项目编号： （DJCP2019XXXXX）-XXXXX

**目录**

1. [概述 1](#_bookmark0)
2. [目标 1](#_bookmark1)
3. [等级测评中可能产生的风险 1](#_bookmark2)
4. [风险规避措施 2](#_bookmark3)

# 概述

风险规避是风险应对的一种方法，是指通过计划的变更来消除风险或风险发生的条件，保护目标免受风险的影响。为了有效应对本次等级测评过程中可能存在的各类风险，特制定本方案。

# 目标

通过分析本次等级测评中可能发生的风险，并针对风险制定相应的风险规避措施，以降低或消除在等级测评风险发生的可能性，有效保证测评对象的安全性及可用性。

# 等级测评中可能产生的风险

在对 XXX 大学全流程数字化采购系统进行等级测评中除了摸清信息系统安全情况外，也会在工作过程中产生下如风险：

1、影响系统正常运行的风险

在现场测评时，需要对设备和系统进行一定的验证测试工作，部分测试内容需要上机验证并查看一些信息，这就可能对系统运行造成一定的影响，甚至存在误操作的可能。此外，使用测试工具进行漏洞扫描测试、性能测试及渗透测试等，可能会对网络和系统的负载造成一定的影响，渗透性攻击测试还可能影响到服务器和系统正常运行， 如出现重启、服务中断、渗透过程中植入的代码未完全清理等现象。

2、敏感信息泄露风险

测评人员有意或无意泄漏被测系统状态信息，如网络拓扑、IP 地址、业务流程、业务数据、安全机制、安全隐患和有关文档信息等。

3、木马植入风险

测评人员在渗透测试完成后，有意或无意将渗透测试过程中用到的测试工具未清理或清理不彻底，或者测试电脑中带有木马程序，带来在XXX 大学全流程数字化采购系统中植入木马的风险。

# 风险规避措施

针对上述风险，我们在等级测评项目中将采取如下措施加以规避：

1、签署委托测评协议

在测评工作正式开始之前，北京 XXXX 公司和被测评单位需要以委托协议的方式明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等，使得测评双方对测评过程中的基本问题达成共识。

2、签署保密协议

北京 XXXX 公司与被测评单位签署保密协议，以约束测评相关方现在及将来的行为。保密协议应规定测评相关方保密方面的权利与义 务。测评过程中获取的相关系统数据信息及测评工作的成果属被测评 单位所有，北京XXXX 公司对其的引用与公开应得到被测评单位的授权，否则被测评单位将按照保密协议的要求追究测评机构的法律责任。

3、现场测评工作风险的规避

现场测评之前，北京XXXX 公司应与被测评单位签署现场测评授

权书，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。测评机构进行验证测试和工具测试时，应避开业务高峰期，在系统资源处于空闲状态时进行；被测评单位也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；上机验证测试由测评人员提出需要验证的内容，被测评单位的管理人员进行实际操作。整个现场测评过程要求被测评单位全程监督。

4、测评现场还原

测评工作完成后，测评人员应将测评过程中获取的所有管理权限交回，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。

细化的风险规避措施工作内容如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **内容** | **可能存在的风险** | **风险等级** | **控制措施** |
| 信息资产调研 | 资产信息泄漏 | 高 | 保密协议、规章、制度、法律、法  规 |
| 安全管理测评 | 安全管理信息泄漏 | 高 | 合同、保密协议、规章、制度、法  律、法规 |
| 网络设备测评/ 安全设备测评 | 误操作引起设备崩溃或数据丢失、损坏 | 高 | 规范测评流程； 严格选择测评师；  签署《现场测评授权书》甲方进行全程监控；  制定可能的恢复计划 |
| 网络/安全设备资源占  用 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |

|  |  |  |  |
| --- | --- | --- | --- |
| **内容** | **可能存在的风险** | **风险等级** | **控制措施** |
| 漏洞扫描/渗透测试 | 网络流量 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |
| 主机资源占用 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |
| 设备死机 | 高 | 提前进行数据备份，制定恢复策略 |
| 控制台审计 | 误操作引起系统崩溃或数据丢失、损坏 | 高 | 规范审计流程； 严格选择测评师；  甲方进行全程监控；  制定可能的恢复计划； |
| 网络流量和主机资源  占用 | 低 | 避开业务高峰 |
| 应用测评 | 产生非法数据，致使系  统不能正常工作 | 中 | 做好系统备份和恢复措施 |
| 异常输入（畸形数据、极限测试）导致系统崩  溃 | 高 | 做好系统备份和恢复措施签署《现场测评授权书》 |
| 测评痕迹 | 木马、内容篡改等 | 高 | 对测评痕迹进行清理 |