# 分项报价表

项目编号：ZFCG-T2018074号

项目名称：许昌市审计局“信息系统安全等级测评”项目

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 系统名称 | 单位 | 数量 | 总价 |
| 1 | 审计管理系统（三级） | 次 | 1 | 152500元 |
| 2 | 地税联网审计系统（三级） | 次 | 1 | 152500元 |
| 合计 | 大写：叁拾万伍仟元整  小写：305000元 | | | |

供应商：河南省鼎信信息安全等级测评有限公司

# 项目技术方案

## 项目概况

### 项目概述

当前，我国信息安全面临的形势仍然十分严峻，维护国家信息安全的任务非常艰巨、繁重。随着我国经济的持续发展和国际地位的不断提高，我国的基础信息网络和重要信息系统面临的安全威胁和安全隐患比较严重，计算机病毒传播和网络非法入侵十分猖獗，网络违法犯罪持续大幅上升，犯罪分子利用一些安全漏洞，使用黑客病毒技术、网络钓鱼技术、木马间谍程序等新技术进行网络盗窃、网络诈骗、网络赌博等违法犯罪，给用户造成严重损失。

在中央27号文件《国家信息化领导小组关于加强信息安全保障工作的意见》中，都权威性的阐述了等级保护的必要性。信息安全等级保护制度是国家信息安全保障的基本制度、基本策略、基本方法，是当今发达国家的通行做法，也是我国多年来信息安全工作经验的总结。开展信息安全等级保护工作，有利于同步建设，有利于指导和服务，有利于保障重点，有利于明确责任，有利于产业发展。

从行为主体上看，按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，具体的信息系统单位，如医院，是等级保护工作落实的行为主体，各单位有义务和责任把国家安全置于首位，企业安全服从并服务于国家安全。只有认识提高了，才会在行动中把国家安全与企业安全有机统一起来，把落实等级保护工作变成一种自觉的行为，遵循“自主保护，国家监督”的原则。

依据《信息安全等级保护管理办法》（公通字[2007]43号），信息系统运营、使用单位在进行信息系统备案后，都应当选择测评机构进行等级测评。等级测评是测评机构依据《信息系统安全等级保护测评要求》等管理规范和技术标准，检测评估信息系统安全等级保护状况是否达到相应等级基本要求的过程，是落实信息安全等级保护制度的重要环节。

在信息系统建设、整改时，信息系统运营、使用单位通过等级测评进行现状分析，确定系统的安全保护现状和存在的安全问题，并在此基础上确定系统的整改安全需求。 在信息系统运维过程中，信息系统运营、使用单位定期委托测评机构开展等级测评，对信息系统安全等级保护状况进行安全测试，对信息安全管控能力进行考察和评价，从而判定信息系统是否具备《信息系统信息安全等级保护实施指引》中相应等级安全保护能力。而且，等级测评报告是信息系统开展整改加固的重要指导性文件，也是信息系统备案的重要附件材料。等级测评结论为信息系统达到相应等级的基本安全保护能力，运营、使用单位应当根据等级测评报告，制定方案进行整改，尽快达到相应等级的安全保护能力。

### 项目需求

信息系统进行安全等级测评是国家推行等级保护制度的重要环节，也是信息系统安全建设和管理的重要组成部分。为全面分析许昌市审计局信息系统安全保护现状、排查安全隐患和薄弱环节，有针对性地进行安全系统建设，拟对许昌市审计局重要信息系统进行等级保护测评。

依据《信息安全等级保护管理办法》（公通字[2007]43号）、《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2008）、《信息系统安全等级保护实施指南》（信安字[2007]10号）、《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号）（含附件）、按照公安部、人社部、工信部有关文件要求，为全面提升许昌市审计局信息系统的安全保障能力和防护水平，对许昌市审计局信息系统进行全面的安全等级测评，并依据等级保护测评结果出具详实的测评报告和整改建议，并协助许昌市审计局完成整改工作。

### 项目范围及目标

1. **项目范围**

主要对审计管理系统（三级）、地税联网审计系统（三级）进行安全等级测评。

1. **项目目标**

本次项目目标是通过上述信息系统实施等级保护测评工作，发现可能存在的问题，并提出可行性整改方案，经专家评审和用户单位确认，出具公安部门认定的系统安全保护等级测评报告，并协助完成信息系统安全等级保护定级备案工作。

## 等级测评技术方案

### 2.1工作遵循原则

1. 先进性原则

从实际需求出发，对此次测评项目进行全面规划，采用现代化的理念和技术，对许昌市审计局的测评做到合理化、科学化，达到低投资、高效益；提交的报告着眼于先进、适应未来发展，并具有可发展的潜力、可整改性及可操作性。

1. 可靠性

**人员可控性**

河南鼎信将派遣由经验的顾问、测评师和工程师参加本项目的等级测评工作，同时还会安排由经验的项目管理人员、质量保证人员、标准化审核人员等支持项目的工作。

如果根据项目的具体情况，后期需要进行人员调整时，必须经过正规的项目变更程序，并得到双方的正式认可和签署。

**工具可控性**

河南鼎信项目组所使用的所有技术工具都事先通告客户方。并且在必要时可以应客户方的要求，向客户方介绍主要工具的使用方法，并进行一些测试实验。

**项目过程可控性**

本评估项目的管理将依据PMI项目管理方法学。特别是在项目管理中突出“沟通管理”，达到项目过程的可控性。

为了保证河南鼎信的工作能够按照工程进度计划实施，客户方组成的项目组工作需要在双方开展项目实施之前举行会议，予以讨论，正式形成文字材料，即书面确定客户方项目组的职责和义务。项目实施期间双方将本着友好合作的态度完成各自的职责。

1. 可维护性

项目测评过程中，需综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全测评规划。坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。

1. 安全性

河南鼎信所有参与本项目的项目组成员将与客户方签署保密协议，对工作过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，保证不会利用此数据进行任何侵害客户方的任何损害行为。

1. 应用性

在本次项目安全测评服务中，河南鼎信将采用公认的ISO 27001、GB/T 20984-2007信息安全评测规范（最新国家标准）以及国家信息安全等级保护指南等安全标准进行系统测评的工作，针对资产重要程度分别提供不同频率和方式的安全测评，帮助用户了解客观真实的自身网络系统安全现状，规划适合自己网络系统环境的安全策略，并根据科学合理的安全策略来实施后续的安全服务、选型与部署安全产品以及建立有效的安全管理规章制度，从而全面完整的解决可能存在的风险隐患。

1. 合规性

在本次项目安全测评服务中，除了依据相关的国内和国际标准之外，还根据本项目的需要，遵循河南鼎信公司质量管理与控制标准，严格把控项目实施质量。

### 2.2标准规范

1. 信息安全管理标准
2. 信息系统安全管理管理要求（GB/T20269-2006）
3. 信息系统安全工程管理要求（GB/T20282-2006）
4. 信息安全管理体系标准BS7799 （ISO/IEC 17799）
5. 信息安全管理标准ISO/IEC 13335
6. ISO 7498
7. 技术与工程标准
8. 安全系统工程能力成熟度模型SSE-CMM
9. 信息产品通用测评准则ISO/IEC 15408（GB/T18336）
10. 《信息安全与风险管理指南》（GB/Z 24364-2009）
11. 《信息安全管理体系要求》（GB/T 22080-2008）
12. 《信息安全管理实用规则》（GB/T 22081-2008）
13. 《信息安全事件管理指南》（GB/Z 20985-2007）
14. 计算机信息系统安全等级保护划分准则（GB 17859-1999）
15. 信息系统安全等级保护实施指南（GB/T 25058-2010）
16. 信息系统安全保护等级定级指南（GB/T 22240-2008）
17. 信息系统安全等级保护基本要求（GB/T 22239-2008）
18. 信息系统通用安全技术要求（GB/T 20271-2006）
19. 信息系统等级保护安全设计技术要求（GB/T 25070-2010）
20. 信息系统安全等级保护测评要求
21. 信息系统安全等级保护测评过程指南
22. 信息安全等级保护相关标准及规范
23. 《中华人民共和国计算机信息系统安全保护条例》 （1994年国务院147号令）
24. 《信息安全等级保护管理办法》（公通字[2007]43号）
25. 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）
26. 《2006-2020年国家信息化发展战略》（中办发[2006]11号）
27. 《中华人民共和国保守国家秘密法》（1988年9月5日中华人民共和国主席令第6号公布）
28. 《中华人民共和国保守国家秘密法实施办法》（国家保密局文件国保发[1990]1号）
29. 《中华人民共和国国家安全法》（主席令68号，1993年2月22日第七届全国人民代表大会常务委员会第三十次会议通过）
30. 《中华人民共和国计算机信息系统安全保护条例》（国务院令147号）
31. 《计算机信息系统保密管理暂行规定》（国家保密局文件国保发[1998]1号）
32. 《计算机信息系统国际联网保密管理规定》（国家保密局文件国保发[1999]1号）
33. 《中华人民共和国计算机信息网络国际联网管理暂行规定》（国务院令195号）
34. 《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》（1997年12月8日国务院信息化工作领导小组审定）
35. 《计算机病毒防治管理办法》（2000年4月26日中华人民共和国公安部第51号令）
36. 《计算机信息网络国际联网安全保护管理办法》（1997年12月11日国务院批准，1997年12月30日公安部发布）
37. 《计算机信息系统安全专用产品分类原则》（1997年4月公安部发布）
38. 《计算机信息系统安全保护等级划分准则》（1999年9月国家技术监督局发布）
39. 《互联网电子公告服务管理规定》（信息产业部2000年10月8日第4次部务会议通过）
40. 《互联网站从事登载新闻业务管理暂行规定》（国务院新闻办公室和信息产业部11月7日联合发布）
41. 《计算机信息系统安全等级保护划分准则》（GB/T17859-1999）
42. 《计算机信息系统安全等级保护网络技术要求》（GA/T387-2002）
43. 《计算机信息系统安全等级保护操作系统技术要求》（GA/T388-2002）
44. 《计算机信息系统安全等级保护数据库管理系统技术要求》（GA/T389-2002）
45. 《计算机信息系统安全等级保护通用技术要求》（GA/T390-2002）
46. 《计算机信息系统安全等级保护管理要求》（GA/T391-2002）
47. 《计算机机房场地安全要求》（GB9361-88）

### 2.3技术路线

针对两个信息系统的等级测评将遵循国家相关标准，从信息系统基本情况调研开始，通过合理选择对象、指标、方法完成现场测评实施，并通过整体测评形成测评结论。

技术路线如下图所示：



图 6‑2信息系统等级测评技术路线

鉴于信息系统的信息安全保护能力与国家标准要求可能存在的差距，根据国家信息安全等级保护相关政策与技术标准，按照信息安全等级保护二、三级的要求，对信息系统进行安全等级测评工作，及时发现问题并通过整改提高整体安全防护能力，为后续的等级测评奠定良好的技术基础。

等级测评流程如下图所示：



图 6‑3 等级测评流程图

### 2.4等级测评方案

1. 测评内容

对信息安全等级保护状况进行测评，应包括两个方面的内容：一是安全控制测评，主要测评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，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。

对安全控制测评的描述，使用测评单元方式组织。测评单元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：物理安全、网络安全、主机安全、应用安全和数据安全五个层面上的安全控制测评；安全管理测评包括：安全管理机构、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的安全控制测评。

系统整体测评涉及到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。因此，全面地给出系统整体测评要求的完整内容、具体实施方法和明确的结果判定方法是很困难的。测评人员应根据特定信息系统的具体情况，结合本标准要求，确定系统整体测评的具体内容，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。

具体见下图：

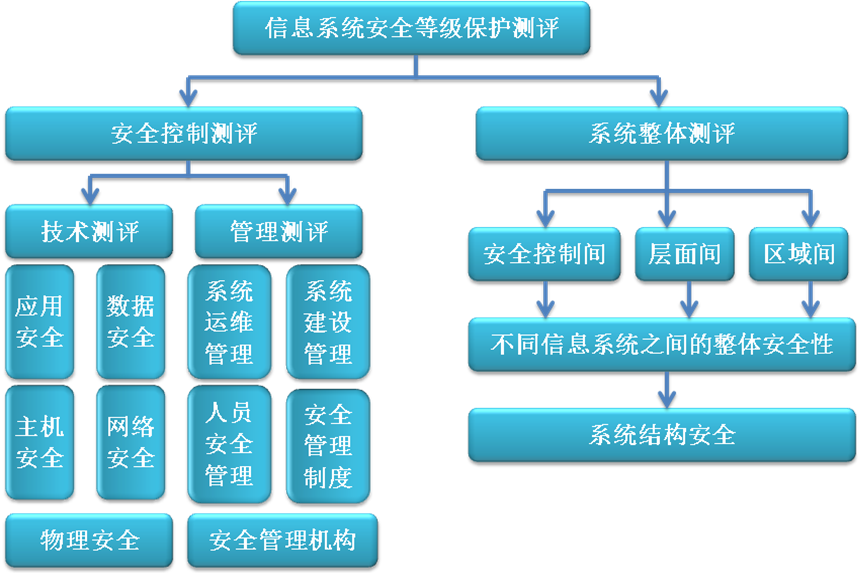


图 4测评内容

1. 测评工具

* **静电测试计**

CR-2型静电电压表是在吸收国内外先进静电仪表的基础上,经广大用户多年使用并多次改进的袖珍式非接触数字式静电测量表。CR-2型静电电压表可以测量物体表面的静电电压值和静电电荷的正负极性特征。CR-2是通过防静电材料表壳形成接地通路，因此，在测量过程中操作人员无需戴防静电腕带。CR-2采用三位半数字液晶显示屏显示电压值，显示值每秒更新三次。显示的测量值与被测物体的距离相关。

* **电磁干扰**

泰仕1392手持式场强测试仪，能够准确测试物理环境中的电磁场辐射强度，并可准确量测低至50Hz/60Hz电磁场辐射的不同频宽。

* **温湿度测试**

WSB-1-H2高精度（原装进口温度元件）温湿度表，具有相对湿度功能，最高/最低温度记忆显示功能，最高/最低相对湿度记忆显示功能，适用于通讯机房的温度湿度检测；通过河南省质量监督局检测校正。

* **漏洞测评工具**

绿盟远程安全评估系统，版本号V6.0R02F00SP08，是绿盟科技结合多年的漏洞挖掘和安全服务实践经验，自主研发的新一代漏洞管理产品，它高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面，是专业的"漏洞管理专家"。绿盟远程安全评估系统通过对服务器和网络设备进行扫描，对被检系统进行攻击性的安全漏洞和隐患扫描，并提交评估报告，提供相应的整改措施。先于黑客发现并弥补漏洞，防患于未然，这种预防性的安全检查最大限度地揭示了现存网络系统中存在的安全隐患，配合行之有效的漏洞修补措施，可以将网络系统的运行风险降至最低。

1. 测评方法

本次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。

* **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机构测评、人员安全管理测评、系统建设管理测评和系统运维管理测评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招标方的实际需求。

* **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物理安全测评、主机安全测评、网络安全测评、应用安全测评和数据安全及备份恢复等技术类测评任务，以及安全管理类测评任务。

在物理安全测评任务中，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招标方的实际需求。

在主机安全测评、网络安全测评、应用安全测评和数据安全及备份恢复等测评任务中，测评人员综合采用文档查阅与分析、安全配置核查和网络监听与分析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招标方的实际需求。

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招标方的实际需求。

* **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招标方的实际需求，并进一步应用于对目标系统进行安全性整体分析。

综合数据分析和差距分析结果形成等级测评报告。

1. 测评流程

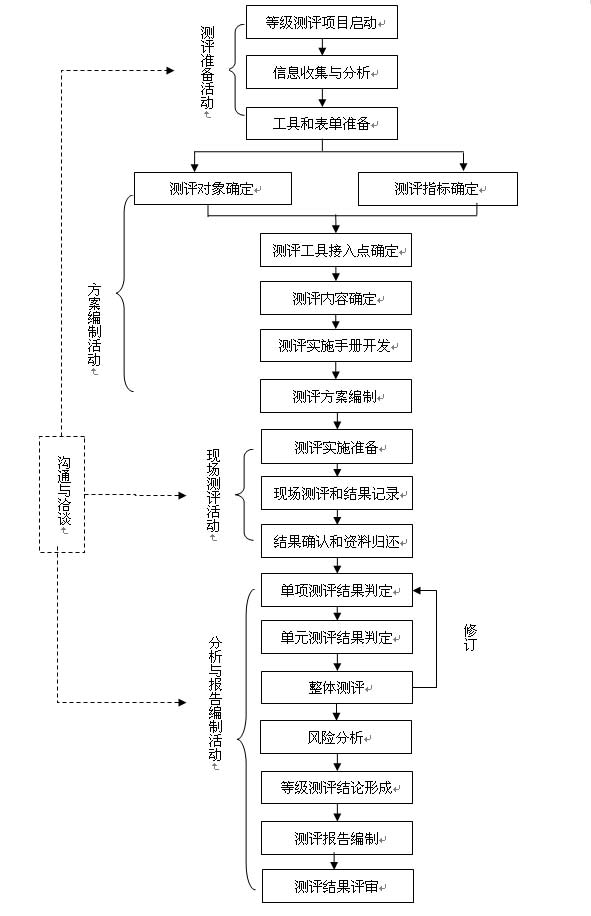


图 6‑25信息系统等级测评流程图

#### 测评准备阶段

##### 项目启动

在项目启动任务中，我司组建等级测评项目组，获取测评委托单位及被测系统的基本情况，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基本准备。

##### 系统调研

测评人员将综合利用表格调研、分档分析和访谈等方法，利用测评委托方提供的资料、基本情况调研表的反馈结果以及访谈结果对目标系统进行信息收集和分析，为后续的定级复审和测评工作准备必要的基础信息。

