**报告编号：110193XX-XXXX1**

**项目编号：（DJCPXXXXXXXXX**

**网络安全等级保护**

**XXX 大学全流程数字化业务系统等级测评报告**

# 委托单位： XXX 大学 测评单位： 北京 XXXX 公司 报告时间： 2021 年 04 月 02 日

### 说明：

一、每个备案系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下：

第一组为系统备案表编号，由 2 段 16 位数字组成，可以从公安机

关颁发的系统备案证明（或备案回执）上获得。第 1 段即备案证明编

号的前 11 位（前 6 位为受理备案公安机关代码，后 5 位为受理备案

的公安机关给出的备案单位的顺序编号）；第 2 段即备案证明编号的

后 5 位（系统编号）。

第二组为年份，由 2 位数字组成。例如 09 代表 2009 年。

第三组为测评机构代码，由测评机构推荐证书编号最后六位数字组成。其中，前两位为省级行政区划数字代码的前两位或行业主管部门编号：00 为公安部，11 为北京，12 为天津，13 为河北，14 为山西，15 为内蒙古，21 为辽宁，22 为吉林，23 为黑龙江，31 为上海， 32 为江苏，33 为浙江，34 为安徽，35 为福建，36 为江西，37 为山东，41 为河南，42 为湖北，43 为湖南，44 为广东，45 为广西，46 为海南，50 为重庆，51 为四川，52 为贵州，53 为云南，54 为西藏， 61 为陕西，62 为甘肃，63 为青海，64 为宁夏，65 为新疆，66 为新疆兵团。90 为国防科工局，91 为国家能源局，92 为教育部。后四位为公安机关或行业主管部门推荐的测评机构顺序号。

第四组为本年度系统测评次数，由两位构成。例如 02 表示该系统

本年度测评 2 次。

### 网络安全等级测评基本信息表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **被测对象** | | | | | | | | |
| **被测对象名称** | | XXX 大学全流程数字化业务系统 | | | **安全保护等级** | | 第二级（S2A2G2） | |
| **备案证明编号** | | 1XXXXXX | | | | | | |
| **被测评单位** | | | | | | | | |
| **单位名称** | XXX 大学 | | | | | | | |
| **单位地址** | XXX | | | | | **邮政编码** | | XXX |
| **联系人** | **姓名** | | XXX | **职务/职称** | | XXX | | |
| **所属部门** | | XXX | **办公电话** | | XXX | | |
| **移动电话** | | XXX | **电子邮件** | | XXX | | |
| **测评机构** | | | | | | | | |
| **单位名称** | XXX | | | | | **机构代码** | | DXXX |
| **单位地址** | XXX | | | | | **邮政编码** | | XXX |
| **联系人** | **姓名** | | XXX | **职务/职称** | | XXX | | |
| **所属部门** | | XXX | **办公电话** | | XXX | | |
| **移动电话** | | XXX | **电子邮件** | | XXX | | |
| **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** | |  | | |

# 声明

本报告是XXX 大学全流程数字化业务系统的等级测评报告。本报告是对XXX 大学全流程数字化业务系统的整体安全性进行

检测分析，针对等级测评过程中发现的安全问题，结合风险分析，提出合理化建议。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件

（或子系统）都应重新进行等级测评，本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

XXX

2021 年 04 月 02 日

# 等级测评结论

|  |  |  |  |
| --- | --- | --- | --- |
| **测评结论和综合得分** | | | |
| **被测对象名称** | XXX 大学全流程数字化业务系统 | **安全保护等级** | 第二级（S2A2G2） |
| **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 | | |
| **被测对象描述** |  | | |
| **测评工作描述** |  | | |
| **等级测评结论** | **XX** | **综合得分** | XX |

**总体评价**

通过对信息系统基本安全保护状态的分析，XXX 大学（以下简称“被测评单位”）针对“XXX 大学全流程数字化业务系统”面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。

在安全物理环境方面：XXX。在安全通信网络方面：XXX。在安全区域边界方面：XXX。在安全计算环境方面：XXX。在安全管理中心方面：XXX。在安全管理制度方面：XXX。在安全管理机构方面：XXX。在安全管理人员方面：XXX。在安全建设管理方面：XXX。在安全运维管理方面：XXX。综上所述，XXX。

# 主要安全问题及整改建议

**1、安全物理环境**

**2、安全通信网络**

**3、安全区域边界**

**4、安全计算环境**

**5、安全管理制度**

**6、安全管理机构**

**7、安全管理人员**

**8、安全建设管理**

**9、安全运维管理**

# 目录

[网络安全等级测评基本信息表 I](#_bookmark0)

[声明 II](#_bookmark1)

[等级测评结论 III](#_bookmark2)

[总体评价 IV](#_bookmark3)

[主要安全问题及整改建议 V](#_bookmark4)

[目录 VI](#_bookmark5)

[正文表格索引 XII](#_bookmark6)

[附录表格索引 XIII](#_bookmark7)

[插图索引 XV](#_bookmark8)

1. [测评项目概述 1](#_bookmark9)
   1. [测评目的 1](#_bookmark10)
   2. [测评依据 1](#_bookmark11)
   3. [测评过程 2](#_bookmark12)
   4. [报告分发范围 3](#_bookmark14)
2. [被测对象描述 4](#_bookmark15)
   1. [被测对象概述 4](#_bookmark16)
      1. [定级结果 4](#_bookmark17)
      2. [业务和采用的技术 4](#_bookmark19)
      3. [网络结构 4](#_bookmark20)
   2. [测评指标 5](#_bookmark22)
      1. [安全通用要求指标 5](#_bookmark23)
      2. [安全扩展要求指标 8](#_bookmark27)
      3. [其他安全要求指标 8](#_bookmark29)
      4. [不适用安全要求指标 8](#_bookmark31)
   3. [测评对象 16](#_bookmark33)
      1. [测评对象选择方法 16](#_bookmark34)
      2. [测评对象选择结果 17](#_bookmark35)
3. [单项测评结果分析 23](#_bookmark46)
   1. [安全物理环境 24](#_bookmark47)
      1. [已有安全控制措施汇总分析 24](#_bookmark48)
      2. [主要安全问题汇总分析 24](#_bookmark49)
   2. [安全通信网络 24](#_bookmark50)
      1. [已有安全控制措施汇总分析 24](#_bookmark51)
      2. [主要安全问题汇总分析 24](#_bookmark52)
   3. [安全区域边界 24](#_bookmark53)
      1. [已有安全控制措施汇总分析 24](#_bookmark54)
      2. [主要安全问题汇总分析 24](#_bookmark55)
   4. [安全计算环境 24](#_bookmark56)
      1. [网络设备和安全设备 24](#_bookmark57)
      2. [服务器和终端 24](#_bookmark58)
      3. [应用和数据 25](#_bookmark59)
      4. [其他系统和设备 25](#_bookmark60)
   5. [安全管理中心 25](#_bookmark61)
      1. [已有安全控制措施汇总分析 25](#_bookmark62)
      2. [主要安全问题汇总分析 25](#_bookmark63)
   6. [安全管理制度 25](#_bookmark64)
      1. [已有安全控制措施汇总分析 25](#_bookmark65)
      2. [主要安全问题汇总分析 25](#_bookmark66)
   7. [安全管理机构 25](#_bookmark67)
      1. [已有安全控制措施汇总分析 25](#_bookmark68)
      2. [主要安全问题汇总分析 25](#_bookmark69)
   8. [安全管理人员 25](#_bookmark70)
      1. [已有安全控制措施汇总分析 26](#_bookmark71)
      2. [主要安全问题汇总分析 26](#_bookmark72)
   9. [安全建设管理 26](#_bookmark73)
      1. [已有安全控制措施汇总分析 26](#_bookmark74)
      2. [主要安全问题汇总分析 26](#_bookmark75)
   10. [安全运维管理 26](#_bookmark76)
       1. [已有安全控制措施汇总分析 26](#_bookmark77)
       2. [主要安全问题汇总分析 26](#_bookmark78)
   11. [其他安全要求指标 26](#_bookmark79)
   12. [验证测试 26](#_bookmark80)
       1. [漏洞扫描 27](#_bookmark82)
       2. [渗透测试 29](#_bookmark86)
   13. [单项测评小结 29](#_bookmark87)
       1. [控制点符合情况汇总 29](#_bookmark88)
       2. [安全问题汇总 32](#_bookmark90)
4. [整体测评结果分析 34](#_bookmark92)
   1. [安全控制点间安全测评 34](#_bookmark93)
   2. [区域间/层面间安全测评 34](#_bookmark94)
   3. [整体测评结果汇总 34](#_bookmark95)
5. [安全问题风险分析 35](#_bookmark99)
6. [等级测评结论 38](#_bookmark103)
7. [安全问题整改建议 40](#_bookmark106)

