**记录编号：P2021XXXXX-GF01**

**AAAAA**

**BBBBB**

**等级保护测评方案**

|  |  |
| --- | --- |
| **系统名称：** | **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](#_Toc80268260)

[1.1 项目简介 1](#_Toc80268261)

[1.2 测评依据 1](#_Toc80268262)

[2. 被测系统描述 1](#_Toc80268263)

[2.1 承载的业务情况 1](#_Toc80268264)

[2.2 定级情况 2](#_Toc80268265)

[2.3 网络结构 3](#_Toc80268266)

[2.4 系统构成 4](#_Toc80268267)

[2.4.1 物理机房 4](#_Toc80268268)

[2.4.2 网络设备 4](#_Toc80268269)

[2.4.3 安全设备 4](#_Toc80268270)

[2.4.4 服务器/存储设备 4](#_Toc80268271)

[2.4.5 终端/现场设备 5](#_Toc80268272)

[2.4.6 系统管理软件/平台 5](#_Toc80268273)

[2.4.7 业务应用系统/平台 5](#_Toc80268274)

[2.4.8 数据类别 5](#_Toc80268275)

[2.4.9 安全相关人员 5](#_Toc80268276)

[2.4.10 安全管理文档 6](#_Toc80268277)

[2.5 安全服务 7](#_Toc80268278)

[3. 测评对象与指标 7](#_Toc80268279)

[3.1 测评指标 7](#_Toc80268280)

[3.1.1 安全通用要求指标 7](#_Toc80268281)

[3.2 测评对象 11](#_Toc80268282)

[3.2.1 测评对象选择方法 11](#_Toc80268283)

[3.2.2 测评对象选择结果 12](#_Toc80268284)

[3.3 现场测评时间安排 16](#_Toc80268285)

[4. 测评方法与工具 17](#_Toc80268286)

[4.1 测评方法 17](#_Toc80268287)

[4.2 主要测评工具 18](#_Toc80268288)

[5. 测评内容与实施 18](#_Toc80268289)

[5.1 通用安全要求 18](#_Toc80268290)

[5.1.1 安全物理环境测评 18](#_Toc80268291)

[5.1.2 安全通信网络测评 26](#_Toc80268292)

[5.1.3 安全区域边界测评 29](#_Toc80268293)

[5.1.4 安全计算环境测评 34](#_Toc80268294)

[5.1.5 安全管理中心测评 45](#_Toc80268295)

[5.1.6 安全管理制度测评 49](#_Toc80268296)

[5.1.7 安全管理机构测评 51](#_Toc80268297)

[5.1.8 安全管理人员测评 55](#_Toc80268298)

[5.1.9 安全建设管理测评 59](#_Toc80268299)

[5.1.10 安全运维管理测评 68](#_Toc80268300)

[5.2 工具测试 88](#_Toc80268301)

[5.3 测评风险及应对措施 89](#_Toc80268302)

[5.4 整体测评 90](#_Toc80268303)

[等级保护测评方案用户确认 94](#_Toc80268304)

# 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进行信息安全等级保护测评。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》和JR/T 0071.2-2020：《金融行业网络安全等级保护实施指引 第 2 部分：基本要求》标准，对BBBBB进行信息安全等级保护测评，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》和JR/T 0071.2-2020：《金融行业网络安全等级保护实施指引 第 2 部分：基本要求》标准的（第三级）S2A3G3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》

JR/T 0071.2-2020：《金融行业网络安全等级保护实施指引 第 2 部分：基本要求》

JR/T 0072—2020：《金融行业网络安全等级保护测评指南》

以下标准为本次测评的参考标准：

GB/T 17859—1999《计算机信息系统 安全保护等级划分准则》

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》

# 被测系统描述

## 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 业务截图

图2.2 业务截图-2

图2.3 业务截图-3

图2.4 业务截图-4

## 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，对国家安全造成一般损害,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，对国家安全造成一般损害,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（S2A3G3）。

