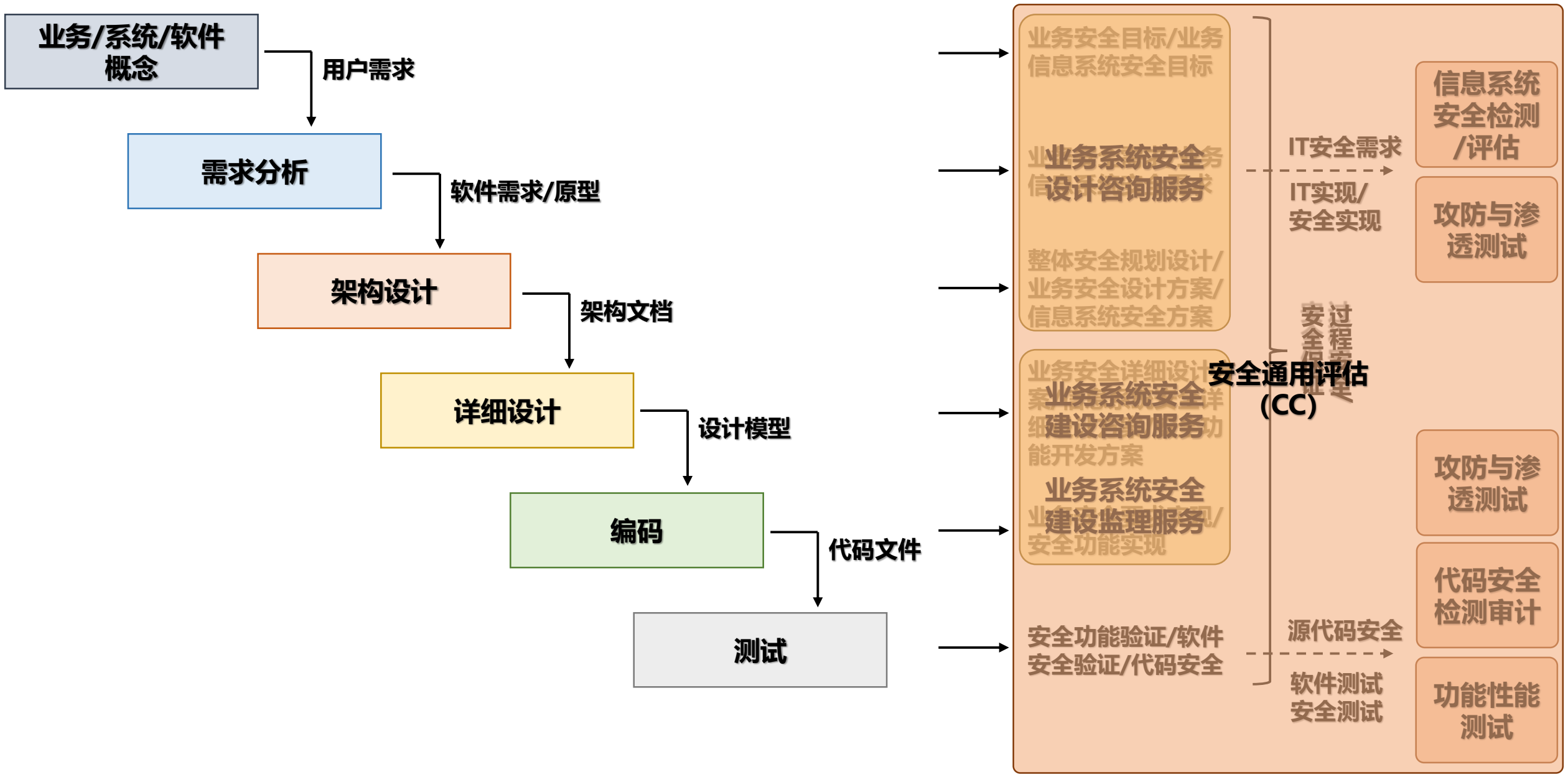
电子政务业务应用系统安全检测技术探讨

徐根炜

信息安全共性技术国家工程研究中心副主任

01、软件安全检测服务


业务/系统/软件概念
用户需求
需求分析
软件需求/原型
架构设计
架构文档
详细设计
设计模型
编码
代码文件
测试
业务安全目标/业务信息系统安全目标
业务系统安全设计咨询服务
整体安全规划设计/业务安全设计方案/信息系统安全方案
业务系统安全建设咨询服务
业务系统安全建设监理服务
安全功能验证/软件安全验证/代码安全
IT安全需求
IT实现/安全实现
安全通用评估(CC)
源代码安全
软件测试安全测试
信息系统安全检测/评估
攻防与渗透测试
攻防与渗透测试
代码安全检测审计
功能性能测试

02、软件功能性能测试与检测服务

（1）概述

应用、平台和产品功能、性能测试

标准与方法 | **流程** | **工具**

功能测试内容

- 安装测试：安装正确性、安装设置正确性、安装提示正确性
- 界面测试：功能验证、操作控制验证、操作连动验证
- 流程测试：基本流程、分支覆盖、组合覆盖、业务场景
- 兼容性测试：操作系统兼容性、浏览器兼容性、历史数据兼容性、第三方软件兼容性
- 文档测试：内容全面、指导正确

测试方法

- 冒烟测试
- 静态检查
- 流程模拟测试
- 业务模拟测试
- 场景模拟测试
- 异常操作测试
- 集成测试
- 代码走查
- 体验测试

性能测试内容

- 本地性能
- 网络性能
- 服务器性能
- 数据库性能

测试方法

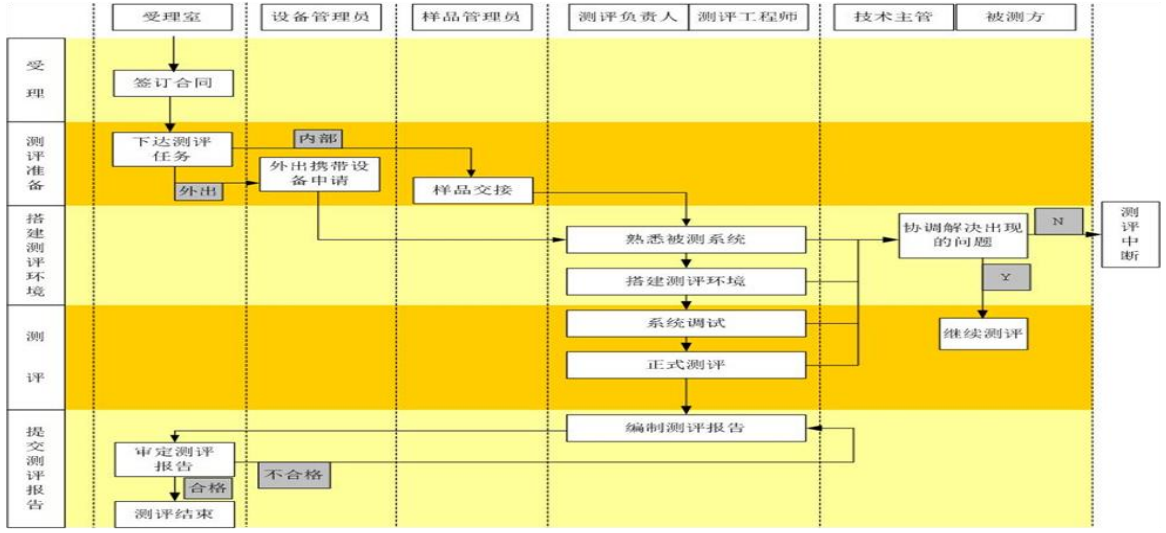
- 压力测试
- 配置测试
- 容量测试
- 恢复性测试
- 稳定性测试
- 极限测试
- 恢复性测试
- 大数据量测试

（1）概述

应用、平台和产品功能、性能测试

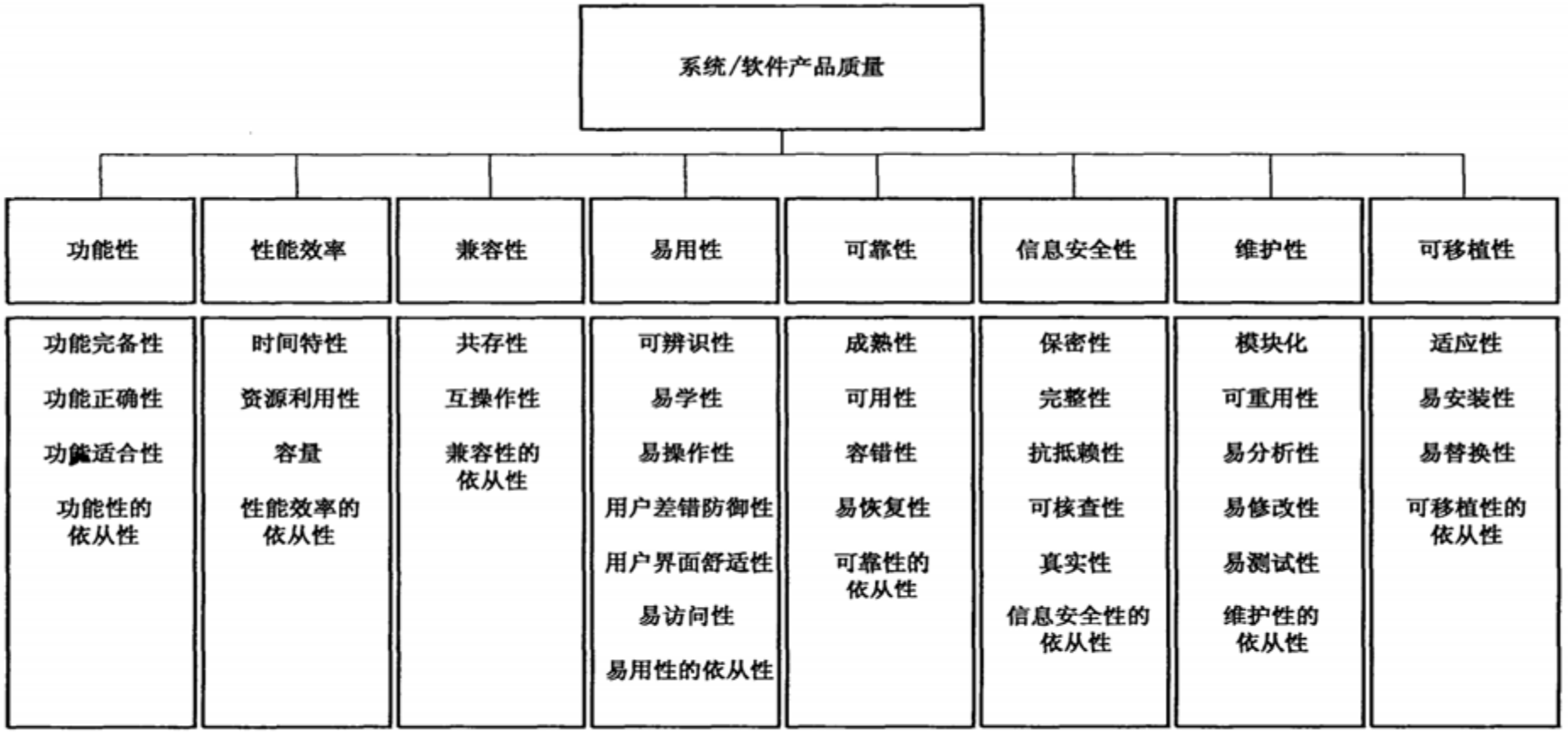
标准与方法 | **流程** | **工具**

测试服务流程



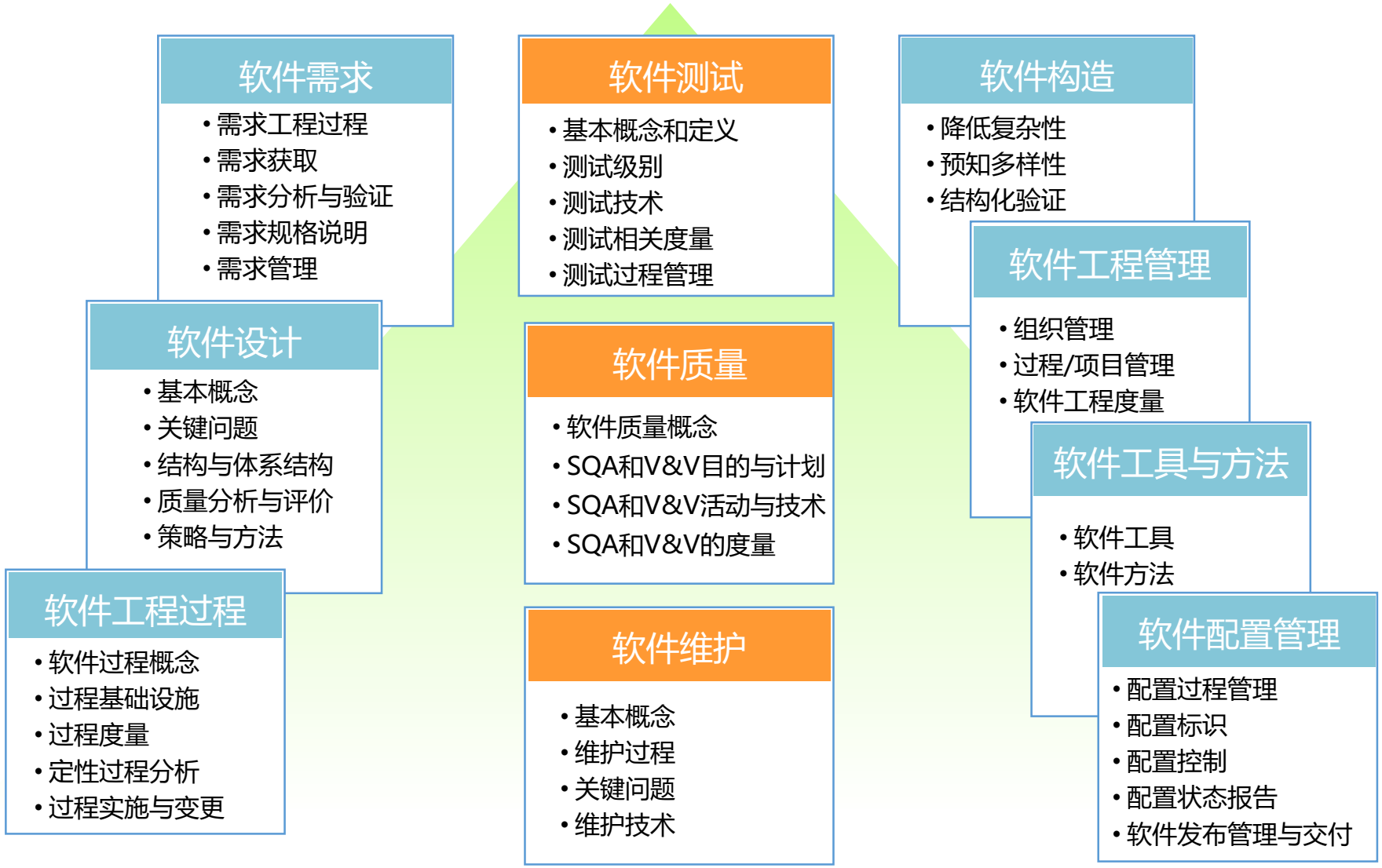
标准的测试管理流程

（2）基本概念



产品质量模型

（2）基本概念


软件需求
• 需求工程过程
• 需求获取
• 需求分析与验证
• 需求规格说明
• 需求管理
软件测试
• 基本概念和定义
• 测试级别
• 测试技术
• 测试相关度量
• 测试过程管理
软件构造
• 降低复杂性
• 预知多样性
• 结构化验证
软件设计
• 基本概念
• 关键问题
• 结构与体系结构
• 质量分析与评价
• 策略与方法
软件质量
• 软件质量概念
• SQA和V&V目的与计划
• SQA和V&V活动与技术
• SQA和V&V的度量
软件工程管理
• 组织管理
• 过程/项目管理
• 软件工程度量
软件工具与方法
• 软件工具
• 软件方法
软件工程过程
• 软件过程概念
• 过程基础设施
• 过程度量
• 定性过程分析
• 过程实施与变更
软件维护
• 基本概念
• 维护过程
• 关键问题
• 维护技术
软件配置管理
• 配置过程管理
• 配置标识
• 配置控制
• 配置状态报告
• 软件发布管理与交付

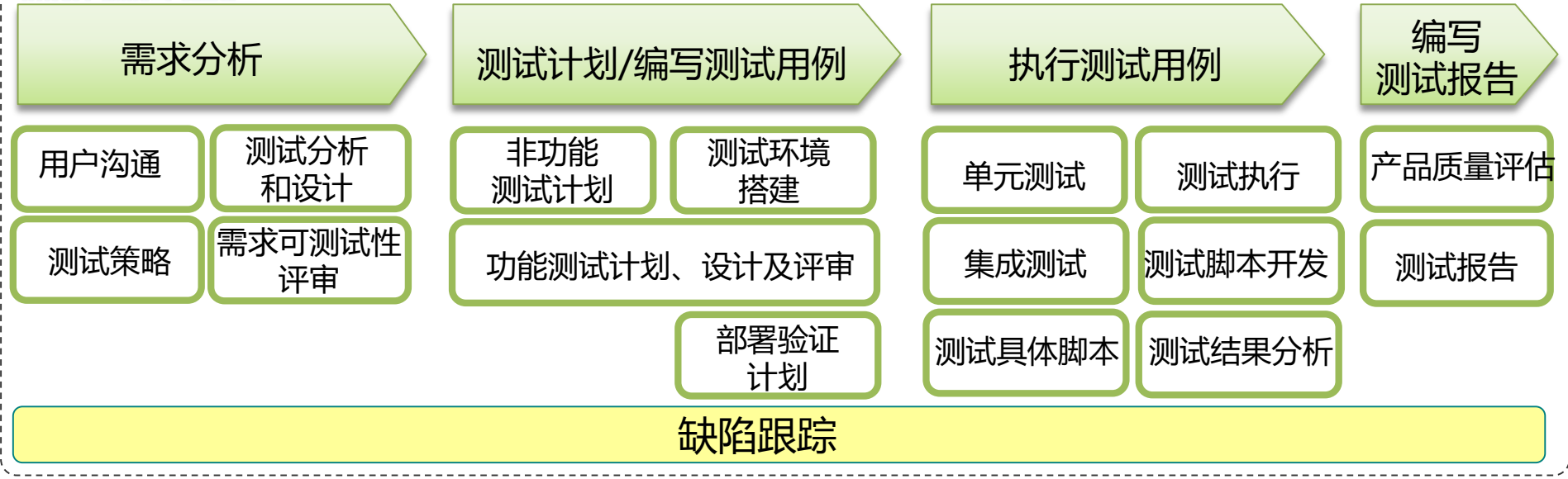
（3）软件工程中的软件测试服务

➢ 覆盖软件开发全过程 ➢ 软件质量保证的最主要活动 ➢ 软件开发过程的记录和度量

软件开发流程

业务分析 → 需求定义 → 架构设计 → 详细设计 → 编程和单元测试 → 系统测试 → 发布/部署

软件测试流程



（3）软件工程中的软件测试服务

软件测试流程

根据软件测试模型，设计出详细的软件测试流程。每个阶段的工作进行针对性工作计划安排。

总结评估阶段

测试执行阶段

测试设计阶段

测试计划阶段

初始阶段

阶段

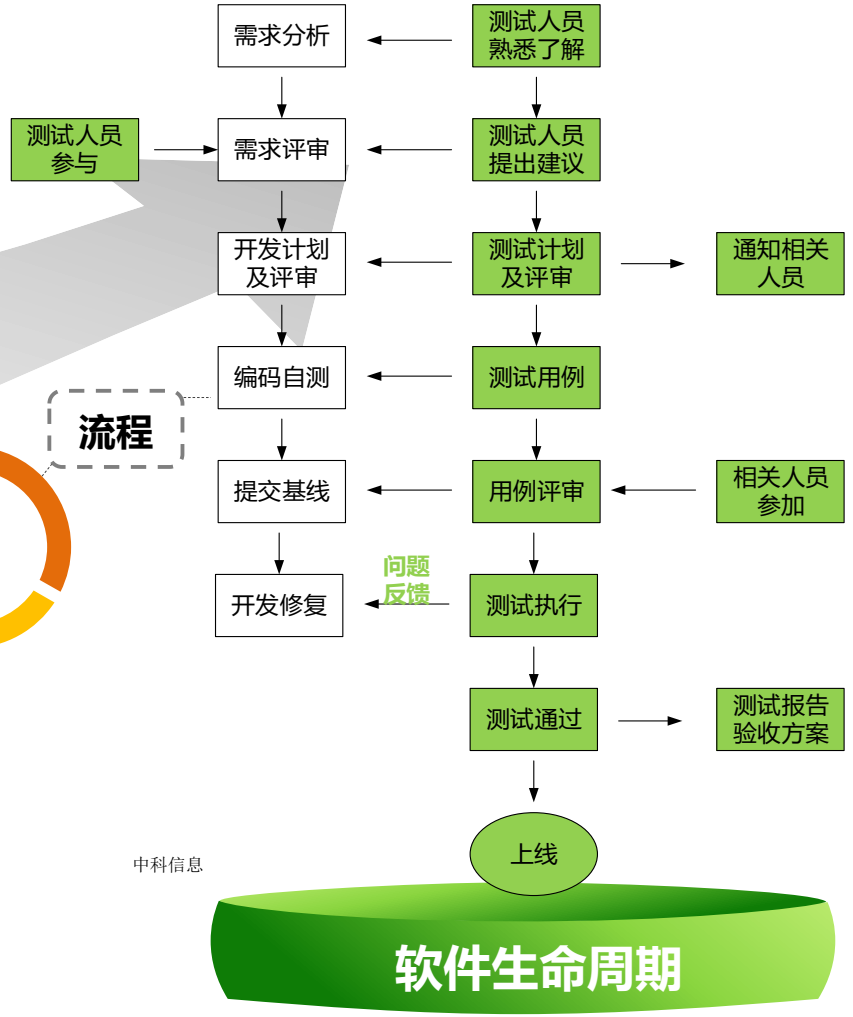
流程

意义

1 分阶段管理和监督

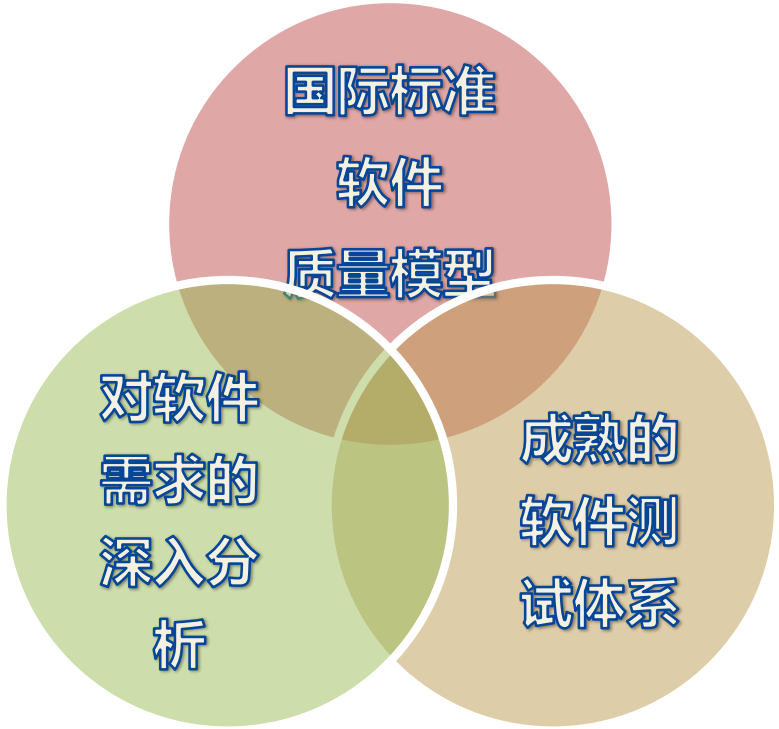
2 及时对工作内容进行

3 调整工作内容方便快



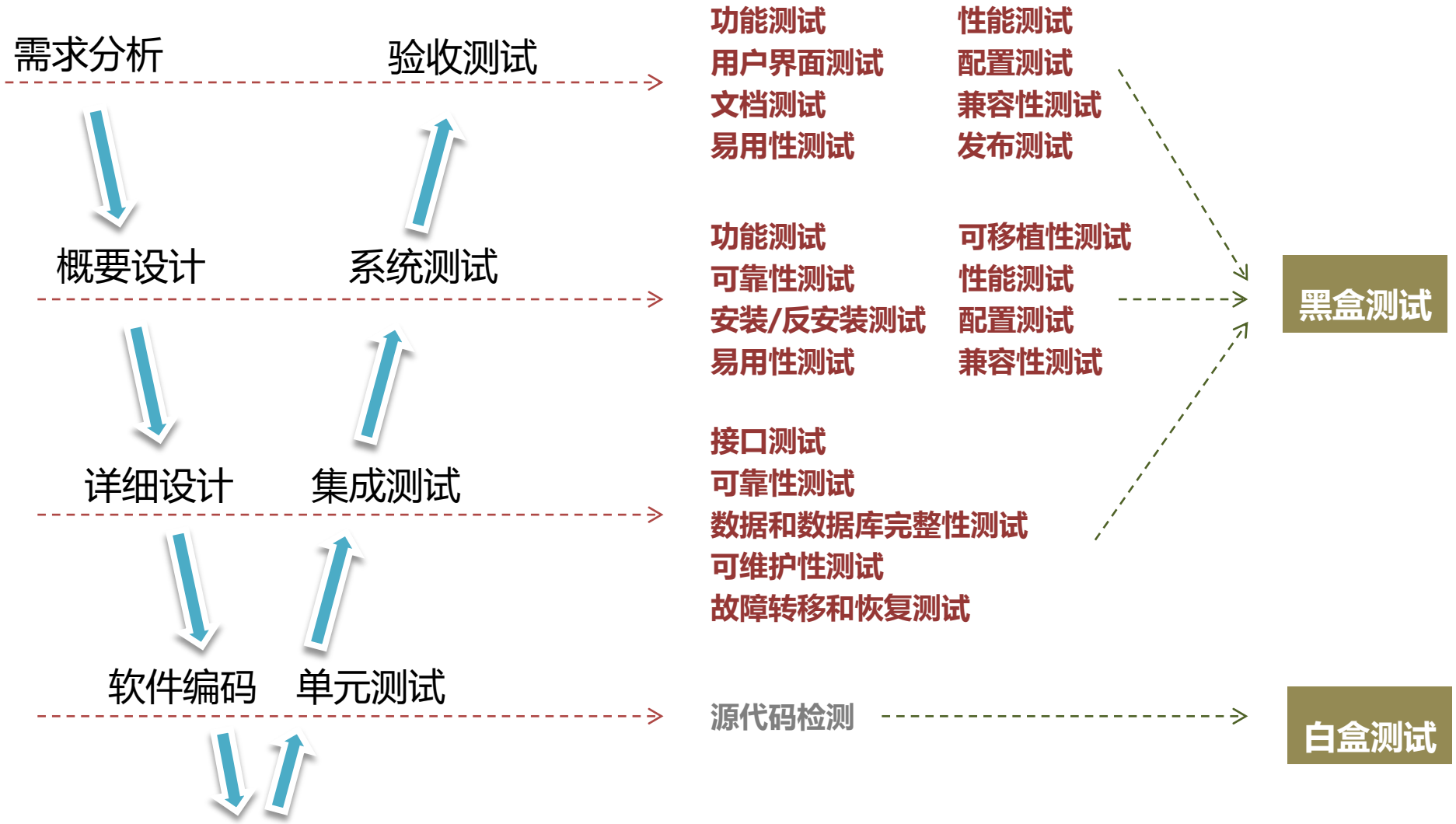
（4）软件测试服务的理念

以质量模型为基础，以测试体系为指导，以全面覆盖需求为目标的全方位质量保证活动。



（5）软件测试服务的全景图

（6）软件测试服务内容


需求分析
验收测试
概要设计
系统测试
详细设计
集成测试
软件编码
单元测试
功能测试
性能测试
用户界面测试
配置测试
文档测试
兼容性测试
易用性测试
发布测试
功能测试
可移植性测试
可靠性测试
性能测试
安装/反安装测试
配置测试
易用性测试
兼容性测试
接口测试
可靠性测试
数据和数据库完整性测试
可维护性测试
故障转移和恢复测试
源代码检测
黑盒测试
白盒测试

（6）软件测试服务内容——功能

测试内容

- 安装测试：安装正确性、安装设置正确性、安装提示正确性
- 界面测试：功能验证、操作控制验证、操作连动验证
- 流程测试：基本流程、分支覆盖、组合覆盖、业务场景
- 文档测试：内容全面、指导正确

测试方法

- 冒烟测试
- 静态检查
- 流程模拟测试
- 业务模拟测试
- 场景模拟测试
- 异常操作测试
- 集成测试
- 代码走查
- 体验测试

测试工具

- 手工测试
- 自动化测试
  - QTP
  - Selenium
  - Autoit

（6）软件测试服务内容——性能

测试内容

- 本地性能
- 网络性能
- 服务器性能
- 数据库性能
- 系统容量
- 系统稳定性
- 系统容错性

测试方法

- 压力测试
- 配置测试
- 容量测试
- 恢复性测试
- 稳定性测试
- 极限测试
- 恢复性测试
- 大数据量测试

测试工具

- LoadRunner

  功能强大、支持协议多、可集群加载压力、通用性强。

- Jmeter

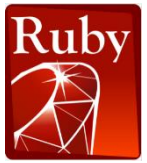
  轻巧快捷、脚本开发容易、可跨平台操作。

- Nmon

  详细的Linux、AIX等系统的资源监控。

- Ruby

  单文件编程、方便管理、脚本易学易用。



（6）软件测试服务内容——易用性

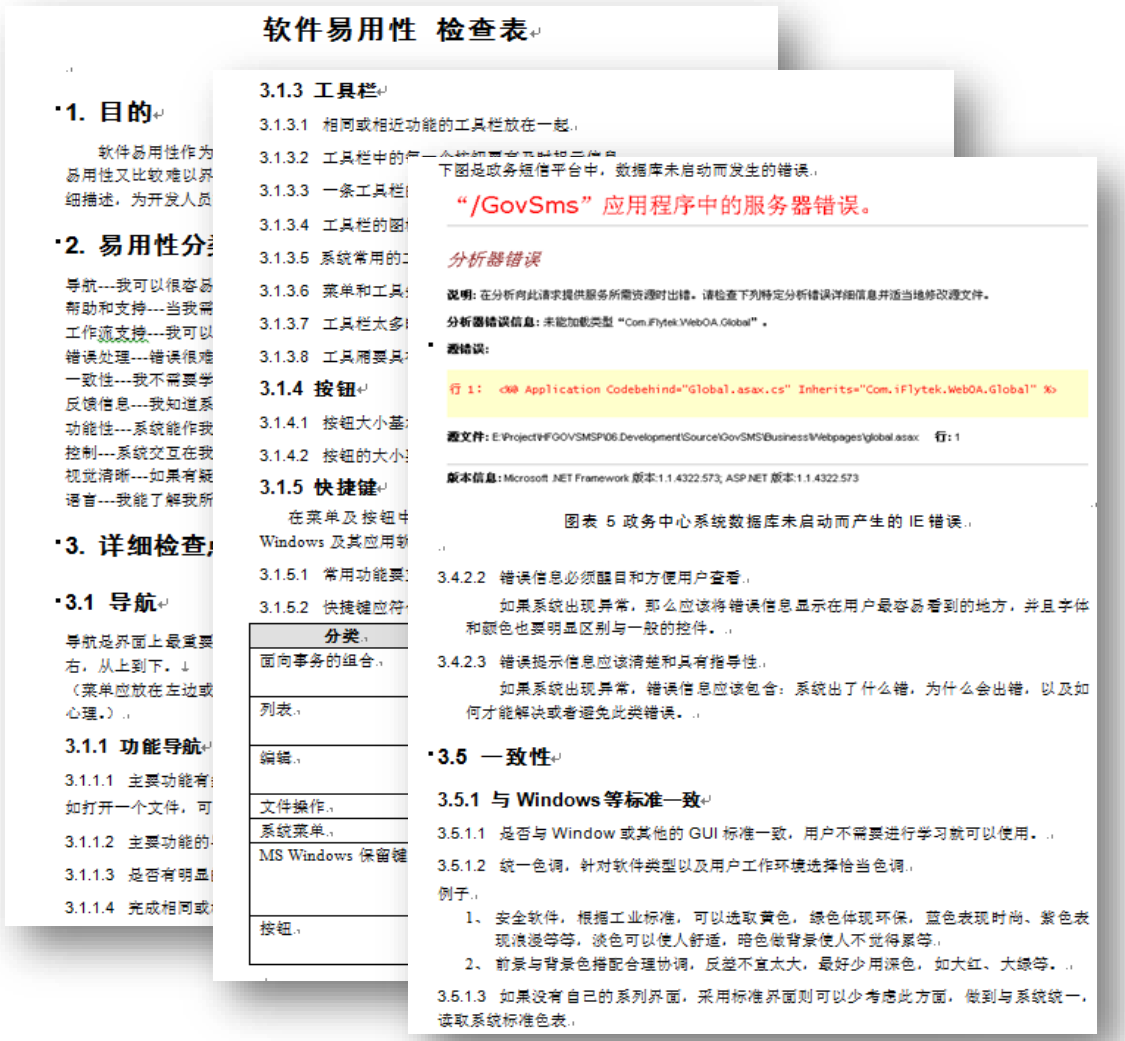
测试内容

- 易理解性
- 易学性
- 易操作性
- 吸引性

测试方法

- 售前售后信息反馈
- 调查问卷
- 日常积累
- 同类系统参考

软件易用性检查表



软件易用性 检查表

1. 目的

3.1.3 工具栏

3.1.4 按钮

3.1.5 快捷键

3.1 导航

3.1.1 功能导航

“/GovSms”应用程序中的服务器错误。

分析器错误

图表 5 政务中心系统数据库未启动而产生的 IE 错误

3.5 一致性

3.5.1 与 Windows 等标准一致

（6）软件测试服务内容——接口

测试内容

- 前后台接口
- 内部接口
- 外部接口
- 接口一致性
- 多接口兼容性
- 接口性能
- 接口稳定性

测试方法

- 标准请求测试
- 挡板测试
- 开发驱动和桩
- 接口性能测试
- 接口并发测试
- 接口大数据量测试

测试工具

- SoapUI

快速创建和执行自动化功能，提供完整的测试覆盖，支持所有的标准协议和技术。

（6）软件测试服务内容——兼容性

测试内容

- 多系统兼容性测试
- 操作系统兼容性
- 浏览器兼容性
- 历史数据兼容性
- 第三方软件兼容性

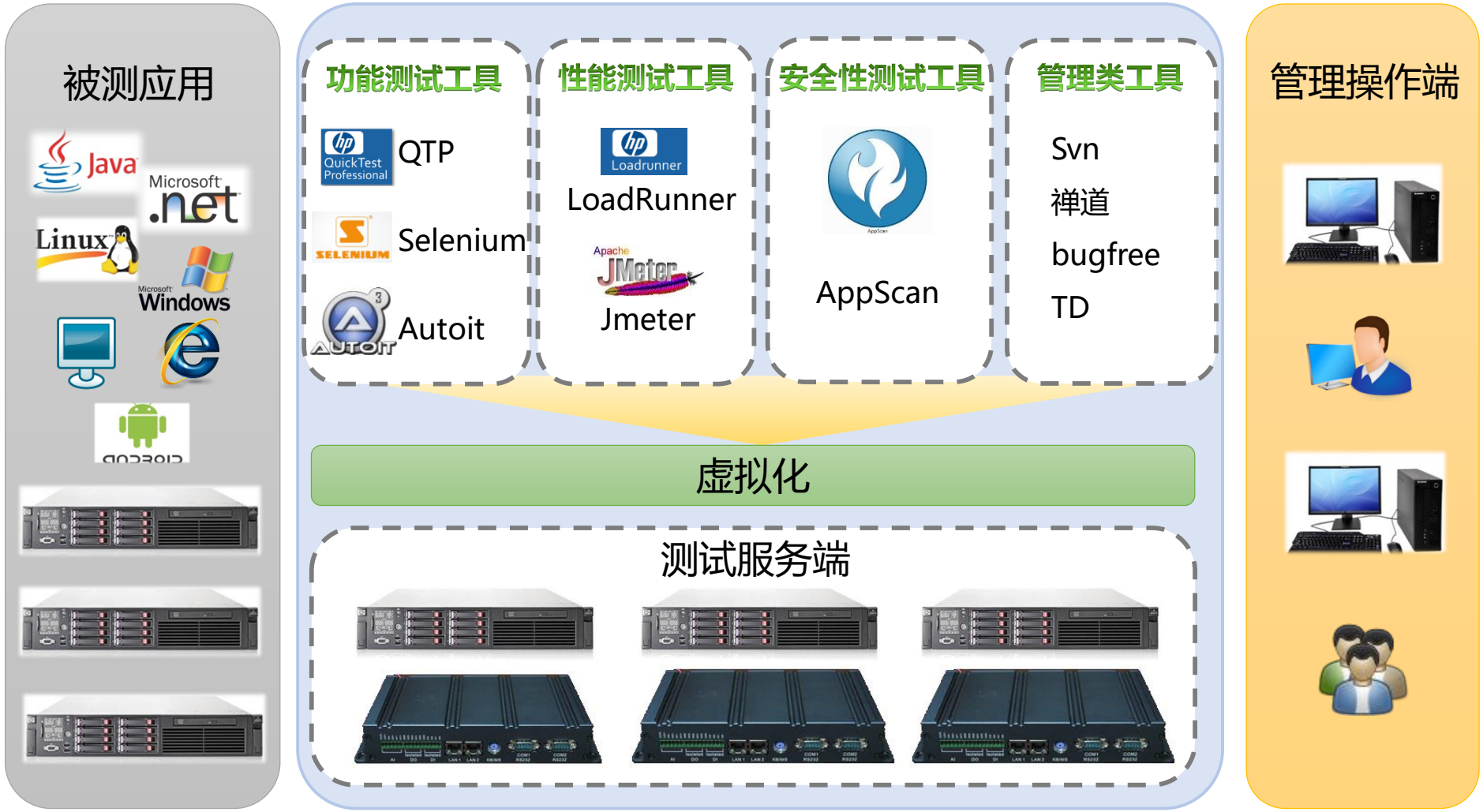
测试方法

- 跨系统长流程测试
- 跨系统场景模拟测试
- 模拟增量割接
- 模拟并行割接

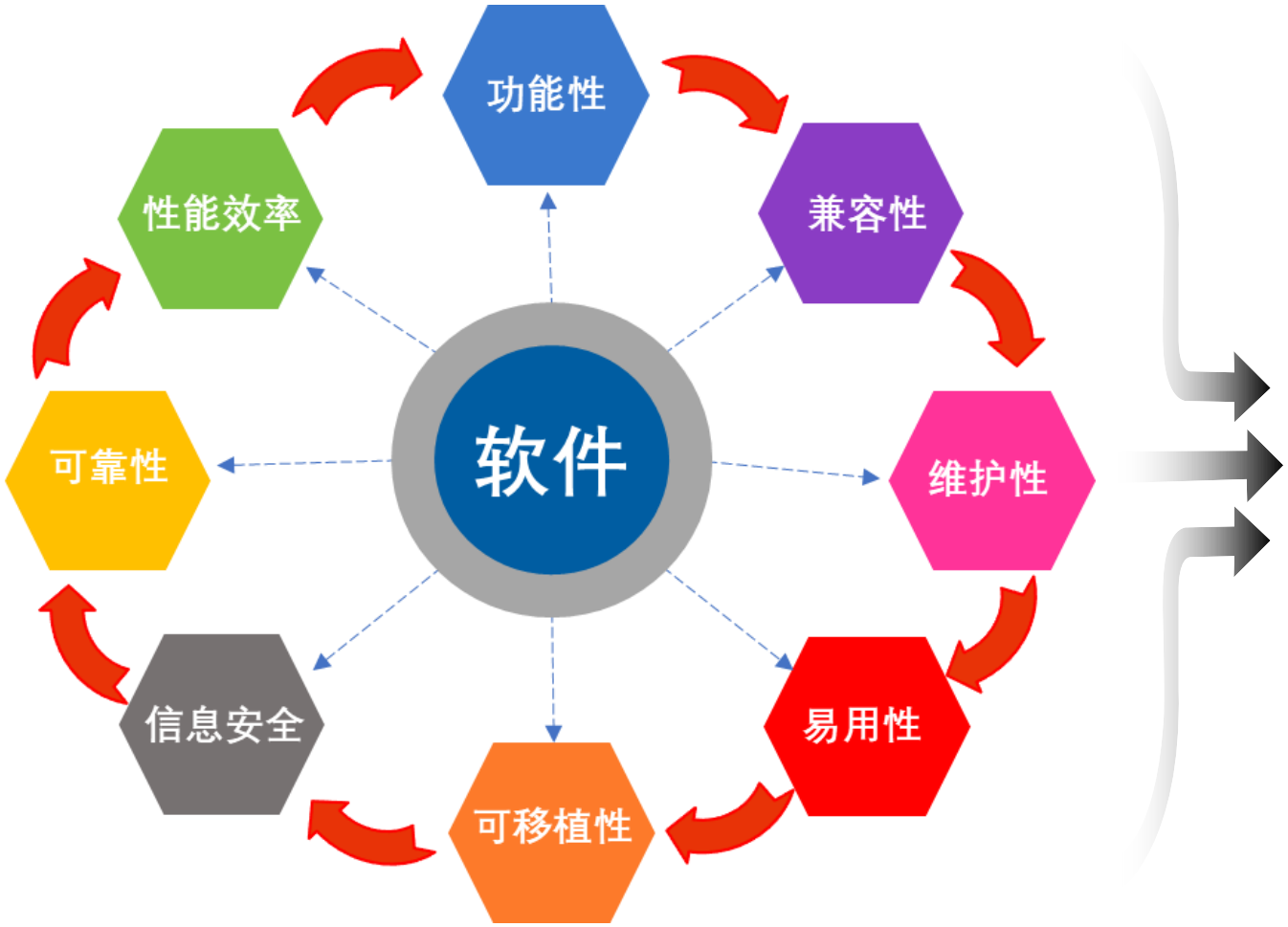
测试工具

- 手工测试
- 自动化测试


（7）软件测试环境的准备


被测应用
Java
Microsoft .net
Linux
Microsoft Windows
功能测试工具
QTP
Selenium
Autoit
性能测试工具
LoadRunner
Jmeter
安全性测试工具
AppScan
管理类工具
Svn
禅道
bugfree
TD
虚拟化
测试服务端
管理操作端

（8）软件功能性能测试的意义和作用



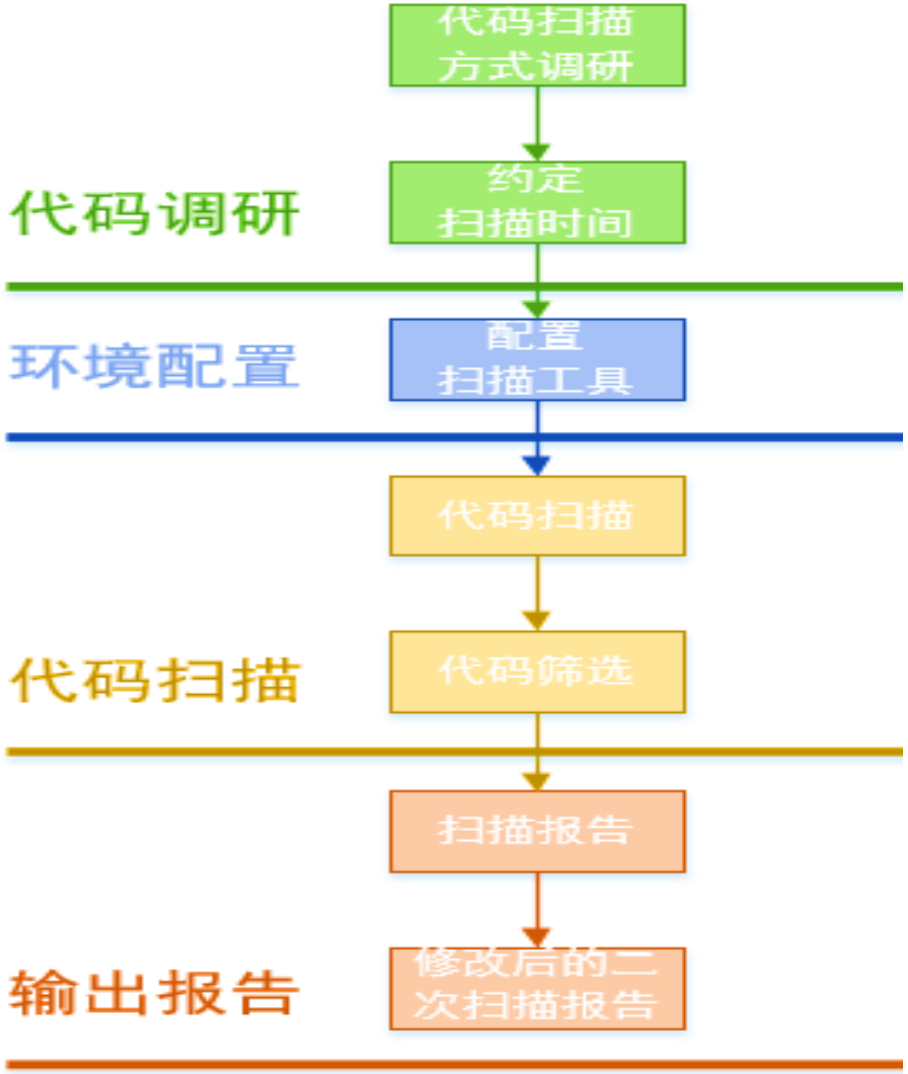
软件测试

所有软件都存在一些共有的特性。通过对这些特性的检测，保证软件产品的质量。就是软件测试需要做的工作。

目录

CONTENT

源代码安全检测/审计是依据CVE(Common Vulnerabilities & Exposures)公共漏洞字典表、OWASP十大Web漏洞（Open Web Application Security Project) 2013，以及设备、软件厂商公布的漏洞库，结合专业源代码安全检测工具对各种程序语言编写的源代码进行检测，并对结果进行安全审计。能够为客户提供包括安全编码规范咨询、源代码安全检测、源代码安全审计、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。



（2）服务依据的相关标准

在软件开发阶段查找软件自身程序设计中存在的安全隐患，并检查应用程序对非法侵入的防范能力，在系统投入运行前进行安全性测试，从源头上控制安全。参考标准如下：

国际标准

- ISO17961 C代码安全标准
- C安全编码标准：开发安全、可靠、稳固系统的98条规则
- C和C++安全编码
- Java安全编码标准
- Java编码指南:75条可靠和安全编码的建议
- MISRA-C-2004 工业标准的C编程规范

国家标准

- GB/T 28169-2011 嵌入式软 C语言编码规范
- GB/T 20983-2007 信息安全技术 网上银行系统信息安全保障评估准则
- GJB/Z141-2004 Z 军用软件测试指南
- GJB/Z142-2004 Z 军用软件安全性分析指南
- GJB/Z 102-1997 软件可靠性和安全性设计准则

行业标准

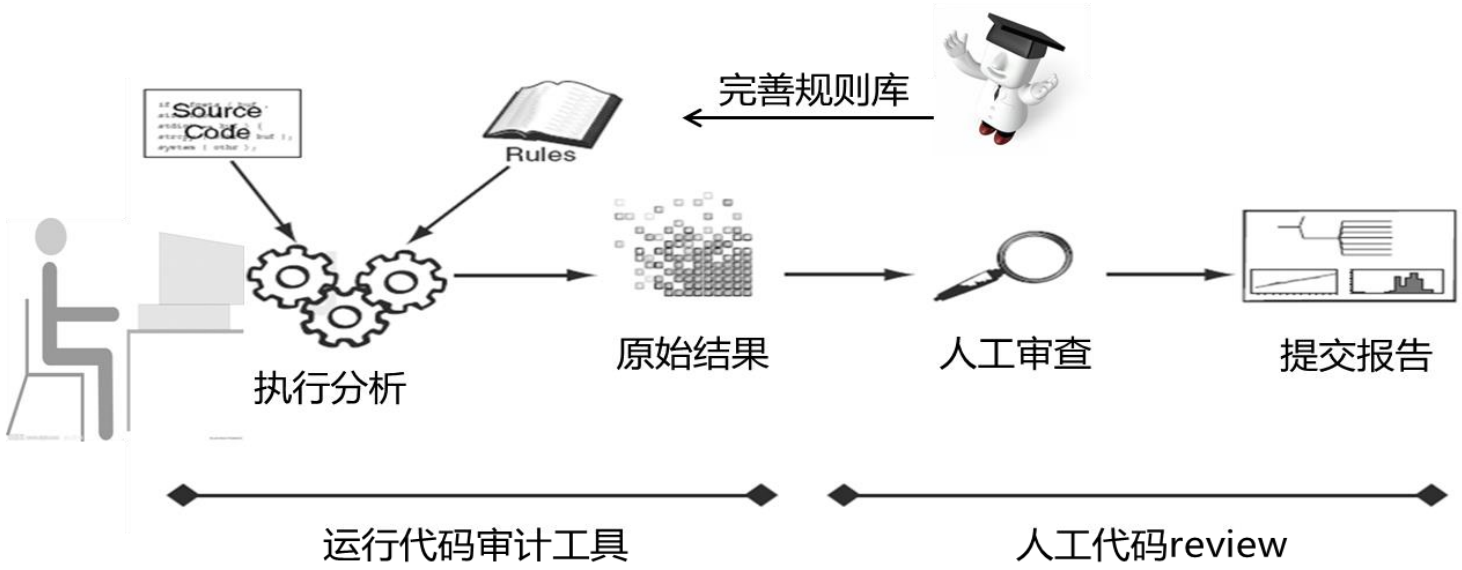
- QJ 3128-2001航天型号软件C语言安全子集
- JR/T 0101-2013 银行业软件测试文档规范
- JR/T 0068-2012 网上银行系统信息安全通用规范
- HS/T 28-2010海关信息系统信息安全风险评估规范
- HS/T 33-2011 NET安全编码规范
- HS/T 34-2011代码复查指南

（3）服务的基本工作流程

源代码审计

标准与方法　流程　工具

源代码审计具体实施流程如下：



- **构建集成（Build Integration）**

该阶段首先确认是否把集成到构建编译系统。

- **转换（Translation）**

该阶段用一系列命令集把源代码收集起来，然后用相应 的构建标识（ID）把源代码转换成一种内格式的“中间代 码”，构建ID总是被扫描的项目标识（ID）。

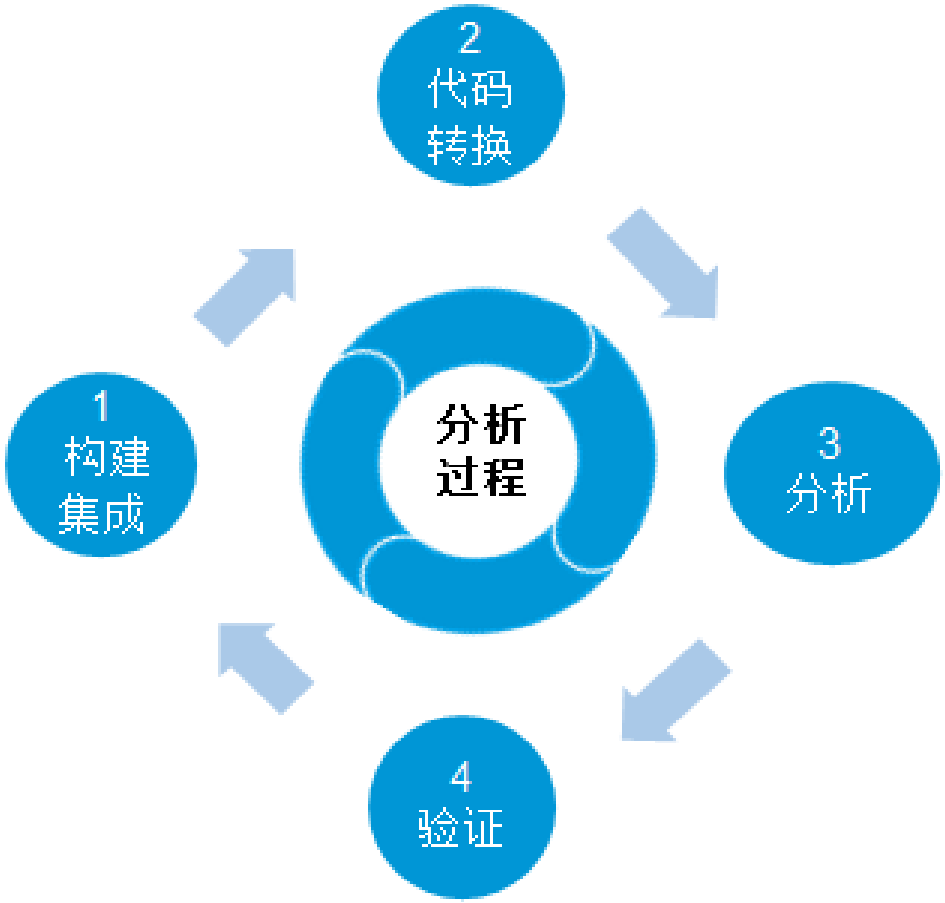
- **分析（Analysis）**

分析转换阶段的代码，生成一个Fortify格式的文件作为结果文件，通常扩展名为.fpr。

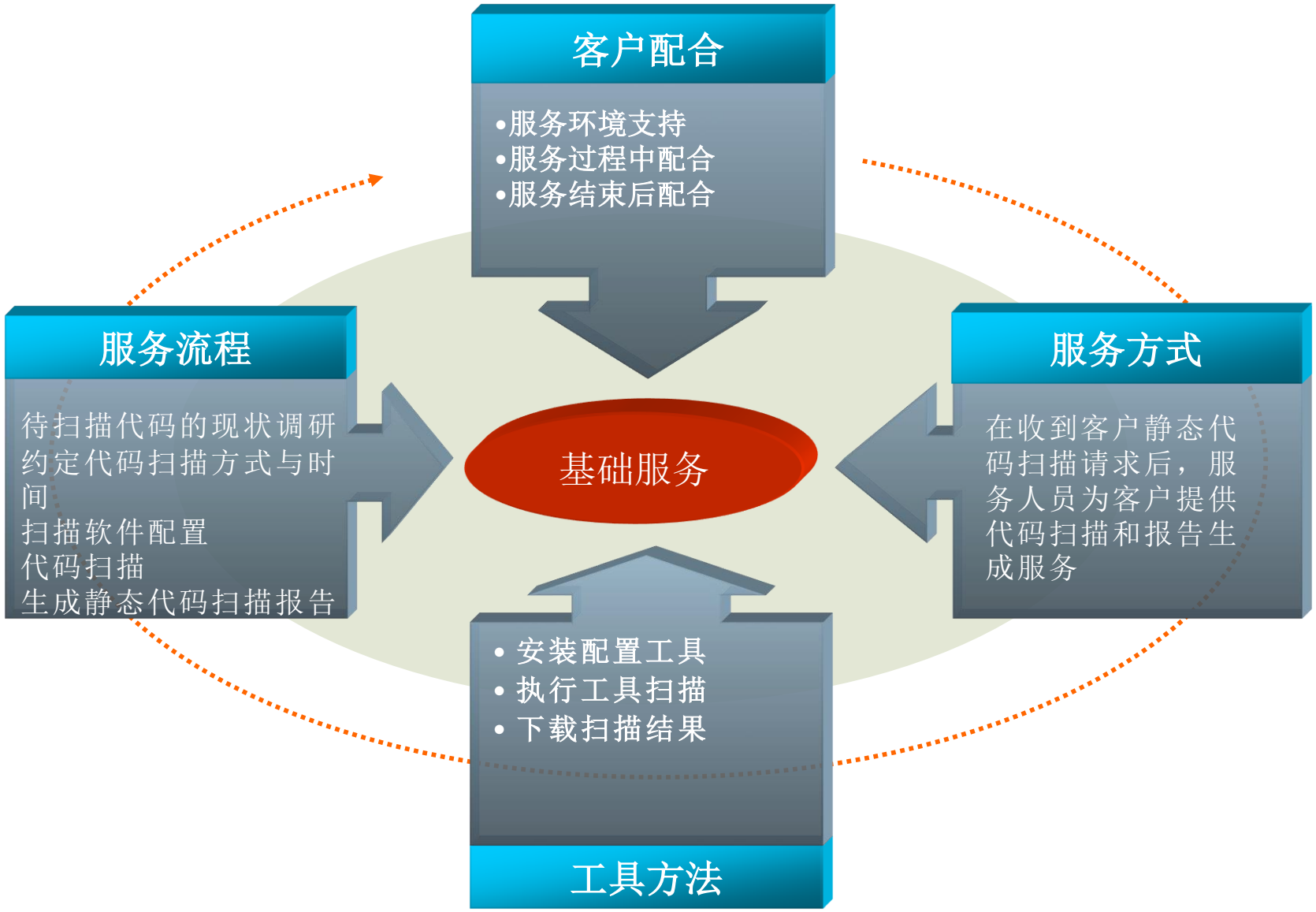
- **转换验证和分析（Verification & Analysis）**

该阶段确保源文件用正确的规则包扫描，且没有严重错误出现。

源代码分析过程



（4）源代码安全检测服务的内容



- 提供应用代码检测工具自动生成的静态代码扫描报告
- 报告格式支持PDF格式

TestTarAndGzip.java, line 92 (Unreleased Resource: Streams)

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		
Abstract:	The function testUnGzip() in TestTarAndGzip.java sometimes fails to release a system resource allocated by FileInputStream() on line 92.		
Sink:	TestTarAndGzip.java:92 gzis = new GZIPInputStream(new java.io.FileInputStream())		

```
90   public void testUnGzip() {
91     try {
92       GZIPInputStream gzis = new GZIPInputStream(new FileInputStream("e:/test.tar.gz"));
93       FileOutputStream fos = new FileOutputStream("e:/test.tar");
94       IOUtils.copy(gzis,fos);
```

TestTarAndGzip.java, line 98 (System Information Leak)

Fortify Priority:	Low	Folder	Low
Kingdom:	Encapsulation		
Abstract:	The function testUnGzip() in TestTarAndGzip.java might reveal system data or debugging information by calling printStackTrace() on line 98. The information revealed by printStackTrace() could help an adversary form a plan of attack.		
Sink:	TestTarAndGzip.java:98 printStackTrace()		

```
96       fos.close();
97     } catch (FileNotFoundException e) {
98       e.printStackTrace();
99     } catch (IOException e) {
100      e.printStackTrace();
```

示例

Report Overview

Report Summary

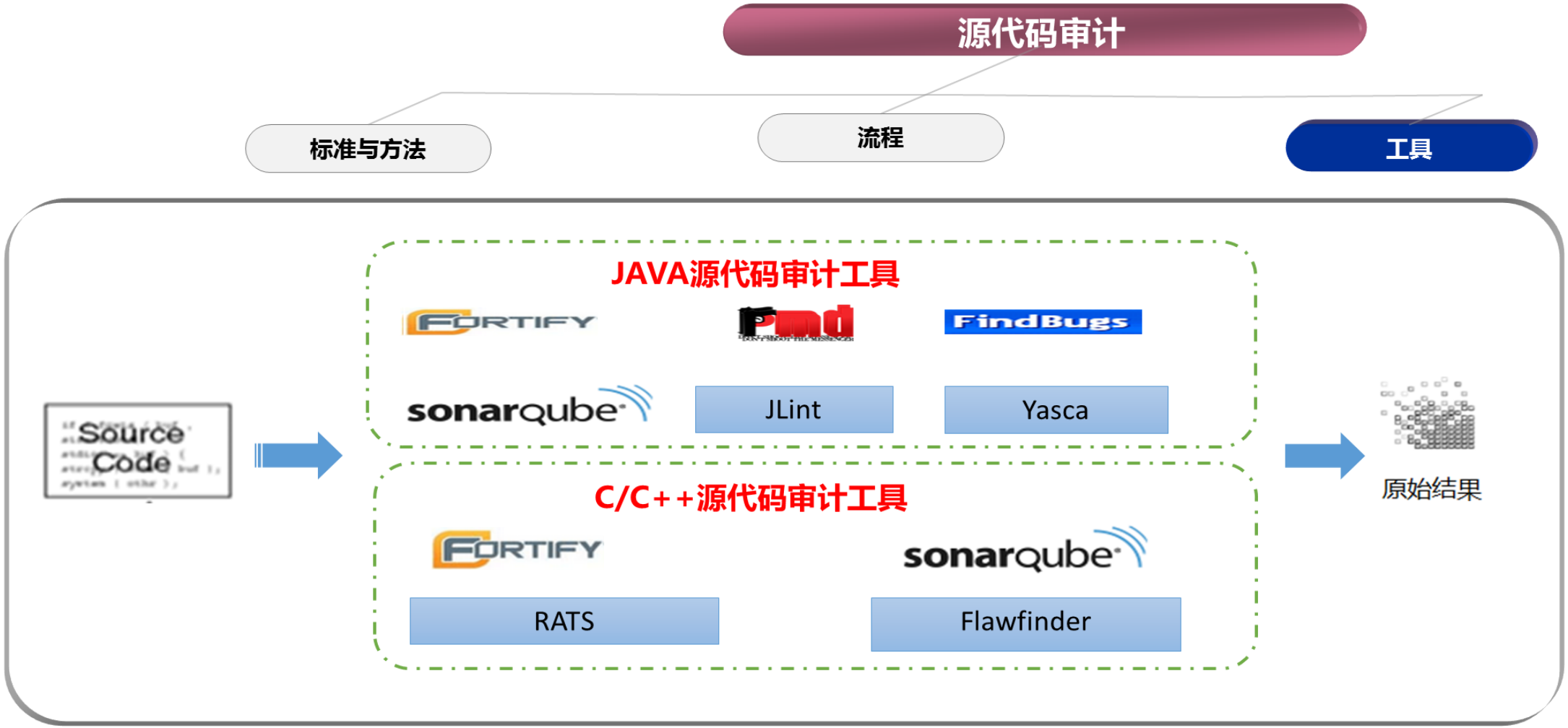
On Nov 29, 2013, a source code review was performed over the cms code base. 294 files, 4,838 LOC (Executable) were scanned. A total of 449 issues were uncovered during the analysis. This report provides a comprehensive description of all the types of issues found in this project. Specific examples and source code are provided for each issue type.

Issues by Fortify Priority Order	
Low	306
High	115
Critical	22
Medium	6

The scan found 449 issues.

Issues by File Name	
cms-web/src/main/test/org/konghao/backup/TestTarAndGzip.java	42
basic-common/src/main/java/org/konghao/basic/util/ImageUtil.java	40
basic-common/src/main/java/org/konghao/basic/util/TarAndGzipUtil.java	35
basic-common/src/main/java/org/konghao/basic/util/BackupFileUtil.java	30
basic-common/src/main/java/org/konghao/basic/util/Captcha.java	14
basic-common/src/main/java/org/konghao/basic/util/MySQLUtil.java	14
basic-common/src/main/java/org/konghao/basic/util/EnumUtils.java	12
cms-web/src/main/test/org/konghao/backup/TestCmd.java	12
cms-web/src/main/test/org/konghao/backup/TestSmb.java	10

（6）支撑服务交付的相关工具



（7）源代码安全检测服务价值

目录

CONTENT

（1）评估与合规性检测服务须遵循的标准

主要标准

- 《信息安全技术　网络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基本要求》(GB/T22239-2019)
- 《信息安全技术网络安全等级保护测评要求》(GB/T28448-2019)
- 《信息安全风险评估规范》(GB/T20984)
- 《信息系统安全保障评估框架》(GB/T20274)
- 《信息安全管理体系要求》(ISO/IEC 27001)
- 等

其他相关标准

《计算机信息系统安全保护等级划分准则》(GB 17859-1999)

《信息系统通用安全技术要求》（GB/T20271）

《网络基础安全技术要求》（GB/T20270）

《操作系统安全技术要求》（GB/T20272）

《数据库管理系统安全技术要求》（GB/T20273）

《终端计算机系统安全等级技术要求》（GA/T671）

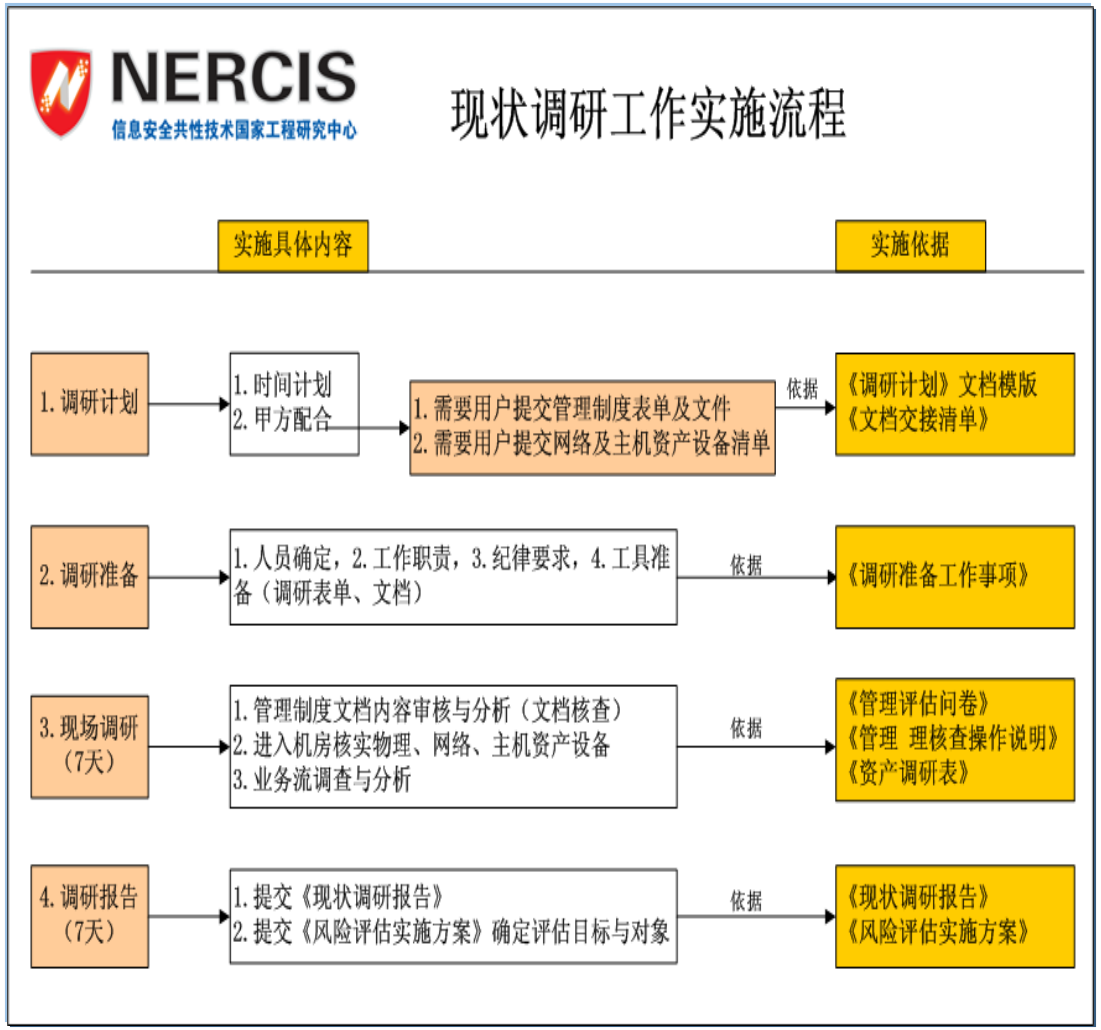
《信息系统安全管理要求》（GB/T20269）

《信息系统安全工程管理要求》（GB/T20282）

04、业务应用的系统安全检测与测试

（2）评估与合规性检测服务的一般性流程

（3）系统支撑环境的调研

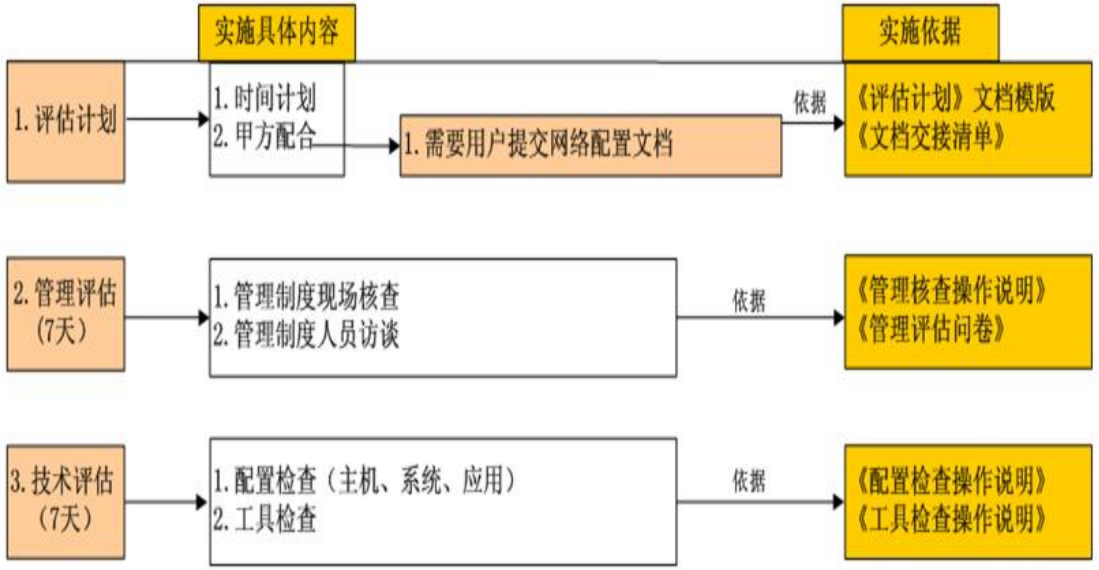


调研项目	调研重点关注内容	调研成果
核心网络设备	根据支撑软件运行的核心网络资产与拓扑核实物理位置与逻辑连接	《网络资产调研表》
主机/系统资产	根据支撑软件运行的主机资产清单表核实主机物理位置与逻辑连接	《主机资产调研表》
应用业务调研	业务内容，应用情况，使用现状，物理及逻辑连接	《应用资产调研表》
管理制度调研	人员访谈的方式完成配套管理制度调研，列出管理制度文档主机目录结构	《管理核查问卷》 《技术核查问卷》 《人员资产调研表》 《网络整体安全评估表 《服务器整体安全评估表》

- 《现状调研报告》
- 《系统安全检测与评估实施方案》

04、业务应用的系统安全检测与测试

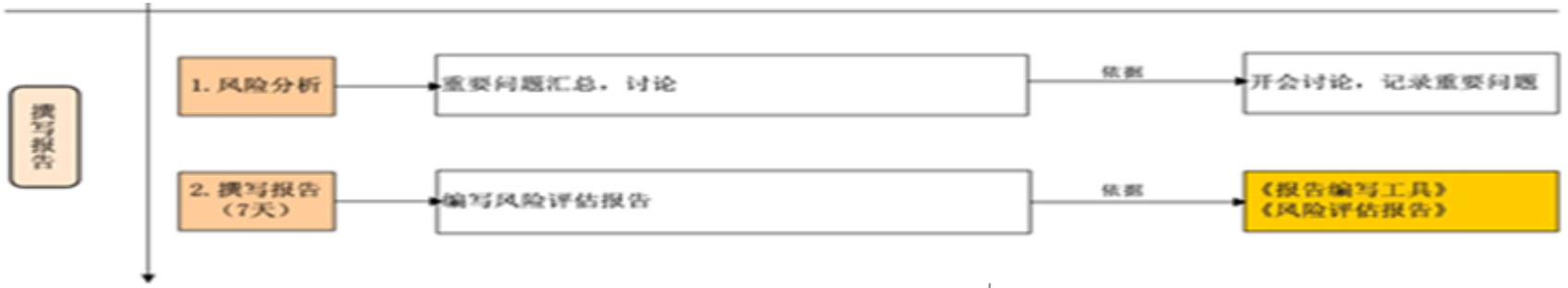
（4）系统和设备级的检查、检测和评估



检测/评估	重点工作内容与工作方式	成果
主机配置检查	依据主机配置评估表与操作手册，结合利用主机配置提取脚本完成主机系统的评估 **（系统配置抓图与脚本工具配置提取）**	《主机评估表单》 《重要问题列表》
网络配置检查	依据甲方提供的设备配置文档，利用网络设备评估表分析设备安全状况 **（安全设备配置抓图）**	《网络设备评估表单》 《重要问题列表》
系统漏洞扫描	对主机系统实施现场扫描（单线程）	生成《主机漏洞扫描报告》
管理制度核查	与主机、网络配置检查人员配合，识别管理制度的现状核查，**发现管理脆弱性，识别安全防护措施的有效性**	《脆弱性问题汇总报告》

04、业务应用的系统安全检测与测试

（5）检测、评估分析过程



- 资产分析
- 安全防护措施有效性分析
- 脆弱性分析
- 威胁分析
- 风险分析

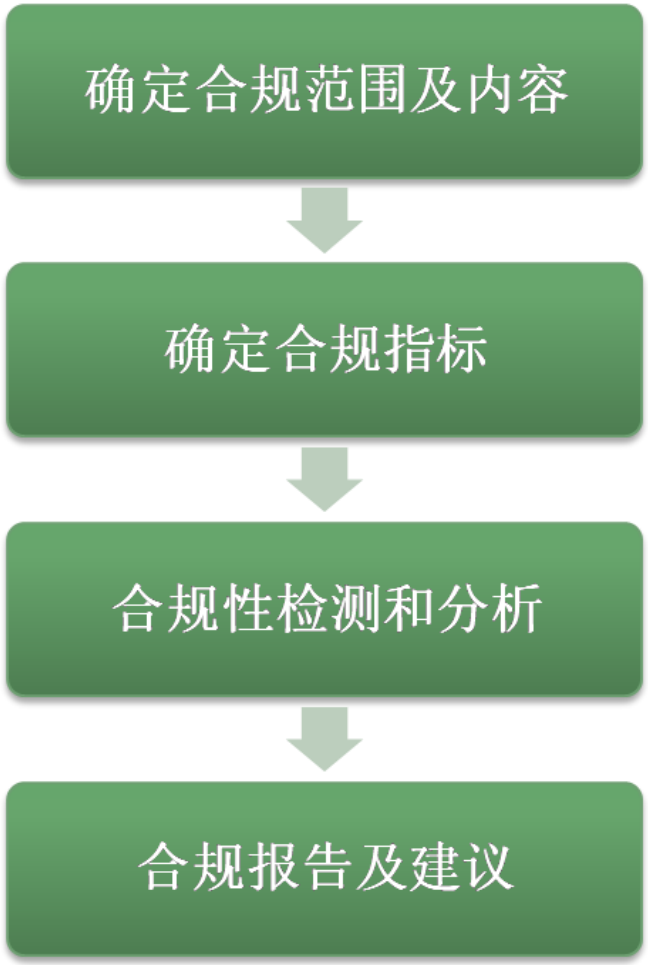
- 风险分析方法
- 资产分析
- 安全防护措施有效性分析
- 脆弱性分析
- 威胁分析
- 风险值计算

根据两个方面开展检测与评估工作：1、参考风险评估相关标准、等级保护相关标准，形成风险评估和等级保护差距分析；2、根据软件系统支撑的业务领域的相关标准，形成合规性分析；综合后形成该系统的安全检测与评估报告

（6）系统合规分析

采用合规性检测的方法分析信息系统中存在的安全问题和隐患，通过综合的检测分析，找出信息系统面临的风险，及合规性差异。

合规性检测过程共分四个部分，首先要确定合规性检测的范围和内容，然后确定合规指标，按照合规指标的要求进行合规性检测和分析，最后得出合规报告并提出整改的建议。



《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）

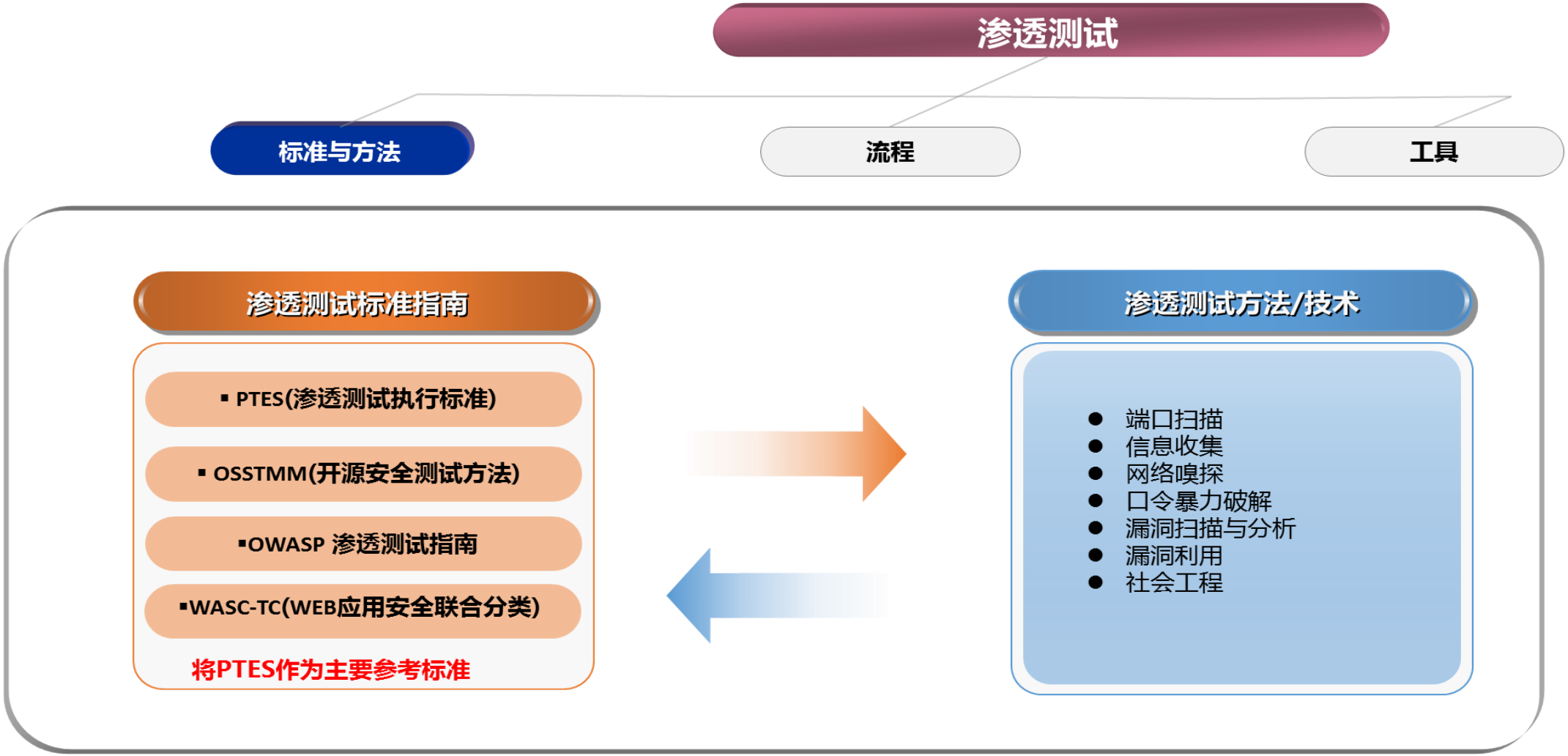
（7）系统安全检测/评估的意义

- 帮助准确了解信息系统安全现状；
- 帮助全面了解信息安全管理现状；
- 在安全事故爆发之前避免、减少或转移风险；
- 为系统建设及网络安全决策和管理提供依据；
- 满足相关政策法规（如：等级保护）要求。

目录

CONTENT

（1）渗透测试的标准和方法



（2）渗透测试的基本流程

渗透 测试

标准与方法　流程　工具

1.信息收集

- 系统架构、功能模块、网络拓扑、配置信息
- 开放端口
- 软件版本、所使用操作系统、数据库、中间件
- 身份认证、三权分立、审计功能
- 网络数据包抓取

2.漏洞分析

- 分析不安全项配置项
- 分析开放端口
- 分析软件、版本相关的漏洞依赖操作系统、数据库、web服务的相关漏洞
- 分析抓取的数据
- 分析分析身份认证、审计日志、三员管理，服务能否被卸载掉、绕过，明文存储口令

3.渗透攻击

- 对开放端口进行远程脚本利用
- 对口令进行破解，进行本地脚本利用
- 使用工具对web管理端进行sql注入、xss跨站、命令执行、敏感信息泄露等进行渗透
- 身份认证、审计日志、三员管理中的口令绕过、权限提升、停止审计渗透

4.报告输出

将安全检测中发现的问题
以及检测方法加以总结，
形成报告

（3）渗透测试的基本工具和环境

◆ 数据收集
- 通过漏洞扫描工具收集网络、主机、系统、应用已知漏洞信息，针对目前没有公开发布的溢出漏洞，采用人工综合获取。通过信息收集分析，测试者可以相应地、有针对性地制定入侵攻击的计划，提高入侵的成功率。信息收集的方法包括主机网络扫描、端口扫描、操作类型判别、应用判别、账号扫描、配置判别等等。

◆ 漏洞分析
- 通过分析收集来的数据，可发现高、中、低三个级别的风险、漏洞、溢出问题，组合成入侵者可能利用的途径，确认可以被利用的漏洞：

◆ 漏洞利用
- 利用网络边界设备配置漏洞、主机所提供的高风险服务、自行和外包开发的应用程序代码溢出、数据库调用注入等问题进行渗透测试。并通过漏洞提升操作权限跳转相邻可信系统。

◆ 缓冲区溢出测试
- 缓冲区溢出漏洞大量存在于各种应用中，通过向缓冲区写入超过缓冲区长度的内容，造成缓冲区溢出，破坏程序的堆栈，使程序转而执行其他的指令来获得系统特权等。

◆ 拒绝服务测试
- 通过构造发送长度超过65535字节的ICMP Echo Request 数据包、大量的SYN包、测试目标机防护TCP/IP协议栈崩溃的能力。

◆ 分布式拒绝服务测试
- 利用分散在因特网各处的测试服务器同时对目标机发起拒绝服务的操作，测试目标机对突发安全攻击事件的监察能力及抵御措施。

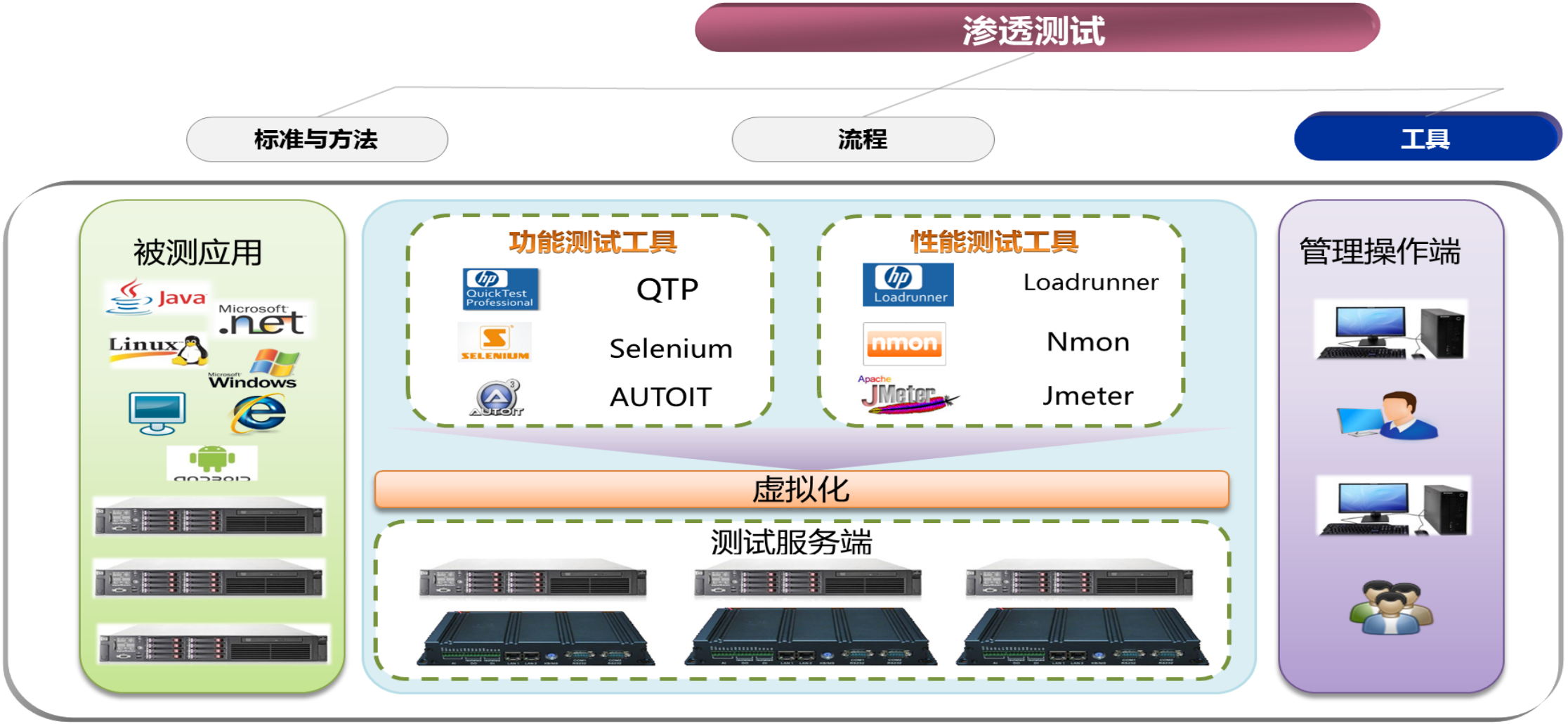
◆ DNS地址欺骗测试
- 利用RFC协议、BIND应用中的某些不完善的地方，获取特权身份执行任意命令。

◆ 数据库注入测试
- 提交特殊构建的一段数据库查询代码，根据程序返回的结果，获得敏感数据，测试输入数据的合法性判断的能力。

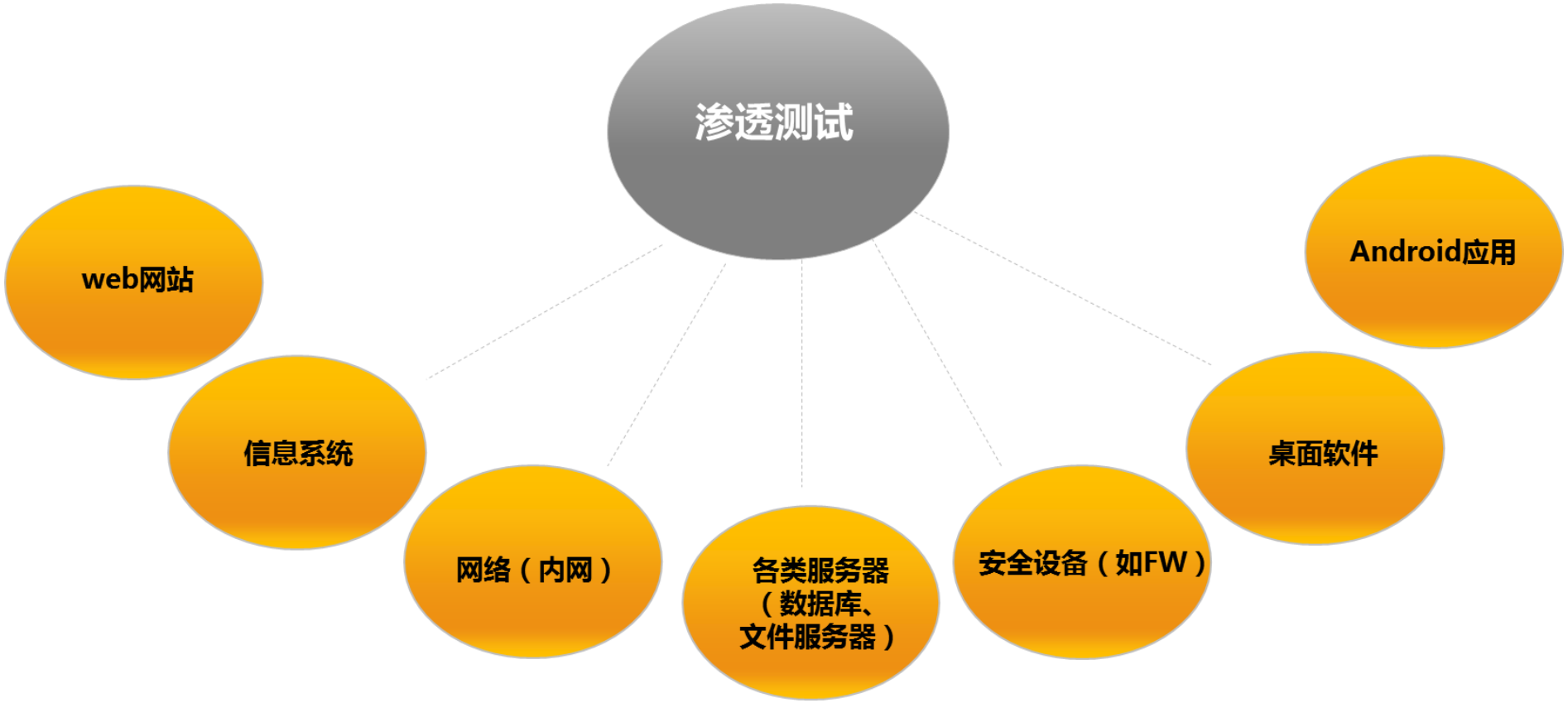
◆ 防火墙透穿测试
- 通过设备配置策略的合法服务及端口，获取敏感数据，并利用专业工具与技术建立隐秘隧道跳转可信网络。

- 边界区域安全超级漏扫设备
- IIS溢出分析利用工具
- 跨平台漏洞扫描设备
- 数据库漏洞扫描工具
- 应用服务探测设备
- DDOS模拟攻击工具
- 数据库注入利用工具
- 权限提升工具
- 数据旁路截取工具
- 恶意代码分析工具
- 加固脚本及系统CheckList
- ……

（3）渗透测试的基本工具和环境

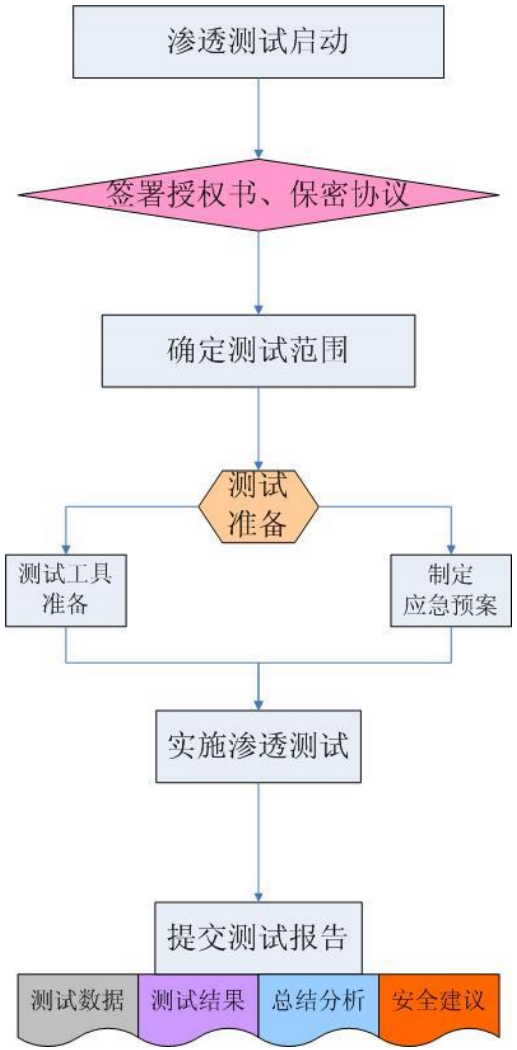


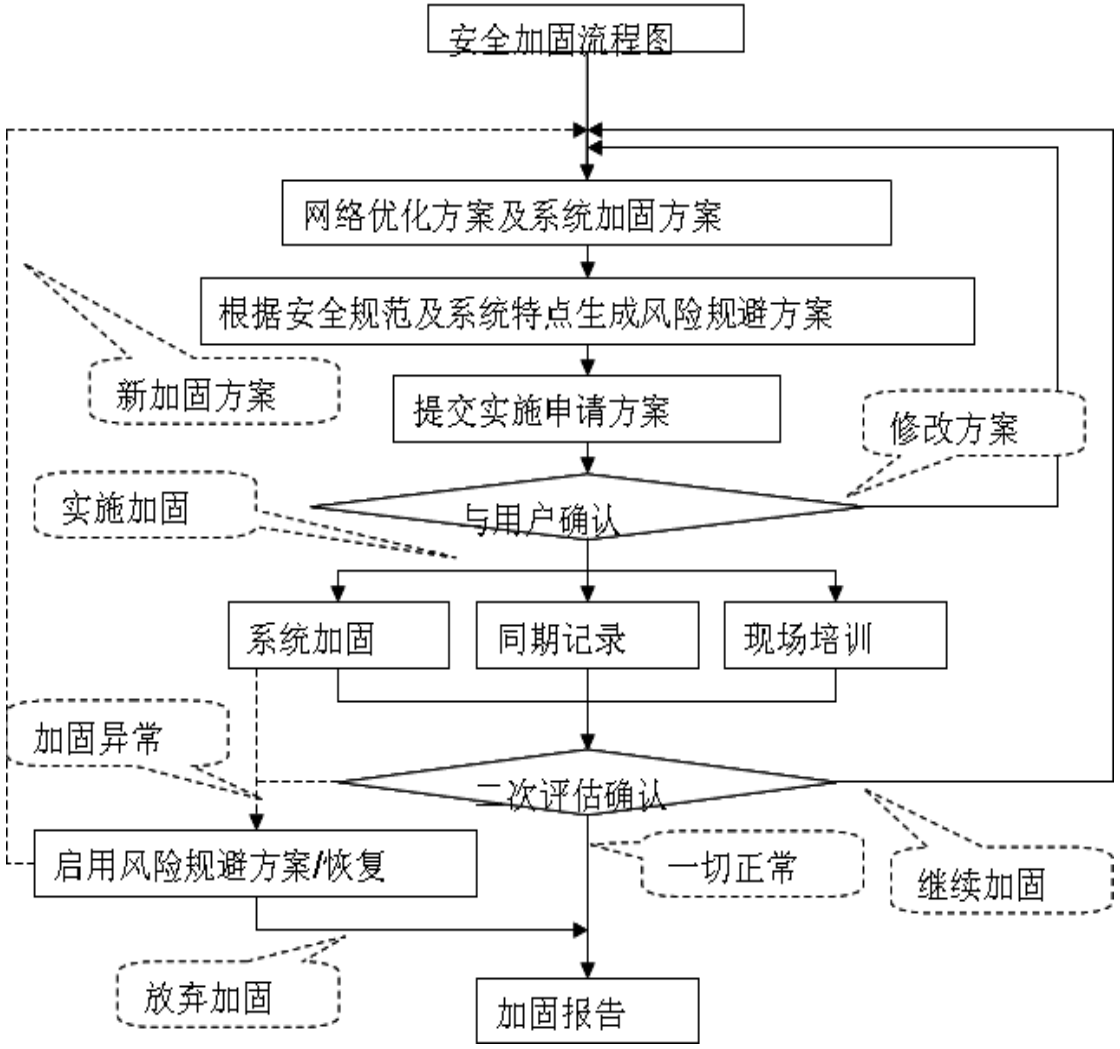
（4）测试对象类别


渗透测试
web网站
信息系统
网络（内网）
各类服务器（数据库、文件服务器）
安全设备（如FW）
桌面软件
Android应用

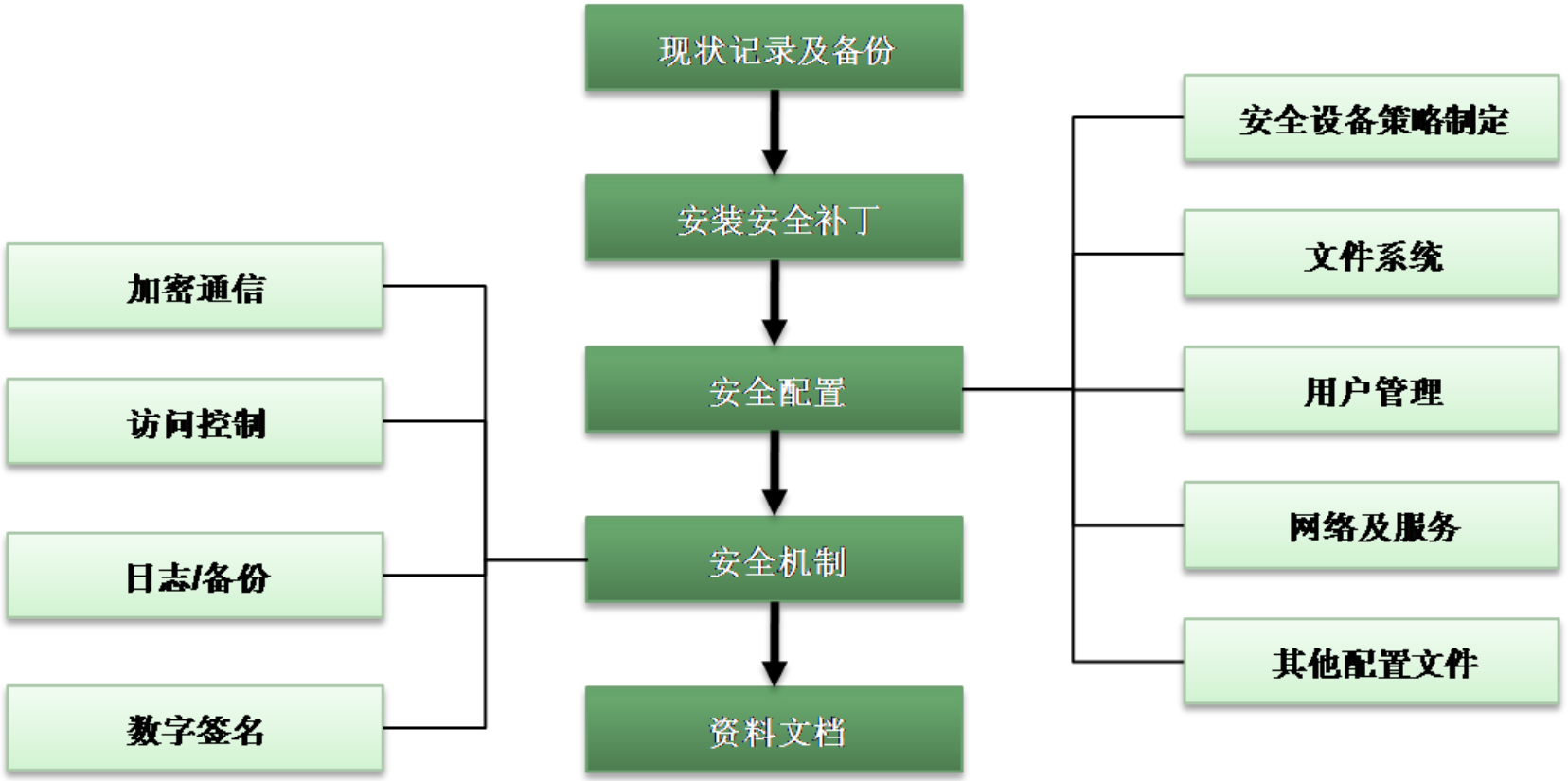
05、业务应用系统的渗透和攻防测试

（6）渗透攻防测试与系统加固





（6）渗透攻防测试与系统加固



（7）渗透测试与系统加固的意义和作用

- 帮助用户识别信息系统被入侵的可能性；
- 查找并封堵信息系统潜在的安全风险与漏洞；
- 验证信息系统目前安全措施的防护强度；
- 在入侵者发起攻击前封堵可能被利用的攻击途径；
- 为信息系统安全整改提供数据依据。

目录

CONTENT

06、软件系统安全评估　　（1）标准及模型

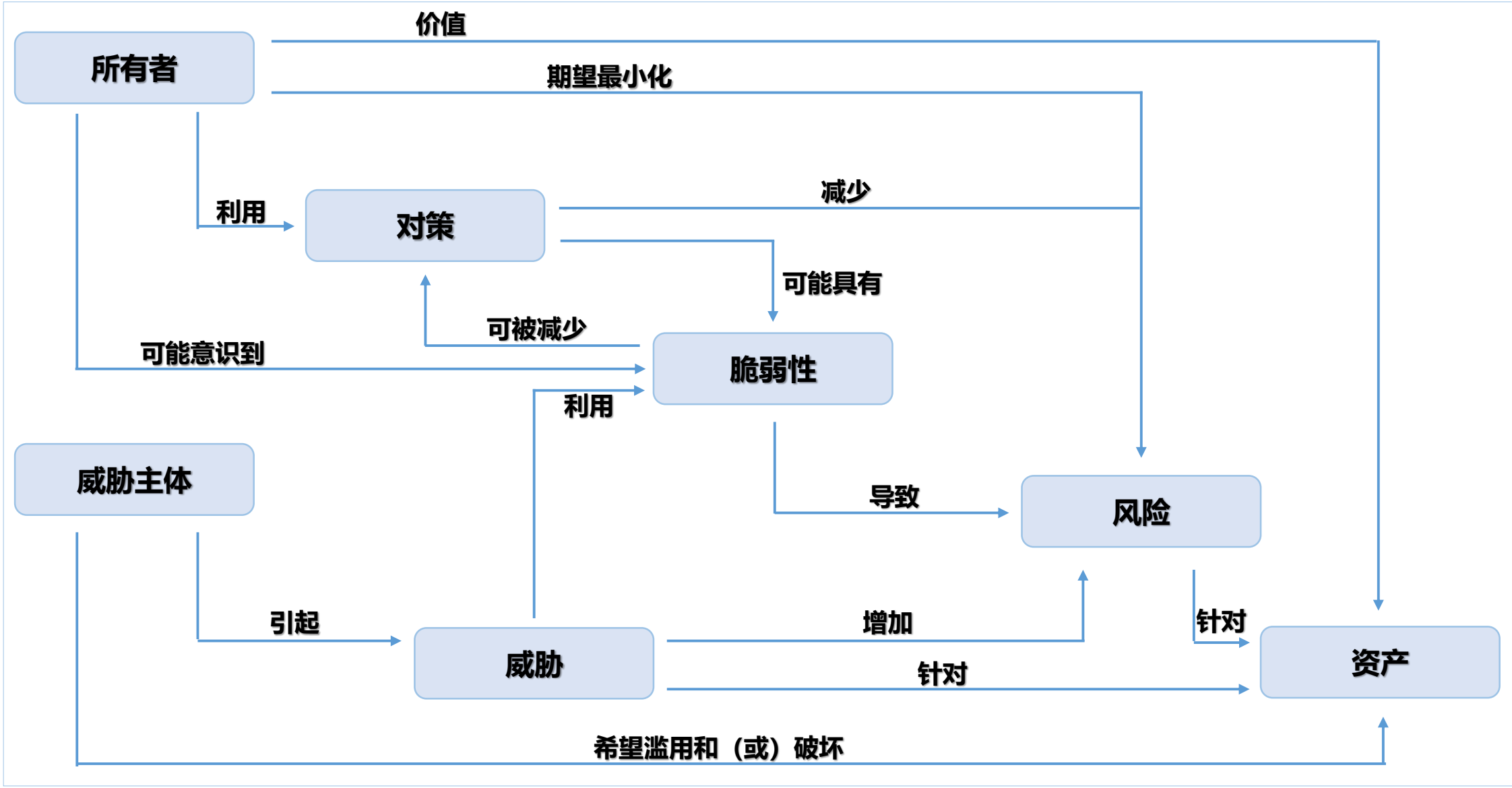
《信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型》（GB/T 18336.1-2008）
《安全技术 信息技术 信息技术安全性评估准则 第2部分：安全功能要求》（GB/T 18336.2-2008）
《信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求》（GB/T 18336.3-2008）

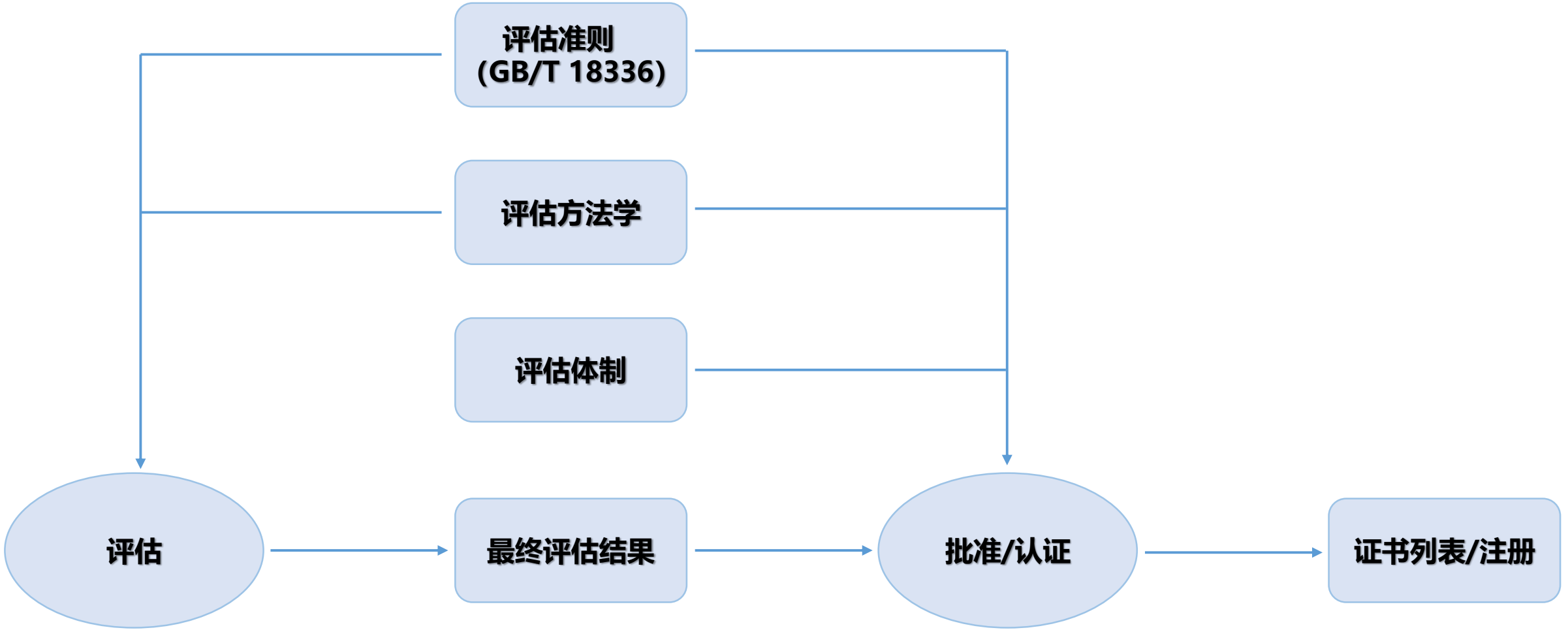
EAL1	功能测试级	适用在对正确运行要求有一定信心的场合，此场合下认为安全威胁并不严重。如：个人信息保护
EAL2	结构测试级	在交付设计信息和测试结果时，需要开发人员的合作。但在超出良好的商业运作的一致性方面，不要花费过多的精力。
EAL3	系统测试和检查级	在不大量更改已有合理才开发实现的前提下，允许一位尽责的开发人员在设计阶段从正确的安全工程中获得最大限度的保证。
EAL4	系统设计，测试和复查级	它使开发人员从正确的安全工程中获得最大限度的保证，这种安全工程基于良好的商业开发实践，这种实践很严格，但并不需要大量专业知识，技巧和其他资源。 在经济合理的条件下，对一个已经存在的生产线进行翻新时，EAL4是所能达到的最高级别。
EAL5	半形式化设计和测试级	开发者能从安全工程中获得最大限度的安全保证，该安全工程是基于严格的商业开发实践，靠适度应用专业安全工程技术来支持的。EAL5以上的级别是军用信息设备，用于公开密钥基础设施的信息设备应达到的标准。
EAL6	半形式化验证设计和测试级	开发者通过安全工程技术的应用和严格的开发环境获得高度的认证，保护高价值的资产能够对抗重大风险。
EAL7	形式化验证设计和测试级	适用于风险非常高或有高价值资产值得更高开销的地方。

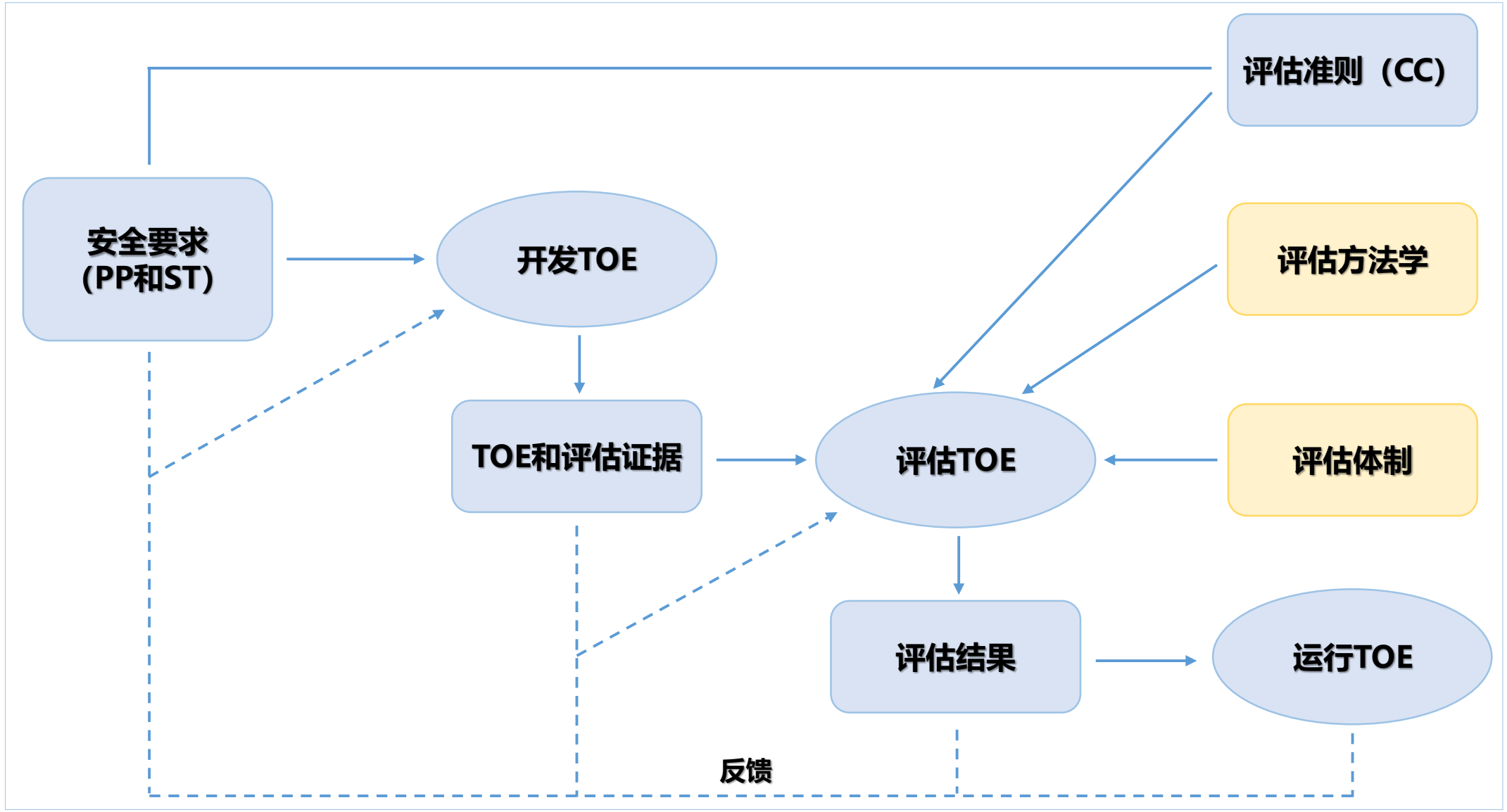
CC：通用准则(Common Criteria)
EAL：评估保证级(Evaluation Assurance Level)
IT：信息技术(Information Technology)
PP：保护轮廓(Protection Profile)
SF：安全功能(Security Function)
SFP：安全功能策略(Security Function Policy)
SOF：功能强度(Strength of Function)

ST：安全目标(Security Target)
TOE：评估对象(Target of Evaluation)
TSC：TSF 控制范围(TSF Scope of Control)
TSF：TOE 安全功能(TOE Security Functions)
TSFI：TSF 接口(TSF Interface)
TSP：TOE 安全策略(TOE Security Policy)

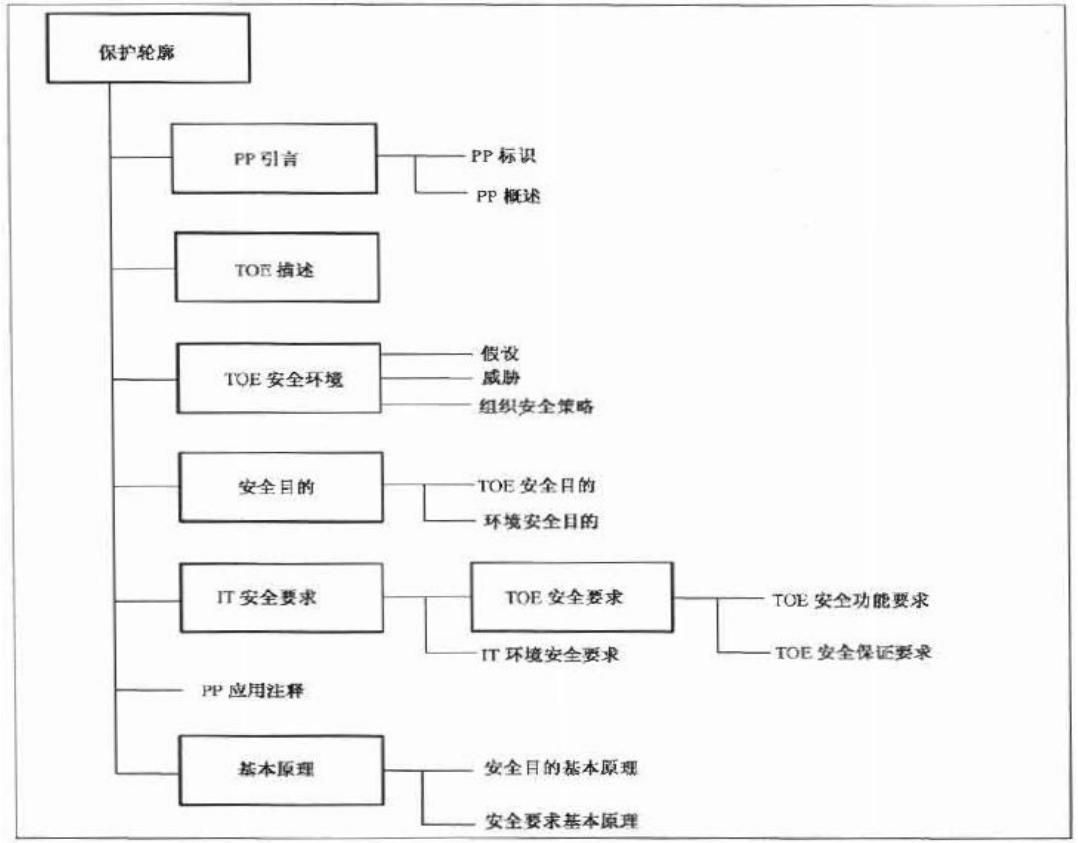
06、软件系统安全评估　　（2）安全概念及其关系

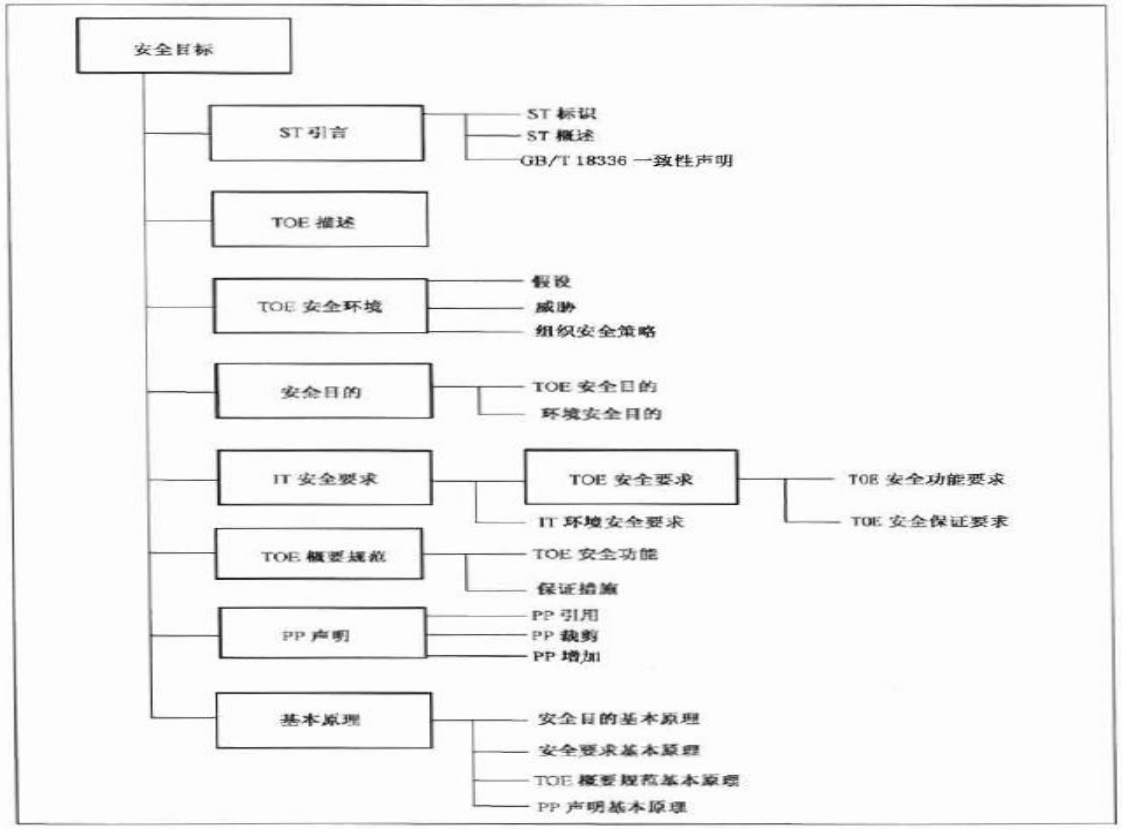



评估准则
(GB/T 18336)
评估方法学
评估体制
评估
最终评估结果
批准/认证
证书列表/注册


评估准则（CC）
安全要求
(PP和ST)
开发TOE
评估方法学
TOE和评估证据
评估TOE
评估体制
评估结果
运行TOE
反馈

保护轮廓（PP）：一个PP为一类TOE定义了一组与实现无关的IT安全要求。这类TOE试图满足客户对IT安全性的通用需求，因此客户不必依赖特定TOE就能构建或引用一个PP来表示他们的IT安全需求。



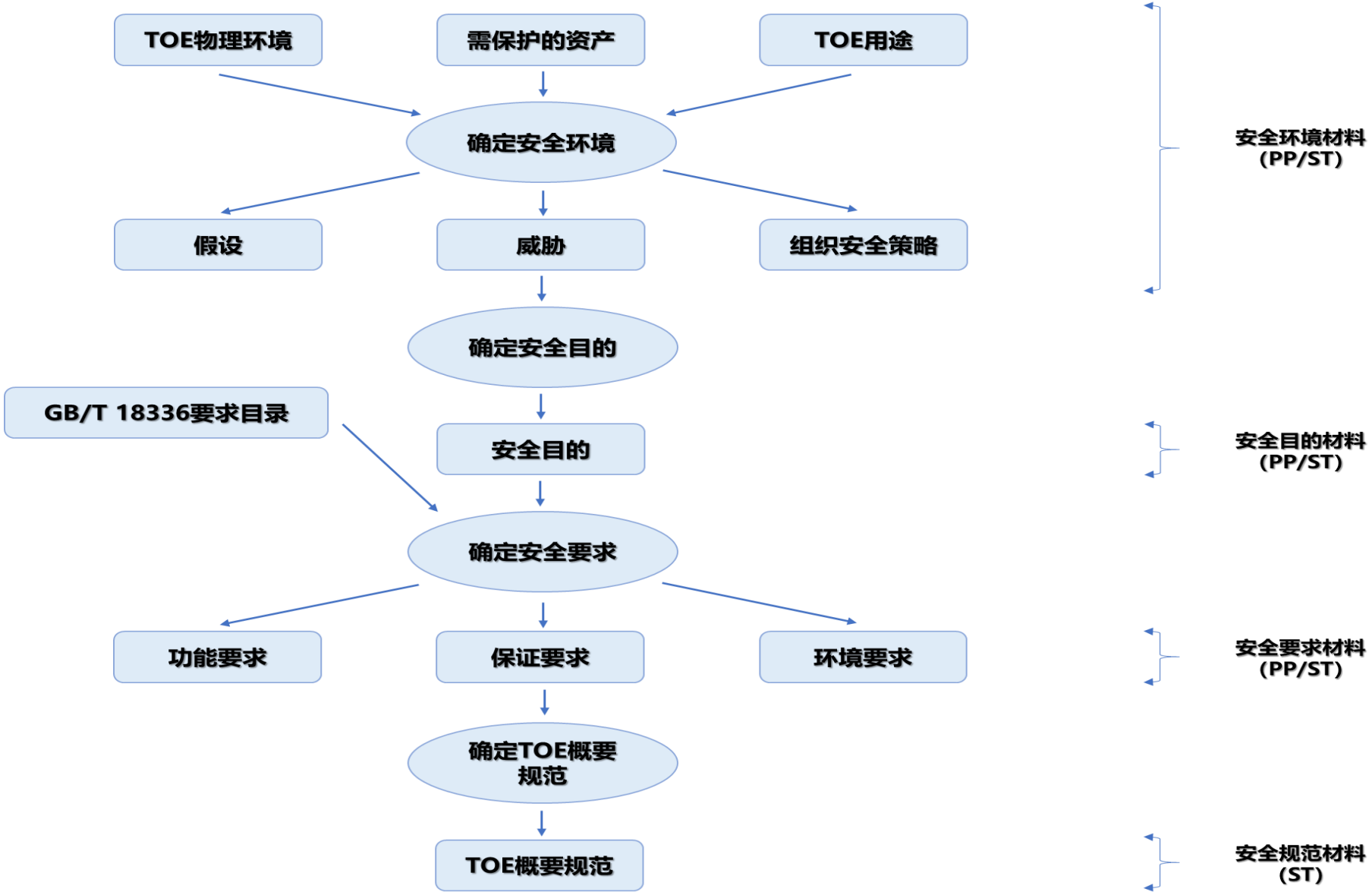


安全目标（ST）：一个ST包含一个既定TOE的IT安全要求，并规定了该TOE应提供的安全功能和保证措施以满足所提出的安全要求。一个TOE的ST是开发者、评估者和适当的客户之间对TOE安全特性和评估范围达成一致的基础，ST的读者不限于那些对TOE生产和评估负有责任的人员，那些负责管理、营销、才有、安装、配置、操作和使用TOE的人员也可以是ST的读者。
ST可合并一个或多个PP的要求或宣称符合一个或多个PP。

功能类和保证类	
功能（11）	保证（10）
FAU类：安全审计	APE类：PP评估
FCO类：通信	ASE类：ST评估
FCS类：密码支持	ACM类：配置管理
FDP类：用户数据保护	ADO类：交付和运行
FIA类：标识和鉴别	ADV类：开发
FMT类：安全管理	AGD类：指导性文档

功能类和保证类	
功能（11）	保证（10）
FPR类：隐私	ALC类：生命周期支持
FPT类：安全功能保护	ATE类：测试
FRU类：资源利用	AVA类：脆弱性评定
FTA类：TOE访问功能类和保证类	AMA类：维护
FTP类：可信路径/信道	

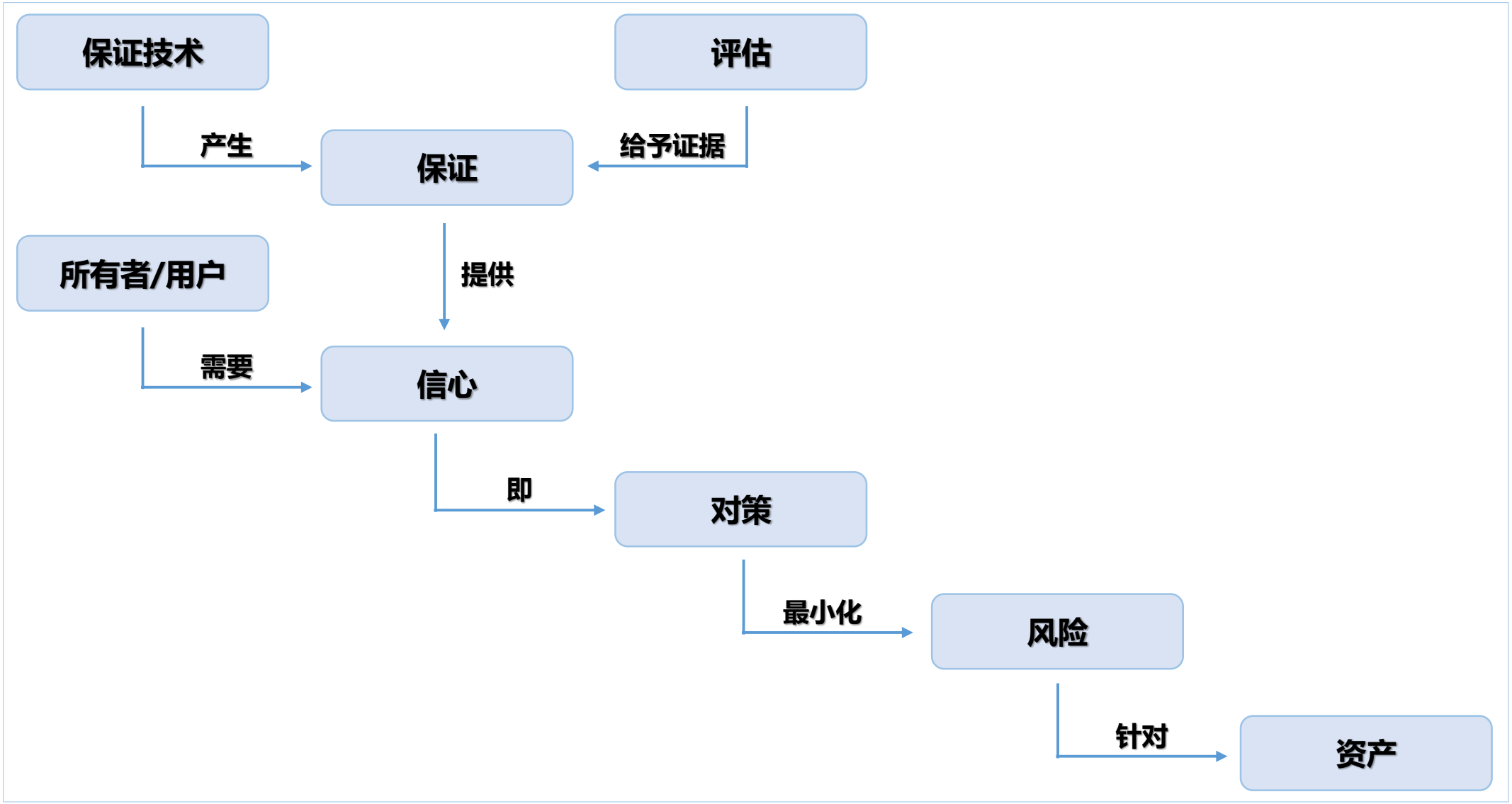
06、软件系统安全评估　　（4）要求与规范的导出



06、软件系统安全评估　　（5）评估保证级

保证类	保证族	评估保证级所包含的保证组件						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
配置管理	ACM_AUT　CM 自动化				1	1	2	2
	ACM_CAP　CM 能力	1	2	3	4	4	5	5
	ACM_SCP　CM 范围			1	2	3	3	3
交付和运行	ADO_DEL　交付		1	1	2	2	2	3
	ADO_IGS　安装、生成和启动	1	1	1	1	1	1	1
开发	ADV_FSP　功能规范	1	1	1	2	3	3	4
	ADV_HLD　高层设计		1	2	2	3	4	5
	ADV_IMP　实现表示				1	2	3	3
	ADV_INT　TSF 内部					1	2	3
	ADV_LLD　低层设计				1	1	2	3
	ADV_RCR　表示对应性	1	1	1	1	2	2	3
	ADV_SPM　安全策略模型				1	3	3	3
指导性文档	AGD_ADM　管理员指南	1	1	1	1	1	1	1
	AGD_USR　用户指南	1	1	1	1	1	1	1
生命周期支持	ALC_DVS　开发安全			1	1	1	2	2
	ALC_FLR　缺陷纠正							
	ALC_LCD　生命周期定义				1	2	2	3
	ALC_TAT　工具和技术				1	2	3	3
测试	ATE_COV　测试覆盖		1	2	2	2	3	3
	ATE_DPT　测试深度			1	1	2	2	3
	ATE_FUN　功能测试		1	1	1	1	2	2
	ATE_IND　独立测试	1	2	2	2	2	2	3
脆弱性评定	AVA_CCA　隐蔽信道分析					1	2	2
	AVA_MSU　误用			1	2	2	3	3
	AVA_SOF　TOE 安全功能强度		1	1	1	1	1	1
	AVA_VLA　脆弱性分析		1	1	2	3	4	4

06、软件系统安全评估　　（8）通用评估准则评估的意义和作用



目录

CONTENT

07、服务总结

（1）国家级CNAS测评实验室

中国合格评定国家认可委员会

实验室认可证书

（注册号：CNAS L7966）

兹证明：

中科信息安全共性技术国家工程研究中心有限公司

北京市海淀区杏石口路中部 65 号益园文化创意产业基地 C 区 1 号楼 4 层，100195

符合 ISO/IEC 17025：2005《检测和校准实验室能力的通用要求》（CNAS-CL01《检测和校准实验室能力认可准则》）的要求，具备承担本证书附件所列检测服务的能力，予以认可。

获认可的能力范围见标有相同认可注册号的证书附件，证书附件是本证书组成部分。

签发日期：2015-09-15

有效期至：2018-09-14

初次认可：2015-09-15

中国合格评定国家认可委员会授权人

中国合格评定国家认可委员会（CNAS）经国家认证认可监督管理委员会（CNCA）授权，负责实施合格评定国家认可制度。CNAS是国际实验室认可合作组织（ILAC）和亚太实验室认可合作组织（APLAC）的多边互认协议成员。本证书的有效性可登陆www.cnas.org.cn获认可的机构名录查询。

CNAS检测服务实验室认可

四层体系文件

1. 质量手册
2. 程序文件
3. 指导类/规范类手册
4. 技术/质量记录表格

07、服务总结

（2）完善的测试管理流程

标准的测试管理流程

测试用例管理

- 测试执行
- 测试数据
- 测试环境
- 测试套件
- 测试脚本
- 测试工具
- 手工测试
- 自动化测试

测试计划管理

- 集成测试目标
- 新功能测试目标
- 功能回归测试目标
- 系统性能测试目标

测试缺陷管理

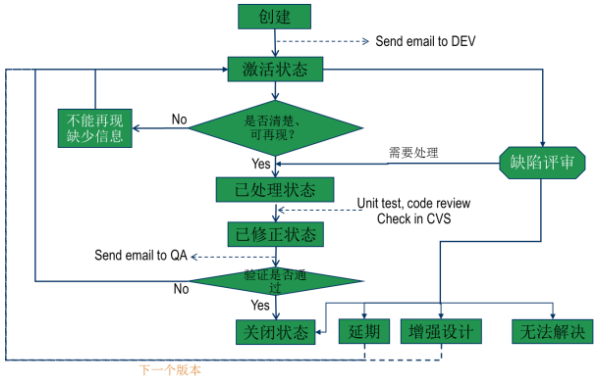
- 缺陷报告
- 缺陷生命周期
- 缺陷跟踪
- 趋势分析
- 分布分析
- 缺陷清除率
- 质量评估
- 缺陷预防

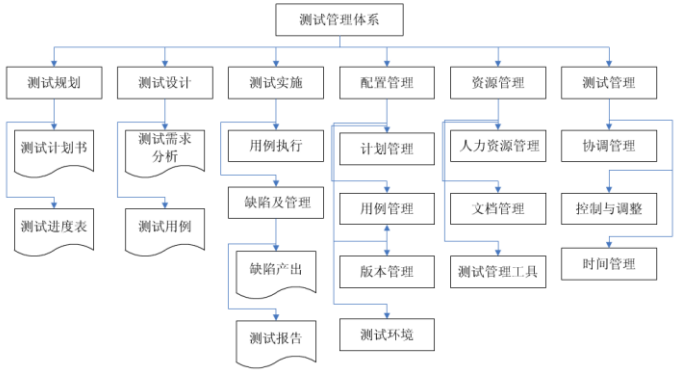
测试阶段管理

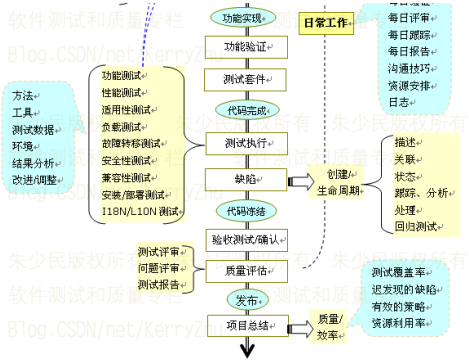
- 需求审查
- 设计审查
- 单元测试
- 集成测试
- 系统测试
- 验收测试
- α/β测试
- 回归测试
- 冒烟测试

测试风险管理

- 需求变更，测试人员、环境、技术、工具等
- 广度、深度
- 风险评估与控制
- 寻找缓解风险的策略
- 体现在测试计划中
- 在测试过程中进行监控和处理

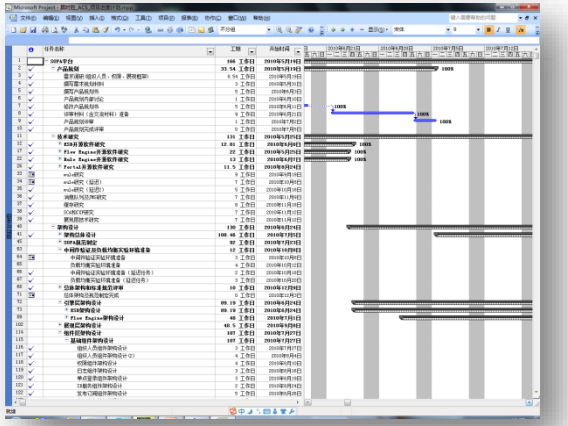




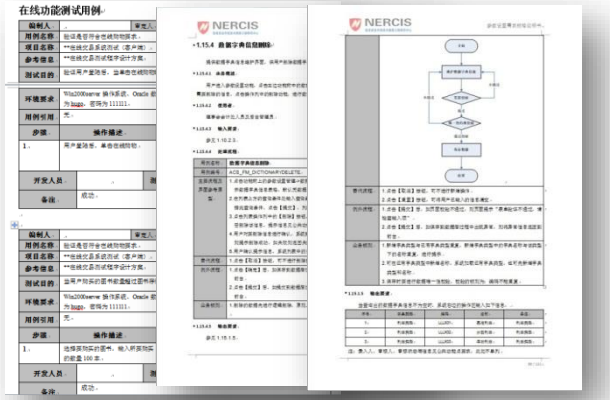


07、服务总结　　（2）完善的测试管理流程

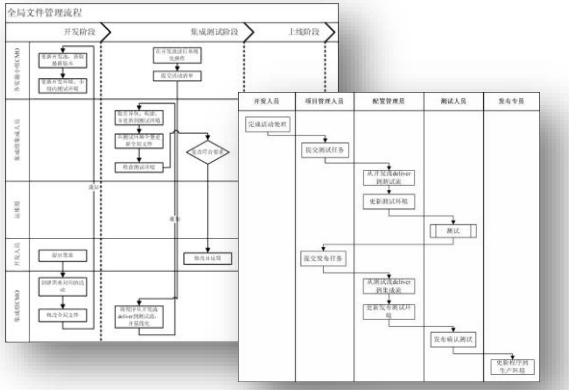
测试规划管理



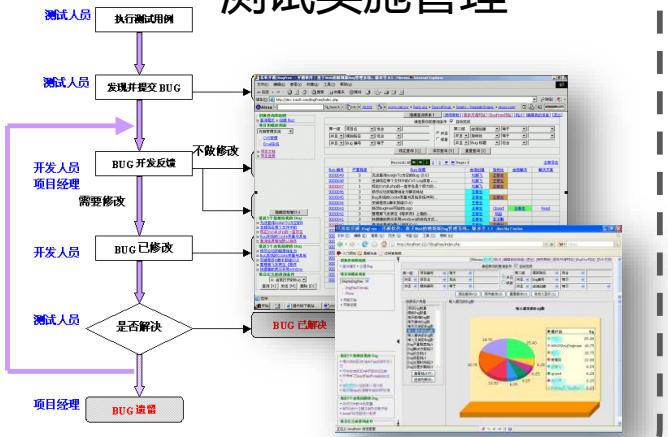
测试设计管理



测试配置管理



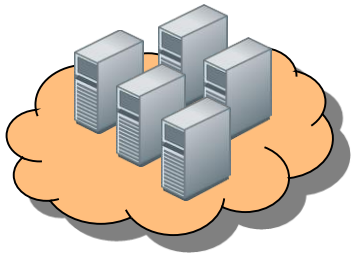
测试实施管理



（2）完善的测试管理实践

信息安全产品

安卓智能手机



云服务平台

国产软硬件平台相关产品

针对信息安全产品、移动终端、云平台以及国产软硬件平台相关产品等进行测评，依据安全测评的技术、方法、标准和流程，提供全周期的软件产品测评服务。

- 功能测试
- 性能测试
- 安全性测试
- 易用性测试
- 接口测试
- 集成测试

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE