况，从GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中选择与被测对象的保护等级相对应的基本要求作为测评指标。下表为GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中的测评指标。

### 安全通用要求指标

| 安全通用要求测评指标类（GB/T 22239-2019） | | | | | |
| --- | --- | --- | --- | --- | --- |
| 技术/管理 | 安全层面 | 类数量 | | | |
| S3 | A3 | G3 | 小计 |
| 技术要求 | 安全物理环境 | 1 | 1 | 8 | 10 |
| 安全通信网络 | 1 | 0 | 2 | 3 |
| 安全区域边界 | 1 | 0 | 5 | 6 |
| 安全计算环境 | 7 | 1 | 3 | 11 |
| 安全管理中心 | 0 | 0 | 4 | 4 |
| 管理要求 | 安全管理制度 | N/A | | 4 | 4 |
| 安全管理机构 | 5 | 5 |
| 安全管理人员 | 4 | 4 |
| 安全建设管理 | 10 | 10 |
| 安全运维管理 | 14 | 14 |
| 合计（S3A3G3） | | | | | 71（类） |

## 测评对象

### 测评对象选择方法

测评对象是等级测评的直接工作对象，也是在被测对象中实现特定测评指标所对应的安全功能的具体系统组件。因此，选择测评对象是编制测评方案的必要步骤，也是整个测评工作的重要环节。恰当选择测评对象的种类和数量是整个等级测评工作能够获取足够证据、了解到被测对象的真实安全保护状况的重要保证。

依据GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》确定本次测评对象。本次测评对象采用抽查的方法，即抽查信息系统中具有代表性的组件作为测评对象，并且在测评对象确定任务中应兼顾工作投入与结果产出两者的平衡关系。在确定测评对象时，除了考虑资产的重要程度以外，还应遵循以下原则：

1. 恰当性：选择的设备、软件系统等满足相应等级的测评强度要求；

2. 重要性：抽查对被测对象来说重要的服务器、数据库和网络设备等；

3. 安全性：抽查对外暴露的网络边界；

4. 共享性：抽查共享设备和数据交换平台/设备；

5. 代表性：抽查尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统类型。

针对所测信息系统的保护等级，测评对象的选取原则可参照下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 保护等级  测评对象 | 第一级 | 第二级 | 第三级 | 第四级 |
| 机房 | 主机房 | 主机房 | 主机房  部分辅机房 | 主机房  全部辅机房 |
| 介质存放环境 | -- | 存储重要数据介质的存放环境 | 存储重要数据介质的存放环境 | 介质的存放环境 |
| 办公场地 | -- | -- | 办公场地 | 办公场地 |
| 网络架构 | 整个系统 | 整个系统 | 整个系统 | 整个系统 |
| 安全设备 | 防火墙、入侵检测设备、防病毒网关等 | 防火墙、入侵检测设备、防病毒网关等 | 防火墙、入侵检测设备、防病毒网关等 | 防火墙、入侵检测设备、防病毒网关等 |
| 边界网络设备 | 路由器、防火墙、认证网关等 | 路由器、防火墙、认证网关等 | 路由器、防火墙、认证网关、边界接入设备（如楼层交换机）等 | 路由器、防火墙、认证网关、边界接入设备（如楼层交换机）等 |
| 网络互联设备 | 对整个系统的安全性起决定作用的网络设备，如核心交换机、路由器 | 对整个系统或其局部的安全性起决定作用的网络设备，如核心交换机、汇聚层交换机、核心路由器 | 对整个系统或其局部的安全性起决定作用的网络设备，如核心交换机、汇聚层交换机、路由器 | 主要网络互联设备，包括核心和汇聚层交换机 |
| 主机 | 承载核心业务或数据的服务器（操作系统和数据库） | 承载核心或重要业务、数据的服务器（操作系统和数据库）  重要管理终端 | 承载主要业务、数据的服务器（操作系统和数据库）  管理终端  主要业务应用系统终端 | 主要服务器（操作系统和数据库）  管理终端  主要业务应用系统终端 |
| 应用系统 | 核心业务应用系统 | 核心、主要业务应用系统 | 能够完成不同业务使命的业务应用系统  业务备份系统 | 全部应用系统  业务备份系统 |
| 安全人员 | 主管人员 | 主管人员  各方面的负责人员 | 主管人员  各方面的负责人员  具体负责安全管理的当事人  业务负责人 | 主管人员  各方面的负责人员  具体负责安全管理的当事人  业务负责人 |
| 管理制度 | 主要管理制度和记录 | 所有管理制度和记录 | 所有管理制度和记录 | 所有管理制度和记录 |
| 相同配置的设备数量 | 至少1台 | 至少2台 | 至少2台 | 至少3台 |

### 测评对象选择结果

#### 物理机房

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

#### 网络设备

| **序号** | **设备名称** | **虚拟设备** | **系统及版本** | **品牌**  **型号** | **用途** | **重要**  **程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

#### 安全设备

| **序号** | **设备名称** | **虚拟**  **设备** | **系统**  **及版本** | **品牌**  **型号** | **用途** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### 服务器/存储设备

| **序号** | **设备名称** | **所属业务应用系统/平台名称** | **虚拟设备** | **操作系统**  **及版本** | **数据库管理系统及版本** | **中间件及版本** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

#### 终端/现场设备

| **序号** | **设备名称** | **虚拟**  **设备** | **操作系统/**  **控制软件及版本** | **设备类别/用途** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

#### 系统管理软件/平台

| **序号** | **管理软件/平台名称** | **所在设备名称** | **版本** | **主要功能** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### 业务应用系统/平台

| **序号** | **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** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

