第五部分：CC与信息安全工程

CC（Common Criteria）综述

CC（Common Criteria）

- 共同准则(Common Criteria)是一个国际认可的ISO标准（ISO15408），被用于政府以及其他组织去评定IT产品的安全和保障
- CC标准提供了唯一的方式去表达安全需求并定义一套严格的准则；
- 通过该准则，产品的安全方面（比如，开发环境，安全功能性，和安全弱点的处理）能被有的放矢的进行评估。

CC的基本结构

- 三个部分
  - 第一部分 简介和一般模型
  - 第二部分 安全功能要求
  - 第三部分 安全保证要求
- 配套的评估方法
  - 信息技术安全通用评估方法（CEM、ISO/IEC 18045）

CC评价准则的结构

- **第一部分：介绍和总体模型**
  - 对CC评价准则的介绍。定义IT安全评价和描述模型的一般概念和原则，提出选择和定义说明产品和系统IT安全客体的明确的组织的安全要求。
- **第二部分：安全功能要求**
  - 用标准化的方法对评价目标（TOE）建立一个明确的安全要求的部件功能集合。功能集合分类为部件（components）、族（families）和类（classes）

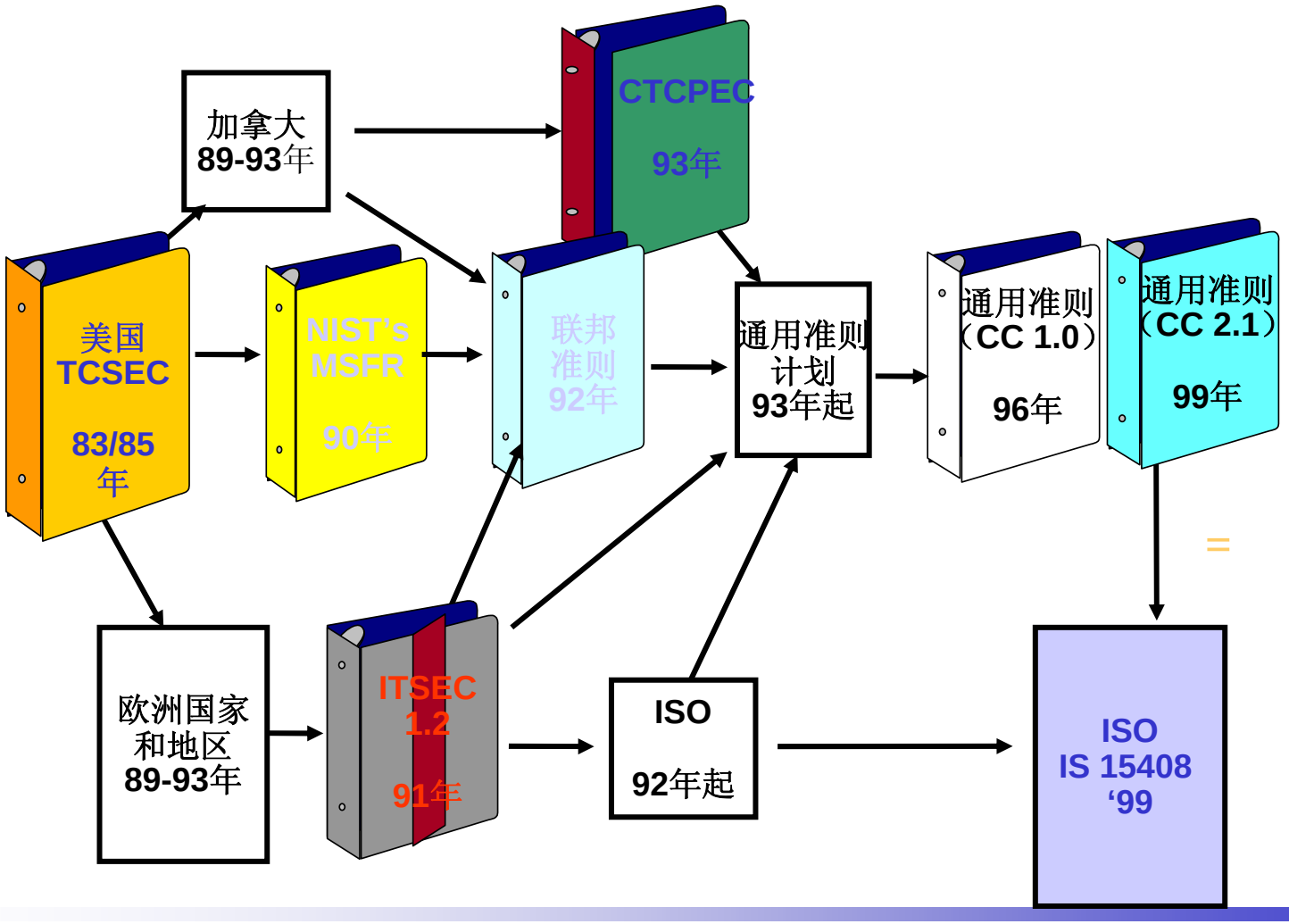
CC评价准则的结构

- **第三部分：安全保证要求**
  - 用标准化的方法对评价目标（TOE）建立一个明确的安全要求的保证部件的集合。对保护方案（PP）和安全目标（ST）进行定义，并且对安全评价目标（TOE）提出安全评价保证级别（EAL）

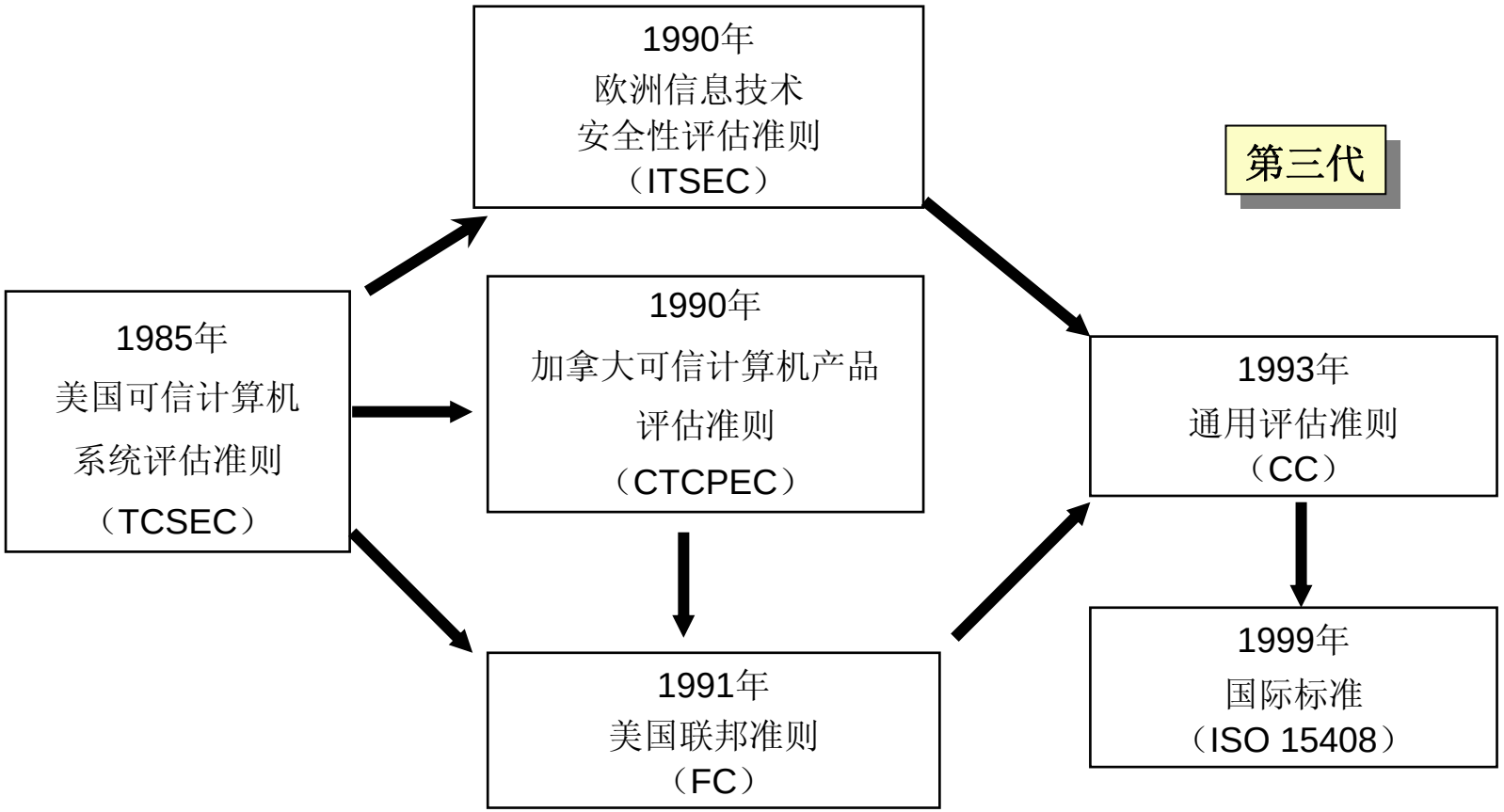
CC标准的读者对象

- 用户：通过风险和策略的分析，比较评价的不同产品和系统，选择适合自己使用的产品和系统。
- 开发者：支持开发者认识满足自己产品和系统的安全要求，制定保护轮廓（PP），确定安全目标（ST），支持开发者开发自己的评价目标（TOE），在评价方法学帮助开发者，以共识的评价结果评价自己开发的产品和系统。
- 评价者：正式审查评价目标时为评价者提供一个评价准则，用于评价评价目标（TOE）和安全要求的一致性
- 其它：对于对IT安全有兴趣和有责任的人起到一个导向和参考材料的作用，机构中的系统监管和安全官员确定安全策略和要求

测评标准的发展过程

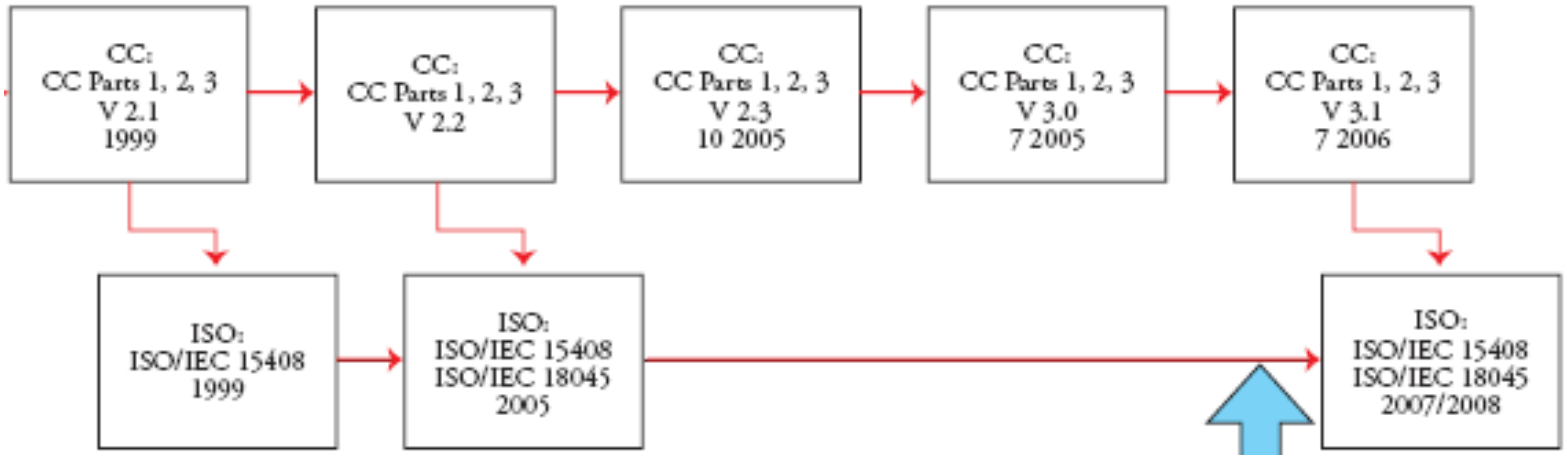

加拿大
89-93年
CTCPEC
93年
美国
TCSEC
83/85
年
NIST's
MSFR
90年
联邦
准则
92年
通用准则
计划
93年起
通用准则
（CC 1.0）
96年
通用准则
（CC 2.1）
99年
=
欧洲国家
和地区
89-93年
ITSEC
1.2
91年
ISO
92年起
ISO
IS 15408
'99

CC标准的由来


1990年
欧洲信息技术
安全性评估准则
（ITSEC）
第三代
1985年
美国可信计算机
系统评估准则
（TCSEC）
1990年
加拿大可信计算机产品
评估准则
（CTCPEC）
1993年
通用评估准则
（CC）
1991年
美国联邦准则
（FC）
1999年
国际标准
（ISO 15408）