[附录 A 被测对象资产 42](#_bookmark108)

* 1. [物理机房 42](#_bookmark109)
  2. [网络设备 42](#_bookmark111)
  3. [安全设备 42](#_bookmark113)
  4. [服务器/存储设备 43](#_bookmark115)
  5. [终端/现场设备 44](#_bookmark117)
  6. [系统管理软件/平台 44](#_bookmark119)
  7. [业务应用系统/平台 44](#_bookmark121)
  8. [数据类别 44](#_bookmark123)
  9. [安全相关人员 45](#_bookmark125)
  10. [安全管理文档 45](#_bookmark127)

[附录 B 上次测评问题整改情况说明 47](#_bookmark129)

[附录 C 单项测评结果汇总 48](#_bookmark130)

* 1. [安全物理环境 48](#_bookmark131)
  2. [安全通信网络 48](#_bookmark134)
  3. [安全区域边界 49](#_bookmark137)
  4. [安全计算环境 49](#_bookmark140)
     1. [网络设备和安全设备 49](#_bookmark141)
     2. [服务器和终端 52](#_bookmark144)
     3. [应用和数据 53](#_bookmark147)
     4. [其他系统和设备 55](#_bookmark150)
  5. [安全管理中心 55](#_bookmark153)
  6. [安全管理制度 56](#_bookmark155)
  7. [安全管理机构 56](#_bookmark157)
  8. [安全管理人员 56](#_bookmark159)
  9. [安全建设管理 57](#_bookmark161)
  10. [安全运维管理 57](#_bookmark164)
  11. [其他安全要求指标 58](#_bookmark167)

[附录 D 单项测评结果记录 59](#_bookmark169)

* [D.1 安全物理环境 59](#_bookmark170)
  + [D1.1 某校区信息中心机房 59](#_bookmark171)
  + [D1.2 某校区信息中心机房 59](#_bookmark172)
* [D.2 安全通信网络 59](#_bookmark173)
  + [D2.1 安全通信网络 59](#_bookmark174)
* [D.3 安全区域边界 59](#_bookmark175)
  + [D3.1 安全边界 59](#_bookmark176)
* [D.4 安全计算环境 59](#_bookmark177)
  + [D4.1 核心交换机 59](#_bookmark178)
  + [D4.2 某校区汇聚交换机 59](#_bookmark179)
  + [D4.3 服务器接入交换机 59](#_bookmark180)
  + [D4.4 办公区接入交换机 59](#_bookmark181)
  + [D4.5 运维接入交换机 59](#_bookmark182)
  + [D4.6 日志审计 59](#_bookmark183)
  + [D4.7 Web 应用防火墙 59](#_bookmark184)
  + [D4.8 堡 垒机 59](#_bookmark185)
  + [D4.9 漏洞扫描 59](#_bookmark186)
  + [D4.10 上网行为管理 59](#_bookmark187)
  + [D4.11 入侵检测 59](#_bookmark188)
  + [D4.12 内网防火墙 59](#_bookmark189)
  + [D4.13 出口防火墙 60](#_bookmark190)
  + [D4.14 XXX 大学全流程数字化业务系统 60](#_bookmark191)
  + [D4.15 Nginx 中 间件 60](#_bookmark192)
  + [D4.16 Tomcat 60](#_bookmark193)
  + [D4.17 应用服务器 60](#_bookmark194)
  + [D4.18 数据库服务器 60](#_bookmark195)
  + [D4.19 反代服务器 60](#_bookmark196)
  + [D4.20 运维终端 60](#_bookmark197)
  + [D4.21 数据库系统 60](#_bookmark198)
  + [D4.22 管理数据 60](#_bookmark199)
  + [D4.23 业务数据 60](#_bookmark200)
  + [D4.24 审计数据 60](#_bookmark201)
  + [D4.25 用户数据 60](#_bookmark202)
* [D.5 安全管理中心 60](#_bookmark203)
  + [D5.1 安全管理中心 60](#_bookmark204)
* [D.6 安全管理制度 60](#_bookmark205)
  + [D6.1 安全管理制度 60](#_bookmark206)
* [D.7 安全管理机构 60](#_bookmark207)
  + [D7.1 安全管理机构 60](#_bookmark208)
* [D.8 安全管理人员 60](#_bookmark209)
  + [D8.1 安全管理人员 60](#_bookmark210)
* [D.9 安全建设管理 60](#_bookmark211)
  + [D9.1 安全建设管理 61](#_bookmark212)
* [D.10 安全运维管理 61](#_bookmark213)
  + [D10.1 安全运维管理 61](#_bookmark214)

[附录 E 漏洞扫描结果记录 62](#_bookmark215)

* 1. [应用系统 62](#_bookmark216)
  2. [主机服务器 62](#_bookmark217)
  3. [网络设备、安全设备 62](#_bookmark218)

[附录 F 渗透测试结果记录 64](#_bookmark219)

[附录 G 常见威胁列表 65](#_bookmark220)

**正文表格索引**

[**表 2- 1 定级结果 4**](#_bookmark18)

[**表 2- 2 安全通用要求指标 5**](#_bookmark24)

[**表 2- 3 安全扩展要求指标 8**](#_bookmark28)

[**表 2- 4 其他安全要求指标 8**](#_bookmark30)

[**表 2- 5 不适用安全要求指标 8**](#_bookmark32)

[**表 2- 6 物理机房 17**](#_bookmark36)

[**表 2- 7 网络设备 17**](#_bookmark37)

[**表 2- 8 安全设备 18**](#_bookmark38)

[**表 2- 9 服务器/存储设备 18**](#_bookmark39)

[**表 2- 10 终端/现场设备 19**](#_bookmark40)

[**表 2- 11 系统管理软件/平台 19**](#_bookmark41)

[**表 2- 12 业务应用系统/平台 20**](#_bookmark42)

[**表 2- 13 关键数据类别 20**](#_bookmark43)

[**表 2- 14 安全相关人员 20**](#_bookmark44)

[**表 2- 15 安全管理文档 21**](#_bookmark45)

[**表 3- 1 应用系统漏洞扫描结果统计表 28**](#_bookmark83)

[**表 3- 2 主机漏洞扫描结果统计表 28**](#_bookmark84)

[**表 3- 3 网络设备、安全设备漏洞扫描结果统计表 28**](#_bookmark85)

[**表 3- 4 测评结果分类统计表 29**](#_bookmark89)

[**表 3- 5 安全问题汇总表 32**](#_bookmark91)

[**表 4- 1 修正后的安全问题汇总表 34**](#_bookmark96)

[**表 5- 1 安全问题风险分析表 35**](#_bookmark100)

[**表 6- 1 等级测评结论判别依据 38**](#_bookmark104)

[**表 6- 2 安全风险汇总表 38**](#_bookmark105)

[**表 7- 1 安全问题整改建议表 40**](#_bookmark107)

# 附录表格索引

[**附录 A 表-1 物理机房 42**](#_bookmark110)

[**附录 A 表-2 网络设备 42**](#_bookmark112)

[**附录 A 表-3 安全设备 42**](#_bookmark114)

[**附录 A 表-4 服务器/存储设备 43**](#_bookmark116)

[**附录 A 表-5 终端/现场设备 44**](#_bookmark118)

[**附录 A 表-6 系统管理软件/平台 44**](#_bookmark120)

[**附录 A 表-7 业务应用系统/平台 44**](#_bookmark122)

[**附录 A 表-8 关键数据类别 44**](#_bookmark124)

[**附录 A 表-9 安全相关人员 45**](#_bookmark126)

[**附录 A 表-10 安全管理文档 45**](#_bookmark128)

[**附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分） 48**](#_bookmark132)

[**附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分） 48**](#_bookmark133)

[**附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分） 48**](#_bookmark135)

[**附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分） 49**](#_bookmark136)

[**附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分） 49**](#_bookmark138)

[**附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分） 49**](#_bookmark139)

[**附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分） 49**](#_bookmark142)

[**附录 C 表-8 安全计算环境单项测评结果汇总表（安全扩展要求部分） 52**](#_bookmark143)

[**附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分） 52**](#_bookmark145)

[**附录 C 表-10 安全计算环境单项测评结果汇总表（安全扩展要求部分） 53**](#_bookmark146)

[**附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分） 53**](#_bookmark148)

[**附录 C 表-12 安全计算环境单项测评结果汇总表（安全扩展要求部分） 55**](#_bookmark149)

[**附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分） 55**](#_bookmark151)

[**附录 C 表-14 安全计算环境单项测评结果汇总表（安全扩展要求部分） 55**](#_bookmark152)

[**附录 C 表-15 安全管理中心单项测评结果汇总表 55**](#_bookmark154)

[**附录 C 表-16 安全管理制度单项测评结果汇总表 56**](#_bookmark156)

[**附录 C 表-17 安全管理机构单项测评结果汇总表 56**](#_bookmark158)

[**附录 C 表-18 安全管理人员单项测评结果汇总表 56**](#_bookmark160)

[**附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分） 57**](#_bookmark162)

[**附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分） 57**](#_bookmark163)

[**附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求） 57**](#_bookmark165)

[**附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分） 58**](#_bookmark166)

[**附录 C 表-23 其他指标单项测评结果汇总表 58**](#_bookmark168)

**插图索引**

[**图 1.1 等级保护测评工作流程图 2**](#_bookmark13)

[**图 2.1 网络拓扑图 4**](#_bookmark21)

[**图 3.1 漏洞扫描工具接入测试示意图 27**](#_bookmark81)

# 测评项目概述

## 测评目的

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。

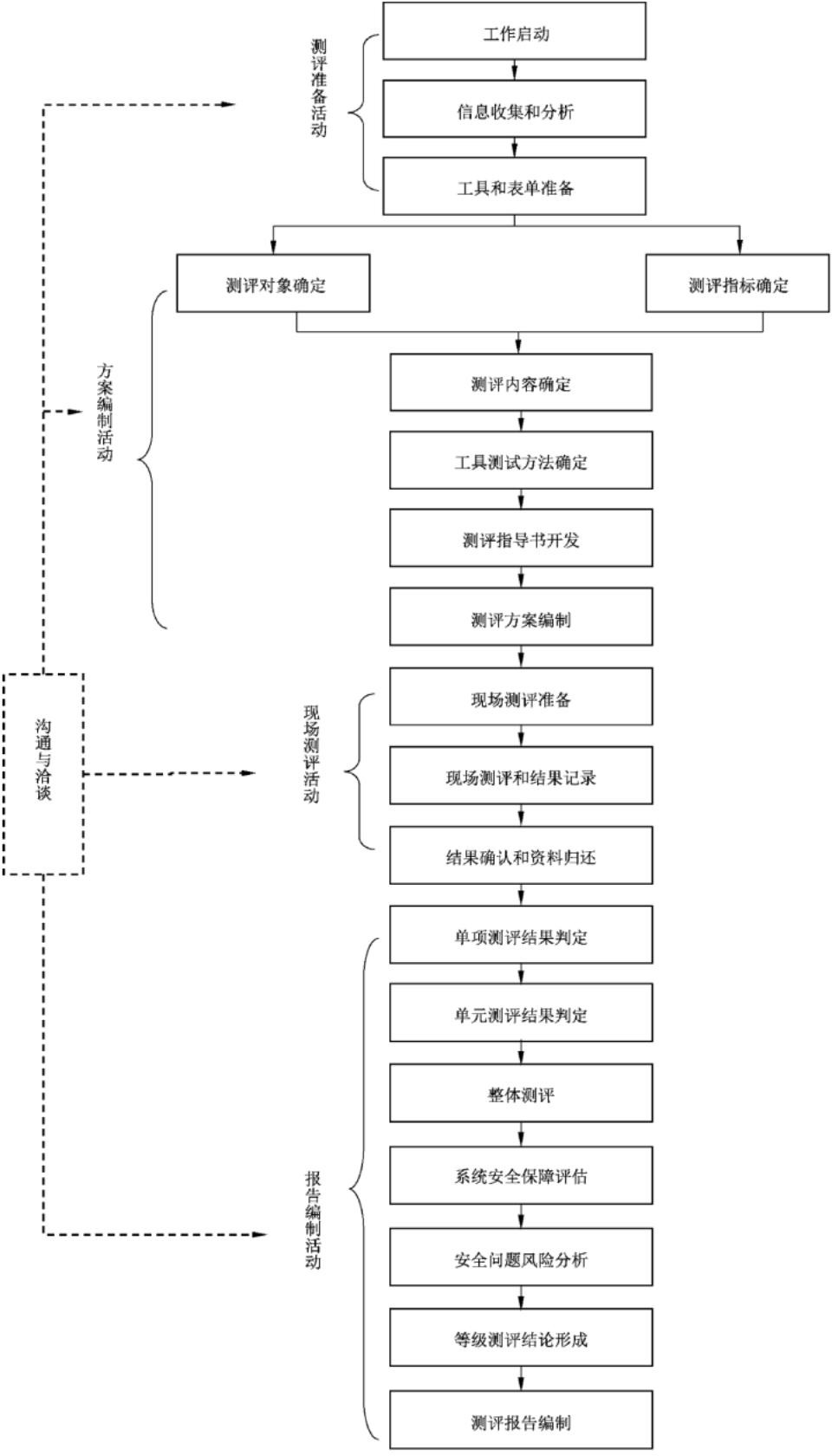
为进一步提高信息系统的保障能力，根据《信息安全等级保护管理办法》（公通字【2007】43 号）的精神，XXX 大学委托北京 XXXX 公司（XX）对 XXX 大学全流程数字化业务系统实施等级测评，以期发现信息系统和等级保护标准的差距以及存在的安全隐患，为后续的安全整改工作提供参考依据。

## 测评依据

测评过程中主要依据的标准：

* + 1. GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》
    2. GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》
    3. GB/T 20984-2007：《信息安全技术 信息安全风险评估规范》
    4. GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》
    5. GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》
    6. GB 17859-1999：《计算机信息系统安全保护等级划分准则》
    7. GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》

## 测评过程



**图 1.1 等级保护测评工作流程图**

## 报告分发范围

1. **被测对象描述**
   1. **被测对象概述**

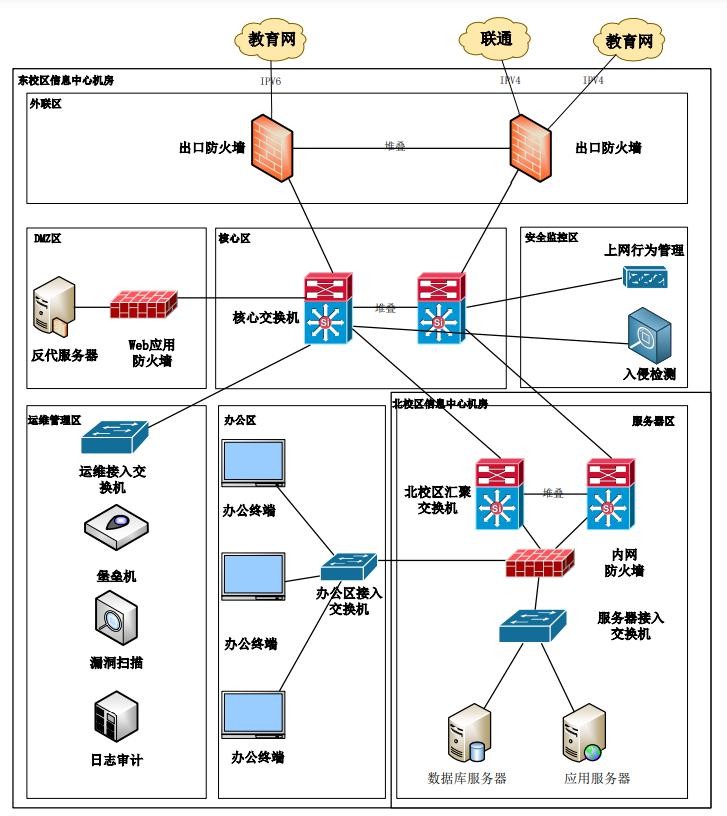
### 定级结果

**表 2- 1 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** |
|  |  |  |  |

### 业务和采用的技术

* + 1. **网络结构**



**图 2.1 网络拓扑图**

## 测评指标

### 安全通用要求指标

**表 2- 2 安全通用要求指标**

|  |  |  |
| --- | --- | --- |
| **安全类**[**1**](#_bookmark25) | **安全控制点**[**2**](#_bookmark26) | **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 |

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** |
|  | 可信验证 | 1 |
| 安全计算环境 | 身份鉴别 | 3 |
| 访问控制 | 4 |
| 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 |

|  |  |  |
| --- | --- | --- |
| **安全类1** | **安全控制点2** | **测评项数** |
| 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 |
| 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 |

### 安全扩展要求指标

**表 2- 3 安全扩展要求指标**

|  |  |  |  |
| --- | --- | --- | --- |
| **扩展类型** | **安全类** | **安全控制点** | **测评项数** |
| **本次测评不涉及** | | | |

### 其他安全要求指标

**表 2- 4 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** |
| **本次测评不涉及** | | | |

### 不适用安全要求指标

**表 2- 5 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）应遵循最小安装的原则，仅安装需要的组 件和应用程序； |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 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； |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| a）应遵循最小 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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； |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| b）应关闭不需要的系统服务、默认共享和高 危端口； |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 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； |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 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。 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  | 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； |  |  |
| b）应提供异地数据备份功能， 利用通信网络 将重要数据定 时批量传送至 备用场地。 |  |  |
| 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |  |  |
|  |  |
| b）应具有登录失败处理功能， 应配置并启用 结束会话、限制非法登录次数 和当登录连接 超时自动退出 等相关措施； |  |  |
|  |  |
| c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |  |  |
|  |  |
| 访问控制 | a）应对登录的用户分配账户和权限； |  |  |
|  |  |
| b）应重命名或删除默认账户， |  |  |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 修改默认账户的默认口令； |  |  |
| c）应及时删除 或停用多余的、过期的账户，避免共享账户的 存在； |  |  |
|  |  |
| d）应授予管理用户所需的最小权限，实现管理用户的权限分离。 |  |  |
|  |  |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组 件和应用程序； |  |  |
| b）应关闭不需要的系统服务、默认共享和高 危端口； |  |  |
| c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |  |  |
| 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， |  |  |
|  |  |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 并将验证结果形成审计记录送至安全管理中心。 |  |  |
| 数据完整性 | a）应采用校验技术保证重要 数据在传输过 程中的完整性。 |  |  |
|  |  |
| 剩余信息保护 | a）应保证鉴别信息所在的存 储空间被释放 或重新分配前 得到完全清除。 |  |  |
|  |  |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； |  |  |
| b）应禁止未授权访问和非法使用用户个人信息。 |  |  |
| 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； |  |  |
|  |  |
|  |  |
| 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。 |  |  |
| 入侵防范 | c）应通过设定终端接入方式 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 或网络地址范围对通过网络进行管理的管理终端进行限制； |  |  |
| d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； |  |  |
| 数据完整性 | a）应采用校验技术保证重要 数据在传输过 程中的完整性。 |  |  |
| 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； |  |  |
| b）应提供异地数据备份功能， 利用通信网络 将重要数据定 时批量传送至 备用场地。 |  |  |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组 件和应用程序； |  |  |
| b）应关闭不需要的系统服务、默认共享和高 危端口； |  |  |
| d）应提供数据有效性检验功 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 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； |  |  |
| 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。 |  |  |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； |  |  |
| b）应禁止未授权访问和非法使用用户个人信息。 |  |  |
| 剩余信息保护 | a）应保证鉴别信息所在的存 储空间被释放 或重新分配前 得到完全清除。 |  |  |
|  |  |
| 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； |  |  |
|  |  |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  |  |  |  |
| b）应禁止未授权访问和非法使用用户个人信息。 |  |  |
|  |  |
|  |  |
|  |  |
| 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； |  |  |
| 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。 |  |  |
| 等级测评 | a）应定期进行等级测评，发现不符合相应等 级保护标准要 求的及时整改； |  |  |
| b）应在发生重大变更或级别发生变化时进行等级测评； |  |  |
| 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； |  |  |
| b）应与选定的外包运维服务商签订相关的协议，明确约定 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全类** | **安全控制点** | **不适用项** | **不适用对象** | **原因说明** |
|  |  | 外包运维的范围、工作内容。 |  |  |
| **表中不适用指标数量** | | | |  |

## 测评对象

### 测评对象选择方法

“XXX 大学全流程数字化业务系统”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“XXX 大学全流程数字化业务系统”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. 管理终端和主要应用系统终端；
      10. 能够完成系统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

* + - 1. **物理机房**

**表 2- 6 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 |  | 非常重要 |
| 2 | 某校区信息中心机房 |  | 非常重要 |

### 网络设备

**表 2- 7 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** |
| 1 | 核心交换机 | × |  |  | 数据交换 | 非常重要 |
| 2 | 某校区汇聚交换机 | × |  |  | 数据交换 | 非常重要 |
| 3 | 服务器接入交换机 | × |  |  | 数据交换 | 非常重要 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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** |
| 4 | 办公区接入交换机 | × |  |  | 数据交换 | 重要 |
| 5 | 运维接入交换机 | × |  |  | 数据交换 | 重要 |

### 安全设备

**表 2- 8 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** |
| 1 | 出口防火墙 | × |  |  | 访问控制 | 非常重要 |
| 2 | 上网行为管理 | × |  |  | 上网行为管控 | 非常重要 |
| 3 | 入侵检测 | × |  |  | 入侵行为检测 | 非常重要 |
| 4 | 内网防火墙 | × |  |  | 访问控制 | 非常重要 |
| 5 | Web 应用防火墙 | × |  |  | 应用层防护 | 非常重要 |
| 6 | 堡垒机 | × |  |  | 运维管理 | 非常重要 |
| 7 | 漏洞扫描 | × |  |  | 漏洞扫描 | 重要 |
| 8 | 日志审计 | × |  |  | 运维管理 | 重要 |

### 服务器/存储设备

**表 2- 9 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** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| 1 | 应用服务器 | XXX 大学全流程数字化业务系统 | × |  |  |  | 非常重要 |
| 2 | 数据库服务器 | XXX 大学全流程数字化业务系统 | × |  |  |  | 非常重要 |
| 3 | 反代服务器 | XXX 大学全流程数字化业务系统 | × |  |  |  | 非常重要 |

### 终端/现场设备

**表 2- 10 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** |
| 1 | 运维终端 | × | Windows10 专业版 | 运维管理 | 重要 |

### 系统管理软件/平台

**表 2- 11 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** |
| 1 | 数据库系统 | 数据库服务器 |  |  | 非常重要 |

### 业务应用系统/平台

**表 2- 12 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** |
| 1 | XXX 大学全流程数字化业务系统 | XXX 大学全流程数字化业务系统 Web 端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 |  |  | 非常重要 |
| 2 | Nginx 中间件 | 数据代理 |  |  | 重要 |
| 3 | Tomcat | Web 服务支撑 |  |  | 重要 |

### 数据类别

**表 2- 13 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 | 审计数据 | XXX 大学全流程数字化业务系统 | 完整性 |
| 4 | 管理数据 | XXX 大学全流程数字化业务系统 | 完整性 |

### 安全相关人员

**表 2- 14 安全相关人员**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **姓名** | **岗位/角色** | **联系方式** |
| 4 |  |  |  |

### 安全管理文档

**表 2- 15 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 | 《XX 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》 | 安全域划分操作手册。 |

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

# 单项测评结果分析

单项测评内容包括“2.2.1 安全通用要求指标”、“2.2.2 安全扩展要求指标” 以及“2.2.3 其他安全要求指标”中涉及的安全类和安全要求条款，内容包括已有安全控制措施汇总分析和主要安全问题汇总分析两个部分，单项测评结果汇总、详细结果记录及符合程度参见报告附录。

## 安全物理环境

### 已有安全控制措施汇总分析

### 主要安全问题汇总分析

* 1. **安全通信网络**

### 已有安全控制措施汇总分析

### 主要安全问题汇总分析

* 1. **安全区域边界**

### 已有安全控制措施汇总分析

### 主要安全问题汇总分析

* 1. **安全计算环境**

### 网络设备和安全设备

* + - 1. **已有安全控制措施汇总分析**
      2. **主要安全问题汇总分析**
    1. **服务器和终端**
       1. **已有安全控制措施汇总分析**
       2. **主要安全问题汇总分析**
    2. **应用和数据**
       1. **已有安全控制措施汇总分析**
       2. **主要安全问题汇总分析**
    3. **其他系统和设备**
       1. **已有安全控制措施汇总分析**
       2. **主要安全问题汇总分析**
  1. **安全管理中心**

### 已有安全控制措施汇总分析

### 主要安全问题汇总分析

* 1. **安全管理制度**

### 已有安全控制措施汇总分析

### 主要安全问题汇总分析

* 1. **安全管理机构**

### 已有安全控制措施汇总分析

### 主要安全问题汇总分析

* 1. **安全管理人员**

### 已有安全控制措施汇总分析

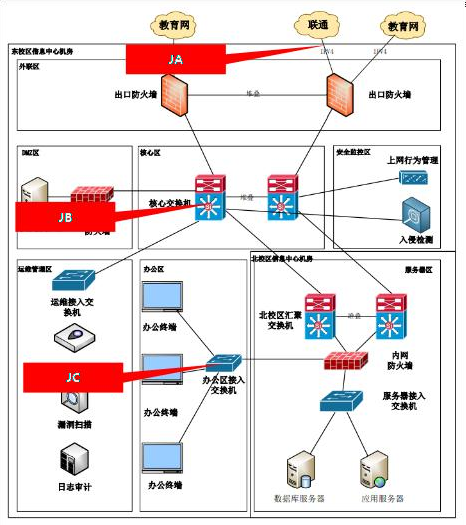
### 主要安全问题汇总分析

* 1. **安全建设管理**

### 已有安全控制措施汇总分析

### 主要安全问题汇总分析

* 1. **安全运维管理**
     1. **已有安全控制措施汇总分析**
     2. **主要安全问题汇总分析**
  2. **其他安全要求指标**
  3. **验证测试**



**图 3.1 漏洞扫描工具接入测试示意图**

对“XXX 大学全流程数字化业务系统”进行测评，涉及到漏洞扫描工具、渗透性测试工具集等多种测试工具。为了发挥测评工具的作用，达到测评的目的， 各种测评工具需要接入到被测系统网络中，并配置合法的网络 IP 地址。

针对被测系统的网络边界和抽查设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置各测试工具接入点，如图 3.1 所示：

### 漏洞扫描

根据接入点 JA 的漏洞扫描结果，汇总如下：

**表 3- 1 应用系统漏洞扫描结果统计表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **站点名称** | **扫描链接数** | **安全漏洞数量** | | | |
| **低** | **中** | **高** | **小计** |
| 1 |  |  |  |  |  |  |
| **安全漏洞数量小计** | | |  |  |  |  |

根据接入点 JB 的漏洞扫描结果，汇总如下：

**表 3- 2 主机漏洞扫描结果统计表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **IP 地址** | **操作系统** | **安全漏洞数量** | | | |
| **低** | **中** | **高** | **小计** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| **安全漏洞数量小计** | | |  |  |  |  |

根据接入点 JC 的漏洞扫描结果，汇总如下：

**表 3- 3 网络设备、安全设备漏洞扫描结果统计表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **IP 地址** | **操作系统** | **安全漏洞数量** | | | |
| **低** | **中** | **高** | **小计** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **IP 地址** | **操作系统** | **安全漏洞数量** | | | |
| **低** | **中** | **高** | **小计** |
| 11 |  |  |  |  |  |  |
| **安全漏洞数量小计** | | |  |  |  |  |