## 网络结构

添加系统网络架构图

图2.2 网络拓扑

图2.x 网络拓扑

网络架构图说明。

至少说明边界、区域划分、主要的设备等。

## 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** |
| --- | --- | --- | --- |
|  | 系统管理数据 |  | 保密性、完整性 |
|  | 业务数据 |  | 保密性、完整性 |
|  | 鉴别信息 |  | 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

根据被测系统定级情况，从JR/T 0071.2-2020：《金融行业网络安全等级保护实施指引 第 2 部分：基本要求》中选择与被测系统的保护等级相对应的基本要求作为测评指标；根据需要进一步调整某些测评指标，形成测评指标列表。下表为JR/T 0071.2-2020：《金融行业网络安全等级保护实施指引 第 2 部分：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（JR/T 0071.2-2020：《金融行业网络安全等级保护实施指引 第 2 部分：基本要求》） | | | | | |
| 技术/管理 | 安全层面 | 类数量 | | | |
| S2 | 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 | 5 | 5 |
| 安全建设管理 | 10 | 10 |
| 安全运维管理 | 14 | 14 |
| 合计（S2A3G3） | | | | | 72（类） |

### **安全扩展要求指标**

本次测评未涉及安全扩展要求指标。

## 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，也是在被测系统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、了解到被测系统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：抽查对被测系统来说重要的服务器、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。



### **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 | 对应用系统进行漏洞扫描、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

根据信息系统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，获取证据以证明信息系统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，获取证据以证明信息系统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，获取证据以证明信息系统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** |
|  | AWVS | Acunetix | 14.5 | 14.3.210628104 |
|  | Nessus professional | Tenable Network Security | 8.15.0 | 202107020132 |
|  | 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 | V6.0R024F00SP06 | V6.0R02F01.2400 |
|  | 明鉴Web应用弱点扫描器 | 杭州安恒信息技术股份有限公司 | V6.0.1.10 | V6.1.115 |
|  | 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**

#### 测评内容

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 1 | 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。 |
| 2 | 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。 |
| 3 | c）机房应避开火灾危险程度高的区域，周围100米内不得有加油站、燃气站等危险建筑。（F3） |
| 4 | 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。 |
| 5 | b）应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。（F3） |
| 6 | 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。 |
| 7 | b）应将通信线缆铺设在隐蔽安全处。 |
| 8 | 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，非7\*24小时人员值守和巡查的机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。（F3） |
| 9 | d）应建立机房视频监控系统和动环监控系统，并对监控内容进行记录，对机房风冷水电设备、消防设施、门禁系统等重要设施实行连续24小时全面监控，视频监控记录和门禁系统出入记录至少保存3个月。（F3） |
| 10 | 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。 |
| 11 | 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。 |
| 12 | c）机房应通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。（F3） |
| 13 | 防火 | a）机房应设置火灾自动消防系统，能够通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式进行自动检测火情、自动报警，并自动灭火。（F3） |
| 14 | 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。 |
| 15 | 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。 |
| 16 | d）机房应备有一定数量的对电子设备影响小的手持式灭火器，消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发。（F3） |
| 17 | e）机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收，纸张、磁带和胶卷等易燃物品要放置于防火柜内。（F3） |
| 18 | f）主机房宜采用管网式洁净气体灭火系统，也可采用高压细水雾灭火系统，应同时设置两种火灾探测器，且消防报警系统应与空调系统、新风系统、门禁系统、灭火系统联动，凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。（F3） |
| 19 | g）应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。（F3） |
| 20 | h）机房应设置消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用，在机房通道上应设置显著的消防标志。（F3） |
| 21 | 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。 |
| 22 | 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。 |
| 23 | c）为便于地下积水的转移，漏水隐患区域地面周围应设排水沟或地漏等排水设施，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。（F3） |
| 24 | d）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。 |
| 25 | e）应对温湿度调节设备安装漏水报警装置，并设置防水堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。（F3） |
| 26 | 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。 |
| 27 | 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。 |
| 28 | c）主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F3） |
| 29 | 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。 |
| 30 | b）机房应采用专用温湿度调节设备，并应满足机房监控系统的要求。（F3） |
| 31 | c）温湿度调节设备的工作能力应满足机房负载要求，并应保有一定的余量。（F3） |
| 32 | 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。 |
| 33 | 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。 |
| 34 | c）应设置冗余或并行的电力电缆线路为计算机系统供电。 |
| 35 | d）应提供应急供电设施，以备供电系统临时停电时启用，并确保应急供电设施能在UPS供电时间内到位，每年需进行应急供电设施的带负载模拟演练，并定期对备用电力供应设备及应急供电设施进行检修和维护，确保其能正常使用。（F3） |
| 36 | e）UPS供电系统的冗余方式应采用N+1、N+2、2N、2（N+1）等方式，未建立备用发电机应急供电系统的单位，UPS后备时间至少1小时，已建立备用发电机应急供电系统的单位，UPS后备时间应满足至少15分钟以上。（F3） |
| 37 | f）机房内要求采用机房专用插座，市电、UPS电源插座分开，满足负荷使用要求。（F3） |
| 38 | g）计算机系统应选用铜芯电缆，避免铜、铝混用，若不能避免时，应采用铜铝过渡头连接。（F3） |
| 39 | h）机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。（F3） |
| 40 | i）机房重要区域、重要设备应提供UPS单独供电。（F3） |
| 41 | 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，如：业务处理能力能满足业务高峰期需要的50%以上。（F3） |
| 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，双线路设计时，宜由不同的电信运营商提供。（F3） |
| 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，并按照国家密码管理部门与行业有关要求使用密码算法。（F3） |
| 7 | b）应采用校验技术保证通信过程中数据的保密性，并按照国家密码管理部门与行业有关要求使用密码算法。（F3） |
| 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。 |