CC标准的发展

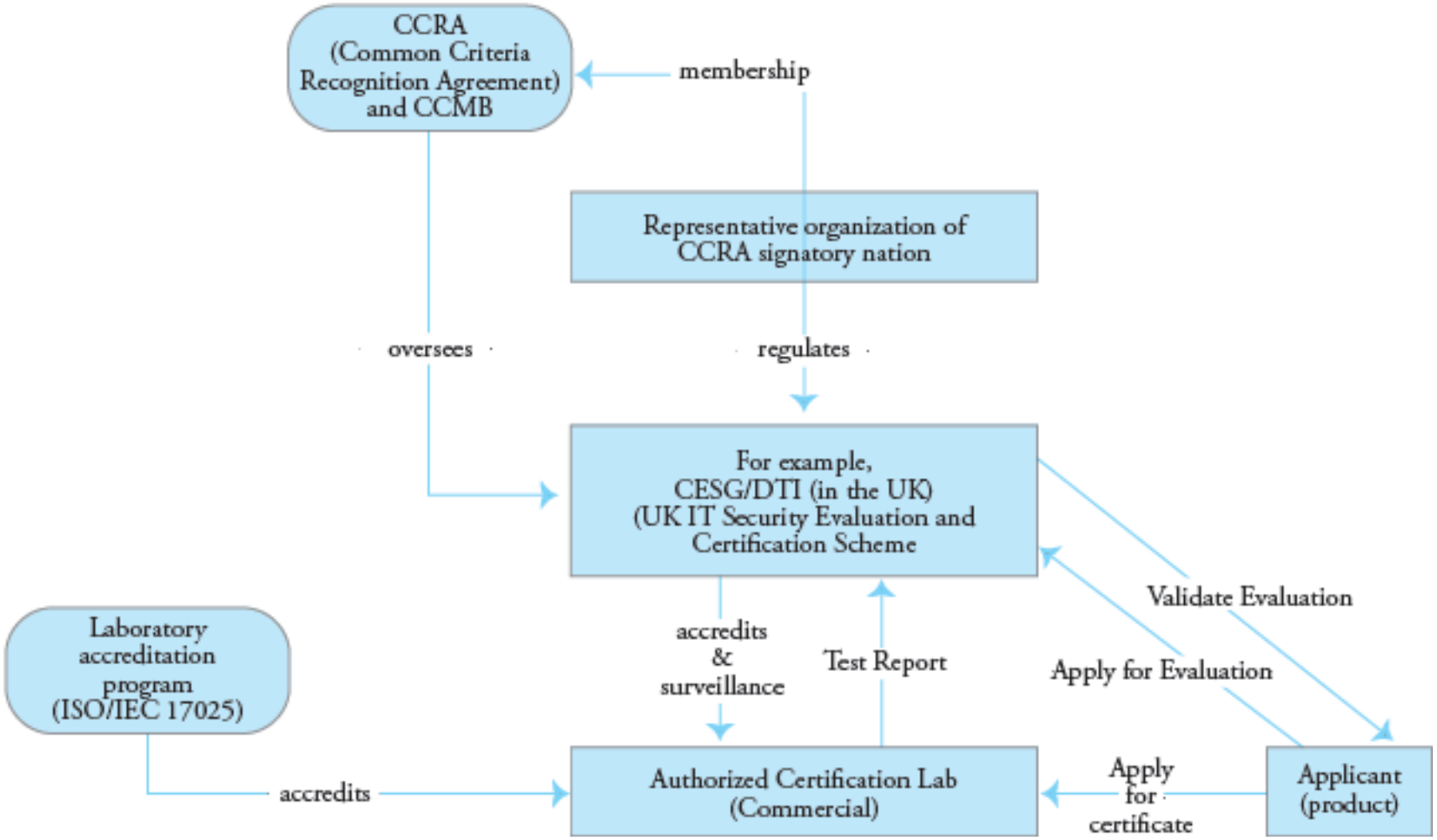
- CC标准 1993.6 启动
- CC1.0 1996.1 出版
- CC2.0 1998.5 出版
- CC2.1 ISO/IEC15408 1999.12 GB/T 18336-2001
  - Information technology—Security techniques—Evaluation criteria for IT security
- ISO/IEC SC 27 ——WG 3 established to focus on CC-related work items



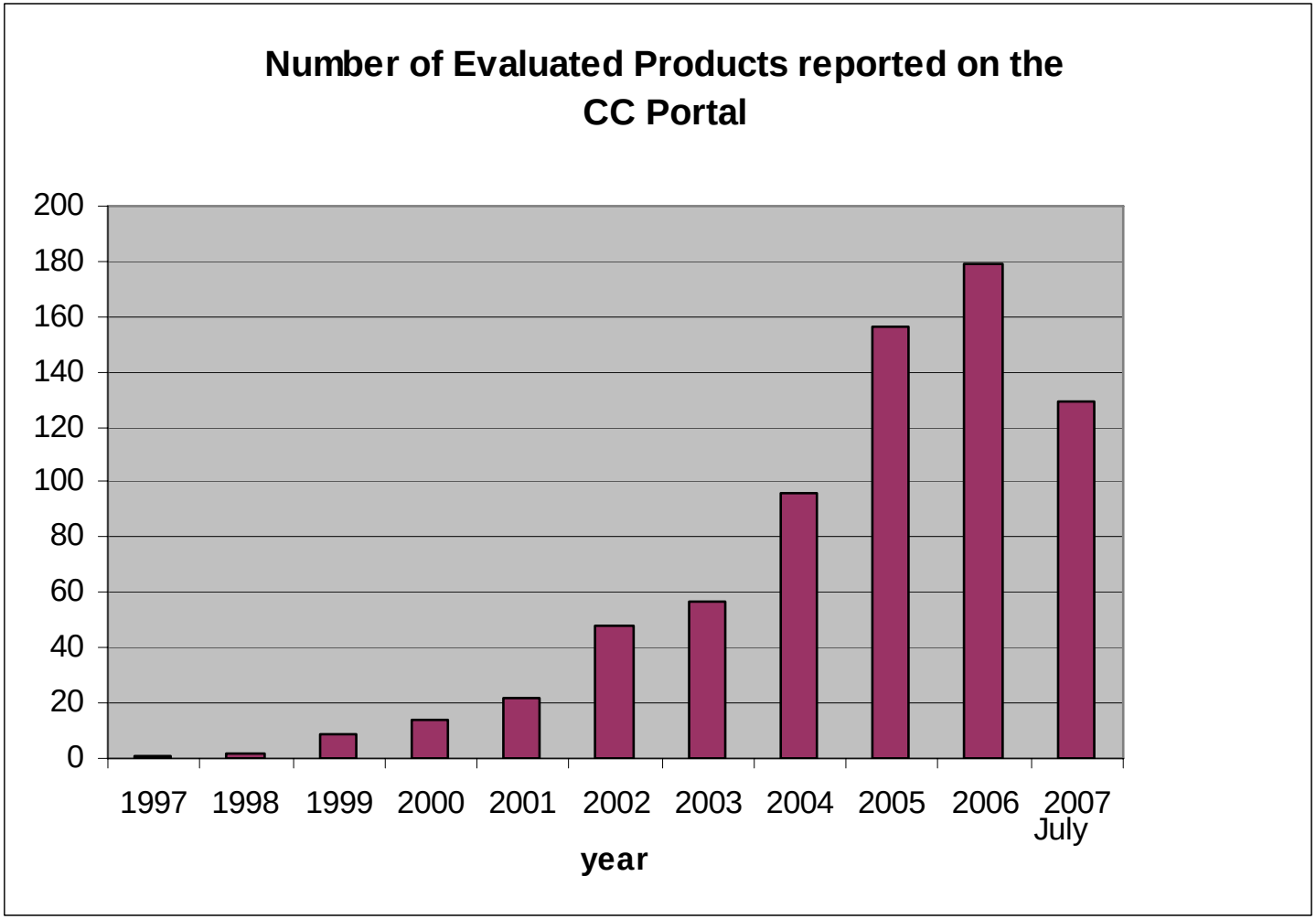
CCRA通用评估准则互认协定

- CC Recognition Arrangement (CCRA) 1998.10签署
- 明确了该体系下认证产品可以得到广泛的认可，目前互认的安全保证级别（EAL）最高为4级，该协定组织明确规定了通用评估准则和相关的通用评估方（CEM:Common Evaluation Methodology）作为互认协定所使用的标准基础。
- 24个成员国（12个Certificate authorizing，12个Certificate consuming），中国未加入
  - Certificate authorizing拥有自己的评估认证体系进行认证证书的颁发并接受互认，它们是澳大利亚、加拿大、法国、德国、日本、韩国、荷兰、新西兰、挪威、西班牙、英国和美国；
  - Certificate consuming可以接受和认可来自上述国家颁发的认证结果，它们是奥地利、捷克、丹麦、芬兰、希腊、匈牙利、印度、以色列、意大利、新加坡、瑞典和土耳其

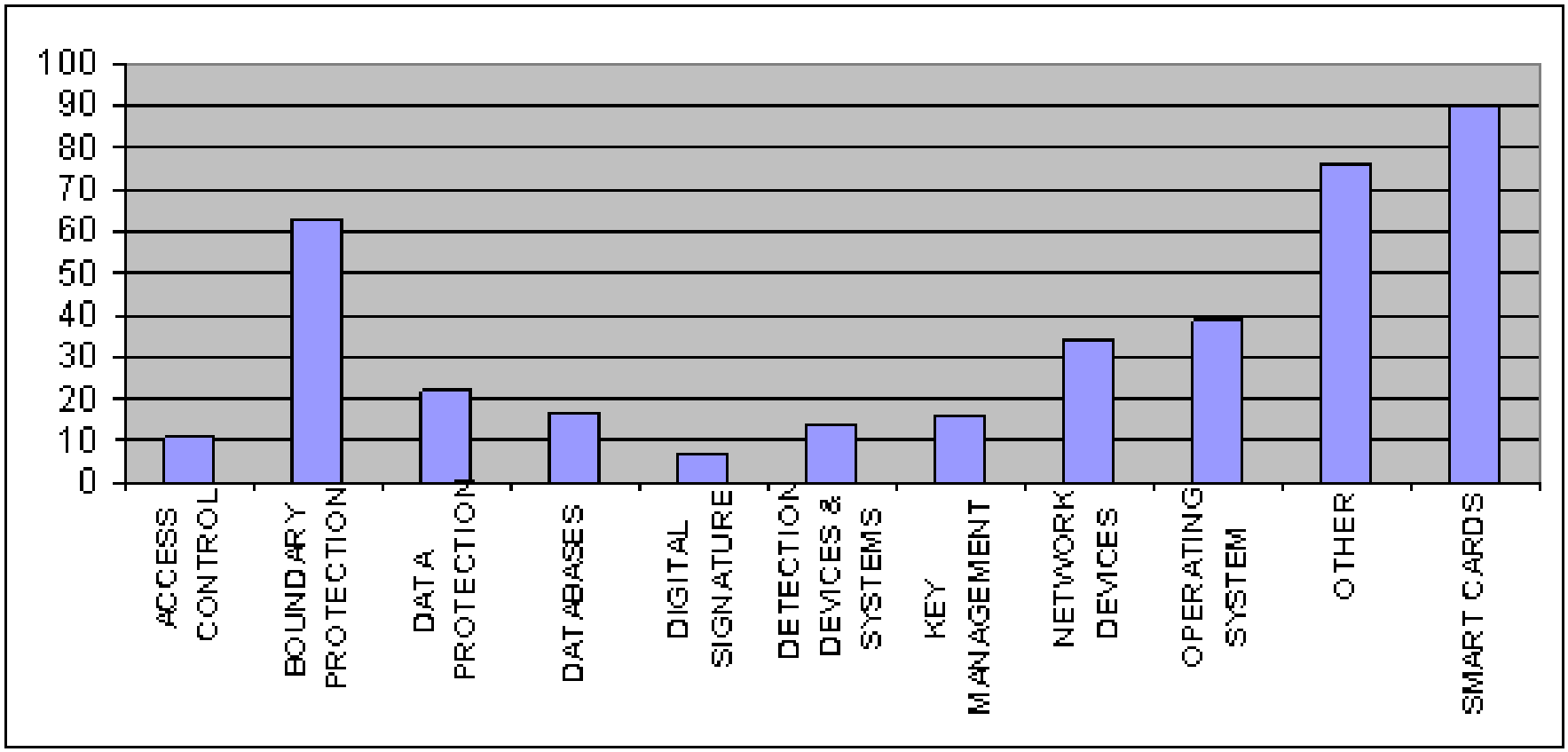
CCRA认证体系


CCRA
(Common Criteria
Recognition Agreement)
and CCMB
membership
Representative organization of
CCRA signatory nation
oversees
regulates
For example,
CESG/DTI (in the UK)
(UK IT Security Evaluation and
Certification Scheme
Validate Evaluation
Laboratory
accreditation
program
(ISO/IEC 17025)
accredits
&
surveillance
Test Report
Apply for Evaluation
accredits
Authorized Certification Lab
(Commercial)
Apply
for
certificate
Applicant
(product)

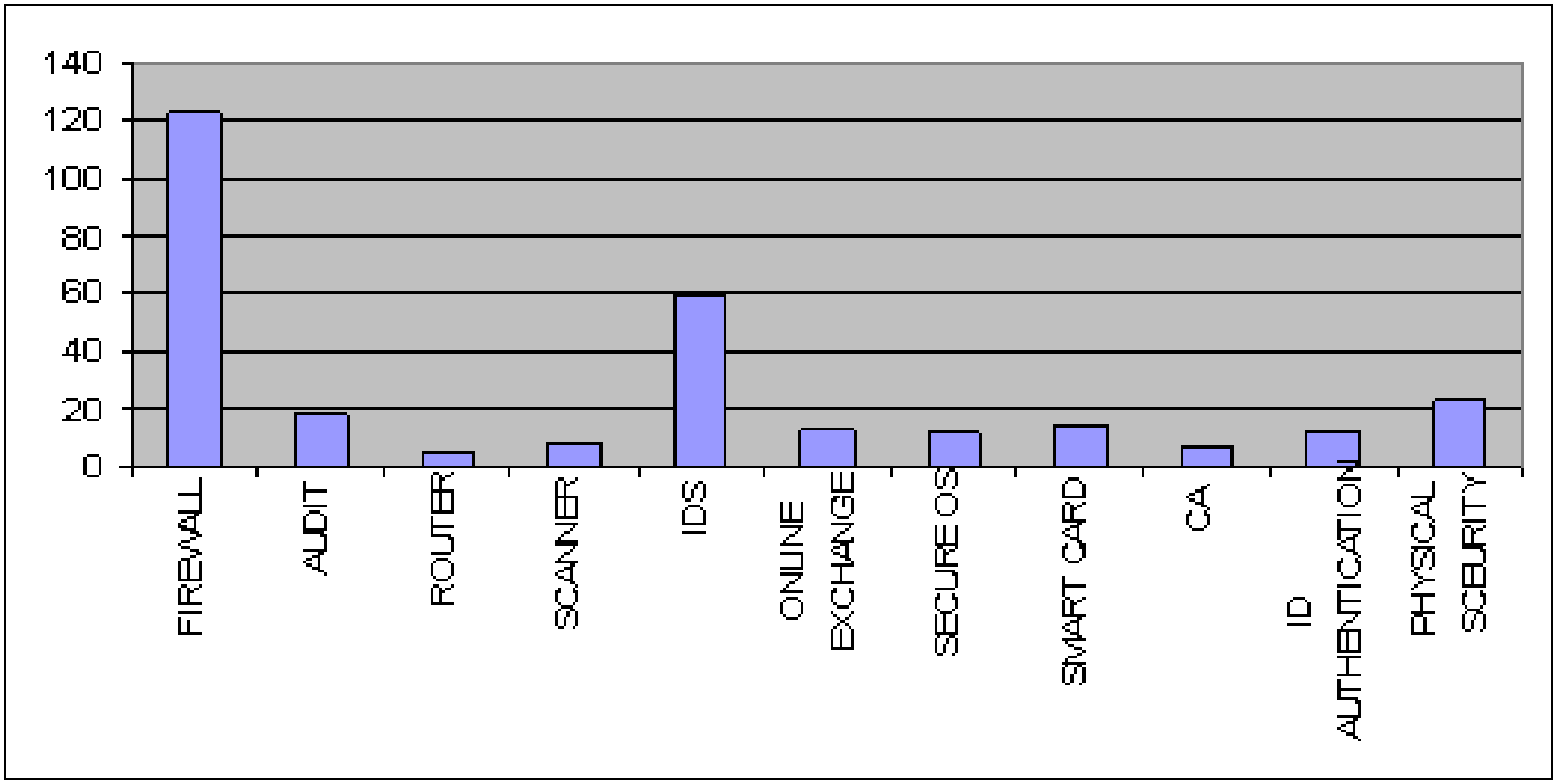
基于CC认证的产品数量



CCRA认证的产品类型



中国产品认证的类型


140
120
100
80
60
40
20
0
FIREWALL
AUDIT
ROUTER
SCANNER
IDS
ONLINE EXCHANGE
SECURE OS
SMART CARD
CA
ID AUTHENTICATION
PHYSICAL SECURITY

CC标准
基本概念、框架、内容

术语

- CC (Common Criteria) 通用准则
- TOE(Target of Evaluation) 评估对象
- PP(Protection Profile) 保护轮廓
- ST(Security Target) 安全目标
- TSF(TOE Security Functions) TOE安全功能要求
- EAL(Evaluation Assurance Level) 评估保证级
- TSP(TOE Security Policy) TOE安全策略

评估目标 (TOE)

- IT产品或系统及其相关的管理指南和用户指南文档，是评估的对象

保护轮廓 (PP)

- 满足特定的消费者需求的一类TOE的独立于实现的一组安全要求
  - 回答：“我们在安全解决方案中需要什么?”
  - 独立于实现
  - PP制定者
    - 任何想表达安全需求的人 (如：商业消费者、消费者团体)
    - 任何提供支持IT安全需求的产品的人
    - 其它人…

安全目标 (ST)

- 依赖于实现的一组安全要求和说明，用作指定TOE的评估基础。
- ST回答如下问题： “您在安全解决方案中提供什么?”
- 依赖于实现
- ST的作者:
  - 产品销售者
  - 产品开发者
  - 产品集成者

TSP和TSF

- TOE Security Policy

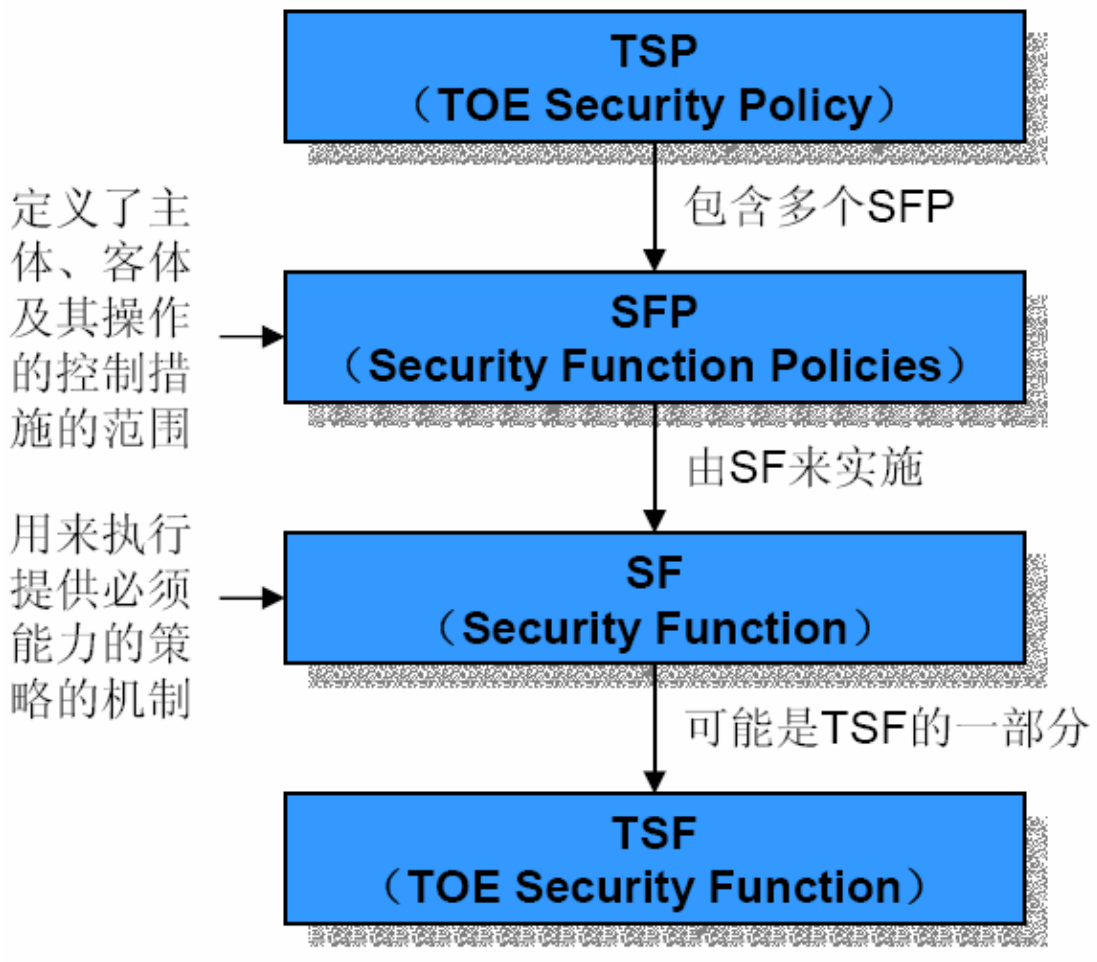
  （TSP）

  - 控制TOE中资产如何管理、保护和分发的规则

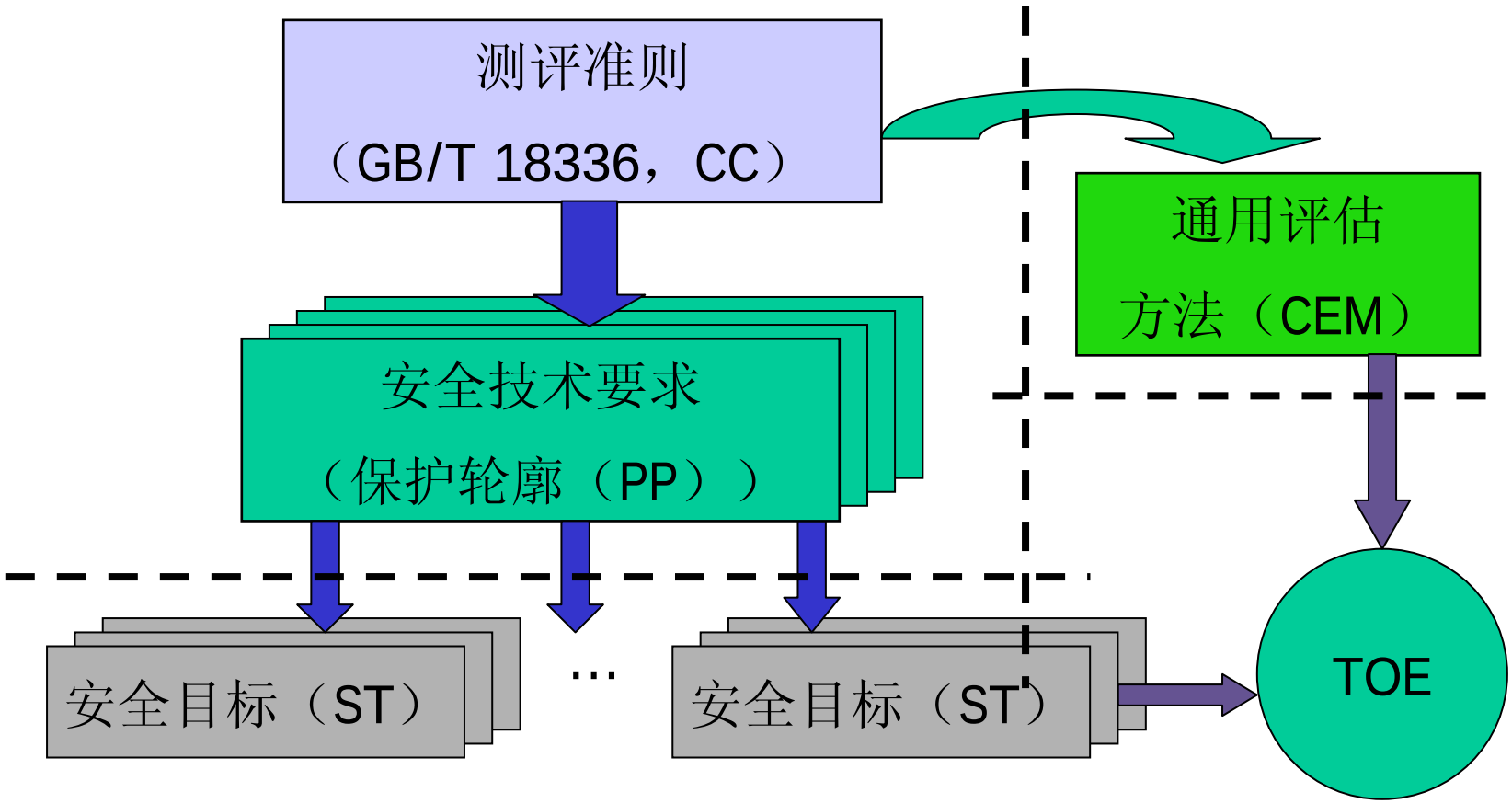
- TOE Security Functions

  （TSF）

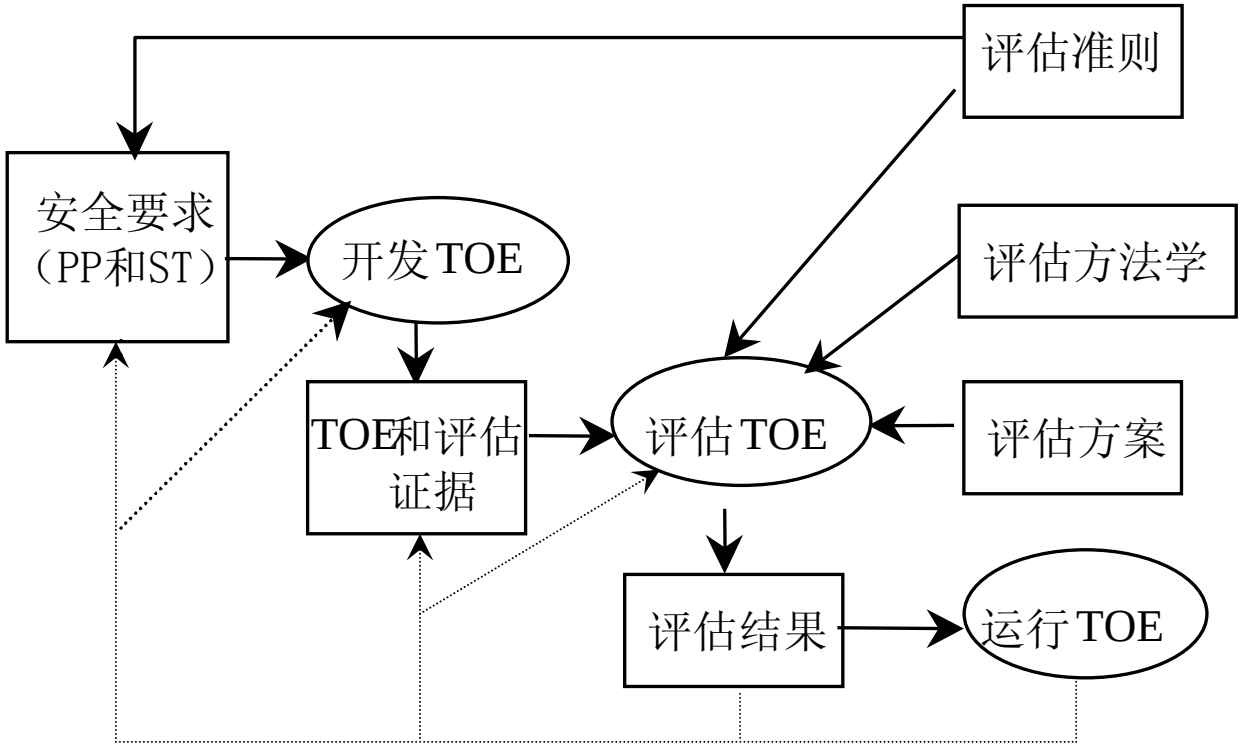
  - 必须依赖于TSP正确执行的TOE的所有部件



以CC为基础的信息安全测评



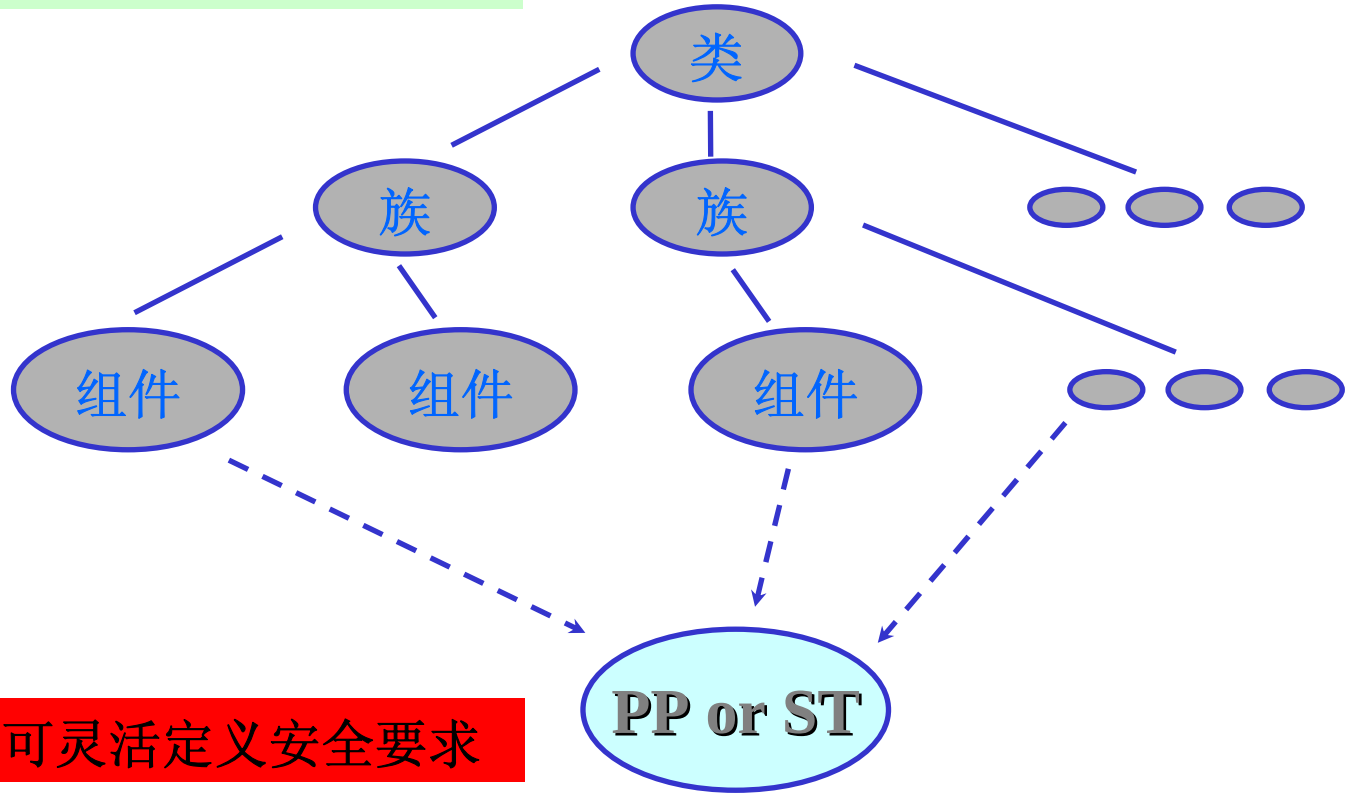
TOE评估过程



TOE：产品、系统或子系统

CC安全要求的层次

功能或保证要求



可灵活定义安全要求

通用准则CC之安全功能要求

CC共包含的11个安全功能类：

- FAU类：安全审计
- FCO类：通信
- FCS类：密码支持
- FDP类：用户数据保护
- FIA类：标识与鉴别
- FMT类：安全管理
- FPR类：隐秘
- FPT类：TFS保护
- FRU类：资源利用
- FTA类：TOE访问
- FTP类：可信信道/路径

安全保证要求（CC 2.1 版）

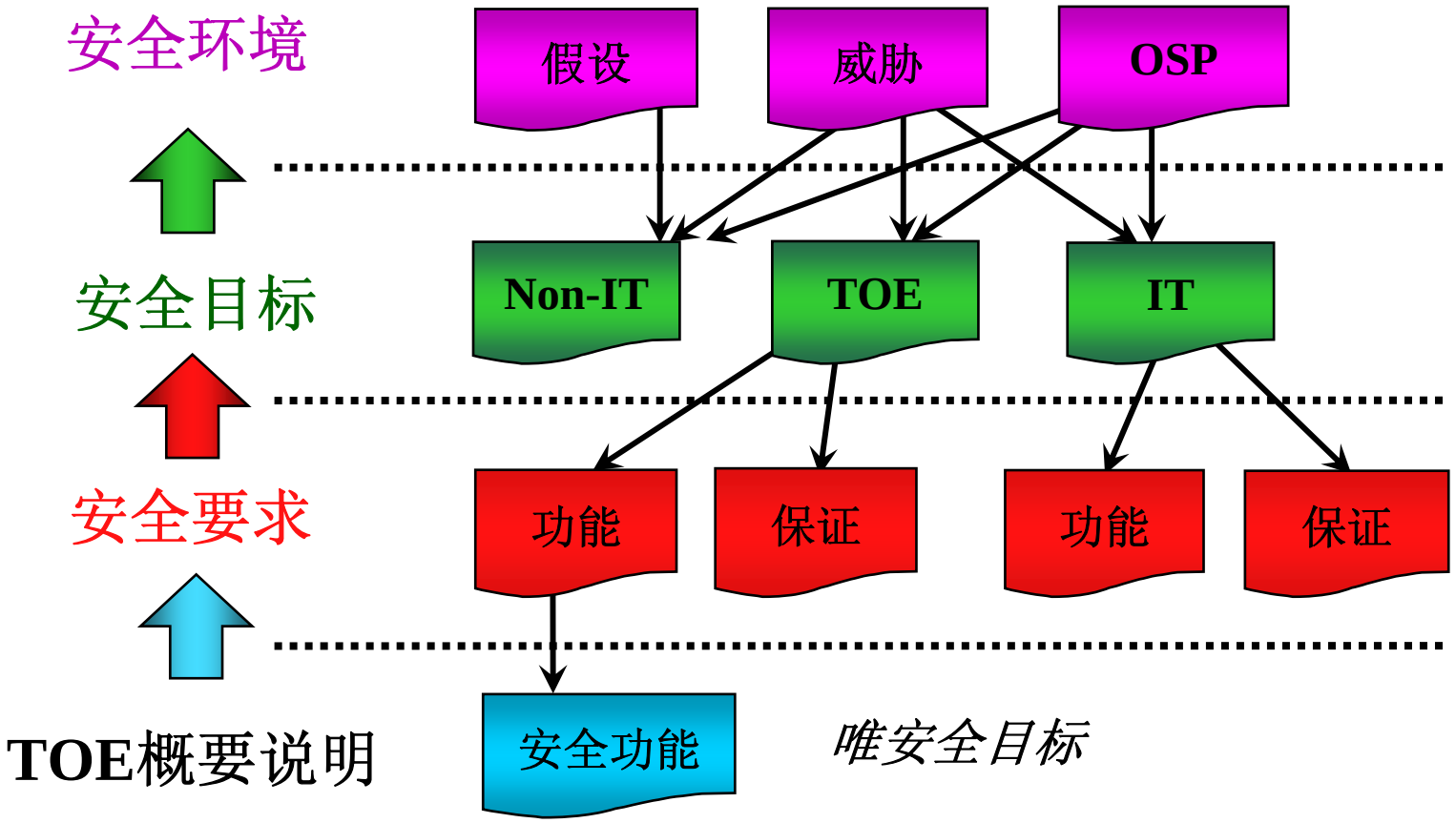
TOE保证

- ✓ 配置管理 (ACM)
- ✓ 交付与运行 (ADO)
- ✓ 开发文档 (ADV)
- ✓ 指南文档 (AGD)
- ✓ 生命周期支持 (ALC)
- ✓ 测试 (ATE)
- ✓ 脆弱性评估 (AVA)

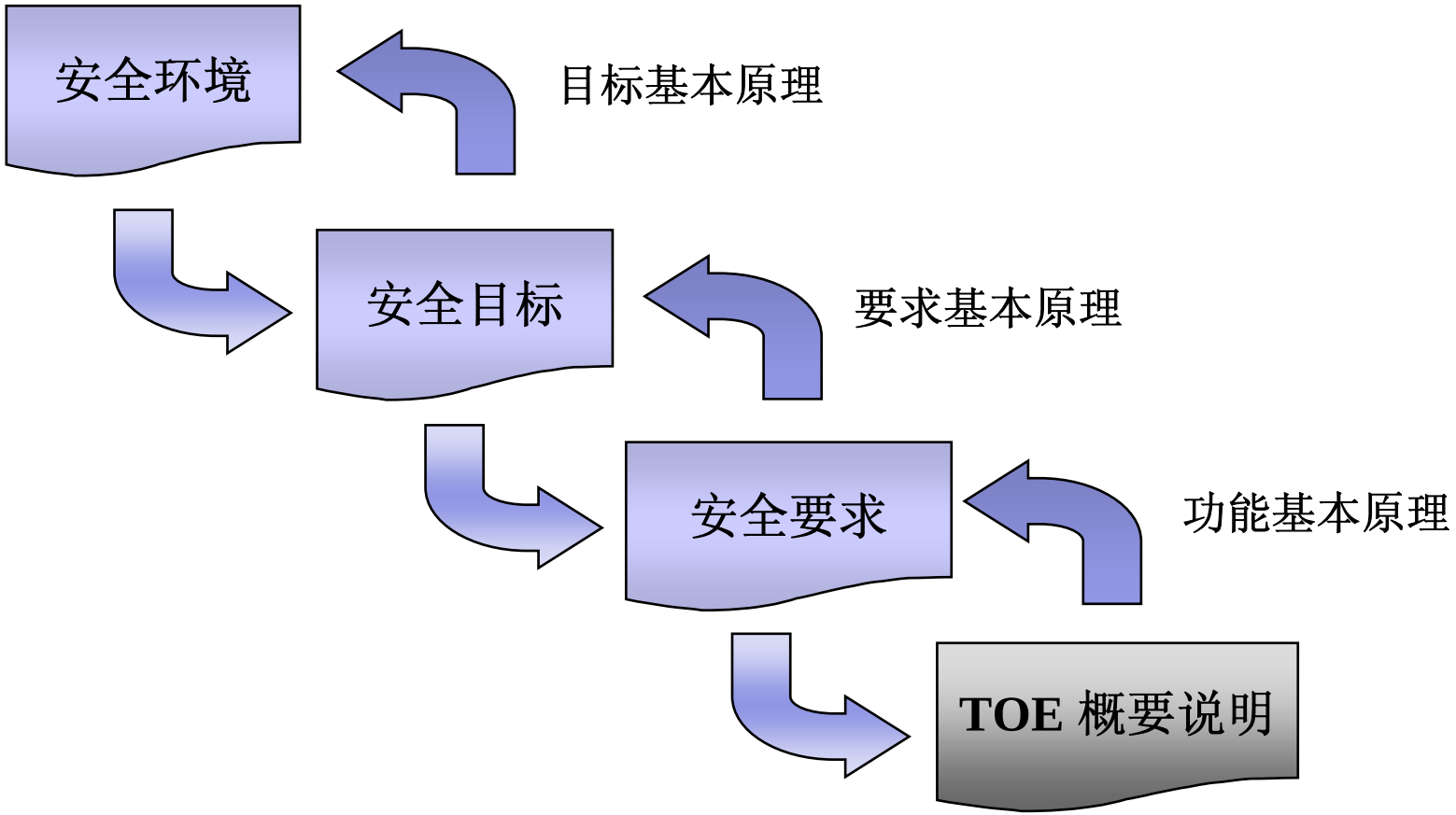
保证说明

- ✓ PP评估 (APE)
- ✓ ST评估 (ASE)
- ✓ 保证的维持 (AMA)

PP/ST 说明框架


安全环境
假设
威胁
OSP
安全目标
Non-IT
TOE
IT
安全要求
功能
保证
功能
保证
TOE概要说明
安全功能
唯安全目标

PP/ST 说明框架抽象



PP/ST 的内容既比较

保护轮廓（PP）

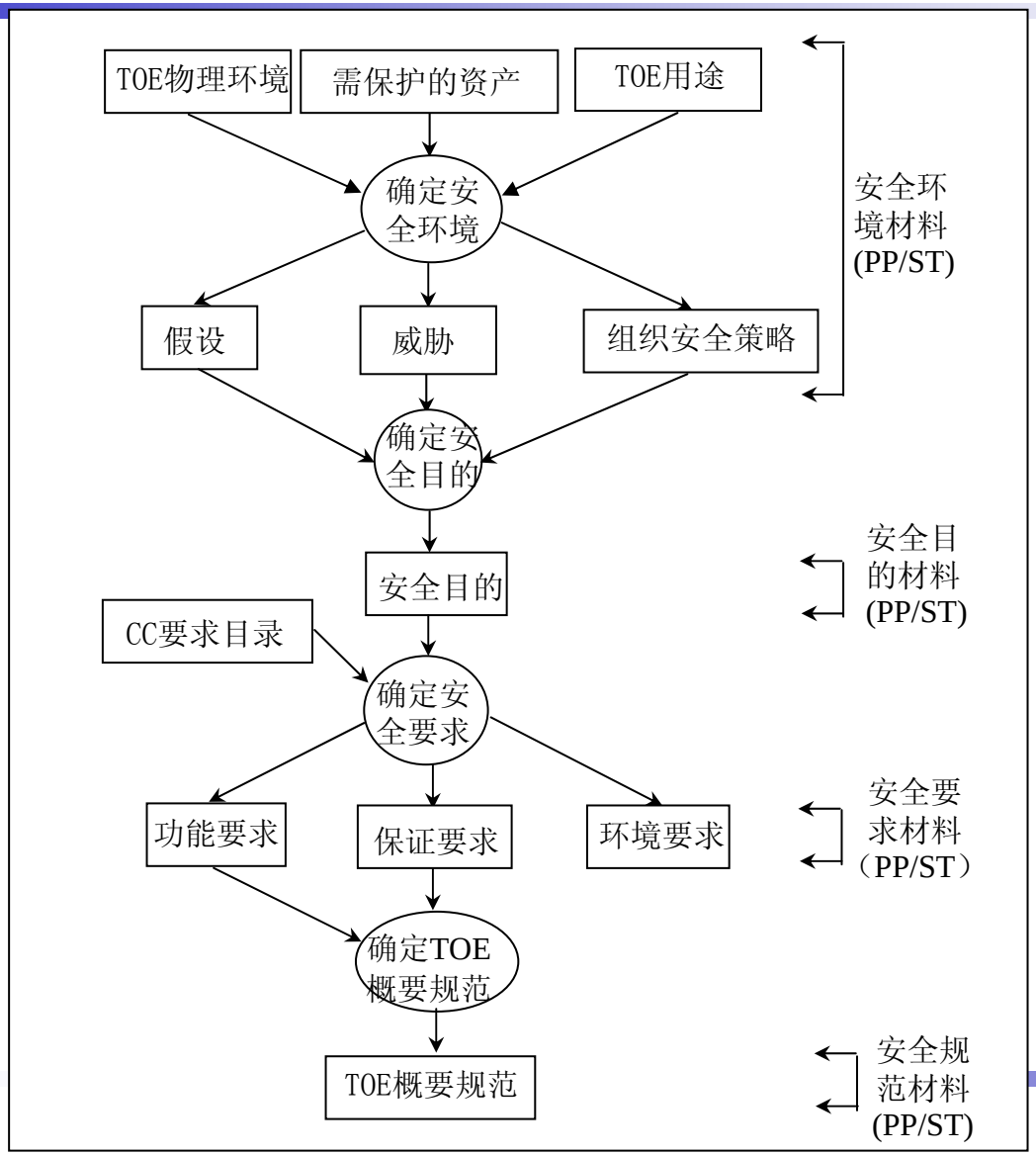
- 标识
- 概况
- TOE描述
- 安全环境
  - ✓ 假设、威胁、政策
- 安全目标
- 安全要求
  - ✓ 功能，保证 (EAL)
- 基本原理

安全目标（ST）

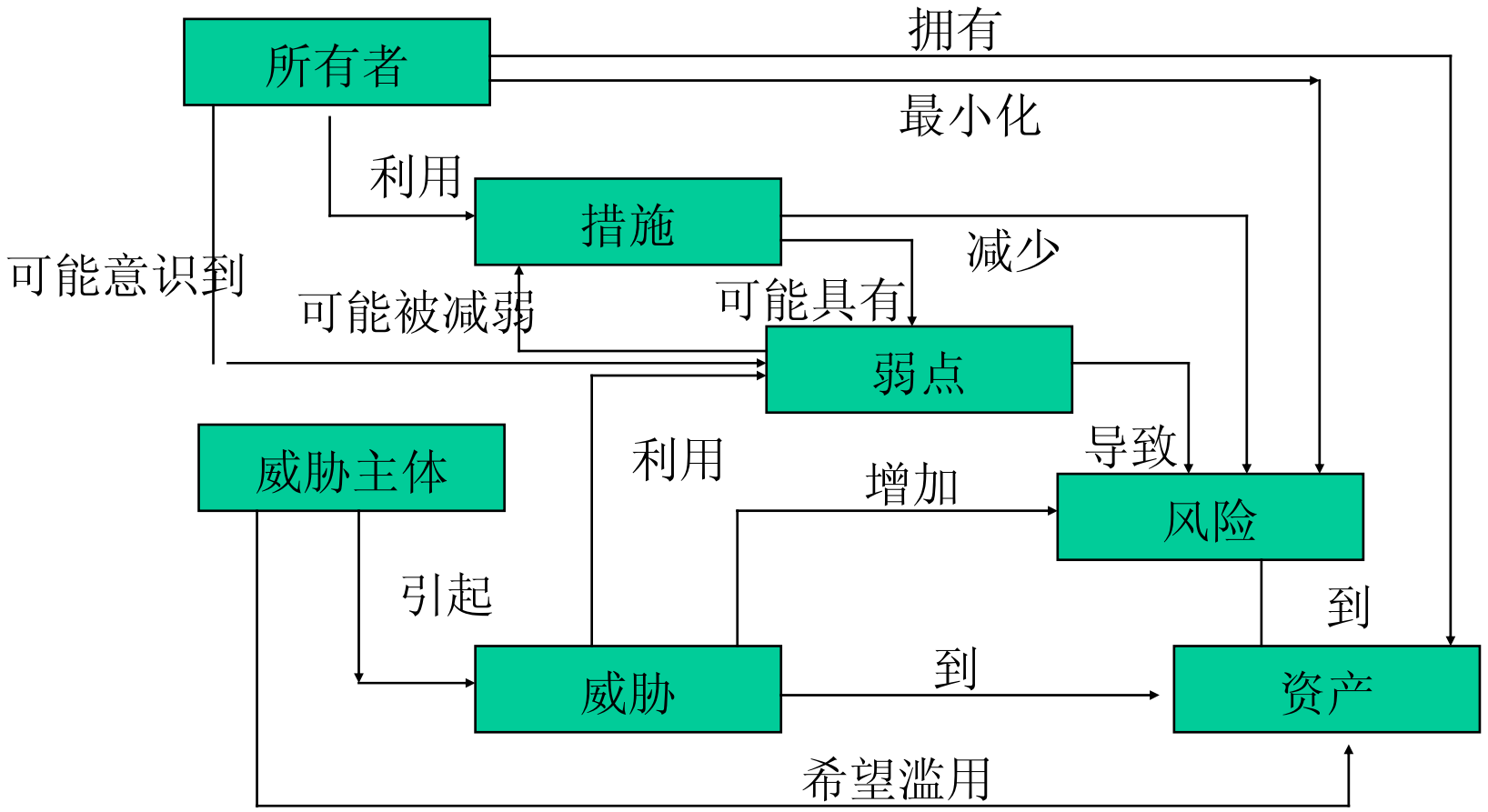
- 标识
- 概况
- TOE描述
- 安全环境
  - ✓假设、威胁、政策
- 安全目标
- 安全要求
  - ✓功能，保证 (EAL)
- 基本原理

- TOE 概要说明
- CC 符合性声明
- PP 声明

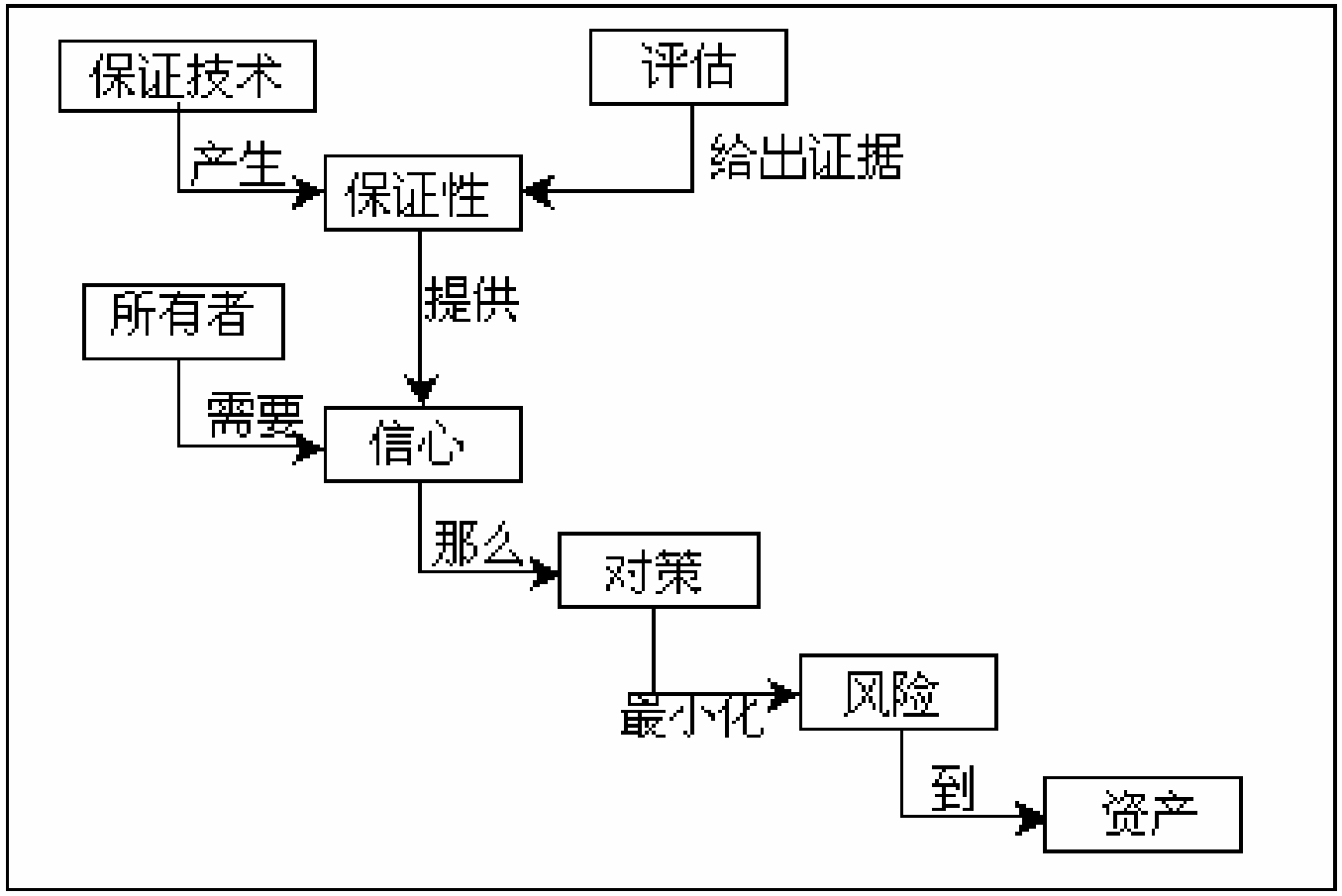
保护轮廓和安全目标的开发过程



CC安全思想-风险管理

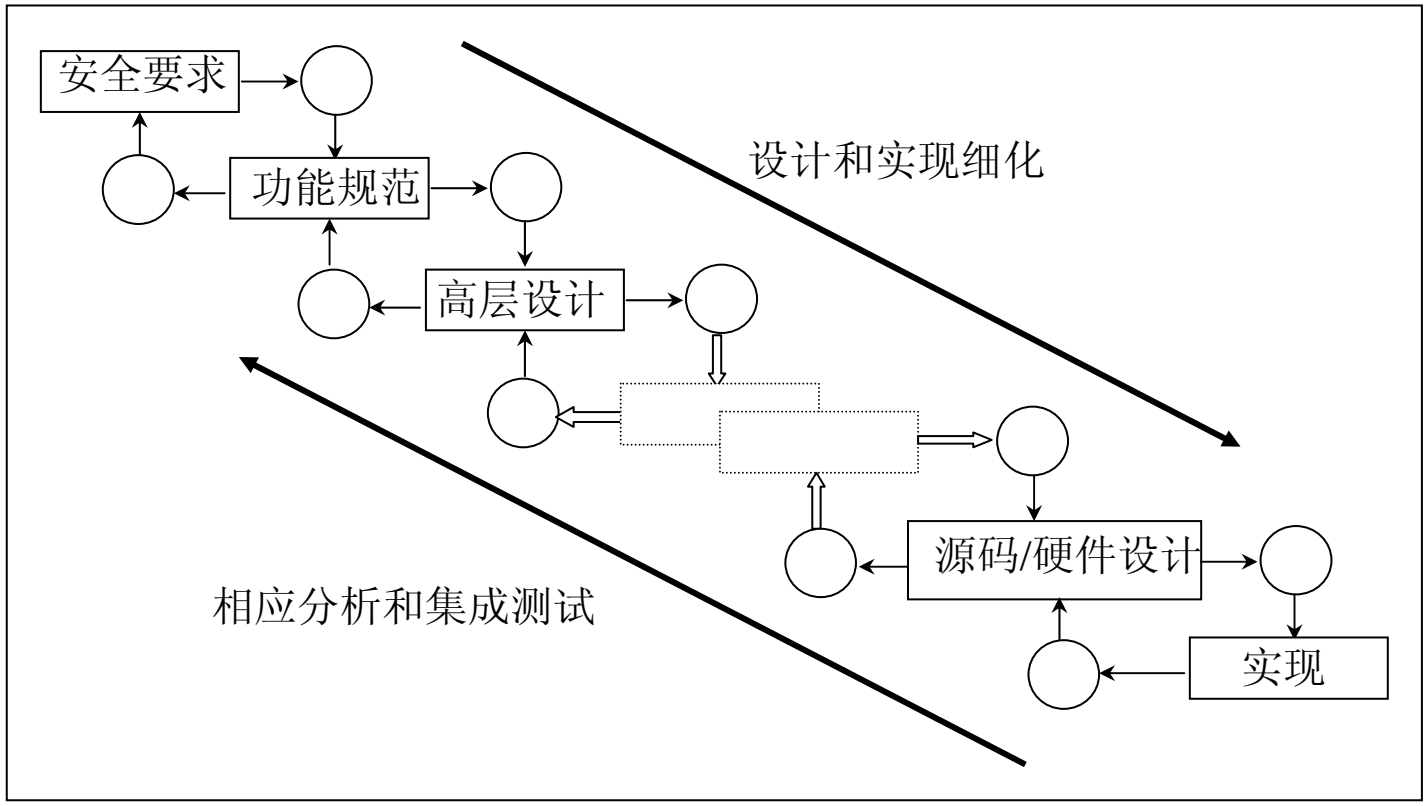

所有者
拥有
最小化
利用
措施
减少
可能意识到
可能被减弱
可能具有
弱点
威胁主体
利用
导致
增加
风险
引起
到
威胁
到
资产
希望滥用

评估概念和关系



评估概念和关系

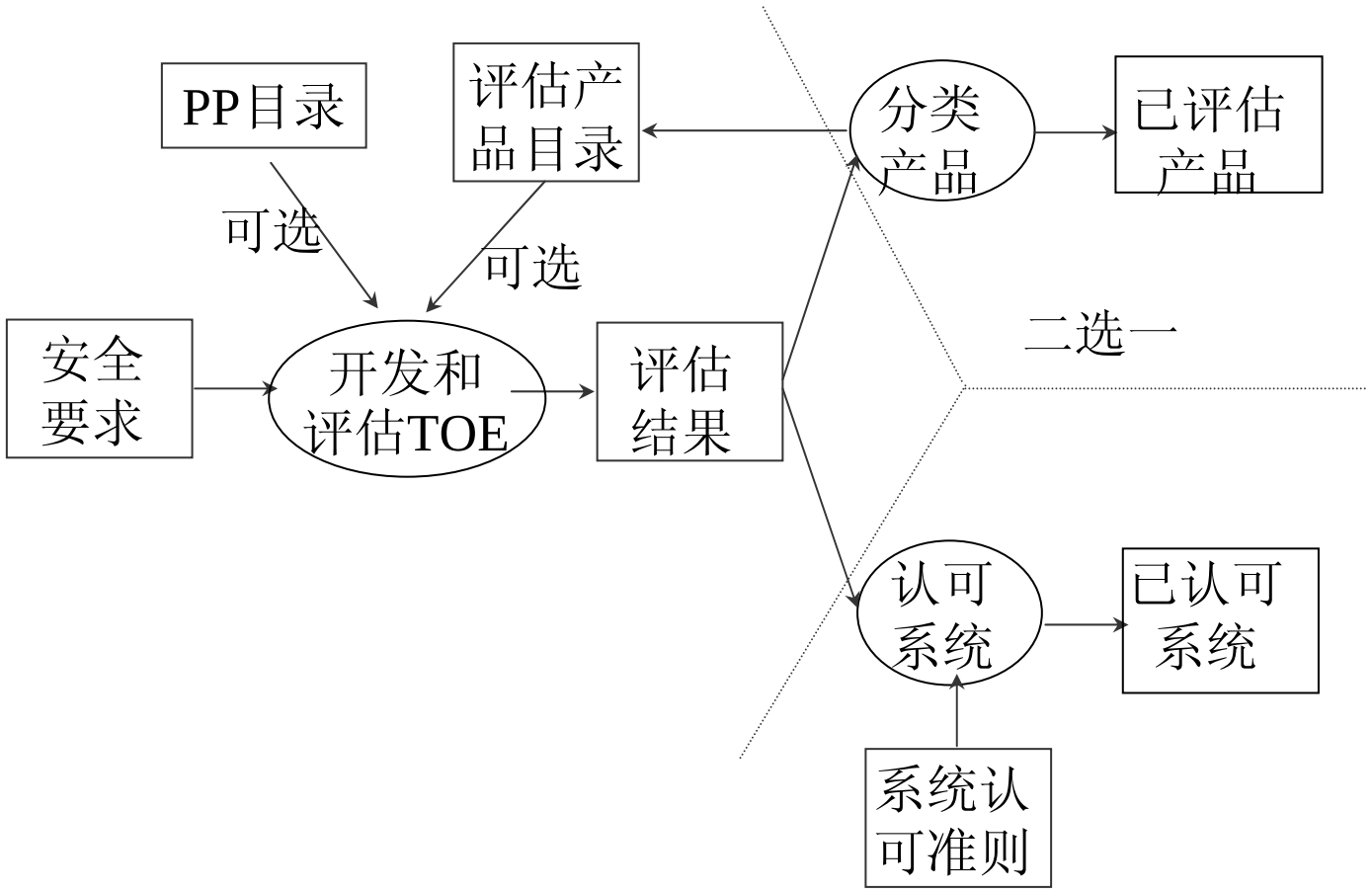
CC对TOE开发过程的概述



CC的应用范围

- CC不描述人员和运行安全（这些安全措施必须在安全环境中讨论），也不描述评估的有效性和其他使系统更有效的管理措施
  - 不包括属于行政性管理安全措施的评估准则；
  - 不包括物理安全方面（诸如电磁辐射控制）的评估准则；
  - 不包括密码算法固有质量评价准则

CC评估结果对其他过程的支持



通用准则CC的七个评估保证级（EAL）

- EAL1：功能测试
- EAL2：结构测试
- EAL3：系统测试和检查
- EAL4：系统设计、测试和复查
- EAL5：半形式化设计和测试
- EAL6：半形式化验证的设计和测试
- EAL7：形式化验证的设计和测试

CC 3.1								
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR	*(ALC_FLR subactivities optional at all EALs)*						
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

评估级别的现实指导意义

级别	保证	风险	费用	时间	开发者支持	形式化分析	应用领域
EAL1	低	低	最少	2	可无	无	个人及简单商用，需保护的信息价值较低。
EAL2	中低	较低	较少	5	有限	无	个人、一般商用或简单政用，需保护的信息价值不太高，信息敏感但不保密，安全风险较低的环境。
EAL3	中	中	中等	8	较多	无	具有适当安全需求的一般政用、特定商用和简单军用。存在中度的安全风险。
EAL4	中高	中高	较高	11	全面	无	具有较高安全需求的特定政用、关键商用和一般军用环境。
EAL5	高	高	很高	14	全面	半	用于安全需求很高的关键政府部门、核心商用、特种军事环境
EAL6	极高	极高	极高	17	全面	半	用于具有极高安全需求的政府要害部门、要害商用环节和要害军事环境。
EAL7	最高	最高	最高	21	全面	形式化	用于具有最高安全需求的核心处理领域，包括政府、军队、商业领域的极关键机构和场所的极关键信息处理环境。

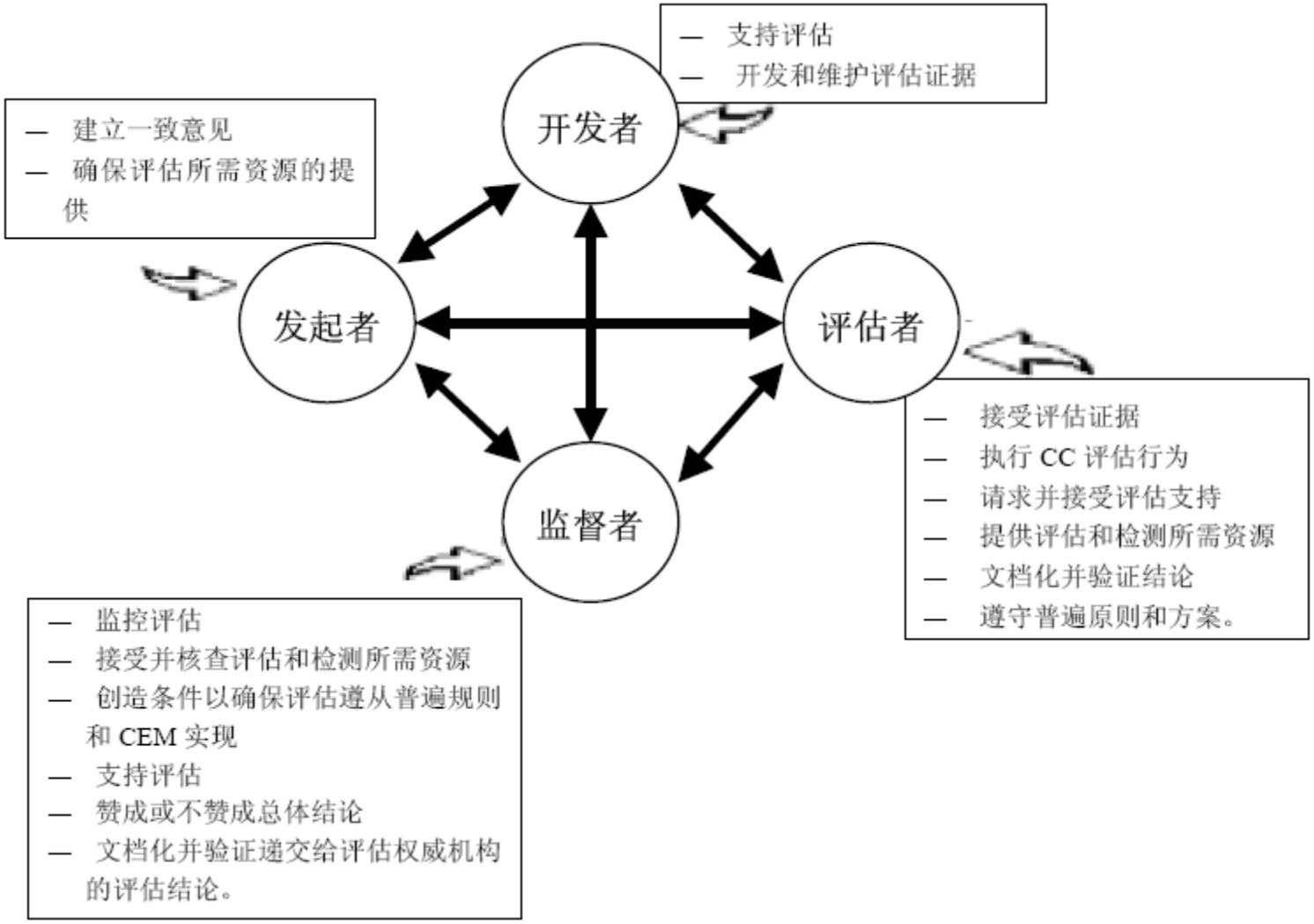
CEM简介

- 通用评估方法（Common Evaluation Methodology，CEM）是为CC评估而开发的一种国际公认方法，CEM支撑着信息安全评估的国际互认
- CEM主要是针对评估者而开发的，其他团队（开发者、监督者等）也可从CEM中得到一些有用的信息
- PP开发者（一组用户代表或IT产品的一个制造商）使用CEM：
  - 有利于在执行PP评估的一致性和独立性方面证实PP方面的应用

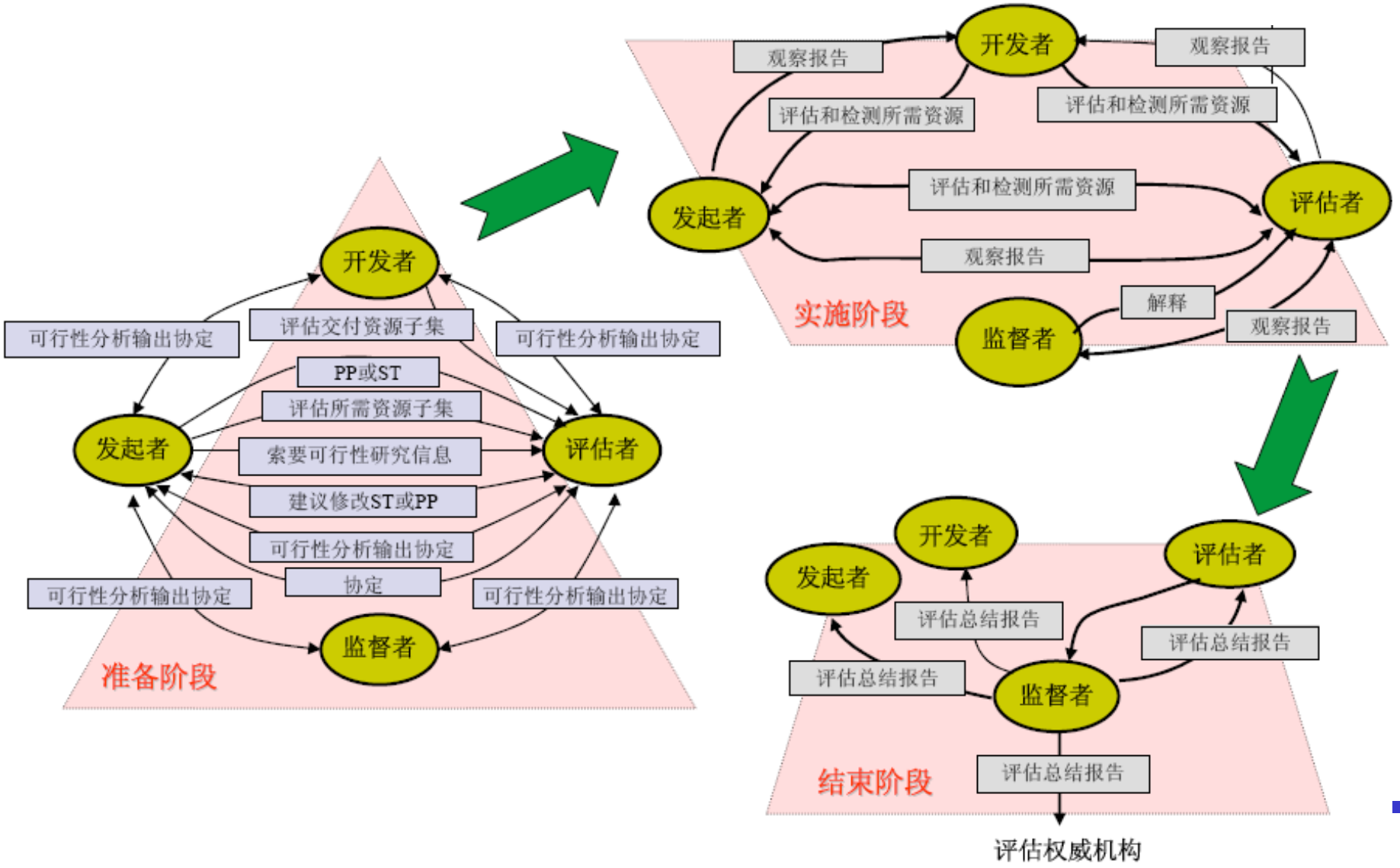
CEM简介（续）

- TOE开发者（产品制造商，系统集成商，或其他解决方案提供者）使用CEM有利于：
  - 在PP和ST中，文档化提出的安全特性可被独立地证实和验证；
  - 开发者的顾客将更容易确信TOE提供了所声称的安全特性；
  - 评估后的产品在所组成的安全系统中可以更有效地使用
- 评估发起者（启动一个评估的组织实体，可以是开发者或顾客）：
  - 把CEM用于以文档形式提出TOE的安全特性，并要求评估者独立地证实和验证
- 评估者使用CC时要与CEM一致
- 监督者是所进行的评估过程与CC、CEM一致性的实体

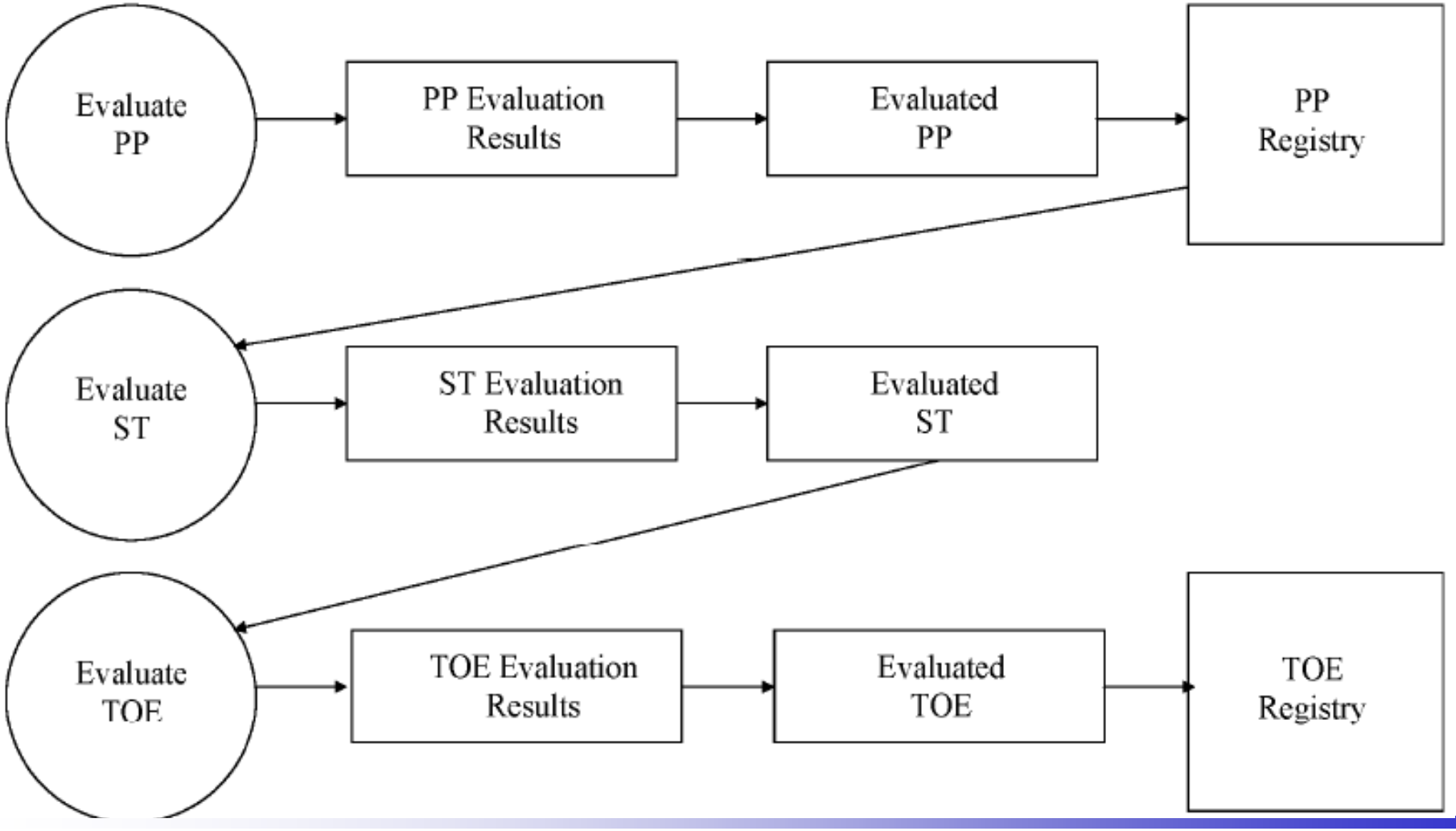
评估的角色和职责关系


开发者
— 支持评估
— 开发和维护评估证据
发起者
— 建立一致意见
— 确保评估所需资源的提供
评估者
— 接受评估证据
— 执行 CC 评估行为
— 请求并接受评估支持
— 提供评估和检测所需资源
— 文档化并验证结论
— 遵守普遍原则和方案。
监督者
— 监控评估
— 接受并核查评估和检测所需资源
— 创造条件以确保评估遵从普遍规则和 CEM 实现
— 支持评估
— 赞成或不赞成总体结论
— 文档化并验证递交给评估权威机构的评估结论。

评估过程概述


开发者
可行性分析输出协定
评估交付资源子集
可行性分析输出协定
PP或ST
评估所需资源子集
发起者
索要可行性研究信息
评估者
建议修改ST或PP
可行性分析输出协定
协定
可行性分析输出协定
可行性分析输出协定
监督者
准备阶段
开发者
观察报告
观察报告
评估和检测所需资源
评估和检测所需资源
发起者
评估和检测所需资源
评估者
观察报告
实施阶段
解释
监督者
观察报告
开发者
评估者
发起者
评估总结报告
评估总结报告
评估总结报告
监督者
结束阶段
评估总结报告
评估权威机构

PP、ST和TOE评估的结果



CC2.1 安全功能类（Class）

■ Class FAU: Security Audit

- 安全审计包括识别、记录、存储和分析那些与安全相关活动（即由TSP控制的活动）有关的信息。检查审计记录结果可用来判断发生了哪些安全相关活动以及哪个用户要对这些活动负责。
- 6个子类：安全审计自动应答（FAU_ARP），安全审计数据产生（FAU_GEN），安全审计分析（FAU_SAA），安全审计查阅（FAU_SAR），安全审计事件选择（FAU_SEL），安全审计事件存储（FAU_STG）

CC2.1 安全功能类（Class）

■ Class FCO：Communication

- 用于确保在数据交换中参与方的身份。既确保发送者不能否认，又确保接收者不能否认收到。
- 2个子类：原发抗抵赖（FCO_NRO），接收抗抵赖（FCO_NRR）

CC2.1 安全功能类（Class）

■ Class FCS：Cryptographic support

- 产品或系统含有密码功能时，将使用密码支持类。
- 2个子类：密钥管理（FCS_CKM），密码运算（FCS_COP）

CC2.1 安全功能类（Class）

■ Class FDP：User data protection

- 规定了与保护用户数据相关的所有安全功能要求和策略。涉及用户数据输入、输出和存储。分为四组子类，这些子类处理TOE内部在输入、输出和存储期间的用户数据，以及和用户数据直接相关的安全属性。
- 13个子类：访问控制策略（FDP_ACC），访问控制功能（FDP_ACF）， 数据鉴别（FDP_DAU），输出到TSF控制之外（FDP_ETC），信息流控制策略（FDP_IFC），信息流控制功能（FDP_IFF），从TSF控制之外输入（FDP_ITC），TOE内部传送（FDP_ITT），残余信息保护（FDP_RIP），反转（FDP_ROL），存储数据的完整性（FDP_SDI），TSF间用户数据传送的保密性保护（FDP_UCT），TSF间用户数据传送的完整性保护（FDP_UIT）

CC2.1 安全功能类（Class）

■ Class FIA：Identification and authentication

- 提出了用户身份确定和验证、与TOE交互的授权，以及每个授权用户安全属性的正确关联等三方面的安全要求。
- 6个子类：鉴别失败（FIA_AFL），用户属性定义（FIA_ATD），秘密的规范 （FIA_SOS），用户鉴别（FIA_UAU），用户标识 （FIA_UID），用户-主体绑定（FIA_USB）。

CC2.1 安全功能类（Class）

■ Class FMT：Security Management

- 规定了安全属性、数据和功能三方面的管理，也定义不同管理角色及其相互作用。
- 6个子类：TSF功能管理（FMT_MOF），安全属性管理（FMT_MSA），TSF数据管理（FMT_MTD），撤消（FMT_REV），安全属性到期（FMT_SAE），安全管理角色（FMT_SMR）

CC2.1 安全功能类（Class）

■ Class FPR：Privacy

- 要求为用户提供其身份不被其他用户发现或滥用的保护。
- 4个子类：匿名（FPR_ANO），假名（FPR_PSE），不可关联性（FPR_UNL），不可观察性（FPR_UNO）

CC2.1 安全功能类（Class）

■ Class FPT：Protection of the TSF

- TSF指的是TOE安全功能，TSF类侧重于保护TSF数据，而不是用户数据。FPT类的组件对保证TOE中的SFP不被篡改和旁路是必需的。
- 16个子类：根本抽象机测试（FPT_AMT），失败保护（FPT_FLS），输出TSF数据的可用性（FPT_ITA），输出TSF数据的保密性（FPT_ITC），输出TSF数据的完整性（FPT_ITI），TOE内TSF数据的传送（FPT_ITT），TSF物理保护（FPT_PHP），可信恢复（FPT_RCV），重放检测（FPT_RPL），参照仲裁（FPT_RVM），域分离（FPT_SEP），状态同步协议（FPT_SSP），时间戳（FPT_STM），TSF间TSF数据的一致性（FPT_TDC），TOE内TSF数据复制的一致性（FPT_TRC），TSF自检（FPT_TST）

CC2.1 安全功能类（Class）

■ Class FRU：Resource utilisation

- 支持所需资源的可用性。容错子类提供保护以防止由TOE失败引起的上述资源不可用。服务优先级子类确保资源将被分配到更重要的和时间要求更苛刻的任务中，而且不能被优先级低的任务所独占。资源分配子类提供可用资源的使用限制，从而防止用户独占资源。
- 3个子类：容错（FRU_FLT），服务优先级（FRU_PRS），资源分配（FRU_RSA）

CC2.1 安全功能类（Class）

■ Class FTA：TOE access

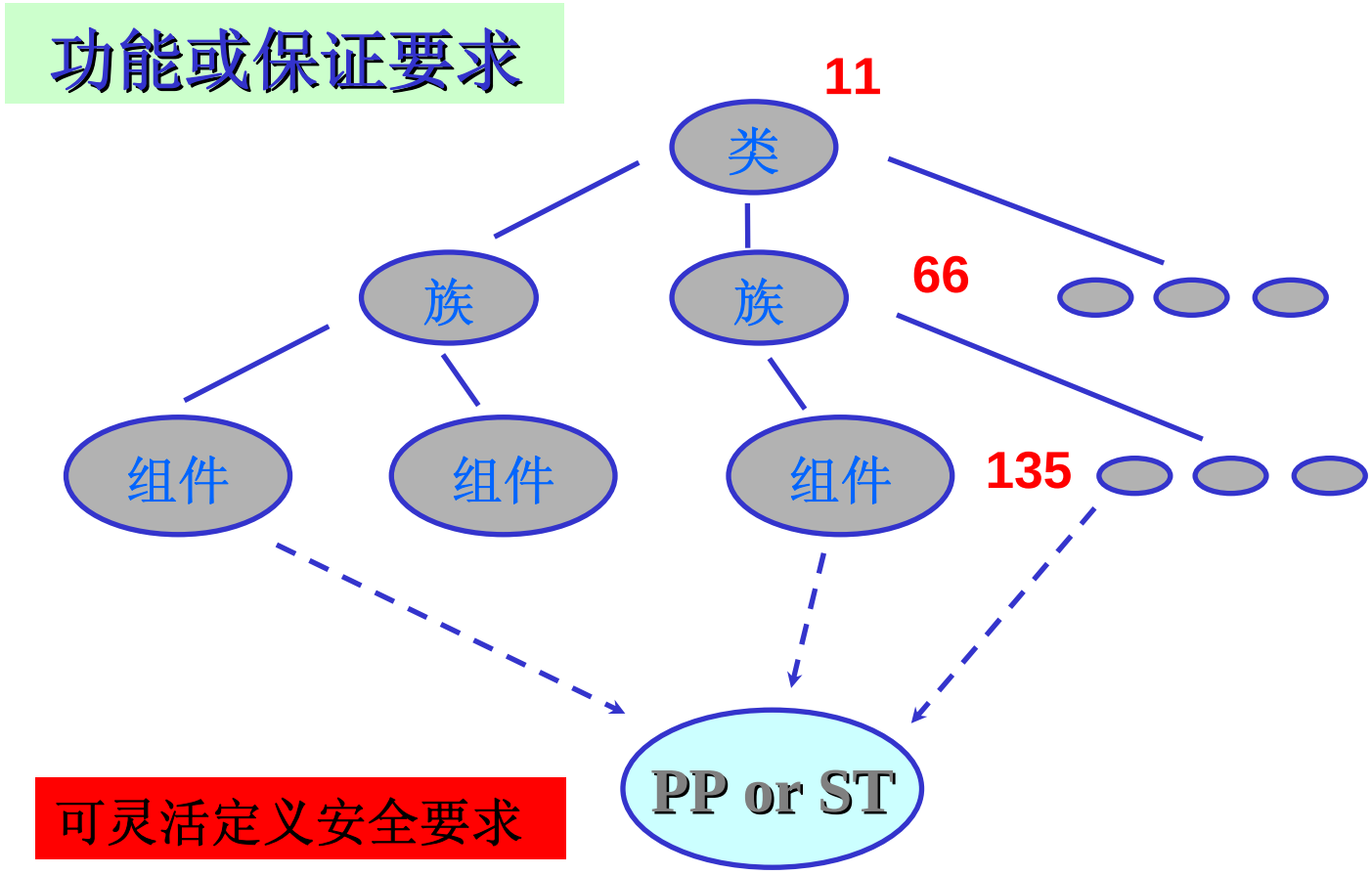
- 规定了用以控制建立用户会话的一些功能要求，是对标识和鉴别类安全要求的进一步补充。
- 6个子类：可选属性范围限定（FTA_LSA），多重并发会话限定(FTA_MCS)，会话锁定（FTA_SSL），TOE访问旗标（FTA_TAB），TOE 访问历史(FTA_TAH)，TOE会话建立(FTA_TSE)

CC2.1 安全功能类（Class）

■ Class FTP：Trusted path/channels

- 规定了关于用户和TSF之间可信通信路径，以及TSF和其他可信IT产品间可信通信信道的要求。
- 2个子类：TSF间可信信道（FTP_ITC），可信路径（FTP_TRP）

CC安全要求的层次



CC2.1 保证类（Class）

■ Class ACM：Configuration Management

- 配置管理(CM—Configuration Management)通过在细化和修改TOE及其它有关信息的过程中进行规范和控制，确保TOE的完整性。配置管理（CM）阻止对TOE进行非授权的修改、添加或删除，这保证了用于评估的TOE和文档确是准备交付的TOE和文档。
- 3个子类：配置管理自动化（ACM_AUT），配置管理能力（ACM_CAP），配置管理范围（ACM_SCP）

CC2.1 保证类（Class）

■ Class ADO：Delivery and Operation

- 该类规定了TOE交付、安装、生成和启动方面的措施、程序和标准，以确保TOE所提供的安全保护在这些关键过程中不被泄漏。
- 2个子类：交付（ADO_DEL），安装、生成和启动（ADO_IGS）

CC2.1 保证类（Class）

■ Class ADV：Development

- 定义了ST中从TOE概要规范到实际TSF的逐步细化的一系列要求。每一个产生结果的TSF表示都提供信息，以帮助评估者决定TOE的功能要求是否被满足了。
- 7个子类：功能规范（ADV_FSP），高层设计（ADV_HLD），实现表示（ADV_IMP），TSF内部（ADV_INT），低层设计（ADV_LLD），表示对应性（ADV_RCR），安全策略模型（ADV_SPM）

CC2.1 保证类（Class）

■ Class AGD：Guidance documents

- 从开发者提供的可操作文档的易懂性、覆盖范围和完整性等方面定义了指导性要求。该文档提供两种类型的信息，一类是针对用户，另一类针对管理员，这是TOE安全运行的一个重要因素。
- 2个子类：管理员指南（AGD_ADM），用户指南（AGD_USR）

CC2.1 保证类（Class）

■ Class ALC：Life cycle support

- 通过采用一个为TOE开发的所有步骤定义的生命周期模型，明确了保证要求。这个生命周期包括纠正缺陷的程序和策略，以及保护开发环境的工具、技术和安全措施的正确使用。
- 4个子类：开发安全（ALC_DVS），缺陷纠正（ALC_FLR），生命周期定义（ALC_LCD），工具和技术（ALC_TAT）

CC2.1 保证类（Class）

■ Class ATE：Tests

- 陈述了论证TSF满足TOE安全功能要求的测试要求。
- 4个子类：覆盖范围（ATE_COV），深度（ATE_DPT），功能测试（ATE_FUN），独立性测试（ATE_IND）

CC2.1 保证类（Class）

- **Class AVA：Vulnerability assessment**
  - 该类定义了与识别可利用的脆弱性相关的安全要求，这些脆弱性可能在开发、集成、运行、使用和配置时进入TOE。
  - 3个子类：隐蔽信道分析（AVA_CCA），误用（AVA_MSU），TOE安全功能强度（AVA_SOF）

CC小结

- 一组规则集，是描述IT产品和系统安全的语言
- 灵活的架构，可以定义自己的要求
- 一种评估方法，充分突出“保护轮廓”，将评估过程分“功能”和“保证”两部分；
- 通过提供一套通用的用于IT产品与系统的安全功能要求集，以及在安全评估中适应于该功能集的安全保证措施要求集来实现的，目前最全面的评价准则