一、 等保测评服务方案

（一）服务目标

信息安全等级保护制度是我国的一项基本国策，为配合我国网络强国战略，对采购人进行等级保护测评，投标人出具的测评报告必须满足国家对等级保护测评报告的各项要求。

从信息安全责任制落实情况讲，被测单位基本构建了从单位最高管理层到执行管理层以及具体业务运营层的组织体系，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岗位。

（二） 等级保护测评方法

1、访谈

访谈是指测评人员通过引导信息系统相关人员进行有目的的、有针对性的交流以帮助测评人员理解、澄清或取得证据的过程。访谈的对象是人员，典型的访谈人员包括信息安全主管、系统建设负责人、系统运维负责人、物理安全负责人、人事管理相关人员、信息系统安全管理员、系统管理员、网络管理员、数据库管理员、安全审计员、资产管理员、文档管理员、软件开发人员、机房维护人员、机房值守人员等。访谈使用的工具是访谈表单。针对技术要求，使用‘访谈’的方法进行测评的目的是为了了解信息系统的全局性（包括局部，但不是细节）、方向性、策略性和过程性信息，一般不涉及到具体的实现细节和具体技术措施；针对管理要求，访谈的内容应该较为详细和明确。访谈的作用：一是了解基本情况，作为下一步测评工作的基础；二是访谈结果作为判断与其他几种测评方式所得到证据是否一致；三是作为相关管理方面实现要求与否的直接证据。作为第二级以上包含二级的信息系统访谈广度在数量上做到基本覆盖，深度上做到较为全面。

2、检查

检查是指测评人员通过对测评对象（如制度文档、各类设备、安全配置等）进行观察、查验、分析以帮助测评人员理解、澄清或取得证据的过

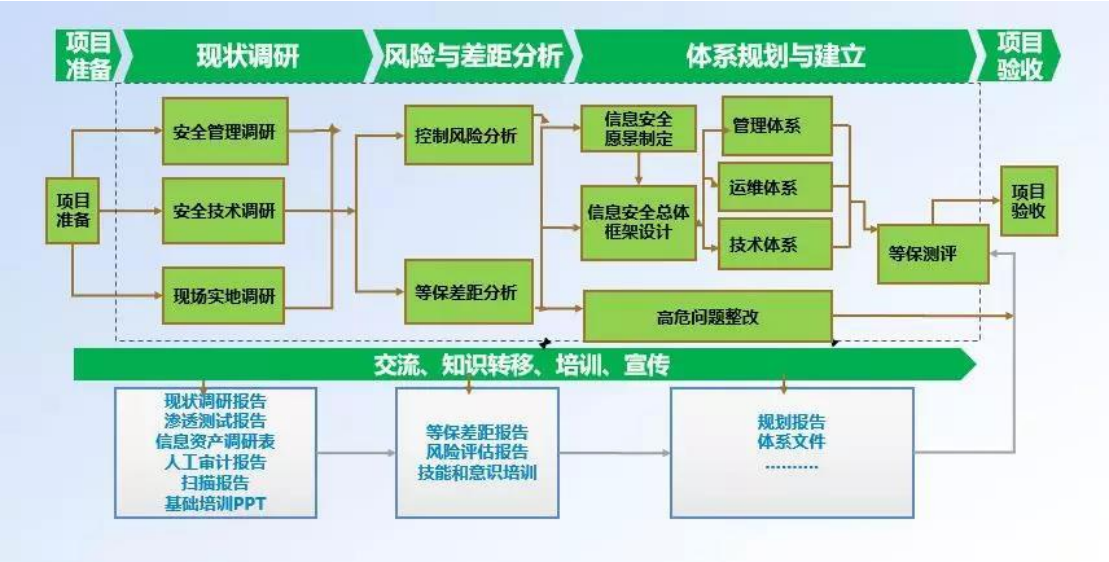
程。检查对象包括各类设备及标识、各种系统、安全配置、安全框架及规划、机房物理环境、存储介质、资源敏感标记、备份和恢复功能、高可用性、各类制度和规定、各种操作规程和手册、各类文档、各类文件、各类记录、各类计划方案及报告、各类预案框架、各类信息表及说明书、各类检查表、各类清单、各类合同及协议、各类材料、授权书、联系表等。检查用到的主要工具是核查表。针对技术要求，‘检查’的内容应该是具体的、较为详细的机制配置和运行实现；针对管理要求，‘检查’方法主要用于规范性要求（检查文档）。作为第二级以上包含二级的信息系统检查广度对测评对象在数量上抽样，在种类中基本覆盖，在深度上做到较全面。

3、工具测试

工具测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程。测试的广度体现在被测试的机制种类和数量上；测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出对象的广度不同。测试的深度体现在执行的测试类型上：功能/性能测试和渗透测试；功能/性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入信息系统。

（三） 服务内容

1、等级保护整体服务方案工作流程



a. 等保整改与安全建设

1）明确整改思路

2）进行风险评估

3）通过现场访谈、现场测试等方式，完成《差距分析报告》

4）形成等保整改方案

5）进行等保整改建议

b. 等保测评

1）制定测评咨询工作计划

2）准备等保测评所需要的文档和资料

3）配合测评机构的现场测评工作

c. 等保检查

1）开展自查

2）进行行业检查

3）准备检查所需要的文档和资料

4）配合公安机关的现场检查工作

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，并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，通过自身的安全产品、安全服务，可协助用户完成等级保护各个阶段的实施和建设，确保用户严格按照等级保护的过程规划并建设自己的安全保障体系，更好地支撑应用和业务的开展，为用户信息安全保障体系“保驾护航”。

2、测评服务方在等级保护各个阶段将协助用户完成的任务和工作

a. 具体包括：

1)等级保护差距分析

通过风险评估可以发现信息系统的安全现状与需要达到的安全等级或目标的差异，使信息系统的管理和使用单位可以在技术和管理方面进行有针对性的加强和完善，使单位的信息系统安全工作有的放矢。

2)等级保护整改建议方案

测评服务方根据评估的结果和信息系统确认的保护等级，结合《信息系统安全等级保护基本要求》以及其它相关整改标准中对各级别信息系统的技术、管理和运维方面的要求，制定相应的安全保护措施，完成等级保护整改建议方案的设计。

依据公通字[2007]43 号文的要求，信息系统定级工作完成后，运营、使用单位首先要按照相关的管理规范和技术标准进行安全建设和整改，使用符合国家有关规定、满足信息系统安全保护等级需求的信息技术产品，进行信息系统安全建设或者改建工作。

等级保护整改的核心是根据用户的实际信息安全需求、业务特点及应用重点，在确定不同系统重要程度的基础上，进行重点保护。整改工作要遵循国家等级保护相关要求，将等级保护要求体现到方案、产品和安全服务中去，并切实结合用户信息安全建设的实际需求，建设一套全面保护、重点突出、持续运行的安全保障体系，将等级保护制度确实落实到企业的信息安全规划、建设、评估、运行和维护等各个环节，保障企业的信息安

全。

3)等级保护整改实施

测评服务方将依据规划向用户提供详细设计和等级保护系统建设服务，确保保障等级能够达到信息系统所要求的保护等级，或者协助用户进行等级保护的实施，对承建商的工作进行监理。

4)等级保护测评咨询

在信息系统进行完成定级和整改实施之后，需要通过测试手段对信息系统的安全技术和安全管理上各个层面的安全控制进行整体性验证，测评服务方提供的测评咨询服务将协助用户通过等级保护测评工作。

5)等级保护检查咨询

在信息系统进行完成定级和整改实施之后，国家主管机关将对信息系统的安全技术和安全管理各个层面的安全控制进行检查，测评服务方将协助用户准备检查所需要的文档和资料，配合公安机关开展现场的检查工作。

3、测评服务内容

安全层面	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
	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
	入侵防御	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
	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
	剩余信息防护	1
	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	2
安全管理机构	岗位设置	3
	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
	安全方案设计	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
	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	3
	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

（四） 测评指标

1、技术要求

技术要求分类体现了从外部到内部的纵深防御思想。对等级保护对象的安全防护应考虑从通信网络到区域边界再到计算环境的从外到内的整体防护，同时考虑对其所处的物理环境的安全防护。对级别较高的等级保护对象还需要考虑对分布在整个系统中的安全功能或安全组件的集中技术管理手段。

1）安全物理环境

安全通用要求中的安全物理环境部分是针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、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、电力供应和电磁防护。

2）安全通信网络

安全通用要求中的安全通信网络部分是针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网等；涉及的安全控制点包括网络架构、通信传输和可信验证。

3）安全区域边界

安全通用要求中的安全区域边界部分是针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

4）安全计算环境

安全通用要求中的安全计算环境部分是针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、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、数据备份与恢复、剩余信息保护和个人信息保护。

5）安全管理中心

安全通用要求中的安全管理中心部分是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理。涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

2、管理要求

管理要求分类体现了从要素到活动的综合管理思想。安全管理需要的“机构”、“制度”和“人员”三要素缺一不可，同时还应对系统建设整

改过程中和运行维护过程中的重要活动实施控制和管理。对级别较高的等级保护对象需要构建完备的安全管理体系。

1）安全管理制度

安全通用要求中的安全管理制度部分是针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

2）安全管理机构

安全通用要求中的安全管理机构部分是针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

3）安全管理人员

安全通用要求中的安全管理人员部分是针对人员管理模式提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

4）安全建设管理

安全通用要求中的安全建设管理部分是针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、安全产品

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、系统交付、等级测评和服务供应商管理。

5）安全运维管理

安全通用要求中的安全运维管理部分是针对安全运维过程括环境管理、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、应急预案管理和外包运维管理。

二、安全和风险管理方案

（一）风险管理制度

概述

风险管理(Risk Management，RSKM)过程的目的在于识别潜在的问题，以便策划处理风险的活动（识别、分析评估和缓解）和在必要时在整个项目生存周期中实施这些活动，缓解不利的影响，实现项目目标。

本规范建立组织级的风险管理策略，定义风险参数。项目经理依据本规范在测评项目策划阶段进行风险识别、风险评估以及制定风险缓解措施。在项目的生命周期内，依照风险管理规范的要求持续地识别、评估、监控和缓解风险，确保有效地抵御或缓解具有关键影响的风险。

适用范围

适用于公司所有测评项目的风险管理过程。

角色与职责

角色	职责
项目经理	负责项目的风险管理，策划风险管理活动 在项目中识别风险，分析、评估风险，制定缓解措施和应急措施 跟踪监控风险的发生，及时采取缓解措施 当风险发生时，转入问题管理过程 必要时启动应急措施
项目组成员	识别、提出风险 协助项目经理处理风险 跟踪所负责的风险，及时采取缓解措施
部门经理	及时了解项目中高级别的风险以及缓解措施 提供风险管理所需的资源。

开启准则

当项目启动时或项目进入新的里程碑阶段时，项目经理依照风险管理过程，负责组织对项目进行风险识别。

输入

新建测评项目

项目立项过程和策划过程中所产生的信息，是新建项目风险管理过程的输入，应当成为风险识别的基础和依据。

在测项目

项目监督和控制过程中所产生的信息，是在测试项目进入新里程碑阶段时风险管理过程的输入，应当成为风险识别的基础和依据。

有效的风险管理是为了尽量减小风险对项目的影响，而有系统地进行策划，以防止或缓解风险。包括：在项目策划过程中，与干系人合作，尽早识别风险，分析和评估风险影响，制定风险缓解措施；在项目监督和控制过程中，处理已识别的风险，在必要时实施风险缓解计划，并持续识别、评估风险，针对新识别的风险制定缓解措施。

主要活动

风险识别

项目经理负责在项目启动时和项目生命周期内，定期组织进行风险识别，确定会对项目进度、成本和质量构成不利影响的风险来源，以及风险产生的条件，对风险特征和可能造成的后果进行描述。

进行风险识别的目的，是找出可能导致费用超支、进度推迟或性能降低等影响项目目标实现的潜在问题，建立《项目风险管理报告》。

《项目风险管理报告》应定期审查，重新检查可能的风险来源和调整风险产生的条件，以便于进一步发现尚未被识别的风险。

常用的风险识别方法包括以下几种：

类比法

类比法是指，通过获取《风险数据表》，和已实施的类似项目的《项目风险管理报告》所积累的风险数据，系统化、规范化的识别风险。

《风险数据表》应按类别对所有与项目有关且可能发生的风险进行描述，帮助项目经理集中识别常见的、已知的和可预测的风险，如产品规模风险、人力资源风险、需求风险、管理风险及技术风险等。同时《风险数据表》应针对每个风险提出相应的缓解措施建议，指导项目经理制定项目风险缓解措施。

项目组根据本项目的特点，获取类似项目的《项目风险管理报告》，结合组织财富库中《风险数据表》的内容进行完善后，形成本项目的《项目风险管理报告》。

风险评估

项目经理负责运用风险参数（风险概率、风险影响、风险值等）对每个已识别风险进行评价和分类，并确定其优先级。

风险评估应采用定量风险分析方法，对风险的发生概率和风险的影响进行分析，计算出风险值（风险值＝风险概率*风险影响），再根据风险值排定风险的相对优先顺序。同时，还应确定风险阈值（控制点），以便明确风险的可接受度或不可接受度。

风险参数

风险概率

风险概率指的是风险实际发生的可能性。在实际应用中，可以用自然语言来表达数字概率范围。

下表列出了五段概率分级体系中自然语言和数字概率范围的映射关系。在计算风险概率时，用来计算的概率值等于概率范围的中间值取整。

概率范围	用来计算的概率值	自然语言表达
1%至 20%	10%	非常不可能
21%至 40%	30%	不太可能
41%至 60%	50%	一半一半
61%至 80%	70%	可能
81%至 99%	90%	几乎肯定

风险影响

风险的影响通过设置五级风险影响等级值来衡量。通过风险发生后对项目目标（成本增加、进度增加和技术方面）的影响程度进行判断。

等级	风险影响值	成本增加	进度增加	技术影响
低	1	低于 1%	<1 周或<1%	对性能有轻微影响
中	2	低于 5%	<2 周或<5%	对性能有中等影响
较高	3	低于 10%	<0.5 月或<10%	对性能有较大影响
很高	4	低于 20%	<1 月或<20%	对性能有严重影响
危急	5	超过 20%	超过 1 月或 >20%	可能无法完成任务

如果对成本、进度和技术多方面都有影响，先分别从多方面判断风险影响值，最终取多个值中的最大值。

风险值

风险值＝风险概率*风险影响

风险阈值

风险阈值是风险的控制点，对于达到该阈值的风险，需要制定风险缓解措施。

风险阈值定义为 1.5。

项目的风险评估

项目经理应根据风险参数中定义的评价原则，对《项目风险管理报告》中的每一个风险进行评估，确定风险的概率、风险影响并计算风险值。

项目风险排序

项目经理负责对项目风险排列优先顺序。风险优先级的排序原则为：风险值高者优先，风险值相同时风险概率高者优先。

排列优先顺序的目的在于，将资源有效运用在缓解对项目影响最大的风险上。根据风险排序优先级由高到低，引导项目组进行风险管理工作。

风险排序结果应包括风险编号、风险描述、提出人、可能发生阶段、风险概率、风险影响、风险值等，并立即更新到《项目风险管理报告》中。风险排序将成为风险缓解阶段的主要输入。

风险缓解

风险缓解是针对那些对项目来说最重要的风险（风险值达到风险阈值）

拟订风险缓解措施的过程。项目经理负责根据风险评估的结果，针对重要的风险拟订风险缓解措施。

对于风险值达到“风险阈值”的每一个风险，项目经理应当制定风险缓解计划，包括：缓解方式、缓解措施、责任人等。

缓解方式包括风险规避、风险转移、风险接受、风险减弱。

在制定风险缓解措施时，项目经理可参照组织的《风险数据表》，优先保证高优先级风险的缓解措施所需要的资源。对于优先级排名前三位的风险，项目经理应判断是否要制定应急措施，以便在风险发生时及时应对。

高优先级的风险可以考虑制定多个缓解措施，在进行多种缓解措施选择时，需要引用《决策分析和决定过程》。

在制定项目总体成本计划时应考虑风险管理的成本。风险缓解措施应记录在《项目风险管理报告》中，成为风险监控阶段的主要输入。

风险监控

项目经理负责在项目管理过程中定期监督每个风险的状态，并在适当时实施风险缓解措施。风险监控的输出应当包括风险缓解措施以及更新的风险管理报告。

风险管理是一个连续的过程，因此在项目实施过程中需要遵循预先制定的计划定期监督风险和风险缓解措施的状态和执行结果。风险应从三个方面进行监控：

监控风险的状态

项目经理负责监控风险的状态并对风险缓解措施的执行情况进行跟踪，

将风险状态和缓解措施执行情况记录于《项目风险管理报告》。

风险状态包括：

- 风险被缓解，关闭。
- 风险已发生，转入问题管理，关闭。
- 监控中，缓解措施正在实施。
- 监控中。
- 新识别风险。
- 风险触发条件已不存在。

缓解措施执行情况包括：

- 正在执行。
- 已执行。
- 更新缓解措施。

应急措施的执行

当风险发生时，项目经理应将其转入项目问题管理过程，遵循《项目监督和控制过程》进行问题跟踪。在高级别风险发生后，项目经理应及时上报高层分管领导，执行应急措施。

风险持续管理

项目经理负责对项目进行持续地风险识别、评估、缓解和监控工作，并将输出结果更新到《项目风险管理报告》中。

输出

- 《项目风险管理报告》

- 《风险数据表》

终止准则

项目结项完成。

（二）风险管理流程图

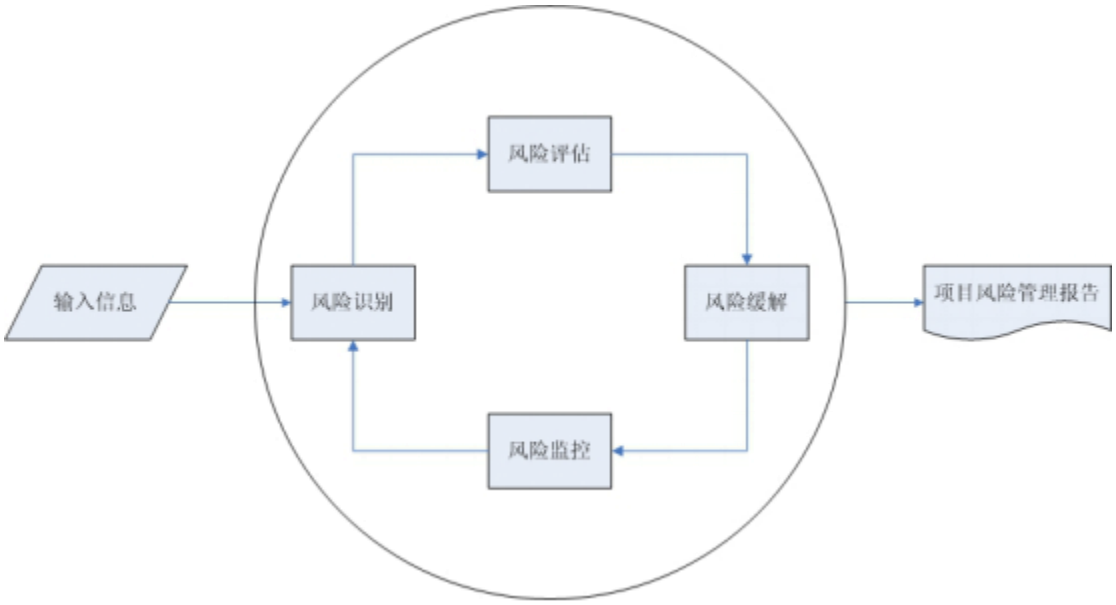


图 1:风险管理示意图

（三）项目验收

安全服务项目验收将在项目完成后召开项目验收会议，由项目双方的负责人员共同参加。

1）召开项目验收会议

项目验收会议应在项目结束一周内举行，由项目双方的负责人及验收组成员共同参加。

2）项目验收合格定义

本次等级测评项目在满足以下条件后，视为验收合格

（1）被测系统方书面证明本次等级测评活动未对被测方系统造成影响，系统仍然正常运行。

（2）测评机构提供被测评系统的按照公安部格式编写的等级测评报告，并附带系统整改建议书。

3）应提交的文件

本次项目所涉及的等级保护测评报告及系统整改建议书。

4）双方签署验收报告

验收结束后，由双方项目负责人签署验收报告

三、项目质量控制保证

（一）项目质量保障内容

为有效保障等级保护测评工作的质量，防止发生质量异常，提升效率，确保质量满足客户需求，我公司将测评质量监督管理纳入公司总体质量管理体系，由公司法人代表授权等级测评质量主管与质量部门对测评的质量进行控制，其主要职责如下：

1）全面领导等保测评的质量管理工作，监督执行有关等保测评必须遵循的各种政策、法律法规，并传达法律法规对测评工作的重要性；

2）对等保测评的质量和质量管理工作全面负责，确保开展工作的各种资源；

3）负责主持特定质量方针、质量目标，并确保质量管理体系得以完善和有效运行；

4）主持质量管理体系的策划、建立，并完善实现等保测评工作的质量方针、质量目标所必须的组织机构，确保质量部门各类人员的职责和权限得到规定与沟通；

5）主持管理评审和质量工作会，定期总结分析质量体系运行情况，不断改进完善；

6）负责组织对等保测评过程文档进行审核评估，批准签发《等级测评报告》

记录控制：

1）开展测评工作的各项目组执行《等级保护测评项目质量监督管理制度》对质量管理体系所需的质量记录予以控制，并保持、维护有效的质量记录，以证明符合各项要求及质量管理体系得到有效运行。

2）《项目质量监督管理制度》规定了质量记录的鉴别、储存、调阅、保护、保存期限及作废处理办法和程序。

测评过程的质量监督管理：

由各项目组负责对等保测评项目的被测系统的详细情况进行分析，为实施测评做好文档及测试工具，从而完成测评项目的测评准备过程活动；进入测评实施过程活动后开发与被测信息系统相适应的测评内容及实施方法，为测评实施提供最基本的文档和指导方案；在测评实施活动过程中，按照测评方案的总体要求，分步实施所有测评项目，包括单项测评和系统整体测评两个方面，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；最后进入分析与报告编制过程，综合评价被测信息系统保护状况，并形成测评报告文本。整个测评活动应与质量管理体系的其他要求相一致，质量主管与部门同步对测评活动的以下各项目进行监督管理：

1）根据被测评单位要求/相关的质检规范、国标、法律法规要求，确定有关工程的质量目标及要求；

2）了解客户的等级保护测评需求，编制《项目计划书》，全面满足被测评单位要求。

3）根据等级保护测评相关法规和技术标准的要求针对测评过程，策划并实施各项验证、确认、访谈、检验等测评活动，留下相关的记录。

4）对各项测评过程及测评验收提供所需的记录，规划结果必须以测评报告的形式输出。

➢ 对测评活动中输入输出的各类作业指导书、记录表单、报告及选取的测评设备必须进行评审，确保其准确和稳定。并做相应的验证及分析。

➢ 输入包括：功能和性能的要求；适用的法律法规要求；成熟的作业指导书；

➢ 对所有的输入进行评审：确保输入是充分的，适宜的，要求不可自相矛盾，完整，清楚；

➢ 保证测评活动中的各类输出记录的完整性和准确性；

➢ 针对测评输入进行验证，并在放行前得到被测评单位批准；

针对测评输出（如测评记录和测评报告）进行评审，通过审批后方可提交客户。

（二）安全保障原则

整体性原则

要求在网络发生被攻击、破坏事件的情况下，必须尽可能地快速恢复网络信息中心的服务，减少损失。因此，信息安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。

有效性与实用性原则

不能影响系统的正常运行和合法用户的操作活动。网络中的信息安全和信息共享存在一个矛盾：一方面，为健全和弥补系统缺陷或漏洞，会采取多种技术手段和管理措施；另一方面，势必给系统的运行和用户的使用造成负担和麻烦，尤其在网络环境下，实时性要求很高的业务不能容忍安全连接和安全处理造成的时延和数据扩张。如何在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户记忆、存储工作和安全服务器的存储量、计算量，应该是一个信息安全设计者主要解决的问题。

安全性评价与平衡原则

对任何网络，绝对安全难以达到，也不一定是必要的，所以需要建立合理的实用安全性与用户需求评价与平衡体系。安全体系设计要正确处理需求、风险与代价的关系，做到安全性与可用性相容，做到组织上可执行。评价信息是否安全，没有绝对的评判标准和衡量指标，只能决定于系统的用户需求和具体的应用环境，具体取决于系统的规模和范围，系统的性质和信息的重要程度。

标准化与一致性原则

系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，这样才能确保各个分系统的一致性，使整个系统安全地互联互通、信息共享。

技术与管理相结合原则

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。

统筹规划，分步实施原则

由于政策规定、服务需求的不明朗，环境、条件、时间的变化，攻击手段的进步，安全防护不可能一步到位，可在一个比较全面的安全规划下，根据网络的实际需要，先建立基本的安全体系，保证基本的、必须的安全性。随着今后随着网络规模的扩大及应用的增加，网络应用和复杂程度的变化，网络脆弱性也会不断增加，调整或增强安全防护力度，保证整个网络最根本的安全需求。

等级性原则

等级性原则是指安全层次和安全级别。良好的信息安全系统必然是分为不同等级的，包括对信息保密程度分级，对用户操作权限分级，对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、链路层等），从而针对不同级别的安全对象，提供全面、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

动态发展原则

要根据网络安全的变化不断调整安全措施，适应新的网络环境，满足新的网络安全需求。

易操作性原则

首先，安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

自主和可控性原则

网络安全与保密问题关系着一个国家的主权和安全，所以网络安全产品不可能依赖于从国外进口，必须解决网络安全产品的自主权和自控权问题，建立我们自主的网络安全产品和产业。同时为了防止安全技术被不正当的用户使用，必须采取相应的措施对其进行控制，比如密钥托管技术等。

权限分割、互相制约、最小化原则

在很多系统中都有一个系统超级用户或系统管理员，拥有对系统全部资源的存取和分配权，所以它的安全至关重要，如果不加以限制，有可能由于超级用户的恶意行为、口令泄密、偶然破坏等对系统造成不可估量的损失和破坏。因此有必要对系统超级用户的权限加以限制，实现权限最小化原则。管理权限交叉，有几个管理用户来动态地控制系统的管理，实现互相制约。对于普通用户，则实现权限最小原则，不允许其进行非授权以外的操作。

四、安全培训方案

截止到 2018 年近 75%的网络安全时间发生的根本原因是来自于内部员工操作不规范、不好的行为习惯疏忽大意等造成的。没有网络安全就没有国家安全，人的安全是企业安全的最后一道防线，培养企业全员网络信息安全意识刻不容缓。

通过培训、工具检测、题目检测等方式来提高企业员工安全意识，帮助企业打造网络安全生态，建立完善的企业安全管理制度；建立企业员工对网络安全的正确认识与企业规范的管理制度，帮助企业规范员工日常行为，使员工深刻认识网络安全的重要性，并按照制度进行工作；从安全角度培养企业员工网络安全素质，提升企业整体安全水平，是企业安全防护能力在现有基础上得到提升，持续良性发展，避免不必要的损失。

五、人员保密管理

项目组人员应自觉遵守保密法规制度，知悉应当承担的保密义务和法律责任，并作出以下承诺：

一、认真遵守国家保密法律、法规和规章制度，履行保密义务；

二、认真遵守本人工作单位与测评委托方签订的保密协议；

三、认真遵守测评委托方其他各项安全保密的相关协议；

四、对参与的信息化项目和服务所涉及技术资料和数据信息履行保密义务，未经允许不得擅自发表或使用；

五、离岗时，对仍具有保密性的技术资料和数据信息履行保密义务。

六、合理化建议评价

（一）整改建议方案设计目的

本整改建议方案设计的目的是在其系统定级、等级差距测评结果的基础上，按照国家对信息系统网络安全等级保护的相关建设规范和技术要求，结合测评委托方受评的信息系统的真实情况和具体需求，设计一套完善、全面、合规的整改方案，保证测评委托方受评的信息系统在按照整改方案进行合规性整改后，可顺利通过当地网监的测评和备案，达到信息系统相应等级的等保要求。

（二）整改方案设计原则

依照国家对信息系统网络安全等级保护的相关建设规划和技术要求，在其整改方案设计中应当遵循以下的原则：

1）适度安全原则

任何信息系统都不能做到绝对的安全，在进行信息系统的安全等级保护整改规划中，要在安全需求、安全风险和安全成本之间进行平衡和折中，过多的安全要求必将造成安全成本的迅速增加和运行的复杂性。

适度安全也是等级保护建设的初衷，因此在进行等级保护设计的过程中，一方面要严格遵循基本要求，从技术和管理两个层面加强防护措施，保障信息系统的机密性、完整性和可用性，另外也要综合成本的角度，针对受评的信息系统的实际风险，提出对应的保护强度，并按照保护强度进

行安全防护系统的设计和建设，从而有效控制成本。

2）重点保护原则

在整改方案设计中，应根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

3）技术管理并重原则

网络安全问题从来就不是单纯的技术问题，把防范黑客入侵和病毒感染理解为网络安全问题的全部是片面的，仅仅通过部署安全产品很难完全覆盖所有的网络安全问题，因此必须要把技术措施和管理措施结合起来，更有效的保障受评的信息系统的整体安全性，形成一个技术和管理并重的系统整改方案。

4）分区分域建设原则

对信息系统进行安全保护的有效方法之一就是分区分域，由于信息系统中各个信息资产的重要性是不同的，并且访问特点也不尽相同，因此需要把具有相似特点的信息资产集合起来，进行总体防护，从而可更好地保障安全策略的有效性和一致性，比如把业务服务器集中起来单独隔离，然后根据各业务部门的访问需求进行隔离和访问控制；另外分区分域还有助于对网络系统进行集中管理，一旦其中某些安全区域内发生安全事件，可通过严格的边界安全防护限制事件在整网蔓延。当然，分区分域建设还需结合适度安全原则进行综合考虑，对整个架构较为简单的信息系统，需分析分区分域建设的必要性。

5）标准性原则

信息系统网络安全建设是非常复杂的过程，在设计信息系统时，进行安全体系规划中单纯依赖经验，是无法对抗未知的威胁和攻击，因此需要遵循相应的安全标准，从更全面的角度进行差异性分析。在整改方案设计方面，应重点考虑设计架构的合规性、参考依据的合规性、需求分析的合规性、设计思路的合规性、整改内容的合规性和产品选用的合规性。

6）动态调整原则

网络安全问题不是静态的，它总是随着管理相关的组织策略、组织架构、信息系统和操作流程的改变而改变，因此必须要及时跟踪信息系统的变化情况，调整安全保护措施。

7）成熟性原则

整改方案设计中所采用的安全措施和安全产品，在技术和管理上都应是可行、可靠、成熟的，应是被检验确实能够解决安全问题并在很多项目中有成功应用的。

8）客观性原则

整改方案设计应建立在之前完成的信息系统等级保护合规性测评和差距分析的基础上，设计方应遵循客观性原则对整个信息系统进行客观、直接的评价。因此整改方案所设计的安全措施和安全策略一方面能够符合国家信息系统等级保护的相关要求，另一方面又能够很好地解决受评的信息系统中真实存在的各类安全问题，满足其特性需求。