#### 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。 |
| 2 | 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。 |
| 3 | 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。 |
| 4 | 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。 |
| 5 | 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。 |
| 6 | 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。 |
| 7 | 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。 |
| 8 | 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，控制粒度为端口级。（F3） |
| 9 | 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。 |
| 10 | f）应对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。（F3） |
| 11 | g）应定期检查并锁定或撤销网络设备中不必要的用户账号。（F3） |
| 12 | 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。 |
| 13 | 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。 |
| 14 | 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。 |
| 15 | 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。 |
| 16 | e）应采取技术手段对高级持续威胁进行监测、发现。（F3） |
| 17 | f）应建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。（F3） |
| 18 | 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。 |
| 19 | 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。 |
| 20 | 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。 |
| 21 | b）应记录无线网络接入行为，形成日志进行留存，保存时间不少于6个月。（F3） |
| 22 | c）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。 |
| 23 | d）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，审计记录保存时间不少于6个月。（F3） |
| 24 | e）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。 |
| 25 | f）所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致。（F3） |
| 26 | 可信验证 | a）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。 |

#### 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** |
| --- | --- | --- |
| 1 | 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，静态口令应在8位以上，由字母、数字、符号等混合组成并定期更换。（F2） |
| 2 | 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。 |
| 3 | 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。 |
| 5 | 访问控制 | a）应对登录的用户分配账户和权限。 |
| 6 | b）应重命名或删除默认账户，修改默认账户或预设账户的默认口令。（F2） |
| 7 | 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。 |
| 8 | 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。 |
| 9 | e）应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。（F2） |
| 10 | 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。 |
| 11 | 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。 |
| 12 | 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，审计记录保存时间应不少于6个月。（F3） |
| 13 | d）应对审计进程进行保护，防止未经授权的中断。 |
| 14 | e）对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。（F3） |
| 15 | f）审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正确性。（F3） |
| 16 | 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。 |
| 17 | b）应关闭不需要的系统服务、默认共享和高危端口。 |
| 18 | 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。 |
| 19 | 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。 |
| 20 | e）应能通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时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。（F3） |
| 21 | 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。 |
| 22 | g）所有安全计算环境设备应全部专用化，不得进行与业务不相关的操作。（F3） |
| 23 | h）应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3） |
| 24 | 恶意代码防范 | a）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，将其有效阻断并定期统一进行升级和更新防恶意代码库。（F3） |
| 25 | b）应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3） |
| 26 | 可信验证 | a）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。 |
| 27 | 数据完整性 | a）应采用校验技术保证重要数据在传输和存储过程中的完整性。（F2） |
| 28 | 数据保密性 | a）应采用加密或其他保护措施保证鉴别信息在传输和存储过程中的保密性。（F2） |
| 29 | 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，采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指标（如RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放，数据保存期限依照国家相关规定。（F3） |
| 30 | 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。 |
| 31 | 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。 |
| 32 | d）对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F3） |
| 33 | e）为满足灾难恢复策略的要求，应对关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。（F3） |
| 34 | f）数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星期为周期的数据冗余。（F3） |
| 35 | g）异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资源（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F3） |
| 36 | 剩余信息保护 | a）应保证操作系统、数据库系统和应用系统用户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，无论这些信息是存放在硬盘上还是内存中。（F2） |
| 37 | 个人信息保护 | a）金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F3） |
| 38 | b）应仅采集和保存业务必需的用户个人金融信息。（F3） |
| 39 | c）应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限应禁止未授权访问和非法使用用户个人金融信息。（F3） |
| 40 | d）金融机构应依据JR/T0171—2020对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3） |
| 41 | e）金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F3） |
| 42 | f）应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3） |
| 43 | g）开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3） |

#### 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** |
| --- | --- | --- |
| 1 | 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。 |
| 2 | 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。 |
| 3 | c）应每月对设备的配置文件进行备份，发生变动时应及时备份。（F3） |
| 4 | d）应使用自动化技术手段对设备运行状况进行实时监测，运维人员应每天定期查看并记录系统运行状况。（F3） |
| 5 | e）应每季度检验网络设备软件版本信息，并通过有效测试验证后进行相应的升级，同时留存测试验证相关记录。（F3） |
| 6 | 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。 |
| 7 | b）应通过审计管理员对审计记录进行分析，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。 |
| 8 | c）应严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审计用户的权限分离，避免非授权的删除、修改或覆盖。（F3） |
| 9 | 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。 |
| 10 | 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。 |
| 11 | 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。 |
| 12 | 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。 |
| 13 | 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。 |
| 14 | d）应对分散在各个设备上的安全事件、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。（F3） |
| 15 | 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。 |
| 16 | f）应能对网络中发生的各类安全事件进行识别、报警、分析、响应和处置。（F3） |
| 17 | g）应具有对高频度发生的相同安全事件进行合并告警， 避免出现告警风暴的能力。（ F3） |

#### 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， 并编制形成网络安全方针制度文件。（ F3） |
| 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。 |
| 3 | 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。 |
| 4 | 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。 |
| 5 | 制定和发布 | a）金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应制定适用辖内的安全管理制度。（F3） |
| 6 | b）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。 |
| 7 | c）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。 |
| 8 | 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** |
| --- | --- | --- |
| 1 | 岗位设置 | a）网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F3） |
| 2 | b）应设立由本机构领导、业务与技术相关部门主要负责人组成的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，负责协调本机构及辖内网络安全管理工作，决策本机构及辖内网络安全重大事宜。（F3） |
| 3 | c）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。 |
| 4 | d）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。 |
| 5 | e）应设立专门的网络安全审计岗位，负责网络安全审计制度和流程的实施，制订和执行网络安全审计计划，对网络安全整个生命周期和重大事件等进行审计。（F3） |
| 6 | f）应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。（F3） |
| 7 | g）除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开展本部门的网络安全管理工作。（F3） |
| 8 | 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。 |
| 9 | b）应配备专职安全管理员，实行A、B岗制度，不可兼任。（F3） |
| 10 | 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。 |
| 11 | b）应针对系统投入运行、重要资源（如敏感数据等资源）的访问、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。（F3） |
| 12 | 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。 |
| 13 | d）用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系，权限变更应执行相关审批流程，并有完整的变更记录。（F3） |
| 14 | e）应建立系统用户及权限清单， 定期对员工权限进行检查核对， 发现越权用户要查明原因并及时调整， 同时清理过期用户权限， 做好记录归档。（F3） |
| 15 | 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。 |
| 16 | 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。 |
| 17 | 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。 |
| 18 | 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。 |
| 19 | 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。 |
| 20 | c）应建立对门户网站内容发布的审核、管理和监控机制。（F3） |
| 21 | d）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，要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对安全检查结果进行通报并报上一级机构科技部门备案。（F3） |
| 22 | e）应制定违反和拒不执行安全管理措施规定的处罚细则。（F3） |

#### 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** |
| --- | --- | --- |
| 1 | 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。 |
| 2 | 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。 |
| 3 | 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。 |
| 4 | d）应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F3） |
| 5 | e）凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不应从事网络安全管理工作。（F3） |
| 6 | 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。 |
| 7 | 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。 |
| 8 | 人员考核 | a）应定期对各个岗位的人员进行安全技能及安全认知的考核。（F3） |
| 9 | b）应对关键岗位的人员进行全面、严格的安全审查和技能考核。（F3） |
| 10 | c）应对考核结果进行记录并保存。（F3） |
| 11 | 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。 |
| 12 | 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。 |
| 13 | c）每年应至少对网络安全管理人员进行一次网络安全培训。（F3） |
| 14 | 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。 |
| 15 | 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。 |
| 16 | c）应对允许被外部人员访问的网络资源建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控。（F3） |
| 17 | d）外部人员离场后应及时清除其所有的访问权限。 |
| 18 | e）获得系统访问授权的外部人员应签署保密协议，不得进行非授权的增加、删除、修改、查询数据等操作，不得复制和泄露金融机构的任何信息。（F3） |

#### 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** |
| --- | --- | --- |
| 1 | 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。 |
| 2 | 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。 |
| 3 | c）应保证定级结果经过相关部门的批准。 |
| 4 | d）应将备案材料报主管部门和相应公安机关备案。 |
| 5 | 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。 |
| 6 | 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。 |
| 7 | 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。 |
| 8 | 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。 |
| 9 | 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。 |
| 10 | c）各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F3） |
| 11 | d）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。 |
| 12 | e）扫描、检测类网络安全产品应仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。（F3） |
| 13 | f）应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告。（F3） |
| 14 | g）应定期对各类网络安全产品产生的日志和报表进行备份存档， 至少保存6个月。（ F3） |
| 15 | h）应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。（F3） |
| 16 | 自行软件开发 | a）应将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试中使用。（F3） |
| 17 | b）应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制。（F3） |
| 18 | c）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。 |
| 19 | d）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。 |
| 20 | e）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。 |
| 21 | f）应保证在软件开发过程中对代码规范、代码质量、代码安全性进行审查，在软件安装前对可能存在的恶意代码进行检测。（F3） |
| 22 | g）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。 |
| 23 | h）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。 |
| 24 | i）在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。（F3） |
| 25 | 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。 |
| 26 | b）应保证开发单位提供软件设计文档和使用指南。 |
| 27 | 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。 |
| 28 | d）应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F3） |
| 29 | e）应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F3） |
| 30 | f）应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。（F3） |
| 31 | 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。 |
| 32 | b）应制定安全工程实施方案控制工程实施过程。 |
| 33 | c）应通过第三方工程监理控制项目的实施过程。 |
| 34 | d）应制定灾难备份系统集成与测试计划并组织实施，通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。（F3） |
| 35 | e）系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F3） |
| 36 | 测试验收 | a）应根据设计方案或合同要求等制订测试验收方案，并依据测试验收方案实施测试验收，在测试验收过程中应详细记录测试验收结果，形成测试验收报告。（F3） |
| 37 | b）应由项目承担单位（部门）或公正的第三方制订安全测试方案，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，并将测试报告报科技部门审查。（F3） |
| 38 | c）新建应用系统投入生产运行前，原则上应进行不少于1个月的模拟运行和不少于3个月的试运行。（F3） |
| 39 | d）对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方案、数据备份与系统恢复措施、应急处置措施后，经系统用户和主管领导审批同意后，才能开展测试工作，以确保生产系统的安全。（F3） |
| 40 | 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。 |
| 41 | b）应对负责运行维护的技术人员进行相应的技能培训。 |
| 42 | c）应提供建设过程文档和运行维护文档。 |
| 43 | d）外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将采用的关键安全技术措施和核心安全功能设计对外公开。（F3） |
| 44 | 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。 |
| 45 | b）应在发生重大变更或级别发生变化时进行等级测评。 |
| 46 | c）应选择公安部认可的全国等级保护测评机构推荐目录中的测评单位进行等级测评，并与测评单位签订安全保密协议。（F3） |
| 47 | 服务供应商选择 | a）应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。（F3） |
| 48 | b）应确保服务供应商的选择符合国家的有关规定。 |
| 49 | c）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。 |
| 50 | d）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。 |

#### 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** |
| --- | --- | --- |
| 1 | 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，填写机房值班记录、巡视记录。（F3） |
| 2 | b）应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。 |
| 3 | c）机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F3） |
| 4 | d）机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F3） |
| 5 | e）应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F3） |
| 6 | f）进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F3） |
| 7 | g）应设置弱电井，并留有足够的可扩展空间。（F3） |
| 8 | h）机房所在区域应安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于3个月，销毁录像等资料应经单位主管领导批准后实施。（F3） |
| 9 | i）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。 |
| 10 | 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。 |
| 11 | 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。 |
| 12 | 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。 |
| 13 | 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。 |
| 14 | 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，应选择安全可靠的传递、交接方式，做好防信息泄漏控制措施，并对介质的归档和查询等进行登记记录。（F3） |
| 15 | c）所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F3） |
| 16 | d）对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F3） |
| 17 | e）对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F3） |
| 18 | f）应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F3） |
| 19 | g）应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安全区域。（F3） |
| 20 | h）应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。（F3） |
| 21 | i）应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F3） |
| 22 | 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。 |
| 23 | 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。 |
| 24 | c）设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前应请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。（F3） |
| 25 | d）应制定规范化的故障处理流程，建立详细的故障日志（包括故障发生的时间、范围、现象、处理结果和处理人员等内容）。（F3） |
| 26 | e）新购置的设备应经过验收，验收合格后方能投入使用。（F3） |
| 27 | f）应制定设备管理规范，根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护责任。（F3） |
| 28 | g）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。 |
| 29 | h）需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复性销毁处理，同时备案；信息消除处理仅限于废止设备仍将在金融机构内部使用的情况，否则应进行信息的不可恢复性销毁。（F3） |
| 30 | 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。 |
| 31 | 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。 |
| 32 | 网络和系统安全管理  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。 |
| 33 | 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。 |
| 34 | 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。 |
| 35 | 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。 |
| 36 | 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，重要运维操作要求至少两人在场，保留记录，并由操作和复核人员进行确认，维护记录和确认记录应至少妥善保存6个月。（F3） |
| 37 | f）应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，经过审批后才可开通，操作过程中应保留不可篡改的审计日志，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。（F3） |
| 38 | g）各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F3） |
| 39 | h）网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不应对外公开，未经科技主管部门授权，任何外部机构与人员不应检测或扫描机构内部网络。（F3） |
| 40 | i）金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F3） |
| 41 | j）所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。（F3） |
| 42 | k）系统管理员不应兼任业务操作人员，系统管理员不应对业务数据进行任何增加、删除、修改等操作，系统管理员确需对系统数据库进行业务数据维护操作的，应征得业务部门审批，并详细记录维护内容、人员、时间等信息。（F3） |
| 43 | l）每半年应至少进行一次漏洞扫描，对发现的安全漏洞及时进行修补，扫描结果应及时上报。（F3） |
| 44 | m）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。 |
| 45 | n）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。 |
| 46 | o）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。 |
| 47 | p）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。 |
| 48 | q）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。 |
| 49 | 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。 |
| 50 | b）应定期验证防范恶意代码攻击的技术措施的有效性。 |
| 51 | c）客户端应统一安装病毒防治软件，设置用户口令和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。（F3） |
| 52 | 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。 |
| 53 | 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。 |
| 54 | 密码管理 | a）应遵循密码相关的国家标准和行业标准。 |
| 55 | 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。 |
| 56 | c）应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。（F3） |
| 57 | d）系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，并每半年更换，口令密码的强度应满足不同安全性要求。（F3） |
| 58 | e）系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。（F3） |
| 59 | f）密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责，密钥资料须保存在保险柜内，保险柜钥匙由专人负责，使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。（F3） |
| 60 | g）确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F3） |
| 61 | h）应支持各类环境中密码设备使用、管理权限分离。（F3） |
| 62 | 变更管理 | a）变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认。（F3） |
| 63 | b）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。 |
| 64 | c）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。 |
| 65 | d）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。 |
| 66 | e）变更前应做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪。（F3） |
| 67 | f）如果需要对生产环境进行重大变更，应按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同意后，再进行变更操作，以确保生产系统的安全。（F3） |
| 68 | g）当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性，应尽量减少紧急变更。（F3） |
| 69 | 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。 |
| 70 | 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。 |
| 71 | 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。 |
| 72 | d）应每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。（F3） |
| 73 | e）应每季度对备份数据的有效性进行检查，备份数据要实行异地保存。（F3） |
| 74 | f）恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并妥善保管。（F3） |
| 75 | g）灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。（F3） |
| 76 | h）应建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册。（F3） |
| 77 | i）金融机构应根据信息系统的灾难恢复工作情况，确定审计频率，应每年至少组织一次内部灾难恢复工作审计。（F3） |
| 78 | j）应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。（F3） |
| 79 | k）应建立灾难备份系统，主备系统实际切换时间应少于RTO时间，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F3） |
| 80 | 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。 |
| 81 | 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。 |
| 82 | 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。 |
| 83 | 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。 |
| 84 | 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，业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字确认。（F3） |
| 85 | 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。 |
| 86 | c）应每年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。（F3） |
| 87 | d）在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。（F3） |
| 88 | e）突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F3） |
| 89 | f）突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F3） |
| 90 | g）实施报告制度和启动应急预案的单位应当实行重大突发事件24小时值班制度。（F3） |
| 91 | h）应定期对原有的应急预案重新评估，修订完善。 |
| 92 | i）应急演练结束后，应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F3） |
| 93 | 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。 |
| 94 | 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。 |
| 95 | 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。 |
| 96 | 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。 |
| 97 | e）应要求外包运维服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F3） |
| 98 | f）应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F3） |

#### 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 |

## 云计算安全测评扩展要求

本次测评未涉及云计算安全测评扩展要求。

## 工具测试

本次测评的信息系统为第三级信息系统，根据第三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1个扫描工具接入点（接入点JA），如下图所示：

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

“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** |
| --- | --- | --- | --- | --- |
|  | AWVS | 应用系统 | JB | -- |
|  | Nessus professional | 服务器、网络设备、安全设备 | JA | -- |
|  | 绿盟远程安全评估系统RSAS | 服务器、网络设备、安全设备 | JA | -- |
|  | 明鉴Web应用弱点扫描器 | 应用系统 | JB | -- |
|  | 渗透测试工具集V1.0 | 应用系统 | JB | -- |

## 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系统的实际情况，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，分析出位于安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心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，分析出位于安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心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)