目录

1. [项目概述 1](#_bookmark0)
2. [测评依据 1](#_bookmark1)
3. [技术思路 1](#_bookmark2)
   1. [测评指标 1](#_bookmark3)
   2. [测评对象选择方法 4](#_bookmark6)
   3. [测评方法 5](#_bookmark7)
      1. [访谈 5](#_bookmark8)
      2. [检查 5](#_bookmark9)
      3. [测试 6](#_bookmark10)
   4. [测试工具 6](#_bookmark11)
   5. [工作内容 7](#_bookmark12)
4. [项目组织 9](#_bookmark13)
   1. [组织架构 9](#_bookmark14)
   2. [人员信息 12](#_bookmark15)
5. [项目实施计划 12](#_bookmark16)
   1. [测评基本流程 12](#_bookmark17)
   2. [实施计划 14](#_bookmark18)
6. [项目质量管理和控制 15](#_bookmark19)
   1. [过程质量控制管理 15](#_bookmark20)
      1. [过程质量管理风险 15](#_bookmark21)
      2. [过程质量风险控制 16](#_bookmark22)
   2. [变更控制管理 21](#_bookmark23)
      1. [变更管理存在的风险 21](#_bookmark24)
      2. [变更管理控制方法 21](#_bookmark25)
   3. [项目风险管理 22](#_bookmark26)
      1. [项目进度风险的管理 22](#_bookmark27)
      2. [项目协作与沟通风险的管理 24](#_bookmark28)
      3. [测评工作引入风险的管理 26](#_bookmark29)
   4. [保密控制管理 28](#_bookmark30)
      1. [人员保密管理 28](#_bookmark31)
      2. [设备保密管理 29](#_bookmark32)
      3. [文档保密管理 29](#_bookmark33)
7. [被测方签字确认 30](#_bookmark34)

### 项目概述

根据《中华人民共和国网络安全法》、《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》等政策法规及文件要求，北京 XXXX 公司计划对XXX 大学全流程数字化业务系统进行网络安全等级保护测评。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 大学委托北京 XXXX 公司计划于 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）相应等级的安全要求，找出 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，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安全防护能力，为等级保护工作的进一步开展提供指导。

### 测评依据

测评过程中主要依据的标准和文件如下：

* + 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 22240-2020《信息安全技术 网络安全等级保护定级指南》
  + GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》
  + GB/T 28449-2019《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）

### 技术思路

#### 测评指标

测评指标选取 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中第二级系统基本要求指标，包括“技术要求”中的第三级通用指标类（G2），业 务信息安全性指标类（S2），业务服务保证类（A2），以及“管理要求”中的所有

要求，安全控制指标如下表：

|  |  |  |
| --- | --- | --- |
| **安全类**[**1**](#_bookmark4) | **安全控制点**[**2**](#_bookmark5) | **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 |
| 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** |
|  | 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 |
| 外包软件开发 | 2 |

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

#### 测评对象选择方法

第二级信息系统的等级测评，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。可以抽查的测评对象种类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）和部分辅机房，应将放置了服务于信息系统的局部（包括整体）或对信息系统的局部（包括整体）安全性起重要作用的设备、设施的辅机房选取作为测评对象；
    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、入侵检测设备和防病毒网关等；
    6. 边界网络设备（可能会包含安全设备），包括路由器、防火墙、认证网关和边界接入设备（如楼层交换机）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、汇聚层交换机、路由器等；
    8. 承载被测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. 管理终端和主要业务应用系统终端；
    10. 能够完成被测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。

在本级信息系统测评时，信息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，每类应至少抽查两台作为测评对象。

#### 测评方法

本次等级测评现场实施过程中将综合采用访谈、检查和测试等测评方法。

##### 访谈

访谈是指测评人员通过与被测系统有关人员（个人/群体）进行交流、询问等活动，获取证据以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，访谈方法主要应用于安全管理机构测评、人员安全管理测评、系统建设管理测评和系统运维管理测评等安全管理类测评任务中。

在安全管理类测评任务中，测评人员依据定制的测评指导书（访谈问题列表） 对相关人员进行访谈，获取与安全管理有关的评估证据用于判断特定的安全管理措施是否符合国家相关标准以及委托方的实际需求。

##### 检查

检查是指测评人员通过对评估对象进行观察、查验、分析等活动，获取证据 以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，检查方 法的应用范围覆盖了安全物理环境测评、安全通信网络测评、安全区域边界测评、安全计算环境测评和安全管理中心等技术类测评任务，以及安全管理类测评任务。

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。

在安全通信网络测评、安全区域边界测评、安全计算环境测评和安全管理中心等测评任务中，测评人员综合采用文档查阅、网络拓扑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），用于判断目标系统各个层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

测试是指评估人员使用预定的方法/工具使评估对象产生特定的行为，通过查看、分析这些行为的结果，获取证据以证明信息系统安全保护措施是否有效的一类方法。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。

在安全通信网络、安全区域边界、安全计算环境等测评任务中，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。

#### 测试工具

绿盟远程安全评估系统（以下简称 RSAS）是由绿盟科技自主研发的漏洞管理工具，已获得《计算机信息系统安全专用产品销售许可证》以及英国西海岸实验室的 Checkmark 认证，能够通过采用高效、智能的漏洞识别技术主动对目标系

统中的资产进行漏洞检测、分析，并给用户提供专业、有效的漏洞防护建议。RSAS 的漏洞信息（10000 多条）精选于绿盟科技中文漏洞知识库，涵盖了常见操作系统、数据库、网络设备和应用程序的绝大多数可以远程利用的漏洞以及本地漏洞， 已获得 CVE 兼容性认证。

Web 网站脆弱性评估工具，可通过自动执行应用安全漏洞测试，扫描网站以识别嵌入的漏洞。通过对每个问题进行特定于扫描的说明，简化对扫描结果的解释。也支持通过模拟攻击来测试应用中的漏洞，最后根据安全风险的严重程度对漏洞进行风险等级划分。它使您能够在部署应用之前对其进行测试，然后持续不断评估生产环境中的风险。通过提供的修复步骤快速生成修订，包括代码示例和任务列表，帮助最大限度地保护 Web 应用免遭攻击、降低昂贵的数据泄露风险。

#### 工作内容

|  |  |  |  |
| --- | --- | --- | --- |
| **测评活动** | **工作内容** | | **输出** |
| 测评准备活动 | 项 目  启动 | 成立项目组，编制项目计划书，包含项目概述、工作依  据、技术思路、工作内容和项目组织等。 | 项目计划书 |
| 信 息  收 集  和 分析 | 收集被测系统总体描述文件，详细描述文件，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次等级测评报告等。 | 被测信息系统情况调研表 |
| 工 具  和 表  单 准备 | 调试本次测评过程中将用到的测评工具：漏洞扫描工具、 渗透性测试工具、性能测试工具和协议分析工具等。准备各类表单：现场测评授权书、文档交接单、会议记录  表单、会议签到表单。 | 选用的测评工具清单，打印的各类表  单 |
| 方案编制活动 | 需 求调研 | 根据已了解到的被测系统信息，分析被测系统及其涉及的业务应用系统，与信息化部门协商本次测评系统的测  评对象、范围、内容等。 | 被测系统总体情况 |
| 作 业  指 导  书 开发 | 描述单个测评对象，测评方法，操作步骤，以及预期结果。 | 作业指导书 |
| 测 评  方 案 | 项目概述、测评对象、测评指标、测试工具接入点、单  元测评实施内容等。 | 测评方案 |

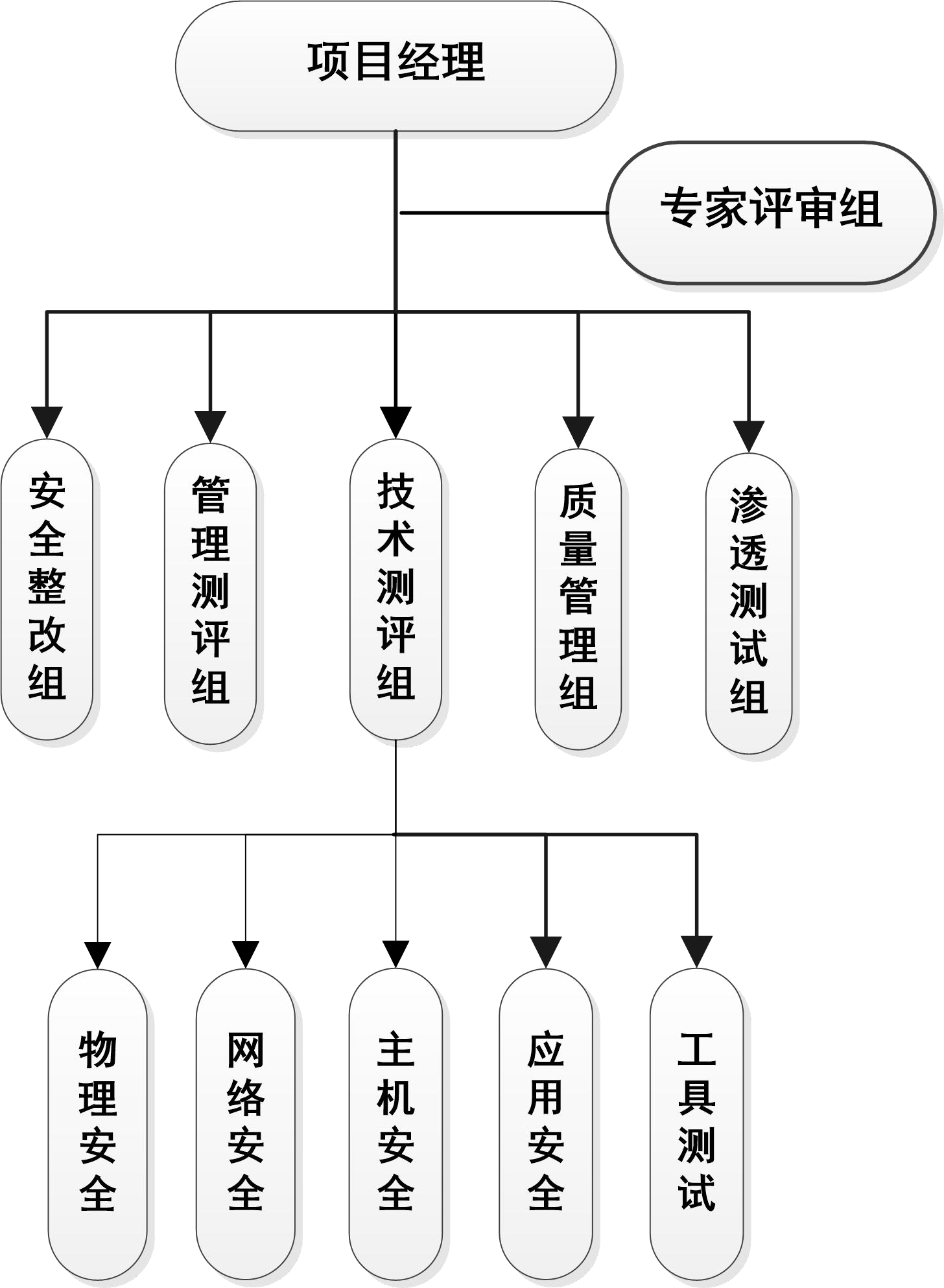
|  |  |  |  |
| --- | --- | --- | --- |
|  | 编制 |  |  |
| 方 案  评审 | 召开专家评审会，对测评方案进行评审 | 方案评审意  见 |
| 现场测评活动 | 现 场  测 评准备 | 召开测评现场首次会，测评机构介绍测评工作，交流测评信息。测评双方确认现场测评需要的各种资源，包括测评委托单位的配合人员和需要提供的测评条件等，确  认被测系统已备份过系统及数据。 | 测评活动配合表单 |
| 现 场  测 评  和 结  果 记录 | 通过访谈、文档审查、配置检查、工具测试和实地察看等方法，按测评指标项逐项开展测试，记录测评结果。 | 分层面的测评结果记录表 |
| 测 评  结 果  分 析  及 研讨 | 整理分析测评过程中的记录，形成问题分析表单。召开测评结果分析会，测评双方对测评结果进行确认，提出整改计划及整改建议。 | 被测系统问题分析及整改建议表。 |
| 整改问题及建议 | 现状  分析 | 信息系统已经采用安全技术与管理措施的状况进行分  析。 | 问题汇总单 |
| 问 题  分析 | 依据等级测评过程中发现的技术与管理安全问题，提出  整改建议。 |
| 方 案  设计 | 设计总体安全整改方案，包括安全技术及安全管理两部  分。 |
| 复测 | 现 场  测评 | 对初测中发现的问题进行回归测试。 | 复测结果记  录表 |
| 分析与报告编制活动 | 单 项  测 评  结 果判定 | 针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据，形成初步单项测评结果。 | 测评报告的单元测评的结果记录部  分 |
| 整 体测评 | 针对单项测评结果的不符合项，采取逐条判定的方法， 从安全控制间、层面间和区域间出发考虑，给出整体测  评的具体结果，并对系统结构进行整体安全测评。 | 测评报告的整体测评部  分 |
| 风 险 | 依据等级保护的相关规范和标准，采用风险分析的方法 | 测评报告的 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 分析 | 分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。 | 测评结果汇总及风险分析和评价部  分 |
| 测 评  结 论形成 | 在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。 | 测评报告的测评结果汇  总部分 |
| 测 评  报 告  编 制  及 评审 | 形成测评报告，包括概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等。 | 经过评审和确认的被测系统等级测评报告 |

### 项目组织

* 1. **组织架构**

为保障测评工作的顺利实施，北京 XXXX 公司交付部精选管理和技术人员组成项目团队，由项目经理、技术测评组、管理测评组、安全整改远程支持组、渗透测试组构成。同时，为了满足保密要求并保证项目质量，成立专家评审组、质量管理组。项目组织架构如图所示：



1. 项目经理

主持测评项目组的日常工作，按项目计划组织实施等级保护测评及相关工作进展；保持沟通，及时了解客户的需求，及时反馈阶段性的成果；跟踪项目的进度，协调项目组成员之间的合作；主导编写项目计划书、测评方案、问题列表、等级保护测评报告等。

1. 技术测评组

等级保护测评的技术检查部分，划分为六个测评方向，包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、工具测试。

* + 安全物理环境

负责信息系统的物理环境安全检查并记录测评结果，完成“等级测评报告” 中安全物理环境相关的部分内容。

* + 安全通信网络

负责信息系统的网络安全检查（网络结构、流量控制、通信安全等）并记录

测评结果，完成“等级测评报告”中安全通信网络相关的部分内容。

* + 安全区域边界

负责信息系统网络区域边界安全检查（包括区域边界设备、区域控制措施等） 并记录测评结果，完成“等级测评报告”中安全区域边界相关的部分内容。

* + 安全计算环境

负责信息系统所有单项设备（服务器、数据库、应用系统、数据备份等）的安全检查，并记录测评结果，完成“等级测评报告”安全计算环境相关的部分内容。

* + 工具测试

负责信息系统的网络和主机相关安全漏洞的工具扫描以及渗透测试，完成“等级测评报告”中工具测评相关的部分内容。

1. 管理测评组

负责信息系统的安全管理检查并记录测评结果，完成“等级测评报告”中安全管理相关部分内容。

1. 安全整改指导组

协助客户进行信息系统的安全整改，负责远程指导信息系统问题整改工作。

1. 专家评审组

专家评审组对本项目产生的过程文档，例如测评方案、作业指导书、测评记录表、等级测评报告、风险评估报告、问题汇总单等进行技术评审与检查，以找出其中的缺陷，反馈给项目经理。项目经理对过程文档上的不合格项或潜在的不合格项进行确认，采取相应的纠正和预防措施。

1. 质量管理组

严格按照《质量管理体系文件》要求和国家《信息系统 网络安全等级保护测评过程指南》和《信息系统 网络安全等级保护测评要求 》等规范文件，并严格遵循 ISO9001：2000 质量管理体系进行质量管理，对存在的不合格或潜在的不合格，质量管理组将向项目经理提交“测评质量审核报告”，项目经理对报告上的不合格项或潜在的不合格项进行确认，采取相应的纠正和预防措施，质量管理组跟踪验证改进措施的效果，直到合格为止。

1. 渗透测试组

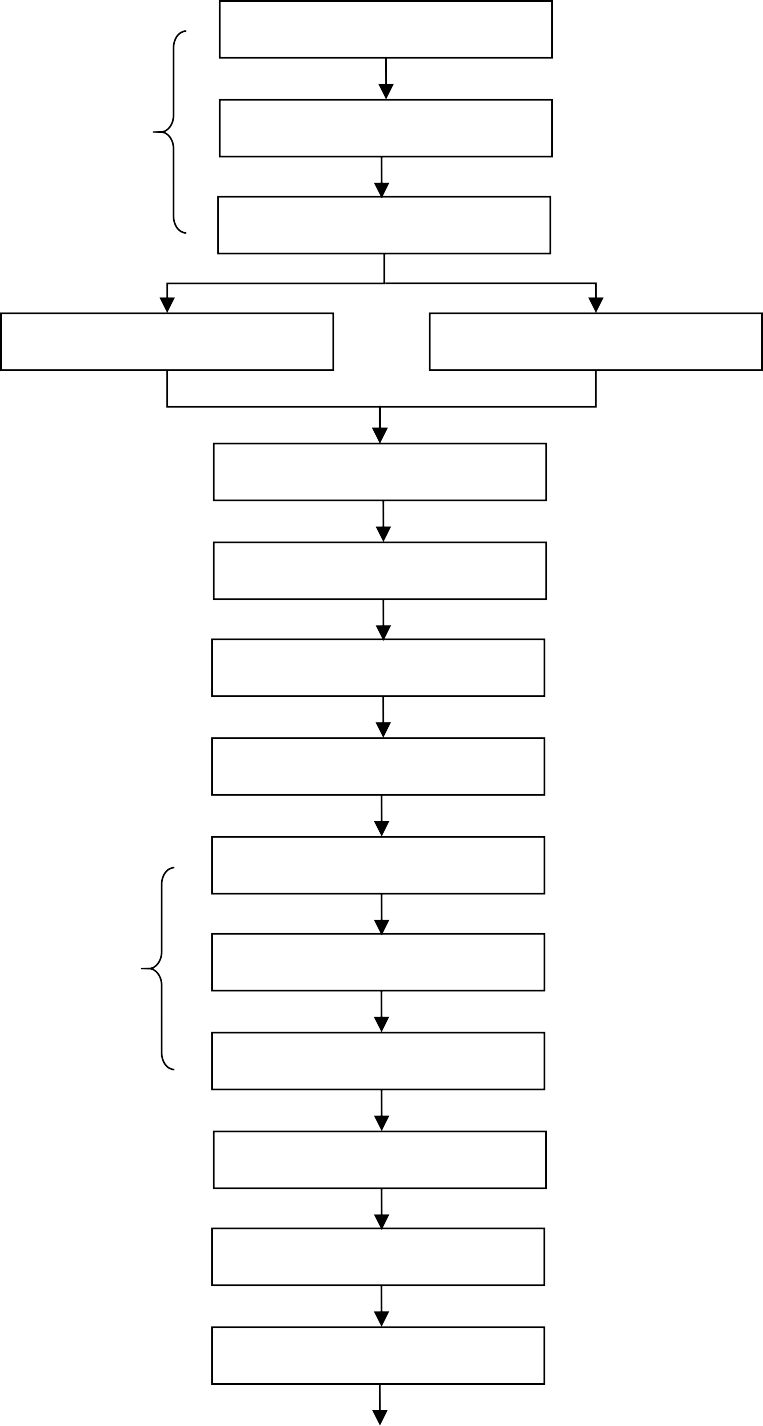
对被测系统开展渗透测试，负责完成“等级测评报告”中渗透测试相关的部分内容。

#### 人员信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **姓名** | **性别** | **人员资质** | **岗位** |
| 1 | XXX | 女 | XXX | XXX |
| 2 | XXX | 男 | XXX | XXX |
| 3 | XXX | 男 | XXX | XXX |
| 4 | XXX | 男 | XXX | XXX |

### 项目实施计划

* 1. **测评基本流程**



等级测评项目启动

信息收集与分析

工具和表单准备

测评对象确定

测评指标确定

测评工具接入点确定

测评内容确定

测评指导书开发

测评方案编制

测评实施准备

现场测评和结果记录

结果确认和资料归还

单项测评结果判定

单元测评结果判定

整体测评

系统安全保障评估

安全问题风险分析

等级测评结论形成

测评报告编制

测评准备活动

现场测评活动

分析与报告编制活

方案编制活动

* 1. **实施计划**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **阶段** | **工作内容** | **时间计划** | **对方配合内容** | **阶段输出** |
| 项目准备 | 起草项目计划 | 2 个工作日 | / | 项目计划书 |
| 评审论证 |
| 项目计划分解 |
| 评审论证 |
| 系统调查 | 准备调查表 | 2 个工作日 | 《配合填写信息系统基本情况调查表》 | 信息系统调查表现场记录表 |
| 收集调查结果 |
| 调查材料分析整  理 |
| 测评准备 | 制定核查方案 | 1 个工作日 | 审阅《等级保护测评方案》、  《风险告知书》、签字确认 | 测试工具准备， 测评方案 |
| 评审论证 |
| 制定测试方案 |
| 评审论证 |
| 准备测试工具 |
| 模拟环境测试 |
| 现场测评 | 准备委托书等现  场文档 | 5 个工作日 | 审阅签署《现场测评授权书》首次会议《会议签到表》  依据首次测评发现的所有问题清单进行问题整改  《现场记录表确认签字》  复测会议《复测会议签到表》  《复测记录表确认  签字》  《复测会议签到表》现场配合详情请参照等级测评方案中第 8 章 | 现场测评授权委托书、测试计划、测试报告 |
| 测试方案调整和  确认 |
| 制定核查计划 |
| 现场核查 |
| 记录核查结果 |
| 制定测试计划 |
| 现场测试 |
| 记录测试结果 |
| 报 告 | 核查材料整理 | 5 个工作日 | / | 等级测评报告 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 测试材料整理 |  |  |  |
| 撰写测评报告 |
| 评审论证 |
| 总结整个工作过  程 |

1. **项目质量管理和控制**
   1. **过程质量控制管理**
      1. **过程质量管理风险**

等级测评项目的质量是整个测评工作的核心，如测评质量没有保障，整个测评工作的意义就无从谈起。在质量管理方面，主要从以下几点进行说明：

##### 测评准备阶段

本活动是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，为实施测评做好文档及测试工具等方面的准备。

##### 方案编制阶段

本活动是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是开发与被测信息系统相适应的测评内容、测评实施手册等，形成测评方案。

##### 现场测评阶段

本活动是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格执行测评实施手册，分步实施所有测评项目，包括单项测评和系统整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

##### 分析与报告编制阶段

本活动是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《信息系统 网络安

全等级保护测评要求》的有关要求，通过单项测评结果判定和系统整体测评分析等方法，分析整个系统的安全保护现状与相应等级的保护要求之间的差距，综合评价被测信息系统保护状况，并形成测评报告文本。

### 过程质量风险控制

1. 测评准备阶段

a. 没有项目计划

项目计划是对整个测评工作进行项目描述、工作流程、技术思路、工作内容和项目组织，时间控制等控制，保证项目能够按期顺利的完成。

风险点:如果没有制作项目计划，会导致后期项目任务不明确、管理无序、失控，工作不能按期完成。

控制方法：在进行测评工作之前，做好项目计划，对每个测评人员明确分工。

1. 方案编制阶段
2. 测评指标选取不准确

测评指标是在被测系统基本情况分析后，得出被测系统的定级结果，包括业务信息安全保护等级和系统服务安全保护等级。从 GB/T 22239-2019《信息系统网络安全等级保护基本要求》中选择相应等级的安全，包括对 ASG 三类安全要求的选择。

风险点：如果测评指标选取不明确，会造成错误定级，按照错误的等级进行测评工作，使用错误的测评方法，将造成测评结果偏离，例如：某单位系统服务安全保护等级为 2 级；则该系统的测评指标将包括 GB/T 22239-2019《信息系统网络安全等级保护基本要求》“技术要求”中的 2 级通用指标类（G2），2 级业务信息安全指标类（S2），2 级系统服务安全指标类（A2），以及第 2 级“管理要求”中的所有指标类。如果指标错误，会影响到后期的所有工作，耗费了各方面的资源，使项目不能按期顺利完成，同时也给公司带来巨大的损失。

控制方法：通过召开评审会，详细分析被测单位的信息系统，对被测单位做好准确定级，明确测评指标，顺利做好测评工作。

1. 项目组每个成员包括工具测试人员开发测评指导书时对测评方法选取不

当

测评指导书是具体指导测评人员如何进行测评活动的文件，是现场测评的工具、方法和操作步骤等的详细描述，是保证测评活动可以重现的根本。因此，测评实施手册应当尽可能详尽、充分。

风险点：如果测评指导书不使用，会直接导致测评工作的错误进行，包括测评项（每个测评项可能对应多个测评方法）、测评方法（访谈、文档审查、配置检查、工具测试和实地察看等多种方法）、操作步骤和预期结果等。这样所做的整个过程都将是一个错误的过程，所做的工作也就没有应用价值，会延长工期， 会造成违约赔偿问题，在人员、财力、时间的浪费上都无法弥补，也会影响到公司的荣誉。

控制方法：把各层面上的测评指标结合到具体测评对象上，并说明具体的测评方法，如此构成一个个可以具体测评实施的单元。参照《信息系统 网络安全等级保护测评要求》，结合已选定的测评指标和测评对象，概要说明现场测评实施的工作内容来编制测评实施手册，完成之后，对其进行评审，通过以后，由技术负责人签字确认。

1. 测评实施工期时间测算不准确

测评实施工期是对整个项目进行的一个时间控制，这样便于把握整个项目的进展。

风险点：测评实施工期不准，使整个项目的工期延后，测评质量下降，影响后续项目的开展。

控制方法：召开评审会，由专家选取项目实施工期。

1. 测评现场人员分工计划不合理

风险点：专业技术人员分配不合理，会造成对测评的测评不够全面、深入， 不能得到完整要的数据，不能站在合适的技术人员的角度去测评系统。另外，现场测评人员分工不合理，影响项目的进展，人员太多造成现场混乱，现场测评时间浪费，工作质量下降，人员太少会使测评任务无法按期完成。

控制方法：通过评审会，对项目进行分析，合理的安排测评人员。

1. 测评方案没有评审

测评方案是等级测评工作实施的基础，指导等级测评工作的现场实施活动。测评方案应包括但不局限于以下内容：项目概述、测评对象、测评指标、测评工

具的接入点、单项测评实施、系统测评实施以及配套的测评实施手册等。

风险点：测评方案没有经过评审就投入使用，其中有些信息可能不准确、不全面或者是错误的，如果按照这样的测评方案进行，就会造成误操作，效率降低， 测评结果也会有偏差，将不能得到准确可靠的数据。

控制方法：召开方案评审会，详细分析被测系统的整体结构、边界、网络区域、重要节点等。初步判断被测系统的安全薄弱点。分析确定测评对象、测评指标和测试工具接入点，确定测评内容及方法。编制测评方案文本，并对其内部评审。取得被测机构对测评方案所有内容的签字确认，对测评方案进行认可，并签字确认。

1. 测评方案在内部评审时没有签字和批准

风险点：测评方案没有经过签字和批准就进行测评，如果方案发生变化，而测评人员又不知道，这样就会造成不必要的损害，已经做过的测评工作就需要重新进行。

控制方法：测评方案在内部评审时签字批准后再投入项目中。

1. 现场测评阶段
2. 测评方案未经被测单位签字认可就开展实施

风险点：测评方案没有经过被测方签字和批准就进行测评，会使公司承担一定的法律和事故责任，对公司在信誉、财力上造成一定的损害。

控制方法：测评方案经过被测单位签字确认后在进行项目的实施。

1. 现场测评正式进场前未与委托方签署《现场测评授权书》

风险点：现场测评正式进场前未与委托方签署《现场测评授权委托书》，造 成对现场测评需要的各种资源，包括被测单位的配合人员和需要提供的测评条件， 现场测评实施具体时间不明确，无法确定测评项目双方责任。

控制方法：现场测评正式进场前与委托方签署《现场测评授权委托书》。

1. 项目负责人没有根据委托方提出的意见和建议，对测评方案进行必要的更

新

风险点：如果没有按照委托方的意见对测评方案进行更新，项目将不能顺利

的往下开展，委托方将会不配合测评工作的开展，另外测评结果也会有偏差，甚至造成测评项目停止。

控制方法：根据委托方提出的意见和建议，项目负责人对测评方案进行必要的更新，并做更新记录，重新进行内部评审并获得批准后重新装订测评方案。

1. 测评结果的记录不准确

测评结果是整个测评过程的一个记录，测评人员与被测系统有关人员（个人

/群体）进行交流、讨论、检查等活动，获取相关证据，了解有关信息的数据反映。

风险点：测评结果错误，将不能给被测单位信息做一个正确的反映，对所做的访谈、文档审查、配置检查、工具测试和实地察看等这些方面的数据都不能真实体现，严重的话可能需要重新进行测评，那将会造成不可估量的损失。

控制方法：可以通过现场录音，校准员对结果进行校准。

1. 测评结果没有用户签字确认

风险点：没有经过用户签字的测评结果是没有可信度的，如果其中存在问题， 用户可能会否认，降低对测评结果的可信度，影响到后续的工作。

控制方法：现场测评后的记录应及时让用户签字确认。

1. 管理类测评文档审查中，测评人员对文档审查的覆盖面不全

管理类测评文档是对测评流程进行记录的一个过程，包括现场测评准备、访谈、文档审查、配置检查、工具测试、实地察看、测评结果确认。

风险点：管理类测评文档审查中，测评人员对文档审查的覆盖面不全，这样会缺少某方面的资料，使测评结果参考不够全面，影响后续工作。

控制方法：建立管理类文档审查清单。

1. 测评核查表审查结果记录落实

核查表是按照被测单位的等级要求进行核查的测评项清单。

风险点：如果不对测评核查表审核的结果进行记录，就不知道哪些设备核查过，哪些没有核查，不便于结果的统计，容易造成漏查。

控制方法：对已查设备做好记录，制作补查表，进行补查。

j. 上机验证存在误操作的风险

风险点：上机误操作会得到错误的数据，使测评结果不准确，可能会对系统造成一定的影响，造成系统数据丢失，或损害到了其中的某些配置。

控制方法：测评人员要有一定的专业技术知识储备，原则上由被测单位技术

人员按照作业指导书进行操作，要有一定的应急预案，在上机操作之前对机器上的资料进行备份。

1. 分析与报告阶段
2. 测评分析应根据信息系统的不同等级进行不同强度的分析和概括

在现场测评工作结束后，测评机构应对现场测评获得的测评结果进行汇总分析，形成等级测评结论，并编制测评报告。测评人员在初步判定单项测评结果后， 还需进行系统整体测评，经过系统整体测评后，有的单项测评结果可能会有所变化，需进一步修订单项测评结果，而后形成等级测评结论。

风险点：不同信息系统被定为不同的等级，应进行不同强度的分析和概括， 等级、强度不能够相适应的进行分析，会对测评最终的测评报告造成偏差，影响被测单位的系统结果分析。

控制方法：按照不同等级测评强度的要求，进行不同等级强度的分析和概括。

1. 整体测评不应只考虑单项测评结果

风险点：系统整体测评如果只考虑单项测评结果，不能针对单项测评的不符合项，采取逐条判定的方法，也不能够从安全控制间、层面间和区域间出发考虑， 给出系统整体测评的具体结果和结论，会影响到系统结构的整体安全测评。

不对其他相关项进行分析，无法正确判断该测评项与其他相关安全控制项能否发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足。

不能分析出与该测评项相关的其他层面测评对象能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足。

不能分析出该测评项相关的其他区域测评对象能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足。

控制方法：从安全角度分析被测系统整体结构的安全性，从系统角度分析被测系统整体安全防范的合理性。整体测评除要考虑单项测评结果之外，应根据不同信息系统的特点，进行有针对性的分析，召开内部专家人员会议共同分析讨论， 对测评结果进行补充。

1. 单项测评项的测评结果判定不准确

风险点：测评指标的单项测评结果情况不准确，对测评结果将不能给出真实的反映，会对下面的整体测评造成一定的影响。

控制方法：按层面分别汇总不同测评对象对应测评指标的单项测评结果情况， 包括测评多少项，符合要求的多少项等内容，一般以表格形式列出。表格中清楚的描绘出测评对象，测评指标。并以“”表示“符合”，“”表示部分符合， “×”表示“不符合”，“N/A”表示“不适用”。这样对单项测评结果的判断就很 清晰准确了，另外由质量监督员对判定结果进行审核，出现争议，由技术负责人 进行仲裁。

1. 对测评报告的审核没有通过评审会进行

风险点：测评报告的审核如果没有通过评审会进行，中间存在的问题可能就无法体现出来，对被测单位的系统状况也无法清晰的了解，可能会得到不准确的结论。

控制方法：对测评报告的审核应通过评审会进行，应选择具有高职称的技术人员实施参加。

1. 没有对测评报告的编制格式统一

风险点：测评报告的编制格式不统一，容易造成文档混乱，不便于管理，也不方便查询。

控制方法：定制统一的文档编号规范，文档盖章规范。

## 变更控制管理

### 变更管理存在的风险

项目组成员受外部因素影响出现变动。

在项目进行过程中，项目组成员因工作调动、外出学习、身体健康等原因， 需要变更人员、调整成员分工的情况，会对测评按时保质完成造成影响。

### 变更管理控制方法

风险点：在项目进行过程中，项目组成员因工作调动、外出学习、身体健康等原因，需要变更人员、调整成员分工的情况，会对测评按时保质完成造成影响。

控制方法：在项目组成立后，原则不允许人员中途退出。确实无法避免，由项目经理指派其他有能力的人员代替，相关人员需写出工作移交报告，妥善完成工作交接程序。

## 项目风险管理

### 项目进度风险的管理

##### 项目进度管理存在的风险

项目进度管理在项目管理体系中是比较重要的一个方面，要求在保证项目质量的前提下按时完成项目是项目进度管理的主要目的。项目进度管理主要从项目时间计划和项目时间控制等方面对项目进行管理，保证测评项目按时完成。等级测评项目管理中应关注以下几点：

1. 与委托方交涉过程中委托方不重视等级测评造成的项目时间拖延，如需要委托方确认的项目计划书委托方迟迟不给答复，需要委托方提供的资料委托方不按时交给项目组等；
2. 没有合理安排现场测评活动时间，造成无法进行现场测评和造成委托方损失等情况。如安排在委托方工作繁忙阶段做测评、安排在被测系统业务高峰期做渗透测试等活动；
3. 没有合理计划项目周期造成成本增加影响其他项目工作进行；
4. 项目中时间把握不准确造成项目时间延误，如在现场测评阶段和方案编制阶段时间的把握不准确，导致阶段工作没有按时完成等。

##### 项目进度管理控制方法

时间管理关系效益，因此需要在项目的启动阶段时对项目合理的计划，与委托方沟通使其对测评工作充分重视，并与其协商合理安排现场测评时间，把握阶段时间控制。具体方法如下：

##### 现场准备阶段

**风险点**：被测单位为测评项目组提供其所需要的各种资料，包括被测单位的各种方针文件、规章制度及相关过程管理记录、被测系统总体描述文件网络拓扑图、管理记录文档等。若委托方提交相关信息系统资料超期、不及时将导致项目

整体工期拖延。

**控制方法**：应对委托方详细介绍测评的重要性和必要性，说明提供信息资料对整个测评过程的重要性。提供详细的信息系统资料准备清单，指导被测单位准备相关信息资料。

##### 方案编制阶段

1. **风险点**：测评方案初稿未通过测评项目组全体成员评审

若评审时间过长将影响项目后续工作开展。测评项目组将确定的测评方案提交给被测单位后，被测单位应对该测评方案进行签字认可，但若迟迟未认可签字， 将致使后续工作没有办法进行，影响项目整体进度。

**控制方法：**1、项目组制定会议日程，对计划内的任务要准时完成。

2、方案经与委托方协商确定后，随着项目的开展，应适时提醒委托方提供时间、人员等的配合。

1. **风险点：**安排工具测试时没有避开被测系统的业务高峰期。

**控制方法：**实施现场测评或工具测试前应充分与被测单位进行协商，确定合适的时间点实施测评。

1. **风险点：**测评实施整体工期测算不准确导致工期拖延项目成本提高、影响其它后续项目工作安排。

**控制方法：**测评方案初稿形成后应召开内部专家评审会，针对时间安排、测评对象等关键点进行评审并签字确认。

1. 现场测评阶段

风险点：现场测评阶段需召开现场测评首次会，测评项目组介绍测评工作， 交流测评信息，进一步明确测评计划和方案中的内容。测评双方确认现场测评需要的各种资源，包括被测单位的配合人员和需要提供的测评条件等。被测单位签署现场测评授权委托书。但现场准备阶段时间控制不好耗费了很长时间，造成的项目工期的延误。

控制方法：对项目准备阶段进行时间计划，制定首次测评现场会会议日程。

1. 分析报告阶段

风险点：在分析报告阶段要进行单项测评结果判定、单项测评结果汇总分析、系统整体测评分析、综合测评结论形成、测评报告编制等五个阶段。阶段间的工

作环环相扣，如果时间安排不合理将导致下一阶段的工作无法继续或整体工期拖延。

控制方法：制定详细的分析报告阶段时间计划。项目组成员间积极沟通，协调工作开展。

### 项目协作与沟通风险的管理

##### 协作与沟通原则

为保证项目顺利实施，项目组成员应遵循互相协作、主动沟通和尽早沟通的原则。项目实施中，只有互相协作、尽早沟通、主动沟通才能及时发现问题和解决问题，保证项目的顺利实施。

##### 沟通管理方法

为避免项目人员被动式、应付式沟通，随意而行、混乱无序，为让项目人员明确自己的沟通职责，特制定下列沟通计划：

1. 与委托方的沟通
2. 在测评准备阶段，业务受理人员应告知委托方信息系统等级测评所必须提交的详细资料；
3. 项目负责人应在测评项目立项后，应向委托方揭示测评风险，说明测评过程中可能带来的风险，并说明风险规避的方法；
4. 在测评项目准备阶段，项目负责人应与委托方沟通，对测评时间、人员等做出合理安排，以保证测评实施工期避开被测系统的业务高峰期，确保测评项目顺利完成；
5. 项目负责人在测评方案通过内部评审后，及时与委托方交流，明确告知委托方测评范围，以便委托方提供与测评方案吻合的配合资源（人力、场地）；
6. 测评核查表审查结果记录一定要由委托方人员签字，确保记录结果的有效性；
7. 现场测评时，项目组成员与委托方人员沟通时，应采用对方能接受的沟通风格。注意肢体语言、语态给对方的感觉。始终向委托方传递一种诚实，公正态度。不论在何种情况下，都要避免与委托方人员产生言语上的冲突；
8. 测评组作为一个整体对外意见要一致，一个团队要用一种声音说话，避免

委托方对测评人员公平公正度产生误解；

1. 现场测评时，如果出现测评人员与委托方沟通效果不理想，要及时认识问题，寻求相关领导和职能部门的协助，合理的借用外部力量达到项目组的既定目标。
2. 部门间沟通
3. 在委托方提交信息系统等级测评所必需的资料后，交付部应会同业务受理部，组织专家对委托方提供的资料做详细分析和整理。判定测评项目是否可以立项，以保证测评工作顺利开展；
4. 交付部应定期与质量保障部沟通，以便质量保障部提供相应的软、硬件保障，确保测评质量。
5. 项目组成员间沟通
6. 项目组成员内部沟通应注重文档化，实现团队项目经验的有效积累；
7. 项目组成员在项目实施中应注重技术性沟通，方便项目新成员提高技术水平；
8. 项目负责人通过各种途径将意图传递给项目执行人员并使项目执行人员理解和执行。避免项目执行人员理解不清最终导致项目混乱甚至项目失败；
9. 项目组成员在完成各自的测评工作后，应以项目日报形式向项目负责人汇报，以便项目负责人把握项目进度；
10. 项目组成员完成测评报告后，报告所得出的结论应协商一致，避免委托方对测评报告的结果提出异议。
11. 与领导的沟通
12. 应清楚各级领导的权限和角色，解决问题时一定是要找到关键路径上的关键领导，避免将问题同时抛给多个领导，造成领导之间的沟通成本加大，影响问题的解决效率；
13. 对于项目中不可能完成的工作，不要一味的向领导妥协，这既是对工作的负责，也是对项目组的负责。

通过多方面的沟通管理，为提升信誉度，与客户建立良好的合作关系，打好坚实的基础。

### 测评工作引入风险的管理

##### 测评工作过程的风险

1. 验证测试影响系统正常运行

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

1. 敏感信息泄漏

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

1. 对测评结果存有争议

测评机构和被测单位对测评结果可能存在争议。

##### 风险管理控制方法

为了对测评过程存在的风险进行有效规避，将针对测评流程通过如下几个阶段实施风险管理：

##### 测评准备阶段

1. **风险点：**准备阶段在与委托方进行初次沟通协商后，需要委托方提供一定量的信息系统相关资料，以便通过这些资料的了解研究，确定下一步测评工作的开展方法，而这些资料可能涉及到委托方的内部机密，如果此类资料丢失或泄露， 将对委托方产生较大影响及造成经济损失。

**控制方法：**在与委托方首次沟通时，签署《委托阶段保密协议》；从委托方获取资料时，应填写《资料交接单》，并经委托方签字确认后方可使用。

1. **风险点：**测评实施过程中可能需要对设备和系统进行上机检查，渗透测试等，而这些操作可能会对委托方的系统运行设备安全等造成一定威胁，如果在测评项目准备阶段没有向委托方陈述此类题，可能将导致实施过程中的委托方系统服务中断，设备宕机等问题。

**控制方法**：在与委托方沟通协调时，签署《风险告知书》，并建议其做相应的保护措施，被测方制定应急预案。

1. **风险点**：测评工作是一项严密而又复杂的工作，其内容涉及信息系统的各个方面，如果测评准备阶段没有将测评工作的意义及流程告知委托方，将造成后

期配合上的隐患，导致项目进展缓慢，或无法有序开展。

**控制方法：**与委托方沟通协调时，有必要对项目目的、流程及需要配合的事宜完整的告知委托方，避免由此引发的不理解，不配合。

1. **风险点**：测评工作需要有相当专业技术能力的人员和相关测评工具的配合， 如果测评工具准备不当或测评人员知识储备量不足，都将对测评工作的开展及测 评结果造成影响。

**控制方法：**组织测评队伍时应对相关人员资格进行审核，有关设备的操作人员需定期培训，并在确定了测评所需设备后，对所需设备进行校准。

1. **风险点**：由于测评过程中涉及到上机检查，实地查看等，检查过程中如遇突发情况或突发威胁，如没有对此类情况进行充分考虑，势必造成测评过程的中断、造成设备损坏甚至人身事故。

**控制方法：**对可能涉及到的安全事故应制定相应的《应急预案》保护措施， 并通告全体测评人员。

1. 方案编制阶段
2. **风险点**：方案编制时，需对项目所需的时间、人员安排等做出科学合理的规划，否则不但会造成人员时间浪费，还会增加项目成本。

控制方法：方案初稿应进行内部专家评审，并由技术负责人签字确认方可定稿。

1. **风险点**：测评方案中涉及到委托方的机密信息，如果对方案的流转，存储控制不当，将造成委托方资料泄密的严重后果。

控制方法：进入方案编制阶段后，应通过文件加密等方式禁止项目无关人员查阅此方案，方案确定后，如需递交委托方时，应经相关负责人批准后亲自送达至委托方，并经委托方签字确认接收。

1. 现场测评阶段
2. **风险点**：现场测评过程中部分项目需要工具测试或上机验证，此过程中势必会对系统运行造成一定影响，并存在一定风险，如果在未告知用户的情况下进行此类操作，不但可能会对用户系统造成危害甚至经济损失，还会对项目后续工作形成阻碍。

控制方法：在确认需要进行工具测试或上机验证时，应再次将此操作可能产

生的危害告知委托方，并建议其做相应的保护措施；需上机验证的，应尽量要求委托方提供专人操作，如必须测评人员操作的，应与委托方签署委托协议，明确责任。

1. **风险点**：现场测评过程中部分项目需要实地查看，此过程中可能涉及到精密仪器、电力环境等的确认，如果未与委托方充分协调可能造成设备损坏或人身安全事故。

控制方法：在实地查看过程中应由委托方配专职人员协同讲解，避免单人查看操作，出现事故后立即执行《应急方案》措施。

1. **风险点**：现场测评过程中涉及到需要委托方提供的备阅文档，如果不进行相关保护及确认，容易造成资料丢失、外泄等情况。

控制方法：现场测评工程需要委托方提供文档时应与其签订《资料交接单》， 待资料使用完毕后根据《资料交接单》提供的清单，逐一核查，统一归还并签字确认。

1. 分析与报告阶段
2. **风险点**：对现场测评结果进行综合分析是一项细致全面的工作，如果对系统分析不到位或不全面，必定会影响最终的结果报告，造成报告失真。

控制方法：测评结果分析工作应由资深测评工程师或专家担任，综合评定后的初稿需经内部专家评审会评审通过，并签字确认方能定稿。

1. **风险点**：结果报告中涉及到委托方的机密信息，如果对报告的流转，存储控制不当，将造成委托方资料泄密的严重后果。

控制方法：进入报告编制阶段后，应通过文件加密等方式禁止项目无关人员查阅此报告，报告确定后，如需递交委托方时，应经相关负责人批准后亲自送达至委托方，并经委托方签字确认接收。

## 保密控制管理

### 人员保密管理

1. 未经授权方书面许可，被授权方测评人员不得将所知的授权方秘密信息以任何方式提供给任何第三方；
2. 未经授权方书面许可，被授权方测评人员不得擅自披露授权方的秘密信息；
3. 除了双方约定的工作目的之外，未经授权方书面许可，被授权方测评人员不得擅自使用授权方的秘密信息；
4. 对于项目实施过程中采集到的数据、信息和服务结果的保管、访问， 被授权方无关人员不能访问；因工作需要必须访问的人员，被授权方应进行严格的访问控制；被授权方应对管理以上秘密信息的人员进行严格筛选；
5. 被授权方测评人员在项目实施过程中负有风险预估、及时预报的责任， 在具有风险性的工作进行之前应向授权方说明该项工作将带来的影响；
6. 被授权方保证，不会利用与本次等级测评项目相关的秘密信息为自己或第三方开发信息、技术和产品，或与另一方进行商业竞争。

### 设备保密管理

1. 未经授权方书面许可，被授权方的移动设备、个人信息处理设备等不得擅自接入授权方的生产及办公网络；
2. 授权方以书面形式同意被授权方使用一定的资源，如网络、NOTES 等， 被授权方只能将其用于本次项目工作目的，不得从事任何侵害授权方利益的活动；
3. 授权方以书面形式同意被授权方使用的工具、技术和方法，如扫描、测试等，被授权方只能将其用于本次项目工作目的，不得用来从事任何侵害授权方利益的活动。

### 文档保密管理

1. 未经授权方书面许可，被授权方不得带走从授权方得到的任何文档、图纸、资料、磁盘、胶片等载有授权方秘密信息的介质；
2. 被授权方因工作需要必须携带的数据资料，须经授权方书面许可后加密或封条存储；
3. 工作期满离开时，被授权方应将包含授权方秘密信息的一切资料及其复印件如数交还授权方，未经授权方书面许可，被授权方不得擅自保留。

# 被测方签字确认

受 **XXX 大学** 委托，北京 XXXX 公司对 **XXX 大学全流程数字化业务系统**进行 等级测评工作，在项目准备阶段，经过认真讨论和研究后制定了《**XXX 大学全流程数字化业务系统网络安全等级保护测评项目计划书**》。如果被测评单位对该项 目计划书中涉及的时间、人员、流程等安排没有异议，请在下方的 “同意该项 目计划”栏中签字，如果有异议，请填写异议条款，北京 XXXX 公司将依据“异议条款”对项目计划书进行修改和变更以期最终就测评项目计划书达成一致意见。对项目计划书意见如下：

一、同意该项目计划

签字确认： XXX

签字日期：2020 年 10 月 29 日

二、不同意，异议如下：

1、

2、

签字确认： 签字日期： 年 月 日