#### 数据资源

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| --- | --- | --- | --- |
|  | 鉴别数据 |  | 保密性、完整性 |
|  | 重要业务数据 |  | 保密性、完整性 |
|  | 重要审计数据 |  | 保密性、完整性 |
|  | 重要配置数据 |  | 保密性、完整性 |
|  | 重要个人信息 |  | 保密性、完整性 |

#### 安全相关人员

| **序号** | **姓名** | **岗位/角色** | **联系方式** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### 安全管理文档

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
|  |  | 机构总体安全方针和政策方面的管理制度 |
|  |  | 部门设置、岗位设置及工作职责定义方面的管理制度 |
|  |  | 授权审批、审批流程等方面的管理制度 |
|  |  | 安全审批和安全检查方面的管理制度 |
|  |  | 管理制度、操作规程修订、维护方面的管理制度 |
|  |  | 人员录用、离岗、考核等方面的管理制度 |
|  |  | 人员安全教育和培训方面的管理制度 |
|  |  | 人员沟通合作方面的管理制度 |
|  |  | 第三方人员访问控制方面的管理制度 |
|  |  | 工程实施过程管理方面的管理制度 |
|  |  | 产品选型、采购方面的管理制度 |
|  |  | 软件外包开发或自我开发方面的管理制度 |
|  |  | 测试、验收、交付方面的管理制度 |
|  |  | 机房安全管理方面的管理制度 |
|  |  | 办公环境安全管理方面的管理制度 |
|  |  | 资产、设备、介质安全管理方面的管理制度 |
|  |  | 配置设施、软硬件维护方面的管理制度 |
|  |  | 网络安全管理（网络配置、帐号管理等）方面的管理制度 |
|  |  | 系统安全管理（系统配置、帐号管理等）方面的管理制度 |
|  |  | 系统监控、风险评估、漏洞扫描方面的管理制度 |
|  |  | 病毒防范方面的管理制度 |
|  |  | 系统变更控制方面的管理制度 |
|  |  | 备份和恢复方面的管理制度 |
|  |  | 安全事件报告和处置方面的管理制度 |

## 现场测评时间安排

| **序号** | **日期** | **时间** | **测评内容** | **测评方法** | **配合人员** |
| --- | --- | --- | --- | --- | --- |
|  | 2021.X.X | 9:30-17:00 | 安全管理制度测评 | 现场查看安全管理制度及管理执行记录文件 | 安全管理员 |
| 9:30-12:00 | 安全通信网络测评 | 查看网络拓扑、边界防护等基本防护措施、三防措施等 | 网络管理员 |
| 13:30-17:00 | 安全计算环境测评 | 检查网络设备、安全设备的策略配置情况 | 网络管理员 |
|  | 2021.X.X | 9:30-17:00 | 安全管理机构测评 | 现场查看安全管理机构相关制度 | 安全管理员 |
| 9:30-17:00 | 安全计算环境测评 | 检查服务器、数据库、终端等操作系统的安全配置情况 | 系统管理员 |
| 9:30-17:00 | 安全扫描 | 对主机进行漏洞扫描 | 系统管理员 |
|  | 2021.X.X | 9:30-17:00 | 安全管理人员测评 | 现场查看安全管理人员相关制度 | 安全管理员 |
| 12：30-17：00 | 安全物理环境检查 | 现场查看机房、办公环境的人员访问和环境管理情况 | 安全管理员 |
|  | 2021.X.X | 9:30-17:00 | 安全建设管理测评 | 现场查看安全建设管理相关制度 | 安全管理员 |
| 9:30-17:00 | 安全管理中心测评 | 检查安全管理中心配置情况 | 安全管理员 |
|  | 2021.X.X | 12:30-17:00 | 安全扫描 | 对系统进行漏洞扫描、对应用系统进行渗透性测试 | 应用管理员、网络管理员 |
| 12:30-17:00 | 安全运维管理测评 | 现场查看安全运维管理相关制度、文件 | 系统管理员 |
|  | 2021.X.X | 9:30-17:00 | 测评中待确认项以及证据类文档检查（主要针对管理制度） | 访谈/检查 |  |
| 9:30-17:00 | 现场测评问题汇总 | 整理现场测评情况 |  |
| 14:30-17:00 | 现场测评问题汇总 | 末次会议 | 项目所有相关人员 |

# 测评方法与工具

## 测评方法

根据网络安全等级保护测评准则，现场测评的方法包括检查、访谈和测试等三类，在此基础上进行综合风险分析。

 访谈是测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取证据以证明网络安全等级保护措施是否有效的一种方法。访谈对象涉及安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心和安全管理等方面的内容。

 检查不同于行政执法意义上的监督检查，是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明网络安全等级保护措施是否有效的一种方法。检查包括文档核查和配置核查两种，涉及安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心和安全管理等方面的内容。

 测试是测评人员通过对测评对象按照预定的方法/工具使其产生特定的行为等活动，查看、分析输出结果，获取证据以证明网络安全等级保护措施是否有效的一种方法。测试对象主要涉及安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心和安全管理等方面的内容。

 通过访谈相关安全管理人员、检查配置、规章制度、日常记录、漏洞扫描等手段，结合文件检查和现场核查进行测评。

 风险评估过程包含资产识别与赋值、脆弱性评估、威胁评估、现有的安全控制措施评估、风险评价等过程。

## 主要测评工具

本次测评使用以下测试工具，表格中的测评工具版本为目前的最新版本，实际测试前将更新版本到最新，采用最新版本进行测试。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **工具名称** | **厂商** | **系统版本** | **漏洞库版本** |
|  | 绿盟远程安全评估系统RSAS | 北京神州绿盟信息安全科技股份有限公司 |  |  |
|  | Nessus professional | Tenable Network Security |  |  |
|  | 明鉴Web应用弱点扫描器 | 杭州安恒信息技术股份有限公司 |  |  |
|  | Webray | 盛邦安全 |  |  |
|  | 渗透测试工具集V1.0 | 开源 | -- | -- |

表格中的软件版本为工具当前的最新版本，在测试前更新版本到最新。

# 测评内容与实施

## 通用安全要求

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

* + - 1. **测评内容**

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； |
|  | b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 |
|  | 物理访问控制 | a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 |
|  | 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； |
|  | b）应将通信线缆铺设在隐蔽安全处； |
|  | c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。 |
|  | 防雷击 | a）应将各类机柜、设施和设备等通过接地系统安全接地； |
|  | b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 |
|  | 防火 | a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； |
|  | b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； |
|  | c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 |
|  | 防水和防潮 | a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； |
|  | b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； |
|  | c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 |
|  | 防静电 | a）应采用防静电地板或地面并采用必要的接地防静电措施； |
|  | b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 |
|  | 温湿度控制 | a）应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 |
|  | 电力供应 | a）应在机房供电线路上配置稳压器和过电压防护设备； |
|  | b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求； |
|  | c）应设置冗余或并行的电力电缆线路为计算机系统供电。 |
|  | 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； |
|  | b）应对关键设备实施电磁屏蔽。 |

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
|  | 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； |
|  | b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 |
|  | 物理访问控制 | a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 |
|  | 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； |
|  | b）应将通信线缆铺设在隐蔽安全处。 |
|  | 防雷击 | a）应将各类机柜、设施和设备等通过接地系统安全接地。 |
|  | 防火 | a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； |
|  | b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； |
|  | 防水和防潮 | a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； |
|  | b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。 |
|  | 防静电 | a）应采用防静电地板或地面并采用必要的接地防静电措施； |
|  | 温湿度控制 | a）应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 |
|  | 电力供应 | a）应在机房供电线路上配置稳压器和过电压防护设备； |
|  | b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求； |
|  | 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； |

#### 测评实施

* 文档查阅

测评人员对测评委托方提交的安全物理环境相关文档（含制度、记录等）等进行查看和分析，并记录相关证据。

* 机房实地观测

测评人员在配合人员的陪同下对机房的安全措施进行现场观测，并记录相关证据。

* 人员访谈

测评人员根据文档查阅和实地观测的测评结果，针对部分不确定项目访谈相关安全人员，获取补充证据。

* 结果确认

测评人员向配合人员提交安全物理环境测评的初步结果记录。测评双方对初步结果进一步分析和修订后，认可形成安全物理环境测评结果记录。

#### 配合需求

| 配合项目 | 需求说明 |
| --- | --- |
| 配合人员 | 机房安全管理员，陪同测评人员出入机房，并提供相关的文档（如机房出入人员记录，精密空调等基础设施的维护记录，机房和机房所在建筑的设计竣工验收文件等） |
| 安全权限 | 测评人员在测评实施期间出入机房的许可 |
| 办公环境 | 会议室 |

### 安全通信网络测评

#### 测评内容

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 1 | 网络架构 | a）应保证网络设备的业务处理能力满足业务高峰期需要； |
| 2 | b）应保证网络各个部分的带宽满足业务高峰期需要； |
| 3 | c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； |
| 4 | d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； |
| 5 | e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。 |
| 6 | 通信传输 | a）应采用校验技术或密码技术保证通信过程中数据的完整性； |
| 7 | b）应采用密码技术保证通信过程中数据的保密性。 |
| 8 | 可信验证 | a）可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，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 1 | 网络架构 | c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； |
| 2 | d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； |
| 3 | e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。 |
| 4 | 通信传输 | a）应采用校验技术保证通信过程中数据的完整性。 |
| 5 | 可信验证 | a）可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，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |

#### 测评实施

* 安全配置核查与人工验证

由测评人员分别针对选定的网络互联和安全设备的安全保护能力提出测评要求，配合人员通过展示带宽分配、网段划分、区域隔离等方法来提供测评证据，并由测评人员进行记录。

* 访谈与分析

测评人员访谈网络运维相关人员，并对照网络拓扑图分析网络架构与带宽分配、网段划分、区域隔离情况，记录相关结果。

* 文档查阅

测评人员根据安全配置核查与访谈的测评结果，针对部分不确定项目查阅相关的安全文档，获取补充证据。

* 结果确认

测评人员向配合人员提交安全通信网络测评的初步结果记录。测评双方对初步结果进一步分析和修订后，认可形成安全通信网络测评结果记录。

#### 配合需求

| 配合项目 | 需求说明 |
| --- | --- |
| 配合人员 | 网络管理员，配合工作包括：   1. 登录网络互联/安全设备，展示带宽分配、网段划分、区域隔离等配置参数 2. 提供网络互联/安全设备的配置参数截图 3. 提供必要的文档类证据（如网络拓扑图等） |
| 安全权限 | 如目标网络互联/安全设备只能本地管理，需要测评人员具有在测评实施期间出入机房的许可 |
| 办公环境 | 如可远程管理相关网络设备，应提供可远程访问的测评环境 |

### 安全区域边界测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 边界防护 | a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； |
| b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制； |
| c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制； |
| d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 |
| 2 | 访问控制 | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； |
| b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； |
| c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； |
| d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； |
| e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 |
| 3 | 入侵防范 | a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； |
| b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为 |
| c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； |
| d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 |
| 4 | 恶意代码和垃圾邮件防范 | a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； |
| b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 |
| 5 | 安全审计 | a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |
| c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |
| d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 |
| 6 | 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护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，在检测到其可信性受到破坏后进行报警， 并将验证结果形成审计记录送至安全管理中心。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 边界防护 | a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。 |
| 2 | 访问控制 | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； |
| b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； |
| c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； |
| d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。 |
| 3 | 入侵防范 | a) 应在关键网络节点处监视网络攻击行为。 |
| 4 | 恶意代码和垃圾邮件防范 | a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。 |
| 5 | 安全审计 | a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |
| c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| 6 | 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警， 并将验证结果形成审计记录送至安全管理中心。 |

#### 测评实施

* 安全配置核查与人工验证

由测评人员分别针对选定的网络互联和安全设备的安全保护能力提出测评要求，配合人员通过展示具体配置参数或实际操作/演练（如用户登录）等方法来提供测评证据，并由测评人员进行记录。

* 工具测试与分析

将漏洞扫描工具接入选定的交换机端口，对网络设备和安全设备进行扫描，协议分析工具接入选定的交换机配置的镜像端口，进行监听和数据包捕捉，并对漏洞扫描结果和抓包结果进行初步分析，对入侵检测设备记录结果进行初步分析，记录相关结果。

* 访谈与分析

测评人员访谈网络运维相关人员，记录并验证与安全策略的符合情况。

* 文档查阅和分析

测评人员根据安全配置核查、人工验证和网络监听与分析的测评结果，针对部分不确定项目查阅相关的安全文档，获取补充证据。

* 结果确认

测评人员向配合人员提交安全区域边界的初步结果记录，测评双方对初步结果进一步分析和修订后，认可形成安全区域边界测评结果记录。

#### 配合需求

| 配合项目 | 需求说明 |
| --- | --- |
| 配合人员 | 网络管理员，配合工作包括：   1. 登录网络互联/安全设备，展示安全防护、访问控制相关配置参数 2. 提供网络互联/安全设备的配置参数截图   审计员，配合工作包括： 展示审计日志的配置和保护实施 |
| 安全权限 | 如目标网络互联/安全设备只能本地管理，需要测评人员具有在测评实施期间出入机房的许可 |
| 办公环境 | 如可远程管理相关网络设备，应提供可远程访问的测评环境 |

### 安全计算环境测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 身份鉴别 | a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |
| c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； |
| d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别， 且其中一种鉴别技术至少应使用密码技术来实现。 |
|  | 访问控制 | a) 应对登录的用户分配账户和权限； |
| b) 应重命名或删除默认账户，修改默认账户的默认口令； |
| c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在； |
| d) 应授予管理用户所需的最小权限，实现管理用户的权限分离； |
| e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； |
| f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； |
| g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 |
|  | 安全审计 | a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |
| c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |
| d) 应对审计进程进行保护，防止未经授权的中断。 |
|  | 入侵防范 | a) 应遵循最小安装的原则，仅安装需要的组件和应用程序； |
| b) 应关闭不需要的系统服务、默认共享和高危端口； |
| c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； |
| e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； |
| f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 |
|  | 恶意代码防范 | 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 |
|  | 可信验证 | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和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，在检测到其可信性受到破坏后进行报警，并将验证 结果形成审计记录送至安全管理中心。 |
|  | 数据完整性 | a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； |
| b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 |
|  | 数据保密性 | a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； |
| b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 |
|  | 数据备份恢复 | a) 应提供重要数据的本地数据备份与恢复功能； |
| b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； |
| c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。 |
|  | 剩余信息保护 | a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； |
| b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 |
|  | 个人信息保护 | a) 应仅采集和保存业务必需的用户个人信息； |
| b) 应禁止未授权访问和非法使用用户个人信息。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 身份鉴别 | a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |
| c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |
|  | 访问控制 | a) 应对登录的用户分配账户和权限； |
| b) 应重命名或删除默认账户，修改默认账户的默认口令； |
| c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在； |
| d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。 |
|  | 安全审计 | a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |
| c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
|  | 入侵防范 | a) 应遵循最小安装的原则，仅安装需要的组件和应用程序； |
| b) 应关闭不需要的系统服务、默认共享和高危端口； |
| c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； |
| e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
|  | 恶意代码防范 | 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。 |
|  | 可信验证 | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证 结果形成审计记录送至安全管理中心。 |
|  | 数据完整性 | a）应采用校验技术保证重要数据在传输过程中的完整性。 |
|  | 数据备份恢复 | a) 应提供重要数据的本地数据备份与恢复功能； |
| b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
|  | 剩余信息保护 | a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。 |
|  | 个人信息保护 | a) 应仅采集和保存业务必需的用户个人信息； |
| b) 应禁止未授权访问和非法使用用户个人信息。 |

#### 测评实施

* 安全配置核查与人工验证

由测评人员针对选定的网络互联/安全设备的安全保护能力、主机系统、应用系统提出测评要求，配合人员通过展示具体配置或实际操作/演练等方法来提供测评证据，并由测评人员进行记录。

* 工具测试与分析

将主机扫描设备连入被测主机系统所在的局域网，验证主机系统的安全配置；将抓包工具设备连入被测应用系统所在的局域网，验证应用系统的通信保密性，并对抓包结果进行分析；对检查的身份鉴别、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、个人信息保护等方面的结果进行初步分析，记录相关结果。

* 访谈与分析

与网络互联/安全设备、主机系统、应用系统相关人员进行访谈，记录并验证与安全策略的符合情况。

* 文档查阅和分析

测评人员根据安全配置核查、主机系统扫描结果、人工验证、抓包结果、现场检查的测评结果，针对不确定项，查阅相关文档，获取补充证据。

* 结果确认

测评人员向配合人员提交安全计算环境的初步结果记录，测评双方对初步结果进一步分析和修订后，认可形成安全计算环境测评结果记录。

#### 配合需求

|  |  |
| --- | --- |
| 配合项目 | 需求说明 |
| 配合人员 | 系统管理员，配合工作包括：登录主机系统，展示权限分配；提供必要的文档类证据；登录应用系统，展示权限分配；提供必要的文档类证据；提交与数据安全及备份恢复相关的文档；展示备份的结果文件；恢复备份文件，验证备份文档有效性 网络管理员，配合工作包括：登录网络互联/安全设备，展示权限分配；提供必要的文档类证据； 审计员，配合工作包括：展示审计日志的配置和保护实施 |
| 测评环境 | 允许测试设备接入被测应用系统、主机系统所在的局域网络 |
| 安全权限 | 测评人员查看网络互联/安全设备、主机系统、应用系统等的安全配置选项的许可 |

### 安全管理中心测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 系统管理 | a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； |
| b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 |
|  | 审计管理 | a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； |
| b) 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |
|  | 安全管理 | a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； |
| b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 |
|  | 集中管控 | a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； |
| b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； |
| c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； |
| d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； |
| e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； |
| f) 应能对网络中发生的各类安全事件进行识别、报警和分析。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 系统管理 | a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； |
| b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 |
|  | 审计管理 | a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； |
| b) 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |

#### 测评实施

* 安全配置核查与人工验证

由测评人员针对信息系统的安全管理中心提出测评要求，配合人员通过展示对系统的资源和运行进行配置、控制和管理等情况；对审计记录进行分析和处理等情况；对系统中的安全策略进行配置的情况；管理网段中部署集中监控、审计设备的情况。通过展示具体的配置参数、审计分析记录、集中监控模块等，来提供测评证据，并由测评人员进行记录。

* 访谈与分析

与安全管理中心相关人员进行访谈，记录并验证与安全管理中心实施符合情况。

* 文档查阅和分析

测评人员根据针对不确定项，查阅相关文档，获取补充证据。

* 结果确认

测评人员向配合人员提交安全管理中心的初步结果记录，测评双方对初步结果进一步分析和修订后，认可形成安全管理中心测评结果记录

#### 配合需求

|  |  |
| --- | --- |
| 配合项目 | 需求说明 |
| 配合人员 | 系统管理员，配合工作包括：展示对系统的资源和运行进行配置、控制和管理等情况 审计管理员，配合工作包括：展示对审计记录进行分析和处理等情况 安全管理员，配合工作包括：展示对系统中的安全策略进行配置的情况 网络管理员，配合工作包括：展示信息系统集中管控的管控情况 |
| 安全权限 | 测评人员查看系统的资源安全配置选项、审计记录分析情况、安全策略配置情况、系统集中管控等情况的许可 |

### 安全管理制度测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 安全策略 | a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 |
| 2 | 管理制度 | a) 应对安全管理活动中的各类管理内容建立安全管理制度； |
| b) 应对管理人员或操作人员执行的日常管理操作建立操作规程； |
| c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。 |
| 3 | 制定与发布 | a) 应指定或授权专门的部门或人员负责安全管理制度的制定； |
| b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。 |
| 4 | 评审和修订 | a）应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
| 1 | 安全策略 | a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 |
| 2 | 管理制度 | a) 应对安全管理活动中的各类管理内容建立安全管理制度； |
| b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。 |
| 3 | 制定与发布 | a) 应指定或授权专门的部门或人员负责安全管理制度的制定； |
| b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。 |
| 4 | 评审和修订 | a）应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 |

#### 测评实施

* 文档查阅与分析

测评人员对测评委托方提交的安全管理文档（如制度、记录等）进行查看和分析，并记录相关证据。

* 人员访谈

测评人员根据文档查阅和分析的测评结果，针对部分不确定项目访谈相关安全人员，获取补充证据。

* 结果确认

测评人员向配合人员提交安全管理制度测评的初步结果记录。测评双方对初步结果进一步分析和修订后，认可形成安全管理制度测评结果记录。

#### 配合需求

| 配合项目 | 需求说明 |
| --- | --- |
| 配合人员 | 文档管理员，提供必要的制度类、记录类等文档 |
| 安全主管 |
| 测评环境 | 会议室 |

### 安全管理机构测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 岗位设置 | a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权； |
| b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； |
| c) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 |
|  | 人员配备 | a) 应配备一定数量的系统管理员、审计管理员和安全管理员等； |
| b) 应配备专职安全管理员，不可兼任。 |
|  | 授权和审批 | a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； |
| b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； |
| c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。 |
|  | 沟通和合作 | a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； |
| b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； |
| c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 |
|  | 审核和检查 | a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； |
| b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； |
| c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 岗位设置 | a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； |
| b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 |
|  | 人员配备 | a) 应配备一定数量的系统管理员、审计管理员和安全管理员等。 |
|  | 授权和审批 | a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； |
| b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程。 |
|  | 沟通和合作 | a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； |
| b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； |
| c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 |
|  | 审核和检查 | a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 |

