**{系统名称}**

**网络安全等级测评方案**

|  |  |
| --- | --- |
| **系统名称：** | **{系统名称}**  |
| **委托单位：** | **{单位名称}**  |
| **测评单位：** | **XX市第一测评中心**  |
| **方案时间：** | **{方案结束时间}**  |

网络安全等级测评基本信息表

|  |
| --- |
| **被测对象** |
| **被测对象名称** |  | **安全保护等级** |  |
| **备案证明编号** |  |
| **等级保护对象形态** |

|  |  |  |
| --- | --- | --- |
| ☑传统IT系统 | ☑云计算 | ☐采用移动互联技术的系统 |
| ☐物联网 | ☐工业控制系统 | ☐大数据 | ☐其他系统 |

 |
|

|  |
| --- |
| **被测单位** |
| **单位名称** |  |
| **单位地址** |  | **邮政编码** |  |
| **联系人** | **姓名** |  | **职务/职称** |  |
| **所属部门** |  | **办公电话** |  |
| **移动电话** |  | **电子邮件** |  |

 |
|

|  |
| --- |
| **测评单位** |
| **单位名称** | XX市第一测评中心 | **机构代码** | 0001 |
| **单位地址** | XX市第一大道68号 | **邮政编码** | 123456 |
| **联系人** | **姓名** | xx | **职务/职称** | 项目经理 |
| **所属部门** | 测评部 | **办公电话** | 12345678 |
| **移动电话** | 188xxxxxxxx | **电子邮件** | xx@xxx.com |
| **审核批准** | **编制人** |  | **编制日期** |  |
| **审核人** |  | **审核日期** |  |
| **批准人** |  | **批准日期** |  |

 |
| **方案确认** |
| **审核确认** | **确认人** |  | **确认日期** |  |

# 概述

## 项目简介

安全等级测评的目的是通过对目标系统在安全技术及管理方面的测评，对目标系统的安全技术状态及安全管理状况做出初步判断，给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

为进一步提高信息系统的保障能力，根据《信息安全等级保护管理办法》（公通字2007【43】号）的精神，{单位名称}委托XX市第一测评中心对{系统名称}实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

## 测评范围

依据本次安全等级测评的范围，选取的测评对象需覆盖到被测系统相关的业务系统、机房、核心网络设备和网络安全设备、重要业务系统所涉及到的操作系统、数据库和中间件。

对于测评范围内的测评对象，根据抽样覆盖面全和抽样数量合理的原则，综合考虑被测对象数量、类型、部署方式和网络部署位置等因素，选取典型的、适量的测评对象进行抽测。

确认所有安全相关人员，针对所负责的安全部分进行抽样访谈，并对所有安全管理相关文档进行全面检查。

## 测评过程

本次等级测评分为四个过程：测评准备过程、方案编制过程、测评实施过程、分析与报告编制过程。具体如图 1.1 所示。其中，各阶段的时间安排如下：

1、{调研开始时间～调研结束时间}，测评准备过程。

2、{方案开始时间～方案结束时间}，方案编制过程。

3、{实施开始时间～实施结束时间}，现场实施过程。

4、{报告开始时间～报告结束时间}，分析与报告编制过程。



图 1.1 等级保护测评工作流程图

## 测评依据

测评过程中主要依据的标准：

主要依据：

GB 17859-1999：《计算机信息系统 安全保护等级划分准则》

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》

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 20984-2022《信息安全技术 信息安全风险评估方法》

参考依据：

 《{系统名称}网络安全等级测评调研表》

 《{系统名称}安全等级保护定级报告》

# 被测等级保护对象情况

## 定级情况

表 2‑1 {系统名称}定级结果

| **被测对象名称** | **安全保护等级** | **业务信息安全等级** | **系统服务安全等级** |
| --- | --- | --- | --- |
|  |  |  |  |

## 承载的业务情况

## 网络结构

## 系统构成

### 机房

表 2‑2 机房

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

### 网络设备

表 2‑3 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

表 2‑4 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

表 2‑5 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

表 2‑6 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

表 2‑7 系统管理软件/平台

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

### 业务应用软件/平台

表 2‑8 业务应用软件/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** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

### 关键数据类别

表 2‑9 关键数据类别

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| --- | --- | --- | --- |
|  |  |  |  |

### 安全相关人员

表 2‑10 安全相关人员

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

### 安全管理文档

表 2‑11 安全管理文档

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
|  |  |  |

## 前次测评问题整改情况说明

# 测评对象与指标

## 测评对象

### 测评对象选择方法

{系统名称}等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合{系统名称}的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

(1) 主机房（包括其环境、设备和设施等）和灾备机房；

(2) 存储被测系统重要数据的介质的存放环境；

(3) 办公场地；

(4) 整个系统的网络拓扑结构；

(5) 安全设备，包括防火墙等；

(6) 边界网络设备，包括路由器、楼层交换机等；

(7) 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

(8) 承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

(9) 管理终端和主要{系统名称}终端；

(10) 能够完成{系统名称}不同业务使命的业务应用系统；

(11) 业务备份系统；

(12) 信息安全主管人员、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；

(13) 涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

### 测评对象选择结果

#### 机房

表 3‑1 机房

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

#### 网络设备

表 3‑2 网络设备

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

#### 安全设备

表 3‑3 安全设备

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

#### 服务器/存储设备

表 3‑4 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

表 3‑5 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

表 3‑6 系统管理软件/平台

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

#### 业务应用系统/平台

表 3‑7 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** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

#### 数据类别

表 3‑8 数据类别

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| --- | --- | --- | --- |
|  |  |  |  |

#### 安全相关人员

表 3‑9 安全相关人员

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

#### 安全管理文档

表 3‑10 安全管理文档

| **序号** | **文档名称** | **主要内容** |
| --- | --- | --- |
|  |  |  |

## 测评指标

### 安全通用要求指标

表 3‑11 安全通用要求指标

| **安全类** | **安全控制点** | **测评项数** |
| --- | --- | --- |
| **安全通用要求** |
| 安全物理环境 | 物理位置选择 | 2 |
| 物理访问控制 | 1 |
| 防盗窃和防破坏 | 3 |
| 防雷击 | 2 |
| 防火 | 3 |
| 防水和防潮 | 3 |
| 防静电 | 2 |
| 温湿度控制 | 1 |
| 电力供应 | 3 |
| 电磁防护 | 2 |
| 安全通信网络 | 网络架构 | 5 |
| 通信传输 | 2 |
| 可信验证 | 1 |
| 安全区域边界 | 边界防护 | 4 |
| 访问控制 | 5 |
| 入侵防范 | 4 |
| 恶意代码和垃圾邮件防范 | 2 |
| 安全审计 | 4 |
| 可信验证 | 1 |
| 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 |
| **安全通用要求指标数量统计** | 211 |

### 安全扩展要求指标

表 3‑12 安全扩展要求指标

| **扩展类型** | **安全类** | **控制点** | **测评项数** |
| --- | --- | --- | --- |
| **云计算安全扩展要求** |
| 云计算安全扩展要求 | 安全物理环境 | 基础设施位置 | 1 |
| 安全通信网络 | 网络架构 | 5 |
| 安全区域边界 | 访问控制 | 2 |
| 入侵防范 | 4 |
| 安全审计 | 2 |
| 安全计算环境 | 身份鉴别 | 1 |
| 访问控制 | 2 |
| 入侵防范 | 3 |
| 镜像和快照保护 | 3 |
| 数据完整性和保密性 | 4 |
| 数据备份恢复 | 4 |
| 剩余信息保护 | 2 |
| 安全管理中心 | 集中管控 | 4 |
| 安全建设管理 | 云服务商选择 | 5 |
| 供应链管理 | 3 |
| 安全运维管理 | 云计算环境管理 | 1 |
| **安全扩展要求指标数量统计** | 46 |

### 其他安全要求指标

表 3‑13 其他安全要求指标

| **安全类** | **安全控制点** | **特殊要求描述** | **测评项数** |
| --- | --- | --- | --- |
| N/A | N/A | N/A | N/A |

# 测评方法与工具

## 测评方法

本次测评中涉及的测评方法主要包括：

### 访谈

访谈是指测评人员与被测评组织内的有关人员就测评所关注的问题进行有针对性的询问和交流的过程，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

访谈深度（即访谈内容的详细程度）以及访谈的广度（即对被测评组织中员工角色类型以及每种类型中人数的覆盖程度）由测评人员依据不同的测评需要进行选择和判断。

### 检查

检查是指对测评对象（如规范、机制或行为）进行观察、调查、评审、分析或核查的过程。与访谈类似，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

比较典型的检查行为包括：对安全配置的核查、对安全策略的分析和评审等。

### 测试

测评是指在特定环境中运行一个或多个评估对象（限于机制或行为）并将实际结果与预期结果进行比较的过程。测评的目标是判定对象是否符合预定的一组规格。测评过程可以帮助评估者获得证据。测试可以分为以下两类：

漏洞扫描：测试人员利用漏洞扫描工具对被测系统资产进行扫描，发现系统存在的漏洞隐患。

渗透测试：测试人员可以利用所有可用的资料和手段来企图绕开被测评项目的安全特性。

### 风险分析

依据《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022），采用风险分析的方法分析信息系统等级测评结果中存在的安全问题（等级测评结果中部分符合项或不符合项的汇总结果）可能对信息系统安全造成的影响。

分析过程包括：

1. 判断安全问题被威胁利用的可能性，可能性的取值范围为高、中和低；
2. 判断安全问题被威胁利用后，对信息系统安全（业务信息安全和系统服务安全）造成的影响程度，影响程度取值范围为高、中和低；
3. 综合1）和2）的结果对信息系统面临的安全风险进行赋值，风险值的取值范围为高、中和低；
4. 结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。
5. 以列表形式给出等级测评发现安全问题以及风险分析和评价情况。

## 主要测评工具

设备漏洞扫描测试使用xxxxxxxx，渗透测试使用xxxxxxxx。

# 工具测评

## 风险和规避措施

### 设备漏洞扫描

**设备包括网络设备、安全设备、主机设备（操作系统），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管理程序（WEB、 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管理程序，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。

### 渗透测试说明

**渗透性测试根据测试者在测试前掌握被测信息多少的不同可分为：**

* **黑盒测试：**

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。

* **白盒测试：**

渗透性测试安全工程师可以通过正常渠道向被测机构要求，取得各种资料，包括网络拓扑、员工资料甚至网站或其他程序的代码片段，也能够与被测机构内部的其他员工（业务人员、开发人员、管理人员等）进行面对面的沟通。这类测试的目的是模拟组织内部雇员的越权操作，和预防万一组织重要信息泄露，网络黑客能利用这些信息对组织构成的危害。

* **灰盒测试：**

对测试对象有一定的了解，主要是模拟离职的员工或合作伙伴，他们对组织的结构比较了解。但不在公司内部，没有权限访问。

**根据渗透者所处的位置也可以分为：**

* **内部测试：**

渗透测试安全工程师由内部网络发起测试，这类测试能够模拟组织内部违规操作者的行为。最主要的“优势”就是绕过了防火墙的保护。

* **外部测试：**

渗透测试安全工程师完全处于外部网络（如互联网、第三方机构），模拟从组织外部发起的攻击行为，可能来自于对组织内部信息一无所知的攻击者，也可能来自于对组织内部信息一清二楚的攻击者。

