**2024年重庆高速公路数字化应用私有云平台等保测评**

**技术规范书**

2024年10月

目录

[1. 项目概述 2](#_Toc179621877)

[1.1. 项目背景 2](#_Toc179621878)

[1.2. 项目目标 2](#_Toc179621879)

[1.3. 项目依据 2](#_Toc179621880)

[2. 等保测评服务方案 3](#_Toc179621881)

[2.1. 定级备案 3](#_Toc179621882)

[2.2. 测评范围 3](#_Toc179621883)

[2.3. 测评原则 3](#_Toc179621884)

[2.4. 测评方法 4](#_Toc179621885)

[2.5. 测评对象 5](#_Toc179621886)

[2.6. 测评流程 6](#_Toc179621887)

[2.7. 测评内容 10](#_Toc179621888)

[2.8. 测评结果判定 11](#_Toc179621889)

[2.9. 测评工具 12](#_Toc179621890)

[3. 项目质量控制管理 12](#_Toc179621891)

[3.1. 项目实施要求 12](#_Toc179621892)

[3.2. 过程质量控制管理 12](#_Toc179621893)

[3.3. 变更控制管理 15](#_Toc179621894)

[4. 服务成果 15](#_Toc179621895)

# 项目概述

## 项目背景

为贯彻落实习近平总书记加强网络安全建设工作的重要指示精神，切实提升重要信息系统安全防护能力，严防发生重大网络安全事件，按照网络安全等级保护制度2.0标准开展等级保护测评。

网络安全等级保护测评（简称等级测评）是在《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）等法规要求的信息系统等级保护——定级、备案、建设整改、等级测评、监督检查五个规定动作中的重要一环，依据国家法律、法规和技术标准对被测系统进行技术和管理两个方面进行全面测试、检查和评估，真实反映系统的安全保护能力，寻找问题和差距，为信息系统建设整改提供建议和依据。

## 项目目标

根据我单位信息安全相关工作要求，开展等级保护测评工作，并达成以下工作目标：

（1）聘请专业测评公司，通过测评、渗透、漏洞扫描等方式发现待测评系统存在的安全风险，并针对发现的安全问题，通过专业的技术手段进行合理分析，正确评估风险，完成整改工作。

（2）通过测评后，测评公司对测评系统出具网络安全等级测评报告，并提交至公安机关网安部门审核报备。

## 项目依据

下列文件中的条款通过本规范的引用而成为本规范的条款，除本技术规范书特别规定外，投标方所提供的测评标准均应遵循公安部相关文件要求和我单位的相关文件要求，所用的标准必须是其最新版本；如果这些标准内容矛盾时，应按最高标准的条款执行或按双方商定的标准执行；如果投标方选用本技术规范书规定以外的标准时，需提交与这种替换标准相当的或优于规定标准的证明，供我单位确认。

《信息安全等级保护管理办法》（公通字[2007]43号）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息安全风险评估规范》（GB/T 20984-2007）

# 等保测评服务方案

## 定级备案

按照《信息安全等级保护管理办法》、《信息安全技术 网络安全等级保护基本要求》等法规和标准的要求，按照“准确定级、严格审批、及时备案、认真整改、科学测评”的总体原则，对业务应用系统进行定级备案。

输出：

* 《信息系统安全等级保护定级报告》
* 《信息系统安全等级保护定备案表》
* 《信息系统安全等级保护定备案证明》

## 测评范围

本项目按照网络安全等级保护的要求进行测评。通过测评，准确反映以上信息系统的安全防护能力现状，对发现的问题进行深入分析，提供安全咨询服务，提出安全整改建议，出具网络安全等级保护测评报告。

测评指标和对象：测评指标和对象选择须符合国标《GB/T 28448-2019网络安全等级保护测评要求》的相关要求。

测评范围主要包括：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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

## 测评原则

测评项目的方案设计与实施应满足以下原则：

符合性原则：应符合国家信息安全等级保护制度及相关法律法规，指出防范的方针和保护的原则。

标准性原则：方案设计、实施与信息安全体系的构建应依据国内、国际的相关标准进行。

规范性原则：项目实施由专业的等级测评师依照规范的操作流程进行，在实施之前将详细量化出每项测评内容，对操作过程和结果提供规范的记录，以便于项目的跟踪和控制。

可控性原则：项目实施的方法和过程要在双方认可的范围之内，实施进度要按照进度表进度的安排，保证项目实施的可控性。

整体性原则：安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

最小影响原则：项目实施工作应尽可能小的影响网络和信息系统的正常运行，不能对信息系统的运行和业务的正常提供产生显著影响。

保密原则：为保障我公司利益，测评公司对我方提供的所有资料以及在测评过程中所接触到的商业秘密、技术资料、客户信息等资料和信息负有保密义务，未经授权不得泄露给任何单位和个人。

## 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。

① 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制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面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。

② 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、安全通信网络、安全区域边界、安全计算环境、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、安全区域边界、安全计算环境、安全管理中心等测评任务中，测评人员综合采用文档查阅与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），用于判断目标系统在主机、网络和应用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。

③ 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。

在网络安全、主机安全和应用安全等测评任务中，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。

## 测评对象

依照网络安全等级保护的要求、参考业界权威的安全风险评估标准与模型，从信息系统的核心资产出发，以威胁和弱点为导向，对比网络安全等级保护的具体要求，全方面对信息系统进行全面评估。

测评对象种类主要考虑以下几个方面：

1．整体网络拓扑结构；

2．机房环境、配套设施；

3．网络设备：包括路由器、核心交换机、汇聚层交换机等；

4．安全设备：包括防火墙、IDS/IPS、防病毒网关等；

5．主机系统（包括操作系统和数据库系统）；

6．业务应用系统；

7．重要管理终端（针对三级以上系统）；

8．安全管理员、网络管理员、系统管理员、业务管理员；

9．涉及到系统安全的所有管理制度和记录。

根据信息系统的测评强度要求，在执行具体的核查方法时，在广度上要做到从测评范围中抽取充分的测评对象种类和数量；在执行具体的检测方法，在深度上要做到对功能等各方面的测试。

## 测评流程

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
* 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，测评工作流程如下图所示：



**测评工作流程图**

1. 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。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 工作启动 | 项目计划书 | 项目概述、工作依据、技术思路、工作内容和项目组织等 |
| 信息收集和分析 | 填好的调查表格 | 被测系统的安全保护等级、业务情况、数据情况、软硬件情况、管理模式和相关部门及角色等。 |
| 工具和表单准备 | 选用的测评工具清单 打印的各类表单：现场测评授权书、文档交接单、会议记录表单、会议签到表单。 | 现场测评授权、交接的文档名称、会议记录项目、会议签到项目。 |

1. 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指导书测评指导书，形成测评方案。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 测评对象确定 | 测评方案的测评对象部分 | 被测系统的整体结构、边界、网络区域、重要节点、测评对象等 |
| 测评指标确定 | 测评方案的测评指标部分 | 被测系统定级结果、测评指标 |
| 测评内容确定 | 测评方案的单元测评实施部分 | 单元测评实施内容 |
| 工具测试方法确定 | 测评方案的测试工具接入点部分 | 测试工具接入点及测试方法 |
| 测评指导书开发 | 测评指导书 | 各测评对象的测评内容及方法 |
| 测评方案编制 | 测评方案文本 | 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 |

③ 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，严格执行测评指导书测评指导书，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。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 现场测评准备 | 会议记录、确认的测评授权书、更新后的测评计划和测评程序 | 工作计划和内容安排，双方人员的协调，测评委托单位应提供的配合 |
| 访谈 | 技术安全和管理安全测评的测评结果记录或录音 | 访谈记录 |
| 文档审查 | 管理安全测评的测评结果记录 | 管理制度和管理执行过程文档的记录 |
| 配置检查 | 技术安全测评的网络、主机、应用测评结果记录 | 检查内容的记录 |
| 工具测试 | 技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 | 漏洞扫描、渗透性测试、性能测试、入侵检测和协议分析等内容的技术测试结果 |
| 实地察看 | 技术安全测评的安全物理环境和管理安全测评结果记录 | 检查内容的记录 |
| 测评结果确认和资料归还 | 现场核查中发现的问题汇总、证据和证据源记录、测评委托单位的书面认可文件 | 测评活动中发现的问题、问题的证据和证据源、每项检查活动中测评委托单位配合人员的书面认可 |

④ 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《信息安全技术 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、单元测评结果判定、整体测评、系统安全保障评估和风险分析等方法，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。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 单项测评结果判定 | 等级测评报告的单元测评的结果记录部分 | 分析被测系统的安全现状（各个层面的基本安全状况）与标准中相应等级的基本要求的符合情况，给出单项测评结果。 |
| 单项测评结果汇总分析 | 等级测评报告的单元测评的结果汇总部分 | 汇总统计单项测评结果，给出针对每个对象的单元测评结果。 |
| 整体测评 | 等级测评报告的整体测评部分 | 分析被测系统整体安全状况及对单项测评结果的修订情况。 |
| 系统安全保障评估 | 测评报告的系统安全保障评估部分 | 汇总被测定级得分情况，并总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况 |
| 风险分析 | 等级测评报告的风险分析和评价部分 | 分析被测系统存在的风险情况。 |
| 等级测评结论形成 | 等级测评报告的等级测评结论部分 | 对测评结果进行分析，形成等级测评结论。 |
| 测评报告编制 | 等级测评报告 | 单项测评记录和结果，单项测评结果汇总，整体测评过程及结果，风险分析过程及结果，等级测评结论，安全建设整改建议等。 |

## 测评内容

网络安全等级保护测评包括两个方面的内容：一是安全控制测评，主要测评网络安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

安全控制测评使用测评单元方式组织，分为安全技术测评和安全管理测评两大类。安全技术测评包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个层面上的安全控制测评；安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的安全控制测评。

* **通用技术测评：**

(1)安全物理环境测评（物理位置的选择、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）；

(2)安全通信网络测评（网络架构、通信传输、可信验证）；

(3)安全区域边界测评（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）；

(4)安全计算环境测评（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）；

(5)安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

* **通用管理测评：**

(1)安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

(2)安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

(3)安全管理人员测评（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）；

(4)安全建设管理测评（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、系统支付、等级测评、服务测评机构选择）；

(5)安全运维管理测评（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）。

## 测评结果判定

网络安全等级保护的测评结论分为优、良、中、差四个等级，其中测评结论“差”的判别依据是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。具体的判定依据见下表：

|  |  |
| --- | --- |
| **测评结论** | **判别依据** |
| 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）。 |
| 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。 |

## 测评工具

WEB应用测试工具AppScan

WEB应用测试工具AppScan（以下简称“AppScan”）是一个针对WEB应用系统的安全扫描工具，提供WEB漏洞检测、配置审查以及漏洞利用等功能。

国瑞信安等保测试工具箱

国瑞信安等保测试工具箱是一个集成系统基本情况管理、系统主要配置检查、系统检查结果分析的综合等级保护安全检查工具平台，能够管理，检查和分析7种常用的机房设备检查工具和3种常用的网络类扫描工具，并集成了信息等级保护安全检查专业知识和信息安全等级保护安全检查专业分析。可帮助用户通过工具检查的结果，结合专业的知识库系统，充分了解信息系统中存在的安全风险与信息系统对应的等级保护等级之间的差距。通过定期对信息系统进行安全自我检测与评估，提升信息系统的等级保护合规性和抗风险能力。

# 项目质量控制管理

## 项目实施要求

1.测评公司应结合待测评系统特点，在项目实施过程中，测评公司成立相应的项目组，指定一名专职的项目经理协调和调度项目实施工作，制定计划方案，描述测评人员的组成、资质证书及各自职责的划分。

2.如需在待测评系统等级保护测评实施过程中采用在线测评工具，各种工具软件由测评公司推荐，经我公司确认后由项目实施方提供并在工作中使用。

3.为保证项目的顺利实施，测评公司应加强实施过程中的风险控制，双方应充分讨论并明确测评及评估对系统可能带来的风险和隐患，确定测评及评估对象、测评及评估方法和工具，并制定应急恢复措施。

4.在项目服务周期内，测评公司应协助我公司重大信息安全检查工作或重大网络安全安保工作，向我公司提供远程或现场相关的技术支撑服务。

## 过程质量控制管理

1. 测评准备过程质量管理

（1）项目负责人、技术评审组在项目合同签订前应对实施项目的能力和资源进行讨论，确保满足要求后启动项目。

（2）项目实施组成员按照各自分工准备现场调研所需的各种调查表。

（3）项目实施组完成必要的准备工作之后，项目负责人与测评委托单位协调现场调研时间。

（4）项目实施组初次与测评委托单位接触时，应首先召开项目启动会议，向测评委托单位介绍等级测评的意义和作用，测评工作的基本流程和工作方法，并揭示测评可能带来的风险和规避方法等。

（5）项目实施组成员通过与测评委托单位人员交谈，了解其信息化建设状况与发展，获得被测系统的基本情况，并提供所需的基本资料清单。

（6）项目实施组成员根据分工，分别分析了解到的被测系统的相关情况，包括行业特征、主管机构、网络拓扑结构、硬件设备部署情况、范围及边界、业务范围、业务种类及特性、业务流程、业务安全保护等级、组织管理结构、管理策略、部门设置和部门在业务运行中的作用、岗位职责、物理环境、地理位置、背景信息、联络方式等。

（7）网络组负责熟悉被测系统相关的网络设备和安全设备，并准备和打印核查表单；

（8）主机组负责熟悉被测系统相关的操作系统和数据库系统，并准备和打印核查表单。

（9）应用组负责熟悉被测系统的各个应用系统及其业务流程等，并准备和打印核查表单。

（10）测试组负责调试、熟悉本次测评过程中将用到的测评工具，包括漏洞扫描工具、渗透性测试工具、性能测试工具和协议分析工具等。

（11）管理组负责熟悉被测系统运营/使用单位的组织机构、管理文档等资料，并准备和打印核查表单。

2. 方案编制过程质量管理

（1）根据现场调研过程了解到的被测系统基本情况，项目实施组成员共同分析确定被测系统的整体结构、系统边界、网络区域、重要节点、测评对象、测评工具接入点及测评内容等。

（2）项目负责人根据项目实施组讨论确定的各项内容，对被测系统进行描述，并编制测评方案。

（3）项目负责人组织项目评审组成员对测评方案文档的适用性、可行性及准确性实施内部评审，并在会议签到表上进行登记。

（4）项目负责人负责与测评委托单位进行测评方案各项内容的沟通与协调，并将修订版本提交项目评审组讨论，形成测评方案定稿。同时，应得到测评委托单位对该测评方案的书面确认。

（5）已经形成定稿的测评方案未经项目负责人的批准不得随意调整、修改。

（6）项目实施组成员根据分工，分别针对各个测评对象编制测评实施手册。

（7）质量管理组负责测评方案评审会议的会议过程记录，并将测评方案定稿、测评实施手册、会议签到表及评审记录归档。

3.现场测评过程质量管理

（1）项目实施组对被测系统实施现场测评之前，应首先召开测评现场首次会，向测评委托单位介绍测评工作，明确测评时间安排、具体的工作内容及对方配合人员，并要求其对被测系统进行备份。

（2）测评项目负责人与测评委托单位负责人签署授权委托书。

（3）项目实施组成员应在确认用户已做好关键数据备份之后，依据测评实施手册，分别对每个测评对象实施测评，并如实、详实记录测评获取的各项证据，并要求配合人员对整个测评过程进行监督。

（4）项目实施组成员对测评完毕的测评证据进行整理汇总，对漏掉和需要进一步验证的内容实施补充测评。

（5）项目负责人负责召开测评现场结束会，测评双方对测评过程中发现的问题进行现场确认。

（6）项目实施组归还测评过程中借阅的所有文档资料，并要求对方在借阅记录上签字确认。

4. 分析及报告编制过程质量管理

（1）项目实施组成员根据各自现场测评获取的证据，针对每个测评项，分析该测评项的适用性及符合情况。

（2）项目实施组成员汇总分析各测评项的符合情况，并进行整体测评分析。

（3）项目负责人根据项目实施组成员汇总分析及整体测评分析的结果，编制等级测评报告，说明系统存在的安全隐患和缺陷，并给出改进建议。

（4）项目负责人组织项目评审组成员对测评报告文档的合理性及准确性实施内部评审，并根据评审情况修订测评报告，形成测评报告定稿。

（5）参加测评报告评审的各人员应在会议签到表上进行登记。

（6）质量管理组负责测评报告评审会议的会议过程记录，将测评报告、测评结果记录表单、会议签到表及评审记录归档，并负责测评报告的打印、盖章及交付。

## 变更控制管理

1．变更提出人可以为：

（1）项目组实施人员

（2）项目组管理人员

（3）委托方

（4）信息安全主管部门人员

2. 变更的提出

变更提出人填写《变更申请单》，提交项目负责人或项目负责人指定的人员。

3. 变更的评估

由项目经理领导或指导具体人员负责对变更进行评估，评估参与者包括：项目负责人、项目技术总监、相关技术小组组长、相关技术人员、用户方技术人员、用户代表。评估的方面包括：

（1）技术影响

（2）范围影响

（3）费用影响

（4）时间影响

（5）风险影响

（6）资源影响

（7）其他相关影响

4．批准

由项目负责人做出变更批准或不批准的决定，书面签字并做相应记录。

5. 变更实施

项目负责人调整所有变更所涉及的项目计划，保持计划的完整性。项目负责人负责将相关决定和计划通知变更相关人员，对重大变更通知所有相关人员。可能引起项目基线变更的申请，应由项目总监签字同意方为有效。

# 服务成果

投标方完成项目实施工作后，应提供以下项目成果：

|  |  |
| --- | --- |
| **序号** | **文档名称** |
| 1 | 《网络安全等级保护初评报告》 |
| 2 | 《渗透测试报告》 |
| 3 | 《漏洞扫描报告》 |
| 4 | 《网络安全等级保护测评报告》 |