调研内容包括被测评系统的基本信息、物理位置、行业特征、管理框架、管理策略、网络及设备部署、软硬件重要性及部署情况、范围及边界、业务种类及重要性、业务流程、业务数据及重要性、业务安全保护等级、用户范围、用户类型以及被测评系统所处的运行环境等等。其中，现场访谈内容包括：

1. 访谈网络管理员，确认网络结构、网络产品部署、安全产品部署方面的基本情况信息；
2. 访谈主机操作系统管理员和数据库管理员，确认服务器和终端的基本情况信息以及部署情况；
3. 访谈应用开发或日常管理人员，确认应用软件的基本情况信息、关键数据类型以及业务安全需求；
4. 访谈安全主管、安全管理员及系统建设、运行维护负责人，了解单位的信息安全组织结构、信息安全管理制度文件体系构成情况。

根据配置数据、业务数据不同的数据类型分别由网络管理员、主机操作系统管理、数据库管理员、应用系统日常维护人员等配合相关人员开展调研工作。

收集和分析的结果将形成目标系统的三层次框架模型，以网络层为基础层，明确区域划分及关键网络设备；主机设备将嵌入到整个网络中，与网络层共同承载业务应用；顶层则为业务应用层，描述了业务（数据）流程在区域和设备间的流动。

威胁相关结果可通过综合分析表格调研数据和目标系统运行历史数据（如IDS记录）获得。

##### 工具和表单准备

测评项目组成员在进行现场测评之前，应熟悉与被测系统相关的各种组件、调试测评工具、准备各种表单等。

1. 测评人员调试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。
2. 测评人员模拟被测系统搭建测评环境。
3. 准备和打印表单，主要包括：现场测评授权书、文档交接单、会议记录表单、会议签到表单等。

#### 方案编制阶段

##### 确定测评对象

测评对象的确定一般采用抽查的方法，即：抽查信息系统中具有代表性的组件作为测评对象。在确定测评对象时，需遵循以下原则：

* + 重要性，应抽查对被测评系统来说重要的服务器、数据库和网络设备等；
  + 安全性，应抽查对外暴露的网络边界；
  + 共享性，应抽查共享设备和数据交换平台/设备；
  + 代表性，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统类型；
  + 恰当性，选择的设备、软件系统等应能符合相应等级的测评强度要求。

##### 确定测评指标

应根据目标系统的安全保护等级选择测评指标集合。如，目标系统的安全保护等级为第三级（S3A3G3），其测评指标应包括《信息安全等级保护实施指引》6.2节三级要求。

##### 确定测评工具接入点

信息系统应进行工具测评，工具测评可能用到漏洞扫描器、渗透测评工具集、协议分析仪等测评工具。

1. 确定需要进行工具测评的测评对象；
2. 选择测评路径。一般来说，测评工具的接入采取从外到内，从其他网络到本地网段的逐步逐点接入，即：测评工具从被测系统边界外接入、在被测系统内部与测评对象不同网段及同一网段内接入等几种方式；
3. 根据测评路径，确定测评工具的接入点；
4. 从被测系统边界外接入时，测评工具一般接在系统边界设备（通常为交换设备）上。在该点接入漏洞扫描器，扫描探测被测系统的主机、网络设备对外暴露的安全漏洞情况；
5. 从系统内部与测评对象不同网段接入时，测评工具一般接在与被测对象不在同一网段的内部核心交换设备上；
6. 在系统内部与测评对象同一网段内接入时，测评工具一般接在与被测对象在同一网段的交换设备上；
7. 结合网络拓扑图，采用图示的方式描述测评工具的接入点、测评目的、测评途径和测评对象等相关内容。

##### 确定测评内容与方法

将测评对象与测评指标进行映射构成测评内容，并针对不同的测评内容合理的选择测评方法形成具体的测评实施内容。

测评方法包括访谈、检查和测试等三种，具体到测评对象上可细化为文档审查、配置检查、工具测试和实地察看等，每个测评项可能对应多个测评方法。

##### 测评指导书开发

测评指导书是指导和规范测评人员现场测评活动的文档，包括测评项、测评方法、操作步骤和预期结果等四部分。在测评对象和指标确定的基础上，将测评指标映射到各测评对象上，然后结合测评对象的特点，选择应采取的测评方法并确定测评步骤和预期结果，形成不同测评对象的具体测评指导书。

##### 制定测评方案

综合以上章节结果内容，以及测评工作计划形成测评方案。

#### 现场测评阶段

##### 单元测评

依据目标系统的安全测评方案以及相应测评对象的测评作业指导书，按照《信息安全等级保护实施指引》相应级别要求，采用等级保护测评的方法进行差距分析。单元测评内容覆盖到被测系统安全技术的五个层面和安全管理的五个方面。安全技术的五个层面具体为：物理安全、网络安全、主机安全、应用安全、数据安全和备份恢复，安全管理的五个方面具体为：安全管理制度、安全管理机构、人员安全管理、系统建设安全管理和系统运维安全管理。

1. **物理安全**

物理安全检查将通过访谈和检查的方式评测目标系统的物理安全保障情况。主要涉及对象为机房。在内容上，物理安全层面测评实施过程涉及10个工作单元。

1. **网络安全**

网络安全检查将通过访谈、检查和测试的方式评测目标系统的网络安全保障情况。主要涉及对象包括网络设备、网络安全设备以及网络拓扑结构等三大类对象。在内容上，网络安全层面测评过程涉及8个工作单元。

1. **主机安全**

主机系统安全检查将通过访谈、检查和测试的方式评测目标系统的主机系统安全保障情况。在内容上，主机系统安全层面测评实施过程涉及7个工作单元。

1. **应用系统安全**

应用安全检查将通过访谈、检查和测试的方式评测目标系统的应用安全保障情况。在内容上，应用安全层面测评实施过程涉及9个工作单元。

1. **数据安全及备份恢复**

数据安全及备份恢复评估将通过访谈和检查的方式评测目标系统的数据安全及备份恢复保障情况。本次测评重点检查系统的数据在采集、传输、处理和存储过程中的安全及安全备份恢复情况。在内容上，实施过程涉及3个工作单元。

1. **安全管理制度**

安全管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。在内容上，安全管理制度测评实施过程涉及3个工作单元。

1. **安全管理机构**

安全管理机构测评将通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。 在内容上，安全管理机构测评实施过程涉及5个工作单元。

1. **人员安全管理**

人员安全管理测评将通过访谈和检查的形式评测人员安全方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。 在内容上，人员安全管理测评实施过程涉及5个工作单元。

1. **系统建设管理**

系统建设管理测评将通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，系统建设管理测评实施过程涉及9个工作单元。

1. **系统运维管理**

系统运维管理测评将通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，系统运维管理测评实施过程涉及13个工作单元。

1. **工具测试**

工具测试主要为漏洞扫描任务。

利用操作系统和常见应用漏洞扫描，可以获取目标设备开放的端口及服务，检测出目标系统中存在的操作系统和常见应用漏洞，如缓冲区溢出漏洞、系统或应用程序弱口令漏洞、系统或应用程序因未及时更新补丁所暴露出的漏洞等。

将漏洞扫描工具接入到目标系统中的不同网络（安全）区域的交换机上（如下图所示），并根据不同的目标设备类型（如思科路由设备、AIX主机等）来选择指标集合实施漏洞扫描。

扫描接入点和扫描路径的设置原则包括：

* 覆盖正常用户访问路径；
* 覆盖关键安全设备；
* 本地扫描覆盖全部目标主机和网络设备；
* 覆盖可能的攻击路径（互联网、低安全区、易接入区域等）。

利用WEB应用漏洞扫描，可以发现如下漏洞信息：

* 检测SQL注入、XSS、表单绕过、表单弱口令、各类CGI弱点等；
* 检测网页木马。

测评方案编制阶段，将依据调研结果合理选择接入点和扫描路径。

##### 整体测评

信息系统的整体测评，就是在单元测评结果的基础上，结合工具测试的结果评价信息系统的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。信息系统整体测评应从安全控制点间、层面间和区域间等方面进行安全分析和测评。

安全控制点间安全测评是指对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

层面间安全测评是指对同一区域内的两个或者两个以上不同层面安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

区域间安全测评是指对两个或者两个以上不同物理或逻辑区域间安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

#### 报告编制阶段

现场测评工作结束后，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。

##### 单元测评结果判定

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。任务描述：

1. 针对每个测评项，分析该测评项所对抗的威胁在被测系统中是否存在，如果不存在，则该测评项应标为不适用项。
2. 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。

##### 单元测评结果汇总

一是以表格形式汇总测评结果。表格以不同颜色对测评结果进行区分，部分符合的安全子类采用黄色标识，不符合的安全子类采用红色标识。

二是以柱状图形式统计不同设备和安全子类的测评结果。

三是以表格形式汇总信息系统中存在的安全问题。

##### 整体测评结果汇总

从安全控制间、层面间、区域间和系统结构等方面对单元测评的结果进行验证、分析和整体评。

1. 控制间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。

例如，主机层面的身份鉴别与访问控制之间关系密切，应关注他们之间的关联互补作用。

例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。

例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

1. 层面间安全测评

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作。

实际环境，重点研究不同层面上相同或相似的安全控制（如主机系统层面与应用层面上的身份鉴别之间的关系），以及技术与管理上各层面的关联关系，分析出哪些安全控制间可能会存在安全功能上的增强和补充作用。

1. 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。

整体结构的安全性测评应从信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等入手，结合不同位置上可能面临的威胁、可能暴露的脆弱性等，综合判定信息系统的整体布局是否合理、整体是否安全有效等。

在检查信息系统安全保护措施的具体实现方式和部署情况后，结合其业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范是否恰当合理。

例如，由于信息系统边界上的网络入侵防范设备的管理接口连接方式不当，可能使网络访问控制出现旁路，出现信息系统整体安全防范不当。

##### 风险分析和评价

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信息系统等级测评结果中存在的安全问题（等级测评结果中部分符合项或不符合项的汇总结果）可能对信息系统安全造成的影响。

分析过程包括：

1）判断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；

2）判断安全问题被威胁利用后，对信息系统安全（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；

3）综合1）和2）的结果对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；

4）结合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。

以列表形式给出等级测评发现安全问题以及风险分析和评价情况。

##### 等级测评结论

综合第3、4、5章的测评与分析结果，对信息系统基本安全保护状态进行综合判断，并给出等级测评结论，应表述为“符合”、“基本符合”或者“不符合”。

##### 安全建设整改建议

应在报告中针对系统存在的主要安全问题提出安全建设和整改意见。并通过总结单元测评、整体测评、风险分析和评论中的相关缺陷，结合《技术指引》和《管理指引》的相关要求，提出切合工作实际的整改思路和方法。

#### 工作产品

本项目完成后，提交的工作产品包括：

1. 《审计管理系统安全等级测评报告》；
2. 《地税联网审计系统安全等级测评报告》；

## 实施方案

信息安全等级保护是国家信息安全保障的基本制度，等级保护的整体实施工作包括等级保护定级与备案、等级保护差距分析、系统安全建设与整改、等级测评等几个阶段。定级是等级保护实施的基础性工作，是进行相应等级安全建设的依据。用户完成定级工作之后，更主要的是依据等级保护基本要求，进行等级化安全体系的设计与建设，最终符合国家等级保护的基本要求。用户必须在深入理解定级的根本要求、充分调查评估信息资产价值和安全风险的基础上才能完成准确定级，形成整改建设技术方案，最终顺利通过专家评审。

同时等级保护的建设是个长期的过程，需要花费大量的时间、精力和财力，本着为用户服务的态度，河南鼎信推出了等级保护专业服务，提供包括定级备案、差距分析、方案制订、实施、测评、检查等各个环节的服务，协助用户完成等级保护的实施和建设，为用户信息安全保障体系“保驾护航”

### 3.1项目实施承诺

河南省鼎信信息安全等级测评有限公司作为业界极具影响力的信息安全测评机构，对信息系统安全等级保护测评项目给予高度重视，并将指派公司多名高级等级测评师进入项目小组，直接掌控项目的技术水平和质量。河南省鼎信信息安全等级测评有限公司将根据信息系统安全等级保护测评项目的具体要求，结合自己的业界经验及项目管理经验，努力满足提出的对本项目的目标。在项目管理、测评实施、项目验收、售后服务等项目环节中做到守时、保质，使此项目成为精品和典范。

### 3.2项目组织结构

为了保障项目的顺利实施，河南鼎信方面根据本项目的实际情况精选管理和技术人员组成项目实施团队，由项目经理、技术主管、技术评审组、网络安全组、主机安全组、应用安全组和工具测试组组成。同时，为了满足招标方保密要求并保证项目质量，设立质量主管、保密安全员与档案管理员。

河南鼎信邀请招标方指定项目负责人和技术评审专家，并选派质量控制人员共同参与项目管理。

#### 项目组织方式规划



图 7项目组织结构图

#### 项目责任人清单

##### 项目人员职责

项目实施团队的职责及承担任务详细描述如下。

1. **项目经理：**

项目经理是本项目的负责人，其任务是对项目过程实行全面的管理，具体体现在对项目目标的把握，并组织会议制定计划和报告项目的进展，并在不确定环境下对不确定问题组织集体讨论决策，在必要的时候进行沟通、谈判及解决冲突。

项目经理所应承担责任主要有：

* 保证项目的目标在实施中前后一致，实现客户的目标；
* 对各种项目资源进行适当的管理和充分有效的使用；
* 与客户进行及时有效的沟通，及时商讨项目进展状况；
* 保证项目的成功，保证项目按时、在预期内达到预期的效果；
* 协调项目中的各个角色和各种关系，为项目成员创造良好的工作环境。

1. **技术评审组：**

由河南鼎信资深专家组成技术评审组，技术评审组独立于项目实施团队内其他组工作，其主要任务是针对项目实施过程中的主要技术思路和工作产品的技术合理性进行把关，包括但不限于对测评方案、整改建设书、等级测评报告等项目交付物的审核。

1. **技术主管**

主要任务是针对项目实施过程中的主要技术思路和工作产品的技术合理性进行把关，包括但不限于对测评方案、整改建设书、等级测评报告等项目交付物的审核。

1. **质量主管**

主要任务是根据河南鼎信质量管理体系要求，对项目实施进度、产品质量等实施管理。

1. **网络安全组**

职责描述：负责招标方目标系统的网络安全测评，包括调查了解目标系统的网络拓扑结构以及相关网络互联和安全设备的基本信息，开发/修订相应的测评指导书并实施安全配置检查，完成整改建议书和等级测评报告中的网络安全部分，并配合主机、应用和工具测试组以及安全管理组的工作。

1. **主机及应用安全组**

职责描述：负责招标方目标系统的主机和应用（含中间件平台）安全测评。主机安全主要包括调查了解目标系统的主机运行的操作系统和数据库管理系统的基本信息，开发/修订相应的测评指导书并实施安全配置检查，完成整改建议书和等级测评报告中的应用安全部分，并配合网络、应用和工具测试组以及安全管理组的工作；应用安全主要包括调查了解应用系统的用户、业务流程、数据分类、部署情况和安全需求，设计应用测评用例和应用测评指导书，并实施安全功能验证、安全配置检查，完成整改建议书和等级测评报告中的应用安全部分，配合网络、主机和工具测试组以及安全管理组的工作。

1. **工具测试组**

职责描述：负责目标系统的外部渗透和内部渗透测试，包括调查了解网络、系统和应用现状，准备渗透测试工具、制订渗透测试计划和方案，实施外部渗透和内部渗透测试，完成整改建议书和等级测评报告的相关内容，同时配合网络、主机和应用等其他测评小组的测评工作。

1. **安全管理组**

职责描述：负责分析和评审招标方提交的各类技术、管理文档；基于《金融行业信息系统信息安全等级保护实施指引》和《金融行业信息系统信息安全等级保护测评指南》，针对招标方的物理环境、安全管理等方面的要求，准备安全核查记录表、制定安全核查计划、实施现场物理安全和安全管理状况核查，完成整改建议书、等级测评报告中的管理部分，配合网络、主机、应用等其他测评组的工作。

1. **保密安全员**

主要任务是根据河南鼎信和本项目的保密要求对项目保密控制实施管理。

1. **档案管理员**

主要任务是对项目各阶段中间文档、工作产品及调阅的甲方文档进行集中管理。

### 3.3项目实施计划

河南省鼎信信息安全等级测评有限公司为了确保对许昌市审计局信息系统等级评测项目能够在用户要求时间内按时完成（签订合同后30个工作日内完成项目成果），特制定了详细的测评项目实施时间进度计划表，详见下表：

表 17等级测评实施进度计划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **实施阶段** | **工作内容** | **配合需求** | **工作日** | **阶段工作产品** |
| **项目启动会** | 项目组全体人员参加；介绍项目实施方案、明确实施内容与相关人员。 | 甲方主管领导、相关部门负责人 | 1天 | **项目实施计划** |
| **调研表填写方法说明会** | 介绍填写《信息系统调研表》的注意事项； | 甲方相关技术人员 | --- |
| 系统调研 | 表格调研：2）基于表格调研结果进行现场调研；3）文档收集与分析。 | 1、熟悉业务应用系统的相关人员2、安全主管、系统管理员、网络管理员、安全管理员等相关人员 | 3天 | **信息系统调研表** |
| 1）汇总分析；2）形成目标系统层次全景描述 | --- |
| 方案编制 | 确定工作内容：1）确定测评对象；2）确定指标；3）准备作业指导书。 | --- | 3天 | **信息系统测评方案** |
| 1）方案评审；2）方案修订与确认。 | --- |
| **测评方案评审会** | 对测评方案进行评审，同时由乙方介绍现场测评计划及甲方配合事项。甲乙双方主要技术人员参会旁听。 | 甲方技术评审组及主要技术人员 | 1天 | --- |
| 现状测评 | 1）机房安全测评；2）安全配置核查（含主机、网络、安全及应用）；3）工具测试（含漏洞扫描、验证及渗透测试）。 | 1、熟悉业务应用系统的相关人员2、安全主管、系统管理员、网络管理员、安全管理员等相关人员3、访谈需要运行部门、开放商、人事等部门指定人员配合。4、独立办公室，可容纳20-30人5、一个可以上网的端口。 | 7天 | **现场结果记录表** |
| 1）现场结果初步汇总；2）测评结果现场小结。 |
| **现状测评小结会** | 对现场测评的初步结果交流。 | 需要运行部门、开放商、人事等部门技术配合。 | 1天 | --- |
| 整改建议 | 1）测评结果单项判断；2）整体分析；3）问题危害分析。 | --- | 3天 | **信息系统整改建议** |
| 形成问题整改建议 | ---- |
| **整改建议评审会[[1]](#footnote-2)** | 甲、乙双方技术评审组对整改建议进行评审。甲乙双方主要技术人员参会旁听。 | 甲方主管领导、运行部门、研发部门、人事等部门、专家评审组及主要技术人员。 | 0.5天 | --- |
| 整改指导 | 依据问题和建议指导河南商丘市财政局信息中心组织的安全建设整改工作 | 乙方配合甲方指导整改 | 0.5天 | --- |
| 等级测评 （复测评） | 1）编制测评方案 2）现场测评 | 1、熟悉业务应用系统的相关人员2、安全主管、系统管理员、网络管理员、安全管理员等相关人员3、访谈需要运行部门、开放商、人事等部门指定人员配合。4、独立办公室，可容纳20-30人5、一个可以上网的端口。 | 2天 | **二次现场结果记录表** |
| 报告编制 | 1）两次测评结果汇总分析；2）形成测评结论；3）形成测评报告 | --- | 7天 | **等级测评报告** |
| **报告评审会** | 甲、乙双方技术评审组对测评报告进行评审。甲乙双方主要技术人员参会旁听。 | 甲方技术评审组及主要技术人员 | 1天 | --- |
| **项目工作汇报会** | 项目组全体人员参加；乙方介绍项目过程、测评工作主要内容、测评中发现的主要问题及整改情况、最终测评结论等。 | 甲方主管领导、运行部门、开放商、人事等部门、专家评审组及主要技术人员。 | --- |
| **预计工期：30工作日** | | | | |

### 3.4项目管理标准

为了保证许昌市审计局信息系统等级评测项目实施的质量和进度，本项目将参考并遵守一些国际上最新的相关信息安全工程标准和最新的研究成果，如：

* PMI项目管理方法学
* SSE-CMM信息安全工程成熟度模型
* IATF信息系统安全工程（ISSE）过程模型

### 3.5项目管理方法

河南鼎信项目管理主要分为五大程序组，包括项目的启动，计划，执行，控制和总结。项目管理应用多领域管理技巧包括项目时间管理、项目范围管理、项目成本管理、项目质量管理、项目人力资源管理、项目交流管理、项目风险管理和项目整合管理。

河南鼎信项目管理的基础是PMI的项目管理体系和系统安全工程成熟度模型SSE－CMM。

SSE-CMM的目的是建立和完善一套成熟的、可度量的安全工程过程。该模型定义了一个安全工程过程应有的特征，这些特征是完善的安全工程的根本保证。这个安全工程对于任何工程活动均是清晰定义的、可管理的、可测量的、可控制的并且是有效的。SSE-CMM模型及其评定方法汇集了业界常见的实施方法，提供了一套业界范围内（包括政府及产业）的标准度量体系，确保了项目实施活动后，能够得到的一个完整意义上的安全结果。

PMI的项目管理知识体系则把项目管理归纳为范围管理、时间管理、成本管理、质量管理、人力资源管理、风险管理、采购管理、交流管理和整合管理九大知识领域。PMI知识体系为许昌市审计局信息系统安全等级测评项目管理提供了指南。

河南省鼎信信息安全等级测评有限公司项目管理方法则整合了PMI的项目管理体系和SSE－CMM系统安全工程成熟度模型，强调分布于整个项目生命周期中各个环节的安全工程活动，包括概念定义、需求分析、设计、开发、集成、安装、运行、维护及更新项目，并不断改进工程实施的现状，达到提高系统安全、产品安全和工程服务安全的质量和可用性并降低成本，充分体现了河南省鼎信信息安全等级测评有限公司在项目管理和实施方面的能力。

对于许昌市审计局信息系统等级评测项目，建议可通过建立工作细分结构（Work Breakdown Structure，WBS）明确项目的工作内容，这样不仅定义了工作内容，同时也定义了工作任务之间的关系，明确了工作界面。项目的WBS是对工作计划、进度、费用、技术状态进行部署和跟踪控制等管理活动的基础。

### 3.6项目管理计划

#### 制定项目总体计划书

由于许昌市审计局信息系统等级评测项目的时间紧、任务重，我们采取了并行作业的方式。在项目具有合作意向的时候，我们就着手测评指导书和检查表的制作，利用复用检查的方法，节省时间。同时采用项目管理流程中对时间进度的有效管理手段，保证在紧缩时间的同时能达到项目的质量要求。

在多年项目实施经验积累的基础上，逐步形成适合不同类型项目的实施指南。公司高级测评师将根据对项目细节的分析与研究，形成适合许昌市审计局信息系统等级评测项目的详细、切实的项目测评指导书，并形成关键性技术文件。

项目测评指导书将始终贯彻于整个项目实施过程之中，是整个测评项目实施的指导性技术文件。具体项目实施时，按照该指导书的精神和具体内容对整个项目中各个具体项目细节进行微调，以确保整个项目能够顺利、按时完成。

#### 项目人力资源管理

许昌市审计局信息系统等级评测项目小组由测评委托方、河南省鼎信信息安全等级测评有限公司联合组成，对整个项目的测评实施负责。项目小组各成员各有分工，分工恰当，保证没有职责不清，没有重复责任，没有失控区域。项目小组成员的选定基于多种方面，作为许昌市审计局信息系统安全等级测评估项目的项目经理除了具备必备的项目管理的知识和能力以及相关的资格认证外，还必须具备类似项目管理的成功经验；具有多方面的管理能力，包括领导能力，交流能力，协商能力，处理纠纷和矛盾的能力，解决问题的能力；能鼓舞整个团队的士气，指导团队的工作。各分项技术人员必须具备相关专业如计算机网络专业的高级教育背景，同时又有从事类似项目的项目管理经验。

#### 项目时间进度管理

许昌市审计局信息系统安全等级测评估项目大致可以分为以下几个阶段：

* 信息系统调研
* 测评方案确认与调整
* 现场测评
* 分析与编制测评报告
* 编制安全整改技术方案

许昌市审计局信息系统等级评测项目执行时间计划的制定包括了诸多工作，比如：项目分项任务的定义，任务之间逻辑关系的确定，完成分项任务所需要时间的估算等。

除了工具的应用外，更重要的是保持与项目小组各成员之间的沟通，透过正式及非正式的渠道去了解真实情况。项目经理可通过定期的项目进度小组会议了解项目的进度和小组所遇到的困难或问题，并寻求解决方法。在必要时，重大的问题需向项目变更控制委员会报告、请求指示。

对项目进度的控制，主要是通过每日检查、项目定期状态报告和周例会制度，采用了主动影响、跟踪项目主要因素的方法，确保项目向正面方向发展。当项目执行计划发生变化时，及时确认变化，并找出解决问题的方法，把更改的进度拖回到受控范围内。

对许昌市审计局信息系统等级评测项目执行时间的保证通过在计划阶段精确估算，风险预留等方式，把项目的资源保证到对项目整体进度起制约影响的任务上去。

在执行阶段主要应用以下两种时间压缩方式：

* 通过对项目成本和时间的制约关系的分析，决定怎样用最少的成本增加得到最大的时间压缩
* 通过分析项目执行中的逻辑关系，分析风险因素，权衡重复劳动的可能性，把正常情况下有前后依靠关系调整成为可以平行操作的任务

#### 项目质量管理

在许昌市审计局信息系统等级评测项目中，我们主要将从项目质量计划和项目质量控制两方面入手。项目质量的计划是质量保证的关键，现代质量控制理论普遍认为质量首先在于计划，其次在于检验。质量计划包括定义出项目各子系统需要满足的质量标准。

在做质量管理计划时，将细定义出进行质量控制的流程和规定。质量控制包括对测评各阶段的输出文档、测评记录数据几方面进行控制。在质量控制过程中，积极配合现场建立的要求，我们将遵从许昌市审计局信息系统等级评测项目的管理流程，做好测评相关工作。在测评工具功能、性能的质量控制方面，将采用最新的行业标准或者是约定标准进行测试控制。

#### 项目范围管理

许昌市审计局信息系统等级评测项目测评范围的计划，包括定义项目测评阶段的划分及其每一阶段的交付物（包括产品、服务和文档资料）。这些交付物将作为项目阶段是否结束可以转入下一阶段的检验标准。河南省鼎信信息安全等级测评有限公司在与许昌市审计局确认后，将成为与客户之间对合同执行情况进行评判的共同标准。恰如其分的实施范围的分解，是项目成功的关键。不做项目内容细分解，项目进程的节奏随时可能被突如其来的问题所扰乱，引起重复劳动，增加项目所需要的时间。

#### 项目交流及文档资料管理

项目的交流包括确保及时地产生、收集、发送、储存和处理项目的信息，它在人、观念和信息之间提供关键的链接。在交流计划阶段，将定义出谁需要什么信息、什么时候需要及怎样传递信息。随着项目的进一步发展，交流计划将不断更新和优化。

### 3.7项目管理与实施

河南省鼎信信息安全等级测评有限公司将采用良好的客户服务支持体系，规范的项目管理标准与规则，先进的项目管理技术，按许昌市审计局信息系统等级评测项目招标文件的要求，严格履行规定职责，保障项目的顺利进行。以下从河南省鼎信信息安全等级测评有限公司针对许昌市审计局信息系统等级评测项目的实施承诺、项目管理方法、质量保证体系、针对本项目的管理计划等几个方面介绍河南省鼎信信息安全等级测评有限公司的项目管理控制体系。

## 项目风险规避方案

许昌市审计局信息系统技术要求高、工程管理复杂。基于以上因素，结合长期信息系统安全测评过程中的经验教训，在许昌市审计局项目中必须采取谨慎的风险管理措施，以确保工程在质量、时间和效益上都能达到预定目标。

风险管理对明确项目范围，制定有效的进度计划、质量保证计划和成本估算有着积极的作用，有助于工程参建各方了解工程的本质，消除各类风险，实现工程的建设目标。

项目风险管理是通过对项目相关的内外因素的分析，对潜在的意外损失进行识别、评估，并根据项目的具体情况采取相应的措施，确保在主观上尽可能地做到有备无患，如果风险因素真正地阻碍了项目的实施，也可以及时地寻求切实可行的补偿措施，从而减少意外损失。

### 4.1目标风险

目标风险是由于双方对阶段或整体目标的定义理解产生歧义而形成。

规避方法：由河南鼎信提供给用户方详尽的咨询及分析建议，在实施过程中，根据各阶段实施的实际情况变化，调整和修改实施计划及阶段目标。

### 4.2规模风险

规模风险是由于双方最初对项目的结构规模、扩展能力、单位时间内推广规模估算有误而造成的。

规避方法：在项目规划前期由河南鼎信提供给客户详尽的咨询及分析建议，并经过双方充分的研讨，使做出的项目规划合理适度且行之有效。

### 4.3质量风险

质量风险是由于在项目建设过程中未确立标准的质量考核体系以及对质量指标监控不严造成的。

规避方法：参照标准体系制订相应的规范质量标准并严格考核执行。

### 4.4资源风险

资源风险是由于项目的人力资源及技术资源发生供需不平衡而形成的。

规避方法：在项目规划前期详尽考虑项目建设过程中所需的资源，做出适当的资源规划，合理调配资源。使各种资源达到最佳配置。

### 4.5管理风险

管理风险是由于项目管理层使用不适于本项目的管理方法而形成的。

规避方法：由双方对项目的管理结构进行分析，针对本项目提出适合的项目管理方案，在方案确立后，在项目建设过程中严格履行实施。

### 4.6等级测评可能引入的风险

等级测评实施过程中，对被测系统可能引入新的风险，有以下几方面

1. 验证测试影响系统正常运行；

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查看一些信息，这就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。

1. 工具测试影响系统正常运行；

在现场测评时，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。测试可能会对系统的负载造成一定的影响，漏洞扫描测试和渗透测试可能对服务器和网络通讯造成一定影响甚至伤害。

1. 敏感信息泄漏。

泄漏被测系统状态信息，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。

规避方法：我方要充分估计测评可能给被测系统带来的影响，向被测系统运营、使用单位揭示风险，提前采取预防措施进行规避。同时，我方将于测评委托单位签署委托测评协议、现场测评委托书、保密协议，要求测评委托单位进行系统备份，规范测评活动，及时与测评委托单位沟通等措施规避风险，尽量避免给委托测评单位带来影响。

### 4.7项目风险管理

由于许昌市审计局安全等级测评估项目实施可能涉及的范围、时间及效果都不可能在项目开始时完全确定，因此，在项目进行过程中也相应会出现大量的不确定性，即项目风险。工程实施方案所提到的“风险”是指对项目“不利”的不确定因素。

对项目不利的风险存在于任何项目中，并往往会给许昌市审计局安全等级测评估项目的推进和项目的成功带来负面影响。风险一旦发生，它的影响是多方面的，如导致项目产品/服务的功能无法满足客户的需要、项目费用超出预算、项目计划拖延或被迫取消等，其最终体现为客户满意度的降低。因此，识别风险、评估风险并采取措施应对风险---即风险管理---对项目管理具有十分重要的意义。

#### 风险管理的模型

项目风险管理模型如下：



项目风险管理主要分为以下几个步骤：风险识别、定性/定量风险分析、风险应对计划编制及风险监控。

风险识别

风险识别，是指识别并记录可能对项目造成不利影响的因素。由于项目处于不断发展变化的过程中，因此风险识别也贯穿于整个项目实施的全过程,而不仅仅是项目的开始阶段。风险识别不是一次性的工作，而需要更多系统的、横向的思维。几乎所有关于项目的计划与信息都可能作为风险识别的依据，如项目进度计划、安装结构、项目组织结构、项目范围、类似项目的历史信息等。

定性/定量风险分析

通过风险识别过程所识别出的潜在风险数量很多，但这些潜在的风险对项目的影响是各不相同的。“风险分析”即通过分析、比较、评估等各种方式，对确定各风险的重要性，对风险排序并评估其对项目可能后果，从而使项目实施人员可以将主要精力集中于为数不多的主要风险上，从而使项目的整体风险得到有效的控制。

风险分析主要可采用的方法有：风险概率/影响评估矩阵、敏感性分析、模拟等。在进行上述分析时，主要关注以下几个风险因素：

风险概率：即风险事件发生的可能性的百分比表示。这个数字是通过主观判断而获得的，如专家评估、访谈或根据以前类似项目的历史信息。

风险影响：即风险发生可能对项目造成的影响大小。这种影响可能是时间上的，可能是成本上的，也可能是其他各方面的。

风险值（预期值EMV）：风险值=风险概率×风险影响，是对风险对项目造成的影响的最直接评估，它综合考虑了概率与影响两方面的因素。

风险应对计划编制

风险应对计划的目的在于通过制定相应的措施，来应对风险对项目可能造成的威胁。最常采用的应对威胁的几种措施是：规避、减轻、转移、接受。

规避：即通过消除风险的成因来消除该风险；

减轻：即通过采取措施降低“风险概率”或“风险影响”,从而达到降低风险值的结果；

转移：即将风险转移到另一方，如购买保险、分包等；

接受：即对该风险不采取措施，接受其造成的结果，或在该风险发生后再采取应急计划进行处理。

具体采用何种方式来应对某一风险，取决于该风险的风险值（EMV）、拟采取应对措施的可能成本、项目管理人员对待风险的态度（效用函数）类型等各方面，不可一概而论。

风险应对计划是针对已识别的风险进行的；对于未知-未知的风险，不可能预选制定相应的应对计划或应急计划，因此，可以利用管理储备来应对。

风险监控

风险监控主要包括以下几方面的任务：

在项目进行过程中跟踪已识别风险、监控残余风险并识别新风险：随着项目的实施以及风险应对措施的执行，各种对项目的影响因素处于不断变化的过程中，因此，需要在整个项目过程中，时刻监督风险的发展与变化情况，确定伴随某些风险的消失而来的新的风险并制定相应的处理措施。

保证风险应对计划的执行并评估风险应对计划执行效果。评估的方法可以是项目周期（阶段）性回顾、绩效评估等。

对突发的风险或“接受”的风险采取适当的权变措施。

通过风险监控过程，项目人员持续更新项目风险列表，并通过重复上述各步骤保证项目风险始终处于受控状态。

项目实施的风险管理

不同类型的项目有不同类型的风险，安全项目实施的风险同样有其特殊性。许昌市审计局安全等级测评项目实施过程中的主要风险管理措施如下:

#### 项目实施中的主要风险及应对措施

**项目进度的风险**

由于项目涉及范围广，项目进度的控制绝非易事，它不仅取决公司的技术能力，服务水平，同时也在很大程度上受到对范围控制是否有效、对项目投入（包括人员时间的投入和资金等的投入）是否足够等方面的影响。

而实际实施过程中，并非所有用户对本次安全等级测评估项目实施理解与认同，因此，在项目实施时，可能一味在项目进度计划时求快，甚或是刻意追求某个具有特殊意义的日期作为项目里程碑，将对项目进度控制造成很大压力。当然，也可能由于种种原因，如测评环境不具备、人员没有到位，测评工具问题等等，造成项目进度拖延。因此，河南鼎信将充分考虑各种潜在因素，适当留有余地；任务分解详细度适中，便于考核；在执行过程中，强调项目按进度执行的重要性，在考虑任何问题时，都将保持进度作为先决条件；同时，合理利用赶工及快速跟进等方法，充分利用资源。

**项目人力资源的风险**

人力资源是项目实施过程中最为关键的资源。保证合适的人员以足够的精力参与到项目中来，是项目成功实施的基本保证。河南鼎信在此项目实施中将调动骨干技术人员，保证进入到项目中并承担角色的各类人员满足项目要求。同时，保证项目人员对项目的投入程度。将参与许昌市审计局安全等级测评估项目人员的业绩评估与该项目实施的状况相关联，明确许昌市审计局安全等级测评项目是在该阶段项目相关人员最重要的本职工作。

**对安全认识不正确的风险**

项目针对不同岗位，不同职位的人员展开一系列的安全产品及安全管理的培训，强化安全意识。培养每一个人信息网络用户的“网络安全人人有责”观念。把许昌市审计局安全等级测评项目的网络安全纳入一个人人有责、层层负责、有第一负责人负总责的安全管理体制之中，同时帮助许昌市审计局安全等级测评项目建立网络系统的安全管理机构，把网络管理制度化、规范化。

**对实际环境不熟悉的风险**

由于用户的网络环境及应用会由一定的差别，而且大部分网络应用是由软件开发商开发，不同的开发商所使用的开发工具、数据库、协议等等都不相同，并且网络设备如交换机、路由器也不尽相同，这就对项目的实施提出了很高的要求，各类设备的配置不可能千篇一律，要按实际环境而调整。针对上述情况，工程师将在用户现场认真填写用户环境调查表，并经用户确认后再实施，这样可以避免因用户实际网络环境不熟而导致用户业务中断的风险。

**测评活动引入的新风险**

1. 签署委托测评协议

在测评工作正式开始之前，我方与测评委托单位以委托测评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，后续的工作也以此为基础，避免以后的工作出现大的分歧。

1. 签署保密协议

我方将与测评委托单位签署完善的、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。测评工作的成果属测评委托单位所有，我方对其的引用与公开必须得到测评委托单位的授权，否则测评委托单位可以按照保密协议的要求追究我方的法律责任。

1. 签署现场测评授权书

在现场测评工作开始之前，我方和测评委托单位需要以测评授权的方式明确测评工作中双方的责任，揭示可能的风险，避免可能出现的纠纷和分歧。

1. 现场测评工作风险的规避

进行验证测试和工具测试时，我方与测评委托单位充分的协调，安排好测试时间，尽量避开业务高峰期，在系统资源处于空闲状态时进行，并需要测评委托单位相关技术人员对整个测评过程进行监督；在进行工具测试前，需要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技术人员进行操作，我方测评师根据具体情况提出需要操作的内容，并进行查看和验证，避免由于测评师对某些专用设备不熟悉造成误操作。我方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，征得其同意，必要时对其先进行一些实验。

1. 测评现场还原

测评工作完成后，我方测评人员应交回测评工程中获取的所有特权，归还测评过程中借阅的相关文档，并严格清理测评过程中植入被测系统中的相关代码\程序。

1. 规范化的实施过程

为保证按实施计划、高质量地完成测评工作，我方明确测评记录和测评报告要求，明确测评过程中每一阶段需要产生的相关文档，使测评工作有章可循。在委托测评协议、现场测评授权书和测评方案中，明确双方的人员职责、测评对象、时间计划、测评内容要求等。

1. 沟通与交流

为避免测评工作中可能出现的争议，在测评开始前与测评过程中，我方与测评委托单位进行积极有效的沟通和交流，及时解决测评过程中出现的问题，这对保证测评的过程质量和结果质量有重要的作用。

**项目实施中的风险监控**

采取以下措施对项目实施中的风险进行监控，以防止危及项目成败的风险发生。

建立并及时更新项目风险列表及风险排序。项目管理人员随时关注与关键风险相关因素的变化情况，及时决定何时、采用何种风险应对措施。

风险应对审计：随时关注风险应对措施（规避、减轻、转移）实施的效果，对残余风险进行评估。

建立报告机制，及时将项目中存在的问题反映到项目经理或项目管理层。

定期召集项目干系人召开项目会议，对风险状况进行评估，并通过各方面对项目实施的反应来发现新风险。

## 信息保密管理体系与措施

### 5.1保密承诺

一、保密信息的范围

A、除甲方书面表明为非保密信息外，我方从甲方获取的所有信息及材料，不论是书面、口头、磁记录、光学记录、电子记录还是其它记录形式都属于保密信息，包括但不仅限于：

1. 所有与甲方的业务、经营、计划、交易、市场、财务、目前或将来拟采用的经营方式、财务、交易、信托资产等有关的不被公众领域所知的文件、资料和信息。

2．所有甲方计算机应用系统的IT规划、软件设计方案、数据结构、设计方案、实施方案、技术细节、实现方式、设备参数配置、操作监控手段、数据加密算法、源代码、系统日志等相关信息和技术文档。

3. 所有甲方计算机设备、网络设备、存储设备、安全设备、监控设备的参数配置、IP地址、口令、操作监控手段等相关信息；计算机主机系统和网络设备运行记录、运行报告及应急方案。

4. 所有甲方计算机应用系统中保存的生产数据、业务和管理数据、生产经营信息、密钥、磁条数据及甲方客户信息等相关信息。

5. 所有甲方网络规划、网络架构、网络拓扑、IP地址信息及运行维护方案等相关信息。

6. 所有甲方信息安全规划、策略、设计、实施方案等信息安全方面的相关信息。

7. 所有甲方的项目开发文档、测试文档、实施文档、项目文档、管理文档等。

8. 所有甲方及上下级单位的采购需求、采购计划及与第三方厂商签订的合作规范等信息。

9. 我方在工作过程中发现的甲方系统、管理流程中存在的漏洞、缺陷等。

10. 我方在对甲方进行服务时提交的工作成果。

11、载有保密信息和数据的各类载体。

B、甲方的保密信息不包括：

1. 已成为公共知识或可通过其他正当公开渠道获得的信息。

2. 我方从有权披露该信息的第三方合法获得的且我方对之不负有保密义务的信息。

3. 我方独立于本条款确定的保密信息而自主开发出来的文件、资料和信息。

二、我方的保密义务

1. 我方保证与参与甲方项目的所有人员签订保密规范，并在甲方备案。

2. 我方承诺在保密期内，对保密信息保密，未经甲方书面同意，不将其用于为甲方服务以外的目的，并不将其泄漏给无关雇员以及任何第三方，而且我方应防止甲方保密信息被销毁、丢失或改变。

3. 我方的雇员为甲方利益必须接触相关保密信息时，我方可以将此部分保密信息披露给该雇员，但我方承诺告知该雇员相关的保密义务，并和其签署书面保密规范使其承担与本条款内容相同的保密义务。

4. 不以损害甲方利益的方式使用甲方保密信息。

5. 不出售、转让、复制或仿造甲方保密信息；不将保密信息透漏给与本项目无关的任何人；不在公共场所或私人通信中谈及甲方保密信息。

6. 未经甲方书面许可，不下载、分析和存储甲方保密信息，不将保密信息带离甲方办公场所。

7. 不利用合作之便获取甲方与合作无关的保密信息。

8. 不利用甲方保密信息从事损害甲方利益和声誉的活动。

9. 我方人员如在为甲方服务期间离职，不带走任何甲方保密信息，在保密条款规定的保护期内不泄漏任何甲方保密信息。

10. 不进行其他可能导致甲方保密信息泄漏的活动。

11. 我方保证在服务期间，参与（包含驻场）实施项目的我方人员遵守甲方的各项规章制度。

12. 我方保证自带设备（包含笔记本电脑、移动存储）未经批准严禁接入甲方网络系统内或通过甲方网络系统（包括营业网、开发网、测试网、管理网）下载文件和数据，如果确实因项目需要必须接入的，必须经过甲方部门负责人审批和办理相关准入手续，同时安装甲方提供的防病毒软件和在甲方人员监督下操作。

13. 未经甲方书面同意，我方不在市场宣传中（包括发布广告、成功案例等形式）使用建设银行商标。

14.如果法律规定或监管机构要求我方必须对保密信息或由保密信息得出的任何意见、判断等信息做出披露时，我方承诺立即书面通知甲方，以使甲方能选择采取保护措施。且在披露上述保密信息时，我方必须尽力确保有关部门对被披露的保密信息予以保密。

三、保密信息的交回

1．在双方合作终止后，我方承诺在合作终止之日起七个工作日内履行以下义务：

（1）返还包含保密信息的文件和资料，包括有关复制件或摘要；

（2）销毁无法返还的包含保密信息的文件和资料，包括复制件和电子文档；

（3）提供一份书面声明，确认已销毁所有包含保密信息的文件、资料、电子文档和相关复制件，并附所销毁材料的清单。

（4）未经甲方的书面许可，我方不丢弃和处理任何书面的或其他有形的安全保密信息。

四、保密期限

我方保密义务的期限为五年，其保密义务不随双方合作的终止而终止。

五、责任限制

1. 双方同意甲方对所透露的信息不附带任何种类的保证，不保证保密信息的真实、准确、完整等。

2. 双方同意甲方对于我方因使用甲方提供的保密信息而造成的任何损害不承担赔偿责任。

六、违约责任

如我方或我方人员（包含是否仍在我方公司供职）违反本条款的约定，则甲方有权采取以下措施中的一项或几项：

1.要求我方立即停止侵害。

2.暂停、中止或终止与我方的合作或我方所提供的服务，并要求我方退还已支付款项及同期存款利息。

3.要求我方采取有效措施防止泄密范围及甲方损失的扩大。

4.要求我方赔偿给甲方造成的直接和间接的损失和费用（包括但不限于律师费用、仲裁费用和执行费用等）。

5.其他进一步追究我方法律责任的权利。

### 5.2保密原则

1. 保密原则

公司严格按照《中华人民共和国保密条例》执行，以确保安全测评服务中涉及到用户单位机密以及公司自身测评技术机密的不对外泄漏。机密的保管实行点对点管理办法，落实到人头，做到有法可依，违法必究，责任落实到位。

1. 组织机构建立

公司为保证保密工作的顺利开展，公司以负责人牵头成立保密工作组，组员由档案管理专职人员、技术负责人、项目管理人员和公司总经理组成，并为档案管理配备专用的档案室,针对每个项目由项目负责人及保密安全员负责。

1. 保密内容
2. 技术方案、测评方案、测评报告。
3. 重要会议纪要。
4. 涉及用户敏感信息的各种项目文档
5. 保密实施细则：
6. 在项目合同签订前的技术方案由技术起草者负责保管，对其它部门及外单位人员不得透露任何技术内容及细节；
7. 对使用部门的需求情况由项目负责人落实并保证不得向外界透露，并以书面形式传递给档案管理人员和技术负责人；
8. 档案管理人员对以上信息以书面、电子等方式存档，公司员工在借阅时必须经领导同意且确定借阅时间方可借阅；
9. 档案管理人员不得将机密文件带回家中或带上出入公共场所，相关人员不准随意谈论、泄露机密事项、不准私人打印、复印、抄录文件内容、不得将朋友、他人带入档案室，不得外传、外借相关资料。
10. 起草、打印、复印机密文字资料时由专人负责，其它人不得随意查看；
11. 打印过的废纸和校对底稿应及时清理、销毁；
12. 合同签订后的相关文档资料立即存档，并建立保密所必备的借阅制度；
13. 出现泄密事件后，应立即上报公司负责人，做到机密不得扩散，同时认真追查相关人员的责任。

### 5.3保密实施措施

由于本工项目为许昌市审计局项目，针对该工程的特殊性，并保证工程顺利进行，特制定以下保密措施：

1. 本项目参与人员均按其身份证进行登记。保证所有施工人员均无犯罪前科及“法轮功练习史”；
2. 对参加本工项目的人员进场前按照规定进行保密纪律教育，强化保密意识，并签署保密协议；
3. 加强人员的组织管理，做到有效控制管理，保证参加测评人员不随意活动，人员在测评现场行踪可控可查；
4. 坚决贯彻保密守则：
5. 不该说的秘密，绝对不说；
6. 不该问的秘密，绝对不问；
7. 不该看的秘密，绝对不看；
8. 不该记录的秘密，绝对不记录；
9. 不在非保密本上记录秘密；
10. 不在私人通信中涉及秘密；
11. 不在公共场所和家属、子女、亲友面前谈论秘密；
12. 不在不利于保密的地方存放秘密文件、资料；
13. 不在普通电话、明码电报、普通邮局传达秘密事项；
14. 不携带秘密材料游览、参观、探亲、访友和出入公共场所。
15. 本项目所有文档均进行登记，不得随意带出工地，如需复印，需向总经理请示，经同意后方可在指定地复印，用完后需将复印件收回。
16. 文档员工、保密员工出现工作变动时应及时办理交接手续，交由主管领导签字。

## 应急方案

### 6.1流程

河南鼎信应急响应服务流程如下图所示：



图 8河南鼎信应急响应服务流程

### 6.2应急情况分类

管理员误操作造成的问题。

违反网络安全规程，造成事故。

应用程序设计漏洞造成的事故。

黑客攻击造成，网络故障。

### 6.3详细步骤

#### 事件检测：进行快速评估

**确定事件来源:**

超级用户的失误操作？

内部保密文件的意外泄漏？

来自Internet的攻击？

来自电话网的攻击？

来自内部网络的攻击？

**检查威胁的结果:**

检查系统、服务、数据的完整性、保密性或可用性；

检查攻击者是否侵入了系统；

检查攻击者以后能不能再次随意进入；

入侵者被发现的地点；

损失的程度；

暴露出的主要危险。

必须注意到从一个地点发起的攻击可能隐藏了攻击者的真正所在地。

#### 立即行动：限制损失

如果发生了较为严重的事件，管理负责人和技术负责人应该决定所采取的应急手段以消除威胁，限制损失。

要明确地指出处理事件的人员，确保安全保护指令深入理解；

启动事件日志：记录每一个发生的动作、事件、证据（要有时间和日期）

**可能的立即行动:**

恢复信息；

受到影响的计算机从网络中隔离或关机；

相关的局域网与Internet断开连接；

一个或多个远程访问服务器可以从网络中移走，或关闭；

网络或计算机并不关闭，而是试着在不影响服务的前提下使损失最小化；

立即对日志、数据进行备份，应该保存在磁带上或其它不联机存储设备。

#### 公共关系/社会交往

只有新闻负责人员能够联系新闻界，并发表声明；

如果希望就攻击的细节问题与其它人要讨论，要使用加密带签名（如PGP）的电子邮件；

如果需要，并且得到新闻负责部门的授权，应将事件信息通知其它受影响的站点；

如果要采取的立即措施影响到了对用户提供的服务，要决定要给用户发送什么消息。

#### 详细的情况分析

设定优先级，决定所要做的工作；

评估损失的范围，如分析系统：有没有被改动的文件；有没有被增加/修改的程序或用户帐号；如果发现了修改，在相似的系统上检查这些变动；

证实发生的确切事件；

按要求通知系统管理员、管理部门和纪律部门

#### 恢复：恢复数据、服务、系统

清理系统、恢复数据、程序、服务；

修改系统中存在的漏洞；

不能信任被攻入系统中的程序，将它们与安全的版本进行比较。

### 6.4后续工作

检查是不是所有的服务都已经恢复；

攻击者所利用的漏洞是否已经解决；其发生的原因是否已经处理；

保险措施，法律声明/手续是否已经归档；

应急响应步骤是否需要修改；

如果需要对设备进行修改，使用设备修改的步骤。

## 验收方式

为保证许昌市审计局信息系统等级评测项目实施工作的顺利进行，加强项目验收工作的组织管理，特制定本方案。

### 7.1验收目的

为使许昌市审计局信息系统等级评测项目按照《信息系统安全等级保护基本要求》以及许昌市审计局信息系统等级评测项目要求进行，确保项目竣工后达到有关要求和标准，必须进行项目验收。

### 7.2验收参与人员

1. 许昌市审计局审计管理系统（三级）、地税联网审计系统（三级）涉及的相关管理、技术人员；
2. 河南鼎信项目组人员。

### 7.3验收条件

1. 信息安全等级测评工作已经全部完成；
2. 信息安全等级测评报告和信息系统安全整改建议报告已提交；
3. 已向采购人提供了双方约定的全部信息安全服务文档。

### 7.4验收依据

1. 许昌市审计局信息系统等级评测项目招标文件；
2. 项目合同书；
3. 许昌市审计局信息系统等级评测项目投标文件；
4. 等级保护相关标准。

### 7.5验收流程

项目实施完成具备验收条件后，由河南鼎信、商丘市财政局信息中心共同组织项目的验收工作。项目验收工作主要包括以下几方面内容：

1. 检查项目实施过程文档是否齐全；
2. 检查各个信息系统的等级测评报告是否符合要求；
3. 检查各个信息系统的安全整改技术方案是否符合要求。

### 7.6验收结论

验收结果分为：验收合格、需要复议和验收不合格三种。符合等级保护标准、系统运行安全可靠、任务按期保质完成，视为验收合格；由于提供材料不详难以判断，或目标任务完成不足80%而又难以确定其原因等导致验收结论争议较大的，视为需要复议。

项目凡具有下列情况之一的，按验收不合格处理：

1. 未按项目考核指标或合同要求达到所预定的主要技术指标的；
2. 所提供的验收材料不齐全或不真实的；
3. 项目的内容、目标或技术路线等已进行了较大调整，但未曾得到相关单位认可的；
4. 实施过程中出现重大问题，尚未解决和作出说明，或项目实施过程及结果等存在纠纷尚未解决的；
5. 违反法律、法规的其他行为。

### 7.7验收结论处理

1. 验收结论为验收合格的，河南鼎信项目组将全部验收材料统一装订成册并连同相应的电子文档提交。
2. 验收结论为需要复议的，河南鼎信将补充有关材料或者进行相关说明。
3. 验收结论为验收不合格的，河南鼎信将按照合同要求承担相应责任，并进行限期整改，整改后符合验收条件，重新申请验收。

1. 视评审结果评审会可能有1～2次 [↑](#footnote-ref-2)