**全部安全问题描述参见报告附录 E。**

* + 1. **渗透测试**

本次测评不涉及。

## 单项测评小结

### 控制点符合情况汇总

根据附录 D 中测评项的符合程度得分，以算术平均法合并多个测评对象在同一测评项的得分，得到各测评项的多对象平均分。根据测评项权重，以加权平均合并同一安全控制点下的所有测评项的符合程度得分，并按照控制点得分计算公式得到各安全控制点的 10 分制得分。

n

Σ 测评项的多对象平均分×测评项权重

控制点得分= k=1

n

Σ

k=1

测评项权重

× 10，n 为同一控制点下的测

评项数，不含不适用的测评项。

下表给出了汇总测评结果，表格以不同颜色对测评结果进行区分，不符合的安全控制点采用红色标识，部分符合的安全控制点采用黄色标识。

**表 3- 4 测评结果分类统计表**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **通用**  **/**  **扩展** | **安全类** | **安全控制点** | **安全控制点得**  **分** | **符合情况** | | | |
| **符合** | **部分**  **符合** | **不符合** | **不适用** |
| **安全通用要求** | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **通用**  **/**  **扩展** | **安全类** | **安全控制点** | **安全控**  **制点得分** | **符合情况** | | | |
| **符合** | **部分**  **符合** | **不符合** | **不适用** |
| 1 | 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 |  |  |  |  |  |
| 3 | 防盗窃和防破坏 |  |  |  |  |  |
| 4 | 防雷击 |  |  |  |  |  |
| 5 | 防火 |  |  |  |  |  |
| 6 | 防水和防潮 |  |  |  |  |  |
| 7 | 防静电 |  |  |  |  |  |
| 8 | 温湿度控制 |  |  |  |  |  |
| 9 | 电力供应 |  |  |  |  |  |
| 10 | 电磁防护 |  |  |  |  |  |
| 11 | 安全通信网络 | 网络架构 |  |  |  |  |  |
| 12 | 通信传输 |  |  |  |  |  |
| 13 | 可信验证 |  |  |  |  |  |
| 14 | 安全区域边界 | 边界防护 |  |  |  |  |  |
| 15 | 访问控制 |  |  |  |  |  |
| 16 | 入侵防范 |  |  |  |  |  |
| 17 | 恶意代码和垃圾  邮件防范 |  |  |  |  |  |
| 18 | 安全审计 |  |  |  |  |  |
| 19 | 可信验证 |  |  |  |  |  |
| 20 | 安全计算环境 | 身份鉴别 |  |  |  |  |  |
| 21 | 访问控制 |  |  |  |  |  |
| 22 | 安全审计 |  |  |  |  |  |
| 23 | 入侵防范 |  |  |  |  |  |
| 24 | 恶意代码防范 |  |  |  |  |  |
| 25 | 可信验证 |  |  |  |  |  |
| 26 | 数据完整性 |  |  |  |  |  |
| 27 | 数据备份恢复 |  |  |  |  |  |
| 28 | 剩余信息保护 |  |  |  |  |  |
| 29 | 个人信息保护 |  |  |  |  |  |
| 30 | 安全管  理中心 | 系统管理 |  |  |  |  |  |
| 31 | 审计管理 |  |  |  |  |  |
| 32 | 安全管理制度 | 安全策略 |  |  |  |  |  |
| 33 | 管理制度 |  |  |  |  |  |
| 34 | 制定和发布 |  |  |  |  |  |
| 35 | 评审和修订 |  |  |  |  |  |
| 36 | 安全管  理机构 | 岗位设置 |  |  |  |  |  |
| 37 | 人员配备 |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **通用**  **/**  **扩展** | **安全类** | **安全控制点** | **安全控**  **制点得分** | **符合情况** | | | |
| **符合** | **部分**  **符合** | **不符合** | **不适用** |
| 38 |  |  | 授权和审批 |  |  |  |  |  |
| 39 | 沟通和合作 |  |  |  |  |  |
| 40 | 审核和检查 |  |  |  |  |  |
| 41 | 安全管理人员 | 人员录用 |  |  |  |  |  |
| 42 | 人员离岗 |  |  |  |  |  |
| 43 | 安全意识教育和  培训 |  |  |  |  |  |
| 44 | 外部人员访问管  理 |  |  |  |  |  |
| 45 | 安全建设管理 | 定级和备案 |  |  |  |  |  |
| 46 | 安全方案设计 |  |  |  |  |  |
| 47 | 产品采购和使用 |  |  |  |  |  |
| 48 | 自行软件开发 |  |  |  |  |  |
| 49 | 外包软件开发 |  |  |  |  |  |
| 50 | 工程实施 |  |  |  |  |  |
| 51 | 测试验收 |  |  |  |  |  |
| 52 | 系统交付 |  |  |  |  |  |
| 53 | 等级测评 |  |  |  |  |  |
| 54 | 服务供应商选择 |  |  |  |  |  |
| 55 | 安全运维管理 | 环境管理 |  |  |  |  |  |
| 56 | 资产管理 |  |  |  |  |  |
| 57 | 介质管理 |  |  |  |  |  |
| 58 | 设备维护管理 |  |  |  |  |  |
| 59 | 漏洞和风险管理 |  |  |  |  |  |
| 60 | 网络和系统安全  管理 |  |  |  |  |  |
| 61 | 恶意代码防范管  理 |  |  |  |  |  |
| 62 | 配置管理 |  |  |  |  |  |
| 63 | 密码管理 |  |  |  |  |  |
| 64 | 变更管理 |  |  |  |  |  |
| 65 | 备份与恢复管理 |  |  |  |  |  |
| 66 | 安全事件处置 |  |  |  |  |  |
| 67 | 应急预案管理 |  |  |  |  |  |
| 68 | 外包运维管理 |  |  |  |  |  |
| **安全控制点符合情况数量统计** | | | | |  |  |  |  |

### 安全问题汇总

对单项测评结果中存在的不符合项进行汇总后，形成了下表中的安全问题。

**表 3- 5 安全问题汇总表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **问题**  **编号** | **安全问题** | **测评对象** | **通用/**  **扩展** | **安全类** | **安全**  **控制点** | **测评项** | **测评项**  **权重** |
| **安全通用要求** | | | | | | | |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **问题**  **编号** | **安全问题** | **测评对象** | **通用/**  **扩展** | **安全类** | **安全**  **控制点** | **测评项** | **测评项**  **权重** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 整体测评结果分析

## 安全控制点间安全测评

* 1. **区域间/层面间安全测评**

**安全区域边界与安全计算环境安全计算环境与安全运维管理**

* 1. **整体测评结果汇总**

根据整体测评结果，对安全问题汇总表中的安全问题进行修正，风险等级为“高”、“中”、“低”，修正后的问题风险程度见表 4-1。

**表 4- 1 修正后的安全问题汇总表**[**3**](#_bookmark97)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **问题**  **编号**[**4**](#_bookmark98) | **安全问题描述** | **修正前**  **风险等级** | **修正理由描述** | **修正后**  **风险等级** |
| **安全通用要求** | | | | | |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

3该处仅列出风险等级有所修正的安全问题。

4该处编号与 3.13.2 安全问题汇总表中的问题编号一一对应。

# 安全问题风险分析

针对等级测评结果中存在的所有安全问题，采用风险分析的方法进行危害分析和风险等级判定，得到被测对象安全问题风险分析表见表 5-1。

风险分析主要结合关联资产和关联威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害或损失（风险等级）。风险分析结果的判断综合了相关系统组件的重要程度、安全问题的严重程度、安全问题被关联威胁利用的可能性、所影响的相关业务应用以及发生安全事件可能的影响范围等因素。风险等级根据最大安全危害的严重程度进一步确定为“高”、“中”、“低”。

**表 5- 1 安全问题风险分析表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **问题**  **编号** | **安全类** | **问题描述** | **关联资产**[**5**](#_bookmark101) | **关联威胁**[**6**](#_bookmark102) | **危害分析结果** | **风险**  **等级** |
| **安全通用要求** | | | | | | |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |

5 如风险值和评价相同，可填写多个关联资产。

6 对于多个威胁关联同一个问题的情况，应分别填写。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **问题**  **编号** | **安全类** | **问题描述** | **关联资产5** | **关联威胁6** | **危害分析结果** | **风险**  **等级** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **问题**  **编号** | **安全类** | **问题描述** | **关联资产5** | **关联威胁6** | **危害分析结果** | **风险**  **等级** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 等级测评结论

本次等级测评依据下述公式给出等级测评结论，等级测评结论由综合得分和最终结论构成。

**表 6- 1 等级测评结论判别依据**

|  |  |  |
| --- | --- | --- |
| **测评结论** | **判别依据** | **综合得分计算公式** |
| **优** | 被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统  综合得分 90 分以上（含 90 分）。 | 综合得分计算公式参见表格下方。 |
| **良** | 被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合  得分 80 分以上（含 80 分）。 |
| **中** | 被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合  得分 70 分以上（含 70 分）。 |
| **差** | 被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象  综合得分低于 70 分。 |

**综合得分计算公式**：

q Σp(j)

**（** Σm k **不符合测评项权重** + Σm k **部分符合测评项权重** ∗ 0. 5**）**

100 − [

Σj=1

k=1

i=1

p(j) k=1

Σ

m k i=1

q

Σ

i=1

**测评项权重**

] × 100

q 为被测对象涉及的安全类，p(j)为某安全类对应的总测评项数，不含不适用的测评项，m(k) 为测评项 k 对应的测评对象数，0.5 为部分符合测评项的得分，如果存在高风险安全问题则直接判定等级测评结论为“差”。

**表 6- 2 安全风险汇总表**

|  |  |  |  |
| --- | --- | --- | --- |
| **高风险问题数** | **中风险问题数** | **低风险问题数** | **综合得分** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中对第二级系统的要求，对“XXX 大学全流程数字化业务系统”的安全保护状况通过综合分析评价，等级测评结论如下：

“XXX 大学全流程数字化业务系统”中存在不符合项或部分符合项，系统面临中、低安全风险，本次测评的等级测评结论为 **XX**，综合得分为 **XX** 分。

# 安全问题整改建议

**表 7- 1 安全问题整改建议表**

|  |  |  |  |
| --- | --- | --- | --- |
| **问题**  **编号** | **安全类** | **问题描述** | **安全整改建议** |
| **安全通用要求** | | | |
|  |  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **问题**  **编号** | **安全类** | **问题描述** | **安全整改建议** |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

【正文结束】

# 附录 A 被测对象资产

## 物理机房

**附录 A 表-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 |  | 非常  重要 |
| 2 | 某校区信息中心机房 |  | 非常  重要 |

## 网络设备

**附录 A 表-2 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** |
| 1 | 核心交换机 | × |  |  |  | 非常  重要 | 2 |
| 2 | 某校区汇聚  交换机 | × |  |  |  | 非常  重要 | 2 |
| 3 | 服务器接入  交换机 | × |  |  |  | 非常  重要 | 1 |
| 4 | 办公区接入  交换机 | × |  |  |  | 重要 | 1 |
| 5 | 运维接入交  换机 | × |  |  |  | 重要 | 1 |

注：同类型设备在备注中注明设备数量。

## 安全设备

**附录 A 表-3 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** |
| 1 | 出口防火墙 | × |  |  |  | 非常 | 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
|  |  |  |  |  |  | 重要 |  |
| 2 | 上网行为管  理 | × |  |  |  | 非常  重要 | 1 |
| 3 | 入侵检测 | × |  |  |  | 非常  重要 | 1 |
| 4 | 内网防火墙 | × |  |  |  | 非常  重要 | 1 |
| 5 | Web 应用防  火墙 | × |  |  |  | 非常  重要 | 1 |
| 6 | 堡垒机 | × |  |  |  | 非常  重要 | 1 |
| 7 | 漏洞扫描 | × |  |  |  | 重要 | 1 |
| 8 | 日志审计 | × |  |  |  | 重要 | 1 |

注：同类型设备在备注中注明设备数量。

## 服务器/存储设备

**附录 A 表-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** | **备注** |
| 1 | 应用服务器 | XXX 大学全流程数字化  业务系统 |  |  |  |  | 非常重要 | 1 |
| 2 | 数据库服务器 | XXX 大学全流程数字化业务系统 |  |  |  |  | 非常重要 | 1 |
| 3 | 反代服务器 | XXX 大学全流程数字化  业务系统 |  |  |  |  | 非常重要 | 1 |

注：同类型设备在备注中注明设备数量。

## 终端/现场设备

**附录 A 表-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** | **备注** |
| 1 | 运维终端 | × |  |  | 重要 | 4 |

注：同类型设备在备注中注明设备数量。

## 系统管理软件/平台

**附录 A 表-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** | **备注** |
| 1 | 数据库系统 | 数据库服务器 |  |  | 非常  重要 |  |

注：同类型软件/平台在备注中注明设备数量。

## 业务应用系统/平台

**附录 A 表-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** |
| 1 | XXX 大学全流程数字化业务系  统 |  |  |  | 非常重要 |
| 2 | Nginx 中间件 |  |  |  | 重要 |
| 3 | Tomcat |  |  |  | 重要 |

## 数据类别

**附录 A 表-8 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 |

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

## 安全相关人员

**附录 A 表-9 安全相关人员**

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

## 安全管理文档

**附录 A 表-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 | 《XX 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。 |

|  |  |  |
| --- | --- | --- |
| **序号** | **文档名称** | **主要内容** |
| 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》 | 安全域划分操作手册。 |
| 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。 |

# 附录 B 上次测评问题整改情况说明

本次测评为“XXX 大学全流程数字化业务系统”本年度首次测评。

# 附录 C 单项测评结果汇总

## 安全物理环境

**附录 C 表-1 安全物理环境单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **物理位置选择** | **物理访问控制** | **防盗窃和防破**  **坏** | **防雷击** | **防火** | **防水和防潮** | **防静电** | **温湿度控制** | **电力供应** | **电磁防护** |
| 1 | 某校区信息中心机房 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 2 | 某校区信息中心机房 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 总计测评项 30 个，符合项 26 个，部分符合项 4 个，不符合项 0 个，不适用项 0 个 | | | | | | | | | | | | |

**附录 C 表-2 安全物理环境单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

## 安全通信网络

**附录 C 表-3 安全通信网络单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | |
| **网络架构** | **通信传输** | **可信验证** |
| 1 | 安全通信网络 | 符合 |  |  |  |
| 部分符合 |  |  |  |
| 不符合 |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | |
| **网络架构** | **通信传输** | **可信验证** |
|  |  | 不适用 |  |  |  |
| 总计测评项 4 个，符合项 3 个，部分符合项 0 个，不符合项 1 个，不适用项 0 个 | | | | | |

**附录 C 表-4 安全通信网络单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

## 安全区域边界

**附录 C 表-5 安全区域边界单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | |
| **边界防护** | **访问控制** | **入侵防范** | **恶意代码和垃圾邮**  **件防范** | **安全审计** | **可信验证** |
| 1 | 安全边界 | 符合 |  |  |  |  |  |  |
| 部分符  合 |  |  |  |  |  |  |
| 不符合 |  |  |  |  |  |  |
| 不适用 |  |  |  |  |  |  |
| 总计测评项 11 个，符合项 9 个，部分符合项 0 个，不符合项 2 个，不适用项 0 个 | | | | | | | | |

**附录 C 表-6 安全区域边界单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

## 安全计算环境

### 网络设备和安全设备

**附录 C 表-7 安全计算环境单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
| 1 | 核心  交换 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分 |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
|  | 机 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 2 | 某校区汇聚交换机 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 3 | 服务器接入交换机 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 4 | 办公区接入交换机 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 5 | 运维接入交换机 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 6 | 出口防火墙 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适 |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
|  |  | 用 |  |  |  |  |  |  |  |  |  |  |
| 7 | 上网行为管理 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 8 | 入侵检测 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 9 | 内网防火墙 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 10 | Web 应用防火墙 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 11 | 堡垒机 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 12 | 漏洞扫描 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
|  |  | 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 13 | 日志审计 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
|  | | | | | | | | | | | | |

**附录 C 表-8 安全计算环境单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

### 服务器和终端

**附录 C 表-9 安全计算环境单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
| 1 | 应用服务器 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 2 | 数据库服务器 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适 |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
|  |  | 用 |  |  |  |  |  |  |  |  |  |  |
| 3 | 反代服务器 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 4 | 运维终端 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
|  | | | | | | | | | | | | |

**附录 C 表-10 安全计算环境单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

### 应用和数据

**附录 C 表-11 安全计算环境单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
| 1 | XXX  大学全流程数字化业务  系统 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 2 | Ngin  x 中 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分 |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
|  | 间件 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 3 | Tom cat | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 4 | 数据库系统 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 5 | 用户数据 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 6 | 业务数据 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
| 7 | 审计数据 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **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** | **数据备份**  **恢复** | **剩余信息**  **保护** | **个人信息**  **保护** |
| 8 | 管理数据 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | | | | | | | | | | | | |

**附录 C 表-12 安全计算环境单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

### 其他系统和设备

**附录 C 表-13 安全计算环境单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | |
| **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** |
| 本报告不涉及 | | | | | | | | | | | | | |

**附录 C 表-14 安全计算环境单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全扩展要求** |
| 本报告不涉及 | | | |

## 安全管理中心

**附录 C 表-15 安全管理中心单项测评结果汇总表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | |
| **系统管理** | **审计管理** |
| 1 | 安全管理中心 | 符合 |  |  |
| 部分符合 |  |  |
| 不符合 |  |  |
| 不适用 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | |
| **系统管理** | **审计管理** |
|  | | | | |

## 安全管理制度

**附录 C 表-16 安全管理制度单项测评结果汇总表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | |
| **安全策略** | **管理制度** | **制定和发**  **布** | **评审和修**  **订** |
| 1 | 安全管理制度 | 符合 |  |  |  |  |
| 部分符合 |  |  |  |  |
| 不符合 |  |  |  |  |
| 不适用 |  |  |  |  |
|  | | | | | | |

## 安全管理机构

**附录 C 表-17 安全管理机构单项测评结果汇总表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | |
| **岗位设置** | **人员配备** | **授权和审**  **批** | **沟通和合**  **作** | **审核和检**  **查** |
| 1 | 安全管理机构 | 符合 |  |  |  |  |  |
| 部分符合 |  |  |  |  |  |
| 不符合 |  |  |  |  |  |
| 不适用 |  |  |  |  |  |
|  | | | | | | | |

## 安全管理人员

**附录 C 表-18 安全管理人员单项测评结果汇总表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | |
| **人员录用** | **人员离岗** | **安全意识教育和培**  **训** | **外部人员访问管理** |
| 1 | 安全管理人员 | 符合 |  |  |  |  |
| 部分符合 |  |  |  |  |
| 不符合 |  |  |  |  |
| 不适用 |  |  |  |  |
|  | | | | | | |

## 安全建设管理

**附录 C 表-19 安全建设管理单项测评结果汇总表（安全通用要求部分）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | |
| **定级和备案** | **安全方案设计** | **产品采购和使**  **用** | **自行软件开发** | **外包软件开发** | **工程实施** | **测试验收** | **系统交付** | **等级测评** | **服务供应商选**  **择** |
| 1 | 安全建设管理 | 符合 |  |  |  |  |  |  |  |  |  |  |
| 部分  符合 |  |  |  |  |  |  |  |  |  |  |
| 不符  合 |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |
|  | | | | | | | | | | | | |

**附录 C 表-20 安全建设管理单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

## 安全运维管理

**附录 C 表-21 安全运维管理单项测评结果汇总表（安全通用要求）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | | | | |
| **环境管理** | **资产管理** | **介质管理** | **设备维护管理** | **漏洞和风险管理** | **网络和系统安全管**  **理** | **恶意代码防范管理** | **配置管理** | **密码管理** | **变更管理** | **备份与恢复管理** | **安全事件处置** | **应急预案管理** | **外包运维管理** |
| 1 | 安全运维管  理 | 符  合 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 部分符  合 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **安全通用要求** | | | | | | | | | | | | | |
| **环境管理** | **资产管理** | **介质管理** | **设备维护管理** | **漏洞和风险管理** | **网络和系统安全管**  **理** | **恶意代码防范管理** | **配置管理** | **密码管理** | **变更管理** | **备份与恢复管理** | **安全事件处置** | **应急预案管理** | **外包运维管理** |
|  |  | 不符  合 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 不适  用 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | | | | | | | | | | | | | | | | |

**附录 C 表-22 安全运维管理单项测评结果汇总表（安全扩展要求部分）**

|  |  |  |
| --- | --- | --- |
| **序号** | **测评对象** | **符合情况** |
| 本报告不涉及 | | |

## 其他安全要求指标

**附录 C 表-23 其他指标单项测评结果汇总表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **测评对象** | **符合情况** | **其他安全要求指标** |
| 本报告不涉及 | | | |

# 附录 D 单项测评结果记录

## D.1 安全物理环境

### D1.1 某校区信息中心机房

* **D1.2 某校区信息中心机房**
* **D.2 安全通信网络**
* **D2.1 安全通信网络**
* **D.3 安全区域边界**
* **D3.1 安全边界**
* **D.4 安全计算环境**
* **D4.1 核心交换机**
* **D4.2 某校区汇聚交换机**
* **D4.3 服务器接入交换机**
* **D4.4 办公区接入交换机**
* **D4.5 运维接入交换机**
* **D4.6 日志审计**
* **D4.7 Web 应用防火墙**
* **D4.8 堡垒机**
* **D4.9 漏洞扫描**
* **D4.10 上网行为管理**
* **D4.11 入侵检测**
* **D4.12 内网防火墙**
* **D4.13 出口防火墙**
* **D4.14 XXX 大学全流程数字化业务系统**
* **D4.15 Nginx 中间件**
* **D4.16 Tomcat**
* **D4.17 应用服务器**
* **D4.18 数据库服务器**
* **D4.19 反代服务器**
* **D4.20 运维终端**
* **D4.21 数据库系统**
* **D4.22 管理数据**
* **D4.23 业务数据**
* **D4.24 审计数据**
* **D4.25 用户数据**
* **D.5 安全管理中心**
* **D5.1 安全管理中心**
* **D.6 安全管理制度**
* **D6.1 安全管理制度**
* **D.7 安全管理机构**
* **D7.1 安全管理机构**
* **D.8 安全管理人员**
* **D8.1 安全管理人员**
* **D.9 安全建设管理**
* **D9.1 安全建设管理**
* **D.10 安全运维管理**
* **D10.1 安全运维管理**

# 附录 E 漏洞扫描结果记录

## 应用系统

## 主机服务器

* 1. **网络设备、安全设备**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |
|  |  |  |  |  |
|  |  | | | |

# 附录 F 渗透测试结果记录

本次测评不涉及。

# 附录 G 常见威胁列表

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |