**目录**

1. [概述 1](#_bookmark0)
   1. [项目简介 1](#_bookmark1)
   2. [被测单位基本情况介绍 1](#_bookmark2)
   3. [测评范围 2](#_bookmark3)
   4. [测评依据及规范 2](#_bookmark4)
2. [被测对象描述 2](#_bookmark5)
   1. [定级结果 2](#_bookmark6)
   2. [业务和采用的技术 3](#_bookmark7)
   3. [网络结构 3](#_bookmark8)
   4. [被测对象资产 4](#_bookmark9)
      1. [物理机房 *4*](#_bookmark10)
      2. [网络设备 *4*](#_bookmark11)
      3. [安全设备 *4*](#_bookmark12)
      4. [服务器/存储设备 *5*](#_bookmark13)
      5. [终端/现场设备 *5*](#_bookmark14)
      6. [系统管理软件/平台 *5*](#_bookmark15)
      7. [业务应用系统/平台 *5*](#_bookmark16)
      8. [数据类别 *6*](#_bookmark17)
      9. [安全相关人员 *6*](#_bookmark18)
      10. [安全管理文档 *6*](#_bookmark19)
3. [测评对象和测评指标 8](#_bookmark20)
   1. [测评对象 8](#_bookmark21)
      1. [物理机房 *8*](#_bookmark22)
      2. [网络设备 *8*](#_bookmark23)
      3. [安全设备 *9*](#_bookmark24)
      4. [服务器/存储设备 *9*](#_bookmark25)
      5. [终端/现场设备 *9*](#_bookmark26)
      6. [系统管理软件/平台 *10*](#_bookmark27)
      7. [业务应用系统/平台 *10*](#_bookmark28)
      8. [数据类别 *10*](#_bookmark29)
      9. [安全相关人员 *10*](#_bookmark30)
      10. [安全管理文档 *10*](#_bookmark31)
   2. [测评指标选择 11](#_bookmark32)
      1. [安全通用要求指标 *11*](#_bookmark33)
      2. [不适用安全要求指标 *14*](#_bookmark36)
4. [测评方法与工具 14](#_bookmark37)
   1. [测评方法 26](#_bookmark38)

[4.1.1 访谈 *26*](#_bookmark39)

[4.1.2 核查 *26*](#_bookmark40)

[***4.1.3 测试*** *26*](#_bookmark41)

1. [**测评内容与实施 28**](#_bookmark42)
   1. [**安全物理环境测评** 28](#_bookmark43)
   2. [**安全通信网络测评** 29](#_bookmark44)
   3. [**安全区域边界测评** 30](#_bookmark45)
   4. [**安全计算环境测评** 31](#_bookmark46)
   5. [**安全管理中心测评** 32](#_bookmark47)
   6. [**安全管理制度测评** 32](#_bookmark48)
   7. [**安全管理机构测评** 33](#_bookmark49)
   8. [**安全管理人员测评** 33](#_bookmark50)
   9. [**安全建设管理测评** 34](#_bookmark51)
   10. [**安全运维管理测评** 35](#_bookmark52)
   11. [**云计算安全测评** 36](#_bookmark53)
2. [**工具测试 38**](#_bookmark54)
   1. [**漏洞扫描方案** 38](#_bookmark55)
      1. [***漏洞扫描工具*** *38*](#_bookmark56)
      2. [***工具测试接入点说明*** *38*](#_bookmark57)
      3. [***漏洞扫描范围*** *38*](#_bookmark58)
      4. [***漏洞扫描时间*** *39*](#_bookmark59)
3. [**现场测评风险规避措施 40**](#_bookmark60)
4. [**现场测评工作计划 41**](#_bookmark61)
   1. [**测评项目组成员及分工** 41](#_bookmark62)
   2. [**现场测评实施计划** 41](#_bookmark63)
   3. [**人员配合要求** 44](#_bookmark64)
   4. [**现场工作环境配合要求** 45](#_bookmark65)

# 概述

## 项目简介

根据《中华人民共和国计算机信息系统安全保护条例》、《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护管理规定》等政策法规及文件要求，定级为第二级的 XXX 大学全流程数字化业务系统计划进行等级保护专项测评。为了持续有效提高 XXX 大学全流程数字化业务系统的安全防护能力，受 XXX 大学委托，计划于 2020 年 10 月 26 日起对“XXX 大学全流程数字化业务系统”进行网络安全等级测评。旨在通过本次安全等级测评，检测“XXX 大学全流程数字化业务系统”是否符合《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）对应安全等级的相关要求，指出“XXX 大学全流程数字化业务系统”存在的安全问题并提出相应的整改建议，为XXX 大学进一步完善“XXX 大学全流程数字化业务系统”的安全管理体系、加强“XXX 大学全流程数字化业务系统”的安全防护措施提供依据，为等级保护工作的进一步开展提供指导。

## 被测单位基本情况介绍

“XXX 大学全流程数字化业务系统”主要面向学校教职工，提供采购计划申报审批、采购立项、采购执行管理、合同管理、外贸进口业务、采购监督管理、统计归档管理等功能。

“XXX 大学全流程数字化业务系统”采用 B/S 架构部署在本地机房，使用

HTTPS 协议进行数据传输，保证通信过程中数据的完整性。

XXX 大学《信息安全策略》为网络安全方针和策略文件，明确了网络安全的总目标、原则和安全框架等内容；已编制《国有资产管理办法》《数据备份与恢复管理规定》、《校园网核心机房管理办法》、《网络和信息安全事件应急预案》等管理制度， 管理制度已覆盖网络、主机、系统、数据、应用层面。

## 测评范围

根据“XXX 大学全流程数字化业务系统”等级备案资料中提出的安全域划分方法，并考虑到系统主管和运营单位的有效管理控制范围和安全责任范围，本次安全等级测评的范围选定为“XXX 大学全流程数字化业务系统”所经过网络边界以内的网络及设备。

## 测评依据及规范

测评过程中主要依据的标准和文件如下：

* + - GB/T 17859-1999 《信息安全技术 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 25058-2019《信息安全技术 网络安全等级保护实施指南》
    - 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》
    - 《中华人民共和国网络安全法》(自 2017 年 6 月 1 日起施行)
    - 《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）
    - 《信息安全等级保护管理办法》（公通字〔2007〕43 号）

# 被测对象描述

## 定级结果

表 2- 1【XXX 大学全流程数字化业务系统】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** |
| XXX 大学全流程数字化业务系统 | 第二级 | 第二级 | 第二级 |

## 业务和采用的技术

“XXX 大学全流程数字化业务系统”主要承载的业务是：为 XXX 大学提供招标采购服务，其服务范围为本校内部教师职工等。

“XXX 大学全流程数字化业务系统”采用 B/S 架构部署，使用 HTTPS 协议进行数据传输，保证通信过程中数据的完整性。

## 网络结构

拓扑图描述：

外联区：采用堆叠技术部署两台迪普防火墙设备，实现数据接入和访问控制功能。

核心区：部署两台华为核心交换机，两台交换机以堆叠方式部署，提高了核心区数据交换能力。

DMZ 区：主要部署一台启明星辰 Web 应用防火墙和反代服务器，为外部访问用户提供 Web 服务。

安全监控区：主要部署网康上网行为管理设备和启明星辰入侵检测设备，实现上网行为监控和入侵攻击行为检测的功能。

运维管理区：主要部署华三接入交换机、网瑞达堡垒机、铱讯漏洞扫描设备、网瑞达日志审计设备，实现运维管理、漏洞扫描和日志审计功能。

服务器区：主要部署华三汇聚交换机、启明星辰服务器区防火墙、华三服务器接入交换机和应用服务器、数据库服务器，实现应用层防护、业务数据处理等功能。

办公区：主要部署华三接入交换机以及办公终端，实现终端接入、运维操作等功能。

拓扑图：

图 2- 1XXX 大学全流程数字化业务系统网络拓扑图

## 被测对象资产

### 物理机房

表 2- 2 物理机房

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **机房名称** | **物理位置** | **重要程度** |
| 1 | 某校区信息中心机房 | XXX | 非常重要 |
| 2 | 某校区信息中心机房 | XXX | 非常重要 |

