**记录编号：$项目编号$-GJ01**

**等级保护测评项目计划书**

|  |  |
| --- | --- |
| **系统名称：** | **$项目名称$** |
| **被测单位：** | **$被测单位$** |
| **测评单位：** | **上海计算机软件技术开发中心** |
| **发布日期：** | **$测评准备首日$** |

**文档版本历史表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **作者** | **操作** | **日期** | **说明** |
| V1.0 | $项目成员1$ | 新建 | $测评准备首日1$ |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**文档审核记录表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **审核人** | **审核人签字** | **审核日期** | **说明** |
| V1.0 | $项目经理$ |  | $测评准备首日1$ |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

[1. 概述 1](#_Toc87815266)

[1.1 项目背景 1](#_Toc87815267)

[1.2 项目目的 1](#_Toc87815268)

[1.3 工作依据 1](#_Toc87815269)

[2. 技术思路和工作内容 2](#_Toc87815270)

[2.1 技术思路 2](#_Toc87815271)

[2.2 工作内容 2](#_Toc87815272)

[2.2.1 信息收集和分析 2](#_Toc87815273)

[2.2.2 确定测评范围 3](#_Toc87815274)

[2.2.3 确定测评对象 3](#_Toc87815275)

[2.2.4 确定测评工作方法 3](#_Toc87815276)

[2.2.5 形成测评指标 4](#_Toc87815277)

[2.2.6 开发测评指导书 6](#_Toc87815278)

[2.2.7 制定测评方案 6](#_Toc87815279)

[2.2.8 制定测评工作计划 7](#_Toc87815280)

[2.2.9 实施现场测评 7](#_Toc87815281)

[2.2.10 制定测评报告 7](#_Toc87815282)

[2.3 工作产品 7](#_Toc87815283)

[3. 项目实施方案 7](#_Toc87815284)

[3.1 测评准备活动 8](#_Toc87815285)

[3.2 方案编制活动 8](#_Toc87815286)

[3.3 现场测评活动 8](#_Toc87815287)

[3.4 分析与报告编制活动 8](#_Toc87815288)

[4. 项目组织方案 10](#_Toc87815289)

[4.1 项目组织结构 10](#_Toc87815290)

[4.2 人员组成和职责 10](#_Toc87815291)

[4.3 项目实施计划 11](#_Toc87815292)

[5. 项目质量管理和控制 12](#_Toc87815293)

[5.1 过程质量控制管理 12](#_Toc87815294)

[5.1.1 保护客户的机密性 12](#_Toc87815295)

[5.1.2 测评方法确定 12](#_Toc87815296)

[5.1.3 测评方案的评审 12](#_Toc87815297)

[5.1.4 测评工作的规范化 13](#_Toc87815298)

[5.1.5 测评人员的能力确认 13](#_Toc87815299)

[5.1.6 保障检查设备的有效运行 13](#_Toc87815300)

[5.1.7 测评过程的记录准确、完备 13](#_Toc87815301)

[5.1.8 测评结果和报告的规范化 13](#_Toc87815302)

[5.1.9 测评报告的评审 14](#_Toc87815303)

[5.2 变更控制管理 14](#_Toc87815304)

[5.2.1 项目委托方提出的工程变更。 14](#_Toc87815305)

[5.2.2 项目测评组提出的工程变更 14](#_Toc87815306)

[5.3 项目风险管理 14](#_Toc87815307)

[5.3.1 项目进度风险的管理 14](#_Toc87815308)

[5.3.2 项目协作与沟通风险的管理 15](#_Toc87815309)

[5.3.3 测评工作引入风险的管理 15](#_Toc87815310)

[5.4 保密控制管理 16](#_Toc87815311)

[5.4.1 人员保密管理 16](#_Toc87815312)

[5.4.2 设备保密管理 16](#_Toc87815313)

[5.4.3 文档保密管理 17](#_Toc87815314)

