委 托 服 务 合 同

项 目 名 称 ： 2024年度管委会各部门信息化系统信息安全等级保护服务

委托方（甲方）： 北京经济技术开发区营商环境建设局

受托方（乙方）： 北京中科卓信软件测评技术中心

签 订 地 点 ： 北京经济技术开发区

委 托 服 务 合 同

项 目 名 称 ： 2024年度管委会各部门信息化系统信息安全等级保护服务

委托方（甲方）： 北京经济技术开发区营商环境建设局

受托方（乙方）： 北京中科卓信软件测评技术中心

签 订 地 点 ： 北京经济技术开发区

委托服务合同

甲方：北京经济技术开发区营商环境建设局

乙方：北京中科卓信软件测评技术心

根据《中华人民共和国民法典》及相关法律、法规规定，在遵循平等、自愿、公平和诚实信用的基础上，甲、乙双方经协商一致，就乙方为甲方提供本合同项下相关服务事宜达成如下协议：

第一条 项目名称、服务内容及要求

（一）项目名称：2024年度管委会各部门信息化系统信息安全等级保护服务

服务内容：按照《GB/T22239-2019信息安全技术信息系统安全等级保护基本要求》等相关标准要求对区政府信息系统开展网络安全等级保护测评。从管理和技术两个方面确定与安全保护要求的差距，并对之进行整改，获得等级保护测评报告。根据信息系统实际情况，协助各业务系统所属部门开展责任主体、名称等相关备案工作。

2024年度管委会各部门信息化系统信息安全等级保护服务收集北京经济技术开发区各个业务部门信息化系统信息安全等级保护测评需求，拟针对45个业务系统（其中包含17个已备案三级等保、23个已备案二级等保复测系统和不少于5个新建系统；保证等保测评系统数量不变的情况下，可根据甲方需求进行调整）进行安全现状分析与调研、等级保护差距分析、形成差距分析报告及整改建议书、安全整改监督及安全整改建议、等级保护测评、形成测评报告等信息安全等级保护测评工作、汇总等。

（二）服务标准要求：

1.协助定级备案

针对未定级的信息系统进行定级备案。编写信息系统定级备案表和信息系统定级报告，并协助向公安机关提交定级备案材料，取得信息系统定级备案证明。服务成果：本阶段交付成果包括但不限于《信息系统安全等级保护定级报告》、《信息系统安全等级保护备案表》。

2.协助自查

根据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》等相关标准及信息系统的安全保护等级，通过人员访谈、文档审查、实地察看、配置检查、工具检测等方法从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、

安全管理人员、安全建设管理、安全系统运维等方面对目标信息系统进行安全需求测评分析，查找信息系统现有的安全保护水平与国家信息安全等级保护管理规范和技术标准之间的差距。服务成果：本阶段交付成果包括但不限于《信息系统等级保护差距分析报告》。

3.整改建议

经过信息系统安全等级保护自查，全面地分析和了解目前信息安全建设方面现状基础上，协助信息安全管理人员，特别是领导层更为全面的理解目前业务所面临的风险尤其是高风险，为规划和实施风险应对措施打下基础。以国家相关信息安全标准为依据，结合自身在信息安全服务方面的丰富行业经验，根据信息安全的现状和需求，为信息安全建设提供改进建议，协助信息安全管理人员进行信息系统安全加固整改建设工作，选择合适的风险处理措施予以实施，将风险控制在可接受的水平上，以提升整体信息安全管理和技术水平。最终达到国家规定的信息系统安全等级保护对应安全等级的管理和技术要求。服务成果：本阶段交付成果包括但不限于《信息系统等级保护整改建议》。

4.等级保护测评

根据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》等标准组织开展单位信息系统等级保护测评，衡量单位信息系统的安全保护管理措施和技术措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。依据各个信息系统的安全保护等级，通过人员访谈、文档审查、配置检查、工具检测等方法从安全技术、安全管理等方面，判断信息系统现有的安全保护水平与国家信息安全等级保护管理规范和技术标准要求项之间的符合情况。对信息系统进行整体、全面、公正的评估，对不符合项进行风险分析和风险应对，进行现场等级保护测评，并出具公安部门认可的信息系统安全等级测评报告。

服务成果：本阶段交付成果包括但不限于《信息系统安全等级测评报告》。

服务具体内容和要求详见甲方审核确认后的项目实施方案。

第二条 履行期限、进度与地点

（一）合同履行期限：自合同生效之日开始至服务内容全部完成并通过验收之日止。

（二）具体进度要求如下：

1.本合同生效后【10】日内，乙方应按照甲方要求和合同约定，制定并向甲方提交《项目实施方案》，同时作为本合同附件（附件一）附后。乙方按照甲方审核确认后的项目实施方案组织项目实施。前述经甲方确认后的项目实施方案将作为甲方验收的依据之一。

2.【2024】年【12】月【25】日前完成不少于15个三级系统的复测工作。

3. 乙方完成所有系统的测评工作并出具《信息系统安全等级测评报告》后，提出验收申请，甲方按照合同要求进行验收。

（三）履行地点：北京经济技术开发区。

第三条 合同成果、交付及其验收

（一）合同成果包括：

1. 协助定级备案：本阶段交付成果包括但不限于《信息系统安全等级保护定级报告》、《信息系统安全等级保护备案表》。

2. 协助自查：本阶段交付成果包括但不限于《信息系统等级保护差距分析报告》。

3. 整改建议：本阶段交付成果包括但不限于《信息系统等级保护整改建议》。

4. 等级保护测评：本阶段交付成果包括但不限于《信息系统安全等级测评报告》。

（二）合同成果交付

1. 期限：本项目自合同生效之日起至服务内容全部完成并通过验收之日止。

2. 地点：北京经济技术开发区

3. 方式：现场交付

（三）合同成果验收

1. 验收将依据合同及其附件、国家相关规范、标准，如无国家、行业标准，则应以合理满足本合同及附件的约定，且以甲方事后认可为达到本合同质量要求的依据，由甲方或甲方委托的第三方按甲方确定的时间和方式进行验收。

2. 具体验收标准和流程：乙方应在甲方规定的时限出具服务成果，并及时通知甲方进行验收。

3. 乙方应提交的验收资料：《信息系统安全等级测评报告》。

4. 验收合格的，由甲方或甲方委托的第三方出具项目验收证明。验收不合格的，乙方应依约承担违约责任。

第四条 合同价款与支付

（一）本项目合同价款：人民币【大写：壹佰玖拾叁万】元整（【￥1930000】元）。

前述合同价款业已包含劳务费、人工管理费、税款、加班费等乙方为履行本合同项下义务所应当获得的所有报酬和费用，以及甲方为此项目所有应当支出的费用。除本合同中上述明示的价款外，乙方无权再向甲方额外申请支付其他任何报酬或税费。

（二）支付方式：

双方同意甲方按下列第【 1 】项约定的方式支付合同价款：

1. 分期付款

(1) 合同签订生效，乙方依约提交项目实施方案，且甲方收到乙方提供符合要求的合法有效发票后【 10 】个工作日内，甲方向乙方支付【 70 】%合同价款，即人民币【大写：壹佰叁拾伍万壹仟】元整（【￥1351000 】元）；

(2) 全部服务履约验收合格，且甲方收到乙方提供符合要求的合法有效发票后【 10 】个工作日内支付【 30 】%合同价款，即人民币【大写：伍拾柒万玖仟】元整（【 ￥579000 】元）。

2. 一次性付款

甲方于项目履约验收合格，且收到乙方提供符合要求的合法有效发票后【/】个工作日内一次性向乙方全额支付合同价款。

(三) 乙方应向甲方提供符合甲方要求的合法发票及乙方的账户信息，并保证该账户合法、有效、可用，否则甲方有权拒绝支付合同价款，且不承担任何责任。如乙方向甲方提供的发票不符合本合同约定或法律规定，因此给甲方造成的一切损失由乙方承担。

乙方账户信息：

户　名：北京中科卓信软件测评技术中心

开户行：中国银行北京经济技术开发区分行

账　号：318175318989

(四) 价款明细详见附件二。

第二条 双方的权利义务

(一) 甲方权利义务

1. 甲方有权对《项目实施方案》提出修改意见和进行确认，确定项目主要工作内容和目标，审批项目计划与进度，制定项目验收标准并组织项目的验收。

2. 甲方有权要求乙方严格履行合同义务，配合查询项目资金使用情况；有权向乙方提出具体工作要求，乙方不得以任何理由拒绝或拖延执行。

3. 甲方有权监督、随时审查乙方的服务内容和质量，要求乙方提交符合要求的工作成果，有权对不符合合同规定的内容提出整改意见或更换不合格工作人员，乙方应遵照执行，若不予改正或改正后仍未符合要求的，甲方有权提前解除本合同，乙方应退回甲方已支付的全部款项，并依约承担违约责任。

4. 甲方发现乙方提交的合同成果有违反国家法律法规，不符合政治性、科学性，有低俗内容或出现严重质量问题的，甲方有权提前解除合同，乙方应退回甲方已支付的全部款

项，并依约承担违约责任。

5. 甲方有权组织或委托第三方对乙方实施项目进行评估、项目验收；若乙方未通过评估或验收，乙方应在限期内补充完善或予以改正。否则，甲方有权提前解除合同，乙方应退回甲方已支付的全部款项，并依约承担违约责任。

6. 本合同项下成果的所有权、知识产权及其他相关权利均归甲方所有。乙方除为履行本合同项下义务外不得使用。

7. 按本合同约定向乙方支付合同款。

（二）乙方权利义务

1. 乙方应独立完成合同规定的服务内容，按时提交符合要求的工作成果，严格按照相关文件、项目实施方案开展工作，保证工作内容和质量符合国家法律法规、主管部门标准和甲方的要求。

2. 乙方按照合同约定和项目具体情况派出服务团队人员（详见附件三），不得随意更换服务团队人员，若确需更换需事先征得甲方书面同意，且接替人员的职位、资历应当与被调换的人员相当。乙方指定【 程超 】为项目负责人，联系电话： 15901412185 。

3. 在甲方指导下进行项目实施工作，接受甲方或甲方委托第三方开展的项目监管、检查调研、中期评估、项目验收等，配合甲方完成相关工作计划调整。

4. 乙方保证其在提供服务和形成资料的过程中所使用的文件、资料、软件、背景音乐及其他物品均可合法用于本项目的执行。乙方保证其服务与资料、交付的成果合法、合规且不侵犯任何第三方的知识产权或其他合法权益，不存在任何与此相关的争议，否则一切后果由乙方承担。

5. 乙方须保证其履行本合同项下义务的合法性，并保证甲方不会因此而遭到任何第三方的索赔或陷入任何法律纠纷，否则，相关责任和后果均由乙方自行承担，且乙方亦应承担甲方因此而遭受的任何损失、支出及索赔（包括但不限于诉讼费、仲裁费、律师费、调查费、第三方主张的赔偿金以及其他因此支付的合理开支）。

6. 乙方对其因履行本合同所知悉的与本项目相关的信息以及甲方其他未公开的信息，应当采取适当有效的方式予以保密。

7. 本合同规定的任务不得以任何形式分包或转包。

第三条 违约责任

（一）任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应赔偿因违约给对方造成的一切损失。

（二）乙方未按本合同约定按期提供本合同下任一项成果的，每逾期一日，乙方须向甲方支付本合同价款总额0.1%的违约金。每项违约行为可以单独计算违约金；逾期达10日的，甲方有权解除合同，乙方应向甲方支付合同总价款30%的违约金并赔偿甲方遭受的全部损失。

（三）乙方提供本项目各成果不符合甲方要求的，乙方负责更正和修改，因此造成的所有损失和费用的增加由乙方承担，因此造成逾期交付的，按照前款内容承担逾期违约责任。

（四）因乙方侵犯第三方合法权益造成甲方涉诉或被投诉、举报的，由乙方承担全部责任，并向甲方支付相当于合同总价款30%的违约金，赔偿甲方遭受的全部损失。同时，甲方还有权解除本合同，乙方应退还甲方已支付的全部款项。

（五）若乙方擅自解除、中止或终止本合同的，应退回已收到的合同款，向甲方支付合同总价款30%的违约金，并赔偿甲方遭受的全部损失。

（六）因乙方违反本合同约定而须向甲方支付的任何款项（包括但不限于损失赔偿费用、违约金等），甲方均有权在应向乙方支付的合同款项中予以扣除。

（七）未经甲方书面同意，乙方将承担的工作内容转包、分包、转让或转委托，或者造成保密信息的被盗、泄露或其他有损信息保密的，甲方有权解除合同，乙方应退回已收到的合同款，向甲方支付合同价款30%的违约金，赔偿甲方因此遭受的全部损失。

（八）本条全部损失包括但不限于诉讼费、仲裁费、律师费、调查费、第三方主张的赔偿金以及其他因此支付的合理开支。

第四条 争议的解决

双方因本合同而发生的争议，应首先由甲乙双方协商解决。如协商不能解决的，则任何一方可以向甲方所在地有管辖权的人民法院提起诉讼。讼进行过程中，双方将继续履行本合同未涉仲裁或诉讼的其它部分。

第五条 其它

（一）本合同未尽事宜，双方应友好协商解决并签订《补充协议》。《补充协议》经双方盖章确认后，与本合同具有同等的法律效力。

（二）本合同一式【 陆 】份，具有同等法律效力。甲、乙双方各执【 叁 】份。

（三）本合同经双方签字并加盖公章或合同专用章后生效。

（四）本合同的所有附件均是本合同不可分割的组成部分，与本合同具有同等法律效力。

若附件与合同正文有任何不一致，以合同正文为准。

本合同附件为：一、项目实施方案

二、项目分项报价

三、项目主要人员组成

甲方(盖章)：北京经济技术开发区营商环境建设局

法定代表人/负责人或授权代表（签字）：

日　期：2020年11月11日

乙方(盖章)：北京中科卓信软件测评技术中心

法定代表人/负责人或授权代表（签字）：

日　期：2020年11月11日

附件一

项目实施方案

一、项目总体目标

项目的整体目标是北京经济技术开发区（以下简称经开区）的信息化系统进行全面评估，确保其满足等级保护的安全标准和要求。该测评旨在发现潜在的安全隐患，提供改进措施和建议，以确保网络系统在保密性、完整性和可用性方面达到国家规定的GB/T22240-2020《信息安全技术网络安全等级保护定级指南》及GB/T28448-2019《信息安全技术网络安全等级保护测评要求》等国家安全标准，防止信息泄露、数据损坏、未经授权访问等安全威胁。

通过信息系统等级保护测评，组织可以全面了解系统的安全状况，发现并解决潜在的安全问题，进一步提升网络系统的安全性和可信度。同时，满足GB/T22240-2020《信息安全技术网络安全等级保护定级指南》及GB/T28448-2019《信息安全技术网络安全等级保护测评要求》等国家标准对信息系统安全等级保护的要求，确保各委办局在信息化建设中符合规定的安全标准和要求，为信息系统的稳定运行和业务发展提供有力支持。

二、具体进度

2025年12月25日前完成营商环境建设局不少于45个信息化系统(其中包含17个已备案三级等保、23个已备案二级等保复测系统和不少于5个新建系统；保证等保测评系统数量不变的情况下，可根据甲方需求进行调整)测评服务工作。

三、项目内容和要求

我中心按照《GB/T22239-2019信息安全技术信息系统安全等级保护基本要求》等相关标准要求对区政府信息系统开展网络安全等级保护测评。从管理和技术两个方面确定与安全保护要求的差距，并对之进行整改，获得等级保护测评报告。根据信息系统实际情况，协助各业务系统所属部门开展责任主体、名称等相关备案工作。

2024年度管委会各部门信息化系统信息安全等级保护服务收集经开区业务部门信息化系统信息安全等级保护测评需求，拟针对45个业务系统进行安全现状分析与调研、等级保护差距分析、形成差距分析报告及整改建议书、安全整改监督及安全整改建议、等级保护测评、形成测评报告等信息安全等级保护测评工作。

四、任务目标

针对本项目，我中心将根据国家对信息安全等级保护工作的相关法律和技术标准要求，结合本项目的系统保护等级开展实施与之相应的检查工作。具体如下:

1、负责协助行政审批局对不少于45个信息化系统测评服务工作，最终成果为相关各委办局的等保测评报告；

2、完成对信息化系统梳理工作，包括备案变更系统撤销、系统新增备案、系统等保测评资料汇总等。

五、服务标准要求

（一）协助定级备案

针对未定级的信息系统进行定级备案。编写信息系统定级备案表和信息系统定级报告，并协助向公安机关提交定级备案材料，取得信

息系统定级备案证明。

（二）协助自查

根据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》等相关标准及信息系统的安全保护等级，通过人员访谈、文档审查、实地察看、配置检查、工具检测等方法从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全系统运维等方面对目标信息系统进行安全需求测评分析，查找信息系统现有的安全保护水平与国家信息安全等级保护管理规范和技术标准之间的差距。

（三）整改建议

经过信息系统安全等级保护自查，全面地分析和了解目前信息安全建设方面现状基础上，协助信息安全管理人员，特别是领导层更为全面的理解目前业务所面临的风险尤其是高风险，为规划和实施风险应对措施打下基础。根据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》等相关标准及信息系统的安全保护等级，通过人员访谈、文档审查、实地察看、配置检查、工具检测等方法从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全系统运维等方面对目标信息系统进行安全需求测评分析，查找信息系统现有的安全保护水平与国家信息安全等级保护管理规范和技术标准之间的差距。

（四）等级保护测评

根据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》等标准组织开展单位信息系统等级保护测评，衡量单位信息系统的安全保护管理措施和技术措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。依据各个信息系统的安全保护等级，通过人员访谈、文档审查、配置检查、工具检测等方法从安全技术、安全管理等方面，判断信息系统现有的安全保护水平与国家信息安全等级保护管理规范和技术标准要求项之间的符合情况。对信息系统进行整体、全面、公正的评估，对不符合项进行风险分析和风险应对，进行现场等级保护测评，并出具公安部门认可的信息系统安全等级测评报告。

六、测评工作流程

（一）测评准备

1.实施准备综述

我方根据等级保护基本要求，从安全技术层面和安全管理层面对备案系统进行等级测评，确保所有问题得到正确的解决，保证系统已经达到等级保护相应级别要求，并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，单项测评结果是形成等级测评结论的基础。我方提交正式的等级测评报告，上报公安机关，通过等级保护测评。

（1）成立项目实施团队

为了保障各项实施工作的顺利开展，首先由采购方和我中心共同组建项目实施团队，由领导小组、项目专家组、质量小组和实施小组

等组成。其中，由采购方的信息中心信息化部门主管信息安全工作的领导和安全管理员组成协调小组，主要负责和评测组工作对接，商议工作计划，安排评测组的现场活动，协调各部门或内部人员配合安全评测开展等工作；项目专家组和质量小组由我中心和采购方的信息安全领域专家共同担任，主要对方案和报告的审核；实施小组主要负责提前与被测评单位的协调、沟通及现场的具体测评工作。

（2）信息系统调研

实施小组提前与被测评单位沟通，并下发资产调研表和应用调研表，被测评单位反馈给实施小组后，查阅相关调研表，了解整个系统的构成和保护情况，明确目标系统的范围（特别是信息系统的边界），了解目标系统的详细构成，包括网络拓扑、业务应用、业务流程、设备信息（服务器、数据库、网络设备、安全设备、数据库等）、管理制度等。

2.系统整体测评

系统整体测评涉及信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关，内容复杂且充满系统个性。在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。

3.综合测评分析

综合测评分析包括两个方面的内容：一是安全控制测评分析，主要分析信息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；二是系统整体测评分析，主要测评分析信息系统的整体安

全性。其中，安全控制测评分析是信息系统整体安全测评分析的基础。

（二）协助定级备案方案

1.编写信息系统定级备案表和信息系统定级报告

我中心将针对未定级的信息系统进行定级备案。编写信息系统定级备案表和信息系统定级报告，并协助向公安机关提交定级备案材料，取得信息系统定级备案证明。

在信息系统定级应按照自主定级、专家评审、主管部门审批、公安机关审核的流程进行。信息系统运营使用单位按照《信息安全等级保护管理办法》、《GB/T 22240-2008信息安全技术 信息系统安全等级保护定级指南》、《GA/T 1389-2017 信息安全技术 网络安全等级保护定级指南》，自主确定信息系统的安全保护等级。为保证信息系统定级准确，需组织专家进行评审。有上级主管部门的，应当经上级主管部门审批，跨省或全国统一联网运行的信息系统可以由其主管部门统一确定安全保护等级。最后经公安机关审核把关，合理确定信息系统安全保护等级。

我中心派高级等级测评师协助客户协助梳理系统当前的硬件软件、物理环境、联络人员等系统信息。并对信息系统进行准确的定级，保证系统所定级别符合信息系统的业务安全要求，并协助编写信息系统的定级报告。保证客户顺利完成目标系统定级备案工作。

2.协助取得信息系统定级备案证明

根据等级保护相关的政策，当前定级工作基本上应采取专家评审方式进行，我方将协助甲方开展专家评审工作。

同时根据专家评审的意见，对定级备案材料进行进一步的优化完善。为后一步的报主管部门审核以及网安报备打下良好的基础。

按照等级保护的政策法规，通过专家评审后，需要开展报主管单位审核，最后报当地网安部门进行备案。

（三）协助自查方案

1.安全需求测评分析

根据采购文件的要求，我方将按照等级保护相关要求对目标系统进行差距分析。参照等级保护基本要求的内容，将开展两方面的工作：一是安全控制分析，主要检查信息安全等级保护要求的基本安全控制在目标系统中的实施配置情况；二是整体分析评估，主要检查和分析目标系统的整体安全性。其中，安全控制分析是信息系统整体安全分析评估的基础。

对安全控制分析的描述，使用检查单元方式组织。检查单元分为安全技术检查和安全管理检查两大类。安全技术检查包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个层面上的安全控制检查；安全管理检查包括：安全策略和管理制度、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五个方面的安全控制检查。

安全技术分析包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个层面。

物理安全差距评估将通过访谈和检查的方式评测信息系统的物理安全保障情况。

安全通信网络差距评估将通过访谈、检查和测试的方式评测信息系统的网络和通信安全保障情况。

安全管理制度差距评估将通过访谈和检查的形式评测安全策略和管理制度的制定、发布、评审和修订等情况。

信息系统的安全控制集成到目标系统后，会在层面内、层面间和区域间产生连接、交互、依赖、协同等相互关联关系，使信息系统的整体安全功能与信息系统的结构密切相关，在整体上呈现出一种集成特性。这些集成特性在安全控制的工作单元中是没有完全体现。因此，在安全控制评估的基础上，有必要对集成系统和运行环境进行整体评估。

2.查找差距

差距分析的目的是根据国家信息安全等级保护政策和标准，对确定安全保护等级的网络和信息系统，从技术和管理两方面分析其现有的安全防护措施是否达到相应保护等级的要求。包括如下两部分内容：

技术分析：根据国家信息安全等级保护相应级别的技术要求，对物理和环境环境、网络和通信安全、设备和计算安全、应用和数据安全开展差距分析工作。通过访谈、调研问卷、技术测试、查阅资料等多种手段，逐项分析信息系统安全防护水平与等级保护相应级别技术要求的差距。

管理分析：根据国家信息安全等级保护相应级别的管理要求，通过访谈、调研问卷、查阅资料、要求客户举证等多种手段，逐项分析信息系统安全防护水平与等级保护相应级别技术要求的差距。

根据甲方用户安全等级保护测评项目的实际情况，差距分析实施包括访谈、检查和测试三类。访谈是指我方检查人员与本项目内的有关人员就检查所关注的问题进行有针对性的询问和交流的过程，该过程可以帮助我方了解现状、澄清疑问或获得证据。检查是指对检查对象（如规范、机制或行为）进行观察、调查、评审、分析或核查的过程。与访谈类似，该过程可以帮助我方了解项目现状、澄清疑问或获

得证据。测试是指测评人员针对测评对象按照预定的方法/工具使其产生特定的响应，通过查看和分析响应的输出结果，获取证据以证明信息系统安全保护措施是否得以有效实施的一种方法。在测试范围上，应基本覆盖不同类型的机制，在数量上可以抽样。

我中心依托多年的风险评估经验，根据对采购文件的理解，在本次测评过程中，需要加强对目标系统的渗透测试，通过渗透测试可在一定程度上较好的反映出甲方系统上可能存在的安全隐患，为下一步信息安全建设提供依据。

在本次渗透测试项目中将到达以下的目标：通过渗透测试，测评甲方业务系统的安全隐患，并提供实际可行的安全修复建议。

渗透测试过程主要依据安全专家已经掌握的安全漏洞信息，模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试。这里，所有的渗透测试行为将在甲方的书面明确授权和监督下进行。

我方获取到甲方的书面授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案与甲方进行交流，并得到甲方的认同。

在测试实施之前，我方渗透人员会做到让甲方对渗透测试过程和风险的知晓，使随后的正式测试流程都在甲方的控制下。

这包括：操作系统类型指纹收集；网络拓扑结构分析；端口扫描和目标系统提供的服务识别等。可以采用一些商业安全评估系统（如：ISS、极光等）；免费的测评工具（NESSUS、Nmap 等）进行收集。

在规避防火墙、入侵测评、防毒软件等安全产品监控的条件下进行：操作系统可测评到的漏洞测试、应用系统测评到的漏洞测试（如：Web 应用），此阶段如果成功的话，可能获得普通权限。

渗透测试人员可能用到的测试手段有：扫描分析、溢出测试、口令爆破、社会工程学、客户端攻击、中间人攻击等，用于测试人员顺利完成工程。在获取到普通权限后，尝试由普通权限提升为管理员权限，获得对系统的完全控制权。一旦成功控制一台或多台服务器后，测试人员将利用这些被控制的服务器作为跳板，绕过防火墙或其他安全设备的防护，从而对内网其他服务器和客户端进行进一步的渗透。此过程将循环进行，直到测试完成。最后由渗透测试人员清除中间数据。

渗透测试人员根据测试的过程结果编写直观的渗透测试服务报告。内容包括：具有的操作步骤描述；响应分析以及最后的安全修复建议。

渗透测试完成后，我方渗透人员协助甲方对已发现的安全隐患进行修复。修复完成后，我方渗透测试工程师对修复的结果再次进行远程测试复查，对修复的结果进行检验，确保修复结果有效性。

在渗透测试过程中，虽然我方会尽量避免做影响正常业务运行的操作，也会实施风险规避的计策，们是由于测试过程变化多端，渗透测试服务仍然有可能对网络、系统运行造成一定不同程度的影响，严重的后果是可能造成服务停止，甚至是宕机。比如渗透人员实施系统权限提升操作时，突遇系统停电，再次重启时可能会出现系统无法启动的故障等。

因此，我方会在渗透测试前与甲方详细讨论渗透方案，并采取如下多条策略来规避渗透测试带来的风险：

以下列出了主要应用到的系统自带网络应用、管理和诊断工具，我方渗透测试工程师将用到但不限于只是用以下系统命令进行渗透

测试。

工具名称	风险等级	获取途径	主要用途	存在风险描述	风险控制方法
ping	无	系统自带	获取主机信息	无	无
telnet	无	系统自带	登录系统	无	无
ftp	无	系统自带	传输文件	无	无
tracert	无	系统自带	获取网络信息	无	无
net use	无	系统自带	建立连接	无	无
net user	无	系统自带	查看系统用户	无	无
echo	无	系统自带	文件传输	无	无
nslookup	无	系统自带	获取主机信息	无	无
IE	无	系统自带	获取web信息、进行SQL注入	无	无

以下列出了渗透测试中常用到的网络扫描工具、网络管理软件等工具，这些工具都是网络上的免费软件。我方渗透测试工程师将可能利用到但是不限于利用以下工具。远程溢出代码和本地溢出代码需要根据具体系统的版本和漏洞情况来选择，由于几种类繁杂并且没有代表性，在这里不会一一列出。

工具名称	风险等级	获取途径	主要用途	存在风险描述	风险控制方法
namp	无	www.insecure.org	获取主机开放的服务、端口信息	无	无
nessus	低	www.nessus.org	对主机进行漏	可能造成网络	如果主机负

			洞扫描	资源的占用	载过高，停止扫描
Retina	低	www.eeye.com	对主机进行漏洞扫描	可能造成网络资源的占用	如果主机负载过高，停止扫描
nc	无	http://netcat.sourceforge.net	端口连接工具	无	无
远程溢出工具	中	www.securityfocus.com packetstormsecurity.nl	通过漏洞远程进入系统	溢出程序可能造成服务不稳定	备份数据，服务异常时重启服务
本地溢出工具	中	www.securityfocus.com packetstormsecurity.nl	通过漏洞本地提升权限	溢出程序可能造成服务不稳定	备份数据，服务异常时重启服务

（四）安全整改监督及安全整改建议方案

1.安全整改监督方案

我中心在被测系统通过等级保护测评后，将支撑用户方在公安机关对信息安全等保实施情况的监督检查工作，为用户方提供测试技术支持与服务确保证甲方项目合法合规运行。

（1）服务内容

我中心将按采购方需求，对被测系统展开自查包括漏洞扫描，渗透测试，管理制度落实情况核实，设备策略有效性检查，并对采购方在开展安全问题整改工作中提供安全咨询服务。

（2）协助信息安全管理人员进行信息系统安全加固整改建设工作

为了有效保障网络的安全运行，在对操作系统、数据库、中间件、网络设备、安全设备进行安全检测后，需要对发现的安全风险进行修复。

安全加固服务，是指根据安全加固列表，对目标系统的安全漏洞对进行修复、配置隐患进行优化的过程。加固内容包括但不限于系统补丁更新、本地安全策略加固、危险端口和服务关闭、本地共享关闭等内容。

1. 操作系统加固

可进行安全加固的操作系统包括 Windows、Linux、AIX、HP-Unix、Solaris。操作系统的加固内容如下表所示:

序号	分类	项目
1	账号管理和认证授权	账号、口令、授权、关机设置
2	协议安全配置	IP协议安全、防火墙、SYN攻击防护
3	服务和共享配置	系统服务、默认共享、共享权限
4	日志安全配置	日志审核策略、日志文件设置
5	其它安全配置	空闲超时设置、自动播放、启动项、数据执行保护

2. 数据库安全加固

可进行安全加固的数据库系统包括 Oracle、SQL Server、DB2。数据库的加固内容如下表所示:

序号	分类	项目
1	账号管理和认证授权	账号、口令
2	通信协议安全	网络数据传输安全、信任IP设置

3	日志安全配置	数据库审核策略、数据库日志文件设置
4	其它安全配置	连接超时设置、监听器密码

3. 中间件安全加固

可进行安全加固的中间件系统包括 Tomcat、Apache、WebLogic、WebSphere。中间件系统的加固内容如下表所示:

序号	分类	项目
1	账号管理和认证授权	账号、口令
2	通信协议安全	启用https传输、更改tomcat默认端口
3	日志安全配置	日志记录设置
4	其它安全配置	登录超时、错误重定向、禁止显示文件

4. 网络设备安全加固

可进行安全加固的网络设备包括主流厂商的路由器、交换机。网络设备的加固内容如下表所示:

序号	分类	项目
1	账号管理和认证授权	账号管理、登录安全要求、认证授权
2	通信协议安全	SNMP协议安全、路由协议安全、IP协议安全
3	日志安全配置	日志记录设置
4	其它安全配置	关闭不必要的服务、端口

5. 安全设备加固

可进行安全加固的安全设备是主流厂商的防火墙、入侵防护、安全设备等常见安全设备，安全设备的加固内容如下表所示，具体的加固列表可参见我司的安全设备安全加固规范。

序号	分类	项目
1	账号管理和认证授权	账号、口令、授权
2	访问控制安全	安全策略、远程管理
3	日志安全配置	启用本地日志、启用远程日志
4	增强安全要求	限定管理IP、更改默认Banner、设备自身安全设置

2.安全整改建议方案

（1）整改建议服务目的

我方将根据整改建议清单中涉及安全管理部分缺失的网络安全管理制度、作业指导书和应急方案提供指导服务，指导建立更完善的网络安全基线管理制度体系。主要分为两大方面：安全技术整改咨询和管理制度梳理。技术整改咨询包含网络安全、主机安全、应用安全、数据安全等方面建设整改。管理制度梳理包含信息安全管理机构设置、安全管理制度、人员安全管理、系统建设管理和系统运维管理五个方面。

根据前期的定级、备案结果，同时在完成对目标系统的差异分析之后，通过对全面检查的测评结果发现的问题，结合系统实际情况，完成并提交合理、切实可行的整改建议报告，使目标系统按照整改建议进行加固后达到全面检查和正式测评的要求。

（2）整改建议服务流程

本部分工作内容主要分为两大方面：安全技术咨询和管理制度梳理。

在技术整改咨询方面，主要包括对安全通信网络、安全区域边界、安全计算环境、安全管理中心以及云计算平台作为云租户端的相关问

题的安全整改和加固。具体包括各类设备的正确使用，合理部署。确保整个设备设施安全、可控。在数据库、操作系统、以及应用系统方面所存在的配置漏洞以及软件功能不足进行识别，并给出改进建议，确保整改措施合规有效。

在管理制度梳理方面，我方将协助采购方开展管理体系梳理，部分管理制度落地，依据等级保护要求，梳理管理体系中的方针、制度，使其符合等级保护对应级别的要求。对采购方的系统建设方案、日常系统运行等方面的安全建设方案、安全设计详细方案、安全设计配套方案、安全整改方案等进行咨询并根据相关法律法规进行审定提供安全建设性意见和建议。

结合技术整改咨询和管理制度梳理，针对差距分析的问题协助院方编制整改。同时，我方将与院方建立整改沟通计划，通过电话、视频会议和现场沟通的方式对存在的主要问题、问题产生的原因、整改进行充分交流，协助院方及开发和运维单位快速、有效地开展网络安全整改加固工作，降低系统与等级保护基本要求之前存在的差距，增强系统安全防护能力。

（3）安全技术层面整改内容

针对本项目信息系统的测评结果分析情况，并依据采购方信息系统实际情况，通过分层的方法对信息系统整体进行安全需求分析，安全技术整体上可以从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面按照等级保护标准进行整改。

（4）安全管理层面整改内容

安全策略：制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

管理制度：应制定信息安全工作的总体方针和安全策略，建立安全管理制度和操作规程，形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

制定和发布：应指定或授权专门的部门或人员负责安全管理制度的制定，管理制度应具有统一的格式，对制度进行论证和审定，通过正式、有效的方式发布，并对收发文进行登记。

评审和修订：信息安全领导小组应负责定期审定安全管理制度体系，必要时进行修订。

岗位设置：应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人、系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责，成立指导和管理信息安全工作的委员会或领导小组，明确职责、分工和技能要求。

人员配备：应配备一定数量的系统管理员、网络管理员、专职安全管理员，关键事务岗位应配备多人共同管理。

授权和审批：应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等，建立审批程序，定期审查审批事项，记录审批过程并保存审批文档。

沟通和合作：应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部、兄弟单位、公安机关、电信公司、供应商、业界专家、专业的安全公司、安全组织的合作与沟通，建立外联单位联系列表，聘请信息安全专家作为常年的安全顾问。

审核和检查：安全管理员应负责定期进行安全检查，内部人员或上级单位定期进行全面安全检查，制定安全检查表格实施安全检查，制定安全审核和安全检查制度。

人员录用：应指定或授权专门的部门或人员负责人员录用，严格规范人员录用过程，签署保密协议，从内部人员中选拔从事关键岗位的人员并签署岗位安全协议。

人员离岗：应严格规范人员离岗过程，及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，办理严格的调离手续。

安全意识教育和培训：应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，应对安全责任和惩戒措施进行书面规定并告知相关人员，对定期安全教育和培训进行书面规定，对安全教育和培训的情况和结果进行记录并归档保存。

外部人员访问管理：应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案，对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定。

定级和备案：应明确信息系统的边界和安全保护等级，应确保定级结果经过相关部门的批准。应指定专门的部门或人员负责管理系统定级的相关材料，将系统等级及相关材料报系统主管部门备案。

产品采购和使用：应确保安全产品采购和使用符合国家的有关规定。

自行软件开发：应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制，制定软件开发管理制度，制定代码编写安全规范。

自行软件开发：应根据开发需求测评软件质量，测评软件包中可能存在的恶意代码，审查软件中可能存在的后门。

外包软件开发：应根据开发需求测评软件质量，测评软件包中可

能存在的恶意代码，审查软件中可能存在的后门。

工程实施：应指定或授权专门的部门或人员负责工程实施过程的管理，制定详细的工程实施方案控制实施过程，制定工程实施方面的管理制度。

测试验收：应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告，组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

系统交付：应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

等级测评：在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。

服务供应商商选择：应确保安全服务商的选择符合国家的有关规定。

环境管理：应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理，指定部门负责机房安全，并配备机房安全管理人员，建立机房安全管理制度，加强对办公环境的保密性管理。

资产管理：应编制并保存与信息系统相关的资产清单，建立资产安全管理制度，对资产进行标识。

介质管理：应建立介质安全管理制度。

设备维护管理：应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理，应建立设备安全管理制度。

漏洞和风险管理：应对发现的安全漏洞和隐患及时进行修补或评

估可能的影响后进行修补。

网络和系统安全管理：应指定专人对网络进行管理，应建立网络安全管理制度。应根据业务需求和系统安全分析确定系统的访问控制策略，定期进行漏洞扫描，安装系统的最新补丁程序，建立系统安全管理制度。

恶意代码防范管理：应提高所有用户的防病毒意识，指定专人对网络和系统进行恶意代码测评并保存测评记录，定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录。

配置管理：检查记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数。

密码管理：应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

变更管理：应确认系统中要发生的变更，并制定变更方案，建立变更管理制度，建立变更控制的申报和审批文件化程序。

备份与恢复：应识别需要定期备份的重要业务信息、系统数据及软件系统等，建立备份与恢复管理相关的安全管理制度，建立控制数据备份和恢复过程的程序。

安全事件处置：应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点，制定安全事件报告和处置管理制度，制定安全事件报告和响应处理程序。

应急预案管理：应在统一的应急预案框架下制定不同事件的应急预案，从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障，对系统相关的人员进行应急预案培训、演练、定期审查。

（5）协助编制整改意见

为了有效保障网络的安全运行，在对操作系统、数据库、中间件、网络设备、安全设备进行安全检测后，需要对发现的安全风险进行修复。

整改加固是根据安全加固列表，对目标系统的安全漏洞对进行修复、配置隐患进行优化的过程。整改建议是安全整改加固的基础和依据。加固内容包括但不限于系统补丁更新、本地安全策略加固、危险端口和服务关闭、本地共享关闭等内容。

（五）等级保护测评方案

1.测评服务目标

我方根据等级保护基本要求，从安全技术层面和安全管理层面对备案系统进行等级测评，确保所有问题得到正确的解决，保证系统已经达到等级保护相应级别要求，并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，单项测评结果是形成等级测评结论的基础。我方提交正式的等级测评报告，上报公安机关，通过等级保护测评。

2.测评准备阶段服务流程

（1）测评实施准备综述

准备工作是项目实施的起始阶段，为后续的项目实施完成一些基础性工作，具体工作包括:

1)成立项目实施团队

为了保障各项实施工作的顺利开展，首先由甲方和我方共同组建项目实施团队，由领导小组、项目专家组、质量小组和实施小组等组成。其中，由被评测单位的信息中心信息化部门主管信息安全工作的

领导和安全管理员组成协调小组，主要负责和评测组工作对接，商议工作计划，安排评测组的现场活动，协调各部门或内部人员配合安全评测开展等工作；项目专家组和质量小组由我方和甲方的信息安全领域专家共同担任，主要对方案和报告的审核；实施小组主要负责提前与被测评单位的协调、沟通及现场的具体测评工作。

2)项目计划书编制

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。

3)信息系统调研

实施小组提前与被测评单位沟通，并下发资产调研表和应用调研表，被测评单位反馈给实施小组后，查阅相关调研表，了解整个系统的构成和保护情况，明确目标系统的范围（特别是信息系统的边界），了解目标系统的详细构成，包括网络拓扑、业务应用、业务流程、设备信息（服务器、数据库、网络设备、安全设备、数据库等）、管理制度等。

4)工具和表单准备

明确目标系统的实际情况后，实施小组准备测评工具和各类测评表单。

输入文档为：

■项目计划书；

■信息系统资产调研表；

■信息系统应用调研表；

■物理环境调研表；

■管理安全调研表；

■网络调研表；

■应用调研表；

■测评工具清单。

输出文档为：

■资产调研反馈表；

■应用调研反馈表。

（2）测评指标选取

《网络安全等级保护基本要求》中对不同等级信息系统的安全功能和措施作了具体的要求，信息安全等级测评要根据信息系统的等级从中选取相应等级的安全测评指标，并根据被测评单位信息系统的定级结果，对该系统实施安全等级测评。因此，本次测评将根据目标系统的安全等级选取的测评指标。

1)安全通用要求指标

依据甲方信息系统的暂定定级结果，选择《网络安全等级保护基本要求》中对应级别的安全要求作为等级测评的基本指标。

安全通用要求指标

安全类	安全控制点	测评项数
安全物理环境	物理位置的选择	2
	物理访问控制	1
	防盗窃和防破坏	3
	防雷击	2
	防火	3

安全类	安全控制点	测评项数
	防水和防潮	3
	防静电	2
	温湿度控制	1
	电力供应	3
	电磁防护	2
安全通信网络	网络架构	5
	通信传输	2
	可信验证	1
安全区域边界	边界防护	4
	访问控制	5
	入侵防范	4
	恶意代码和垃圾邮件防范	2
	安全审计	4
	可信验证	1
安全计算环境	身份鉴别	4
	访问控制	7
	安全审计	4

安全类	安全控制点	测评项数
	入侵防范	6
	恶意代码防范	1
	可信验证	1
	数据完整性	2
	数据保密性	2
	数据备份恢复	3
	剩余信息保护	2
	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	2
	集中管控	6
安全管理制度	安全策略	1
	管理制度	3
	制定和发布	2
	评审和修订	1
安全管理机构	岗位设置	3

安全类	安全控制点	测评项数
	人员配备	2
	授权和审批	3
	沟通和合作	3
	审核和检查	3
安全管理人员	人员录用	3
	人员离岗	2
	安全意识教育和培训	3
	外部人员访问管理	4
安全建设管理	定级和备案	4
	安全设计	3
	产品采购和使用	3
	自行软件开发	7
	外包软件开发	3
	工程实施	3
	测试验收	2
	系统交付	3
	等级测评	3

安全类	安全控制点	测评项数
	服务供应商选择	3
安全运维管理	环境管理	3
	资产管理	3
	介质管理	2
	设备维护管理	4
	漏洞和风险管理	2
	网络和系统安全管理	10
	恶意代码防范管理	2
	配置管理	2
	密码管理	2
	变更管理	3
	备份与恢复管理	3
	安全事件处置	4
	应急预案管理	4
	外包运维管理	4

2)渗透测评覆盖指标

我方根据多年在渗透测试的经验,在本次验证测试中所涉及的渗透测试过程中，将主要涉及 SQL 注入类、跨站脚本类、认证会话管

理类、弱口令类、信息未加密类、文件包含类、目录浏览类、不安全的 URL 访问类、溢出漏洞类、信息泄露类、文件上传类、未授权访问类、跨站请求伪造类、未验证的重定向跳转类等渗透测评。具体测试指标见下表:

分类	编号	测试内容
信息收集测试	OTG-INFO-001	搜索引擎信息收集
	OTG-INFO-002	Web服务器指纹识别
	OTG-INFO-003	审查web服务器源文件信息泄露
	OTG-INFO-004	枚举web服务器的应用
	OTG-INFO-005	注释和元数据信息泄露
	OTG-INFO-006	识别应用的入口
	OTG-INFO-007	映射应用程序的执行路径
	OTG-INFO-008	识别web应用框架
	OTG-INFO-009	识别web应用程序
	OTG-INFO-010	映射应用架构
配置管理测试	OTG-CONFIG-001	网络和基础设施配置测试
	OTG-CONFIG-002	应用平台配置测试
	OTG-CONFIG-003	文件扩展处理敏感信息测试
	OTG-CONFIG-004	对旧文件，备份和没有被引用的文件敏感信息的审查
	OTG-CONFIG-005	枚举基础设施和应用程序管理界面
	OTG-CONFIG-006	HTTP方法测试
	OTG-CONFIG-007	HTTP强制安全传输测试

分类	编号	测试内容
	OTG-CONFIG-008	RIA跨域策略测试
身份管理测试	OTG-IDENT-001	角色定义测试
	OTG-IDENT-002	用户注册流程测试
	OTG-IDENT-003	账户配置过程测试
	OTG-IDENT-004	账户枚举和可猜测的用户账户测试
	OTG-IDENT-005	弱的或未实施的用户策略测试
认证测试	OTG-AUTHN-001	凭证在加密通道中得传输测试
	OTG-AUTHN-002	默认用户凭证测试
	OTG-AUTHN-003	弱锁定机制测试
	OTG-AUTHN-004	认证模式绕过测试
	OTG-AUTHN-005	记忆密码功能存在的威胁测试
	OTG-AUTHN-006	浏览器缓存威胁测试
	OTG-AUTHN-007	弱密码策略测试
	OTG-AUTHN-008	弱安全问答测试
	OTG-AUTHN-009	弱密码的更改或重设功能测试
	OTG-AUTHN-010	在辅助信道中较弱的认证测试
授权测试	OTG-AUTHZ-001	目录遍历/文件包含测试
	OTG-AUTHZ-002	绕过授权模式测试
	OTG-AUTHZ-003	权限提升测试
	OTG-AUTHZ-004	测试不安全的直接对象引用
会话管理测试	OTG-SESS-001	会话管理架构绕过测试
	OTG-SESS-002	Cookie属性测试

分类	编号	测试内容
	OTG-SESS-003	会话固定测试
	OTG-SESS-004	会话变量泄露测试
	OTG-SESS-005	跨站伪造请求
输入验证测试	OTG-INPVAL-001	反射型跨站脚本测试
	OTG-INPVAL-002	存储型跨站脚本测试
	OTG-INPVAL-003	HTTP方法篡改测试
	OTG-INPVAL-004	HTTP参数污染测试
	OTG-INPVAL-005	SQL注入测试
	OTG-INPVAL-006	LDAP测试
	OTG-INPVAL-007	ORM注入测试
	OTG-INPVAL-008	XML注入测试
	OTG-INPVAL-009	SSI注入测试
	OTG-INPVAL-010	XPath注入测试
	OTG-INPVAL-011	IMAP/SMTP注入测试
	OTG-INPVAL-012	代码注入测试
	OTG-INPVAL-013	命令注入测试
	OTG-INPVAL-014	缓冲区溢出测试
	OTG-INPVAL-015	潜伏式漏洞测试
	OTG-INPVAL-016	HTTP拆分/走私测试
错误处理测试	OTG-ERR-001	报错信息测试
	OTG-ERR-002	堆栈轨迹测试
加密体系脆弱性测试	OTG-CRYPST-001	弱加密、传输层协议缺陷测试
	OTG-CRYPST-002	Padding Oracle攻击监测

分类	编号	测试内容
	OTG-CRYPST-003	通过未加密信道发送敏感数据测试
业务逻辑测试	OTG-BUSLOGIC-001	业务逻辑数据验证测试
	OTG-BUSLOGIC-002	伪造请求的测试
	OTG-BUSLOGIC-003	完整性检查测试
	OTG-BUSLOGIC-004	进程定时测试
	OTG-BUSLOGIC-005	功能使用次数限制
	OTG-BUSLOGIC-006	工作流程逃逸的测试
	OTG-BUSLOGIC-007	防御应用程序滥用测试
	OTG-BUSLOGIC-008	意外文件类型上传测试
	OTG-BUSLOGIC-009	恶意文件上传测试
客户端测试	OTG-CLIENT-001	测试基于DOM的跨站脚本
	OTG-CLIENT-002	JavaScript执行测试
	OTG-CLIENT-003	HTML注入测试
	OTG-CLIENT-004	客户端URL重定向测试
	OTG-CLIENT-005	CSS注入测试
	OTG-CLIENT-006	客户端资源处理测试
	OTG-CLIENT-007	跨源资源共享测试
	OTG-CLIENT-008	跨站Flash测试
	OTG-CLIENT-009	点击劫持测试
	OTG-CLIENT-010	测试WebSockets
	OTG-CLIENT-011	Web消息测试
	OTG-CLIENT-012	本地存储测试

（3）测评编制

1)形成现场实施方案

在甲方的统一组织下，由项目专家组、实施小组共同讨论、研究，形成《网络安全等级测评方案》。

2)形成统一的项目实施方法

制定网络安全服务工作规范，统一测评工具集和测试用例库，测评技术方法研讨和测评工作规范化制表等工作。

3)信息系统的定级梳理

完成对目标系统的定级备案工作，出具《信息系统定级报告》。

4)确定项目实施范围

以此次投标涉及到的被测信息系统为实施范围。

5)熟悉信息安全服务的内容和环境

采用问卷调研、资料分析和实地调研等方式，充分了解测评对象信息系统的运行状况，初步确认测评对象的信息资产，为现场实施阶段做好准备。

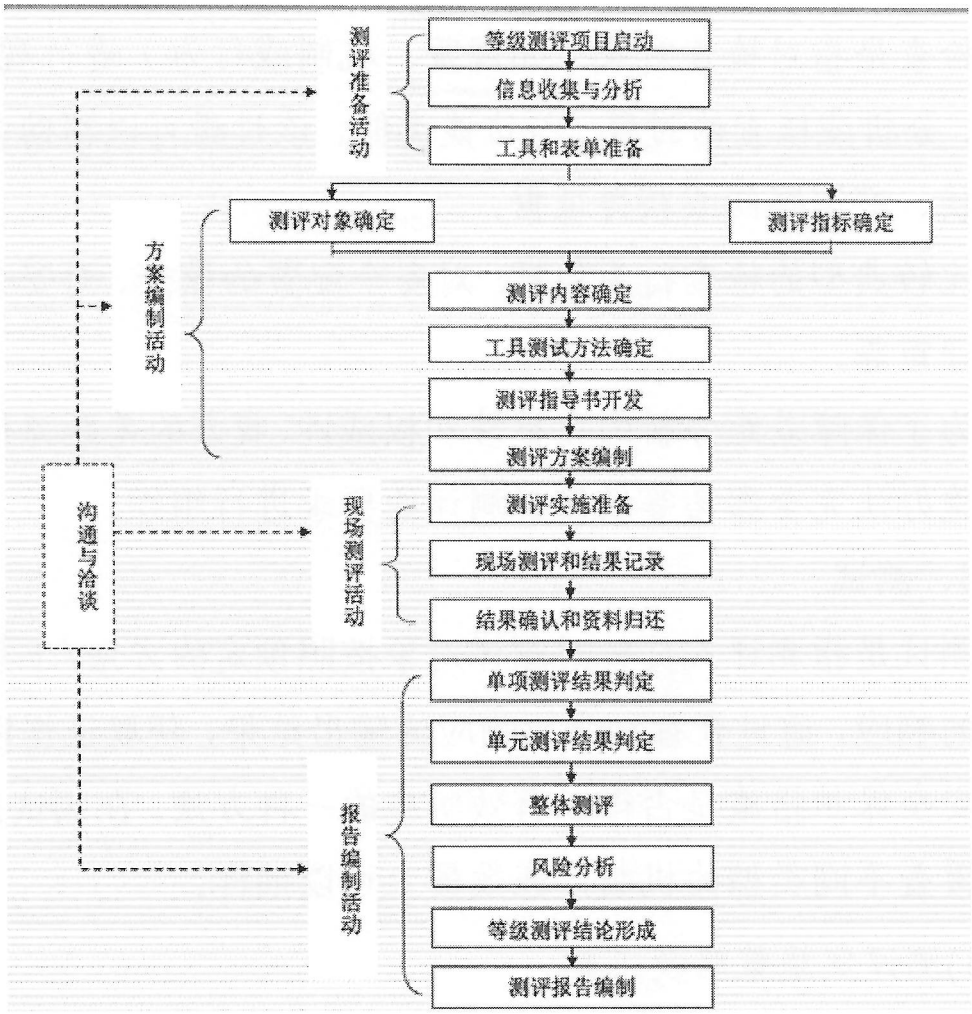
6)确认评测保障条件

与被测评方及时沟通，确认项目实施过程中的保障条件，为现场实施工作的顺利开展打下良好的基础。

3.进行现场等级保护测评

（1）测评实施流程

对于本项目，我方等级保护测评实施过程包括以下四个阶段：



（2）测评实施策略方法及工具

根据甲方的实际情况，整个测评实施的方法包括访谈、检查和测试三类。

1、访谈

访谈是指我方检查人员与本项目内的有关人员就检查所关注的问题进行有针对性的询问和交流的过程，该过程可以帮助我方了解现状、澄清疑问或获得证据。

访谈深度（即访谈内容的详细程度）以及访谈的广度（即对被检查组织中员工角色类型以及每种类型中人数的覆盖程度）由我方检查人员依据不同的检查需要进行选择和判断。

2、检查

检查是指对检查对象（如规范、机制或行为）进行观察、调查、评审、分析或核查的过程。与访谈类似，该过程可以帮助我方了解项目现状、澄清疑问或获得证据。

比较典型的检查行为包括：对安全配置的核查、对安全策略的分析和评审等。

为了保障差距分析的完整性和权威性，我方的差距评估工作的具体实施办法完全参考等级保护测评的要求进行组织。

3、测试

测试是指测评人员针对测评对象按照预定的方法/工具使其产生特定的响应，通过查看和分析响应的输出结果，获取证据以证明信息系统安全保护措施是否得以有效实施的一种方法。在测试范围上，应基本覆盖不同类型的机制，在数量上可以抽样。

1)测评实施策略及工具

利用技术工具（漏洞扫描工具、渗透测试工具、性能测试工具等）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、渗透测试、性能测试等。

测评方法	工具测试
简要描述	利用技术工具，从网络的不同接入点对网络内的主机、服务器、数据库、网络设备、安全设备等进行脆弱性检查和分析
达成目标	发掘系统的安全漏洞
工作条件	1-2人工作环境，电源和网络接入环境，甲方人员、网络、系统配合
工作结果	工具测试结果记录

2)安全扫描策略

通过远程渗透性测试可测评目标系统存在的如下安全漏洞扫描：

序号	安全漏洞名称	漏洞内容描述
1	跨站脚本	向web用户浏览页面插入不加审核的数据导致恶意代码在客户端主机执行
2	主机远程安全	未及时安装补丁或升级的服务器很容易被黑客利用其漏洞进行攻击
3	残留信息	备份文件遗留隐患：在开发过程中，被放在web服务器上而且便于获取的一些旧的、备份的或临时文件容易泄漏敏感信息
4		调试选项遗留隐患：带入生产系统的原调试信息、不被使用的代码或一些后门机制给恶意黑客提供了极大的方便
5	SQL注入	入侵者利用应用程序中，通过未经合法性判断的用户输入数据来构造动态SQL语句的漏洞来改变原SQL语句的含义进而执行任意SQL命令
6	系统信息泄漏	Web服务器在运行中暴露出的错误信息会被攻击者利用来获得站点的行为、结构或配置
7	弱口令	弱口令可以导致非常严重的后果，如造成设备、服务器、应用系统被完全控制等

3)渗透测试

渗透测试主要是通过模拟黑客对目标系统进行渗透测试，发现并分析其存在的设备和计算安全漏洞、敏感信息泄露、SQL 注入漏洞、跨站脚本漏洞及弱口令等安全隐患，检查网站的防篡改能力、防渗透能力、数据库防窃取/防篡改能力、网络安全体系防入侵能力，验证漏洞的危害程度，评估网站的整体安全风险，提出加固建议，从而提

高目标系统的安全抵御能力。总体来说渗透测试分为三种类型:

第一类型:互联网渗透测试，是通过互联网发起远程攻击，比其他类型的渗透测试更能说明漏洞的严重性。

第二类型：外联网渗透测试，通过接入外联网发起远程攻击。

第三类型：内网渗透测试，通过接入内部网络发起内部攻击。

具体实施安排根据甲方的需求，经双方协商确定后进行。

① 基础信息收集

利用扫描工具对甲方提供的渗透测试范围内所有主机进行扫描，获得目标主机群的端口开放情况、主机操作系统类型、web 服务器类型、web 开发语言、后台数据库类型、后台管理入口等基础信息。

② 设备和计算安全分析

借助专用扫描器，分析目标主机群操作系统版本、web 服务器及其他对外开放的服务程序版本及漏洞情况。

如已获取本地部分权限,则借助系统命令或工具进一步深入检查设备和计算安全配置缺陷。

③ 残留及敏感信息分析

人工方式研究网站的典型页面文件及其源代码,并尝试各种可能的残留信息保存方式。如已获取本地部分权限，则借助系统命令或工具检查残留及敏感信息的泄漏情况。

④ 应用安全分析

借助工具分析动态网页中存在的跨站脚本漏洞或 SQL 注入漏洞,在发现可利用漏洞后尝试执行可对系统或数据库进行操作的指令,以检查是否可提升权限。如已获取本地部分权限，则借助系统命令或工具对部分代码进行深入分析。

⑤ 弱口令分析

根据典型的弱口令特点，并结合甲方的特征，建立专门的口令字典。利用工具或手工进行尝试猜测。如获得合法账号，则登录并进一步深入分析。

安全漏洞

通过远程渗透性测试可测评目标系统存在的如下安全漏洞：

序号	安全漏洞名称	漏洞内容描述
1	跨站脚本	向 web 用户浏览页面插入不加审核的数据导致恶意代码在客户端主机执行
2	主机远程安全	未及时安装补丁或升级的服务器很容易被黑客利用其漏洞进行攻击
3	残留信息	备份文件遗留隐患：在开发过程中，被放在 web 服务器上而且便于获取的一些旧的、备份的或临时文件容易泄漏敏感信息
4		调试选项遗留隐患：带入生产系统的原调试信息、不被使用的代码或一些后门机制给恶意黑客提供了极大的方便
5	SQL注入	入侵者利用应用程序中，通过未经合法性判断的用户输入数据来构造动态 SQL 语句的漏洞来改变原 SQL 语句的含义进而执行任意 SQL 命令
6	系统信息泄漏	Web 服务器在运行中暴露出的错误信息会被攻击者利用来获得站点的行为、结构或配置
7	弱口令	弱口令可以导致非常严重的后果，如造成设备、服务器、应用系统被完全控制等

渗透工具介绍

渗透测试人员模拟黑客入侵攻击的过程中使用的是操作系统自带网络应用、管理和诊断工具、黑客可以在网络上免费下载的扫描器、远程入侵代码和本地提升权限代码以及我方自主开发的安全扫描工具。

这些工具经过全球数以万计的程序员、网络管理员、安全专家以及黑客的测试和实际应用，在技术上已经非常成熟，实现了网络检查和安全测试的高度可控性，能够根据使用者的实际要求进行有针对性的测试。但是安全工具本身也是一把双刃剑，为了做到万无一失，我们也将针对系统可能出现的不稳定现象提出相应对策，以确保服务器和网络设备在进行渗透测试的过程中保持在可信状态。

4)配置检查

利用上机验证的方式检查主机、服务器、数据库、网络设备、安全设备、应用系统的配置是否正确，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），测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，从而测试系统是否达到可用性和可靠性的要求。

测评方法	配置检查
简要描述	通过登陆系统控制台的方式，人工核查和分析主机、服务器、数据库、网络设备、安全设备、应用系统的安全配置情况
达成目标	发现配置的安全隐患
工作条件	1-2人工作环境，甲方人员、网络、系统配合
工作结果	配置检查结果记录

配置检查示例

表-安全计算环境作业指导书

控制点	测评项	检查内容	检查方法	推荐值
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	1、应核查用户在登陆时是否采用了身份鉴别措施； 2、应核查用户列表确认用户身份标识是否具有唯一性； 3、应核查用户配置信息或测试验证是否不存在空口令用户； 4、应核查用户鉴别信息是否具有复杂度要求并定期更换。	1、在运行中输入rundll32netplwiz.dll,UsersRunDll或controluserpasswords2，查看是否勾选了“要使用本机，必须输入用户和密码”； 2、控制面板-用户账户-添加或删除用户-检查所有账户是否均启用密码保护。 3、在运行中输入lusrmgr.msc-用户-双击各个用户-检查是否勾选密码永不过期，测评是否存在同名账户； 4、在运行中输入secpol.msc-账户策略-检查密码策略。	1、勾选了“要使用本机,用户必须输入用户名和密码”； 2、均启用密码保护，结合扫描查看是否存在弱口令账户。 3、不存在同名账户。 4、密码策略 1）已启用； 2）8个字符； 3）90天； 4）2天； 5）5个记住的密码 6）未勾选“密码永不过期”。
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	1、应核查是否配置并启用了登录失败处理功能； 2、应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账号锁定等； 3、应核查是否配置并启用了登录连续超时及自动退出功能。	1、Windows系统账户设置密码后默认启用了登录失败处理功 2、在运行中输入secpol.msc-帐户策路一密码策路-检查账户锁定策略； 3、控制面板-外观-更改屏幕保护程序-检查是否启用带口今的屏保程序。 4、在运行中輸入gpe—管理模板—Windows组件—远程桌面服务—远程桌面会话主机—会话时间限制中，查看是否设置“活动但空闲的远程桌面服务会话时间的限制”。	1、Windows默认启用了登录失败处理功能。 2、账户锁定策略 1)30分钟； 2)5次无效登录； 3)30分钟之后。 3、启用屏幕保护程序并勾选“在恢复时显示登录屏幕”,推荐设置等待时间:15分钟。 4、启用“活动状态日空闲的终端服务会话设置时间限制”,推荐设置空闲会话设置时间:15分钟。
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网	应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在	1、查看控制面板-管理工具-服务,是否禁用telnet服务;查看是否启用TerminalServicesl服务(远程桌面)或采取了其它安全	1、禁用telnet服务采取3389远程桌面或其他加密的远程管理方式进行管理。

	络传输过程中被窃听；	网络传输过程中被窃听。	可靠的远程管理方式。 2、右键计算机-属性-远程设置-查看远程桌面与远程协助是否开启。	
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	1、应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别； 2、应核查其中一种鉴别技术是否使用密码技术来实现。	1、是否采用两种或两种以上组合的鉴别技术对管理用户进行身份签别； 2、核查其中一种鉴别技术是否使用国家认可的密码技术来实现。	1、采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户进行身份签别； 2、其中一种签别采用了国家认可的密码技术。
访问控制	a)应对登录的用户分配账户和权限；	1、应核查是否为用户分配了账户和权限及相关设置情况； 2、应核查是否已禁用或限制匿名、默认账户的访问权限。	1、要求提供用户权限对照表，在运行中输入lusrmgr.msc在本地用户和组中查看当前用户是否与与权限对照表一致,并检查各个账户是否建属于相应的组。 2、 1)在运行中输入lumar.msc,检查默认帐户(Administrator、Guest)的访问权限； 2)运行中输入secpol.msc-本地策略-安全选项:“帐户:管理员帐户状态”“帐户:来宾帐户状态”,检查默认帐户(Administrator、Guest）是否已禁用。	1、制定了用户权限表，并根据权限表进行分配账户权限； 2、授予管理员、来宾用户最小的权限，或禁用默认管理员、来宾用户。
	b)应重命名或删除默认账户，修改默认账户的默认口令；	1、应核查是否已经重命名默认账户或默认账户已被删除； 2、应核查是否已修改默认账户的默认口令。	如果1)和2) 1、运行中输入secpol.msc安全选项:“帐户重命名来宾帐户”和帐户:重命名系统管理员帐户”,检查默认帐户(Administrator、Guest)是否重命名或删除。 2、检查启用中的帐户默认(Administrator、Guest)口	1、默认用户已经重命名或已被删除； 2、更改了默认账户的默认口令。

			令是否均已修改。均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本评单元指标要求。	
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	1、应核查是否不存在多余或过期账户,管理员用户与账户之间是否一一对应； 2、应测试验证多余的、过期的账户是否被删除或停用。	1、在运行中输入lusrmgr.msc-在本地用户和组中查看当前用户是否与用户权限对照表一致,检查是否存在多余、过期的账户。 2、询问是否存在共享账户的情况。	1、不存在多余、过期的用户，管理员用户与账户之间一一对应。
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离；	1、应核查是否进行角色划分； 2、应核查管理用户的权限是否已进行分离； 3、应核查管理用户权限是否为其工作任务所需的最小权限。	1、要求提供用户权限对照表，在运行中输入lusrmgr.msc在本地用户和组中查看当前用户是否与与权限对照表一致,并检查各个账户是否隶属于相应的组。 2、查看是否建立了管理员、审计员、操作员等角色,实现了管理用户的权限分离； 3、根据提供的权限表验证是否授予管理用户最小的权限。	1、建立了用户权限分配表明确各帐户权限； 2、建立了管理员、审计员、操作员等角色,实现了管理用户的权限分离； 3、授予管理用户最小的权限。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	1、应核查是否由授权主体(如管理用户)负责配置访问控制策略； 2、应核查授权主体是否依据安全策略配置了主体对客体的访问规则； 3、应测试验证用户是否有可越权访问情形。	1、询问是否由管理员账户对策略进行统一控制。 2、检查服务器操作系统是否依据安全策略配置本机的访问控制规则。 3、检查是否存在多余的管理员权限账户。	1、由管理员账户对策略进行统一控制； 2、依据安全策略配置访问控制规则； 3、无多余管理员权限用户。

	f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	应核查访问控制策略的控制粒度是否达到主体为用户级别或进程级，客体为文件、数据库表、记录或字段级。	Windows操作系统基于自主访问控制机制来实现访问控制,进程权限的控制属于基于角色的访问控制。	Windows默认符合。
	g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	1、应核查是否对主体、客体设置了安全标记； 2、应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。	1、询问主机管理员是否对操作系统的主体(用户级或进程级)与客体(文件、数据库表级)设置了安全标记。 2、检查安全标记主体是否依据强制访问策略对安全标记客体设置了严格的访问限制策略。	1、设置了主机中主体、客体的安全标记； 2、依据访问控制策略严格限制安全记主体对安全记客体的访问权限。
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	1、应核查是否开启了安全审计功能； 2、应核查安全审计范围是否覆盖到每个用户； 3、应核查是否对重要的用户行为和重要安全事件进行审计。	1、查看控制面板-管理工具-本地安全策略-本地策略-审核策略,查看审计策略是否全部开启成功和失败的亩核； 2、若开启日志亩核,默认对全部用户有效； 3、核查是否对重要的用户行为和重要安全事件进行审计。	1、审核策略: 1)审核策略更改成功,失败； 2)审核登录事件成功,失败； 3)审核对象访问成功,失败； 4)审核进程跟踪成功,失败； 5)审核目录服务访问-成功,失败； 6)审核特权使用成功,失败； 7)审核系统事件成功,失败； 8)审核帐户登录事件一成功,失败； 9)审核帐户管理成功,失败； 2、开启审核策略后，默认符合； 3、开启全部策略-成功和失败的审核。

	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	控制面板-管理工具-本地安全策略-本地策略-审核策略。	只要开启了完整的审核策略默认符合。
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	1、应核查是否采取了保护措施对审计记录进行保护； 2、应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。	1、 1)禁止Guest账户访问事件日志，查看注册表: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\security HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\system 下面是否有名为RestrictGuestAcces的键值； 2）查看“本地安全策略”-“用户权利指派”中的“管理审核和安全日志”，查看是否除审计员、administrator外其他用户无权限； 3）询问审计员是否定期对系统日志进行备份，查看备份策略，系统日志留存时间是否符合法律规定要求。	1、 1）添加Reg_DWORD类型的键：RestrictGuestAccess，键值为1，默认符合； 2)审计日志设置只有审计角色才能删除、修改或夏盖等，且删除、修改或覆盖等操作会进行记录。其他用户不能删除修改或盖等； 2、查看系统日志(默认C:\Windows\System32\config,C:\Windows\System32\winevt\Logs)的备份文件，备份文件留存不少于六个月。

	d)应对审计进程进行保护，防止未经授权的中断。	应测试验证通过非审计管理员的其他账户来中断审计进程，验证审计进程是否受到保护。	Windows系统具备了在审计进程自我保护方面功能。	Windows系统具备了在审计进程自我保护方面功能。
入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；	1、应核查是否遵循最小安装原则； 2、应核查是否未安装非必要的组件和应用程序。	1、管理工具-服务-查看可以使用的服务； 2、“控制面板”-“程序和功能”-“打开或关闭Windows功能”-“删除功能”。	1、仅启用必须的角色和功能； 2、关闭不需要组件和应用程序，仅启用必须的功能。
	b)应关闭不需要的系统服务、默认共享和高危端口；	1、应核查是否关闭了非必要的系统服务和默认共享； 2、应核查是否不存在非必要的高危端口。	1、 1）查看控制面板-管理工具-服务，或运行中输入services.msc； 2）查看控制面板-管理工具-计算机管理-共享文件夹； 2、监听端口，命令行输入“netstat-an”。	1、 1）禁用不需要的系统服务（PrintSpooler、RemoteRegistry、DHCPClient、telephony等）； 2）关闭默认共享； 2、关闭非必要的高危端口（135、137、138、139、445、593等）。
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	应核查配置文件或参数是否对终端接入范围进行限制。	询问系统管理员，是否对登录操作系统的终端接入方式、网络地址访问等进行限制，如： 1、开启了主机防火墙或设置TCP/IP筛选功能，并查看相关配置； 2、在网络层面设置访问控制规则进行限制；	对终端接入方式、网络地址范围进行限制。

	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	1、应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块； 2、应测试验证是否对人机接口或通信接口输入的内容进行有效性检验。	默认不适用。	默认不适用。
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	1、应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞； 2、应核查是否在经过充分测试评估后及时修补漏洞。	1、访谈安全管理员,是否定期进行操作系统漏洞扫描,发现漏洞是否经过充分测试评估后及时修补； 2、 1)控制面板系统,查看安装的SP补丁； 2)“控制面板”-“程序和功能”-“查看已安装的更新”； 3、经用户授权,使用漏洞扫描工具和渗透工具对主机进行扫描。	1、定期扫描系统漏洞,及时进行漏洞修补 2、 1)应安装SP4； 2)应安装SP4后续的hotfix； 3、无高风险漏洞。
	f)应能够测评到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	1、应访谈并核查是否有入侵测评的措施； 2、应核查在发生严重入侵事件时是否提供报警。	1、询问是否安装了主机入侵测评系统,查看是否对入侵测评系统的特征库进行定期升级； 2、查看是否在测评到严重入侵事件时提供报警。	1、安装主机入侵测评系统并配置策略,定期对主机入侵测评系统的特征库进行维护升级； 2、发生严重入侵事件时提供报警。
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	1、应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为； 2、应该检查当识别入侵和病毒行为时，是否将其有效阻断。	1、询问是否采用主动免疫可信验证技术； 2、查看是否在测评到入侵和病毒行为时提供有效阻断。	1、采用主动免疫可信验证机制； 2、对入侵和病毒行为进行有效阻断。

可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在测评到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	1、应核查是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证； 2、应核查是否在应用程序的关键执行环节进行动态可信验证； 3、应测试验证当测评到计算设备的可信性受到破坏后是否进行报警； 4、应测试验证结果是否以审计记录的形式送至安全管理中心。	1)应核查是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证； 2)应检查是否在应用程序的所有执行环节进行动态可信验； 3)应测试验证当测评到计算设备的可信性受到破坏后是否进行报警； 4)应测试验证结果是否以审计记录的形式送至安全管理中心； 5)应核查是否能够进行动态关联感知。	1、询问是否用可信验证的设备或组件对操作系统的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证； 2、查看是否也对应用程序的所有执行环节进行动态可信验 3、查看否在测评到操作系统可信性受到破坏后进行实时报警； 4、核查是否将可信性验证记录送至安全管理中心 5、查核是否进行动态关联感知。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；	1、应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了校验技术和密码技术保证完整性； 2、应测试验证在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改、是	1、应访谈安全管理员,询问主机操作系统数据在传输过程中是否有完整性保证措施,具体措施有哪些;在测评到完整性错误时是否能恢复,恢复措施有哪些; 2、应核查主机操作系统是否配备测评系统鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在传输过程中完整性受到破坏的功能;在测评到完整性错误时是否能采取必要的恢复措施。	1、主机操作系统数据在传输过程采取完整性保护措施;在测评到完整性错误时能采取必要的恢复措施; 2、采用加密算法进行完整性保护,在发现完整性被破坏时,丢弃或要求重传相应的数据,且保护措施和恢复措施有效。

		否能否测评到数据在传输过程中的完整性收到破坏并能够及时恢复。		
	b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1)应核查设计文档,是否采用了密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性； 2)应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性； 3)应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改,是否能够测评到数据在存储过程中的完整性受到破坏并能够及时恢复。	1、应访谈安全管理员,询问主机操作系统数据在存储过程中是否有完整性保证措施,具体措施有哪些;在测评到完整性错误时是否能恢复,恢复措施有哪些； 2、应核查主机操作系统是否配备测评系统括但不限于鉴别数据、重要业务数据重要审计数据、重要配置数据、重要视频数据和重要个人信息在存储过程中完整性受到破坏的功能;在测评到完整性错误时是否能采取必要的恢复措施。	1、主机操作系统数据在存储过程采取完整性保护措施;在测评到完整性错误时能采取必要的恢复措施； 2、采用加密算法进行完整性保护,在发现完整性被破坏时,丢弃或要求重置相应的数据,且保护措施和恢复措施有效。

数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	1、应核查系统设计文档，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性； 2、应通过嗅探等方式抓取传输过程中的数据包，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。	默认不适用。	默认不适用。
	b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	1、应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性； 2、应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性； 3、应测试验证是否对指定的数据进行加密处理。	1、访谈系统管理员,询问主机操作系统的鉴别数据、重要业务数据和重要个人信息等是否采用密码技术实现存储保密性； 2、查看主机操作系统的鉴别数据、重要业务数据和重要个人信息等是否采用密码技术实现存储保密性	主机操作系统的鉴别数据、重要业务数据和重要个人信息等采用密码技术实现存储保密性。

数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	1、应核查是否安装备份策略进行本地备份； 2、应核查备份策略设置是否合理、配置是否正确； 3、应核查备份结果是否与备份策略一致； 4、应核查近期恢复测试记录是否能够进行正常的数据恢复。	1、访谈系统管理员,询问是否对操作系统中的重要信息进行备份,备份策略是什么。 2、核查备份配置策略是否正确,备份结果与备份策略结果是否一致。 3、核查近期备份恢复测试记录,查看是否正常。	1、主机操作系统的重要数据定期备份或更新后即时备份； 2、正确配置数据的备份策略,备份结果与备份策略一致； 3、有定期备份恢复测试记录,且能够进行正常的数据恢复。
	b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	应核查是否提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地。	1、访谈系统管理员,询问是否对操作系统中的重要数据通过通信网络将其实时备份至备份场地； 2、核查主机操作系统重要数据的异地实时备份配置是否正确,并且查看其备份结果是否与备份策略一致。	1、操作系统中的重要数据提供异地实时数据备份功能； 2、正确配置数据的异地实时备份策略备份结果与备份策略一致。
	c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	应核查重要数据处理系统(包括边界路由器、边界防火墙、核心交换机、应用服务器和数据库服务器等)是否采用热冗余方式部署。	询问并验证服务器是否采用热冗余方式部署。	若系统实时性要求较高，建议对服务器使用热冗余方式部署。
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；	应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。	默认符合。	引用产品测试结果，信息删除后能清除。
	b)应保证存有敏感数据的存储空间被释放或重	应核查相关配置信息或系统设计文档，敏感数据所在的存	默认符合。	引用产品测试结果，信息删除后能清除。

	新分配前得到完全清除。	储空间被释放或重新分配给其他用户前是否得到完全清除。		
个人信息保护	a)应仅采集和保存业务必需的用户个人信息；	1、应核查采集的用户个人信息是否是业务应用必须的； 2、应核查是否制定了相关用户个人信息保护的管理制度和流程。		
	b)应禁止未授权访问和非法使用用户个人信息。	1、应核查是否采用技术措施限制对用户个人信息的访问和使用； 2、应核查是否制定了有关用户个人信息保护的管理制度和流程。		

5)人员访谈

与目标系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，不同等级信息系统在测评时有不同的要求，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

测评方法	人员访谈

简要描述	通过交流、讨论的方式，对技术和管理方面进行脆弱性检查和分析
达成目标	发掘技术和管理方面存在的安全问题
工作条件	1-2人工作环境，甲方人员配合
工作结果	人员访谈结果记录

人员访谈示例

表-安全运维管理作业指导书

控制点	测评项	检查内容
环境管理	a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	1、应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供配电设备、灭火设备等）进行定期维护； 2、应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员； 3、应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息； 4、应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
	b)应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；	1、应核查机房安全管理制度是否覆盖物理访问、物品进出和环境安全等方面内容； 2、应核查物理访问、物品进出和环境

		安全等相关记录是否与制度相符。
	c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	1、应核查机房安全管理制度是否明确来访人员的接待区域； 2、应核查办公桌面上等位置是否未随意放置了敏感信息的纸档文件和移动介质等。
资产管理	a)应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；	应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容。
	b)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；	1、应访谈资产管理员是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施的选取上是否不同； 2、应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求； 3、应核查资产清单中的设备是否具有相应标识，标识方法是否符合2中相关要求。

	c)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	1、应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）； 2、应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等要求。
介质管理	a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	1、应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理； 2、应核查介质管理记录是否记录介质归档、使用和定期盘点等情况。
	b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	1、应访谈资产管理员介质在物理传输过程中的人员选择、打包、交付等情况是否进行控制； 2、应核查是否对介质的归档和查询等进行登记记录。
设备维护管理	a)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	1、应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护； 2、应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。

	b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；	1、应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容； 2、应核查是否具有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。
	c)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；	1、应访谈设备管理员含有重要数据的设备带出工作环境是否加密措施； 2、应访谈设备管理员对带离机房的设备是否经过审批； 3、应核查是否具有设备带离机房或办公地点的审批记录。
	d)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。	应访谈设备管理员含有存储介质的设备在报废或重用前，是否采取措施进行完全清除或被安全覆盖。
漏洞和风险管理	a)应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	1、应核查是否有识别安全漏洞和隐患的安全报告或记录（如漏洞扫描报告、渗透测试报告和安全通报等）； 2、应核查相关记录是否对发现的漏洞及时进行修补或评估可能的影响后进行修补。

	b)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。	1、应访谈安全管理员是否定期开展安全测评； 2、应核查是否具有安全测评报告； 3、应核查是否具有安全整改应对措施文档。
网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	应核查网络和系统安全管理文档，系统管理员是否划分了不同角色，并定义各个角色的责任和权限。
	b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	1、应访谈运维负责人是否指定专门的部门或人员进行账户管理； 2、应核查相关审批记录或流程是否对申请账单、建立账户、删除账户等进行控制。
	c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略、账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、授权访问最小服务、升级与打补丁、审计日志管理、登录设备和系统的口令更新周期等方面。
	d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	应核查重要设备或系统（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作

		步骤、参数配置等内容。
	e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；	应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。
	f)应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；	1、应访谈网络和系统相关人员是否指定专门部门或人员对日志、监测和报警数据等进行分析统计； 2、应核查是否具有对日志、监测和报警数据等进行分析统计的报告。
	g)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；	1、应访谈网络和系统相关人员调整配置参数结束后是否同步更新配置信息库，并核实配置信息库是否为最新版本； 2、应核查是否具有变更运维的审批记录，如系统连接、安装系统组件或调整配置参数等活动； 3、应核查是否具有变更运维的操作过程记录。

	h)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；	1、应访谈系统相关人员使用运维工具结束后是否删除工具中的敏感数据； 2、应核查是否具有运维工具接入系统的审批记录； 3、应核查运维工具的审计日志记录，审计日志是否不可以更改。
	i)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；	1、应访谈系统相关人员日常运维过程中是否存在远程运维，若存在，远程运维结束后是否立即关闭了接口或通道； 2、应核查开通远程运维的审批记录； 3、应核查针对远程运维的审计日志是否不可以更改。
	j)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。	1、应访谈系统相关人员往来外联连接（如互联网、合作伙伴企业网、上级部门网络等）是否都得到授权与批准； 2、应访谈网络管理员是否定期核查违规联网行为； 3、应核查是否具有外联授权的记录文件。
恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	1、应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识； 2、应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系

		统前进行恶意代码检查。
	b)应定期验证防范恶意代码攻击的技术措施的有效性。	1、若采用可信验证技术，应访谈安全管理员是否未发生过恶意代码攻击事件； 2、若采用防恶意代码产品，应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否未出现过大规模的病毒事件； 3、应核查是否具有恶意代码测评记录、恶意代码库升级记录和分析报告。
配置管理	a)应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；	应访谈系统管理员是否对基本配置信息进行记录和保存。
	b)应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。	1、应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库； 2、应核查配置信息的变更流程是否具有相应的申报审批程序。

密码管理	a)应遵循密码相关国家标准和行业标准；	应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求。
	b)应使用国家密码管理主管部门认证核准的密码技术和产品。	应核查相关产品是否获得有效的国家密码管理主管部门规定的测评报告或密码产品型号证书。
变更管理	a)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；	1、应核查变更方案是否包含变更类型、变更原因、变更过程、变更前评估等内容； 2、应核查是否具有变更方案评审记录和变更过程记录文档。
	b)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；	1、应核查变更控制的申报、审批程序其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容； 2、应核查是否具有变更实施过程的记录文档。
	c)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	1、应访谈运维负责人变更中止或变更失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练； 2、应核查是否具有变更恢复演练记录； 3、应核查变更恢复程序是否规定变更中止或失败后的恢复流程。

备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；	1、应访谈系统管理员有哪些需要定期备份的业务信息、系统数据及软件系统； 2、应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
	b)应规定备份信息的备份方式、备份频度、存储介质、保存期等；	应核查备份与恢复管理制度是否明确备份方式、频度、介质、保质期等内容。
	c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	应核查备份和恢复的策略文档是否根据数据的重要程度制定相应备份恢复策略和程序等。
安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件；	1、应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； 2、应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。
	b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	应核查安全事件报告和处理管理制度是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和响应流程等。

	c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；	应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过程、经验教训、补救措施等内容。
	d)对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。	1、应访谈运维负责人不同安全事件的报告流程； 2、应核查对重大安全事件是否制定不同安全事件报告和处理流程，是否明确具体报告方式、报告内容、报告人等方面内容。
应急预案管理	a)应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；	应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面。
	b)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	应核查是否具有重要事件的应急预案（如针对机房、系统、网络等各方面）。
	c)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；	1、应访谈运维负责人是否定期对相关人员进行应急预案培训和演练； 2、应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等； 3、应核查应急预案记录是否记录演练时间、主要操作内容、演练结果等。

	d)应定期对原有的应急预案重新评估，修订完善。	应核查应急预案修订记录是否定期评估并修订完善等。
外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定；	1、应访谈运维负责人是否有外包运维服务情况； 2、应访谈运维负责人外包运维服务单位是否符合国家相关规定。
	b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；	应核查外部运维服务协议是否明确约定外包运维的范围和工作内容。
	c)应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；	应核查与外部运维服务商签订的协议中是否明确其具有等级保护要求的服务能力。
	d)应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。	应核查外包运维服务协议是否包含可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等内容。

6)文档审查

检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方

案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档）的完整性，以及这些文件之间的内部一致性。

测评方法	文档审查
简要描述	通过文档审核与分析，检查制度、策略、操作规程、制度执行情况记录的完整性和内部一致性
达成目标	发掘技术和管理方面存在的安全问题
工作条件	1-2人工作环境，甲方人员、各类文档资料配合
工作结果	文档审查结果记录

文档审查示例

表-安全管理制度

控制点	测评项	检查内容
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	应核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略。
管理制度	a)应对安全管理活动中的各类管理内容建立安全管理制度；	应核实各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容。
	b)应对管理人员或操作人员执行的日常管理操作建立操作规程；	应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等。
	c)应形成由安全策略、管理制	应核查总体方针策略文件、管理制度和

	度、操作规程、记录表单等构成的全面的安全管理制度体系。	操作规程、记录表单是否全面且具有关联性和一致性。
制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定；	应核查是否由专门的部门或人员负责制定安全管理制度。
	b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。	1）应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容； 2）应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等。
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	1）应访谈信息/网络安全主管是否定期对安全管理制度的合理性和适用性进行审定； 2）应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。

7)实地查看

通过实地观察人员行为、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，测评其是否达到了相应等级的安全要求。

项目名称	实地查看
简要描述	通过现场查看人员行为、技术设施和物理环境状况，检查人员的安全意识、

	业务操作、管理程序和系统物理环境等方面的安全情况。
达成目标	发掘技术和管理方面存在的安全问题
工作条件	1-2人工作环境，甲方人员
工作结果	实地查看结果记录

实地查看示例

表-安全物理环境

控制点	测评项	检查内容	检查方法	推荐值
物理位置选择	a)机房场地应选择在具有防震、防风和防雨等能力的建筑内；	1、应核查所在建筑物是否有建筑抗震设防审批文档； 2、应核查机房是否不存在雨水渗漏； 3、应核查门窗是否不存在因风导致的尘土严重； 4、应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。	访谈、检查	1、有机房的设计/验收文档,包含对机房场地所在建筑具有防震、防风和防雨能力的说明； 2、未发现机房屋顶、商户等存在雨水渗漏情况； 3、未发现门存在因风导致的尘土严重； 4、未发现屋顶、墙体、门窗和地面等存在破损开裂情况。
	b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	应核查机房是否不位于所在建筑的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施。	访谈、检查	机房未设在所在建筑物的顶层或地下室,或机房采取了防水和防潮措施。
物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	1、应核查出入口是否配置电子门禁系统； 2、应核查电子门禁系统是否可以鉴别、记录进入的人员信息。	检查	1)机房出入口配置了电子门禁系统； 2)电子门禁系统可以鉴别别、记录进入的人员信息。

防盗窃和防破坏	a)应将设备或主要部件进行固定，并设置明显的不易除去的标识；	1、应核查机房内设备或主要部件是否固定； 2、应核查机房内设备或主要部件上是否设置了明显且不易除去的标识。	核查	1)机房内设备或主要部件都固定； 2)机房内设备或主要部件上设置了明显且不易除去的标识。
	b)应将通信线缆铺设在隐蔽安全处；	应核查机房内通信线缆是否铺设在隐蔽安全处，如桥架中等。	核查	机房内通信线铺设在隐蔽安全处,如桥架中等。
	c)应设置机房防盗报警系统或设置有专人值守的视频监控系统。	1、应核查机房内是否配置防盗报警系统或专人值守的视频监控系统； 2、应核查防盗报警系统或视频监控系统是否启用。	核查	1)机房内配置防盗报系统或有专人值守的视频监控系统； 2)启用了防盗极系统或视频监控系统。
防雷击	a)应将各类机柜、设施和设备等通过接地系统安全接地；	应核查机房内机柜、设施和设备等是否进行接地处理。	核查	机房内机柜、设施和设备等进行了接地处理。
	b)应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。	1、应核查机房内是否设置防感应雷措施； 2、应核查防雷装置是否通过验收或国家相关部门的技术测评。	核查	1)机房内设置防感应雷措施,例如防雷保安器或过压保护装置等； 2)防雷装置通过验收或国家有关部门的技术测评。
防火	a)机房应设置火灾自动消防系统，能够自动测评火情、自动报警，并自动灭火；	1、应核查机房内是否设置火灾自动消防系统； 2、应核查火灾自动消防系统定期检查或保养记录，确认其是否正常工作，是否可以自动测评火情、自动报警并自灭。	核查	1)机房内设置了火灾自动消防系统； 2)火灾自动消防系统有定期检查或保养,确保其在发牛火情后可以自动测评火情、自动报警并自动灭火

	b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；	应核查机房验收文档是否明确相关建筑材料的耐火等级。	访谈、核查	机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料。
	c)应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。	1、应访谈机房管理员是否进行了区域划分； 2、应核查各区域间是否采取了防火措施进行隔离。	访谈、核查	1)机房进行了区域划分,如主机区、网络区、监控区等； 2)各区城间采取了防火措施进行隔离。
防水和防潮	a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施。	访谈、核查	机房的窗户、屋顶和墙壁是否采取了防雨水渗透的措施,且未出现过漏水、渗透和返潮现象。
	b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；	1、应核查机房内是否采取了防止水蒸气结露的措施； 2、应核查机房内是否采取了排泄地下积水，防止地下积水渗透的措施。	访谈、核查	1)机房内采取了防止水蒸气结露的措施,如具有精密控制湿度的空调、除湿器等； 2)机房内采取了排泄地下积水,防止地下积水渗透的措施,如空调、除湿等设备周围设挡水和排水设施。
	c)应安装对水敏感的测评仪表或元件，对机房进行防水测评和报警。	1、应核查机房内是否安装了对水敏感的检查装置； 2、应核查防水测评和报警装置是否启用。	访谈、核查	1)机房内安装了对水敏感的测评装置,如漏水测评绳等； 2)启用了防水测评和报警装置。
防静电	a)应采用防静电地板或地面并采用必要的接地防静电措施；	1、应核查机房内是否安装了防静电地板或地面； 2、应核查机房内是否采用了防静电措施。	访谈、核查	1)机房内安装了防静电地板或地面； 2)机房内采用了接地防静电措施。

	b)应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。	应核查机房内是否配备了防静电设备。	访谈、核查	机房内配备了防静电设备,例如采用静电消除器、佩防静电手环等。
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	1、应核查机房内是否配备了专业空调； 2、应核查机房内温湿度是否在设备运行所允许的范围内之内。	核查	1)机房是否配备了专用精密空调； 2)精密空调设置的温湿度在机房内设备运行所允许的范围之内。
电力供应	a)应在机房供电线路上配置稳压器和过电压防护设备；	应核查供电线路上是否配置了稳压器和过电压防护设备。	核查	机房供电线路上配置了稳压器和过压防护设备。
	b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；	1、应核查是否配备UPS等后备电源系统； 2、应核查UPS等后备电源系统是否满足设备在断电情况下的正常运行要求。	访谈、核查	1)机房配备了UPS等后备电源系统,且有定期保养记录； 2)UPS等后备电源系统满足设备在断电情况下的正常运行要求,即UPS容量能确保机房设备一段时间的正常运行。
	c)应设置冗余或并行的电力电缆线路为计算机系统供电。	1、应访谈机房管理员机房供电是否来自两个变电站； 2、应核查机房内是否设置了冗余或并行的电力电缆线路为计算机系统供电。	访谈、核查	1)机房供电来自两个不同的变电站； 2)机房内设置了冗余或并行的电力电缆线路为计算机系统供电。

电磁防护	a)电源线和通信线缆应隔离铺设，避免互相干扰；	应核查机房内电源线缆和通信线缆是否隔离铺设。	核查	机房内电源线缆和通信线缆隔离铺设。
	b)应对关键设备实施电磁屏蔽。	应核查机房内是否为关键设备配备了电磁屏蔽装置。	访谈、核查	机房内为关键设备配备了电磁屏蔽装置，如屏蔽机房、机柜等。

（3）测评工具及测试接入点

我方在等级保护测评过程中使用的测评工具严格遵循可控性原则，即所有使用的测评工具将事先提交给甲方检查确认，确保在双方认可的范围之内，而且测评过程中采用的技术手段确保已经过可靠的实际应用。

测试工具接入点选取原则：

1、由低级别系统向高级别系统探测；

2、同一系统同等重要程度功能区域之间要相互探测；

3、由较低重要程度区域向较高重要程度区域探测；

4、由外联接口向系统内部探测；

5、跨网络隔离设备（包括网络设备和安全设备）要分段探测。

根据测试工具接入点选取原则，并结合对甲方的业务承载数据、网络区域的划分来选择本次测试工具安全接入点。每个测试接入点需要提供一个网络可达的 IP 地址及一个可接入网络的网口，以便我方测评人员进行相关测试工作。

4.出具公安部门认可的信息系统安全等级测评报告

本阶段的工作内容主要是对前期现场测评的结果数据进行汇总整理，识别系统中所存在的风险并对高风险进行重点分析，并出具公

安部门认可的信息系统安全等级测评报告。具体的内容包括:

（1）单项测评结果分析

本任务主要是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，单项测评结果是形成等级测评结论的基础。

输入：经过测评委托单位确认的测评证据和证据源记录，测评指导书。

任务描述:

a）针对每个测评项，分析该测评项所对抗的威胁在被测信息系统中是否存在，如果不存在，则该测评项应标为不适用项。

b）分析单个测评项是否有多方面的要求内容，针对每一方面的要求内容，从一个或多个测评证据中选择出“优势证据”，并将“优势证据”与要求内容的预期测评结果相比较。

c）如果测评证据表明所有要求内容与预期测评结果一致，则判定该测评项的单项测评结果为符合；如果测评证据表明所有要求内容与预期测评结果不一致，判定该测评项的单项测评结果为不符合；否则判定该测评项的单项测评结果为部分符合。

根据“优势证据”的定义，具体从测评方式上来看，针对物理安全测评，实地察看证据相比文档审查证据为优势证据，文档审查证据相比访谈证据为优势证据；针对技术安全的其他方面测评，配置检查证据相比访谈证据为优势证据；针对管理安全测评，优势证据不确定，需根据实际情况分析确定优势证据。

输出/产品：测评报告的单元测评的结果记录部分。

（2）单元测评结果判定

本任务主要是将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。

输入：测评报告的单元测评的结果记录部分。

任务描述：

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。

（3）风险分析

测评人员依据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测信息系统安全造成的影响。

输入：填好的调查表格，测评报告的单元测评的结果汇总部分和问题分析部分，测评报告的整体测评部分、测评结果汇总部分。

任务描述：

a）判断整体测评后的单元测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。

b）判断整体测评后的单元测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用后，对被测信息系统的业务信息安全和系统服务安全造成的影响程度，影响程度取值范围为高、中和低。

c）综合a）和b）的结果，对被测信息系统面临的安全风险进行赋值，风险值的取值范围为高、中和低。

d)结合被测信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合

法权益造成的风险。

输出：测评报告的风险分析和评价部分。

（4）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。

输入：测评报告的单元测评的结果记录部分、结果汇总部分和问题分析部分。

任务描述：

a）针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他测评项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，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。

b）针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他层面的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，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。

c）针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他区域的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，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。

d）根据上述 3 方面的整体测评分析情况，调整单元测评结果，

并将调整后的单元测评结果再次汇总，统计符合情况。一般以表格的形式描述。

e) 验证测试结果分析，包括漏洞扫描，渗透测试等。若由于用户原因无法开展验证测试，应将用户签章的“自愿放弃验证测试声明”作为报告附件。

（5）等级测评结论形成

测评人员在整体测评后的单元测评结果汇总、风险分析和评价的基础上，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。

输入：测评报告的测评结果汇总部分，测评报告的风险分析和评价部分。

任务描述：

等级测评结论应表述为“优”、“良”、“中”、“差”。

（6）测评报告编制

测评报告编制测评报告应包括以下内容：测评项目概述、被测信息系统情况、等级测评范围与方法、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、安全建设整改建议等。

其中，测评项目概述部分描述本次测评的测评目的、依据及测评过程等；被测信息系统情况、等级测评范围与方法等部分内容编制时参考测评方案相关部分内容。

输入：测评方案，《信息系统安全等级测评报告模版》，测评报告的单元测评的结果记录部分、结果汇总和问题分析部分、测评结果汇总部分、整体测评部分、风险分析和评价部分、等级测评结论部分。

任务描述：

a）测评人员整理前面几项任务的输出/产品，按照《信息系统安全等级测评报告模版》编制测评报告相应部分。每个被测信息系统应单独出具测评报告。

b）针对被测信息系统存在的安全隐患，从系统安全角度提出相应的改进建议，编制测评报告的安全建设整改建议部分。

c）列表给出现场测评的文档清单和单项测评记录，以及对各个测评项的单项测评结果判定情况，编制测评报告的单元测评的结果记录和问题分析部分。

d）测评报告编制完成后，测评机构应根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息，对测评报告进行评审。

e）评审通过后，由项目负责人签字确认并提交给测评委托单位。

七、服务保障措施

（一）进度保障措施

我中心充分理解甲方的项目需求，对甲方的安全现状有着初步的认识和了解，并与甲方就如何保证项目进度开展深入的探讨。为保障45个信息系统的所有测评工作在服务期内按时完成，并提供高质量的项目交付物成果，我中心采取以下方法以保证整个项目进度：

项目管理方法：项目的管理将依据PMI项目管理方法、我中心服务规范进行管理，除了项目组外，我中心专门成立高层项目管理委员会保障项目的沟通管理，达到项目过程的可控。

项目经理配备：我中心委派的项目经理1名，具备多个大型信息等级保护测评项目的成功案例，全程负责项目的管理、技术质量管控。项目经理具有由公安部信息安全等级保护评估中心颁发的信息安全

等级测评师证书。

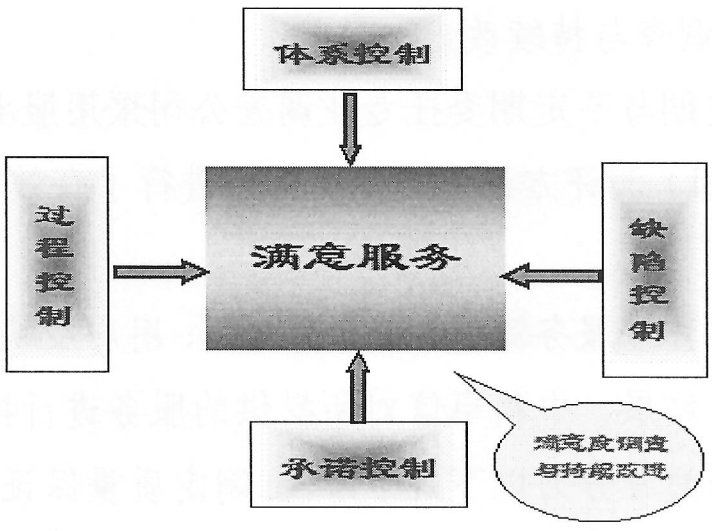
实施人员配备：我中心为本项目配备了能胜任的、足够的实施人员，并且保证在项目实施期间专人专用，在没有得到甲方的允许下绝不更换人员，以确保项目的连续性和可控性。实施人员具有由公安部信息安全等级保护评估中心颁发的信息安全等级测评师初级证书。

技术工具配备：我中心依据甲方的需要和要求，已经配备了符合要求的、足够的等级保护测评工具，并保证在项目实施期间工具专用，以确保项目的连续性和可控性。

（二）质量保证措施

1.质量保障控制体系

为确保整个工程的质量合乎建设要求，在整个项目测试的过程中，需要建立一套科学合理，行之有效的项目质量保证体系。我中心将充分根据建设需求和领导要求，依据 ISO9001-2008 标准，结合中心全面质量管理体系中的各类程序文件以及有关的技术规范，实施全过程的质量管理。



中科卓信软件测评技术中心质量体系

（1）承诺控制

以承诺方式使企业内部管理增加压力，实行自我控制；

向用户承诺的开通时限及服务时限，向用户承诺服务中的标准和规范，只要承诺的，就必须保证服务的兑现。

（2）过程控制

企业内部各个环节提供的工序控制；

内部质量检查控制；

内部工序之间评价控制；

实施流程重组与优化。

（3）体系控制

制定一系列适合企业发展的服务质量指标体系；

加强企业内部服务质量信息反馈体系，发现问题快速传递立即处理；

质量监督体系，实行不定期的明查暗访及内部监督检查；

考核评价体系，质量考核和用户满意度评价及内部客户评价。

（4）满意度调查与持续改进

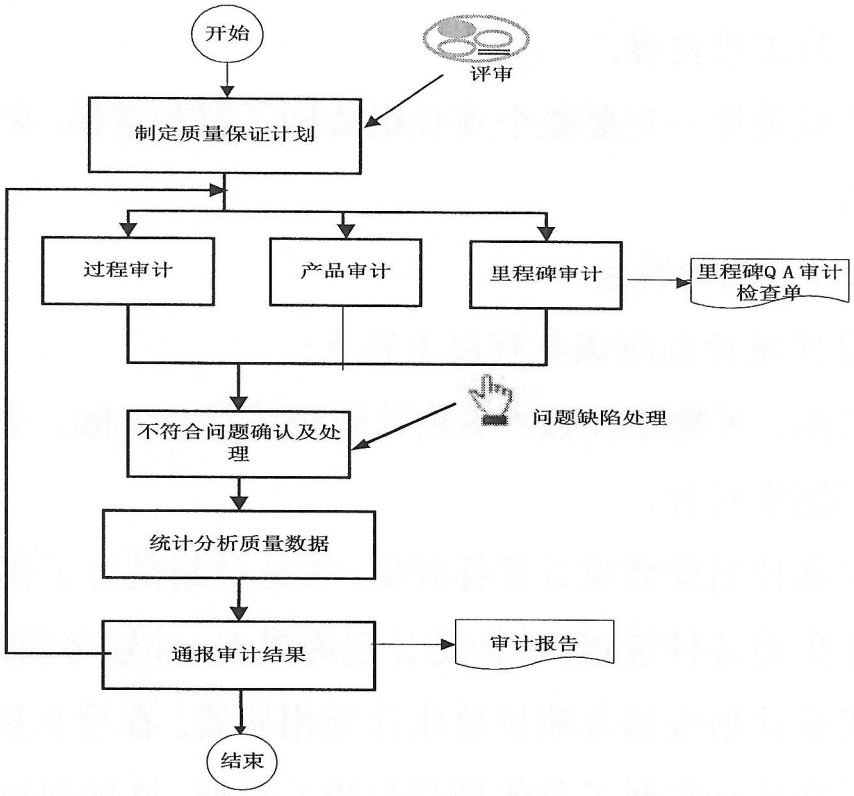
我中心定期与不定期委托专业调查公司采用服务质量用户满意度指数（TCSI）测评方法，对主要客户进行了有效电话访问，进行满意度调查；

根据工作环节服务测评、满意度测评、用户反映的服务问题等做出的最终调查结果，中科卓信对所提供的服务进行持续改进。

质量保证过程分为以下几个阶段：制定质量保证计划；过程审计；产品审计；里程碑审计；不符合问题确认及处理；统计分析度量数据；

通报审计结果。

其过程流程图如下所示:



2.质量管理措施

（1）项目控制

项目实施计划是对项目实施过程的设计和规划,是项目实施阶段的重要环节。

整个测试工作计划在开发项目启动以后开始,直到项目验收结束,项目周期将根据实际项目进度灵活调整。

（2）进度控制

在进度控制与计划控制方面，要注意以下几点:

1) 一定要建立正确的项目实施流程。工程实施流程的确立，明确了工程实施各步骤的顺序。

2) 计划管理。凡事预则立，不预则废。

3) 测试中影响进度的因素较多，要求计划不能一成不变，要不断

随具体情况调整。

4) 因为系统集成一般需要多种学科的配合，可能各人不了解其它人的工作内容。

5) 工程进度一定要整个项目组共同了解和掌握，要求作到步调一致。

（3）项目计划的特点

项目实施计划应该具有以下特点：

1) 具体、可操作性强。实施计划应该符合实际，全面、周到，做到切实可行。

2) 实施计划受到项目目标控制。实施计划是为了实现项目目标而作出的各种策划，目标是计划的灵魂，计划必须符合项目目标。

3) 实施计划应该与项目总体计划相协调。在项目规划阶段，围绕各项目标编制了总体规划和相关计划，这种规划和计划是纲要性的、指导性的，实施计划应该在总体规划和计划的指导下编制，以便与之相适应、相协调。

4) 计划的弹性。计划在实施过程中受到许多因素的干扰，实施计划需要根据条件的变化不断修改或调整。因此，在编制或者修改调整实施计划的过程中，应考虑弹性要求，留有余地。

5) 实施计划的编制贯穿项目实施全过程。项目实施中随着情况的不断变化，每一阶段都应研究、编制、修改、调整计划，同时也要采用滚动的方法详细安排近期计划。所以，项目实施计划是一个持续的、循环的、渐进的过程。

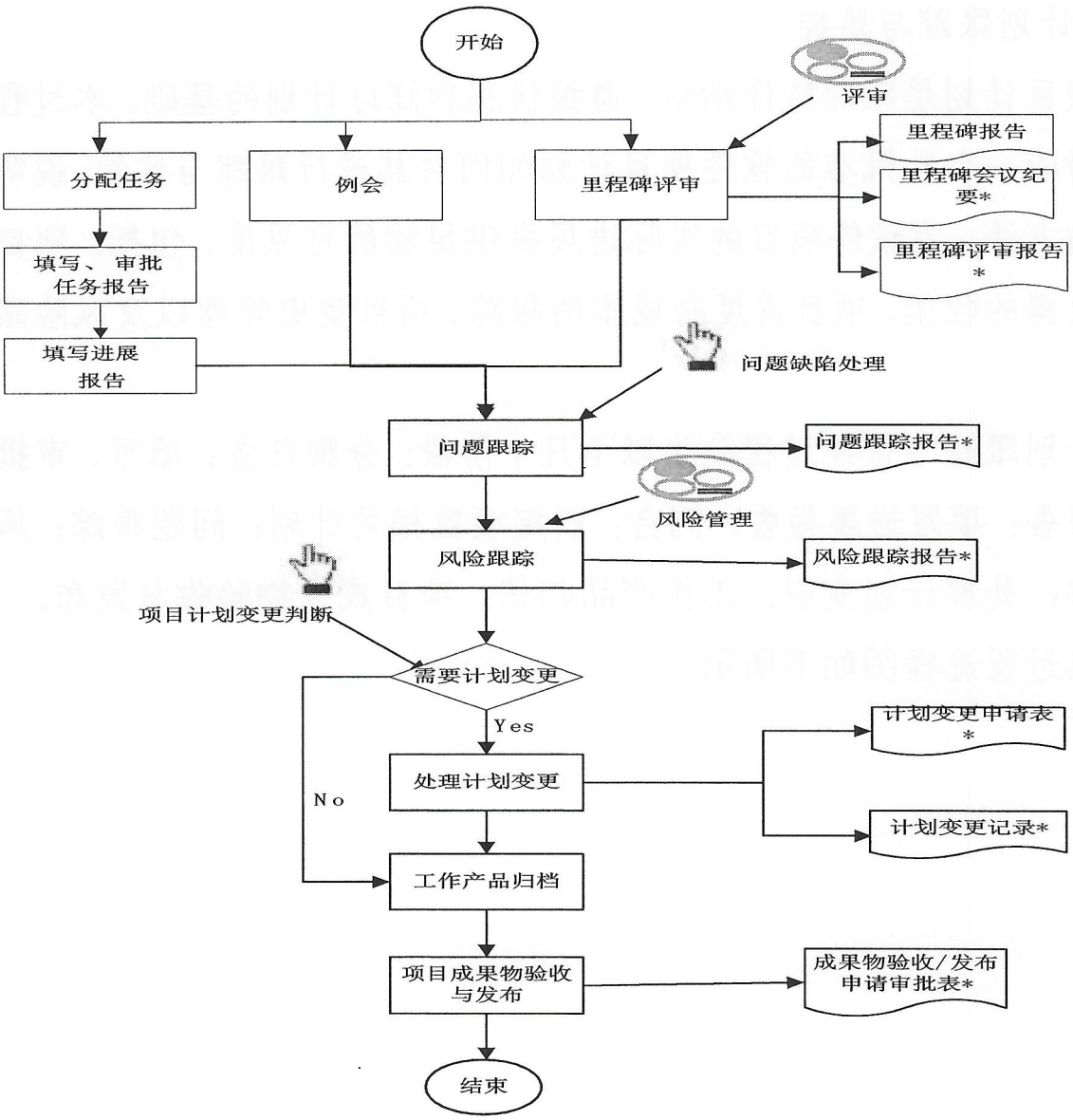
6) 不同项目及不同项目参加者所应编制的计划的内容和范围不同，一般应按任务书或者合同规定的工作范围、工作责任确定。

（4）计划跟踪与监控

项目计划是跟踪软件活动、通报状态和修订计划的基础。本过程指导对应一个已批准的软件项目计划如何对其进行跟踪与监控，说明具体的方法，为软件项目的实际进展提供足够的可见度。包括：项目过程数据的收集、项目进度和成本的跟踪、项目变更管理以及风险跟踪等。

计划跟踪与监控过程分为以下几个阶段：分配任务；填写、审批任务报告；填写进展报告；例会；制定项目相关计划；问题跟踪；风险跟踪；处理计划变更；工作产品归档；项目成果物验收与发布。

其过程流程图如下所示：

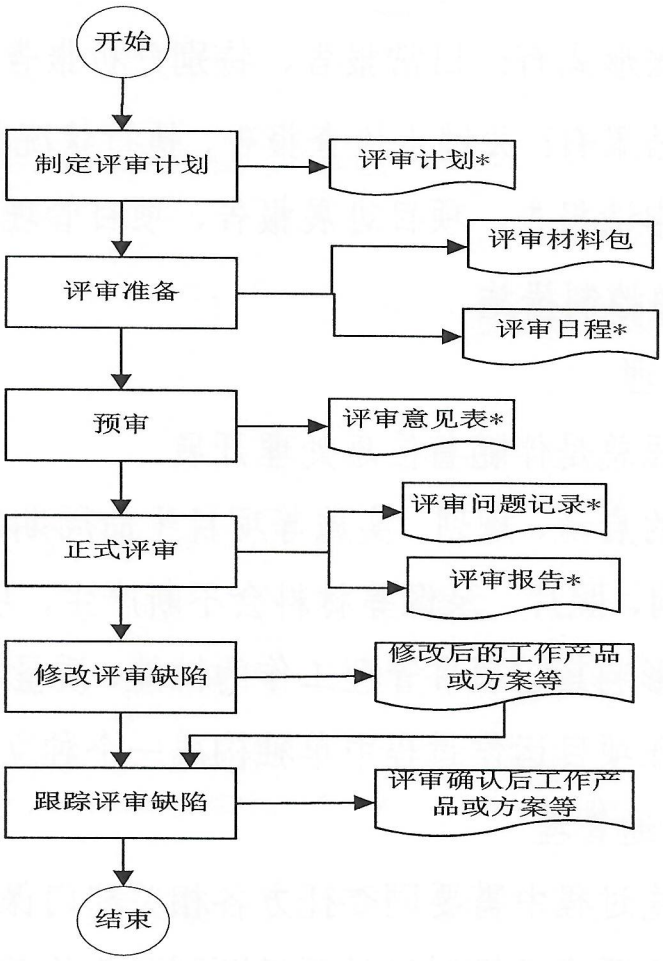


（5）评审

评审的目的是由一组有资格的人员对软件测试各阶段的活动和测试工作产品进行评价，以判断测试活动输出是否符合预期的目标，同时通过评审标识出与规格和标准的偏差。它向相关人员和部门提供充足的证据以证明：测试活动是规范和有效的，测试结果是可靠和真实的。

评审过程分为以下几个阶段：制定评审计划；评审准备；预审；正式评审；修改评审缺陷；跟踪评审缺陷。

其过程流程图如下所示:



3.项目进展控制措施

项目进展报告和阶段报告是项目实施控制的基础。反映了项目当前在进度、费用、质量等方方面面的实际执行情况。在本节对实施各环节产生的主要进展报告做整理。

在全部报告期间，需要收集两种数据和信息:

实际执行的数据，包括活动开始和结束时间；使用或投入的实际资源和成本等；

有关项目范围、进度计划和预算变更的信息。

进展报告的内容包括:

项目进展简介、困难与应对

进展报告一般形式有：日常报告、特别分析报告

进展报告的结果有：关键点检查报告、执行状况报告、任务完成报告、项目变更申请报告、项目进展报告、项目管理报告。

4.信息与沟通控制措施

（1）信息管理

项目管理过程总是伴随着信息处理开展。

随着本项目的启动、规划、实施等项目生命周期的展开，项目的文件、报告、合同、照片、录像等材料会不断产生，项目信息管理的性能和成本直接影响其它项目管理工作的性能、质量和成本，项目信息管理系统必须在项目运作过程中单独构成一个独立的管理环节。

（2）协调沟通管理

本项目在实施过程中需要同委托方各相关部门保持密切的沟通与协调，良好的协调沟通机制将是项目顺利实施的前提。

为保证项目的顺利实施，管理规范和标准、安排工作计划、协调相关资源、解决工作中出现的问题，有效的沟通管理是项目成功的关键。

（3）项目经理

能够使小组每个成员都能发挥能力；

有一定的组织能力；

能够使小组每位成员有成就感；

有提出解决问题方的能力；

对问题的理解有一定的深度；

要能让成员知道软件质量的重要性

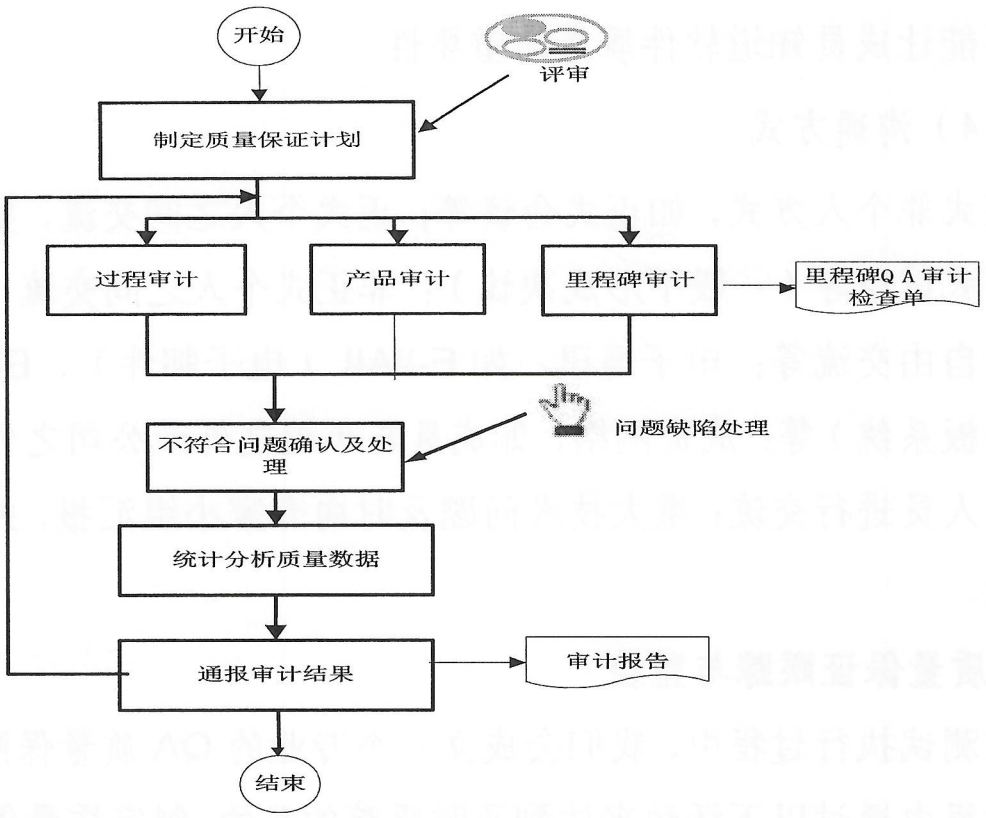
（4）沟通方式

正式非个人方式，如正式会议等；正式个人之间交流，如成员之间的正式讨论等（一般不形成决议）；非正式个人之间交流，如个人之间的自由交流等；电子通讯，如 E-MAIL（电子邮件）、BBS（电子公告板系统）等；成员网络，如成员与小组之外或公司之外有经验的相关人员进行交流；重大技术问题及时向专家小组汇报，并请求技术支援。

5.质量保证跟踪与监控

在测试执行过程中，我们会成立一个专业的 QA 质量保障组，在实施过程中通过以下活动来达到及时跟踪的目的：制定质量保证计划；过程审计；产品审计；里程碑审计；缺陷的确认及处理；统计分析度量数据；通报审计结果。

其过程流程图如下所示：



（1）关键节点/里程碑跟踪与监控

在测试执行过程中，我们会制定整体进度计划、制定准则规范、定期进行过程审核、进行产品审核并定期向监理或用户通报审核情况。详细情况如下：

制定《质量保证计划》：根据进度计划，在项目策划初期，制定质量保证计划，按照该计划实施质量管理工作，对质量保证计划进行配置管理；制定准则规范：与项目经理一起确定项目的过程、产品需遵循的标准、规程、准则、规范。定期进行过程审核：质量保证人员按照既定的标准和规程，每周审核工程活动，验证其符合性，并处理发现的偏离直至问题关闭，审核的结果将记录在《过程审核记录》中；进行产品审核：质量保证人员在《质量保证计划》中规定的结点，对工作产品进行审核，验证其与准则规范的符合性，并处理发现的偏离直至问题关闭，审核的结果将记录在《产品审核记录》中；定期向监理、用户通过审核情况：质量保证人员在用户参与评审活动的节点处，

汇总以往阶段审核的结果，向用户通报审核结果。

（2）关键文档质量控制

通过交叉审查的方式，确认用户文档覆盖需求功能，确认用户文档以产品说明等文档性材料符合项目组要求。

（3）测试暂停和再启动判断

测试暂停标准：

测试环境发生变化（场地、网络、硬件、软件等），又处于不可使用状态；被测样品有大量错误或严重错误，无法继续测试或继续测试无任何意义；被测样品存在主要功能项的缺失，无法满足需求标准或验收标准；被测样品版本在不受控的情况下发生了变化。

测试再启动标准：

严重错误得到修改后，需要重新启动测试；开发组提供错误修改后的安装程序以及再启动测试的相关说明；测试组安装修改后的程序。如有必要，需要重新初始化测试数据，重新执行测试规程，恢复到发生错误前的状态。

（4）测试退出判定

当被测样品满足下列条件时，测试可以退出：

根据测试结果判定准则，从测试角度，被测样品达到运行标准；根据测试结果判定准则，从测试角度，被测样品不符合验收标准；

测试活动暂停，被测样品被退回，并无新样品提交测试。

（5）信息与沟通控制措施

为保证项目的顺利实施，在实施过程中需要各相关部门保持密切的沟通与协调，共同管理规范和标准、安排工作计划、协调相关资源、解决工作中出现的问题。

沟通方式

1)正式非个人方式，如正式会议等；

2)正式个人之间交流，如成员之间的正式讨论等（一般不形成决议）；

3)非正式个人之间交流，如个人之间的自由交流等；

4)电子通讯，如 E-MAIL（电子邮件）、BBS（电子公告板系统）等；

5)成员网络，如成员与小组之外或公司之外有经验的相关人员进行交流；

6)重大技术问题及时向专家小组汇报，并请求技术支援。

（三）保密措施

1.保密责任

我中心承诺遵守保密协议，并对其员工、代理商或关联方的保密责任进行约束。建立相应的内部流程和控制措施，以防止敏感信息泄露。

2.数据保护

我中心承诺采取适当的技术和组织措施，保护采购方系统中存储的敏感信息和数据隐私。确保进行访问控制等操作，以防止未经授权的访问和意外数据损失。

3.信息共享与披露

我中心承诺在未获得中心明确许可的情况下，不得将采购方的机密信息和数据转让给第三方。如果在履行合同过程中需要共享相关信息，要求我中心采取必要的保护措施，并仅限于合同目的使用。

4.终止后的数据处理

我中心承诺在合同终止或服务终止后，按照中心的要求进行数据清除、销毁或返还，并确保不再使用或披露中心的敏感信息。

5.离场安全保密管理

现场测评离场时，如果笔记本电脑为甲方提供，则笔记本电脑须交回甲方。同时由甲方有关人员检查所有的存储介质是否存储非测评需要的电子文档。

八、测评计划

我方将在本年度2024年12月25日前完成不少于15个三级系统的复测工作全周期，并最终出具等保测评报告（各实施内容存在并行阶段）。

任务	服务周期	阶段交付物
安全现状分析与调研	2024年12月25日前	➢《信息系统等级保护差距分析报告》 ➢《信息系统等级保护整改建议》 ➢《信息系统安全等级测评报告》
等级保护差距分析		
形成整改建议、安全整改监督及安全实施		
等级保护测评服务（含报告编制）		

9个月内完成不少于23个二级系统和2个三级系统等级保护复测工作，并最终出具等保测评报告（各实施内容存在并行阶段）。

任务	项目周期	阶段交付物
安全现状分析与调研	9个月内	➢《信息系统等级保护差距分析报告》 ➢《信息系统等级保护整改建议》
等级保护差距分析		
形成整改建议书、安全整改监督及安全实施		

等级保护测评服务（含报告编制）		➢《信息系统安全等级测评报告》

6个月内完成新建系统的定级备案工作，9个月内完成不少于5个新建信息系统等保测评工作，并最终出具等保测评报告（各实施内容存在并行阶段）。

任务	项目周期	阶段交付物
安全现状分析与调研	6个月内完成定级备案，9个月内出具等保测评报告	➢《信息系统安全等级保护定级报告》 ➢《信息系统安全等级保护备案表》 ➢《备案证明》 ➢《信息系统等级保护差距分析报告》 ➢《信息系统等级保护整改建议》 ➢《信息系统安全等级测评报告》
定级备案工作		
等级保护差距分析		
形成整改建议书、安全整改监督及安全实施		
等级保护测评服务（含报告编制）		

附件二

项目分项报价

序号	系统类型	服务内容	数量	单价（元）	总价（元）
1	等级保护测评（三级系统）	对17个已备案三级等保进行复测，具体工作为：安全现状分析与调研、等级保护差距分析、形成整改建议书、安全整改监督及安全实施等级保护测评服务(含报告编制）	17	50000	850000
2	等级保护测评（二级系统）	对23个已备案二级等保进行复测，具体工作为：安全现状分析与调研、等级保护差距分析、形成整改建议书、安全整改监督及安全实施等级保护测评服务(含报告编制）	23	36500	839500
3	新信息系统等级保	对5个新建系统 进行定级备案、安全现状分析与调	5	48100	240500

	护测评	研、等级保护差距分析、形成整改建议书、安全整改监督及安全实施等级保护测评服务（含报告编制）			
4	合计	（含税）			1930000

附件三

项目主要人员组成

序号	姓名	性别	年龄	拟任岗位	联系方式	承担主要的工作
1	程超	男	39	项目负责人	15901412185	负责项目的组织与协调；负责解决项目实施过程中的问题；负责与各方的沟通与确认
2	胡陈勇	男	45	技术支持	18611989800	负责提供技术咨询、支持； 安全设计咨询 定级备案咨询
3	李远金	男	37	测评工程师	15712965895	系统调查；项目计划编制；协调并实施项目计划中确定的活动
4	卢海龙	男	29	测评工程师	18610103463	负责网络、渗透测评
5	蒋再春	男	35	测评工程师	13718494481	负责主机测评
6	孙士杰	女	25	测评工程师	15894883623	负责管理测评
7	高昭	男	27	测评工程师	18210695905	负责主机测评
8	高利文	男	43	测评工程师	13520719629	负责管理测评
9	齐永利	男	36	测评工程师	15010155662	负责主机测评
10	张劲松	男	44	测评工程师	13124769976	负责主机测评
11	叶展	男	27	测评工程师	15869416006	负责管理测评
12	谷刘峰	男	26	测评工程师	15034398893	负责定级、管理
13	刘志恒	男	24	测评工程师	18330838115	负责主机测评

14	李晶	女	51	测评工程师	18710178180	负责管理、网络测评
15	付博雯	女	30	测评工程师	13100962679	负责网络、渗透测评
16	谭天姿	女	24	测评工程师	18710178180	负责主机测评
17	崔嘉	男	36	测评工程师	13601089510	负责网络、渗透测评
18	韩阳阳	女	33	测评工程师	13671355958	负责管理测评
19	张玉荣	男	60	质控经理	13381116683	负责质量管理