### 网络设备

表 2- 3 网络设备

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚**  **拟设备** | **系统及版本** | **品牌及型号** | **用途** | **IP 地址** | **重要**  **程度** |
| 1 | 核心交换机 | × | XXX | XXX | 数据交换 | XXX | 非常  重要 |
| 2 | 某校区汇聚  交换机 | × | XXX | XXX | 数据交换 | XXX | 非常  重要 |
| 3 | 服务器接入  交换机 | × | XXX | XXX | 数据交换 | XXX | 非常  重要 |
| 4 | 办公区接入  交换机 | × | XXX | XXX | 数据交换 | XXX | 重要 |
| 5 | 运维区接入  交换机 | × | XXX | XXX | 数据交换 | XXX | 重要 |

### 安全设备

表 2- 4 安全设备

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚**  **拟设备** | **系统及版本** | **品牌及**  **型号** | **用途** | **IP 地址** | **重要**  **程度** |
| 1 | 出口防火墙 | × | XXX | XXX | 访问控制、入侵防  御、防病毒 | XXX | 非常  重要 |
| 2 | 上网行为管理 | × | XXX | XXX | 上网行为管控 | XXX | 非常  重要 |
| 3 | 入侵检测 | × | XXX | XXX | 入侵行为检测 | XXX | 非常重要 |
| 4 | 服务器区防火  墙 | × | XXX | XXX | 访问控制 | XXX | 非常  重要 |
| 5 | Web 应用防火  墙 | × | XXX | XXX | 应用层防护 | XXX | 非常重要 |
| 6 | 堡垒机 | × | XXX | XXX | 运维管理 | XXX | 非常  重要 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚**  **拟设备** | **系统及版本** | **品牌及**  **型号** | **用途** | **IP 地址** | **重要**  **程度** |
| 7 | 漏洞扫描 | × | XXX | XXX | 漏洞扫描 | XXX | 重要 |
| 8 | 日志审计 | × | XXX | XXX | 运维管理 | XXX | 重要 |

### 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** | **是否虚拟设备** | **操作系统及版本** | **数据库管理系统及**  **版本** | **中间件及版本** | **IP 地址** | **重要程度** |
| 1 | 应用服务器 | XXX 大学  全流程数字  化业务系统 | × | XXX | - | Tomcat V8.0 | XXX | 非常重要 |
| 2 | 数据库服务器 | XXX 大学  全流程数字  化业务系统 | × | XXX | Oracle 11 | - | XXX | 非常重要 |
| 3 | 反代服务器 | XXX 大学  全流程数字  化业务系统 | × | XXX | - | Nginx V1.18 | XXX | 非常重要 |

### 终端/现场设备

表 2- 6 终端/现场设备

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚**  **拟设备** | **操作系统/控**  **制软件及版本** | **设备类别/用途** | **IP 地址** | **重要**  **程度** |
| 1 | 运维终端 | × | Windows 10 专  业版 | 运维管理 | XXX | 一般 |

### 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** | **版本号** | **主要功能** | **URI/API/APK** | **重要程度** |
| 1 | 数据库系统 | 数据库  服务器 | XXX | 数据处理与存储 | - | 非常重要 |

### 业务应用系统/平台

表 2- 8 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** | **URI/A PI/APK** | **重要程度** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | XXX 大学全流程数字化业务系统 | 主要面向学校教职工，提供采购计划申报审批、采购立项、采购执行管理、合同管理、外贸进口业务、采购监督管理、统计归档  管理等功能。 | XXX | XXX | XXX | 非常重要 |
| 2 | Nginx 中  间件 | 数据代理 | XXX | XXX | XXX | 重要 |
| 3 | Tomcat | Web 服务支撑 | XXX | XXX | XXX | 重要 |

### 数据类别

表 2- 9-a 关键数据类别

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| 1 | 用户数据 | XXX 大学全流程数字化业务系统 | 保密性、完整性 |
| 2 | 业务数据 | XXX 大学全流程数字化业务系统 | 保密性、完整性 |
| 3 | 管理数据 | XXX 大学全流程数字化业务系统 | 完整性 |
| 4 | 审计数据 | XXX 大学全流程数字化业务系统 | 完整性 |

### 安全相关人员

表 2- 11 安全相关人员

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **姓名** | **岗位/角色** | **联系方式** |
| 1 | XXX | XXX | XXX |
| 2 | XXX | XXX | XXX |
| 3 | XXX | XXX | XXX |
| 4 | XXX | XXX | XXX |

### 安全管理文档

表 2- 12 安全管理文档

|  |  |  |
| --- | --- | --- |
| **序号** | **文档名称** | **主要内容** |
| 1 | 《信息安全策略》 | 机构总体安全方针和政策方面的管理制度。 |
| 2 | 《教职工招聘和考核管理  办法》 | 关于员工招聘和考核的管理制度。 |
| 3 | 《校园网核心机房管理办  法》 | 关于校园网核心机房环境、消防、操作等方面的管理  制度。 |
| 4 | 《恶意代码（病毒）防范  管理制度》 | 外来人员病毒防范、内部人员病毒防范方面的管理制  度。 |
| 5 | 《安全方案设计管理制  度》 | 安全技术框架、总体建设规划和详细设计、方案工程  实施过程管理方面的管理制度。 |
| 6 | 《变更管理制度》 | 系统变更申报、审批、制度变更方案等方面的管理制  度。 |
| 7 | 《数据备份与恢复管理规 | 关于数据备份和恢复工作流程的管理制度。 |

|  |  |  |
| --- | --- | --- |
| **序号** | **文档名称** | **主要内容** |
|  | 定》 |  |
| 8 | 《网络安全监测预警通报  工作制度》 | 关于安全事件监测、预警、应急演练等方面的管理制  度。 |
| 9 | 《网络安全事件应急处理  流程》 | 启动预案的条件、应急组织构成、应急资源保障、事  后教育和 培训等方面的文件。 |
| 10 | 《机房进入申请》 | 机房进入申请记录。 |
| 11 | 《XXX 大学网站（信息服  务申请备案表）》 | 外部人员接入受控网络申请记录。 |
| 12 | 《信息系统安全等级保护  定级报告》 | 信息系统定级报告。 |
| 13 | 《专家评审意见》 | 信息系统定级专家评审意见。 |
| 14 | 《上线实施计划》 | 被测评系统上线实施计划。 |
| 15 | 《全流程数字化业务系统  操作手册》 | 被测评系统前端用户使用手册。 |
| 16 | 《巡检业务单》 | 机房巡检记录。 |
| 17 | 《安全域划分规范》 | 安全于划分操作手册。 |
| 18 | 《防火墙策略配置要求》 | 防火墙策略配置操作手册。 |
| 19 | 《终端安全管理规范》 | 终端操作手册。 |
| 20 | 《信息系统应急预案》 | 信息系统应急预案。 |
| 21 | 《网络和信息安全事件应  急预案》 | 网络和信息安全事件应急预案 |
| 22 | 《校园网应急预案》 | 校园网应急预案。 |
| 23 | 《培训记录》 | 应急预案培训记录。 |