# 概述

## 项目背景

$系统简介$

## 项目目的

上海计算机软件技术开发中心受$被测单位$委托，对$项目名称$进行信息安全等级保护测评。本项目依据国家GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》标准，对$项目名称$进行信息安全等级保护测评，以验证其是否满足GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》（$等级$）$保护等级$的要求。

## 工作依据

以下标准为本次测评的主要依据标准：

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》

以下标准为本次测评的参考标准：

GB/T 17859—1999 ：《计算机信息系统 安全保护等级划分准则》

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》

# 技术思路和工作内容

## 技术思路



## 工作内容

### 信息收集和分析

信息收集和分析的主要工作包括收集被测系统已有资料、编制和发放调查表、协助填写调查表（采取电话或邮件方式）或现场调查、回收和分析调查结果等。通过该任务了解整个系统的构成和保护情况，为编写测评方案和开展现场测评工作奠定基础。

### 确定测评范围

在了解被测系统的定级情况、网络结构、具体系统构成，以及网络互连设备、安全设备和主机设备的基本信息的基础上，分析划定测评工作的范围。

### 确定测评对象

测评对象是等级测评的直接工作对象，也是在被测系统中实现特定测评指标所对应的安全功能的具体系统组成要素，因此测评对象的选择结果决定了现场测评数据的完整性和充分性，是顺利完成现场测评工作的前提和基础。

测评对象确定任务的主要工作包括：根据系统调查结果得到系统的安全保护等级、业务信息安全保护等级、系统服务安全保护等级；根据上述信息系统等级情况及调查结果中的网络结构、网络设备、安全设备、服务器、终端、数据库、应用系统等，根据测评对象选择方法确定测评对象。

### 确定测评工作方法

测评方法总体上分为三类：访谈、检查和测试。

访谈的目的是对信息系统整体情况进行了解，对各项规章制度颁布与落实情况的了解。如安全管理方面的基本情况就会涉及安全管理机构的设置情况、授权审批流程、整体安全策略、安全制度修订与维护、人员安全管理等内容；系统规划与建设中就会涉及信息系统安全方案总体设计、安全方案论证与评审、工程实施过程管理制度、测试与验收管理制度等内容；系统运维中会涉及事件处置与应急响应制度等内容。

检查是主要的测评手段，通过对测评对象进行观察、查验和分析得出符合性结论。可以进行文档检查(也就是证据类信息的检查)、实地察看(如机房选址、物理环境测评)、配置检查(主要是检查主机操作系统、应用系统、网络交换设备与网络安全设备的配置情况)。

测试主要是按照预定的方法／工具查看和分析响应的结果，是获取信息系统安全保护措施有效性的方法。如使用网络扫描工具验证服务器开放的应用端口，判断边界防火墙设备防护的有效性等。

### 形成测评指标

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》是等级测评依据的主要标准。在等级测评时，这些基本要求可以转化为针对不同被测系统的测评指标。测评指标由业务信息安全保护类、系统服务安全保护类和通用安全保护类组成。

测评指标确定工作主要包括：根据系统调查结果得到系统的安全保护等级、业务信息安全保护等级、系统服务安全保护等级；根据上述信息系统等级情况，从GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中选择与被测系统的保护等级相对应的基本要求作为测评指标；根据需要进一步调整某些测评指标，形成测评指标列表。下表为GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中安全通用要求的测评指标。

采用移动互联技术、云计算技术等的被测对象，或者是物联网、工业控制系统、大数据等特殊类型的被测对象，应选取被测对象安全保护等级所对应的安全扩展要求（云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求、大数据安全扩展要求，安全扩展要求的属性标识均标注为G），与安全通用要求共同组成本次测评指标。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全通用要求测评指标类（GB/T 22239-2019） | | | | | |
| 技术/管理 | 安全层面 | 类数量 | | | |
| S3 | A3 | G3 | 小计 |
| 技术要求 | 安全物理环境 | 1 | 1 | 8 | 10 |
| 安全通信网络 | 1 | 0 | 2 | 3 |
| 安全区域边界 | 1 | 0 | 5 | 6 |
| 安全计算环境 | 7 | 1 | 3 | 11 |
| 安全管理中心 | 0 | 0 | 4 | 4 |
| 管理要求 | 安全管理制度 | N/A | | 4 | 4 |
| 安全管理机构 | 5 | 5 |
| 安全管理人员 | 4 | 4 |
| 安全建设管理 | 10 | 10 |
| 安全运维管理 | 14 | 14 |
| 合计（S3A3G3） | | | | | 71（类） |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全扩展要求测评指标类（GB/T 22239-2019） | | | | |
| 层面 | 云计算 安全扩展要求 | 移动互联 安全扩展要求 | 物联网 安全扩展要求 | 工业控制系统 安全扩展要求 |
| 安全物理环境 | 1 | 1 | 1 | 1 |
| 安全通信网络 | 1 | 0 | 0 | 2 |
| 安全区域边界 | 3 | 3 | 2 | 3 |
| 安全计算环境 | 7 | 2 | 4 | 1 |
| 安全管理中心 | 1 | 0 | 0 | 0 |
| 安全管理制度 | 0 | 0 | 0 | 0 |
| 安全管理机构 | 0 | 0 | 0 | 0 |
| 安全管理人员 | 0 | 0 | 0 | 0 |
| 安全建设管理 | 2 | 2 | 0 | 2 |
| 安全运维管理 | 1 | 1 | 1 | 0 |
| 合计（第三级） | 16 | 9 | 8 | 9 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全通用要求测评指标类（GB/T 22239-2019） | | | | | |
| 技术/管理 | 安全层面 | 类数量 | | | |
| S2 | A2 | G2 | 小计 |
| 技术要求 | 安全物理环境 | 1 | 1 | 8 | 10 |
| 安全通信网络 | 1 | 0 | 2 | 3 |
| 安全区域边界 | 1 | 0 | 5 | 6 |
| 安全计算环境 | 6 | 1 | 3 | 10 |
| 安全管理中心 | 0 | 0 | 2 | 2 |
| 管理要求 | 安全管理制度 | N/A | | 4 | 4 |
| 安全管理机构 | 5 | 5 |
| 安全管理人员 | 4 | 4 |
| 安全建设管理 | 10 | 10 |
| 安全运维管理 | 14 | 14 |
| 合计（S2A2G2） | | | | | 68（类） |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全扩展要求测评指标类（GB/T 22239-2019） | | | | |
| 层面 | 云计算 安全扩展要求 | 移动互联 安全扩展要求 | 物联网 安全扩展要求 | 工业控制系统 安全扩展要求 |
| 安全物理环境 | 1 | 1 | 1 | 1 |
| 安全通信网络 | 1 | 0 | 0 | 2 |
| 安全区域边界 | 3 | 3 | 2 | 3 |
| 安全计算环境 | 5 | 1 | 0 | 1 |
| 安全管理中心 | 0 | 0 | 0 | 0 |
| 安全管理制度 | 0 | 0 | 0 | 0 |
| 安全管理机构 | 0 | 0 | 0 | 0 |
| 安全管理人员 | 0 | 0 | 0 | 0 |
| 安全建设管理 | 2 | 2 | 0 | 2 |
| 安全运维管理 | 1 | 0 | 1 | 0 |
| 合计（第二级） | 13 | 7 | 4 | 9 |

若存在GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》未覆盖（如行业标准等）或者高于被测对象相应安全保护等级的安全要求，应根据情况作为其他安全要求指标，与GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》的安全要求共同组成本次测评指标。其中，其他安全要求指标权重由其提出部门给出并参与最终计分计算。

### 开发测评指导书

根据测评指标选择情况开发测评作业指导书，指导测评人员开展测评活动。

### 制定测评方案

制定测评方案的主要工作包括：根据调查表及委托测评协议书获取方案所需的内容，综合已得到的测评对象、测评指标、测评内容、工具测试方法等内容形成《等级保护测评方案》文本，并对《等级保护测评方案》进行评审。

### 制定测评工作计划

根据被测系统的测评需求与规模，安排适当的人力资源形成测评团队，并制定出相应的测评工作计划表。

### 实施现场测评

实施现场测评时，测评机构首先应与测评委托单位就测评方案达成一致意见，并进一步确定测评配合人员，完成测评作业指导书各项测评内容，获取足够的测评证据。

测评工作的主要任务包括：现场测评准备、现场测评和结果记录、结果确认和资料归还。

### 制定测评报告

制定测评报告时，测评人员通过分析现场测评获得的测评证据和资料，判定单项测评结果及单元测评结果，然后进行整体测评和风险分析，形成等级测评结论，并编制《信息系统安全等级测评报告》。

报告编制活动的主要任务包括：单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制。

## 工作产品

《等级保护测评项目计划书》

《等级保护测评调查表》

《等级保护测评方案》

《等级保护测评现场记录表》

《等级保护测评现场接收/归还文档清单》

《网络安全等级保护等级测评报告》

# 项目实施方案

等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。而测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

## 测评准备活动

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，准备测试工具，为编制测评方案做好准备。

本阶段工作产品：《等级保护测评项目计划书》

## 方案编制活动

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确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评作业指导书，形成测评方案。

本阶段工作产品：《等级保护测评方案》

## 现场测评活动

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，严格执行测评作业指导书，分步实施所有测评项目，包括单元测评和整体测评两个方面，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。

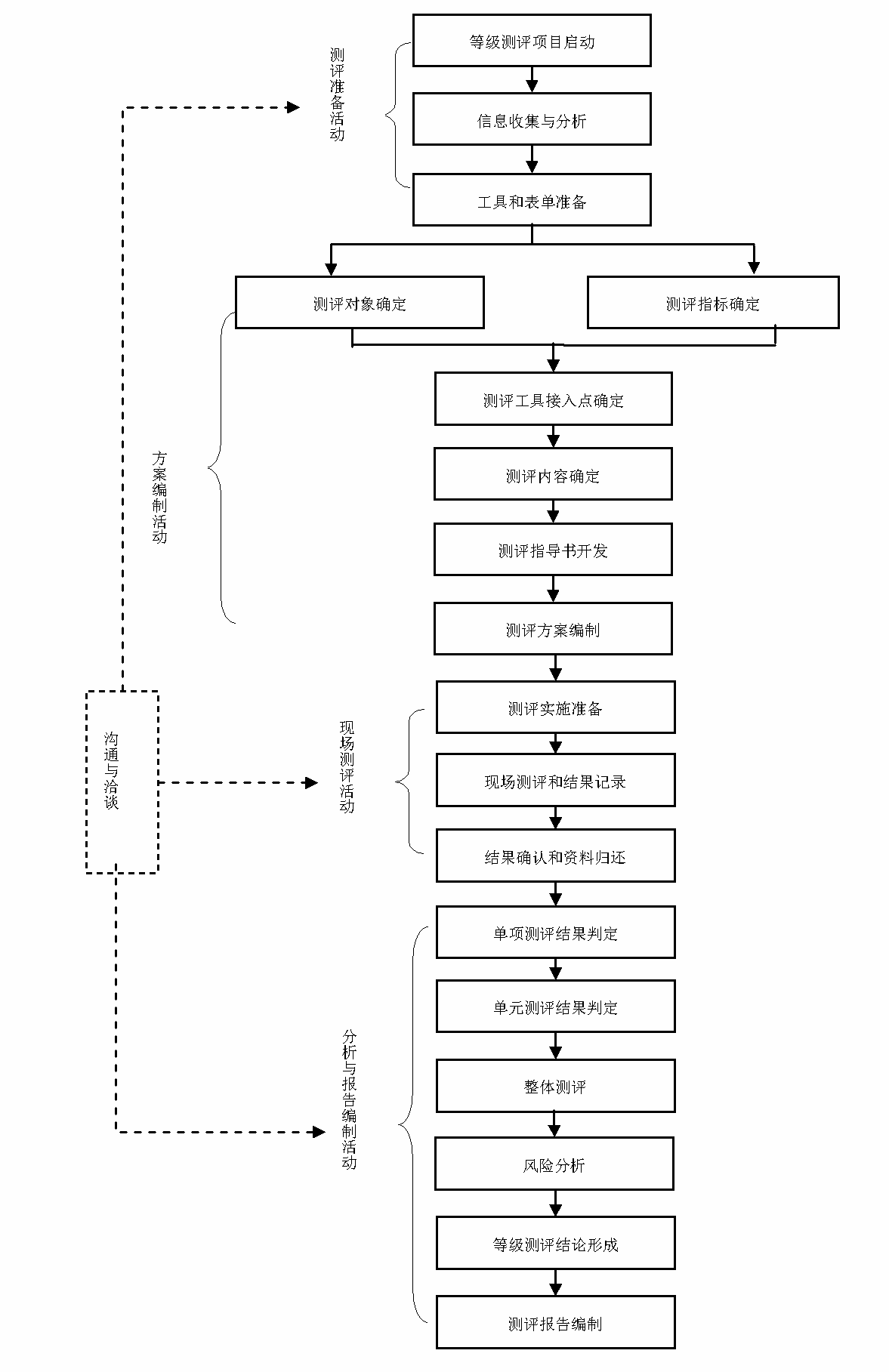
本阶段工作产品：《等级保护测评现场记录表》

《等级保护测评现场接收/归还文档清单》

## 分析与报告编制活动

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国家标准的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出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，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成测评报告文本。

本阶段工作产品：《网络安全等级保护 等级测评报告》



# 项目组织方案

## 项目组织结构

根据被测信息系统的规模，本次测评项目组由项目经理、管理核查组、技术测评组、验证测试组及监督检查组组成。

项目经理负责项目全面管理，工作内容包括制定计划并监督计划执行情况、控制项目进度、监督测评过程、评审阶段性成果及协调解决疑难问题等。

管理核查组负责分析和评审委托单位提交文档，实施现场安全管理监察，完成安全管理制度测评、安全管理机构测评、安全管理人员测评、安全建设管理测评和安全运维管理测评内容，配合技术测评组的工作。

技术测评组负责测评系统的安全物理环境测评、安全通信网络测评、安全区域边界测评、安全计算环境测评、安全管理中心测评，包括实施安全功能验证、安全配置检查测评，完成等级测评报告中的技术部分内容，配合管理测评组的工作。

验证测试组负责对测评系统进行验证测试，包含$是否渗透$。

监督检查组负责对项目实施的各种活动进行监督，及时发现实施过程中存在的问题，并在必要时采取纠正措施。

## 人员组成和职责

| **序号** | **姓名** | **角色** | **资质** | **备注** |
| --- | --- | --- | --- | --- |
|  | 蔡立志 | 项目负责人 | 信息安全（高级）等级测评师 |  |
|  | 吴建华 | 质量监督 | 信息安全（高级）等级测评师 |  |
|  | $项目经理$ | 项目经理 | 信息安全（中级）等级测评师 |  |
|  | $项目成员1$ | 测评工程师（技术） | 信息安全（初级）等级测评师 |  |
|  | $项目成员2$ | 测评工程师  （管理） | 信息安全（初级）等级测评师 |  |
|  | $项目成员2$ | 验证测试工程师 |  |  |

## 项目实施计划

工作具体安排如下：

| **持续时间 (工作日)** | **测试阶段** | **人员** | **目的** | **内容** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 5 | 测评准备 | $项目成员$ | 等级测评项目启动，信息收集与分析，工具和文档准备；  用户填写《信息系统基本情况调查表》。 | 现场会议、客户提交完成的自查表 |  |
| 5 | 方案编制 | $项目成员$ | 明确测试对象、测评指标、测评工具、测试内容，制定测评实施手册、测评计划 | 收集自查表中涉及的配置、管理文档、方案编制测评工具准备 |  |
| 10 | 测评实施 | $项目成员$ | 按照实施手册、测评计划执行测评 | 现场实施，具体时间安排见《测评方案》 | 测评结果的确认可能导致周期延长 |
| 10 | 分析与报告编制过程 | $项目成员$ | 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，测评综合结论形成，报告编制 | 编制项目报告 |  |

**说明：**

* 该项目实施计划中的起始时间为理想状态时间，当出现由于交付物提交延期等情况时，可能导致起始时间的变动，变动包含提前或延期；
* 测试实施内具体时间安排以及人员配合，详见《等级保护测评方案》。

# 项目质量管理和控制

## 过程质量控制管理

### 保护客户的机密性

* 测评双方签署完善的、合乎法律规范的保密协议，以约束双方现在及将来的行为；
* 接收评估任务时，向被评估方详细询问被测评设备和技术资料的保密要求，并做好记录；
* 质量管理组对测评过程中的设备。工具和技术资料进行监督检查，若发现有违反保密制度的现象予以及时纠正和制止，防止偏离进一步蔓延。

### 测评方法确定

* 使用具有适当准确度、现行有效和符合标准要求的方法进行核查和测试；
* 项目负责人组织编制本次项目的测评方案，包括确定测评方法、测评计划安排、工作规程能内容；
* 测评方法的确认包括详细说明该方法如何满足测评要求，该方法的特性。核查有效性声明、成本和风险的平衡关系等；
* 为确保测评方法满足本次测评项目要求，依据测评方法安排必要的验证。

### 测评方案的评审

* 项目负责人组织监督检查人员对测评方案进行评审，以确保测评要素的充分性和适宜性，测评技术的适用性和有效性；
* 评审过程明确评估双方的人员职责、测评对象、测评内容、测评方法、测评记录、执行过程和测评报告要求等内容，评审的记录形成文件；
* 评审后的测评方案得到测评委托单位的书面确认方可实施，此后未经批准不得随意调整、修改。

### 测评工作的规范化

* 项目所依据的均为正式颁布的标准和规范；
* 项目的测评过程严格依据各测评作业指导书来进行。

### 测评人员的能力确认

* 项目组人员均为测评机构在编人员，具备等级测评师的上岗证明；
* 项目组成员均参加了针对本项目的测试方式和测试用例等方面的培训；
* 质量负责人在项目期间负责项目组人员的岗位监督和能力绩效考核。

### 保障检查设备的有效运行

* 项目设备和工具的使用严格办理使用手续并做好记录，遵循设备保密管理要求；
* 质量管理组依据本次项目所使用的设备和工具清单，检查设备和工具在用状态记录、维护记录和故障记录，保证其使用的良好状态；
* 项目实施过程中，质量管理组随时跟踪设备和工具，使其处于受控状态，保证其运行可靠性和有效性。

### 测评过程的记录准确、完备

* 质量管理组确保测评活动和测评过程的可追溯，确保测评记录清晰明了、便于存取、妥善保存和安全保密；
* 项目负责人及时向单位负责人和质量管理组反馈测评过程中存在的问题，并采取纠正措施；
* 质量管理组成员负责对测评记录进行检查，主要包括结果、数据是否在产生的当时进行了记录、记录更改是否规范、作废记录是否写明原因等。

### 测评结果和报告的规范化

* 测评报告应准确、清晰、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；
* 测评报告由相关测评人员签署编制人、再经技术审核人审核签字后转至文档审核部门核准，核准后的报告由测评报告批准人批准签发。

### 测评报告的评审

* 项目负责人组织监督检查人员对测评报告进行评审，确认测评结果的有效性，保证所出具的报告和数据的真实、准确、可靠；
* 评审过程验证和监控记录方式、测评结论等，证实结果质量是否符合要求和能否发现测评系统或结果质量存在的潜在问题；
* 评审记录和结论由项目负责人提交相关部门归档。

## 变更控制管理

### 项目委托方提出的工程变更。

* 项目委托方将变更申请、变更方案提交给项目测评组；
* 项目测评组召集相关工程师根据项目合同、现场实际条件等因素对变更申请、变更方案进行研究，同意的出具书面意见一并交给项目委托方，不同意的出具书面意见后返回项目委托方。

### 项目测评组提出的工程变更

* 项目测评组提出项目变更后，连同变更说明书一并提交给项目委托方；
* 项目委托方如有意见需在规定的时间内反馈给项目测评组。

## 项目风险管理

### 项目进度风险的管理

为避免项目实施过程中，项目进展情况落后于进度计划，难以保证项目按期完成，测评机构对项目活动实施进度进行控制。

* 定期收集项目完成情况的数据，并将实际完成情况数据与计划进度进行比较，一旦发现实际进程晚于计划进程，项目负责人立即采取纠正措施；
* 分析项目变更的原因，评估项目变更对进度计划的影响；
* 在测评实施过程中采取测评任务流程卡方式控制项目进度。

### 项目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，造成人员关系冲突、工作目标偏差、并最终影响项目的有效实施，测评机构在项目期间加强沟通管理。

* 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，做好会议记录，及时整理会议意见；
* 定期提交项目报告（书面或口头报告），汇报项目进程，及时收集反馈信息；
* 采取多种沟通方式，积极保持与测评委托单位的良好关系。

### 测评工作引入风险的管理

为了避免测评工作引入新的安全风险，将可能造成的不良影响降低到测评委托单位可以接受的水平，测评机构在风险揭示、工具验证、连续性考虑和工作纪律等方面进行风险规避。

等保测评工作可能引入的风险包括：

* 可能影响系统正常运行

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验证并查看一些信息，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。

会使用一些技术测试工具进行漏洞扫描测试、性能测试甚至抗渗透能力测试。测试可能对网络和系统的负载造成一定的影响，渗透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的现象。

* 可能泄漏敏感信息

泄露被测信息系统状态信息，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。

为降低以上风险，需采取以下应对措施：

* 签署委托测评协议。

在测评工作正式开始之前，测评方和被测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、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，后续的工作以此作为基础，避免以后的工作出现大的分歧。

* 签署保密协议

测评双方应签署完善的、合乎法律规范的保密协议，以约束测评双方现在及将来的行为。保密协议规定了测评双方保密方面的权利和义务。测评工作的成果属被测评单位所有，测评方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单位的法律责任。

* 现场测评工作风险的规避

进行验证测试和工具测试之前，测评机构要求运营、使用单位对系统及数据进行备份，并对可能出现的事件制定处理方案。

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；上级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。整个现场测评过程要求系统运营、使用单位全程监督。

* 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权限交回，把测评过程中借阅的相关资料文档归还，并将在测评过程中植入被测信息系统中的相关代码/程序等进行严格清理。

* 提前将测评过程中可能遇到的风险揭示给测评委托单位；

## 保密控制管理

### 人员保密管理

人员保密责任范围包括项目组全体人员。

* 项目组全体人员遵守各项安全保密制度与规定；
* 全体人员在项目实施过程中，加强保密意识，明确保密责任，严格落实各项安全保密措施。

### 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。

* 配备专用设备和工具，并设定专门的领用手续；
* 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；
* 测评工作所用的设备和工具必须进行标识，非项目人员不得在项目期间使用带有标识的设备和工具；
* 测评工作所用设备和工具必须设置强密码，保密管理岗位负责人每周做定期验证；
* 测评工作所用工作电脑不得接入网络，保密信息不得随意复制，严禁传输；
* 临时存储设备（u盘）由负责人专门保管，项目期间不得外借，每次数据复制后，必须做好格式化工作。

### 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（非商秘）的各种文件、资料和信息；包括测评机构提供的文件、资料和信息，测评中获取的数据信息；还包括测评过程中产生的工作产品和记录。

* 文件资料设置专柜统一编号，并设专人保管；
* 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印、打印，需要办理审批手续；
* 不得复制、利用、向任何单位和个人透露测评委托单位的文件资料和信息，以及测评过程中获取的数据信息；
* 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。

【本页以下无内容】