## 工具测试接入点说明

表 5‑1 接入点扫描的网络设备和服务器设备列表

| **序号** | **接入点** | **设备名称** | **类型/OS** |
| --- | --- | --- | --- |
|  |  |  |  |

# 测评内容与实施

等级测评的现场实施过程由单项测评和整体测评两部分构成。

对应《基本要求》各安全要求项的测评称为单项测评。整体测评是在单项测评的基础上，通过进一步分析定级对象安全保护功能的整体相关性，对定级对象实施的综合安全测评。

## 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

#### 测评指标

表 6‑1 安全物理环境（通用要求）测评指标

| **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 | 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。 |
| 4 | 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； |
| 5 | b）应将通信线缆铺设在隐蔽安全处； |
| 6 | 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。 |
| 7 | 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； |
| 8 | 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。 |
| 9 | 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； |
| 10 | 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； |
| 11 | 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。 |
| 12 | 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； |
| 13 | 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； |
| 14 | 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。 |
| 15 | 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； |
| 16 | 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。 |
| 17 | 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。 |
| 18 | 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； |
| 19 | 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； |
| 20 | c）应设置冗余或并行的电力电缆线路为计算机系统供电。 |
| 21 | 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； |
| 22 | b）应对关键设备实施电磁屏蔽。 |

#### 测评实施

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。

### 安全通信网络测评

#### 测评指标

表 6‑2 安全通信网络（通用要求）测评指标

| **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。 |

#### 测评实施

安全通信网络测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的安全保护能力。

### 安全区域边界测评

#### 测评指标

表 6‑3 安全区域边界（通用要求）测评指标

| **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； |
| 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 | 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； |
| 11 | 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； |
| 12 | 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； |
| 13 | 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。 |
| 14 | 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； |
| 15 | 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。 |
| 16 | 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； |
| 17 | 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； |
| 18 | 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； |
| 19 | 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。 |
| 20 | 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

安全区域边界测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的网络安全保护能力。

### 安全计算环境测评

#### 测评指标

表 6‑4 安全计算环境（通用要求）测评指标

| **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，身份鉴别信息具有复杂度要求并定期更换； |
| 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； |
| 4 | 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。 |
| 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，修改默认账户的默认口令； |
| 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； |
| 10 | 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； |
| 11 | 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。 |
| 12 | 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； |
| 13 | 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； |
| 14 | 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； |
| 15 | d）应对审计进程进行保护，防止未经授权的中断。 |
| 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； |
| 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 | 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，并将其有效阻断。 |
| 23 | 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。 |
| 24 | 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； |
| 25 | 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。 |
| 26 | 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； |
| 27 | 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。 |
| 28 | 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； |
| 29 | 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； |
| 30 | 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。 |
| 31 | 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； |
| 32 | 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。 |
| 33 | 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； |
| 34 | b）应禁止未授权访问和非法使用用户个人信息。 |

#### 测评实施

安全计算环境测评中，技术检测人员主要关注服务器操作系统、数据库管理系统、网络设备、安全设备以及应用系统在身份鉴别、访问控制、安全审计等方面的安全保护能力，将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况）。

### 安全管理中心测评

#### 测评指标

表 6‑5 安全管理中心（通用要求）测评指标

| **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 | 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； |
| 4 | 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。 |
| 5 | 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； |
| 6 | 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。 |
| 7 | 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； |
| 8 | 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； |
| 9 | 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； |
| 10 | 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； |
| 11 | 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； |
| 12 | 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。 |

#### 测评实施

安全管理中心测评中，技术检测人员将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况），用于评测系统的安全保护能力。

### 安全管理制度测评

#### 测评指标

表 6‑6 安全管理制度（通用要求）测评指标

| **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； |
| 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）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； |
| 6 | 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。 |
| 7 | 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

安全管理类测评中，技术检测人员将以文档查看和分析为主，访谈为辅获取证据，来评测项目委托单位安全管理类措施的落实情况。安全管理类测评主要涉及安全主管、安全管理人员、管理制度文档、各类操作规程文件和操作记录等。