# 测评对象和测评指标

## 测评对象

依据《测评要求》、《测评过程指南》和《报告模板》，信息系统的构成要素包括物理机房、业务应用系统/平台、服务器/存储设备、终端/现场设备、系统管理软件/平台、网络互联设备、安全设备等。本次测评依据相关标准的要求，结合被测信息系统的拓扑结构和业务应用的具体情况，遵循如下原则进行测评对象抽查：

1. 完整性原则，选择的设备、机制等应能满足相应等级的测评强度要求；
2. 重要性原则，抽查重要的服务器、数据库和网络设备等；
3. 安全性原则，抽查对外暴露的网络边界；
4. 共享性原则，抽查共享设备和数据交换平台/设备；
5. 代表性原则，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的类型。

### 物理机房

表 3- 1 物理机房

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **机房名称** | **物理位置** | **重要程度** |
| 1 | 某校区信息中心机房 | XXX | 非常重要 |
| 2 | 某校区信息中心机房 | XXX | 非常重要 |

### 网络设备

表 3- 2 网络设备

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚**  **拟设备** | **系统及版本** | **品牌及型号** | **用途** | **IP 地址** | **重要**  **程度** |
| 1 | 核心交换机 | × | XXX | XXX | 数据交换 | XXX | 非常  重要 |
| 2 | 某校区汇聚交换机 | × | XXX | XXX | 数据交换 | XXX | 非常重要 |
| 3 | 服务器接入  交换机 | × | XXX | XXX | 数据交换 | XXX | 非常  重要 |
| 4 | 办公区接入  交换机 | × | XXX | XXX | 数据交换 | XXX | 重要 |
| 5 | 运维接入交  换机 | × | XXX | XXX | 数据交换 | XXX | 重要 |

### 安全设备

表 3- 3 安全设备

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚**  **拟设备** | **系统及版本** | **品牌及**  **型号** | **用途** | **IP 地址** | **重要**  **程度** |
| 1 | 出口防火墙 | × | XXX | XXX | 访问控制、入侵防御、  防病毒 | XXX | 非常重要 |
| 2 | 上网行为管理 | × | XXX | XXX | 上网行为管  控 | XXX | 非常  重要 |
| 3 | 入侵检测 | × | XXX | XXX | 入侵行为检  测 | XXX | 非常  重要 |
| 4 | 服务器区防火  墙 | × | XXX | XXX | 访问控制 | XXX | 非常  重要 |
| 5 | Web 应用防火  墙 | × | XXX | XXX | 应用层防护 | XXX | 非常重要 |
| 6 | 堡垒机 | × | XXX | XXX | 运维管理 | XXX | 非常  重要 |
| 7 | 漏洞扫描 | × | XXX | XXX | 漏洞扫描 | XXX | 重要 |
| 8 | 日志审计 | × | XXX | XXX | 运维管理 | XXX | 重要 |

### 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** | **是否虚拟设备** | **操作系统及版本** | **数据库管理系统及**  **版本** | **中间件及版本** | **IP 地址** | **重要程度** |
| 1 | 应用服务器 | XXX 大学  全流程数字  化业务系统 | × | XXX | XXX | Tomcat V8.0 | XXX | 非常重要 |
| 2 | 数据库服务器 | XXX 大学  全流程数字  化业务系统 | × | XXX | XXX | - | XXX | 非常重要 |
| 3 | 反代服务器 | XXX 大学  全流程数字  化业务系统 | × | XXX | XXX | Nginx V1.18 | XXX | 非常重要 |

### 终端/现场设备

表 3- 5 终端/现场设备

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **是否虚**  **拟设备** | **操作系统/控**  **制软件及版本** | **设备类别/用途** | **IP 地址** | **重要**  **程度** |
| 1 | 运维终端 | × | XXX | XXX | XXX | 一般 |

### 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** | **版本号** | **主要功能** | **URI/API/APK** | **重要程度** |
| 1 | 数据库系统 | 数据库  服务器 | XXX | XXX | XXX | 非常重要 |

### 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** | **URI/A PI/APK** | **重要程度** |
| 1 | XXX 大学  全流程数  字化业务系统 | 主要面向学校教职工，提供采购计划申报审批、采购立项、采购执行管理、合同管理、外贸进口业务、采购监督  管理、统计归档管理等功能。 | XXX | XXX | XXX | 非常重要 |
| 2 | Nginx 中  间件 | 数据代理 | XXX | XXX | XXX | 重要 |
| 3 | Tomcat | Web 服务支撑 | XXX | XXX | XXX | 重要 |

### 数据类别

表 3- 8-a 关键数据类别

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| 1 | 用户数据 | XXX 大学全流程数字化业务系统 | 保密性、完整性 |
| 2 | 业务数据 | XXX 大学全流程数字化业务系统 | 保密性、完整性 |
| 3 | 管理数据 | XXX 大学全流程数字化业务系统 | 完整性 |
| 4 | 审计数据 | XXX 大学全流程数字化业务系统 | 完整性 |

### 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** |
| 1 | XXX | XXX | XXX |
| 2 | XXX | XXX | XXX |
| 3 | XXX | XXX | XXX |
| 4 | XXX | XXX | XXX |

### 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** |
| 1 | 《信息安全策略》 | 机构总体安全方针和政策方面的管理制度。 |
| 2 | 《教职工招聘和考核管理  办法》 | 关于员工招聘和考核的管理制度。 |
| 3 | 《校园网核心机房管理办  法》 | 关于校园网核心机房环境、消防、操作等方面的管理  制度。 |
| 4 | 《恶意代码（病毒）防范  管理制度》 | 外来人员病毒防范、内部人员病毒防范方面的管理制  度。 |
| 5 | 《安全方案设计管理制  度》 | 安全技术框架、总体建设规划和详细设计、方案工程  实施过程管理方面的管理制度。 |
| 6 | 《变更管理制度》 | 系统变更申报、审批、制度变更方案等方面的管理制  度。 |
| 7 | 《数据备份与恢复管理规  定》 | 关于数据备份和恢复工作流程的管理制度。 |
| 8 | 《网络安全监测预警通报  工作制度》 | 关于安全事件监测、预警、应急演练等方面的管理制  度。 |
| 9 | 《网络安全事件应急处理  流程》 | 启动预案的条件、应急组织构成、应急资源保障、事  后教育和 培训等方面的文件。 |
| 10 | 《机房进入申请》 | 机房进入申请记录。 |
| 11 | 《XXX 大学网站（信息服  务申请备案表）》 | 外部人员接入受控网络申请记录。 |
| 12 | 《信息系统安全等级保护  定级报告》 | 信息系统定级报告。 |
| 13 | 《专家评审意见》 | 信息系统定级专家评审意见。 |
| 14 | 《上线实施计划》 | 被测评系统上线实施计划。 |
| 15 | 《全流程数字化业务系统  操作手册》 | 被测评系统前端用户使用手册。 |
| 16 | 《巡检业务单》 | 机房巡检记录。 |
| 17 | 《安全域划分规范》 | 安全于划分操作手册。 |
| 18 | 《防火墙策略配置要求》 | 防火墙策略配置操作手册。 |
| 19 | 《终端安全管理规范》 | 终端操作手册。 |
| 20 | 《信息系统应急预案》 | 信息系统应急预案。 |
| 21 | 《网络和信息安全事件应  急预案》 | 网络和信息安全事件应急预案 |
| 22 | 《校园网应急预案》 | 校园网应急预案。 |
| 23 | 《培训记录》 | 应急预案培训记录。 |

## 测评指标选择

### 安全通用要求指标

测评指标暂定选取 GB/T 22239-2019《信息安全技术网络安全等级保护基本要

求》中二级系统基本要求指标，包括二级通用指标类（G2），业务信息安全性指标类

（S2），业务服务保证类（A2），安全控制指标如下表：

表 3- 11 安全通用要求指标

|  |  |  |
| --- | --- | --- |
| **安全类**[**1**](#_bookmark34) | **安全控制点**[**2**](#_bookmark35) | **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 | 2 |
| 防雷击 | 1 |
| 防火 | 2 |
| 防水和防潮 | 2 |
| 防静电 | 1 |
| 温湿度控制 | 1 |
| 电力供应 | 2 |
| 电磁防护 | 1 |
| 安全通信网络 | 网络架构 | 2 |
| 通信传输 | 1 |
| 可信验证 | 1 |
| 安全区域边界 | 边界防护 | 1 |
| 访问控制 | 4 |
| 入侵防范 | 1 |
| 恶意代码和垃圾邮件防范 | 1 |
| 安全审计 | 3 |
| 可信验证 | 1 |
| 安全计算环境 | 身份鉴别 | 3 |
| 访问控制 | 4 |

1 安全类对应基本要求中的安全物理环境、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、安全建设管理和安全运维管理等 10 个安全要求类别。

2安全控制点是对安全类的进一步细化，在《基本要求》目录级别中对应安全类的下一级目录。

|  |  |  |
| --- | --- | --- |
| **安全类1** | **安全控制点2** | **测评项数** |
|  | 安全审计 | 3 |
| 入侵防范 | 5 |
| 恶意代码防范 | 1 |
| 可信验证 | 1 |
| 数据完整性 | 1 |
| 数据备份恢复 | 2 |
| 剩余信息保护 | 1 |
| 个人信息保护 | 2 |
| 安全管理中心 | 系统管理 | 2 |
| 审计管理 | 2 |
| 安全管理制度 | 安全策略 | 1 |
| 管理制度 | 2 |
| 制定和发布 | 2 |
| 评审和修订 | 1 |
| 安全管理机构 | 岗位设置 | 2 |
| 人员配备 | 1 |
| 授权和审批 | 2 |
| 沟通和合作 | 3 |
| 审核和检查 | 1 |
| 安全管理人员 | 人员录用 | 2 |
| 人员离岗 | 1 |
| 安全意识教育和培训 | 1 |
| 外部人员访问管理 | 3 |
| 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 | 2 |
| 自行软件开发 | 2 |

|  |  |  |
| --- | --- | --- |
| **安全类1** | **安全控制点2** | **测评项数** |
|  | 外包软件开发 | 2 |
| 工程实施 | 2 |
| 测试验收 | 2 |
| 系统交付 | 3 |
| 等级测评 | 3 |
| 服务供应商选择 | 2 |
| 安全运维管理 | 环境管理 | 3 |
| 资产管理 | 1 |
| 介质管理 | 2 |
| 设备维护管理 | 2 |
| 漏洞和风险管理 | 1 |
| 网络和系统安全管理 | 5 |
| 恶意代码防范管理 | 3 |
| 配置管理 | 1 |
| 密码管理 | 2 |
| 变更管理 | 1 |
| 备份与恢复管理 | 3 |
| 安全事件处置 | 3 |
| 应急预案管理 | 2 |
| 外包运维管理 | 2 |
| **安全通用要求指标数量统计** | | 135 |

### 不适用安全要求指标

表 3- 12 不适用安全要求指标

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
| **安全通用要求** | | | | |
| 安全计算环境 | 入侵防范 | a）应遵循最小 | 核心交换机 | 经检查，网络设备 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 安装的原则，仅安装需要的组 件和应用程序； |  | 不涉及组件和程序安装，此项为不适用。 |
| 某校区汇聚交换机 | 经检查，网络设备不涉及组件和程序安装，此项为不适用。 |
| 服务器接入交换机 | 经检查，网络设备不涉及组件和程序安装，此项为不适用。 |
| 办公区接入交换机 | 经检查，网络设备不涉及组件和程序安装，此项为不适用。 |
| 运维接入交换机 | 经检查，网络设备不涉及组件和程序安装，此项为不适用。 |
| 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； | 核心交换机 | 此设备为交换机设备，此项为不适用。 |
| 某校区汇聚交换机 | 此设备为交换机设备，此项为不适用。 |
| 服务器接入交换机 | 此设备为交换机设备，此项为不适用。 |
| 办公区接入交换机 | 此设备为交换机设备，此项为不适用。 |
| 运维接入交换机 | 此设备为交换机设备，此项为不适用。 |
| a）应遵循最小安装的原则，仅 | 出口防火墙 | 经检查，安全设备不涉及组件和程 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 安装需要的组件和应用程序； |  | 序安装，此项为不适用。 |
| 上网行为管理 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 入侵检测 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 内网防火墙 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| Web 应用防火墙 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 堡垒机 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 漏洞扫描 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 日志审计 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| b）应关闭不需要的系统服务、默认共享和高 危端口； | 出口防火墙 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 上网行为管理 | 经检查，安全设备不涉及组件和程序安装，此项为不 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  |  |  | 适用。 |
| 入侵检测 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 内网防火墙 | 经检查，安全设备不涉及系统服务、默认共享和高危 端口，此项为不适用。 |
| Web 应用防火墙 | 此设备为安全设备，此项为不适用。 |
| 堡垒机 | 此设备为安全设备，此项为不适用。 |
| 漏洞扫描 | 经检查，安全设备不涉及组件和程序安装，此项为不适用。 |
| 日志审计 | 此设备为安全设备，此项为不适用。 |
| 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； | 出口防火墙 | 此设备为安全设备，此项为不适用。 |
| 上网行为管理 | 此设备为安全设备，此项为不适用。 |
| 入侵检测 | 此设备为安全设备，此项为不适用。 |
| 内网防火墙 | 此设备为安全设备，此项为不适用。 |
| Web 应用防火墙 | 此设备为安全设 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  |  |  | 备，此项为不适用。 |
| 堡垒机 | 此设备为安全设备，此项为不适用。 |
| 漏洞扫描 | 此设备为安全设备，此项为不适用。 |
| 日志审计 | 此设备为安全设备，此项为不适用。 |
| 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。 | 内网防火墙 | 此设备为安全设备，此项为不适用。 |
| 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； | 内网防火墙 | 此设备为安全设备，此项为不适用。 |
| 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。 | 内网防火墙 | 此设备为安全设备，此项为不适用。 |
| 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； | Nginx 中间件 | Nginx 软件自身不带身份鉴别功能， 故此项调整为不 适用。 |
| Tomcat | Tomcat 的身份鉴别功能由操作系统实现，故此项调整为不适用。 |
| b）应具有登录失败处理功能， 应配置并启用 结束会话、限制 | Nginx 中间件 | Nginx 软件自身不带身份鉴别功能， 故此项调整为不 适用。 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 非法登录次数和当登录连接超时自动退出等相关措施； | Tomcat | Tomcat 的身份鉴别功能由操作系统实现，故此项调整为不适用。 |
| 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。 | Nginx 中间件 | Nginx 软件自身不涉及用户登录，故此项调整为不适用。 |
| Tomcat | Tomcat 的身份鉴别功能由操作系统实现，故此项调整为不适用。 |
| 访问控制 | a）应对登录的用户分配账户和权限； | Nginx 中间件 | Nginx 软件自身不带身份鉴别功能， 故此项调整为不 适用。 |
| Tomcat | Tomcat 为中间件， 不涉及访问控制， 故此项调整为不 适用。 |
| b）应重命名或删除默认账户， 修改默认账户 的默认口令； | Nginx 中间件 | Nginx 软件自身不涉及用户登录，故此项调整为不适用。 |
| Tomcat | Tomcat 为中间件不涉及该问题，故此项调整为不适用。 |
| 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； | Nginx 中间件 | Nginx 软件自身不涉及用户登录，故此项调整为不适用。 |
| Tomcat | Tomcat 为中间件不涉及该问题，故此项调整为不适用。 |
| d）应授予管理 | Nginx 中间件 | Nginx 软件自身不 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 用户所需的最小权限，实现管理用户的权限分离。 |  | 涉及用户登录，故此项调整为不适用。 |
| Tomcat | Tomcat 为中间件不涉及该问题，故此项调整为不适用。 |
| 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； | XXX 大学全流程数字化业务系统 | 被测对象为应用系统，此项为不适用。 |
| b）应关闭不需要的系统服务、默认共享和高 危端口； | XXX 大学全流程数字化业务系统 | 被测对象为应用系统，此项为不适用。 |
| 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； | XXX 大学全流程数字化业务系统 | 被测对象为应用系统，此项为不适用。 |
| 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。 | XXX 大学全流程数字化业务系统 | 被测对象为应用系统，此项为不适用。 |
| Nginx 中间件 | Nginx 不涉及重要业务数据，故此项为不适用。 |
| Tomcat | Tomcat 为中间件不涉及该问题，故此项调整为不适用。 |
| 数据完整性 | a）应采用校验技术保证重要数据在传输过 | Nginx 中间件 | Nginx 不涉及重要业务数据，故此项为不适用。 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 程中的完整性。 | Tomcat | Tomcat 为中间件不涉及该问题，故此项调整为不适用。 |
| 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。 | Nginx 中间件 | Nginx 不涉及重要业务数据，故此项为不适用。 |
| Tomcat | Tomcat 为中间件不涉及该问题，故此项调整为不适用。 |
| 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； | XXX 大学全流程数字化业务系统 | 应用系统不采集个人信息，此项为不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | XXX 大学全流程数字化业务系统 | 应用系统不采集个人信息，此项为不适用。 |
| 入侵防范 | 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； | 应用服务器 | 测评对象为服务器，故此项调整为不适用。 |
| 数据库服务器 | 测评对象为服务器，故此项调整为不适用。 |
| 反代服务器 | 测评对象为服务器，故此项调整为不适用。 |
| 身份鉴别 | 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。 | 运维终端 | 运维终端已禁止远程登录功能，故此项调整为不适用。 |
| 入侵防范 | c）应通过设定终端接入方式或网络地址范 | 运维终端 | 测评对象为运维终端，只可本地访问，故此项调整为 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 围对通过网络进行管理的管理终端进行限制； |  | 不适用。 |
| 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； | 运维终端 | 测评对象为运维终端，故此项调整为不适用。 |
| 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。 | 运维终端 | 测评对象为运维终端，故此项调整为不适用。 |
| 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； | 运维终端 | 测评对象为运维终端，故此项调整为不适用。 |
| 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。 | 运维终端 | 测评对象为运维终端，故此项调整为不适用。 |
| 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； | 数据库系统 | 测评对象为数据库，故此项调整为不适用。 |
| b）应关闭不需要的系统服务、默认共享和高 危端口； | 数据库系统 | 测评对象为数据库，故此项调整为不适用。 |
| d）应提供数据有效性检验功能，保证通过人机接口输入或 | 数据库系统 | 测评对象为数据库，故此项调整为不适用。 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 通过通信接口输入的内容符合系统设定要求； |  |  |
| 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。 | 数据库系统 | 被测对象为数据库系统，此项为不适用。 |
| 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； | 数据库系统 | 被测系统不采集个人信息，此项为不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 数据库系统 | 被测系统不采集个人信息，此项为不适用。 |
| 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。 | 审计数据 | 审计数据不涉及鉴别信息，故此项为不适用。 |
| 管理数据 | 管理数据不涉及鉴别信息，故此项为不适用。 |
| 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； | 用户数据 | 应用系统不采集用户个人信息，故不适用。 |
| 业务数据 | 应用系统不采集用户个人信息，故不适用。 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  |  | 审计数据 | 应用系统不采集用户个人信息，故不适用。 |
| 管理数据 | 应用系统不采集用户个人信息，故不适用。 |
| b）应禁止未授权访问和非法使用用户个人信息。 | 用户数据 | 应用系统不采集用户个人信息，故不适用。 |
| 业务数据 | 应用系统不采集用户个人信息，故不适用。 |
| 审计数据 | 应用系统不采集用户个人信息，故不适用。 |
| 管理数据 | 应用系统不采集用户个人信息，故不适用。 |
| 安全建设管理 | 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； | 安全建设管理 | 经核查，全流程数字化业务系统为外包开发，不涉及自行软件开发，故此项为不适用。 |
| b）应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。 | 安全建设管理 | 经核查，全流程数字化业务系统为外包开发，不涉及自行软件开发，故此项为不适用。 |
| 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； | 安全建设管理 | 经核查，本次测评为全流程数字化业务系统首次测评，故此项为不适用。 |
| b）应在发生重 | 安全建设管理 | 经核查，测全流程 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 大变更或级别发生变化时进行等级测评； |  | 数字化业务系统 未发生重大变更 或级别发生变化， 故此项为不适用。 |
| 安全运维管理 | 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； | 安全运维管理 | 经核查，被测系统为自运维，故此项为不适用。 |
| 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。 | 安全运维管理 | 经核查，被测系统为自运维，故此项为不适用。 |
| **表中不适用指标数量** | | | | 94 |

# 测评方法与工具

## 测评方法

本次等级测评现场实施过程中将综合采用访谈、核查和测试等测评方法。

### 访谈

访谈是指测评人员通过引导等级保护对象相关人员进行有目的的（有针对性的） 交流以帮助测评人员理解、澄清或取得证据的过程。在访谈的范围上，应基本覆盖 所有的安全相关人员类型，在数量上可以抽样。

### 核查

核查是指测评人员通过对测评对象（如制度文档、各类设备及相关安全配置等） 进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

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

在安全计算环境、安全通信网络、安全区域边界测评任务中，测评人员综合采用文档查阅与分析和安全配置核查等检查方法来获取测评证据（如相关措施的部署和配置情况，特定设备的端口开放情况等），用于判断目标系统在相应安全类采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。

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

### 测试

测试是指测评人员使用预定的方法／工具使测评对象（各类设备或安全配置） 产生特定的结果，将运行结果与预期的结果进行比对的过程。在本次测评过程中， 测试方法主要应用在手工验证、漏洞扫描、渗透测试等测评任务中。

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

在本次测试中，主要采用绿盟远程安全评估系统（NSFOCUS Remote Security Assessment System 简称：NSFOCUS RSAS）进行辅助测试。采用漏洞扫描和渗透测试两种方法完成此次测评的工具测试。

# 测评内容与实施

本次等级测评的现场实施过程由单元测评和整体测评两部分构成。

对应《基本要求》各安全控制点的测评称为单元测评，具体可分为安全物理环境、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 10 个测评任务。

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。

## 安全物理环境测评

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

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。安全物理环境测评具体测评指标描述如下表所示。

表 5- 1 安全物理环境测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 物理位置的选择 | 通过访谈物理安全负责人，检查机房，测评机房物理场所在 位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
| 2 | 物理访问控制 | 检查机房出入口等过程，测评信息系统在物理访问控制方面 的安全防范能力。 |
| 3 | 防盗窃和防破坏 | 检查机房内的主要设备、介质和防盗报警设施等过程，测评 信息系统是否采取必要的措施预防设备、介质等丢失和被破 坏。 |
| 4 | 防雷击 | 检查机房设计/验收文档，测评信息系统是否采取相应的措 施预防雷击。 |
| 5 | 防火 | 检查机房防火方面的安全管理制度，检查机房防火设备等过 程，测评信息系统是否采取必要的措施防止火灾的发生。 |

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 6 | 防水和防潮 | 检查机房及其除潮设备等过程，测评信息系统是否采取必要 措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 检查机房等过程，测评信息系统是否采取必要措施防止静电 的产生。 |
| 8 | 温湿度控制 | 检查机房的温湿度自动调节系统，测评信息系统是否采取必 要措施对机房内的温湿度进行控制。 |
| 9 | 电力供应 | 检查机房供电线路、设备等过程，测评是否具备为信息系统 提供一定电力供应的能力。 |
| 10 | 电磁防护 | 检查主要设备等过程，测评信息系统是否具备一定的电磁防 护能力。 |

## 安全通信网络测评

安全通信网络测评中，测评人员将以配置核查和文档查阅为主，访谈和分析为辅获取证据，用于测评信息系统的网络安全保护能力。

安全通信网络测评涉及的测评对象主要包括网络互联设备、网络安全设备以及网络拓扑结构等。

表 5- 2 安全通信网络测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 网络架构 | 检查整个网络的资源分布、架构是否合理，检查网络设备的性能要求；业务系统对网络带宽的需求；网络区域的合理划分；区域间的有效防护；网络通信线路以及设备的冗余等。 |
| 2 | 通信传输 | 检查网络中传输的数据是否具有完整性校验；数据是否采用加密等安全措施来保障数据的完整性和保密性。 |
| 3 | 可信验证 | 检查是否基于可信根实现预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保“无篡改再执行、有篡改就报警”。 |

## 安全区域边界测评

安全区域边界测评中，测评人员将以配置核查和文档查阅为主，访谈和分析为辅获取证据，用于测评信息系统的网络安全保护能力。

安全通信网络测评涉及的测评对象主要包括网络互联设备、网络安全设备、终端管理设备以及网络拓扑结构等。

表 5- 3 安全区域边界测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 边界防护 | 检查网络边界设备端口、链路是否可靠，是否通过有效的技术措施保障边界设备物理端口可信，防止非授权的网络链路接入；其次，检查是否通过有效的技术措施对外部设备的网络接入行为及内部设备的网络外连行为进行管控，减少外部威胁的引入；同时，检查是否对无线网络的使用进行管控， 防止因无线网络的滥用而引入安全威胁。 |
| 2 | 访问控制 | 检查是否启用有效的访问控制策略，采用白名单机制，仅授权用户能够访问网络资源；应根据业务访问的需要对源地址、目的地址、源端口、目的端口和协议等进行管控；是否能够根据业务绘画的状态信息为进出网络的数据流提供明确的允许、拒绝访问的能力；同时，检查访问控制是否能够对进出网络的数据量所包含的内容及协议进行管控。 |
| 3 | 入侵防范 | 检查是否有从外部网络发起的攻击、内部网络发起的攻击、新型攻击的防范以及检测到入侵攻击时是否及时告警等。 |
| 4 | 恶意代码和垃圾邮件防范 | 检查是否采取技术手段对恶意代码及垃圾邮件加以重点防 范。 |
| 5 | 安全审计 | 检查是否对重要事件进行了审计、审计的内容、审计记录的保护以及特殊行为的审计。 |
| 6 | 可信验证 | 检查是否基于可信根实现预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保“无篡改再执行、有篡改就报警”。 |

## 安全计算环境测评

安全计算环境测评中，测评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），用于评测信息系统的计算环境安全保护能力。

安全计算环境的测评对象主要包括网络设备、服务器/存储设备、终端、系统管理软件、业务应用系统等。

表 5- 4 安全计算环境测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 身份鉴别 | 1)检查测评对象的身份鉴别策略，查看是否提供了身份鉴别措施。 |
| 2 | 访问控制 | 检查测评对象的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。 |
| 3 | 安全审计 | 检查测评对象的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。 |
| 4 | 入侵防范 | 检查测评对象在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 |
| 5 | 恶意代码防范 | 检查测评对象的恶意代码防范情况。 |
| 6 | 可信验证 | 检查是否基于可信根实现预装软件（包括系统引导程序、系统程序、相关应用程序和重要配置参数）的完整性验证或检测，确保“无篡改再执行、有篡改就报警”。 |
| 7 | 数据完整性 | 检查操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。 |
| 8 | 数据保密性 | 检查操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。 |
| 9 | 数据备份和恢复 | 检查信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。 |
| 10 | 剩余信息保护 | 检查鉴别信息的存储空间，被释放或再分配给其他用户前得到完全清除。 |

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 11 | 个人信息保护 | 检查个人信息的采集、存储和使用是否提出了强制保护要求。 |

## 安全管理中心测评

安全管理中心测评主要涉及系统管理、审计管理、安全管理、集中管控几个方面的安全防护能力。

表 5- 5 安全管理中心测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 系统管理 | 检查是否对系统管理员进行身份鉴别、是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作、是否对系统管理操作进行审计， 确保系统管理操作的安全性。 |
| 2 | 审计管理 | 检查是否对审计管理员进行身份鉴别、是否只允许审计管理员通过特定的命令或操作界面进行审计管理操作、是否对审计管理操作进行审计， 确保审计管理操作的安全性。 |

## 安全管理制度测评

表 5- 6 安全管理制度测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 安全策略 | 通过访谈安全主管，检查有关管理制度文档和重要操作规程等过程，测评领导层决定的最高层安全文件，明确网络安全的总体目标和安全管理框架等。 |
| 2 | 管理制度 | 通过访谈安全主管，检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。 |
| 3 | 制定与发布 | 通过访谈安全主管，检查有关制度制定要求文档等过程，测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 |
| 4 | 评审和修订 | 通过访谈安全主管，检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。 |

## 安全管理机构测评

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

表 5- 7 安全管理机构测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 岗位设置 | 通过访谈安全主管，检查部门/岗位职责文件，测评信息系统安全主管部 门设置情况以及各岗位设置和岗位职责情况。 |
| 2 | 人员配备 | 通过访谈安全主管，检查人员名单等文档，测评信息系统各个岗位人员配备情况。 |
| 3 | 授权和审批 | 通过访谈安全主管，检查相关文档，测评信息系统对关键活动的授权和审批情况。 |
| 4 | 沟通与合作 | 通过访谈安全主管，检查相关文档，测评信息系统内部部门间、与外部单位间的沟通与合作情况。 |
| 5 | 审核与检查 | 通过访谈安全主管，检查记录文档等过程，测评信息系统安全工作的审核和检查情况。 |

## 安全管理人员测评

安全管理人员测评主要涉及安全主管、人事管理人员、相关管理制度以及相关工作记录等对象。

表 5- 8 安全管理人员测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 人员录用 | 通过访谈人事负责人，检查人员录用文档等过程，测评信息系统录用 人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
| 2 | 人员离岗 | 通过访谈人事负责人，检查人员离岗安全处理记录等过程，测评信息 系统人员离岗时是否按照一定的手续办理。 |
| 3 | 安全意识教育和培训 | 通过访谈安全主管，检查培训计划和执行记录等文档，测评是否对人 员进行安全方面的教育和培训。 |

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 4 | 外部人员访问管理 | 通过访谈安全主管，检查有关文档等过程，测评对第三方人员访问（物 理、逻辑）系统是否采取必要控制措施。 |

## 安全建设管理测评

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

表 5- 9 安全建设管理测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 定级和备案 | 通过访谈安全主管，检查系统定级相关文档等过程，测评是否按照一 定要求确定系统的安全等级并进行备案。 |
| 2 | 安全方案设计 | 通过访谈系统建设负责人，检查系统安全建设方案等文档，测评系统 整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购和使用 | 通过访谈安全主管、系统建设负责人和安全产品等过程，测评是否按 照一定的要求进行系统的产品采购。 |
| 4 | 自行软件开发 | 通过访谈系统建设负责人，检查相关软件开发文档等，测评自行开发 的软件是否采取必要的措施保证开发过程的安全性。 |
| 5 | 外包软件开发 | 通过访谈系统建设负责人，检查相关文档，测评外包开发的软件是否 采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开 展。 |
| 6 | 工程实施 | 通过访谈系统建设负责人，检查相关文档，测评系统建设的实施过程 是否采取必要的措施使其在机构可控的范围内进行。 |
| 7 | 测试验收 | 通过访谈系统建设负责人，检查测试验收等相关文档，测评系统运行 前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 通过访谈系统运维负责人，检查系统交付清单等过程，测评是否采取 必要的措施对系统交付过程进行有效控制。 |
| 9 | 等级测评 | 通过访谈系统建设负责人，检查系统是否定期进行的等级测评，是否 选择有资质的单位完成此项工作。 |

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 10 | 服务供应商选择 | 通过访谈系统运维负责人，测评是否选择符合国家有关规定的安全服 务单位进行相关的安全服务工作。 |

## 安全运维管理测评

安全运维管理测评主要涉及安全主管、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测评对象。

表 5- 10 安全运维管理测评指标描述

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 1 | 环境管理 | 通过访谈物理安全负责人，检查机房安全管理制度，机房和办公环境等过 程，测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为 等方面进行安全管理。 |
| 2 | 资产管理 | 通过访谈资产管理员，检查资产清单，检查系统、网络设备等过程，测评 是否采取必要的措施对系统的资产进行分类标识管理。 |
| 3 | 介质管理 | 通过访谈资产管理员，检查介质管理记录和各类介质等过程，测评是否采 取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
| 4 | 设备维护管理 | 通过访谈资产管理员、系统管理员，检查设备使用管理文档和设备操作规 程等过程，测评是否采取必要的措施确保设备在使用、维护和销毁等过程 安全。 |
| 5 | 漏洞和风险管理 | 通过访谈系统运维负责人，测评是否采取必要的措施进行识别和评估，针对发现的漏洞和隐患需要及时修补，确保等级保护对象安全、稳定的运行。 |
| 6 | 网络和系统安全管理 | 通过访谈安全主管、网络管理员，检查网络安全管理制度、网络审计日志和网络漏洞扫描报告等过程，测评是否采取必要的措施对网络的安全配置、网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。 |
| 7 | 恶意代码防范管理 | 通过访谈系统运维负责人，检查恶意代码防范管理文档和恶意代码检测记 录等过程，测评是否采取必要的措施对恶意代码进行有效管理，确保系统 具有恶意代码防范能力。 |
| 8 | 配置管理 | 通过访谈安全员，测评是否能够确保信息系统中的配置信息进行记录和保 存，并对配置信息的变更严格把控。 |

|  |  |  |
| --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** |
| 9 | 密码管理 | 通过访谈安全员，检查密码产品采购相关文档，测评采用的相关密码产品、设备是否遵循相关国家标准和行业标准，并加强管理。 |
| 10 | 变更管理 | 通过访谈系统运维负责人，检查变更方案和变更管理制度等过程，测评是 否采取必要的措施对系统发生的变更进行有效管理。 |
| 11 | 备份与恢复管理 | 通过访谈系统管理员、网络管理员，检查系统备份管理文档和记录等过程， 测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
| 12 | 安全事件处置 | 通过访谈系统运维负责人，检查安全事件记录分析文档、安全事件报告和 处置管理制度等过程，测评是否采取必要的措施对安全事件进行等级划分 和对安全事件的报告、处理过程进行有效的管理。 |
| 13 | 应急预案管理 | 通过访谈系统运维负责人，检查应急响应预案文档等过程，测评是否针对 不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审 查等。 |
| 14 | 外包运维管理 | 通过访谈系统运维负责人，检查相关服务协议书，测评是否严格管控外包 运维服务上的选择，服务协议中是否明确指出了服务商的能力要求、工作 范围要求和工作内容等要求。 |

## 云计算安全测评

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **扩展类型** |  | **安全类** | **安全控制点** | **测评项数** |
|  | **云计算安全扩展要求** | | | |
| 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 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **扩展类型** |  | **安全类** | **安全控制点** | **测评项数** |
|  |  |  | 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 |

1. **工具测试**
   1. **漏洞扫描方案**

### 漏洞扫描工具

表 6- 1 测评工具

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **工具用途分类** | **具体描述** |
| 1 | 绿盟远程评估系统 | 系统层、网络层  漏洞检测 | 对网络、主机、数据库进行漏洞扫描工具 |

### 工具测试接入点说明

本次测评的信息系统为第二级信息系统，根据第二级信息系统的测评强度要求， 在测试的广度上，应基本覆盖不同类型的机制，在数量、范围上可以抽样。因此， 对其进行测评，应涉及到漏洞扫描工具等多种测试工具。针对被测系统的网络边界 和测评设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置 3 个测试工具接入点――接入点 JA 到 JC，如图 7 所示，“接入点”标注表示进行工具测试时，需要从该接入点接入，对应的箭头路线表示工具测试数据的主要流向示 意。具体接入点如下图所示：

### 漏洞扫描范围

利用测试工具对操作系统、网络设备、数据库系统进行扫描，可以获取目标设备开放的端口及服务，检测出目标系统中存在的操作系统网络设备、数据库系统和常见应用漏洞，如缓冲区溢出溢出漏洞、系统或应用程序弱口令漏洞、系统或应用程序因未及时更新补丁所暴露出的漏洞等。

本次工具测试的范围是测评对象所涉及的服务器操作系统、网络设备、安全设备、数据库系统、应用系统、客户端、终端设备等。工具测试目标如下表：

表 6- 2 接入点 A 目标设备情况表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **站点名称** | **IP 地址/URL** | **备注** |

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | XXX 大学全流程数字化业务系统 | XXX |  |

表 6- 3 接入点 B 目标设备情况表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **IP 地址/URL** | **备注** |
| 1 | 应用服务器 | XXX |  |
| 2 | 数据库服务器 | XXX |  |
| 3 | 反代服务器 | XXX |  |

表 6- 4 接入点 C 目标设备情况表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **IP 地址/URL** | **备注** |
| 1 | 入侵检测 | XXX |  |
| 2 | 日志审计系统 | XXX |  |
| 3 | 某校区汇聚交换机 | XXX |  |
| 4 | Web 应用防火墙 | XXX |  |
| 5 | 上网行为管理 | XXX |  |
| 6 | 堡垒机 | XXX |  |
| 7 | 服务器接入交换机 | XXX |  |
| 8 | 核心交换机 | XXX |  |
| 9 | 漏洞扫描 | XXX |  |
| 10 | 边界防火墙 | XXX |  |
| 11 | 服务器区防火墙 | XXX |  |

本次测评将工具扫描获取到操作系统、数据库、网络设备、安全设备的漏洞信息进行数据取样，用于后续测评工作中分析及使用。

### 漏洞扫描时间

本次漏洞扫描的时间为 2020 年 11 月 5 日 2020 年 11 月 19 日。

# 现场测评风险规避措施

1、现场测评之前，测评组获取被测评单位签署现场测评授权书。

2、要求被测评单位对系统及数据进行备份，并对可能出现的事件制定应急处理方案。

3、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。如果被测方不允许在生产环境中测试，可配置与生产环境一致的模拟/仿真环境，在模拟/仿真环境下开展漏洞扫描等测试工作。

4、上机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。

5、整个现场测评过程要求系统运营、使用单位全程监督。

6、测评工作完成后，测评人员应将测评过程中获取的所有特权交回，把测评过程中借阅的相关资料文档归还，并将测评环境恢复至测评前状态。

# 现场测评工作计划

## 测评项目组成员及分工

此次测评项目组成员及分工如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 | 角色 | 分工 | 备注 |
| XXX | XXX | XXX |  |
| XXX | XXX | XXX |  |
| XXX | XXX | XXX |  |
| XXX | XXX | XXX |  |
| XXX | XXX | XXX |  |

## 现场测评实施计划

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **工作日** | **工作时间** | **工作内容** | **内容概要** | **配合人员** | **工作地点** | **评测人员** | **所需资源** |
|  |  |  | 召开现场等 |  |  |  | 分管信息安全 |
|  |  |  | 级测评启动 |  |  |  | 工作领导及相 |
| 第一天 |  | 测评机构 |  |  |  |  |  |
|  |  |  | 会，主要是介 | 所有参 |  |  | 关负责人、第三 |
| 至第五 | 上午 | 现场测评 |  |  | 会议室 | 所有人员 |  |
|  |  |  | 绍工作计划， | 与人员 |  |  | 方服务公司人 |
| 天 |  | 启动会 |  |  |  |  |  |
|  |  |  | 工作内容，相 |  |  |  | 员参加现场启 |
|  |  |  | 关配合事项 |  |  |  | 动会 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 网络核查 | 核查内网拓扑图 | 网络管理员、安全管理员 | 办公室 | 网络评测人员 | 接受访谈，根据前期调研情况， 进一步提供内 网网络拓扑图 相关的网络结 构设计、安全区域划分以及区 域之间的隔离 措施等相关材  料 |
| 技术和管理测评 | 应用软件评测 | 系统管理员 | 办公室 | 应用评测人员 | 接受访谈，提供应用系统的管 理账户及口令、操作员账户及  口令； |
| 服务器评测 | 服务器管理员 | 办公室 | 系统评测人员 | 接受访谈，提供服务器主机的系统管理账户及口令、操作员  账户及口令； |
| 数据库评测 | 数据库管理员 | 办公室 | 系统评测人员 | 接受访谈，提供数据库管理系统的系统管理账户及口令、操作员账户及口  令； |
| 管理测评 | 安全管理员 | 办公室 | 管理评测人员 | 接受访谈，提供信息安全管理  体系制度文件； |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 云安全测评 | 系统管理员 | 办公室 | 应用评测人员 | 接受访谈，提供云系统相关资  料； |
| 整理资料 | 对所核查的  资产进行整理 | N/A | 办公室 | 所有人员 |  |
| 整理资料 | 对所核查的  资产进行整理 | N/A | 办公室 | 所有人员 |  |
| 第六天 | 上午 | 资料整理 | 对评测工作现场采集的数据进行整  理 | N/A | 办公室 | 项目组全体成员 |  |
| 下午 | 编写问题整改建议书 | 对测评工作发现的所有安全问题进行整理 并提交整改建议  书 | N/A | 办公室 | 项目组全体成员 |  |
| 第七天 | 上午 | 编写问题整改建议书 | 对测评工作发现的所有安全问题进行整理 并提交整改建议  书 | N/A | 办公室 | 项目组全体成员 |  |
| 下午 | 编写问题整改建议书 | 对测评工作发现的所有安全问题进  行整理 并提 | N/A | 办公室 | 项目组全体成员 |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 交整改建议  书 |  |  |  |  |
| 第八天 | 上午 | 评测结果交流 | 与客户人员对评测结果进行确认，并进行问题交  流 | 信息中心人员 | 办公室 | 所有人员 | 信息安全工作相关负责人、第三方服务公司人员 |
| 下午 | 总结会 | 开总结会议 | 所有人员 | 会议室 | 所有人员 | 分管信息安全工作领导、信息安全工作相关负责人、第三方服务公司人员参加现场启动  会 |

* 1. **人员配合要求**

表 8- 1 人员配合要求

|  |  |
| --- | --- |
| **配合人员** | **具体工作说明** |
| 总体联系人 | 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。各业务部门配合终端安全配置检查。 |
| 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。 |
| 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。 |
| 安全主管 | 现场配合检查组中管理组完成针对岗位设置、人员配备、授权和审 批、沟通和合作、审核和检查等方面访谈工作。 |
| 系统建设负责人 | 现场配合检查组中管理组完成针对系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、 系统交付、系统备案、等级测评、安全服务商选择访谈工作。 |
| 人事负责人 | 现场配合检查组中管理组完成针对人员录用、人员离岗、人员考核、 安全意识教育和培训、外部人员访问管理访谈工作。 |

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。

备注：检查工作人员分为五个小组，至少需要 1 名配合人员，不能同一个人配合多个小组人员。

机房管理人员

表 8- 2 扫描测试配合要求

|  |  |
| --- | --- |
| **配合项目** | **要求说明** |
| 配合人员 | 网络管理员，提供：   1. 对于每个接入点，2 个可用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。 |

## 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；
* 提供一台打印机和打印纸，以便文档的输出。

【正文结束】