网络安全等级保护测评服务

融安云网（北京）技术有限公司
2020年

等保测评发展历程

信息安全等级保护是基本制度、基本国策、基本方法

- 信息安全等级保护是党中央国务院决定在信息系统安全领域实施的基本国策
- 信息安全等级保护是国家信息安全保障工作的基本制度
- 信息安全等级保护是国家信息安全保障工作的基本方法

起步阶段

中华人民共和国计算机信息系统安全保护条例 (1994年2月18日中华人民共和国国务院令147号发布)

→ 2003年9月中办国办颁发《关于加强信息安全保障工作的意见》（中办发[2003]27号）

→ 2004年11月四部委会签《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）

→ 2005年9月国信办文件《关于转发《电子政务信息安全等级保护实施指南》的通知》（国信办[2004]25号）

发展阶段

→ 2006年1月四部委会签《关于印发《信息安全等级保护管理办法的通知》（公通字[2006]7号）

→ 2007年6月公安部、保密局、国密局、国信办联合印发《信息安全等级保护管理办法》（公通字[2007]43号）

→ 2007年7月《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）

↓

2008年发布GB/T 22239—2008《信息系统安全等级保护基本要求》、GB/T 22240—2008《信息系统安全等级保护定级指南》

→ 2009年公安部发文《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）

→ 2010年3月公安部发文《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[303]号）

推行阶段

→ 2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》。

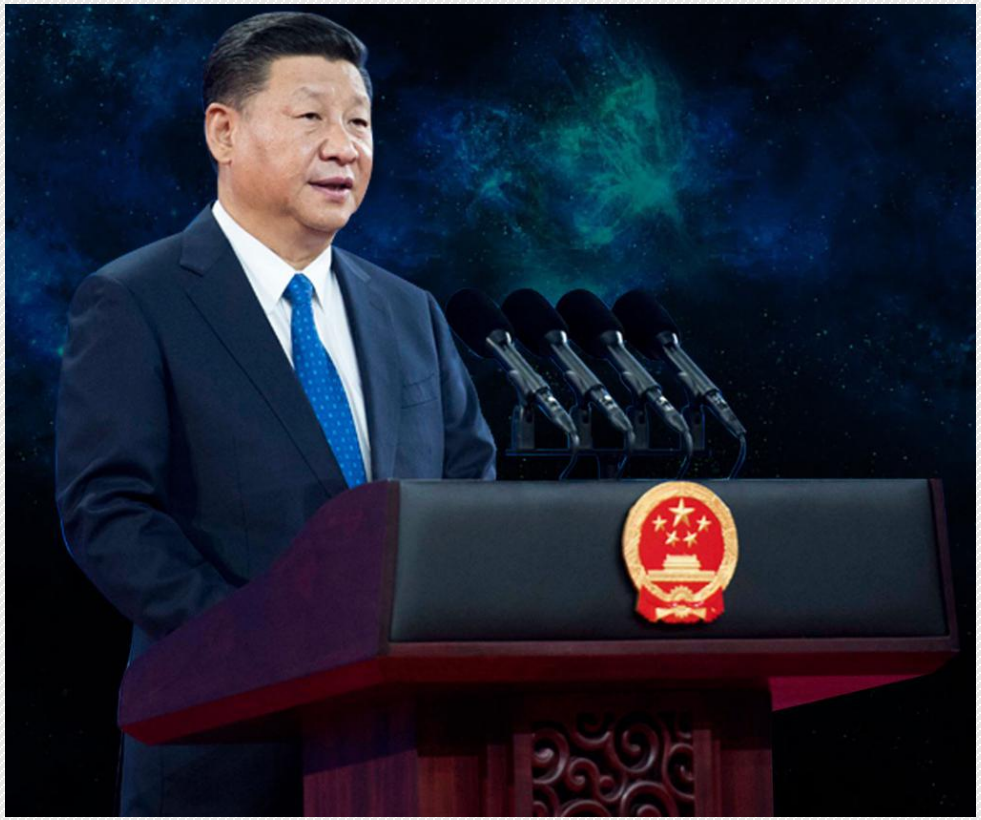
分水岭

→ 2016年6月1日起开始实施《中华人民共和国网络安全法》，在网络安全法里面明确提出等保的条款有：第二十一条、第三十八条、第五十九条大家需要重点关注一下。

新等保阶段

→ 等保2.0

《网络安全法》带动信息安全上升到国家战略高度



习主席4·19讲话

“没有网络安全，就没有国家安全”

网络安全法

2.0 网络安全等级保护条例（征求意见稿）
等保2.0

关键信息基础设施保护条例

安全影响面更广

安全建设深入各行各业，各种场景

关基重点保护

关键基础设施实行重点保护

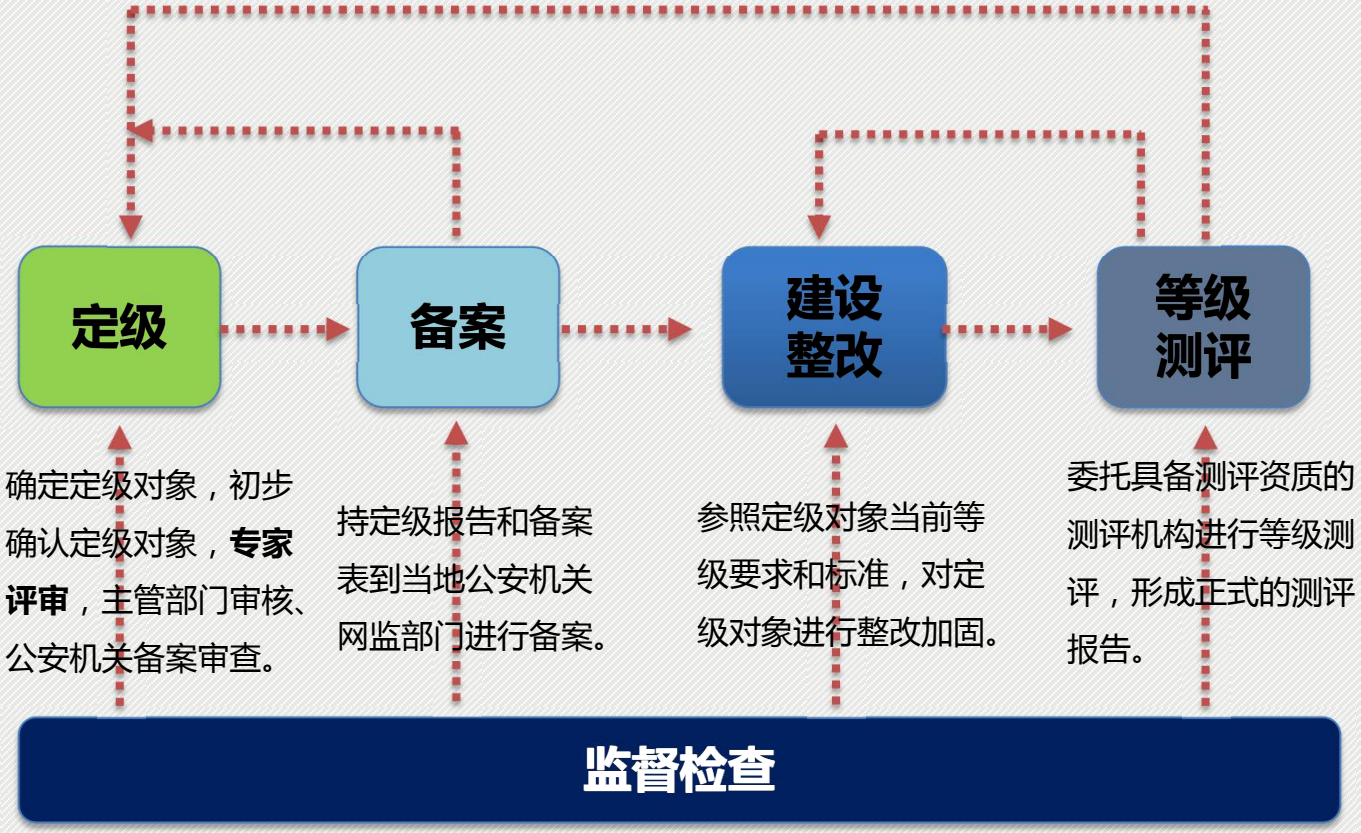
网络安全等级保护测评
重大意义

满足合法合规要求，清晰化责任和工作方法，让安全贯穿全生命周期

提高人员安全意识，树立等级化防护思想，合理分配网络安全投资

明确组织整体目标，改变以往单点防御方式，让安全建设更加体系化

等级保护2.0主要工作流程



向当地公安机关网监部门提交测评报告，配合完成对网络安全等级保护实施情况的检查。

项目流程	涉及角色及分工
定级	【咨询服务机构、用户】 完成定级报告 【专家组】 定级评审
备案	【咨询服务机构、用户、网安】 完成备案工作，取得备案证明
建设整改	差距评估 【咨询服务机构、用户】 完成标准与现状的差距分析，提出整改建议
	方案设计 【咨询服务机构、用户】 设计整改方案，整改实施方案
	整改实施 【咨询服务机构、用户和集成商】 完成部署实施、加固整改
等级测评	【咨询服务机构、用户】配合用户顺利完成测评 【测评机构】开展信息系统测评工作
监督检查	【网安】定期检查或重保抽查

等级保护2.0定级要求解析

定级要求 | 新增定级流程 | 定级对象

原标准

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

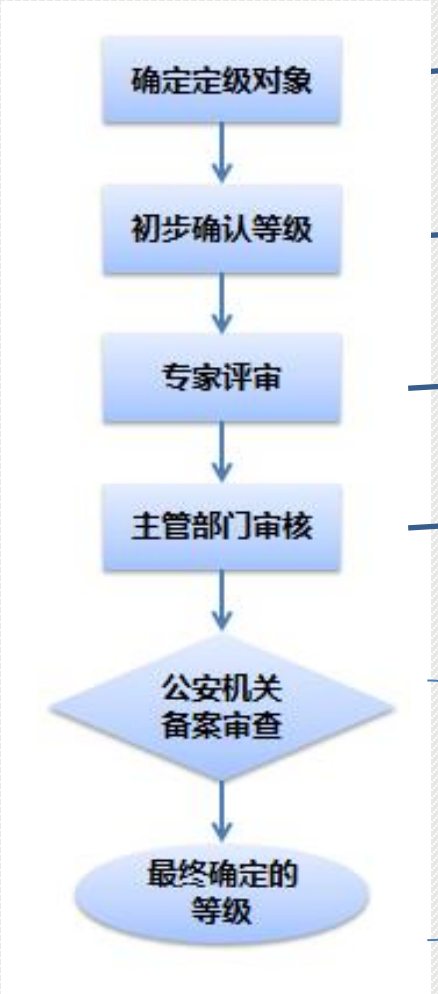
新标准

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

等级保护2.0定级要求解析

定级要求 | 新增定级流程 | 定级对象

② 新增“定级流程”



包括基础信息网络、工业控制系统、云计算平台、物联网、其他信息系统、大数据等。

包括确定受侵害的客体、侵害对客体的侵害程度以及综合判定侵害程度。

定级对象的运营、使用单位应组织信息安全专家和业务专家，对初步定级结果的合理性进行评审，出具专家评审意见。

定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核。

定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营使用单位应组织重新定级；审查通过后最终确定定级对象的安全保护等级。

等级保护2.0定级要求解析

③ 定级对象

- **重新对定级对象进行调整，并进行相应的介绍。2.0定级对象分为基础信息网络、信息系统和其他信息系统，其中信息系统再细分为工业控制系统、物联网、大数据、移动互联以及云计算平台。**

1.0要求

信息系统

~~一个单位内运行的信息系统可能比较庞大，为了体现重要部分重点保护，有效控制信息安全建设成本，优化信息安全资源配置的等级保护原则，可将较大的信息系统划分为若干个较小的、可能具有不同安全保护等级的定级对象。~~

2.0要求

工业控制系统

工业控制系统主要由生产管理层、现场设备层、现场控制层和过程监控层构成，其中：生产管理层的定级对象确定原则见(其他信息系统)。设备层、现场控制层和过程监控层应作为一个整体对象定级，各层次要素不单独定级。

对于大型工业控制系统，可以根据系统功能、控制对象和生产厂商等因素划分为多个定级对象。

物联网

物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。

采用移动互联技术的信息系统

采用移动互联技术的等级保护对象应作为一个整体对象定级，主要包括移动终端、移动应用、无线网络以及相关应用系统等。

大数据

应将具有统一安全责任单位的大数据作为一个整体对象定级， 或将其与责任主体相同的相关支撑平台统一定级。

云计算平台

在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级， 云租户侧的等级保护对象也应作为单独的定级对象定级。

对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

基础信息网络

对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。

跨省全国性业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

其他信息系统

作为定级对象的其他信息系统应具有如下基本特征：

a) **具有确定的主要安全责任单位**。作为定级对象的信息系统应能够明确其主要安全责任单位；

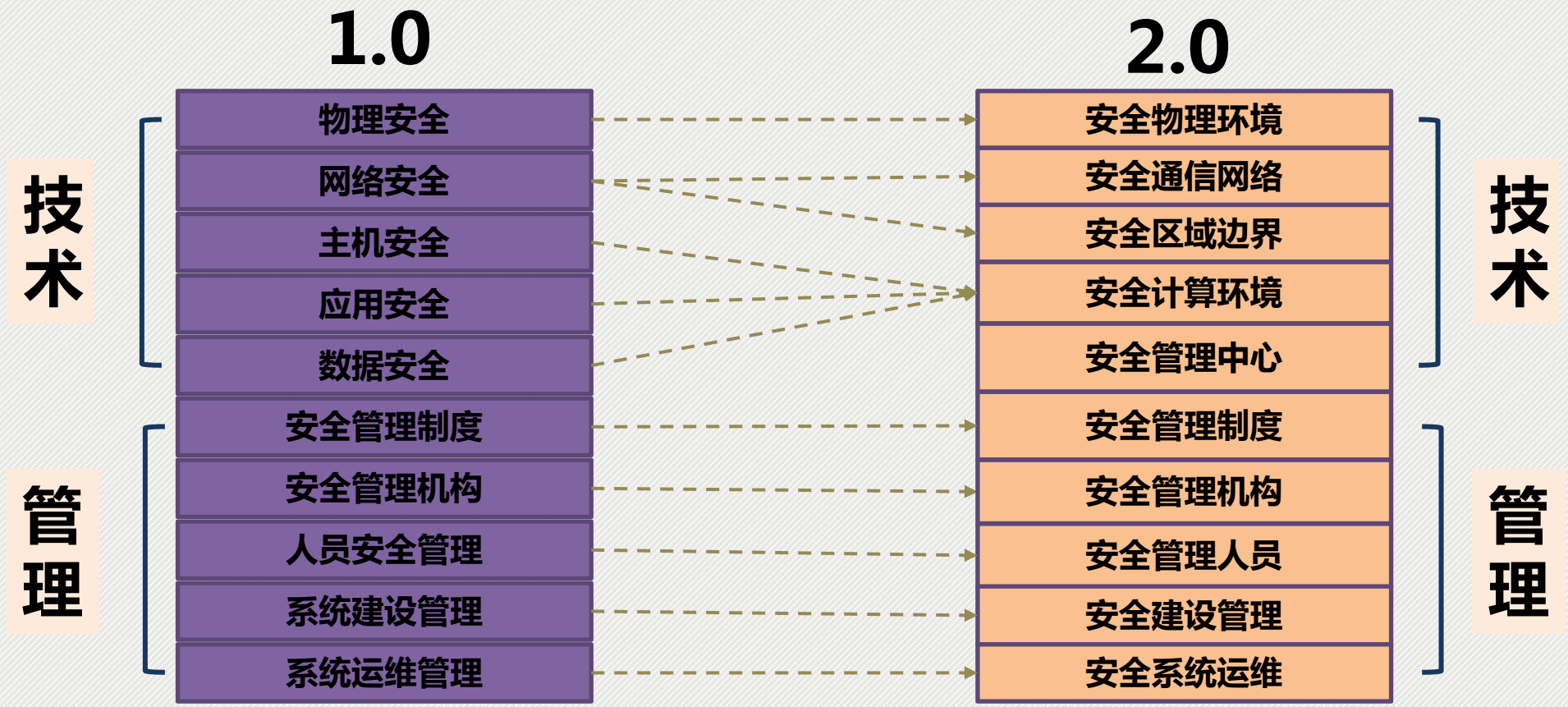
b) **承载相对独立的业务应用。** 作为定级对象的信息系统应承载相对独立的业务应用， 完成不同业务目标或者支撑不同单位或不同部门职能的多个信息系统应划分为不同的定级对象；

c) **具有信息系统的基本要素。** 作为定级对象的信息系统应该是由相关的和配套的设备、 设施按照一定的应用目标和规则组合而成的多资源集合，单一设备（如服务器、终端、网络设备等）不单独定级。

等级保护2.0通用要求解析

整体变化 | 技术 | 管理

□ 安全控制域划分上有较大变化，原有十个安全域重新整合为十个，定义上更精确，内涵更为丰富。



服务过程及交付物

准备阶段

1 系统定级

2 系统备案

- 提供定级服务，出具《信息系统详细描述文件》《信息系统定级报告》
- 协助客户按要求去公安机关办理定级备案手续，提交备案材料《信息系统安全等级保护备案表》

3 差距评估

- 通过访谈、审计、扫描、渗透等方式，对信息系统进行安全评估
- 针对信息系统的定级测评项提供差距分析，出具《信息系统安全等级差距分析报告》《信息系统安全整改建设方案》

建设阶段

4 安全建设

5 等级测评

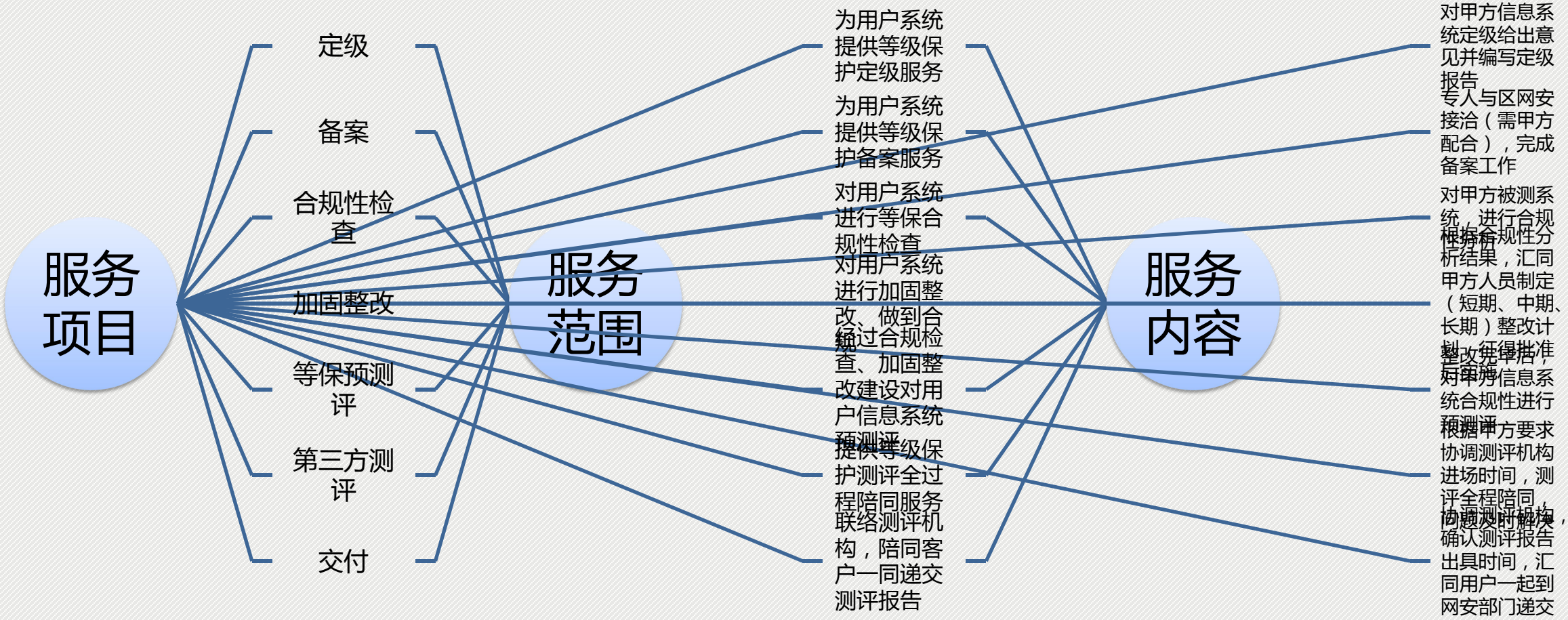
- 提供等级保护安全集成服务，根据《建设方案》提供采购建议，依据客户需求做安全设备上线，并统一配置策略
- 提供合作的等级测评机构备选，对结果负责

持续改进

6 检查监督

- 协助客户每年针对定级系统进行持续的内部评估和测评
- 提供安全攻防演练服务，协助客户针对安全事件做应急备案

服务内容范围


服务项目
定级
备案
合规性检查
加固整改
等保预测评
第三方测评
交付
服务范围
为用户系统提供等级保护定级服务
为用户系统提供等级保护备案服务
对用户系统进行等保合规性检查
对用户系统进行加固整改、做到合规
经过合规检查、加固整改建设对用户信息系统预测评
提供等级保护测评全过程陪同服务
联络测评机构，陪同客户一同递交测评报告
服务内容
对甲方信息系统定级给出意见并编写定级报告
专人与区网安接洽（需甲方配合），完成备案工作
对甲方被测系统，进行合规性分析
根据合规性分析结果，汇同甲方人员制定（短期、中期、长期）整改计划，征得批准后实施
整改完毕后，对甲方信息系统合规性进行预测评
根据甲方要求协调测评机构进场时间，测评全程陪同，协调测评机构
问题及时解决，确认测评报告出具时间，汇同用户一起到网安部门递交

服务阶段及内容交付

阶段划分及内容交付

安全评估阶段

资产调研	威胁分析	技术脆弱性评估	管理脆弱性评估	风险分析与风险评估
通过对系统信息资产进行调研，分析网络结构，进行业务影响的评估。	对系统可能面临的威胁进行分析	通过漏洞扫描、手工检查、渗透测试等技术手段对系统的技术脆弱性进行评估	通过现场访谈、问卷调查、策略审计等手段对系统的管理脆弱性进行评估	对前期获得的数据进行分析，为后期差距分析提供数据基础。

差距分析阶段

差距分析报告	整改方案	信息安全技术培训
依据等保等级要求对系统的差距进行分析，形成差距分析报告	依据等保等级要求及实际业务与安全需求，形成整改方案	对整改可能设计的安全技术和产品进行培训

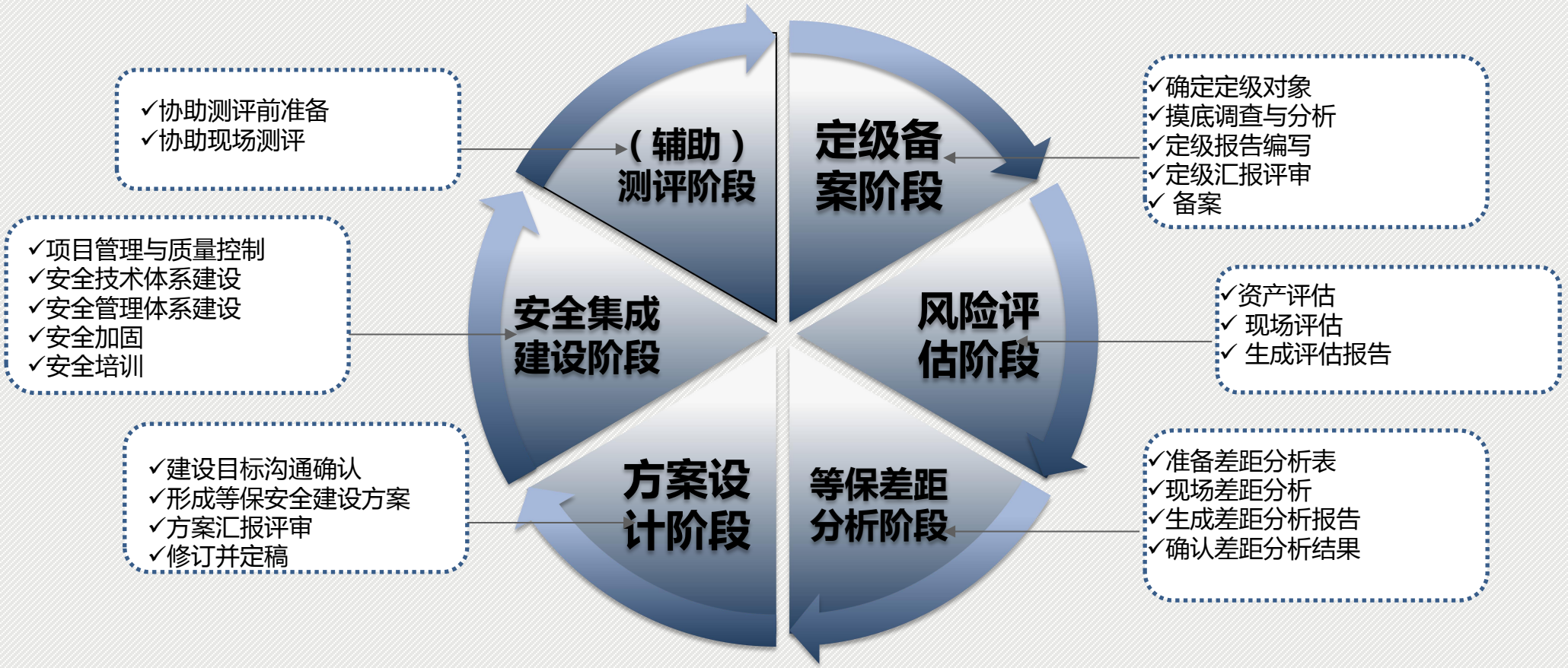
整改实施阶段

整改自检
依据要求对整改后系统进行自检，确保通过测评

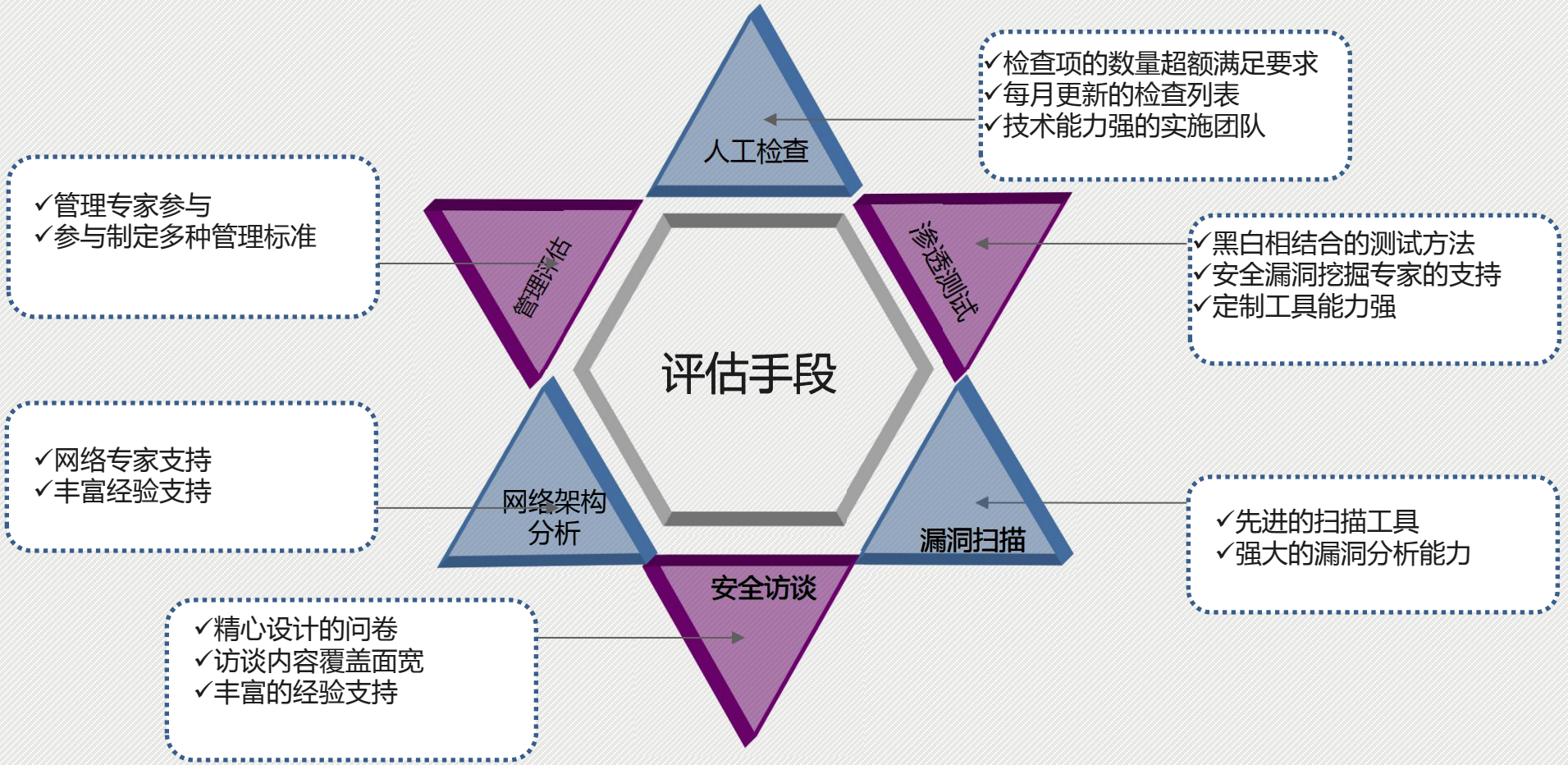
测评阶段

预测评	第三方测评
依据等保要求，进行合规性检查和预判	邀请第三方测评机构对系统进行测评， 协助通过等保三级测评

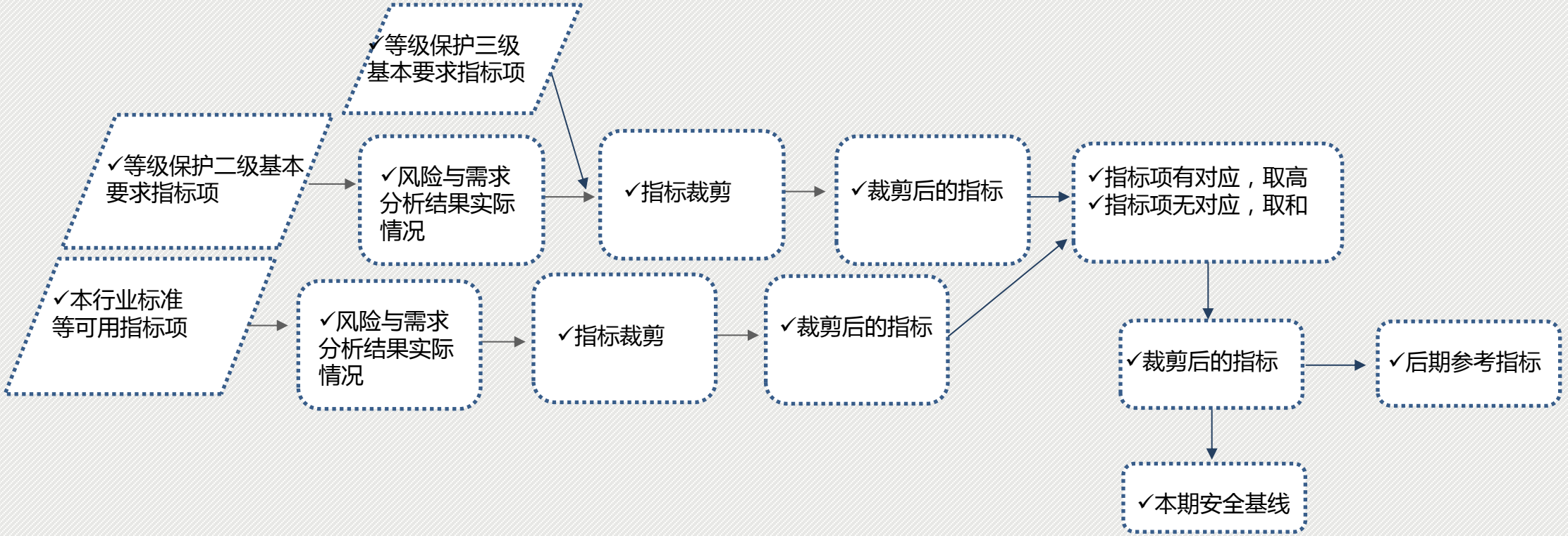
咨询服务内容-实施阶段


✓协助测评前准备
✓协助现场测评
（辅助）测评阶段
定级备案阶段
✓确定定级对象
✓摸底调查与分析
✓定级报告编写
✓定级汇报评审
✓ 备案
✓项目管理与质量控制
✓安全技术体系建设
✓安全管理体系建设
✓安全加固
✓安全培训
安全集成建设阶段
风险评估阶段
✓资产评估
✓ 现场评估
✓ 生成评估报告
✓建设目标沟通确认
✓形成等保安全建设方案
✓方案汇报评审
✓修订并定稿
方案设计阶段
等保差距分析阶段
✓准备差距分析表
✓现场差距分析
✓生成差距分析报告
✓确认差距分析结果

咨询服务内容-风险评估


评估手段
人工检查
渗透测试
漏洞扫描
安全访谈
网络架构分析
管理评估
✓检查项的数量超额满足要求
✓每月更新的检查列表
✓技术能力强的实施团队
✓黑白相结合的测试方法
✓安全漏洞挖掘专家的支持
✓定制工具能力强
✓先进的扫描工具
✓强大的漏洞分析能力
✓精心设计的问卷
✓访谈内容覆盖面宽
✓丰富的经验支持
✓网络专家支持
✓丰富经验支持
✓管理专家参与
✓参与制定多种管理标准

咨询服务内容-差距分析


✓等级保护三级基本要求指标项
✓等级保护二级基本要求指标项
✓本行业标准等可用指标项
✓风险与需求分析结果实际情况
✓风险与需求分析结果实际情况
✓指标裁剪
✓指标裁剪
✓裁剪后的指标
✓裁剪后的指标
✓指标项有对应，取高
✓指标项无对应，取和
✓裁剪后的指标
✓后期参考指标
✓本期安全基线

咨询服务内容-整改加固

等保项目实施阶段的主要工作：
1.差距部分的信息安全设备的采购建议与实施规划；
2.针对业务系统的安全漏洞修补建议；
3.安全加固，包括：操作系统、数据库、中间件、网络设备、安全设备等；
4.信息安全四级管理体系梳理、建设；
5.测评申请书以及相关测评资料准备；

咨询服务内容-协助测评

如何协助客户进行测评？
1.帮客户联系测评中心，并建立良好的商务关系；
2.帮助客户整理所有测评相关的资料；
3.现场测评时，作为客户方的工程师直接应对测评中心的测评师；
4.节约测评时间，提高测评通过率；

咨询服务内容-客户收益

客户收益？
1.根据客户企业实际情况，规划建设信息安全体系；
2.根据客户企业实际情况，合理选型产品；
3.为客户制定符合企业发展规划的整改计划（短期、中期、长期）；
4.为客户打造合规，安全；省事、省时、省力、省钱的解决方案；

服务优势

经验丰富

企业具有标准制定参与经历，对标准的理解更为充分。对等保测评环节有丰富指导经验，对等保整改有丰富的实践经验

方案贴合

大型案例众多，可为客户定制合规且保护客户投资的等保测评、安全规划及运行维护方案

实践广泛

在应用开发类、工程类项目的安全规划、体系建设及标准制定领域有长期实践

客户认可

多次参加公安部组织的护网行动，具有丰富的网络安全攻防经验

人才济济

具备专业稳定的信息安全人才体系，能为用户提供长期、专业、稳定的人才支持

谢谢聆听！