**网络安全等级保护**

**广播电视播控及媒资管理系统**

**项目计划书**

|  |  |
| --- | --- |
| **系统名称：** | 广播电视播控及媒资管理系统（二级） |
| **委托单位：** | 正蓝旗融媒体中心 |
| **测评单位：** | 内蒙古信元网络安全技术股份有限公司 |
| **编制日期：** | 2023年3月 |

**目 录**

[1概述 4](#_Toc35854457)

[1.1 项目背景 4](#_Toc35854458)

[1.2 项目目的 4](#_Toc35854459)

[1.3 工作依据 4](#_Toc35854460)

[2 技术思路和工作内容 4](#_Toc35854461)

[2.1 技术思路 4](#_Toc35854462)

[2.2 工作内容 5](#_Toc35854463)

[2.2.1 测评准备活动 5](#_Toc35854464)

[2.2.2 方案编制活动 6](#_Toc35854465)

[2.2.3 现场测评活动 6](#_Toc35854466)

[2.2.4报告编制活动 6](#_Toc35854467)

[2.3 工作产品 6](#_Toc35854468)

[3 项目实施方案 8](#_Toc35854469)

[3.1 测评准备活动 8](#_Toc35854470)

[3.1.1 等级测评项目启动 8](#_Toc35854471)

[3.1.2 信息收集和分析 8](#_Toc35854472)

[3.1.3 工具和表单准备 9](#_Toc35854473)

[3.2 方案编制活动 9](#_Toc35854474)

[3.2.1 测评指导书开发 9](#_Toc35854475)

[3.2.2 测评方案编制 9](#_Toc35854476)

[3.3现场测评活动 9](#_Toc35854477)

[3.3.1 现场测评准备 10](#_Toc35854478)

[3.3.2 现场测评和结果记录 10](#_Toc35854479)

[3.3.3 结果确认和资料归还 11](#_Toc35854480)

[3.4 报告编制活动 11](#_Toc35854481)

[4 项目组织方案 12](#_Toc35854482)

[4.1 项目组织结构 12](#_Toc35854483)

[4.1.1 测评机构项目组织结构 12](#_Toc35854484)

[4.2.1 测评单位人员构成 12](#_Toc35854485)

[4.2.2 测评机构人员职责 12](#_Toc35854486)

[4.2.3 被测评单位人员构成 13](#_Toc35854487)

[4.2.4 被测评单位人员职责 13](#_Toc35854488)

[4.3 项目实施计划 14](#_Toc35854489)

[5 项目质量管理和控制 15](#_Toc35854490)

[5.1 过程质量控制管理 15](#_Toc35854491)

[5.1.1 测评准备活动质量控制管理 15](#_Toc35854492)

[5.1.2 方案编制活动质量控制管理 16](#_Toc35854493)

[5.1.3 现场测评活动质量控制管理 16](#_Toc35854494)

[5.2 变更控制管理 17](#_Toc35854495)

[5.3 项目风险管理 17](#_Toc35854496)

[5.3.1 进度风险的管理 17](#_Toc35854497)

[5.3.2 协作与沟通风险的管理 17](#_Toc35854498)

[5.3.3 测评工作引入风险的管理 17](#_Toc35854499)

[5.4 保密控制管理 18](#_Toc35854500)

[5.4.1 人员保密管理 18](#_Toc35854501)

[5.4.2 设备保密管理 19](#_Toc35854502)

[5.4.3 文档保密管理 19](#_Toc35854503)

1概述

1.1 项目背景

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，正蓝旗融媒体中心委托内蒙古信元网络安全技术股份有限公司（DJCP2010150053）对广播电视播控及媒资管理系统实施等级测评，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。

1.2 项目目的

本次网络安全等级保护测评工作的测评信息系统为正蓝旗融媒体中心广播电视播控及媒资管理系统1个定级备案的信息系统。通过网络安全等级保护测评，一是掌握信息系统安全状况、排查系统安全隐患和薄弱环节、明确信息系统安全建设整改需求；二是能够衡量出信息系统安全保护措施是否符合网络安全等级保护基本要求，是否具备了相应等级的安全保护能力；三是根据测评结果出具整改建议，指导系统运营、使用单位下一步的具体安全建设、整改工作，最终使系统达到国家网络安全等级保护的相关要求，避免相关安全风险事件的发生。

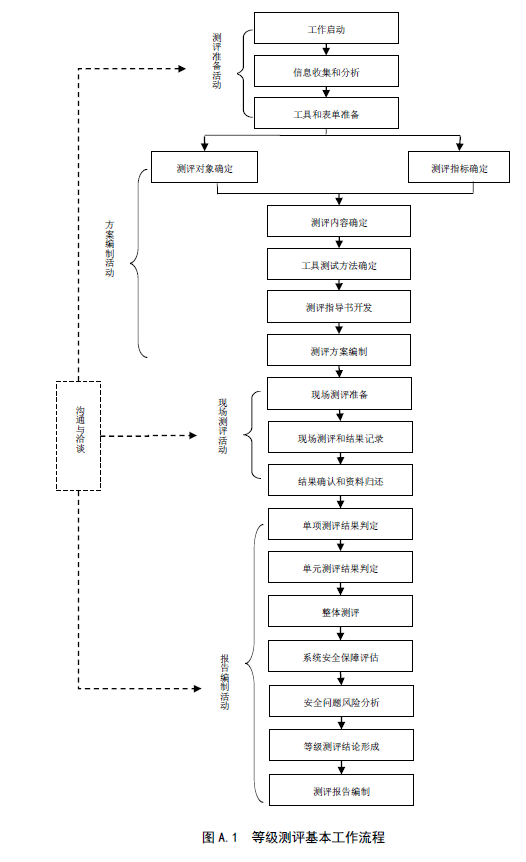
1.3 工作依据

1. 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》
2. GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》
3. GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》
4. GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》
5. GB/T 20984-2007 《信息安全技术 信息安全风险评估模型》

2 技术思路和工作内容

2.1 技术思路

本次项目实施采用如下测试流程：



2.2 工作内容

2.2.1 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

工作任务：测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。

2.2.2 方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料，为现场测评活动提供最基本的文档和指导方案。

工作任务：包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

2.2.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，依据测评方案实施现场测评工作，将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。

工作任务：现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

2.2.4报告编制活动

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（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

工作任务：报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

2.3 工作产品

通过对信息系统进行等级符合性检验，最终出具等级测评报告，可以帮助信息系统运营、使用单位发现信息系统的安全防护能力与国家等级保护要求之间的差距，发现信息系统存在的安全隐患和薄弱环节，指导系统运营、使用单位下一步的具体安全建设、整改工作，最终使系统达到国家等级保护的相关要求，避免相关安全风险事件的发生。

《网络安全等级保护测评报告》，将从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理等各个单元层面以及整体层面明确提出被测信息系统存在的安全隐患和薄弱环节，同时，采用风险分析的方法分析信息系统网络安全等级保护测评结果中存在的安全问题可能对信息系统安全造成的影响。

报告将针对信息系统存在的安全问题，给出相应的改进建议。为信息系统安全建设整改提供安全理论依据，为决策者制定安全策略、构架安全体系以及确定有效的安全措施、选择可靠的安全产品、建设全面的安全防护层次提供规范的指导。

3 项目实施方案

分阶段说明项目的实施过程及每个阶段的工作产品等内容。“项目实施过程划分”可首先说明项目实施分为几个过程，然后分过程说明每个过程的工作内容、工作产品等内容。这个过程可以参考《测评过程指南》标准的四个活动来划分，并增加项目验收过程，也可以根据自身经验划分不同的工作过程。

3.1 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

测评准备活动包括工作启动、信息收集和分析、工具和表单准备三项主要任务。这三项任务的基本工作流程见图1：

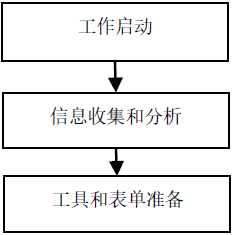


图1 测评准备活动的基本工作流程

3.1.1 等级测评项目启动

项目启动实施过程：在工作启动任务中，测评机构组建等级测评项目组，获取测评委托单位及定级对象的基本情况，从基本资料、人员、计划安排等方面为整个等级测评项目的实施做好充分准备。

项目启动工作产品：项目计划书。

3.1.2 信息收集和分析

信息收集和分析实施过程：测评机构通过查阅被测定级对象已有资料或使用系统调查表格的方式，了解整个系统的构成和保护情况以及责任部门相关情况，为编写测评方案、开展现场测评和安全评估工作奠定基础。

信息收集和分析工作产品：填好的调查表格。

3.1.3 工具和表单准备

工具和表单准备实施过程：测评项目组成员在进行现场测评之前，应熟悉被测定级对象、调试测评工具、准备各种表单等。

工具和表单准备工作产品：选用的测评工具清单，打印的各类表单。

3.2 方案编制活动

方案编制活动中，测评机构整理测评准备活动中获取的定级对象相关资料，为现场测评活动提供最基本的文档和指导方案。

方案编制活动包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制六项主要任务。

3.2.1 测评指导书开发

测评指导书开发实施过程：测评单位根据被测系统的测评对象，开发具体指导测评人员如何进行测评活动的指导书，是现场测评的工具、方法和操作步骤等的详细描述，是保证测评活动规范的根本。

测评指导书开发输出产品：测评指导书，测评结果记录表格。

3.2.2 测评方案编制

测评方案编制实施过程：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、测评内容、测评方法等等。

测评方案编制输出产品：经过评审和确认的测评方案文本，风险规避实施方案文本。

3.3现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，依据测评方案实施现场测评工作，将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。这三项任务的基本工作流程见图3：



3.3.1 现场测评准备

现场测评准备实施过程：测评委托单位对风险告知书签字确认，了解测评过程中存在的安全风险，做好相应的应急和备份工作。 测评委托单位签署现场测评授权书。召开测评现场首次会，测评机构介绍现场测评工作安排，相关方对测评计划和测评方案中的测评内容和方法等进行沟通。测评相关方确认现场测评需要的各种资源，包括测评配合人员和需要提供的测评环境等。现场测评工作正式开启。

现场测评准备输出产品：会议记录，测评方案，现场测评工作计划和风险告知书，现场测评授权书。

3.3.2 现场测评和结果记录

现场测评和结果记录实施过程：现场测评一般包括访谈、文档审查、配置检查、测试和实地察看五个方面。

访谈，测评人员与被测系统有关人员进行交流、讨论等活动，获取相关证据，了解有关信息。

输出产品：技术和管理安全测评的测评结果记录。

文档审查：被测评单位人员将调查表格中提供的所有文档准备充分，测评人员根据GB/T 22239中规定的制度、策略、操作规程等文档是否齐备；检查是否有完整的制度执行情况记录，如机房出入登记记录、电子记录、高等级系统的关键设备的使用登记记录等；检查安全策略以及技术相关文档是否明确说明相关技术要求实现方式；对上述文档进行审核与分析，检查他们的完整性和这些文件之间的内部一致性。

输出产品：技术和管理安全测评的测评结果记录。

实地查看：根据被测定级对象的实际情况，测评人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否符合相应等级的安全要求。

实地查看输出产品：技术安全和管理安全测评结果记录。

配置检查：根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统以及各设备的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等）；如果系统在输入无效命令时不能完成其功能，应测试其是否对无效命令进行错误处理；针对网络连接，应对连接规则进行验证。

输出产品：技术安全测评结果记录。

测试：根据测评指导书，利用技术工具对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透性测试、功能测试、性能测试、入侵检测和协议分析等；备份测试结果。

输出产品：技术安全测评结果记录，测试完成后的电子输出记录，备份的测试结果文件。

3.3.3 结果确认和资料归还

结果确认和资料归还实施过程：测评人员在现场测评完成之后，应首先汇总现场测评的测评记录，对漏掉和需要进一步验证的内容实施补充测评。双方召开测评现场结束会，测评双方对测评过程中得到的证据源记录进行现场沟通和确认。 测评机构归还测评过程中借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认。

结果确认和资料归还输出产品：经过测评委托单位确认的测评证据和证据源记录。

3.4 报告编制活动

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（或称测评证据）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，还需进行单元测评结果判定、整体测评、系统安全保障评估，经过整体测评后，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，而后针对安全问题进行风险评估，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成及测评报告编制七项主要任务。

报告编制活动实施过程：测评机构编制测评报告，并提交给测评委托单位进行验收评审，测评委托单位确认，项目结束。

4 项目组织方案

4.1 项目组织结构

4.1.1 测评机构项目组织结构

4.2 人员构成和职责

项目负责人

质量监督人

技术测试组

管理评估组

工具测试组

4.2.1 测评单位人员构成

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 姓名 | 负责范围 | 联系方式 |
| 1 |  | 项目负责人 |  |
| 2 | 富春蕾 | 质量监督人 | 15661061421 |
| 3 | 王景茹 | 管理测评、现场测评负责人 | 15147690982 |
| 4 |  | 主机测评、网络测评师 |  |
| 5 |  | 渗透测试、工具测试 |  |

4.2.2 测评机构人员职责

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

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

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

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

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

4.2.3 被测评单位人员构成

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 姓名 | 负责范围 | 联系方式 |
|  |  |  |  |

4.2.4 被测评单位人员职责

（1） 测评准备阶段

a) 向测评机构介绍本单位的信息化建设状况与发展情况。

b) 提供测评机构需要的相关资料。

c) 为测评人员的信息收集工作提供支持和协调。

d) 准确填写调查表格。

e) 根据被测定级对象的具体情况，如业务运行高峰期、网络布置情况等，为测评时间安排提供适宜的建议。

f) 制定应急预案。

（2）方案编制阶段

a) 为测评机构完成测评方案提供有关信息和资料。

b) 评审和确认测评方案文本。

c) 评审和确认测评机构提供的风险规避实施方案。

d) 若确定不在生产环境开展测评，则部署配置与生产环境各项安全配置相同的备份环境、生产验证环境或测试环境作为测试环境。

（3）现场测评阶段

a) 测评前备份系统和数据，并了解测评工作基本情况。

b) 协助测评机构获得现场测评授权。

c) 安排测评配合人员，配合测评工作的开展。

d) 对风险告知书进行签字确认。

e) 配合人员如实回答测评人员的问询，对某些需要验证的内容上机进行操作。

f) 配合人员协助测评人员实施工具测试并提供有效建议，降低安全测评对系统运行的影响。

g) 配合人员协助测评人员完成业务相关内容的问询、验证和测试。

h) 配合人员对测评证据和证据源进行确认。

i）配合人员确认测试后被测设备状态完好。

（4）报告编制阶段

a) 签收测评报告。

b)向分管公安机关备案测评报告。

4.3 项目实施计划

**测评项目进度表**

| **实施项目** | **测评周期(天)** | **备注** |
| --- | --- | --- |
| **一、测评准备过程** | 1 |  |
| 项目启动会 | 0.5 | 所有项目参与人员 |
| 现场调查 | 0.5 | 需要系统管理员配合访谈 |
| 工具和文档准备 | 0.5 | 测评机构所有项目人员 |
| **二、方案编制过程** | 1.5 |  |
| 测评方案编制 | 1 | 测评机构所有项目人员 |
| 测评方案审核 | 0.5 | 所有项目参与人员 |
| **三、现场实施过程** | 5 |  |
| 首次会议 | 0.5 | 所有项目参与人员 |
| 安全物理环境 | 0.5 | 需要机房管理员配合 |
| 安全通信网络 | 0.5 | 需要网络管理员配合 |
| 安全区域边界 | 0.5 | 需要网络管理员配合 |
| 安全计算环境 | 2 | 需要网络管理员、主机管理员、应用管理员、数据库管理员、系统管理员、安全管理员、审计管理员配合 |
| 安全管理中心 | 1 | 需要网络管理员、主机管理员、应用管理员、数据库管理员、系统管理员、安全管理员、审计管理员配合 |
| 安全管理制度 | 2 | 需要制度管理员配合，提供管理文档、执行记录。 |
| 安全管理机构 |
| 安全管理人员 |
| 安全建设管理 |
| 安全运维管理 |
| 工具测试 | 1 | 需要系统管理员配合测试  需要网络管理员、系统管理员配合测试 |
| 测试结果初步分析 | 1 | 测评机构所有项目人员 |
| 末次会议 | 0.5 | 所有项目参与人员 |
| **四、报告编制过程** | 13 |  |
| 测评报告编制 | 8 | 项目负责人 |
| 测评报告审核及签发 | 2 | 质量监督人 |
| **总计** | 35 | 测评实施阶段工作可根据现场情况并行操作 |

5 项目质量管理和控制

5.1 过程质量控制管理

质量控制管理包括各工作活动的质量管理和控制措施，主要有项目准备活动中保护客户的机密性；方案编制活动中测评方法确定及测评方案的评审；现场测评活动中测评工作的规范化、测评人员的能力确认、保障检查设备的有效运行及测评过程的记录准确、完备；报告编制活动中测评结果和报告的规范化、测评报告的评审等。

5.1.1 测评准备活动质量控制管理

（1）保护客户的机密性

我测评单位与呼伦贝尔市应急管理局在项目开始前，签署了完善的、合乎法律规范的保密协议，以约束双方现在及将来的行为。我测评单位严格按照保密协议中相关条款执行保密义务。

项目准备阶段，管理检查组及项目主管对参与项目的所有测评人员进行内部保密工作检查并进行记录，检查个人计算机加密软件安装是否正确、使用是否熟练、项目资料是否做了加密处理、内部文件的传递是否遵守保密管理制度要求进行了审批和登记。项目主管对所有测评人员进行保密教育和培训工作，明确了保密范围、保密责任、以及泄密处理措施，加强测评人员的保密意识。

（2）工具和资料准备

项目准备活动中，管理检查组将测评期间所有的监督检查记录准备完善，现场测评时按照项目监督管理制度规定，对测评人员的人员行为规范、保密处理措施、测评工作方法等进行每日抽查并记录，发现问题及时纠正。设备负责人对设备进行检查，保证测评期间设备的有效运行。

5.1.2 方案编制活动质量控制管理

（1）测评方法确定

项目所依据的均为正式发布的标准和规范。项目所使用的核查和测试方法，在仿真环境中进行模拟验证，适当准确度、现行有效、符合标准要求。测评人员在项目开展前进行了大量的培训，能够准确理解测评方法。

（2） 测评方案的评审

项目负责人组织了评审组人员对测评方案进行了内部评审，以确保测评要素的充分性和适当性，测评技术的适用性和有效性。

5.1.3 现场测评活动质量控制管理

（1）测评结果和报告的规范化

测评报告和数据准确、清楚、明确和客观地报告每一项或每一系列的测评结果，并符合测评方法中规定的要求。

（2）结果记录的确认

现场测评人会完成现场测评后，结果记录需要经过质量监督组、部门经理双重审核评审，存在问题的由现场测评人员去客户单位复测。

5.2 变更控制管理

项目实施过程中可能发生的变更有：人员配合协调不及时，导致项目进度延迟；上机进行配置核查和验证时，因为存在误操作，影响系统正常运行；测试工具的接入对系统性能产生影响，引起服务不响应以及系统宕机等现象。

出现上述变更时的控制管理措施：对于人员配合不及时，项目负责人与委托测评单位联系人沟通，临时调整测评对象，改为测评对能够有配合人员的测评对象进行测评；在对测评对象进行测评前测评人员验证测评对象已进行备份方进行测评，对于因上机配置核查和验证误操作导致系统运行的，应立即停止上级操作， 并对系统进行恢复，待系统正常运行后再进行测评，测评人员应对测评方法进行调整；工具测试对系统造成影响，引起服务不响应以及宕机，需要进行重新启动，待系统稳定后再进行测试。

5.3 项目风险管理

5.3.1 进度风险的管理

为了避免项目在实施过程中，项目进展情况落后于进度计划，难以保证项目按期完成，对项目活动实施进度控制。

在测评实施过程中，采取测评任务流程卡控制项目进度，要求每位参与项目的测评人员必须按照提前制定的进度开展测评工作。项目负责人定期收集项目完成情况的数据，并将完成情况数据与进度计划进行比较，一旦发现实际进程落后于计划进程，立即采取纠正措施。

5.3.2 协作与沟通风险的管理

为避免项目实施过程中，项目组内部人员以及测评双方人员由于交流和沟通存在问题，造成工作目标偏差、并最终影响项目的有效实施，在实施项目期间加强沟通管理。通过举行各种项目会议，主要形式包括项目例会、各阶段评审会议、问题讨论会议等，及时整理会议意见和建议，各测评人员定期提交项目报告，汇报项目进程，及时收集反映信息，采用多种沟通方式，积极保持与测评委托单位的关系。在测评开始和测评过程中，双方进行积极有效的沟通交流，及时解决测评中出现的问题，有效保证测评的过程质量和结果质量。

5.3.3 测评工作引入风险的管理

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级查看一些信息，这可能对系统的运行造成一定的影响。另外，还会使用一些技术测试工具进行漏洞扫描测试、性能测试。测试可能对网络和系统的负载造成一定的影响，如出现重启、服务中断等现象。

为避免上述风险，在等级测评过程中采取以下控制措施：

在现场测评工作正式开始之前，我公司和测评委托单位呼伦贝尔市应急管理局签署了现场测评授权书，明确的测评工作中双方的责任，并以书面形式揭示了可能的风险，要求呼伦贝尔市应急管理局采取相关预防措施。

进行验证测试和工具测试时，我公司会与委托测评单位充分的协调，安排好测试时间，避开业务高峰期，在信息系统处于闭式状态时进行，并需要测评委托单位对整个测试过程进行监督；在进行验证测试和工具测试前，要求委托测评单位对关键数据做好备份工作，并对可能出现的影响制定相应的处理方案；上机验证测试原则上由测评委托单位相应的技术人员进行操作，测评人员根据情况提出需要操作的内容，并进行查看和验证，避免由于测评人员对某些专用设备不熟悉造成误操作；我测评机构使用的测试工具在使用前会事先告知测评委托单位，并详细介绍这些工具的用途以及可能对信息系统造成的影响，征得委托测评单位的统一，必要时先进行一些验证。

测评工作完成后，测评人员交回测评过程中获取的所有特权，归还测评过程中借阅的相关资料文档。

5.4 保密控制管理

5.4.1 人员保密管理

人员保密责任范围包括项目组全体人员。项目组全体人员应严格遵守保密制度与规定，落实各项保密措施。测评过程中严格遵守委托测评单位管理规定，不询问与测评工作无关的事宜。现场需要查询的所有资料均在现场进行查看，查看完当天归还委托测评单位，并对文档交接过程进行记录。当天测评工作结束后，所有测评人员将测评资料交予档案管理员并进行登记，个人不得拥有任何测评资料。个人计算机在信息收集、方案编制、报告编制阶段的文档全部采用指定加密软件进行加密，防止信息无故泄露。测评期间，保密信息不得随意复制、严禁传输，因工作需要测评人员传递测评资料均需要经过项目负责人同意并进行内部文件传递登记。项目结束后，测评人员归还所有资料，由档案管理员统一归档。保密管理员在项目期间进行定期保密教育培训，加强测评人员保密意识，明确保密责任。

5.4.2 设备保密管理

设备保密管理范围包括项目信息处理、存储设备及测试工具。测评工作使用专用的设备和工具，并设定了专门人员进行管理，领用过程要按照领用手续来进行。项目组参与人员上岗工作前办理设备领用，工作结束后及时办理归还手续。每日项目结束后设备负责人负责将设备中的测试信息导入指定存储工具并将设备格式化。测评工作所有设备和工具进行标识，非项目人员不得在项目期间使用带有标识的设备和工具。

5.4.3 文档保密管理

文档保密范围包括与测评工作有关的带有密级（非商密）的各种文件、资料和信息，委托测评单位提供的文件、资料和信息，测评中获取的数据信息，测评过程中产生的工作产品和记录。文件资料设专柜统一编号，并设档案管理员专人保管，严格办理文件资料和信息的借阅手续，严格办理现场测评文件资料和信息的交接手续，文件资料和信息的复制、打印，需办理审批手续，不得复制、利用以及向任何单位和个人透漏测评委托单位的文件资料和信息，以及测评中获取的数据信息；配备采用物理隔离的文件服务器，存储项目过程中的电子文档。