#### 测评实施

* 文档查阅与分析

测评人员对测评委托方提交的安全管理文档（如制度、记录等）进行查看和分析，并记录相关证据。

* 人员访谈

测评人员根据文档查阅和分析的测评结果，针对部分不确定项目访谈相关安全人员，获取补充证据。

* 结果确认

测评人员向配合人员提交安全管理机构测评的初步结果记录。测评双方对初步结果进一步分析和修订后，认可形成安全管理机构测评结果记录。

#### 配合需求

| 配合项目 | 需求说明 |
| --- | --- |
| 配合人员 | 文档管理员，提供必要的制度类、记录类等文档 |
| 安全主管 |
| 测评环境 | 会议室 |

### 安全管理人员测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 人员录用 | a) 应指定或授权专门的部门或人员负责人员录用； |
| b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； |
| c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 |
|  | 人员离岗 | a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； |
| b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。 |
|  | 安全意识教育和培训 | a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； |
| b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； |
| c) 应定期对不同岗位的人员进行技能考核。 |
|  | 外部人员访问管理 | a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； |
| b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限， 并登记备案； |
| c) 外部人员离场后应及时清除其所有的访问权限； |
| d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 人员录用 | a) 应指定或授权专门的部门或人员负责人员录用； |
| b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。 |
|  | 人员离岗 | a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； |
|  | 安全意识教育和培训 | a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。 |
|  | 外部人员访问管理 | a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； |
| b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限， 并登记备案； |
| c) 外部人员离场后应及时清除其所有的访问权限。 |

#### 测评实施

* 文档查阅与分析

测评人员对测评委托方提交的安全管理文档（如制度、记录等）进行查看和分析，并记录相关证据。

* 人员访谈

测评人员根据文档查阅和分析的测评结果，针对部分不确定项目访谈相关安全人员，获取补充证据。

* 结果确认

测评人员向配合人员提交安全管理人员测评的初步结果记录。测评双方对初步结果进一步分析和修订后，认可形成安全管理人员测评结果记录。

#### 配合需求

|  |  |
| --- | --- |
| 配合项目 | 需求说明 |
| 配合人员 | 文档管理员，提供必要的制度类、记录类等文档 |
| 安全主管 |
| 测评环境 | 会议室 |

### 安全建设管理测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 定级和备案 | a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； |
| b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； |
| c) 应保证定级结果经过相关部门的批准； |
| d) 应将备案材料报主管部门和相应公安机关备案。 |
|  | 安全方案设计 | a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； |
| b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； |
| c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。 |
|  | 产品采购和使用 | a) 应确保网络安全产品采购和使用符合国家的有关规定； |
| b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； |
| c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。 |
|  | 自行软件开发 | a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； |
| b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； |
| c) 应制定代码编写安全规范，要求开发人员参照规范编写代码； |
| d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制； |
| e) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； |
| f) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； |
| g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。 |
|  | 外包软件开发 | a) 应在软件交付前检测其中可能存在的恶意代码； |
| b) 应保证开发单位提供软件设计文档和使用指南； |
| c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。 |
|  | 工程实施 | a) 应指定或授权专门的部门或人员负责工程实施过程的管理； |
| b) 应制定安全工程实施方案控制工程实施过程； |
| c) 应通过第三方工程监理控制项目的实施过程。 |
|  | 测试验收 | a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； |
| b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 |
|  | 系统交付 | a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； |
| b) 应对负责运行维护的技术人员进行相应的技能培训； |
| c) 应提供建设过程文档和运行维护文档。 |
|  | 等级测评 | a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； |
| b) 应在发生重大变更或级别发生变化时进行等级测评 |
| c) 应确保测评机构的选择符合国家有关规定。 |
|  | 服务供应商选择 | a) 应确保服务供应商的选择符合国家的有关规定； |
| b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； |
| c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 定级和备案 | a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； |
| b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； |
| c) 应保证定级结果经过相关部门的批准； |
| d) 应将备案材料报主管部门和相应公安机关备案。 |
|  | 安全方案设计 | a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； |
| b) 应根据保护对象的安全保护等级进行安全方案设计； |
| c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。 |
|  | 产品采购和使用 | a) 应确保网络安全产品采购和使用符合国家的有关规定； |
| b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。 |
|  | 自行软件开发 | a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； |
| b) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。 |
|  | 外包软件开发 | a) 应在软件交付前检测其中可能存在的恶意代码； |
| b) 应保证开发单位提供软件设计文档和使用指南。 |
|  | 工程实施 | a) 应指定或授权专门的部门或人员负责工程实施过程的管理； |
| b) 应制定安全工程实施方案控制工程实施过程。 |
|  | 测试验收 | a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； |
| b) 应进行上线前的安全性测试，并出具安全测试报告。 |
|  | 系统交付 | a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； |
| b) 应对负责运行维护的技术人员进行相应的技能培训； |
| c) 应提供建设过程文档和运行维护文档。 |
|  | 等级测评 | a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； |
| b) 应在发生重大变更或级别发生变化时进行等级测评 |
| c) 应确保测评机构的选择符合国家有关规定。 |
|  | 服务供应商选择 | a) 应确保服务供应商的选择符合国家的有关规定； |
| b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。 |

#### 测评实施

* 文档查阅与分析

测评人员对测评委托方提交的安全管理文档（如制度、记录等）进行查看和分析，并记录相关证据。

* 人员访谈

测评人员根据文档查阅和分析的测评结果，针对部分不确定项访谈相关安全人员，获取补充证据。

* 结果确认

测评人员向配合人员提交安全建设管理测评的初步结果记录。测评双方对初步结果进一步分析和修订后，认可形成安全建设管理测评结果记录。

#### 配合需求

|  |  |
| --- | --- |
| 配合项目 | 需求说明 |
| 配合人员 | 文档管理员，提供必要的制度类、记录类等文档 |
| 安全主管 |
| 测评环境 | 会议室 |

### 安全运维管理测评

#### 测评内容

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 环境管理 | a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； |
| b) 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； |
| c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 |
|  | 资产管理 | a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； |
| b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； |
| c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。 |
|  | 介质管理 | a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； |
| b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 |
|  | 设备维护管理 | a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； |
| b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等； |
| c) 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密； |
| d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。 |
|  | 漏洞和风险管理 | a) 应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或评估可能的影响后进行修补； |
| b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。 |
|  | 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； |
| b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； |
| c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； |
| d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； |
| e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； |
| f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； |
| g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库； |
| h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； |
| i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； |
| j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。 |
|  | 恶意代码防范管理 | a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； |
| b) 应定期验证防范恶意代码攻击的技术措施的有效性。 |
|  | 配置管理 | a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等； |
| b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 |
|  | 密码管理 | a) 应遵循密码相关国家标准和行业标准； |
| b) 应使用国家密码管理主管部门认证核准的密码技术和产品。 |
|  | 变更管理 | a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施； |
| b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； |
| c) 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 |
|  | 备份与恢复管理 | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等； |
| b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等； |
| c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 |
|  | 安全事件处置 | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件； |
| b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； |
| c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程， 总结经验教训； |
| d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。 |
|  | 应急预案管理 | a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容； |
| b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； |
| c) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； |
| d) 应定期对原有的应急预案重新评估，修订完善。 |
|  | 外包运维管理 | a) 应确保外包运维服务商的选择符合国家的有关规定； |
| b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； |
| c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； |
| d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。 |

| 序号 | 安全子类 | 测评指标描述 |
| --- | --- | --- |
|  | 环境管理 | a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； |
| b) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 |
|  | 资产管理 | a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。 |
|  | 介质管理 | a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； |
| b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 |
|  | 设备维护管理 | a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； |
| b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。 |
|  | 漏洞和风险管理 | a) 应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或评估可能的影响后进行修补。 |
|  | 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； |
| b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； |
| c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； |
| d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； |
| e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； |
|  | 恶意代码防范管理 | a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。 |
|  | 配置管理 | a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。 |
|  | 密码管理 | a) 应遵循密码相关国家标准和行业标准； |
| b) 应使用国家密码管理主管部门认证核准的密码技术和产品。 |
|  | 变更管理 | a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。 |
|  | 备份与恢复管理 | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等； |
| b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等； |
| c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 |
|  | 安全事件处置 | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件； |
| b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； |
| c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程， 总结经验教训。 |
|  | 应急预案管理 | a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； |
| b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； |
|  | 外包运维管理 | a) 应确保外包运维服务商的选择符合国家的有关规定； |
| b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。 |

#### 测评实施

* 文档查阅与分析

测评人员对测评委托方提交的安全管理文档（如制度、记录等）进行查看和分析，并记录相关证据。

* 人员访谈

测评人员根据文档查阅和分析的测评结果，针对部分不确定项目访谈相关安全人员，获取补充证据。

* 结果确认

测评人员向配合人员提交安全运维管理测评的初步结果记录。测评双方对初步结果进一步分析和修订后，认可形成安全运维管理测评结果记录。

#### 配合需求

|  |  |
| --- | --- |
| 配合项目 | 需求说明 |
| 配合人员 | 文档管理员，提供必要的制度类、记录类等文档 |
| 安全主管 |
| 测评环境 | 会议室 |

## 工具测试

本次测评的信息系统为第x级信息系统，根据第x级信息系统的测评力度要求，在测试的广度上，应基本覆盖所有的安全机制，在数量、范围上可以抽样；在测试的深度上，应执行漏洞扫描和渗透测试。

针对被测对象的网络边界和抽查设备、主机和业务应用系统的情况，需要在被测对象中设置2个扫描工具接入点（接入点JA、JB），如下图所示：

接入图

在接入点JA处接入安全漏洞扫描工具，直接测试数据库服务器、应用服务器等相关服务器的主机安全漏洞情况。

在接入点JB处接入渗透测试工具，直接测试BBBBB应用的安全漏洞情况。

“接入点”标注表示进行工具测试时，需要从该接入点接入。

本次工具测试的测试对象包括：

| **序号** | **工具名称** | **测评对象** | **接入点** | **说明** |
| --- | --- | --- | --- | --- |
|  | 绿盟远程安全评估系统RSAS | XXX服务器  XXX.XXX.XXX.XXX | JX |  |

## 测评风险及应对措施

为了避免测评工作引入新的安全风险，将可能造成的不良影响降低到测评委托单位可以接受的水平，测评机构在风险揭示、工具验证、连续性考虑和工作纪律等方面进行风险规避。

等保测评工作可能引入的风险包括：

* 可能影响系统正常运行

在现场测评时，需要对设备和系统进行一定的验证测试工作，部分测试内容需要上机验证并查看一些信息，可能对系统的运行造成一定的影响，甚至存在误操作的可能。

会使用一些技术测试工具进行漏洞扫描测试、性能测试甚至抗渗透能力测试。测试可能对网络和系统的负载造成一定的影响，渗透测试还可能影响到服务器和系统正常运行，如出现重启、服务中断、渗透过程中植入的代码未完全清理的现象。

* 可能泄漏敏感信息

泄露被测信息系统状态信息，如网络拓扑、IP地址、业务流程、安全机制、安全隐患和有关文档信息。

为降低以上风险，需采取以下应对措施：

* 签署委托测评协议

在测评工作正式开始之前，测评方和被测单位需要以委托协议的方式明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求、双方的责任和义务等。使得测评双方对测评过程中的基本问题达成共识，后续的工作以此作为基础，避免以后的工作出现大的分歧。

* 签署保密协议

测评双方应签署完善的、合乎法律规范的保密协议，以约束测评双方现在及将来的行为。保密协议规定了测评双方保密方面的权利和义务。测评工作的成果属被测评单位所有，测评方对其的引用与公开应得到被测评单位的授权，否则被测评单位将按照保密协议的要求追究测评单位的法律责任。

* 现场测评工作风险的规避

进行验证测试和工具测试之前，测评机构要求运营、使用单位对系统及数据进行备份，并对可能出现的事件制定处理方案。

进行验证测试和工具测试时，避开业务高峰期，在系统资源处于空闲状态时进行；上级验证测试由测评人员提出需要验证的内容，系统运营、使用单位的技术人员进行实际操作。整个现场测评过程要求系统运营、使用单位全程监督。

* 测评现场还原

测评工作完成后，测评人员应将测评过程中获取的所有权限交回，把测评过程中借阅的相关资料文档归还，并将在测评过程中植入被测信息系统中的相关代码/程序等进行严格清理。

* 提前将测评过程中可能遇到的风险揭示给测评委托单位

## 整体测评

整体测评是在单元测评的基础上，通过进一步分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评。整体测评主要包括安全控制点间、层面间和区域间相互作用的安全测评。整体测评需要与信息系统的实际情况相结合，因此全面地给出整体测评要求的全部输入，测评实施的具体对象、步骤和方法以及明确的结果判定方法是非常困难的，测评人员应根据被测对象的实际情况，结合本标准的要求，实施整体测评。

* 控制点间安全测评

控制点间的安全测评主要考虑同一区域内、同一层面上的不同控制点间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

在测评控制点间的增强和补充作用时，应先根据安全控制的具体实现和部署方式以及信息系统的实际环境，分析出位于物理安全、网络安全、主机系统安全、应用安全和数据安全等同一层面内的哪些安全技术控制间可能存在安全功能上的增强和补充作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评控制点间的削弱作用时，应先根据安全控制的具体实现方式和部署方式以及信息系统的实际环境，分析出位于物理安全、网络安全、主机系统安全、应用安全和数据安全等同一层面内的哪些安全技术控制间可能会存在安全功能上的削弱作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用后，一个安全控制是否影响另一个安全控制的功能发挥或者给其带来新的脆弱性，使其功能削弱。

如果控制点间优势互补，使单个低等级安全控制发挥的安全功能达到信息系统相应等级的安全要求，则可认为该安全控制没有影响信息系统的整体安全保护能力。如果控制点间存在削弱作用，使某个安全控制的功能等级降低到其安全功能已不能达到信息系统相应等级的安全要求，则可认为该安全控制影响到信息系统的整体安全保护能力。

* 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。安全功能上的增强和补充可以使两个不同层面上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个层面上的安全控制影响另一个层面安全控制的功能发挥或者给其带来新的脆弱性。

在测评层面间的功能增强和补充作用时，应先根据层面的整合集成方式和信息系统的实际环境，重点研究不同层面上相同或相似的安全控制（如主机系统层面与应用层面上的身份鉴别之间的关系），以及技术与管理上各层面的关联关系，分析出哪些控制点间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断层面间整合后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评层面间的功能削弱作用时，应先根据层面的整合集成方式和信息系统的实际环境，分析出哪些安全技术层面间和安全管理方面可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断不同层面整合后，一个层面是否影响另一个层面安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果层面间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果层面间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

* 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。例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。安全功能上的增强和补充可以使两个不同区域上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个区域上的安全功能影响另一个区域安全功能的发挥或者给其带来新的脆弱性。

在测评区域间的功能增强和补充作用时，应先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断区域间互连互通后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评区域间的功能削弱作用时，应先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断不同区域互连互通后，一个区域是否影响另一个区域安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果区域间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果区域间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

* 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。例如，由于信息系统边界上的网络入侵防范设备的管理接口连接方式不当，可能使网络访问控制出现旁路，出现信息系统整体安全防范不当。测评分析信息系统整体结构的安全性，主要是指从信息安全的角度，分析信息系统的物理布局、网络结构和业务逻辑等在整体结构上是否合理、简单、安全有效。测评信息系统整体安全防范的合理性，主要是指从系统的角度，分析研究信息系统安全防范在整体上是否遵循纵深防御的思路，明晰系统边界，确定重点保护对象，在适当的位置部署恰当的安全技术和安全管理措施等。

在测评分析信息系统整体结构的安全性时，应掌握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各种情况，结合业务数据流分析物理布局与网络拓扑之间、网络拓扑与业务逻辑之间、物理布局与业务逻辑之间、不同信息系统之间存在的各种关系，明确物理、网络和业务系统等不同位置上可能面临的威胁、可能暴露的脆弱性等，考虑信息系统的实际情况，综合判定信息系统的整体布局是否合理、主要关系是否简单、整体是否安全有效等。

在测评分析信息系统整体安全防范的合理性时，应熟悉信息系统安全保护措施的具体实现方式和部署情况等，结合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等。

# 等级保护测评方案用户确认

同意按上述**上海计算机软件技术开发中心**的等级保护测评方案对**BBBBB**进行网络安全等级保护测评。

AAAAA

负责人签字：

日期： 年 月 日

【本页以下无内容】

1. 安全服务包括系统集成、安全集成、安全运维、安全测评、应急响应、安全监测等所有相关安全服务。 [↑](#footnote-ref-1)