### 安全管理机构测评

#### 测评指标

表 6‑7 安全管理机构（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 1 | 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； |
| 2 | 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； |
| 3 | 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。 |
| 4 | 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； |
| 5 | b）应配备专职安全管理员，不可兼任。 |
| 6 | 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； |
| 7 | 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； |
| 8 | 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。 |
| 9 | 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； |
| 10 | 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； |
| 11 | 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。 |
| 12 | 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； |
| 13 | 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； |
| 14 | 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。 |

#### 测评实施

安全管理机构测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等技术检测对象。

### 安全管理人员测评

#### 测评指标

表 6‑8 安全管理人员（通用要求）测评指标

| **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 | 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； |
| 5 | 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。 |
| 6 | 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； |
| 7 | 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； |
| 8 | c）应定期对不同岗位的人员进行技能考核。 |
| 9 | 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； |
| 10 | 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； |
| 11 | c）外部人员离场后应及时清除其所有的访问权限； |
| 12 | 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。 |

#### 测评实施

安全管理人员测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等检测对象。

### 安全建设管理测评

#### 测评指标

表 6‑9 安全建设管理（通用要求）测评指标

| **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）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。 |
| 11 | 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； |
| 12 | 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； |
| 13 | 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； |
| 14 | 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； |
| 15 | 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； |
| 16 | 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； |
| 17 | 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。 |
| 18 | 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； |
| 19 | b）应保证开发单位提供软件设计文档和使用指南； |
| 20 | 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。 |
| 21 | 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； |
| 22 | b）应制定安全工程实施方案控制工程实施过程； |
| 23 | c）应通过第三方工程监理控制项目的实施过程。 |
| 24 | 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； |
| 25 | 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。 |
| 26 | 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； |
| 27 | b）应对负责运行维护的技术人员进行相应的技能培训； |
| 28 | c）应提供建设过程文档和运行维护文档。 |
| 29 | 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； |
| 30 | b）应在发生重大变更或级别发生变化时进行等级测评； |
| 31 | c）应确保测评机构的选择符合国家有关规定。 |
| 32 | 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； |
| 33 | 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； |
| 34 | 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。 |

#### 测评实施

安全建设管理测评主要涉及系统建设负责人、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

###  安全运维管理测评

#### 测评指标

表 6‑10 安全运维管理（通用要求）测评指标

| **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； |
| 2 | 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； |
| 3 | 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。 |
| 4 | 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； |
| 5 | 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； |
| 6 | 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。 |
| 7 | 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； |
| 8 | 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。 |
| 9 | 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； |
| 10 | 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； |
| 11 | 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； |
| 12 | 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。 |
| 13 | 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； |
| 14 | 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。 |
| 15 | 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； |
| 16 | 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； |
| 17 | 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； |
| 18 | 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； |
| 19 | 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； |
| 20 | 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； |
| 21 | 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； |
| 22 | 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； |
| 23 | 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； |
| 24 | 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。 |
| 25 | 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； |
| 26 | b）应定期验证防范恶意代码攻击的技术措施的有效性。 |
| 27 | 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； |
| 28 | 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。 |
| 29 | 密码管理 | a）应遵循密码相关国家标准和行业标准； |
| 30 | 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。 |
| 31 | 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； |
| 32 | 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； |
| 33 | 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。 |
| 34 | 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； |
| 35 | 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； |
| 36 | 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。 |
| 37 | 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； |
| 38 | 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； |
| 39 | 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； |
| 40 | 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。 |
| 41 | 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； |
| 42 | 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； |
| 43 | 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； |
| 44 | d）应定期对原有的应急预案重新评估，修订完善。 |
| 45 | 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； |
| 46 | 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； |
| 47 | 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； |
| 48 | 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。 |

#### 测评实施

安全运维管理测评主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

## 扩展安全要求

### 安全物理环境测评

#### 测评指标

表 6‑11 安全物理环境（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全扩展要求 | 基础设施位置 | a）应保证云计算基础设施位于中国境内。 |

#### 测评实施

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，用于评测机房针对安全扩展要求方面的安全保护能力。

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。

### 安全通信网络测评

#### 测评指标

表 6‑12 安全通信网络（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全扩展要求 | 网络架构 | a）应保证云计算平台不承载高于其安全保护等级的业务应用系统； |
| 2 | b）应实现不同云服务客户虚拟网络之间的隔离； |
| 3 | c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； |
| 4 | d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； |
| 5 | e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。 |

#### 测评实施

安全通信网络测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统针对安全扩展要求方面的安全保护能力。

### 安全区域边界测评

#### 测评指标

表 6‑13 安全区域边界（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全扩展要求 | 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； |
| 2 | b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 |
| 3 | 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； |
| 4 | b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； |
| 5 | c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； |
| 6 | d）应在检测到网络攻击行为、异常流量情况时进行告警。 |
| 7 | 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； |
| 8 | b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 |

#### 测评实施

安全区域边界测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统针对安全扩展要求方面的网络安全保护能力。

### 安全计算环境测评

#### 测评指标

表 6‑14 安全计算环境（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全扩展要求 | 身份鉴别 | a）当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 |
| 2 | 访问控制 | a）应保证当虚拟机迁移时，访问控制策略随其迁移； |
| 3 | b）应允许云服务客户设置不同虚拟机之间的访问控制策略。 |
| 4 | 入侵防范 | a）应能检测虚拟机之间的资源隔离失效，并进行告警； |
| 5 | b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； |
| 6 | c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 |
| 7 | 镜像和快照保护 | a）应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； |
| 8 | b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； |
| 9 | c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 |
| 10 | 数据完整性和保密性 | a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定； |
| 11 | b）应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； |
| 12 | c）应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； |
| 13 | d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 |
| 14 | 数据备份恢复 | a）云服务客户应在本地保存其业务数据的备份； |
| 15 | b）应提供查询云服务客户数据及备份存储位置的能力； |
| 16 | c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； |
| 17 | d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 |
| 18 | 剩余信息保护 | a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除； |
| 19 | b）云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。 |

#### 测评实施

安全计算环境测评中，技术检测人员主要关注服务器操作系统、数据库管理系统、网络设备、安全设备以及应用系统在相关安全扩展要求方面的安全保护能力，将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况）。

### 安全管理中心测评

#### 测评指标

表 6‑15 安全管理中心（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全扩展要求 | 集中管控 | a）应能对物理资源和虚拟资源按照策略做统一管理调度与分配； |
| 2 | b）应保证云计算平台管理流量与云服务客户业务流量分离； |
| 3 | c）应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计； |
| 4 | d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。 |

#### 测评实施

安全管理中心测评中，技术检测人员将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况），用于评测系统针对安全扩展要求方面的安全保护能力。

### 安全建设管理测评

#### 测评指标

表 6‑16 安全建设管理（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全扩展要求 | 云服务商选择 | a）应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力； |
| 2 | b）应在服务水平协议中规定云服务的各项服务内容和具体技术指标； |
| 3 | c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等； |
| 4 | d）应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除； |
| 5 | e）应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。 |
| 6 | 供应链管理 | a）应确保供应商的选择符合国家有关规定； |
| 7 | b）应将供应链安全事件信息或安全威胁信息及时传达到云服务客户； |
| 8 | c）应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。 |

#### 测评实施

安全建设管理测评主要涉及系统建设负责人、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

### 安全运维管理测评

#### 测评指标

表 6‑17 安全运维管理（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全扩展要求 | 云计算环境管理 | a）云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。 |

#### 测评实施

安全运维管理测评主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

# 整体测评

系统整体测评主要是在单项测评的基础上，通过测评分析系统在安全控制间、层面间和安全区域间三个方面存在的关联作用验证和分析不符合项是否影响系统的安全保护能力，同时分析系统与其他系统系统边界安全性是否影响系统的安全保护能力，综合测试分析系统的整体安全性是否合理。系统由于运行环境及系统内部结构的关联性，因此需要针对具体的测评单元间的关联关系分析系统整体安全保护能力。具体内容包括：安全控制间安全测评、层面间安全测评、区域间安全测评和系统结构安全测评。**系统整体测评采取风险分析的方式，由测评中心单独完成。**

安全控制间安全测评主要对同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用进行测评，同时，也包括对《基本要求》的要求项与同一区域、同一层面上的非《基本要求》要求的安全控制之间的安全测评。依据不同层面对{系统名称}进行划分，分类分析各个层面中安全控制间存在的关联作用，从系统层面上分析考察单元测评中确定的不符合项对系统整体安全保护能力的影响，及不符合项整改的必要性。

## 安全控制间安全测评

安全控制间安全测评主要对同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用进行测评，同时，也包括对《基本要求》的要求项与同一区域、同一层面上的非《基本要求》要求的安全控制之间的安全测评。依据不同层面对系统进行划分，分类分析各个层面中安全控制间存在的关联作用，从系统层面上分析考察单元测评中确定的不符合项对系统整体安全保护能力的影响，及不符合项整改的必要性。例如：

在物理安全层面中，物理访问控制与防盗窃和防破坏两个控制点之间具有增强的关系，通常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。在网络安全层面中，网络访问控制和边界完整性检查两个控制点之间具有互补和削弱的关系，通常来讲，通过进行边界完整性检查可以检查发现网络访问控制被旁路的可能性。

## 层面间安全测评

层面间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。在进行层面间安全测评时，可以考虑不同层面的两个不同安全控制，也可以同时考虑两个以上不同安全控制的相互作用。对于系统不同层面间相配合的保护措施，需要结合不同层面的安全控制点分析其相互之间存在的关联作用，从而确定某些不符合项对系统整体安全保护能力的影响。例如：

如网络设备防护不符合要求（口令强度不够），该测评项为不符合项，如果网络设备的防护只允许本地登录管理或者限制只能在相应区域内的管理主机上进行网络设备管理，则有可能通过物理安全的访问控制来加强网络设备自身安全防护能力（身份鉴别部分）。

## 区域间安全测评

区域间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。一般边界区域都会和内部某个或某些区域之间发生数据交换；内部不同区域之间也可能因为业务的需要而发生数据交换，需要重点测评这些区域之间的关联作用。

## 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。系统结构安全测评的测评范围是整个信息系统，包括被测系统与其他信息系统系统边界之间的安全测评。信息系统整体结构的安全性主要是指从安全的角度，分析信息系统整体结构的安全性（从安全角度看系统）。整体安全防范的合理性主要是指从系统的角度，分析信息系统安全防范的合理性（以系统的观点看安全防范（体系））。

从系统整体结构层面分析系统的安全防范能力，对于外部安全威胁的防范主要可以从物理环境保护、系统网络访问控制和系统外联边界控制等几个方面考虑：在物理环境层面上，确保系统所在的中心机房的物理安全和物理访问控制，严格限制非法人员直接进入机房环境或非法设备通过机房环境直接连入系统；在系统网络层面上，保证系统网络访问控制能力，限制设备访问，防范非法设备从内部接入系统；在系统外联边界上，通过各种防护手段（防火墙、路由控制等）和限制外联的通路（只存在与其它可控安全系统的连接，不存在直接接入Internet或拨号连出的情况），增强系统的安全保护能力。这几个方面的保护措施相结合，可以对系统进行综合保护，从而确保系统内部安全。整体安全防范的合理性，基于目前部署的安全体系，分析安全设备（如防火墙、防病毒）和安全配置（如访问控制列表）在目前系统中部署是否合理，是否符合成本－效益原则，是否存在重复投资和冗余配置，是否在启用安全措施的同时对系统性能和实际业务需求带来较大负面影响。

# 项目组织

为了保证项目的顺利实施，确保项目质量达到预期目标，XX市第一测评中心将成立项目实施组，以利于加强项目管理和各方面协调合作，使工作和责任更加清晰明确。

项目组组长

质量监督人

技术测试组

管理评估组

渗透测试组

表 8‑1 项目实施组成员表

|  |  |  |  |
| --- | --- | --- | --- |
| **项目组长** |  | **质量监督人** |  |
| **技术测试组人员** |  |
| **管理评估组人员** |  |
| **渗透测试组人员** |  |

**项目组组长：**负责项目具体实施和管理，制定项目实施计划，掌握项目的每个实施过程，解决项目实施中出现的各种具体问题，项目变化的管理，风险管理，与客户进行及时有效的沟通，定期向用户反馈项目进展情况。

**技术测试组：**负责项目具体的技术测试实施，如网络平台测试、系统平台测试、业务应用测试等，定期向测评组组长反馈技术测试进展情况。

**管理评估组：**负责项目具体的安全管理的评估，实施现场访谈、制度核查、执行记录查阅等，定期向测评组组长反馈管理评估进展情况。

**渗透测试组：**负责汇总技术测试中发现的安全隐患，针对发现的安全漏洞，选择适当的攻击工具及方法，模拟入侵行为。

**质量监督人：**对项目实施全过程的质量监控，动态监控质量体系执行情况，对违反质量管理规范的情况提出改进或否决意见，及时出具质量监控报告或意见。

# 配合需求

1. 人员配合要求

表 9‑1 配合人员列表

| **配合项目** | **需求说明** |
| --- | --- |
| 总体协调人 | 能够进行各种工作的跨部门组织协调的人员 |
| 网络管理人员 | 对系统的网络架构、网络设备、安全设备、管理平台部署情况较为熟悉的人员，现场配合检查组中网络组人员完成网络方面的测评和调研工作。 |
| 系统管理人员 | 对系统中的各类主机的操作系统、数据库系统、各类数据备份等情况较为熟悉的人员，现场配合检查组中主机组人员完成主机和部分数据测评工作。 |
| 应用系统开发/运维人员 | 负责各类应用系统情况、熟悉各类应用在系统中实际部署情况的人员，现场配合检查组中应用组人员完成应用的检查工作。 |
| 机房管理人员 | 负责机房管理的人员，现场配合检查组中管理组完成物理安全测评工作。 |
| 安全文档维护人员 | 对所有相关的文档进行整理和管理的人员，现场配合检查组中管理组完成管理测评工作。 |

1. 扫描测试配合要求

表 9‑2 扫描测试配合要求列表

| **配合项目** | **需求说明** |
| --- | --- |
| 配合人员 | 网络管理员，提供：1、（对于每个接入点）可用的以太网电口以及对应的合法IP地址；2、监控网络设备的运行状态。 |
| 主机及业务应用管理员，负责在漏洞扫描期间监控相关主机以及业务应用的运行状态。 |
| 安全权限 | 如接入测评设备时需出入机房，则需要测评人员在测评实施期间出入机房的许可。 |
| 针对 WEB 扫描，需要能够访问目标应用所有应用页面的用户权限。 |

1. 文档资料配合要求

表 9‑3 文档资料配合要求列表

| **文档名称** | **具体说明** |
| --- | --- |
| 各类管理制度文档 | 管理制度、工作单 |
| 其他文档 | 应用系统设计、开发文档 |

4) 现场工作环境配合要求

* 相对独立的办公环境，可以容纳 6-8 人左右；
* 工具测试接入及办公电脑互联网接入；
* 提供一个保险柜，用于保存工作中的各类过程文档，以防止丢失；
* 提供一台打印机和打印纸，以便文档的输出。