目录

1.1. 信息安全等级保护测评

信息安全等级保护，是对信息和信息载体按照重要性等级分级别进行保护，信息安全等级保护测评是依据相关标准，为党政机关、企事业单位信息系统提供安全等级符合性检查及综合风险评估服务，出具系统当前防护能力是否满足信息安全保护等级相关要求的测评结论和报告。

信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段。

测评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、主机系统 安全、应用安全和数据安全等五个层面。

◆**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等五个方面。

公司产品优势：

◆区域优势：兰科集团自 2005 年成立以来一直致力于公安行业产品研发及服务，目前在全国 16 个省，200 多个城市与当地公安管理部门建立合作，公安机关负责信息安全等级保护的监督、检测、指导等职责，等客户有等保相关需求时我公司能够更好的为客户提供区域服务。

◆服务优势：专业团队经验丰富、一对一咨询服务

1.2. 安全咨询

安全咨询，是针对企业或者政府的安全生产管理中存在的问题，安全管理专家从管理、技术、体制、机制提出的解决方案，融合发现问题、分析问题、解决问题。

依托深厚的知识体系和丰富的行业经验，依据国际/国内标准和行业监管规范，协助各行业客户立足于实际现状，面向信息安全风险，采取适当的管理过程和控制措施，建立和维护全面、有效、合规的信息安全管理体系，整体提升信息安全管理成熟度，保障业务运营和战略达成。安全咨询服务主要包含：

◆**信息系统安全风险评估服务**：对客户的重要信息系统，识别和评估信息资产的重要性、安全威胁的可能性、安全脆弱性的严重程度、以及安全控制措施的有效性等要素，对重要信息系统所面临的信息安全风险进行识别和定性评估，并

对所有评估发现的不可接受风险给出对应的安全处置和加固建议，协助客户提升对重要信息系统的安全风险管理和安全保障能力。

◆信息安全保障体系设计规划咨询服务：对于客户基于风险评估结果和监管合规要求，提出的信息安全保障体系设计规划需求，向客户提供专业咨询服务，立足于客户信息处理设施和信息安全管理现状，依据信息安全相关的国际/国内标准规范、协助客户建立信息安全保障的建设目标，选择和组合信息安全控制措施，完成信息安全保障体系架构设计，并合理规划信息安全保障体系的建设步骤和资源投入，最终达成有序提升信息安全风险管控能力，保障信息系统安全运营的目标。

◆信息安全管理体系建设咨询服务：对于客户关于信息安全管理体系（ISMS）的建设和认证需求，向客户提供专业咨询服务，参照国际标准 ISO27001、ISO27002、以及国内标准 GB/T22080、GB/T22081，按照 PDCA 的完整管理过程，确定体系实施范围、实施安全风险评估、选择和实施安全控制措施、编写与制订文档化的体系文件、完成信息安全管理体系的导入运行、实施信息安全管理体系评审和内部审核、推荐和选择体系认证机构并配合完成体系认证审核、培训客户方人员通过内审员认证，从而确保客户建立和维护完整、有效的信息安全管理体系，为客户关键业务运营提供充足的安全保障。

◆重要信息系统信息安全等级保护合规设计与建设咨询服务：参照国家等级保护标准 GB/T22239、GB/T22240 及行业等级保护标准要求，向客户提供重要信息系统信息安全等级保护合规建设过程的专业咨询服务，协助客户完成系统定级和备案、信息安全技术和管理体系设计和实施、以及等级保护测评等工作，确保客户方重要信息系统符合国家和行业关于信息安全等级保护的监管要求，具备足够的信息安全保障能力。

◆信息科技风险管理体系建设咨询服务：主要面向银行业客户提供专业咨询服务，依据人民银行和银监会的监管规范要求，协助银行业客户建立起职责分工明确的“三道防线”信息科技治理架构，以及全面、合规、有效的信息科技风险管控体系，内容范围涵盖信息科技治理、信息科技风险管理、信息科技外包管理、信息科技业务连续性管理、信息安全管理、信息开发与项目建设管理、信息系统运行维护管理、以及信息科技审计监督管理等八方面。通过管理制度、流程、过

程记录等正式文档化的成果交付，确保与信息科技风险管理有关的管理要求实现规范化和常态化落地执行，从而提升银行业客户的信息科技风险管控能力，为银行关键业务持续稳定运营提供保障。

1.3. 安全加固

安全加固服务是根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。其主要目的是：

◆消除与降低安全隐患。

◆周期性的评估和加固工作相结合，尽可能避免安全风险的发生。

1.网络设备安全加固：网络设备的加固主要是针对路由器、交换机系统的软硬件、配置、日志进行优化。网络设备主要包括 CISCO、华为、Juniper、NORTAL，此处以 CISCO 为例，主要加固项包括：Global 服务配置、Interface 服务配置、CDP 配置、Login Banner 配置、Enable secret 配置、Nagle 配置、Ident 配置、超时配置、访问控制配置、VTY 访问配置、用户验证配置、AAA 方式配置、路由命令审计配置、Ingress 和 Egress 路由过滤、Ingress 和 Egress 包过滤、Unicast RPF 配置、路由协议验证配置、CAR 配置、更多安全高级配置。

2.安全产品安全加固：安全产品会有很多种，比如防火墙、入侵检测系统、入侵保护系统、网闸等，这里以防火墙和入侵检测系统为例来说明：防火墙安全设置基本安装配置、访问控制配置、NAT 方式配置、透明方式配置、带宽管理配置、系统管理配置、软件升级配置、用户管理配置、认证配置、实时报警和入侵检测配置、日志分析配置、效率配置、防 DOS 攻击配置、高可靠性测试。入侵检测安全设置软件升级配置、后门测试、端口扫描攻击测试和优化、IWEB 攻击测试和优化、入侵检测系统效率配置和优化、DOS 攻击测试和优化、入侵检测系统高可靠性测试和优化。

3.操作系统安全加固：WINDOWS 系统升级系统补丁、升级病毒库、审计和账号策略、注册表安全设置、关闭不必要的安全服务。

LINUX

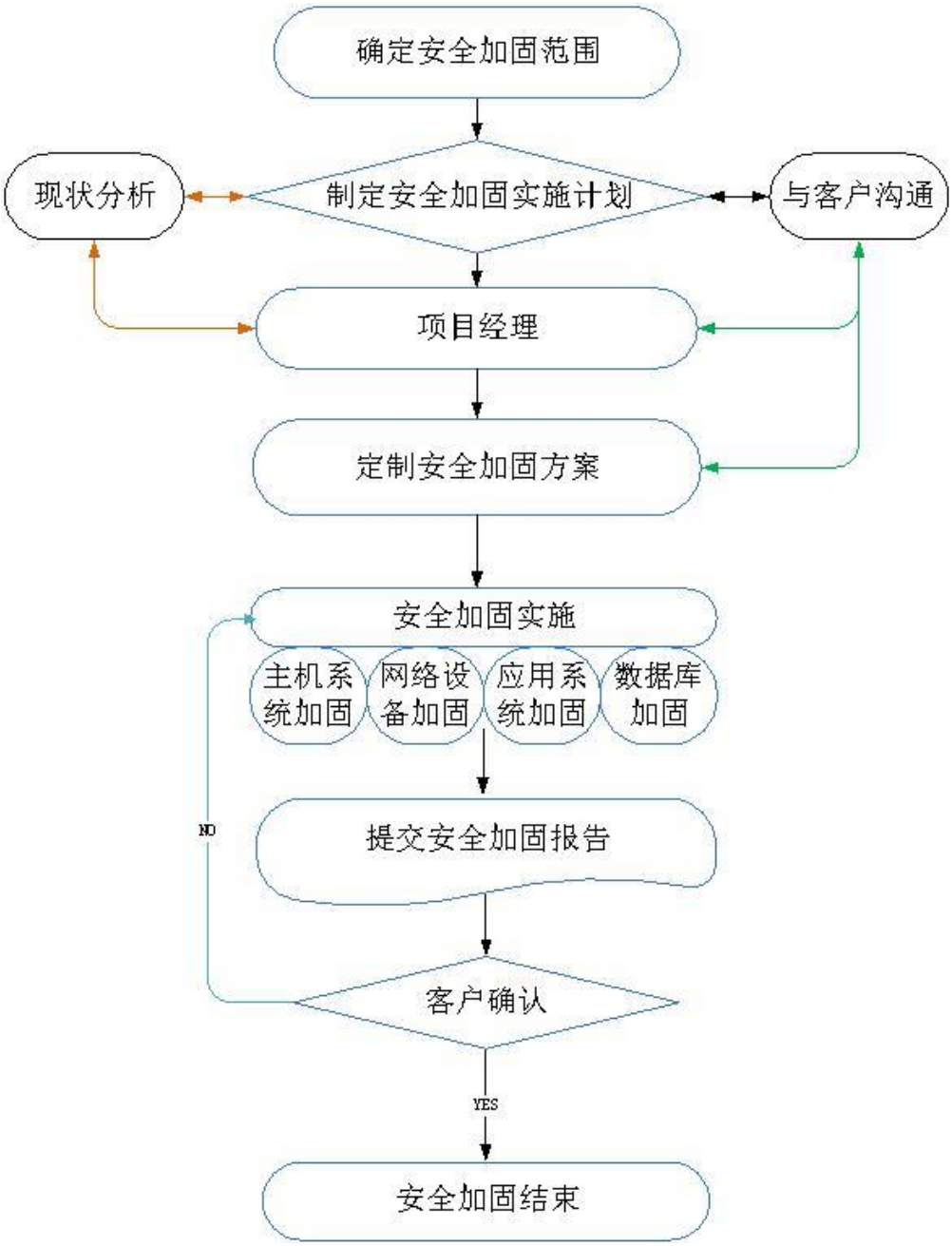
补丁和安装情况、Xinetd 启动的网络服务、不必要的服务、文件/目录控制、账户及环境、系统信任关系、其它安全配置。

AIX

补丁和配置、登录控制、用户、角色控制、密码控制、Inetd 启动的不必要服务、其它不必要服务、其它安全配置、HP-UNIX、补丁和其它软件安装、Inetd 启动的不必要服务、其它不必要服务、系统访问、认证和授权、日志、账户和环境、文件/目录控制。

SOLARIS

补丁安装情况、系统账户管理、不必要的服务（inetd）、其它不必要的服务（rc2 和 rc3）、文件/目录控制、系统信任关系、其它安全配置。



1.4. 安全方案设计

根据对企业的实际调研，获取企业的网络需求，以此来制定企业基础网络建设规划方案和网络设备选型参考。一份完整的解决方案的框架涉及 6 大方面，根据用户的实际需求取舍其中的某些方面。

◆概要安全风险分析

◆实际安全风险分析

◆网络系统的安全原则

◆安全产品（防火墙、防毒墙、身份认证、传输加密、入侵检测）

◆风险评估

◆安全服务

一份完整的网络安全解决方案需从以下 8 个方面来把握。

1. 体现唯一性，由于安全的复杂性和特殊性，唯一性是评估安全方案最重要的一个标准。实际中，每一个特定网络都是唯一的，需要根据实际情况来处理。

2. 对安全技术和安全风险有一个综合把握和理解，包括现在和将来可能出现的所有情况。

3. 对用户的网络系统可能遇到的安全风险和安全威胁，结合现有的安全技术和安全风险，要有一个合适、中肯的评估，不夸大，不缩小。

4. 对症下药，用相应的安全产品、安全技术和管理手段，降低用户的网络系统当前可能遇到的风险和威胁，消除风险和威胁的根源，增强整个网络系统抵抗风险和威胁的能力，增强系统本身的免疫力。

5. 方案中全方面体现出对用户的服务支持。因为产品和技术，都将会体现在服务中，服务来保证质量，服务来提升质量。

6. 在设计方案的时候，要明白网络系统安全是一个动态的、整体的、专业的工程，不能一步到位解决用户所有问题。

7. 方案出来后，不断地和用户进行沟通，能能够及时的得到客户对网络系统在安全方面的要求、期望和所遇到的问题。

8. 方案中涉及的产品和技术，都要经得起验证、推敲和实施，要有理论根据，也要有实际基础。

1.5. 安全监测

安全监控通过实时监控网络或主机活动，监视分析用户和系统的行为，审计系统配置和漏洞，评估敏感系统和数据的完整性，识别攻击行为，对异常行为进行统计和跟踪，识别违反安全法规的行为，使用诱骗服务器记录黑客行为等功能，使管理员有效地监视、控制和评估网络或主机系统。

基于行业领先的自动化检测技术，对 Android、ios 应用进行全方位安全检测，帮助企业快速识别并精准定位安全风险，并提供整改方案，高效便捷的提升移动应用的安全性。

◆**扫描、监测引擎**：扫描引擎基于智能爬虫技术、JavaScript 脚本解析技术，在高效抓取网站页面的基础上，提供包括 SQL 注入和 XSS 在内的 Web 应用漏洞检测，同时检测类型支持 WASC 分类。监测引擎模块根据站点管理者的监管要求，通过对目标站点进行不间断的页面爬取、分析、匹配，为客户的互联网网站提供远程安全监测、安全检查、实时告警，是构建完善的网站安全体系的最好补充。

◆**高频率监测**：可 7*24 小时不间断网站安全实时风险监测，一旦网站出现风险事件，第一时间通知网站运维团队。在监测过程中，采用增量扫描技术，在实现对目标站点进行高频率的风险监测的同时，最大限度地降低了对站点的影响。

◆**网站挂马监测**：高准确率基于行为分析的挂马检测技术，支持静态和动态相结合的主动挂马检测技术，同时可达到最小十分钟的监测周期，并对挂马事件可提供场景文件用于取证。

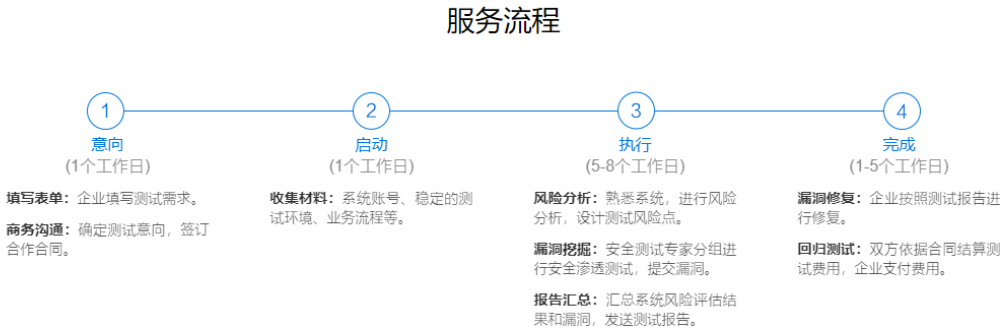
◆**网页篡改监测**：采用独创的静态和动态相结合检测技术，达到互补的效果，能够准确检测出包括各种暗链在内的篡改事件，同时，可以有效地对网页正常变更和篡改事件进行区分，减少了误报率，并对篡改事件可提供场景文件用于取证。

◆**网站敏感内容监测**：采用先进中文分词技术持续对被监测网页的所有文字内容进行分析，依据已设定的模板进行敏感内容判定，其中敏感内容检测模板包括了赌博、邪教、广告、反政治、反政府、化学、社会、黑客等八大类，并对敏感内容事件可提供场景文件用于取证。

◆**网站平稳度监测**：采用实际访问网站的多种方式，持续对被监测站点进行可用性分析，依据设置的超时值或失败次数来判定是否发生平稳度事件。分析的结果曲线可以直观反应站点的可用性情况，同时对断网、DDOS 等事件能够及时

的告警。

◆**调度引擎**：采用动态调度算法，实时监控系统任务情况，对系统内的任务进行调度。该调度模块可细分为非实时调度模块和实时调度模块，非实时调度模块用于周期性的或定时性的任务的资源分配和调度，功能上实现了细粒度的任务调度功能，能满足绝大多数的周期和定时任务的需求。实时调度模块用于任务的实时调度功能，当系统资源紧张，不适合再起动新的扫描时，实时调度引擎会根据系统当前的状态自动对任务的启动进行延迟，直到系统资源足够后再启动扫描。



1.6. 代码审计

代码审计（Code audit）是一种以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析。软件代码审计是对编程项目中源代码的全面分析，旨在发现错误，安全漏洞或违反编程约定。 它是防御性编程范例的一个组成部分，它试图在软件发布之前减少错误。 C 和 C ++源代码是最常见的审计代码，因为许多高级语言（如 Python）具有较少的潜在易受攻击的功能（例如，不检查边界的函数）。

代码审计是依据 CVE 公共漏洞字典表、OWASP 十大 Web 漏洞及设备、软件厂商公布的漏洞库，结合专业源代码扫描工具对各种程序语言编写的源代码进行安全审计。为客户提供包括安全编码规范咨询、源代码安全现状测评、定位源代码中存在的安全漏洞、分析漏洞风险、给出修改建议等一系列服务。

检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议。

代码审计对象包括并不限于对 Windows 和 Linux 系统环境下的以下语言进行

审核：java、C、C#、ASP、PHP、JSP、NET。

内容包括

◆前后台分离的运行架构

◆WEB 服务的目录权限分类

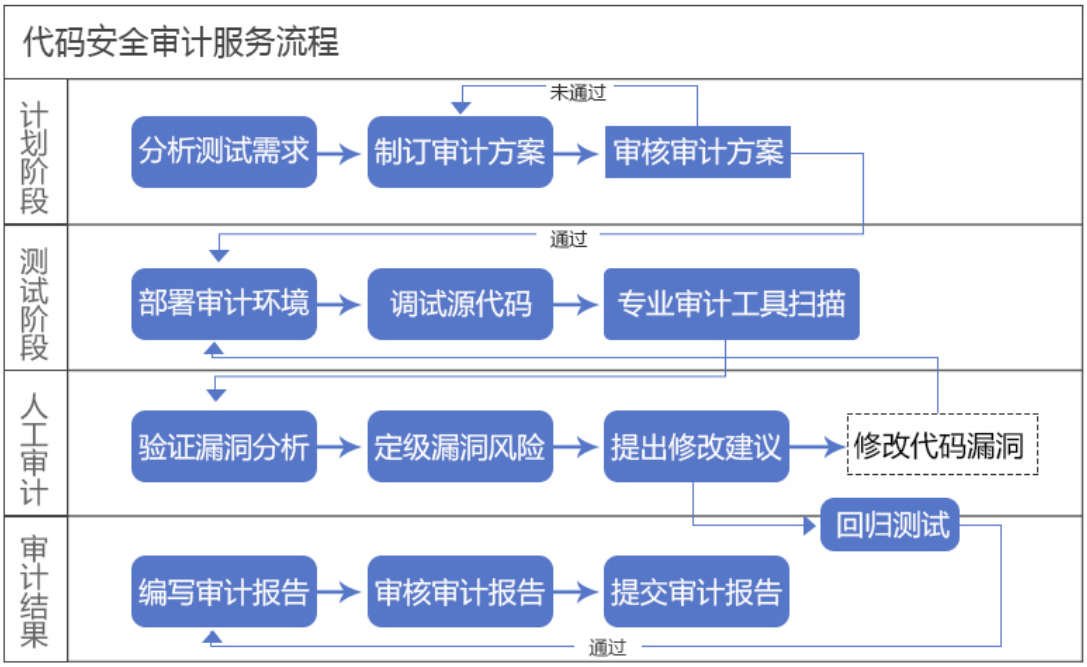
◆认证会话与应用平台的结合

◆数据库的配置规范

◆SQL 语句的编写规范

◆WEB 服务的权限配置

◆对抗爬虫引擎的处理措施



1.7. 渗透测试

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

◆主机操作系统渗透

对 Windows、Solaris、AIX、Linux、SCO、SGI 等操作系统本身进行渗透测试。

◆数据库系统渗透

对 MS-SQL、Oracle、MySQL、Informix、Sybase、DB2、Access 等数据库应用系统进行渗透测试。

◆应用系统渗透

对渗透目标提供的各种应用，如 ASP、CGI、JSP、PHP 等组成的 WWW 应用进行渗透测试。

◆网络设备渗透

对各种防火墙、入侵检测系统、网络设备进行渗透测试。

渗透测试流程如下：

1.明确目标

2.分析风险，获得授权

3.信息收集

4.漏洞探测（手动&自动）

5.漏洞验证

6.信息分析

7.利用漏洞，获取数据

8.信息整理

9.形成报告

1.8. 安全培训

安全培训服务目前聚焦于企业客户，主要面向企业内的信息安全技术和管理人员，从三个不同维度考虑来设计培训课程以满足企业客户获取安全知识和经验的需求，从而使客户最终达到强化安全意识，理解安全理论，掌握安全技术，获得安全实践经验，通过安全认证，能够融会贯通并应用于所在企业的安全建设当中。

◆从业务和行业特性考虑，针对金融、运营商、能源、政府、教育、医疗等行业研究成果和建设方案进行综合培训；

◆从受众知识技能掌握程度，有针对性的设置不同难度等级，分为初级、中级、高级；

◆从知识专业程度角度，提升客户理论能力和实际操作能力，涉及安全意识、安全管理、安全技术、安全实践、安全认证多个方面。

针对特定行业的培训

培训对象：运营商、金融、能源、电力、烟草、医疗、教育等行业信息科技部门负责人、安全主管，安全技术负责人等。

培训目标：

解析与当前安全形势相匹配的行业安全解决方案，协助客户切实改善风险管理水平，抑制安全事件发生，提升客户安全和风险治理水准；

掌握信息安全现状，基于行业常见业务场景了解信息安全风险管理手段，并具备一定威胁和脆弱性消除能力。

课程范围：行业整体安全形势、行业建设整体思路、行业安全建设实例分析、行业关注的技术与研究。

安全管理培训

培训对象：涉及到安全规划、安全建设方案，从事信息安全工作的各行业初、中级安全技术、管理与运维人员

培训目标：提升参培人员的安全意识、安全管理知识水平、安全管理操作能力，增广信息安全的视野，提高本职工作中信息安全管理各项工作的实际操作水平。

课程范围：信息安全标准、等级保护建设、信息安全评估、安全管理体系。

安全技术培训

培训对象：各企业和机构技术管理人员、技术骨干和从事安全技术工作的新晋员工。

培训目标：理论讲解、讲师演示，结合学员实际操练，加强学员对安全的技术的认识，能够进行基本的安全加固、渗透测试和攻防演练等，在攻与防的对立统一中寻求突破。

课程范围：检查与加固、渗透测试、应急响应、代码审计、手机和移动应用、逆向分析、漏洞挖掘等。

1.9. 应急响应

“应急响应”是指一个组织为了应对各种意外事件的发生所做的准备以及在事件发生后所采取的措施。应急响应的对象是指针对计算机或网络所存储、传

输、处理的信息的安全事件，事件的主体可能来自自然界、系统自身故障、组织内部或外部的人、计算机病毒或蠕虫等。按照计算机信息系统安全的三个目标，可以把安全事件定义为破坏信息或信息处理系统 CIA 的行为。

计算机网络安全事件应急响应的对象是指针对计算机或网络所存储、传输、处理的信息的安全事件，事件的主体可能来自自然界、系统自身故障、组织内部或外部的人、计算机病毒或蠕虫等。按照计算机信息系统安全的三个目标，可以把安全事件定义为破坏信息或信息处理系统 CIA 的行为。比如：

◆**破坏保密性的安全事件**：比如入侵系统并读取信息、搭线窃听、远程探测网络拓扑结构和计算机系统配置等；

◆**破坏完整性的安全事件**：比如入侵系统并篡改数据、劫持网络连接并篡改或插入数据、安装特洛伊木马（如 BackOrifice2K）、计算机病毒（修改文件或引导区）等；

◆**破坏可用性(战时最可能出现的网络攻击)的安全事件**：比如系统故障、拒绝服务攻击、计算机蠕虫（以消耗系统资源或网络带宽为目的）等。但是越来越多的人意识到，CIA 界定的范围太小了，比如以下事件通常也是应急响应的对象：

◆**扫描**：包括地址扫描和端口扫描等，为了侵入系统寻找系统漏洞。

◆**抵赖**：指一个实体否认自己曾经执行过的某种操作，比如在电子商务中交易方之一否认自己曾经定购过某种商品，或者商家否认自己曾经接受过订单。

◆**垃圾邮件骚扰**：垃圾邮件是指接收者没有订阅却被强行塞入信箱的广告、政治宣传等邮件，不仅耗费大量的网络与存储资源，也浪费了接收者的时间。

◆**传播色情内容**：尽管不同的地区和国家政策不同，但是多数国家对于色情信息的传播是限制的，特别是对于青少年儿童的不良影响是各国都极力反对的。

◆**愚弄和欺诈**：是指散发虚假信息造成的事件，比如曾经发生过几个组织发布应急通告，声称出现了一种可怕的病毒“Virtual Card for You”，导致大量惊惶失措的用户删除了硬盘中很重要的数据，导致系统无法启动。

1.10. 风险评估

风险评估是对信息资产（即某事件或事物所具有的信息集）所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。从风险管理角度，运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁

及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施。风险评估工作贯穿信息系统整个生命周期，包括规划阶段、设计阶段、实施阶段、运行阶段、废弃阶段等。

评估过程

◆**资产识别与赋值**：对评估范围内的所有资产进行识别，并调查资产破坏后可能造成的损失大小，根据危害和受损的程度为资产进行相对赋值；资产包括硬件、软件、服务、信息和人员等；

◆**威胁识别与赋值**：即分析资产所面临的每种威胁发生的频率，威胁包括环境因素和人为因素；

◆**脆弱性识别与赋值**：从管理和技术两个方面发现和识别脆弱性，根据被威胁利用时对资产造成的损害进行赋值；

◆**风险值计算**：通过分析上述测试数据，进行风险值计算，识别和确认高风险，并针对存在的安全风险提出整改建议。

◆被评估单位可根据风险评估结果防范和化解信息安全风险，或者将风险控制在可接受的水平，为最大限度地保障网络和信息安全提供科学依据。

评估内容

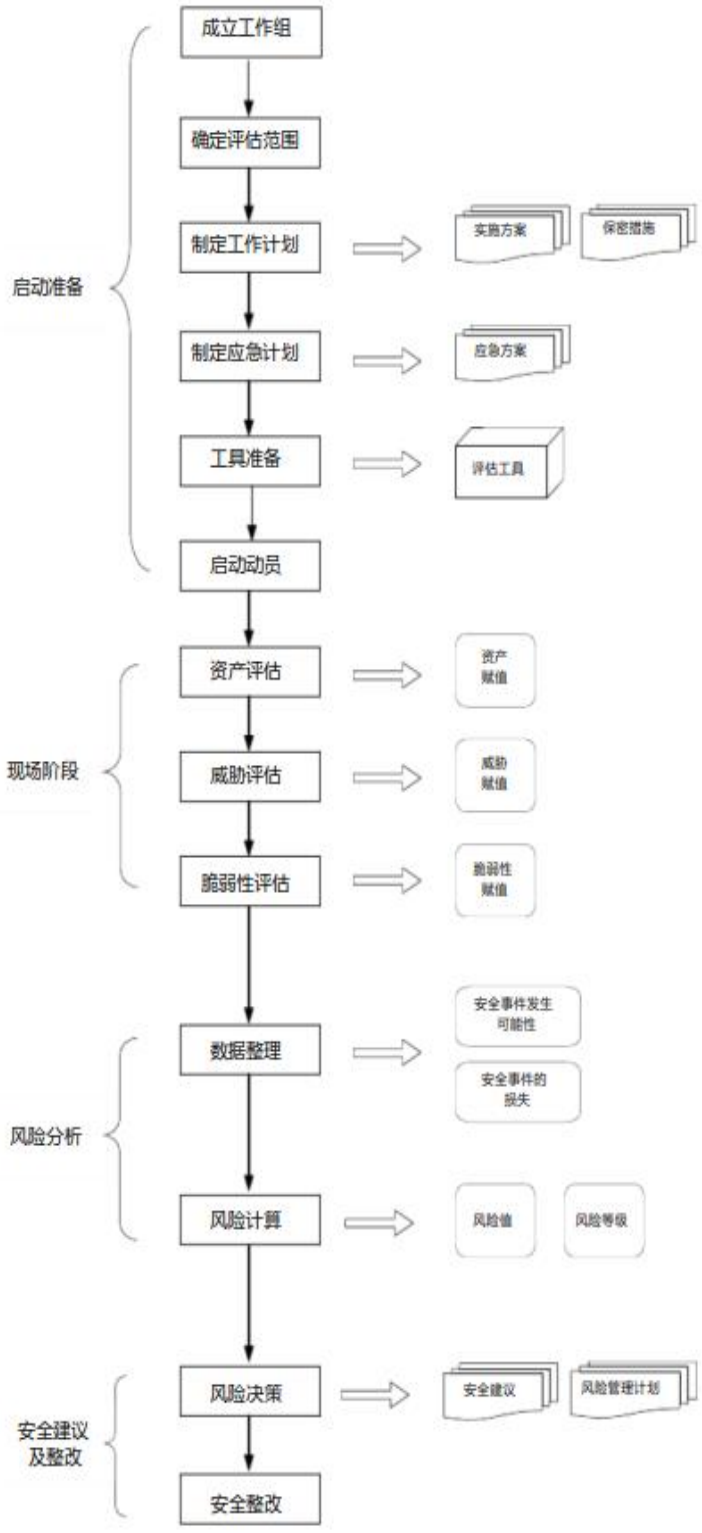
安全服务综合国内外相关标准，展现信息系统当前的安全现状，为下一步控制和降低安全风险、改善安全现状、实施信息系统的风险管理提供决策依据。

◆**主机安全评估**：对主机的配置、服务进行安全评估

◆**系统安全评估**：对各类计算机系统（Windows、Linux 等）的配置、服务和安全防护能力进行评估

◆**网络安全评估**：对网络设备、网络服务、网络拓扑以及 Web 应用等进行评估，得出评估报告

◆**业务系统评估**：评估常见业务应用（ERP、OA、CRM 等）系统。


启动准备
成立工作组
确定评估范围
制定工作计划
实施方案
保密措施
制定应急计划
应急方案
工具准备
评估工具
启动动员
现场阶段
资产评估
资产
赋值
威胁评估
威胁
赋值
脆弱性评估
脆弱性
赋值
风险分析
数据整理
安全事件发生
可能性
安全事件的
损失
风险计算
风险值
风险等级
安全建议及整改
风险决策
安全建议
风险管理计划
安全整改

1.12. 行业解决方案

a) 解决方案概述

为各行业提供二级及三级网络安全等级保护测评服务，并提供网络安全咨询、安全加固、方案设计、安全监测、代码审计、参透测试、安全培训、应急响应及风险评估等服务。

b) 行业覆盖范围

全行业，主要包括：能源、医疗、教育、金融、政府及事业单位等。

c) 解决方案的核心价值(解决什么问题，针对的具体场景)

减少网络安全隐患及风险，面向所有网络环境。

d) 架构设计（需要标明自有产品与阿里云产品在架构中的部署方式）

采取一单一议，根据不同客户提供不同的产品服务，目前服务类型包括：网络安全等级保护二级及三级测评服务、网络安全咨询、安全加固、方案设计、安全监测、代码审计、参透测试、安全培训、应急响应及风险评估等服务。

e)获得的收益（从经济利益、效率提升等方面描述）

强强联手，为客户提供最优的服务，提升客户的服务体验感，增强客户与公司的粘度，为企业带了长久的收益。