TCSEC & CC

南京大学计算机系　黄皓 教授

2010年 12月27日

References

I. **TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA，DoD 5200.28-STD。(Rainbow)**

II. **Information technology – Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model，ISO/IEC 15408-1: 1999 (E)。**

III. **Information technology - Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements，ISO/IEC 15408-2: 1999 (E)。**

IV. **Information technology - Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements，ISO/IEC 15408-3: 1999 (E)。**

Contents

- TCSEC
  - Purpose
  - Fundamental Computer Security Requirements
  - Structure of the Criteria
- Common Criteria

Trusted Computer System Evaluation Criteria (TCSEC)

— December 26, 1985

Purpose — Three objectives

- **Provide guidance to manufacturers**
  - To provide a standard to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements (**with particular emphasis on preventing the disclosure of data**) for sensitive applications.
- **Evaluate the degree of trust**
  - To provide DoD components with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing
- **Provide a basis for specifying security requirements**

- Classify systems into four broad herarchical divisions of enhanced security protection,
  - D
  - C_1,C_2,
  - B_1, B_2, B_3,
  - A_1
- They provide a basis for the evaluation of effectiveness of security controls built into automatic data processing system products.

Fundamental Computer Security Requirements

- Policy
- Accountability
- Assurance
- Documentation

Security Policy

- There must be an explicit and well-defined security policy enforced by the system.

- Security Policy
  - Discretionary Access Control
  - Object Reuse
  - Labels
    - Label Integrity
    - Exportation of Labeled Information
      - Exportation to Multilevel Devices
      - Exportation to Single-Level Devices
      - Labeling Human-Readable Output
    - Subject Sensitivity Labels
    - Device Labels
  - Mandatory Access Control

Accountability — IDENTIFICATION

- Individual subjects must be identified.
  - Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with.
  - This identification and authorization information must be **securely maintained by the computer system** and be **associated with every active element** that performs some security-relevant action in the system.

Accountability — Audit

- Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.
- A trusted system must be able to record the occurrences of security-relevant events in an audit log.
- The capability to select the audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis.
- Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations.

- Accountability
  - Identification and Au2.thentication
    - Trusted Path
  - Audit

ASSURANCE

- In order to assure that the four requirements are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions.
- The basis for trusting such system mechanisms in their operational setting must be clearly **documented** such that it is possible to independently examine the evidence to evaluate their sufficiency.

CONTINUOUS PROTECTION

- The trusted mechanisms must be **continuously protected** against tampering and/or unauthorized changes.

- **Life-cycle** assurance refers to steps taken by an organization to ensure that the system is designed, developed, and maintained using formalized and rigorous controls and standards.
- **Operational assurance** focuses on features and system architecture used to ensure that the security policy is uncircumventably enforced during system operation.

- Assurance
  - Operational Assurance
    - System Architecture
    - System Integrity
    - Covert Channel Analysis
    - Trusted Facility Management
    - Trusted Recovery
  - Life-Cycle Assurance
    - Security Testing
    - Design Specification and Verification
    - Configuration Management
    - Trusted Distribution

- Documentation
  - Security Features User's Guide
  - Trusted Facility Manual
  - Test Documentation
  - Design Documentation

Reference monitor

- Reference monitor
  - enforces the authorized access relationships between subjects and objects of a system.
- Reference validation mechanism
  - validates each reference to data or programs by any user (program) against a list of authorized types of reference for that user.
  - three design requirements
    - tamper proof.
    - always be invoked.
    - small enough to be subject to analysis and tests, the completeness of which can be assured
  - **Early examples of the reference validation mechanism were known as security kernels.**

TRUSTED COMPUTING BASE (TCB)

- Evaluation criteria use the term Trusted Computing Base to refer to the reference validation mechanism, be it a security kernel, front-end security filter, or the entire trusted computer system.
- For general-purpose systems, the TCB will include key elements of the operating system and may include all of the operating system.
- The TCB will necessarily include all those portions of the operating system and application software essential to the support of the policy.
  - For embedded systems, the protection policy may be enforced in the application software rather than in the underlying operating system.
- As the amount of code in the TCB increases, it becomes harder to be confident that the TCB enforces the reference monitor requirements under all circumstances.

DIVISION D : MINIMAL PROTECTION

- This division contains only one class.
- It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

DIVISION C: DISCRETIONARY PROTECTION

- Classes in this division provide
  - for **discretionary protection**
  - for **accountability of subjects and the actions they initiate**

CLASS C1

DISCRETIONARY SECURITY PROTECTION

- The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class C1 requirements

- Security Policy
  - Discretionary Access Control
- Accountability
  - Identification and Authentication
- Assurance
  - Operational Assurance
    - System Architecture
    - System Integrity
  - Life-Cycle Assurance
    - Security Testing
- Documentation
  - Security Features User's Guide
  - Trusted Facility Manual
  - Test Documentation
  - Design Documentation

Class C1 requirements—Security Policy

- Security Policy — Discretionary Access Control
  - TCB必须在ADP中的命名用户和客体（例如，文件、程序）之间进行访问控制。
  - 实施的机制采用“本人/用户组/公共”的控制方式，访问控制列表等，**允许用户来指定和控制**客体由一些单个的用户、一些用户组或者两者的组合。

Class C1 requirements — Accountability

- Identification and Authentication
  - TCB必须要求用户在进行任何TCB期望控制的行为之前声明自己的身份。
  - TCB必须利用一个受到保护的机制（例如，口令）来认证用户的身份。
  - TCB必须保护认证信息，使得任何非授权的用户无法访问认证信息。

Class C1 requirements — Assurance

- Operational Assurance
  - System Architecture
    - TCB能够保护自己的区域免受外部的干扰与损坏（修改它的代码和数据）。
    - TCB控制的资源是系统中的一些用户组和客体。
  - System Integrity
    - 硬件和/或软件的属性应该可以用来周期性地验证在线的TCB硬件和固件操作的正确性。

Class C1 requirements — Assurance

- Life-Cycle Assurance
  - Security Testing
    - 系统的安全功能必须测试过并且与系统的文档描述的一致。
    - 测试结果应当显示系统没有明显的方式让非授权的用户**绕过或击破**TCB的保护机制。

Class C1 requirements — Documentation

- **Security Features User's Guide**
  - 用户手册应有专门章节描述TCB提供的保护机制、使用指南、相互之间的交互。
- Trusted Facility Manual
- Test Documentation
- Design Documentation

Class C1 requirements — Documentation

- Security Features User's Guide
- **Trusted Facility Manual**
  - 给ADP系统管理员的手册必须说明在运行一个安全工具时对它的功能与特权需要考虑的注意事项。
- Test Documentation
- Design Documentation

Class C1 requirements — Documentation

- Security Features User's Guide
- Trusted Facility Manual
- **Test Documentation**
  - 系统开发者应该向评估者提供文档描述
    - 测试计划
    - 测试过程
    - 说明安全机制和安全机制的功能是如何测试的。
- Design Documentation

Class C1 requirements — Documentation

- Security Features User's Guide
- Trusted Facility Manual
- Test Documentation
- **Design Documentation**
  - 必须提供描述开发者的保护思想（philosophy： motivating concepts and principles）。
  - 这些保护思想如何对应到TCB中。
  - 如果TCB由多个模块组成，需要阐述模块之间的接口。

Class C2 — CONTROLLED ACCESS PROTECTION

- Security Policy
  - Discretionary Access Control
  - Object Reuse
- Accountability
  - Identification and Authentication
  - Audit
- Assurance
  - Operational Assurance
    - System Architecture
    - System Integrity
  - Life-Cycle Assurance
    - Security Testing
- Documentation
  - Security Features User's Guide
  - Trusted Facility Manual
  - Test Documentation
  - Design Documentation

Class C2 requirements—Security Policy

- Discretionary Access Control
  - TCB必须在ADP中的命名用户和客体（例如，文件、程序）之间进行访问控制。
  - 实施的机制采用“本人/用户组/公共”的控制方式，访问控制列表等，允许用户来指定和控制客体由一些单个的用户、**一些由单个用户组成的用户组**或者两者的组合，**并且提供限制访问权限扩散的方法**。
    (C1:一些单个的用户、**一些用户**组或者两者的组合.)

    增加:
  - 通过用户自主的行为或默认的方式，自主访问控制机制可以提供阻止对客体非授权访问的控制。这些访问控制可以细化到包含或排除单个的用户。
  - 对一个客体没有访问权限的用户要获得对其访问权限，必须由一个授权的用户来授予。

Class C2 requirements—Security Policy

- Object Reuse
  - 对所有的存储客体中的信息的访问权限在该客体被分配给一个主体之前应该被撤销。
  - 任何一个用户都无法从释放给系统的客体中获得任何先前使用的主体产生的任何信息，包括密文信息。

Class C2 requirements — **Accountability**

- **Accountability**
  - **Identification and Authentication**
    - **TCB必须要求用户在进行任何TCB期望控制的行为之前声明自己的身份。**
    - **TCB必须利用一个受到保护的机制（例如，口令）来认证用户的身份。**
    - **TCB必须保护认证信息，使得任何非授权的用户无法访问认证信息。**
    - 增加：Individual accountability
      （responsibility, answerability, blameworthiness, liability）
      - TCB必须能够对ADP的用户进行单独的标识，并对单独用户实施账户责权（accountability）管理。
      - TCB还必须提供机制将用户的身份与用户的审计行为联系起来。

Class C2 requirements — **Accountability— 审计**

（1）TCB 对它保护的数据访问行为能够建立、维护日志信息，并且能够保护其不被非授权地访问和破坏。

（2）TCB必须确保只有授权的用户能否访问审计信息。

（3）TCB能够记录以下事件的日志信息:

(a) 身份标识与认证的机制的使用;

(b) 在一个用户的地址空间中引入一个对象（如: 打开文件）;

(c) 删除对象;

(d) 计算机操作员、系统管理员、系统安全员实施的行为， 以及其它安全相关的事件。

（4）对于每一个审计事件，日志信息必须记录:

(a) 事件的日期和时间;　　（b）用户

(c) 事件的类型;　　（d）事件是成功还是失败。

（5）对于身份标识与认证事件必须记录请求源（例如终端的标识）。

（6）对象的引入和删除事件必须记录对象的名称。

（7）计算机管理员可以选择记录任何一个事件以及相应的一个或多个用户。

Class C2 requirements — Documentation

- Security Features User's Guide NAR
- Trusted Facility Manual
  - 增加：必须给出查看和维护审计文件、每个审计事件的审计日志的规程。
- Test Documentation NAR
- Design Documentation NAR

DIVISION B:

MANDATORY PROTECTION

- The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division.
- Systems in this division must carry the sensitivity labels with major data structures in the system.
- The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB.
- Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Class B1— LABELED SECURITY PROTECTION

- Security Policy
  - Discretionary Access Control (the same as C2) NAR
  - Object Reuse (the same as C2) NAR
  - **Labels**
  - **Mandatory Access Control**
- Accountability
- Assurance
- Documentation

Class B1 requirements — **Security Policy**

- Labels
  - TCB必须维护每个主体、客体（例如：进程、文件、段、设备等）相关联的**敏感标签**。
  - 将这些标签作为强制访问控制决策的**基础**。
  - 为了输入没有标记的数据，TCB必须**向授权用户请求**并确定该数据的安全级别，所有这些行为都被TCB所**审计**。

Class B1 requirements — **Security Policy**

- Labels
  - **Label Integrity**
    - 敏感性标签必须准确地表示它们所关联的主体或客体的安全等级。
    - 当被TCB输出时，敏感性标签必须准确地无二义性地表示内部标签，并且与所输出的信息关联。

Class B1 requirements — **Security Policy**

- Labels
  - **Exportation of Labeled Information**

    TCB必须指派每个通信信道和I/O设备是单级别的还是多级别的，必须通过手工方式才能改变这种指派，并且可以审计这种改变指派的行为。

    TCB必须能够维护每个通信信道或I/O设备的一个或多个安全级别，并且能审计它们发生的改变。

Class B1 requirements — Security Policy

- Labels
  - Exportation of Labeled Information
    - Exportation to Multilevel Devices
      - 当TCB输出一个对象到多级I/O设备时，该对象的敏感级别也同样被输出，并且以同样的形式（机读或人读的形式）保留在该物理设备上。
      - 当TCB在一个多级通信信道上输入或输出对象时，通道的通信协议必须在敏感性级别和相应的信息之间提供无二义性匹配。
    - Exportation to Single-Level Devices
      - TCB必须具备机制以保证TCB和授权用户在这个单级别设备上进行可靠的指定级别信息的输入或输出的通信。
    - Labeling Human-Readable Output

Class B1 requirements — **Security Policy**

- Labels
  - **Exportation of Labeled Information**
    - **Exportation to Multilevel Devices**
    - **Exportation to Single-Level Devices**
    - **Labeling Human-Readable Output**
      - 系统管理员必须能为输出的标签指定可打印的标签名字。
      - 必须在人可读的信息、页面、硬拷贝（如打印输出）等**开始和结束处作上人可读的敏感标签记号**来代表输出信息敏感性。
      - 默认的情况下在每个人可读信息、页面、打印输出的页面的**顶端和底端作上人可读敏感标签**，它们代表了输出的敏感性或者在页面上信息的敏感性。
      - 默认的情况下以适当的方式对其它人可读的输出（地图、图像等）标上人可读的代表输出的敏感标签。
      - 任何对这些标记的覆盖都必须被TCB审计。

Class B1 requirements — Security Policy

mandatory access control

(1) 对所有的主体和存储类客体(例如进程、文件、设备)实施强制访问控制。

(2) 主体和客体都必须赋予全序的敏感等级和偏序的类别标签，用于强制访问控制的基础。

(3) 要支持两个以上这样的安全级别。

(4) 在所控制的主体和客体之间的访问必须满足:

(a) 下读规则;

(b) 上写规则;

(5) 必须用身份标识与验证信息来验证用户的身份，主体的安全级别和权限应该代表并且不大于用户的安全许可和权限。

Class B1 requirements

- **Accountability**
  - Identification and Authentication

(1) TCB必须要求用户在进行任何TCB期望控制的行为之前声明自己的身份。

(2) TCB必须利用一个受到保护的机制（例如，口令）来认证用户的身份。

(3) TCB必须保护认证信息，使得任何非授权的用户无法访问认证信息。

(4) TCB必须能够对ADP的用户进行单独的标识，并对单独用户实施账户责权（accountability）管理。

(5) TCB还必须提供机制将用户的身份与用户的审计行为联系起来。

(6) TCB必须维护验证单个用户的认证数据，以及单个用户的安全等级和授权信息。这些信息是TCB用来验证用户的身份，确认安全级别，对TCB外部的代表某个用户主体授权。

  - Audit
    - 对象的引入和删除事件必须记录对象的名称和对象的**安全级别**。
    - 计算机管理员可以选择记录任何一个事件以及相应的一个或多个用户的标识以及对象的安全级别。

- Assurance
  - **Operational Assurance**
    - **System Architecture**
      - C1：TCB能够保护自己的区域免受外部的干扰与损坏（修改它的代码和数据）。TCB控制的资源是系统中的一些用户组和客体。
      - C2：增加：TCB应该隔离资源，使得能够控制对它们的访问并进行审计。
      - **增加：TCB可以通过赋予进程以在其控制下的不同的地址空间来实行进程隔离。**
    - System Integrity NAR

- Life-Cycle Assurance
  - Security Testing
    - 必须有完全理解系统实现的测试小组人员对设计文档、源码、目标代码进行彻底的分析与测试。
    - 测试目标包括：（1）发现所有的能够使得TCB外部的主体读、改变或删除那些TCB的强制访问控制和自主访问控制不允许的数据。（2）没有一个主体在未授权的情况下能使得TCB进入无法响应另一个用户的请求。
    - 所有发现的错误都应该被清除或抑制，并且通过重新测试表明错误都被根除，也没有引进新的错误。
  - **Design Specification and Verification**
    - TCB支持的非形式化或形式化的安全策略模型应该在系统的整个生命周期内得到维护，并且可以证实与数据处理系统的原则是一致的。

Class B2 — STRUCTURED PROTECTION

- Trusted path
- Covert channel analysis
- Configuration management

Class B2 requirements — **Security Policy**

- Discretionary Access Control (the same as B1)
- Object Reuse (the same as B1)
- Label

  （1）TCB必须维护每个主体、客体（例如：进程、文件、段、设备等）相关联的敏感标签。这些标签是强制访问控制决策的基础。

  （1）TCB应该维护能被TCB外部的主体所直接或间接访问的ADP系统中的资源（主体、存储客体、ROM等）所关联的敏感标签。Label Integrity (the same as B1)

  - Exportation of Labeled Information (the same as B1)
  - **Subject Sensitivity Label**
  - **Device Labels**

Class B2 requirements — Security Policy

- Discretionary Access Control (the same as B1)
- Object Reuse (the same as B1)
- Label

  Exportation of Labeled Information (the same as B1)

  - **Subject Sensitivity Label**

    在一个交互式会话中一个终端用户所关联的安全级别发生改变时，**TCB**应该立即通知该终端用户。

  - **Device Labels**

    TCB应该对所有接入的物理设备赋予最小和最大的安全级别。这些安全级别被**TCB**的用来实施约束，是设备所在的物理环境所施加的。

mandatory access control

- B1: The TCB shall enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices).
- The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB.
- B1: The following requirements shall hold for all accesses between subjects and objects controlled by the TCB:
- The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects:

Class B2 requirements — Accountability

- Identification and Authentication
  - Identification and Authentication
    - **Trusted Path**

      （1）TCB必须支持在用户与本身之间用来初始登陆和认证的可信信道。

      （2）这个可信信道的通信只能由用户来发起。
  - Audit

    （8）TCB 能够记录所有标识的隐蔽信道的利用事件。

Class B2 requirements — Assurance

- Operational Assurance
  - System Architecture

（5）TCB应该由相互独立的模块组成。TCB应该有效地使用硬件提供的关键机制隔离这些模块，这将与没有这些硬件机制的形成极大的区别。

（6）TCB的设计能够实施最小特权。应该利用像分段等硬件机制来从逻辑上区分不同的存储客体，如只读、可写。完整地定义TCB的接口，明确地标识所有的TCB元素。

- System Integrity
- **Covert Channel Analysis**

  （1）系统的开发者应该彻底地检测存储隐蔽信道，并且用实际测量或估计方法确定每一个检测到的隐蔽信道带的宽。

- **Trusted Facility Management**

  （1）TCB必须区分操作员与管理员的功能。

Class B2 requirements — Assurance

- Life-Cycle Assurance
  - Security Testing

（4）所有发现的错误都应该被改正，并且通过重新测试表明错误都被根除，也没有引进新的错误。

（5）应该证实TCB比较（relatively）能抵御渗透攻击。

（6）测试结果应该表明TCB的实现与DTLS一致。.

Class B2 requirements — Assurance

- Life-Cycle Assurance
  2. Design Specification and Verification

（1）TCB支持的**形式化(B1: 非形式化或形式化)**的安全策略模型应该在自动数据处理系统的整个生命周期内得到维护，并且可以证实与数据处理系统的原则是一致的。

（2）（增加）TCB的DTLS应该完全地和准确地描述了TCB的行为效果、异常和错误消息。应该证实它准确地描述了TCB的接口。

Class B2 requirements — Assurance

- Life-Cycle Assurance

3. Configuration Management

(1) 在TCB的开发与维护过程中，配置管理系统必须维护对DTLS、其它的设计文档、实现方面的文档、源码、目标代码的版本、测试的装置和文档的改变的控制。

(2) 配置管理系统要保证所有的文档和当前TCB代码的一致性。应该具备从源码生成新的TCB版本的工具。

(3) 还应该具备比较新版本与老版本的差异的工具，以便确认所有的改变都在计划内的而且都被用在新的版本中。

Class B2 requirements — Documentation

- Security Features User's Guide
- Trusted Facility Manual

  （5）必须指明TCB中包含访问控制决策机制的模块。

  （6）必须说明修改一个TCB的某个模块而生成新的TCB的过程。
- Test Documentation

  （2）测试文档应该包含用来缩小隐蔽信道带宽的方法的有效性的测试结果。.

Class B2 requirements — Documentation

- Design Documentation

（2）阐述TCB实施的**形式化**的安全模型，并且证明其足以实施安全策略。

（4）展示描述性的顶层规约（descriptive top-level specification(DTLS)）准确地描述了TCB的接口。

（5）必须有文档来描述TCB实现引用监视器的概念，并且解释它是如何阻止被破坏、被绕过，它是正确地实现的。

（6）文档应当描述TCB的结构设计能够便于测试和实施最小特权。

（7）文档应该描述隐蔽信道的分析结果以及限制隐蔽信道的权衡策略。确定出所有可以用来发现存储型隐蔽信道的可审计事件。应该能确定不能通过审计机制检测的隐蔽信道的带宽。

Class B3 **SECURITY DOMAINS**

Class B3 requirements — **Security Policy**

- Discretionary Access Control
  - C2: These access controls shall be capable of including or excluding access to the granularity of a single user.
  - **These access controls shall be capable of specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object.**
  - Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given.
  - **Object Reuse** **(the same as B2)**
- Label (the same as B2)
- Mandatory Access Control (the same as B2)

Class B3 requirements — Accountability

- Identification and Authentication
  - Identification and Authentication
    - **Trusted Path**
      - B2: The TCB shall support a trusted communication path between itself and user for initial login and authentication. Communications via this path shall be initiated exclusively by a user.
      - The TCB shall support a trusted communication path between itself and user for **use when a positive TCB-to-user connection is required.**
      - Communications via this path shall be activated exclusively by a user or the TCB and shall be **logically isolated and unmistakably distinguishable from other paths.**

Class B3 requirements — Accountability

- Audit
  - The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy.
  - This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded
  - if the occurrence or accumulation of these security relevant events continues, the system shall take the lease disruptive action to terminate the event.

Class B3 requirements — Assurance

- Operational Assurance
  - System Architecture
    - The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system.
    - The TCB shall incorporate significant use of layering, abstraction and data hiding.
    - Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.

Class B3 requirements — Assurance

- Operational Assurance
  - System Integrity (the same as B2)
  - Covert Channel Analysis
    - B2: The system developer shall conduct a thorough search for covert storage channels and make a determination of the maximum bandwidth of each identified channel.
    - B3: The system developer shall conduct a thorough search for covert channels and make a determination of the maximum bandwidth of each identified channel.

Class B3 requirements — Assurance

- Operational Assurance
  - Trusted Facility Management
    - B2: The TCB shall support separate operator and administrator functions.
    - B3: ADD: The functions performed in the role of a security administrator shall be identified.
    - The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system.
    - Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

Class B3 requirements — Assurance

- Operational Assurance
  - **Trusted Recovery (ADD)**
    - **Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.**

Class B3 requirements — Assurance

- Life-Cycle Assurance
  - Security Testing
    - The TCB shall be found resistant to penetration.
    - No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain.
  - Design Specification and Verification
    - A convincing argument shall be given that the DTLS is consistent with the model.
  - Configuration Management (the same as B2)

Class B3 requirements — Documentation

- Security Features User's Guide (the same as B2)
- Trusted Facility Manual
  - The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described.
- Test Documentation (the same as B2)
- Design Documentation
  - The TCB implementation shall be informally shown to be consistent with the DTLS. The elements of the DTLS shall be shown, using informal techniques, to correspond to the elements of the TCB.

DIVISION A: VERIFIED PROTECTION

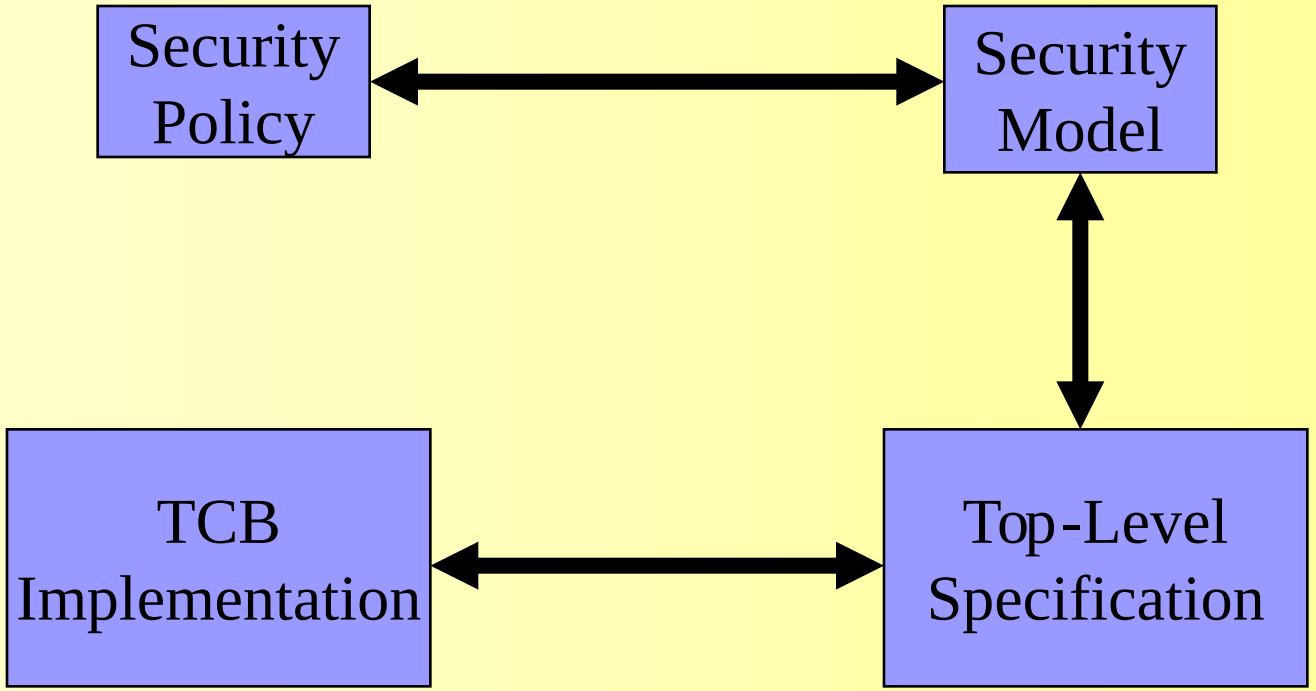
- Use of formal security verification methods
- Extensive documentation
  - TCB meets the security requirements in
    - design, development and implementation.

CLASS (A1): VERIFIED DESIGN

- Functionally equivalent to those in class (B3).
- Formal design specification and verification techniques and the resulting high degree of assurance
- This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design.

Five important criteria for class (A1) design verification

1. A formal model of the security policy
2. Formal top-level specification (FTLS)
3. The FTLS & the model
4. The TCB implementation & the FTLS.
5. Formal analysis techniques

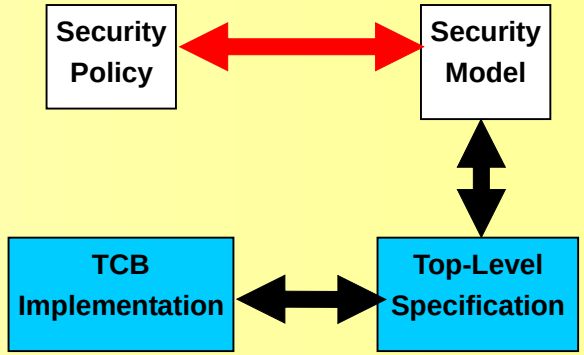

Security Policy
Security Model
TCB Implementation
Top-Level Specification

Five important criteria for class (A1) design verification

1. A formal model of the security policy

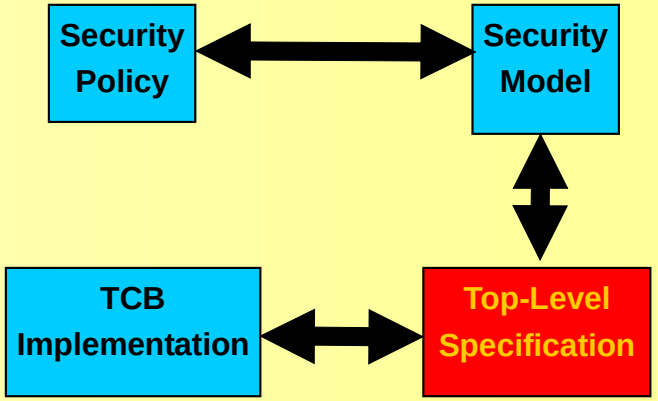
- A formal model of the security policy must be clearly identified and documented
  - including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.

2. Formal top-level specification (FTLS)
3. The FTLS & the model
4. The TCB implementation & the FTLS.
5. Formal analysis techniques



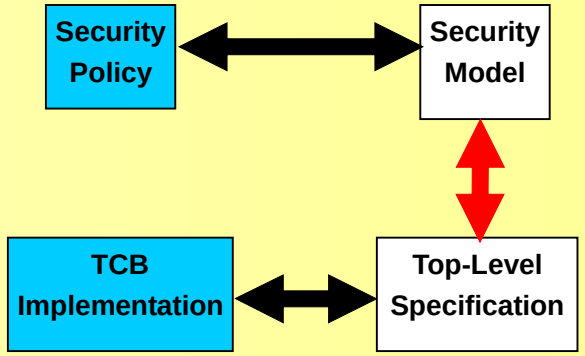
Five important criteria for class (A1) design verification

1. A formal model of the security policy
2. Formal top-level specification (FTLS)
   - An FTLS must be produced that includes abstract definitions of
     - the functions the TCB performs
     - the hardware and/or firmware mechanisms that are used to support separate execution domains.
3. The FTLS & the model
4. The TCB implementation & the FTLS.
5. Formal analysis techniques

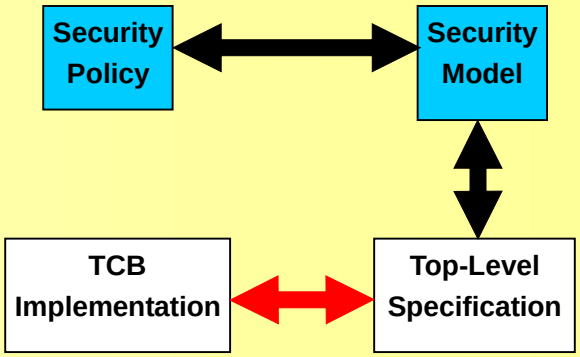


Five important criteria for class (A1) design verification

1. A formal model of the security policy
2. Formal top-level specification (FTLS)
3. **The FTLS & the model**
   - The FTLS of the TCB must be shown to be consistent with the model by formal techniques where possible (i.e., where verification tools exist) and informal ones otherwise.
4. The TCB implementation & the FTLS.
5. Formal analysis techniques



Five criteria for class (A1) design verification



1. A formal model of the security policy
2. Formal top-level specification (FTLS)
3. The FTLS & the model
4. **The TCB implementation & the FTLS.**
   - The elements of the FTLS must be shown, using informal techniques, to correspond to the elements of the TCB.
   - The FTLS must express the unified protection mechanism required to satisfy the security policy
   - And it is the elements of this protection mechanism that are mapped to the elements of the TCB.
5. Formal analysis techniques

Five important criteria for class (A1) design verification

1. A formal model of the security policy
2. Formal top-level specification (FTLS)
3. The FTLS & the model
4. The TCB implementation must be informally shown to be consistent with the FTLS.
5. **Formal analysis techniques**
   - Formal analysis techniques must be used to identify and analyze covert channels. Informal techniques may be used to identify covert timing channels. The continued existence of identified covert channels in the system must be justified.

Evaluation criteria for IT Security
— common criteria

ISO/IEC 15408, 1999

Contents

- **CC的背景**
- 通用模型
- 安全功能需求
- 安全保障需求与安全保障级别
- 安全保护规范（PP）
- 安全对象（security target， ST）

TCSEC的局限性

- TCSEC的范围局限性
  - TCSEC是为评估操作系统而制定的。
  - TCSEC主要考虑政府和军事组织的安全需求。
  - TCSEC不针对完整性、可用性等商业应用非常关键的需求。
  - 1987年发布了TNI。
  - 1992年发布了TDI。
- TCSEC的过程局限性
  - “标准蔓延”：定义TCSEC的评估等级的需求在逐渐扩展。
  - 评估过程花费的时间太长。

TCSEC的贡献

- TCSEC极大地提高了商业部门对计算机安全的需求意识。
- 20世纪90年代，新的安全产品不断涌现，商业部门不再满足于评估等级中的功能需求。
- TCSEC的不足，激起了开发新的评估方法的浪潮。
- 1987年美国计算机安全法规定，由美国国家安全局（NSA）负责保证机密信息和国家安全相关的计算机系统的安全。美国国家标准和技术研究所(NIST)则负责保证处理敏感的和非机密信息的计算机系统的安全。
- 1991年NSA和NIST开始制定新的标准，称为联邦标准FC。

欧洲ITSEC

- 欧洲多国安全评价方法的综合产物，军用，政府用和商用，1991年开始实施。
- 以超越TCSEC为目的，将安全概念分为功能与功能评估两部分。
- 功能准则在测定上分F1-F10共10级。1－5级对应于TCSEC的D到A。6－10级加上了以下概念:

  F6: 数据和程序的完整性　　F7: 系统可用性

  F8: 数据通信完整性　　F9: 数据通信保密性

  F10　包括机密性和完整性的网络安全

- 评估准则分为6级:

  E1: 测试　　E2: 配置控制和可控的分配

  E3: 能访问详细设计和源码　　E4: 详细的脆弱性分析

  E5: 设计与源码明显对应　　E6: 设计与源码在形式上一致。

加拿大CTCPEC

- 1989年公布，专为政府需求而设计
- 与ITSEC类似，将安全分为功能性需求和保证性需要两部分。
- 它给出了多种类型的功能需求的一种目录，引入了“功能一览表”的概念。
- 功能性要求分为四个大类:

  a 机密性　b 完整性　c　可用性　d 可控性

- 在每种安全需求下又分成很多小类，表示安全性上的差别，分级条数为0－5级。

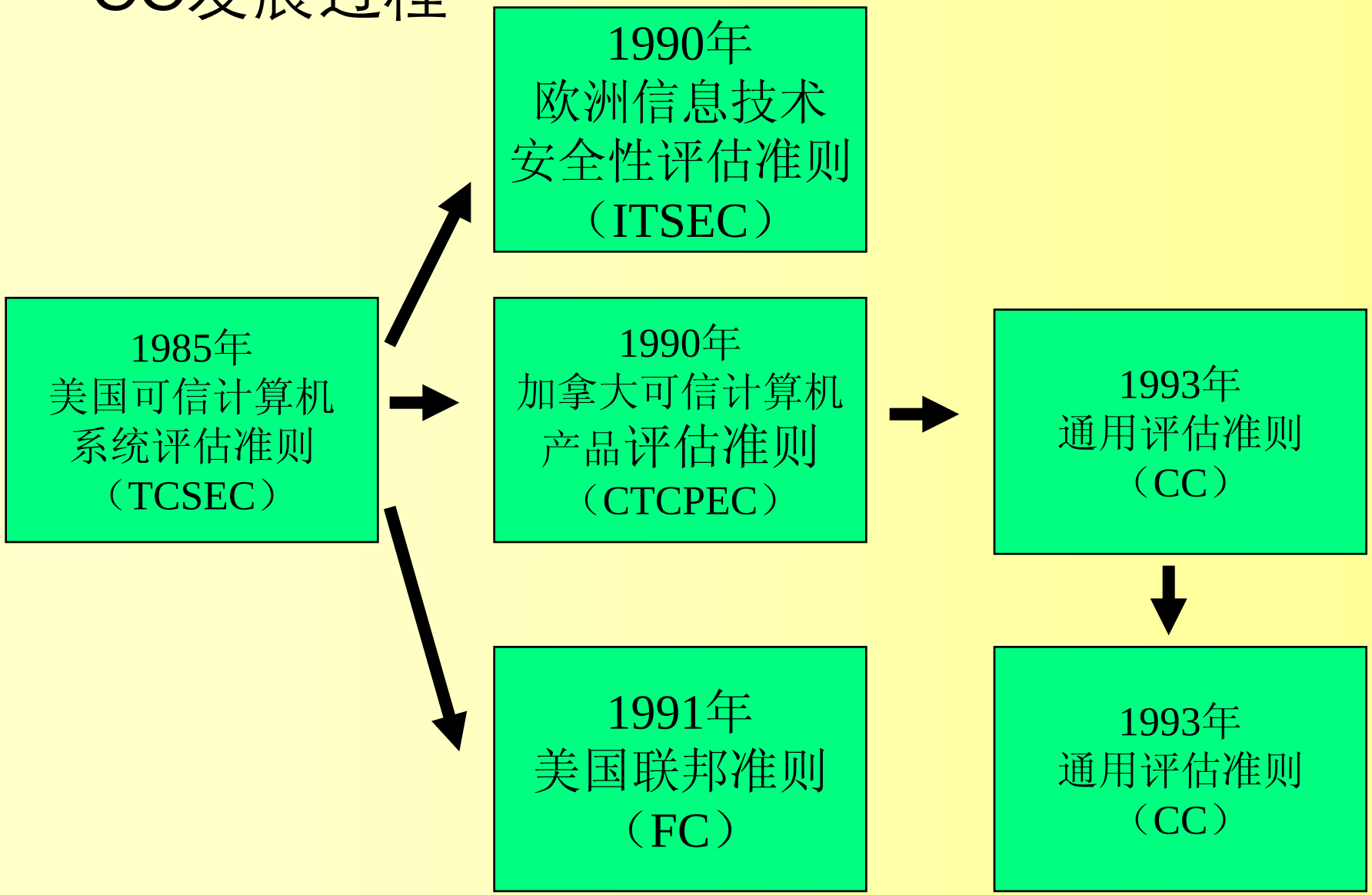
美国联邦准则(FC)

- 对TCSEC的升级1992年12月公布
- 引入了“保护轮廓（Protection Profile）”这一重要概念
- 每个轮廓都包括功能部分、开发保证部分和评测部分。
- 分级方式与TCSEC不同，吸取了ITSEC、CTCPEC中的优点。
- 供美国政府用、民用和商用。

通用准则（Common Criteria）

- 国际标准化组织统一现有多种准则的努力结果;
- 1993年开始，1996年出V 1.0, 1998年出V 2.0。
- 1999年6月成为国际标准，1999年12月ISO出版发行ISO/IEC 15408;
- 主要思想和框架取自ITSEC和FC;

CC发展过程


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

CC project sponsoring organizations

1. **CANADA:** Communications Security Establishment Criteria Coordinator
2. **FRANCE:** Service Central de la Sécurité des Systèmes d'Information (SCSSI)
3. **GERMANY:** Bundesamt für Sicherheit in der Informationstechnik
4. **NETHERLANDS:** Netherlands National Communications Security Agency
5. **UNITED KINGDOM:** Communications-Electronics Security Group Compusec Evaluation Methodology
6. **UNITED STATES - NIST:** National Institute of Standards and Technology Computer Security Division
7. **UNITED STATES - NSA:** National Security Agency

CC project sponsoring organizations

1. **CANADA:** Communications Security Establishment Criteria Coordinator
2. **FRANCE:** Service Central de la Sécurité des Systèmes d'Information (SCSSI)
3. **GERMANY:** Bundesamt für Sicherheit in der Informationstechnik
4. **NETHERLANDS:** Netherlands National Communications Security Agency
5. **UNITED KINGDOM:** Communications-Electronics Security Group Compusec Evaluation Methodology
6. **UNITED STATES - NIST:** National Institute of Standards and Technology Computer Security Division
7. **UNITED STATES - NSA:** National Security Agency

CC的使用对象

- 最终用户
- 开发者
- 评测者

最终用户

- 保证评估结果满足用户的需求。
- 判断被评估的产品或系统是否满足他们的需求（ 风险分析、安全策略）
- 比较不同的产品或系统（安全保证需求）。
- 给予用户一个独立于实现的表达对于产品或系统IT安全措施需求的一种方法： Protection Profile (PP) 。

开发者

- 评价他们开发的产品或系统。
- 明确他们的产品或系统的能够满足的安全需求。
- 支持其他人来评估开发的评估对象。
- 开发者可以声明所开发的产品或系统满足指定的安全功能需求和安全保障需求。

评估者

- 提供评估者来判断评估对象是否满足安全需求的系列准则。
- 描述评估者在评估过程中实施在安全功能上的一般行为。
- 并不固定评估行为的具体步骤。

CC 组成

- 引言和通用模型(General Mode)
- 安全功能需求 (Security functional requirements)
- 安全保障需求(Security assurance requirements)

Part 1, Introduction and general model

- It defines general concepts and principles of IT security evaluation and presents a general model of evaluation.
- Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.
- In addition, the usefulness of each part of the CC is described in terms of each of the target audiences.

Part 2, Security functional requirements

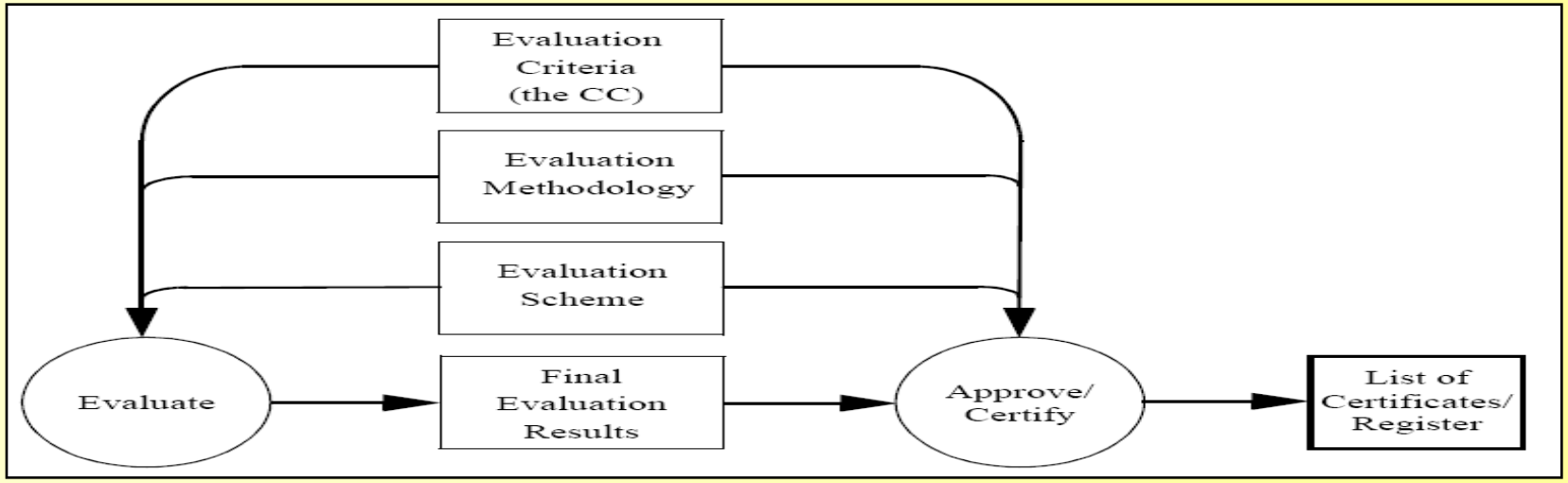
- Establishes a set of functional components as a standard way of expressing the functional requirements for TOEs.
- Part 2 catalogues the set of functional components, families, and classes.

Part 3, Security assurance requirements

- Establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs.
- Part 3 catalogues the set of assurance components, families and classes.
- Part 3 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined CC scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

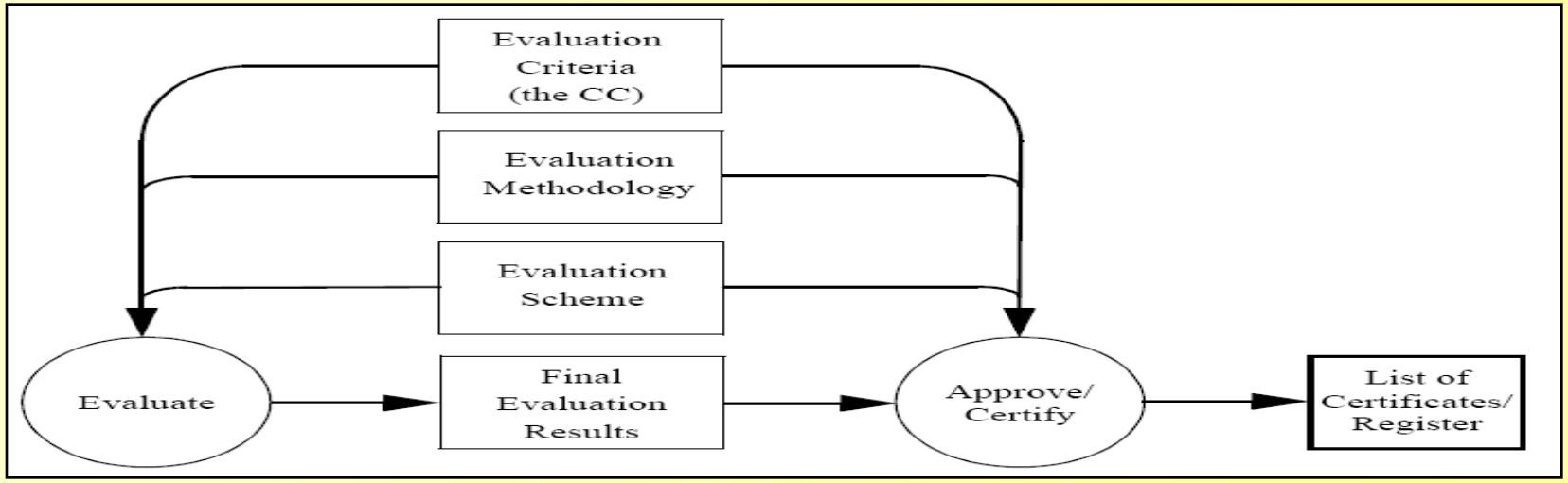
Evaluation context

- In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative **evaluation scheme，that**
  - sets the standards
  - monitors the quality of the evaluations
  - administers the regulations to which the evaluation facilities and evaluators must conform.



Evaluation context

- Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve.
- In order to enhance the consistency of the evaluation findings, the final evaluation results could be submitted to a certification process.
- The evaluation scheme, methodology, and certification processes are the responsibility of the evaluation authorities that run evaluation schemes and are outside the scope of the CC.



Contents

- CC的背景
- **通用模型**
- 安全功能
- 安全保障与安全保障级别
- 安全保护规范
- 安全目标（security target）

关键概念

- 保护轮廓——PP （Protection Profile）
- 安全目标——ST（ Security Target）
- 组件(Component)
- 包（Package)
- 评估保证级——EAL（ Evaluation Assurance Level）

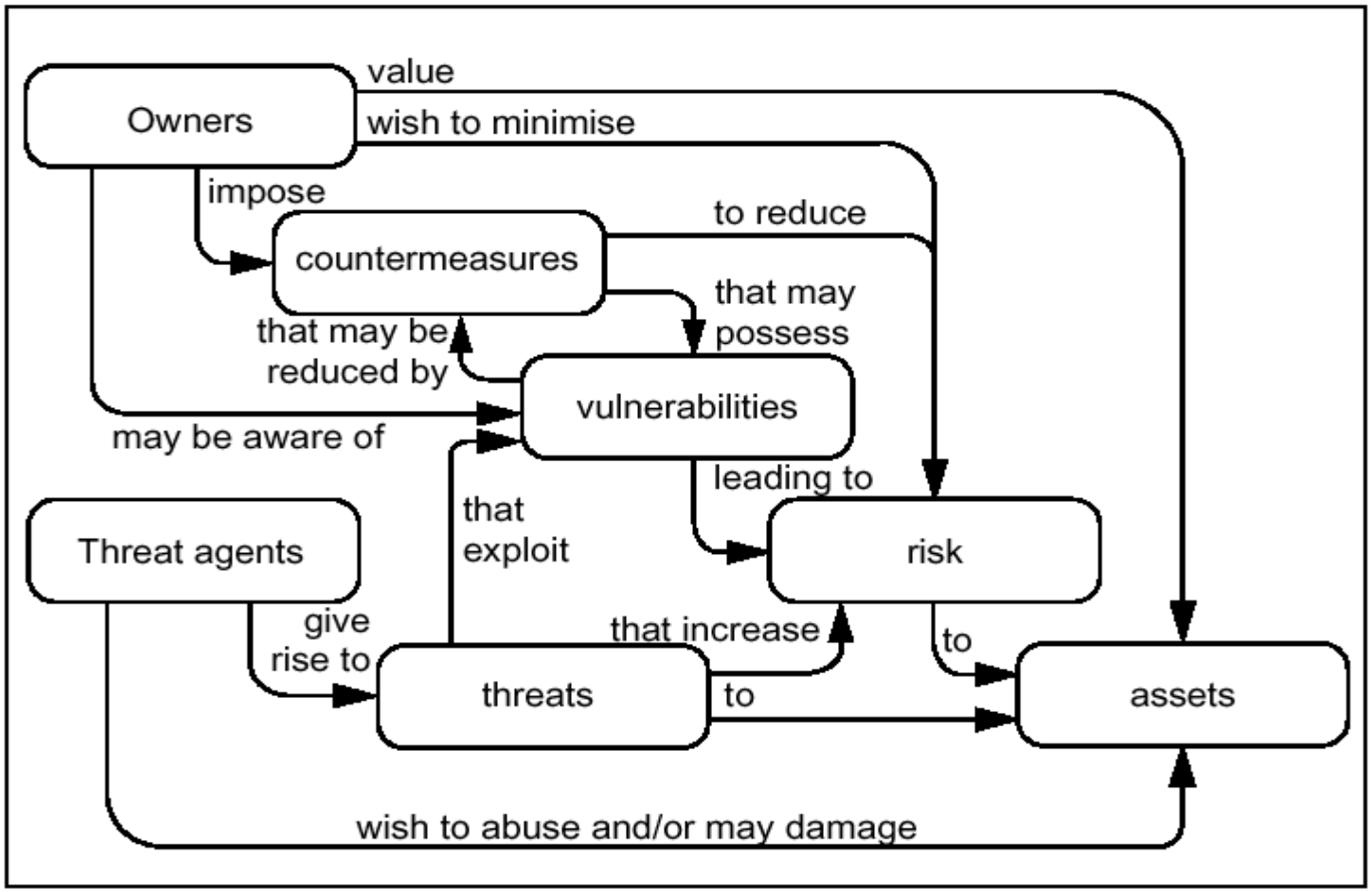
CC 通用模型

(1) 安全概念及其相互关系

(2) CC 的方法

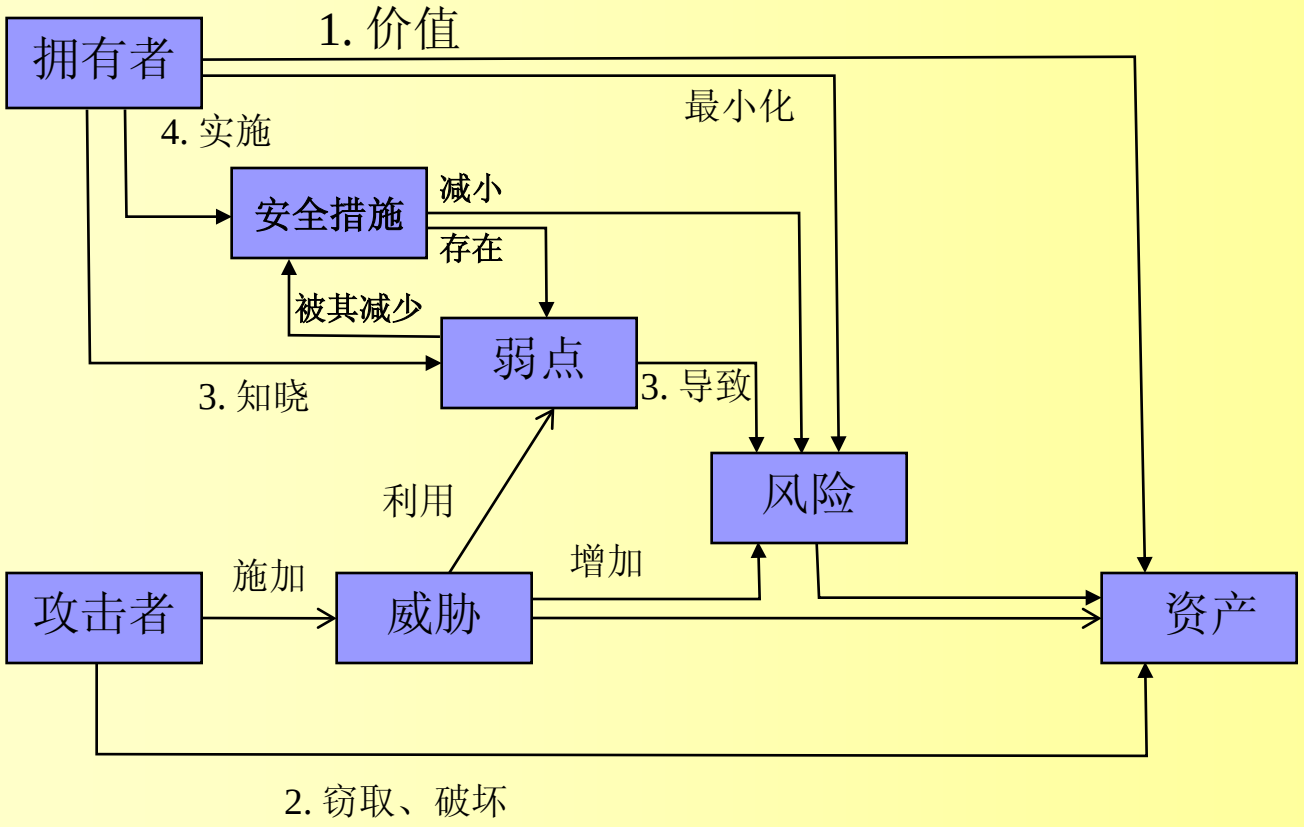
(3) 安全概念

(1)安全概念及其相互关系



Security concepts and relationships

(1)安全概念及其相互关系



安全概念及其相互关系

(1)安全概念及其相互关系

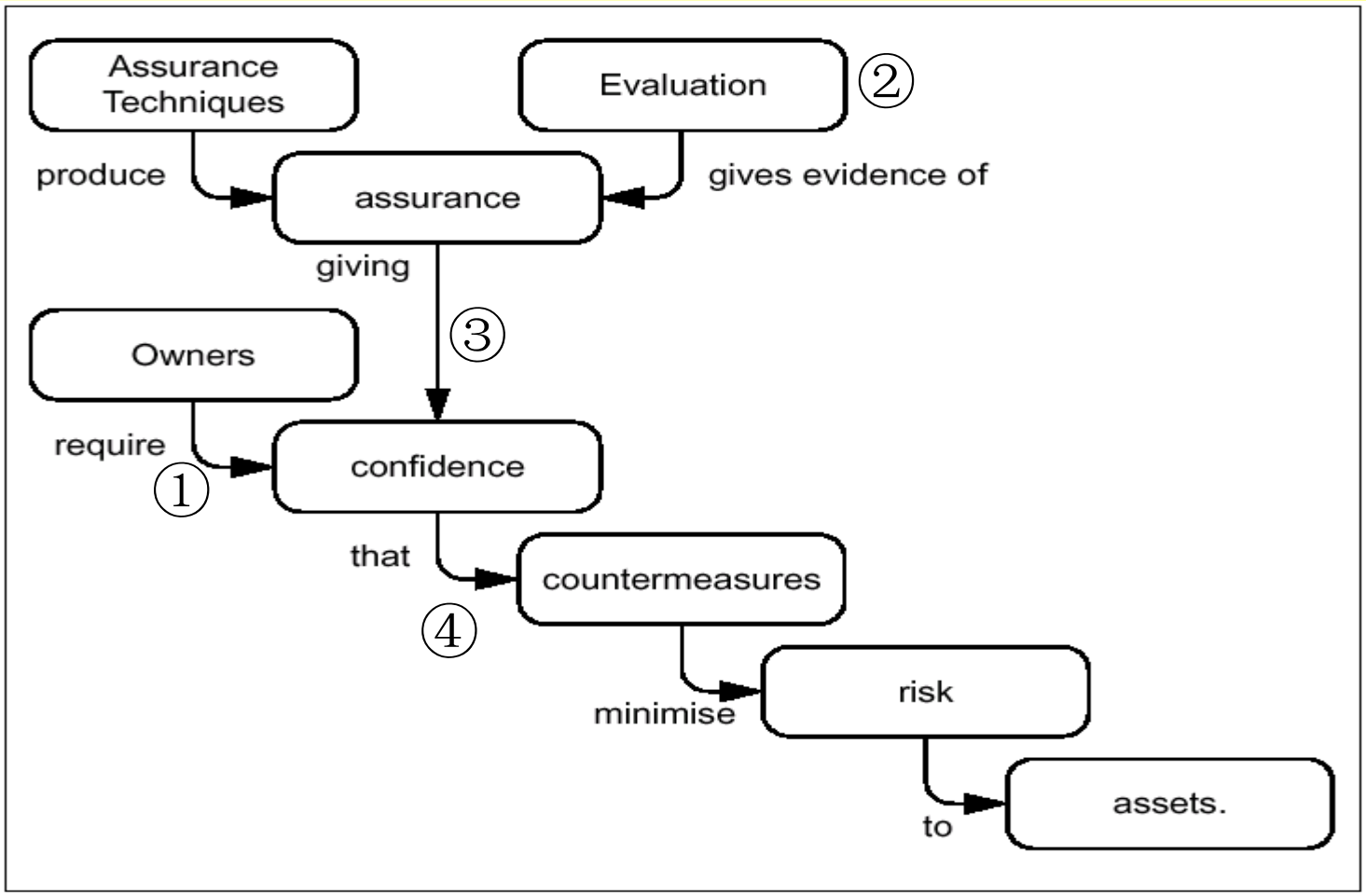
安全就是保护信息资产免受各种威胁，特别是人为的恶意的攻击的威胁。

1. 信息资产的拥有者清楚自己拥有的信息资产的价值。
2. 攻击者也是发现了这个信息资产的价值，要设法窃取或破坏。
3. 拥有者知道所面临的各种威胁，例如：泄露机密信息、篡改信息、失去资产可用性等等。

   拥有者也清楚系统存在着弱点，这些弱点导致信息资产面临风险；攻击者会利用这些弱点，这样就增加了信息资产面临的风险。

   拥有者要将信息资产面临的风险降低到最低。
4. 拥有者通过实施安全措施，系统的弱点将被减少，从而减小信息资产面临的风险。
5. 但是，即便实施了安全措施，系统仍然存在弱点，仍然存在着残余风险。面对着残余的风险，信息资产的拥有者**是否有信心**将这些信息资产暴露在这些残余风险面前。

(1)安全概念及其相互关系



Evaluation concepts and relationships

(1) 安全概念及其相互关系

① Owners will need to be confident that the countermeasures are adequate to counter the threats to assets before they will allow exposure of their assets to the specified threats.

② Owners may not themselves possess the capability to judge all aspects of the countermeasures, and may therefore seek evaluation of the countermeasures.

③ The outcome of evaluation is a statement about the extent to which assurance is gained that the countermeasures can be trusted to reduce the risks to the protected assets.

④ The statement assigns an assurance rating of the countermeasures, assurance being that property of the countermeasures that gives grounds for confidence in their proper operation. This statement can be used by the owner of the assets in deciding whether to accept the risk of exposing the assets to the threats.

⑤ Owners of assets will normally be held responsible for those assets and should be able **to defend the decision** to accept the risks of exposing the assets to the threats.

Statements resulting from evaluation are defensible.

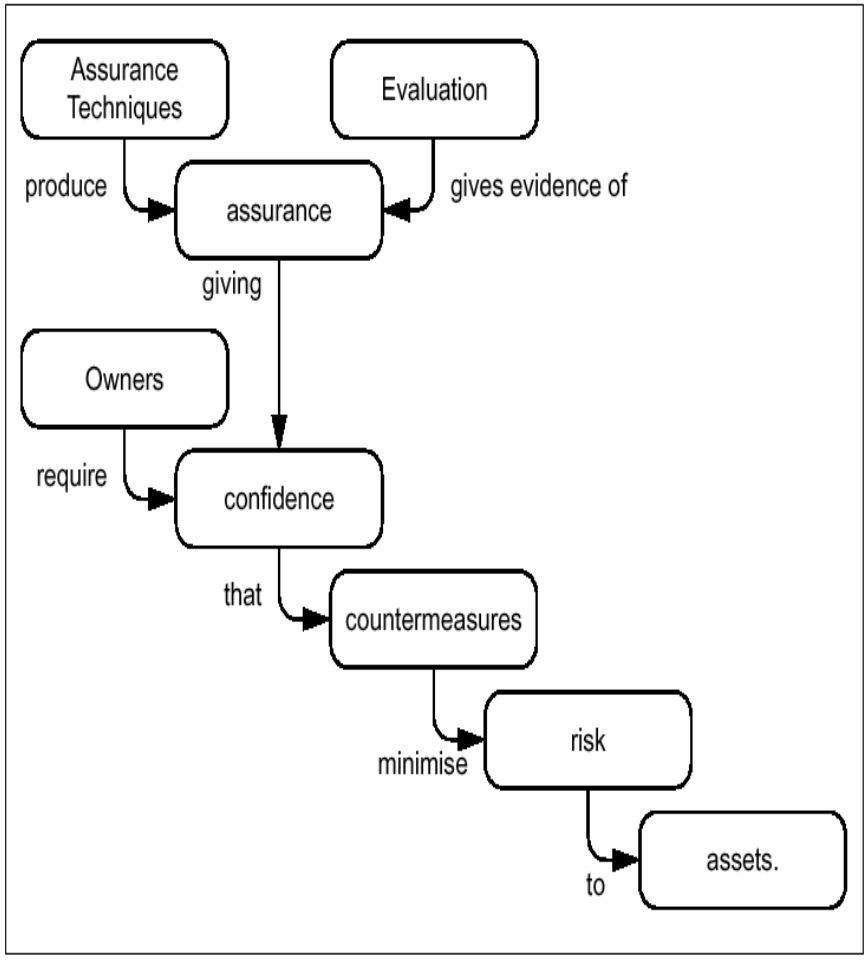
Evaluation should lead to objective and repeatable results that can be cited as evidence.

(1) 安全概念及其相互关系

① Owners will need to be confident that the countermeasures are adequate to counter the threats to assets before they will allow exposure of their assets to the specified threats.

② Owners may not themselves possess the capability to judge all aspects of the countermeasures, and may therefore seek evaluation of the countermeasures.

③ The outcome of evaluation is a statement about the extent to which assurance is gained that the countermeasures can be trusted to reduce the risks to the protected assets.



Evaluation concepts and relationships

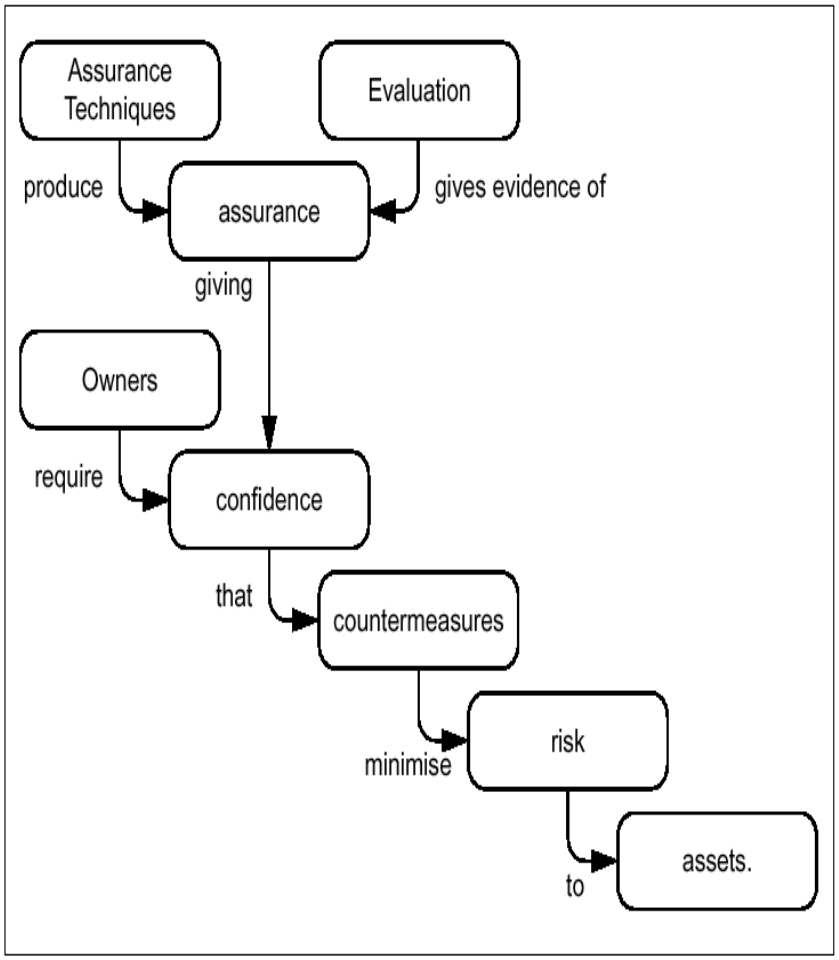
(1) 安全概念及其相互关系

① The statement assigns an assurance rating of the countermeasures, assurance being that property of the countermeasures that gives grounds for confidence in their proper operation. This statement can be used by the owner of the assets in deciding whether to accept the risk of exposing the assets to the threats.

② Owners of assets will normally be held responsible for those assets and should be able **to defend the decision** to accept the risks of exposing the assets to the threats.

Statements resulting from evaluation are defensible.

Evaluation should lead to objective and repeatable results that can be cited as evidence.



Evaluation concepts and relationships

（2） CC 的方法

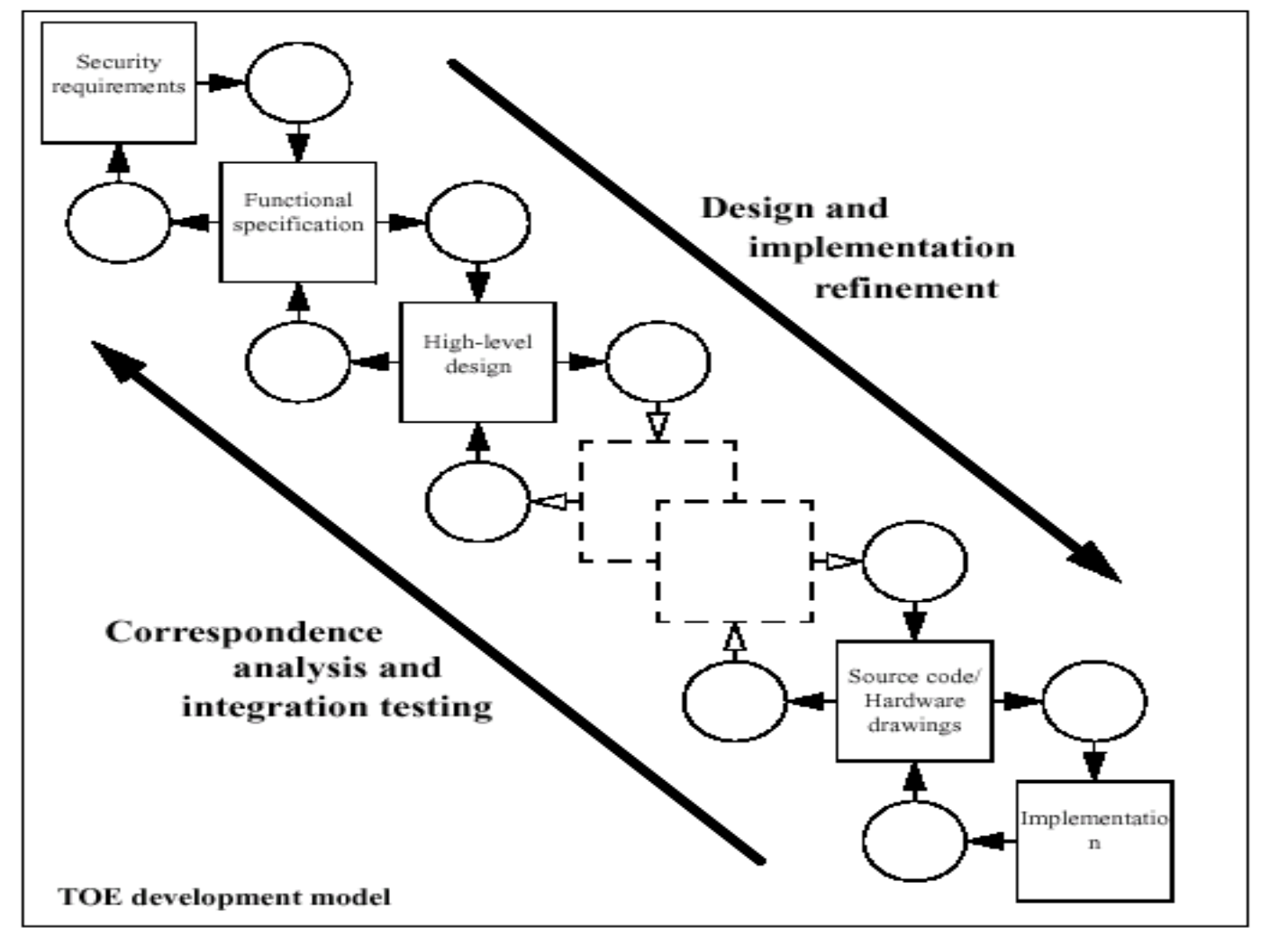
- IT 产品或系统的安全的信心来自于
  - 开发
  - 评价
  - 实施

  的过程。

（2） CC 的方法 — 开发

- **安全目标**：安全产品或安全系统的功能必须能实现用户的安全目标。
- **关注过程**：必须要从产品或系统的开发一开始就考虑其安全需求，否则即使采用良好的工程方法也难以满足用户期望的安全目标。
- **逐层细化**：开发过程就是将安全产品或安全系统的目标到系统的实现进行逐层细化的过程。
  - 底层的细化就是上层功能的分解和设计细节。
  - 最上层是安全目标，最下层是产品或系统的实现。

（2） CC 的方法 — 开发


Security requirements
Functional specification
High-level design
Source code/ Hardware drawings
Implementation
Design and implementation refinement
Correspondence analysis and integration testing
TOE development model

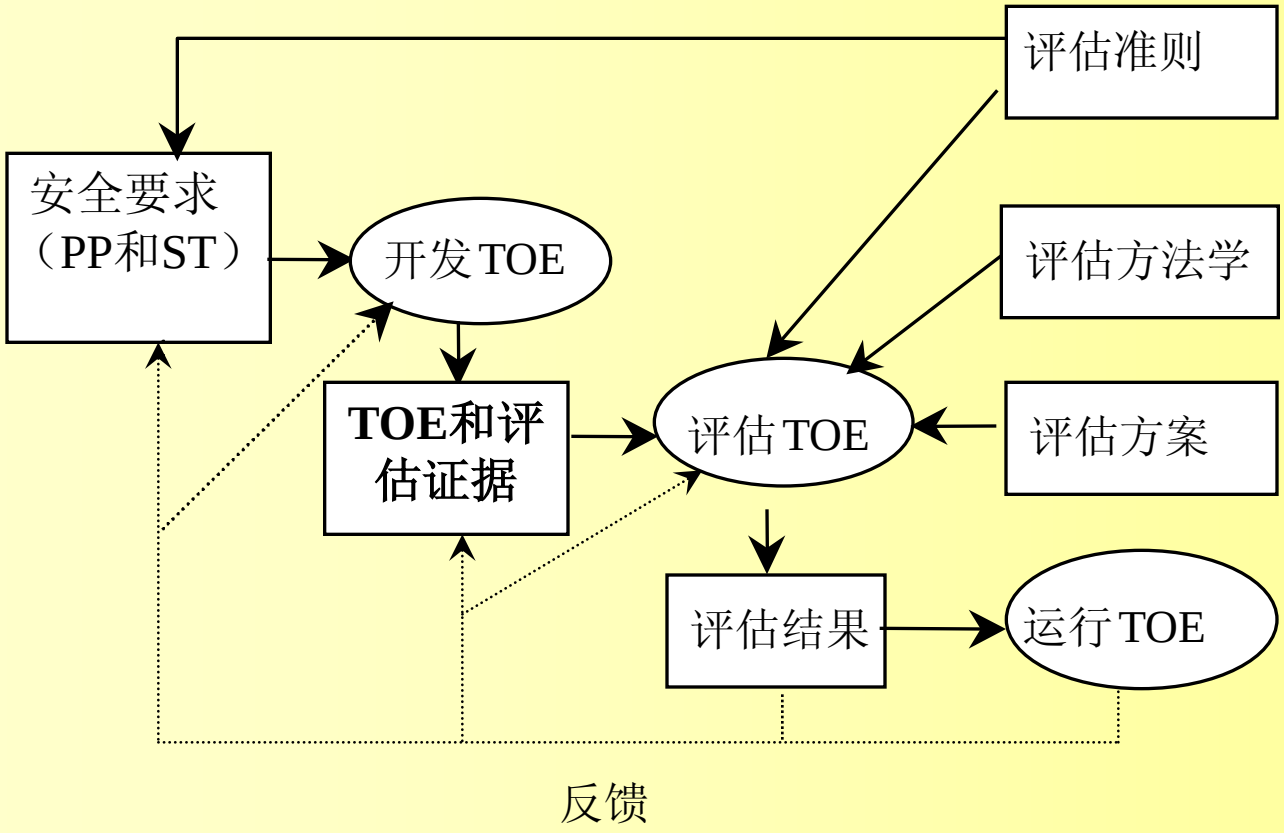
（2） CC 的方法 — 开发

- CC 完全没有要求开发过程采用什么样的开发方法和生命周期，但是，要求有足够的层次来使得每个层次有足够细的粒度阐述需求和实现方法。
  - 每一个层次是上一个层次**完全**细化，也就是上层安全功能、属性和行为的抽象要求都在这层体现出来了。
  - 每一个层次是上一个层次**精确**细化，也就是每一个层次实现的安全功能、属性和行为都是上一个层次所要求的。

（2） CC 的方法 — 开发

- CC 保障性评估必须验明功能规约的各个抽象层次：高层设计、底层设计、系统实现。
- 开发者必须根据所要求的保障级别来证实所采用的开发方法达到了保障性需求。

（2） CC 方法 — TOE 测评


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

（2） CC 方法 — TOE 测评

- 评估任务的主要输入
  - 测评过的ST，作为评估工作的依据。
  - 评估对象。
  - 评估准则、方法和方案。

（2） CC 方法 — TOE 测评

- 评估过程的期望的结果是评估对象满足ST中描述的安全需求。
- 评估值依据评估准则对评估对象得出的结论和依据的报告。
- 依据对安全保障需求的满足情况获得的对评估对象的信任度。

（2） CC 方法 — TOE 测评

- 评测可以从两个方面提高产品或系统的安全性:
  - 评估的旨在发现评估对象中的存在的错误和脆弱性，以便由开发者改正，避免在将来的使用过程中的损失。
  - 开发者为了通过严格的评估，在他们的设计和开发过程需求更加认真仔细。评估过程可以对**原始的需求**、**开发过程**、**最终产品**、**运行环境**进行严格评估。

（2） CC 方法 — 实施

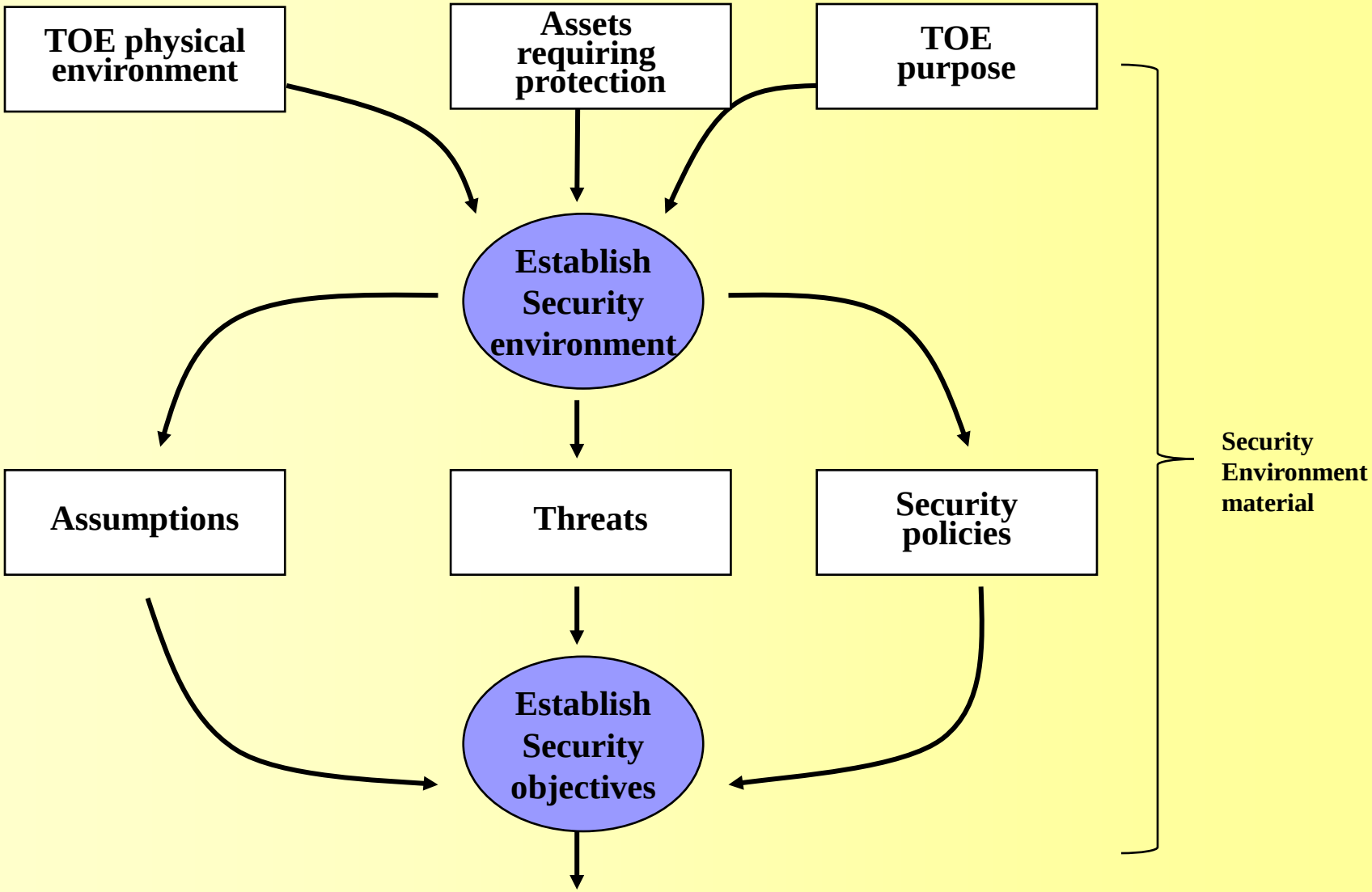
- 用户可以选择测评过的产品或系统应用到他们的环境中。
- 在实施过程中，产品或系统的错误或弱点就会浮现，对环境的假定可能需要更该。
- 开发者会收到反馈，更新产品或系统。
- 更新后的产品或系统需要重新进行评测。

(3) 安全概念

- In order to show that the assets are secure, the security concerns must be addressed at all levels from the most abstract to the final IT implementation in its operational environment.
- A level must contain a reasoned and convincing argument that shows that it is in conformance with the higher level, and is itself complete, correct and internally consistent.

- Security environment
- Security objectives
- Security requirements

CC — General model —Security concepts



Security environment

- To establish the security environment, the PP or ST writer has to take into account:
  - the TOE physical environment
  - the assets
    - requiring protection by the element of the TOE
    - files and databases
    - authorisation credentials and the IT implementation itself
  - the TOE purpose, which would address the product type and the intended usage of the TOE.

Security objectives

- A statement of assumptions which are to be met by the environment of the TOE to be considered secure.
- Characterises a threat in terms of a threat agent, a presumed attack method, any vulnerabilities, and identification of the asset under attack.
- A statement of applicable organisational security policies.

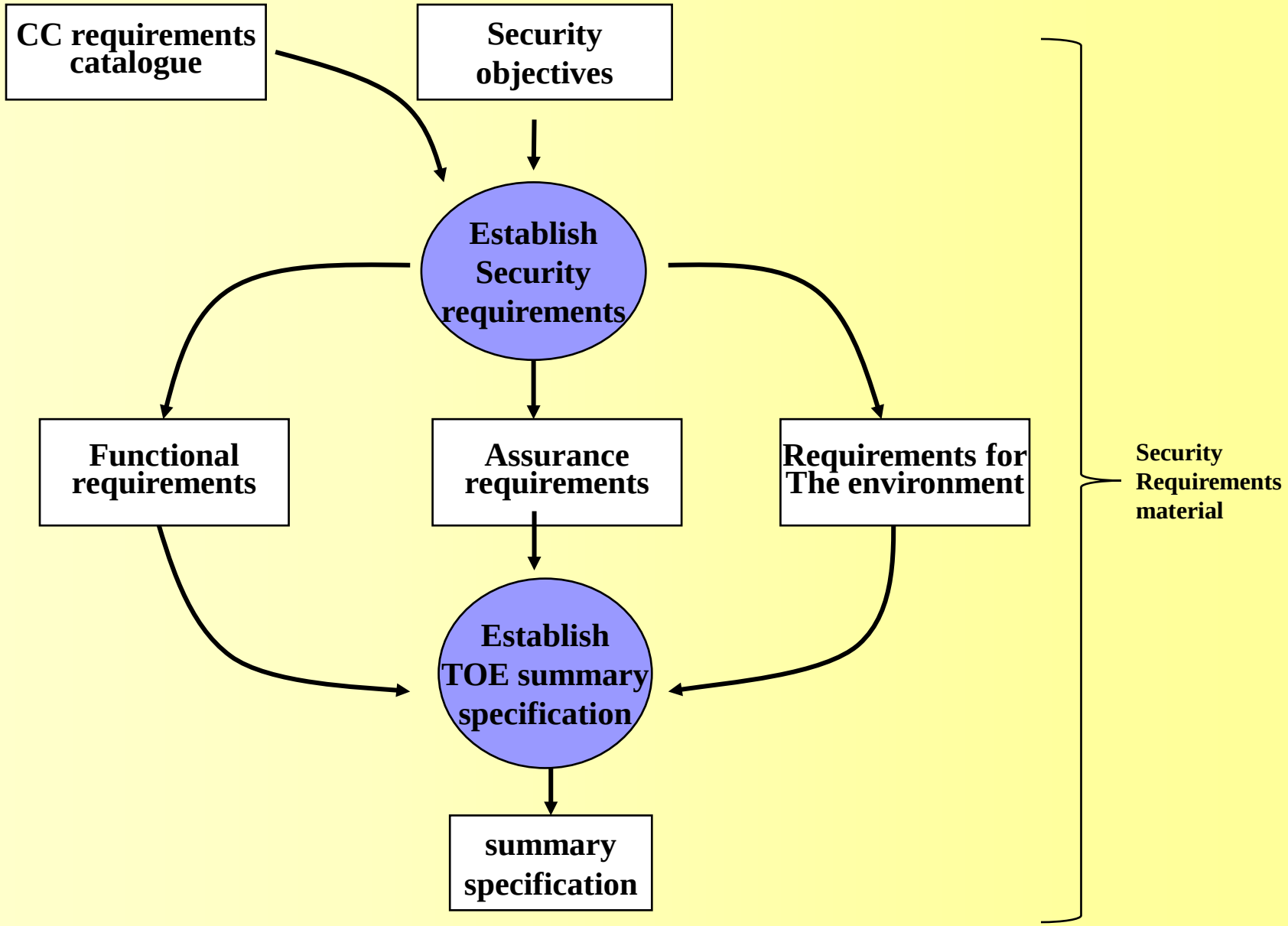
Security objectives

The security environment could then be used to state the security objectives

- Counter the identified threats
- Address identified organisational security policies and assumptions.

- **The security objectives should be consistent with the stated operational aim or product purpose of the TOE, and any knowledge about its physical environment.**
- **Only the security objectives for the TOE and its IT environment are addressed by IT security requirements.**

CC — General model —Security concepts

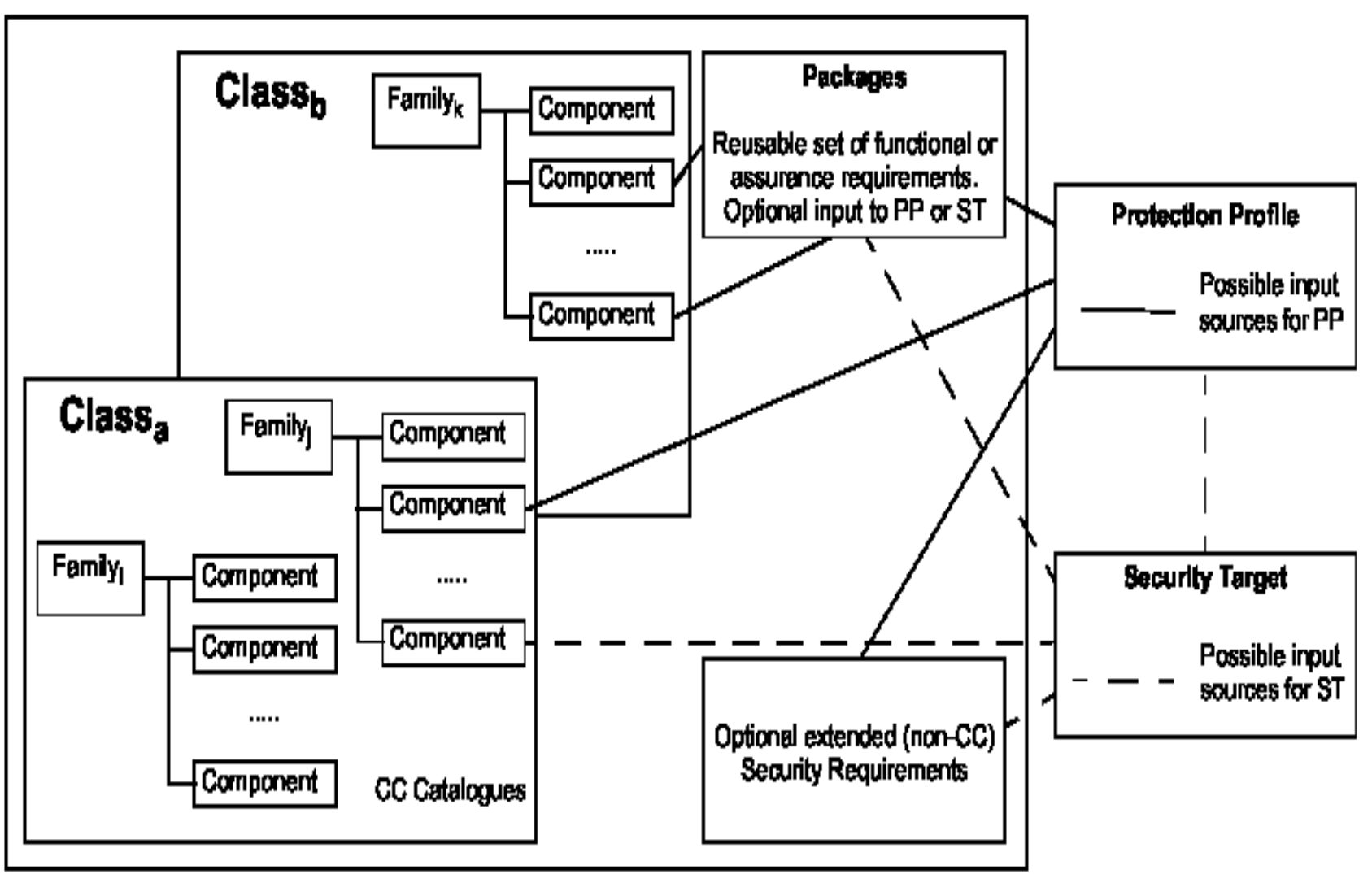


Security requirements

- Functional requirements and assurance requirements
  - Functional requirements define the desired security behaviour, such as identification, authentication, security audit and non-repudiation of origin.
  - The assurance requirements may specify that a minimum strength level consistent with the security objectives is to be claimed.

安全需求

Expression of security requirements



Class

- The term class is used for the most general grouping of security requirements.
  - All the members of a class share a common focus, while differing in coverage of security objectives.
  - The members of a class are termed families.

- Example of CC Classes
  - **Class FAU: Security audit**
  - **Class FCS: Cryptographic support**
  - **Class FDP: User data protection**
  - **Class FIA: Identification and authentication**
  - **Class FMT: Security management**
  - ……

Family

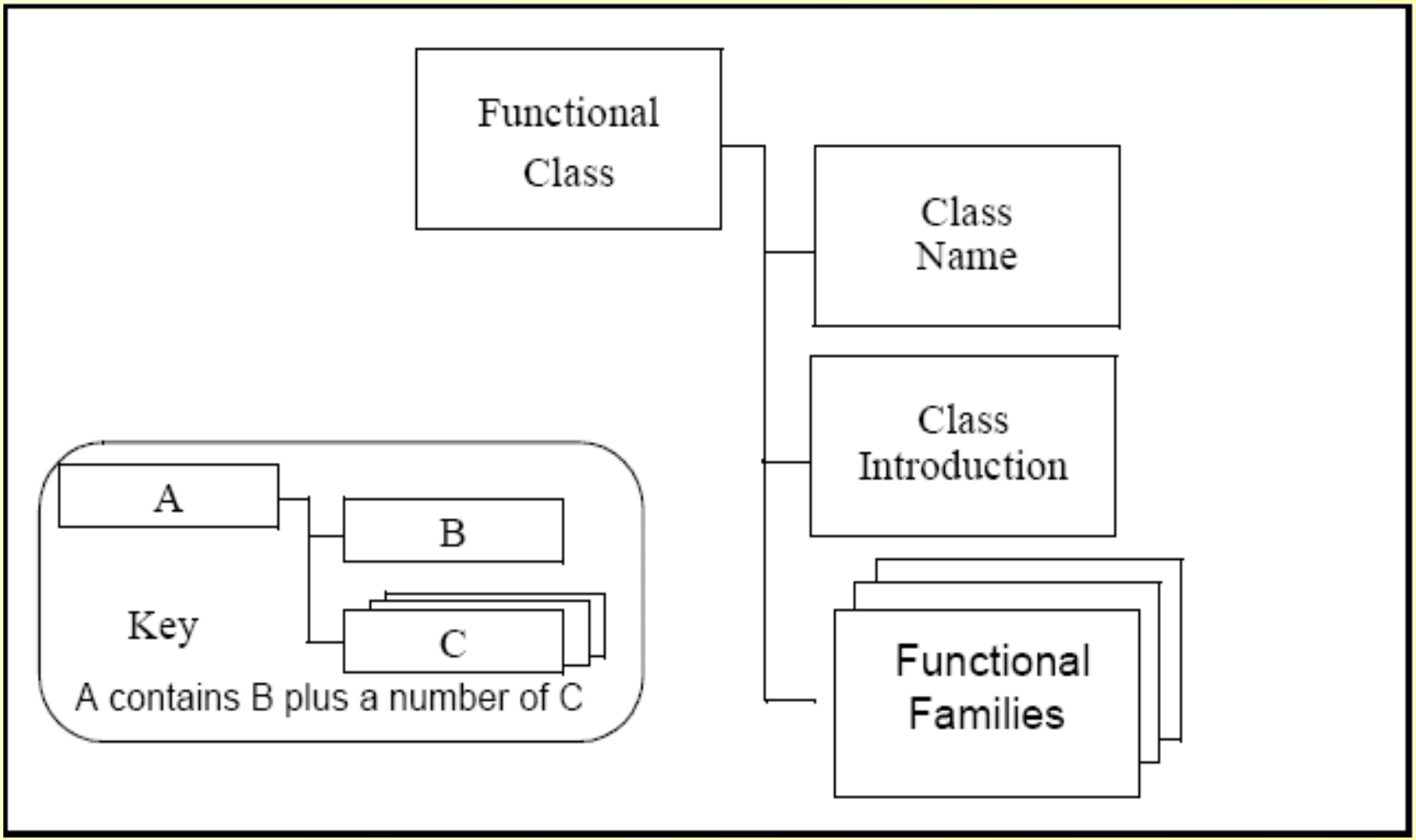
- A family is a grouping of sets of security requirements that
  - share security objectives
  - but may differ in emphasis or rigour.

- **Class FIA: Identification and authentication**
  - FIA_AFL Authentication failures
  - FIA_ATD User attribute definition
  - FIA_SOS Specification of secrets
  - FIA_UAU User authentication
  - FIA_UID User identification
  - FIA_USB User-subject binding

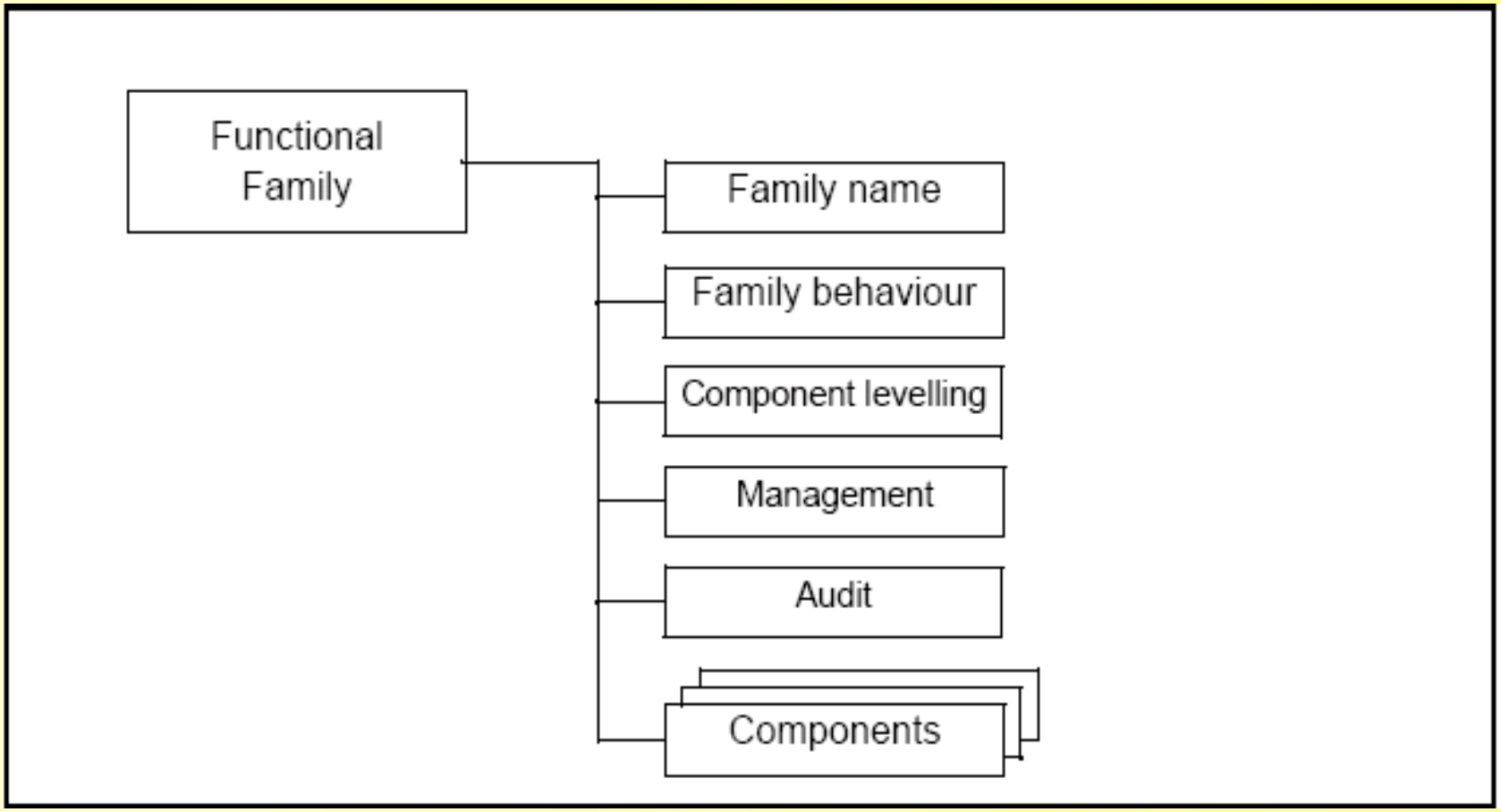
Component

- A component describes a specific set of security requirements and is **the smallest selectable set** of security requirements.
  - The set of components within a family
    - may be ordered to represent increasing strength or capability of security requirements that share a common purpose.
    - may also be partially ordered to represent related non-hierarchical sets.

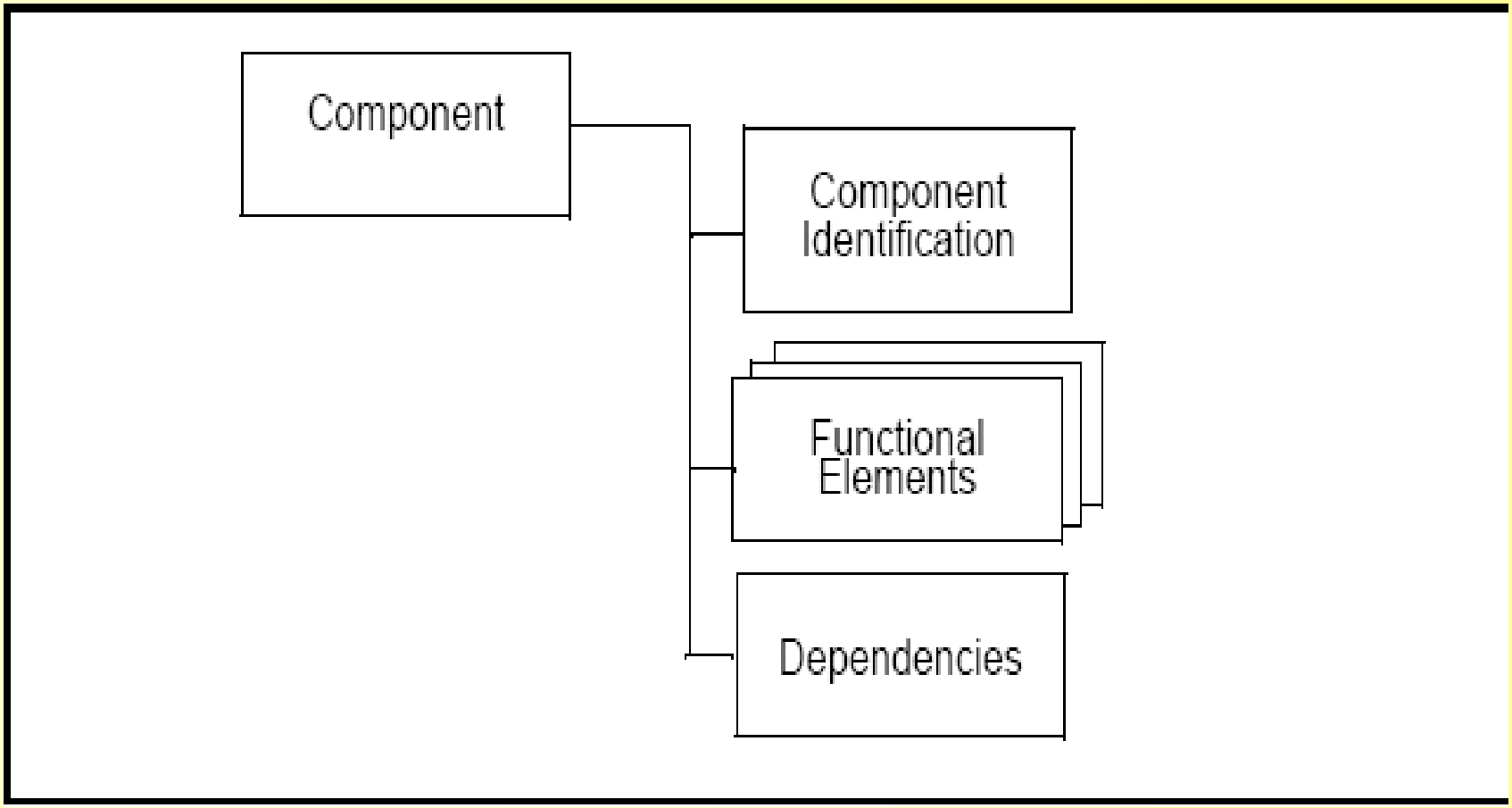
Security Function Requirement — Family



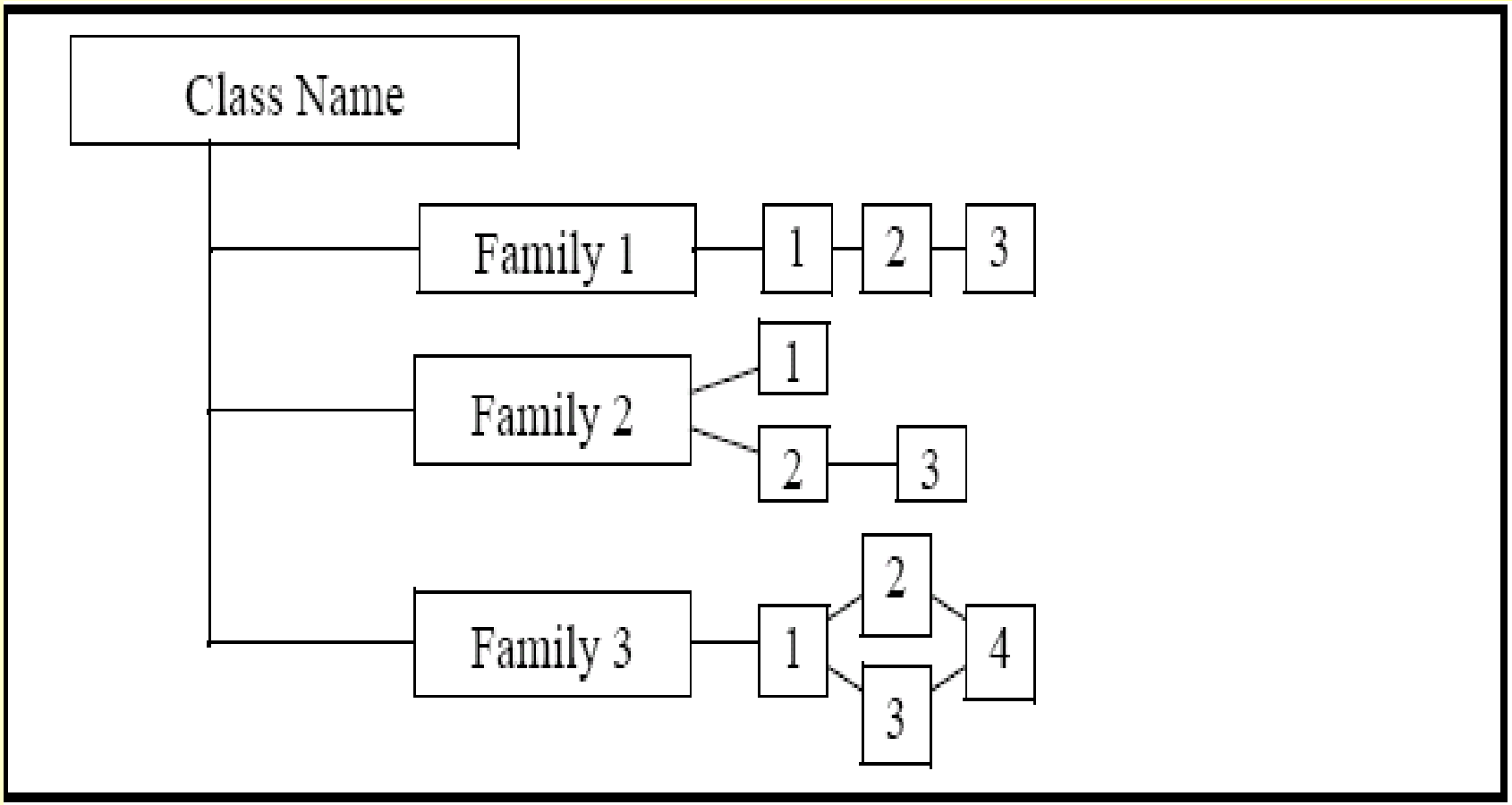
Security Function Requirement — Components



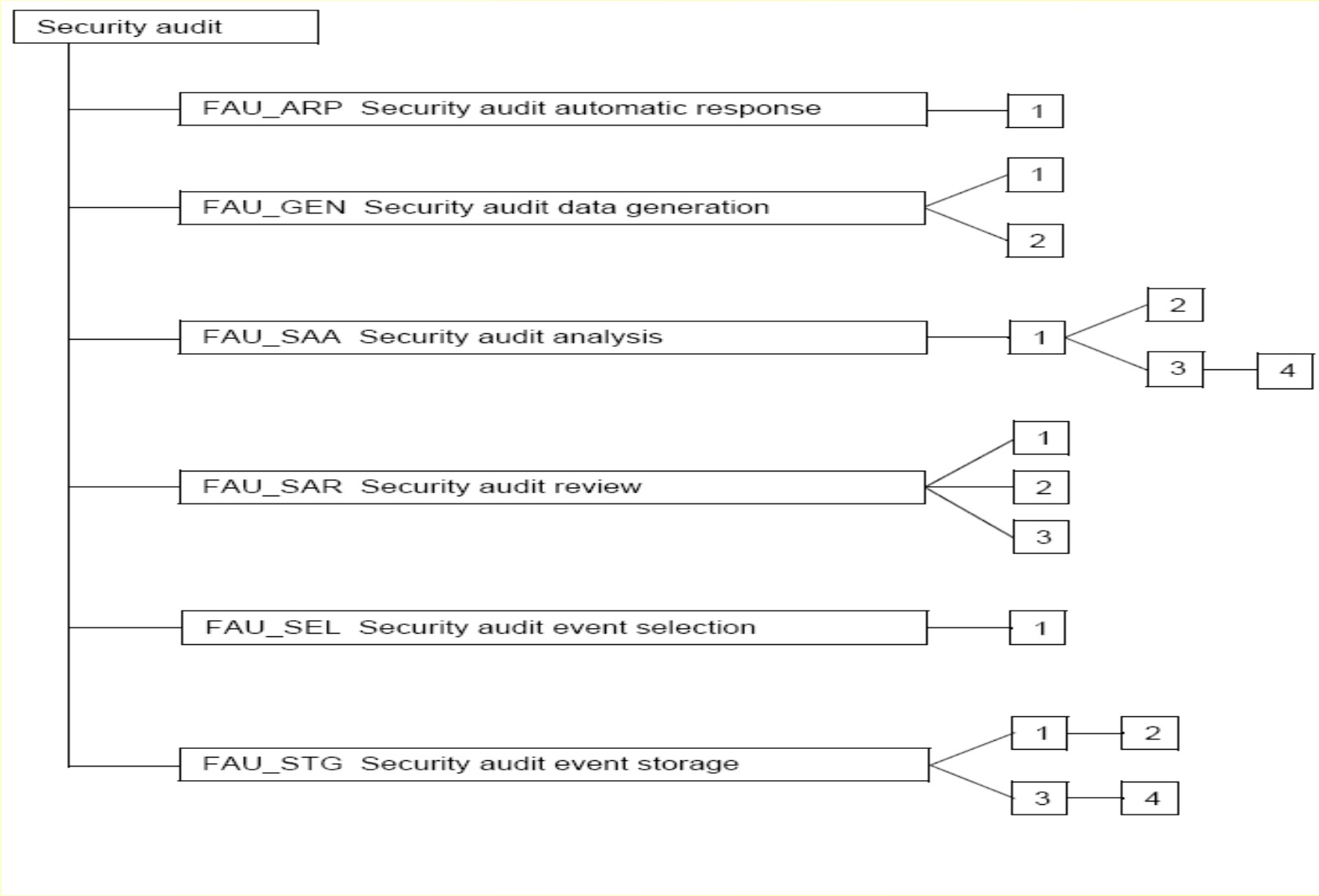
Security Function Requirement — Dependencies



Sample class decomposition diagram



Class FAU: Security audit



安全功能需求

CC安全功能需求

- FAU-安全审计
  - 该类包含6个族，分别是审计自动响应、审计数据生成、审计分析、审计审查、审计事件选择以及审计事件存储。
- FCO-通信
  - 该类包含两个族，分别针对源不可否认性和接收不可否认性。CC是第一个包含这种这种需求的评估方法。
- FCS-密码支持
  - 该类包含两个族，分别处理密钥管理和密码操作。加密算法以及其他题可采用FIPS140-2来评估。

CC安全功能需求

- FDP-用户数据保护
  - 该类有13个族。该类包含两种不同类型的安全策略：访问控制和信息流策略。每种安全策略有两个族，一个族说明策略类型，另一个族说明策略的功能。两种类型的策略有本质上的区别，访问控制策略的决策基于离散的信息集，比如访问控制列表和访问许可，而信息流控制策略针对的是从一个信息库到另一个信息库的信息流。
  - 自主访问控制策略是一种访问控制策略，而强制型访问控制策略是一种信息流控制策略。
- FIA-身份标识和验证
  - 该类包含6个族，分别是认证失败处理、用户属性定义、秘密规范、用户认证、用户身份标识和用户／主体绑定。

CC安全功能需求

- FMT-安全管理
  - 该类包含5个族，分别是安全属性的管理、TSF数据管理、角色管理、TSF功能管理以及撤销管理。
- FPR-隐私性
  - CC是第一种支持该类的评估方法。该类包含的族主要处理匿名性、伪匿名性、不可关联性和不可观测性。
- FPT-安全功能保护
  - 该类包含16个族。描述参考监视需求的族包括TSF物理保护、引用监视、域分离。其他的族处理基础抽象机测试、TSF自检测、可信恢复、导出TSF数据的可用性、导出TSF数据的机密性、导出TSF数据的完整性、内部产品或系统的TSF数据传输、重放险测、状态同步协议、时间戳、TSF间数据一致性、内部产品或系统TSF数据重定位的一致性以及TSF自检测。

CC安全功能需求

- FRU-资源利用
  - 该类包含三个族。分别处理容错、资源分配以及服务优先级
- FTA-TOE访问
  - 该类包含6个族。多个并发会话的限制、会话锁定、访问历史记录、会话的建立、产品或系统访问标识以及可选属性范围限制(系统准入约束)。
- FTP-可信路径
  - 该类分为两个族，即TSF间的可信信道族和可信路径族。

安全保障需求

CC安全保障需求

- ACM-配置管理
  - 该类包含三个族：CM自动化、CM性能和CM范围。
- ADO-交付和操作
  - 该类包含两个族：交付和安装，以及生成和启动。
- ADV-开发
  - 该类包含7个族：功能规范、低层设计、实现描述、TSF内部组织、高层设计、描述一致性和安全策略模型。
- AGD-指南文档
  - 该类包含两个族：管理者指南和用户指南。
- ALC-生命周期
  - 该类包含4个族：安全性开发、缺陷消除、工具及技术和生命周期定义。

CC安全保障需求

- ATE-测试
  - 该类包含4个族：测试范围、测试深度、功能测试、独立性测试。
- AVA-漏洞评估
  - 该类包含4个族：隐信道分析、误用、功能强度和漏洞分析。
- AMA-安全保障维护
  - 该类包含4个族：安全保障维护计划、产品或系统组件分类报告、安全保障维护证据和安全影响分析。

Evaluation assurance level summary

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

安全保障级别

- EAL1：功能测试。该等级需要在安全功能分析的基础上，检查软件商提供的指南和文档，然后进行独立的测试。在安全功能分析中，需要使用功能规范和接口规范。EAL1适用于操作中需要一定的保密性，而同时安全威胁不是很严重的系统。

- EAL2：结构测试。该等级建立在安全功能分析的基础上，这里的安全功能分析包括高层设计分析。像EAL1一样，这种分析需要对产品或者系统进行独立的测试，不仅如此，它还需要软件商提供基于功能规范的测试证据、软件商测试结果的核实、功能强度分析、对明显缺陷的弱点搜索。EAL2适用于需要低级或者中级的独立安全保障，但是又没有完整的开发记录的系统，例如遗留系统。

安全保障级别

- EAL3：系统地测试和检查
  - 在这个级别中，安全功能分析和EAL2中完全一样。除了需要和EAL2一样的支持外，EAL3还需要在软件商测试中使用高层设计，并且使用开发环境控制和配置管理。
- EAL4：系统地设计、测试和检查
  - 该等级中增加了低层设计、完整的接口描述和安全功能分析输入的实现的子集。
  - 该等级还需要一个产品或系统的非形式化安全策略模型。
  - EAL4中的其他安全保障措施需要额外的配置管理，包括自动化。
  - 对现存产品系列进行更新，可能得到的最高EAL就是EAL4。EAL4适用于需要中级或者高级独立安全保障的系统。

安全保障级别

- EAL5：半形式化设计和测试
  - 该等级在EAL4的安全功能分析的基础上，增加了完整的输入实现。
  - 这个等级需要有形式化模型、半形式化的功能规范、半形式化的高层设计以及在不同的规范层次之间半形式化的一致性描述等。
  - 产品或者系统的设计必须模块化。
  - 弱点搜索必须能够处理攻击者可能发起的中级攻击，并且必须提供隐信道分析。
  - 配置管理必须全面广泛。
  - EAL5是能够进行严格的由中等数量计算机安全专家支持的商业开发活动的最高EAL等级。
  - EAL5适用于需要有高级独立安全保障的系统。

安全保障级别

- EAL6：半形式化验证的设计和测试
  - 该等级除了要求有与EAL5安全功能分析的输入相同的输入外，还要求有结构化的实现表达。
  - 在半形式化的一致性中，必须包含半形式化的低层设计。设计必须支持分层和模块化。
  - EAL6中的弱点搜索必须能够处理攻击者可能发起的高级攻击，并且必须有系统化的隐信道分析。必须使用结构化的开发过程。
- EAL7：形式化验证的设计和测试
  - 该等级为最高的安全等级，必须形式化地表达功能规范和高层设计，如果适用，还需要有形式化和半形式化的一致性证明。
  - 产品或系统的设计必须简单。安全功能分析要求测试是建立在实现描述的基础上。
  - 开发者的测试结果的独立性确认必须完整。EAL7适用于威胁极高的环境中，需要实质性的安全工程。

保护规范(Protection Profiles，PP)

保护规范(Protection Profiles，PP)

- CC支持两类评估：对保护规范的评估，以及根据安全目标对产品或者系统进行评估。
- CC保护规范(**Protection Profiles，PP**)是一种与实现无关的安全需求集合，用于描述满足特定客户需求的一类产品或者系统。
- PP详细描述一类产品的威胁、环境问题和假设、安全目标以及CC需求。需求包括功能需求和安全保障需求，其中功能需求由PP的开发者从CC功能需求中选择，安全保障需包括7个EAL中的某一个等级的安全保障需求，也可能包括一些附加的安全保障需求。PP的最后一部分提供了基本原理形式的安全保障证据，以显示PP的完整性、一致性和技术合理性。

保护规范(Protection Profiles，PP)

- 简介
- 产品或者系统族的描述
- 产品或者系统族的安全环境
- 安全目标
- 安全需求
- PP应用说明
- 基本原理

保护规范(Protection Profiles，PP)

- 简介
  - PP标识：用于准确地标识、分类、注册以及交叉引用该PP。
  - PP概述：即PP的概要性叙述，可作为分类和注册中的一个独立摘要。
- 产品或者系统族的描述
  - 该部分描述产品或系统的类型信息和一般的IT特征。
  - 如果产品或者系统的主要功能是安全性，那么该部分还将描述产品或者系统的所适用背景。
- 产品或者系统族的安全环境
  - 使用环境以及用途的假设
  - 对要求保护资源的威胁，描述属性包括威胁的动因、攻击类型以及作为攻击目标的资源；
  - 产品或者系统必须遵守的组织安全策略。

保护规范(Protection Profiles，PP)

- 安全目标
  - 产品或者系统的安全目标，必须能追溯到特定的威胁或组织安全策略;
  - 环境的安全目标，必须能追溯到产品或者系统没有完全对抗的各种威胁，以及产品或者系统没有完全碰到的各种组织策略或假设。
- 安全需求
  - 安全功能需求，一般来自CC。如果没有合适的CC需求，PP开发者可以不引而可以附加其他详细的安全功能需求。
  - 安全保障需求，建立在某个EAL之上。PP的开发者可以在EAL的安全保障需求的基础上，新增CC中的其他安全保障需求，或者新增其他明确的安全保障需求。如果适用的话，该需求还需要包含环境方面的安全需求。

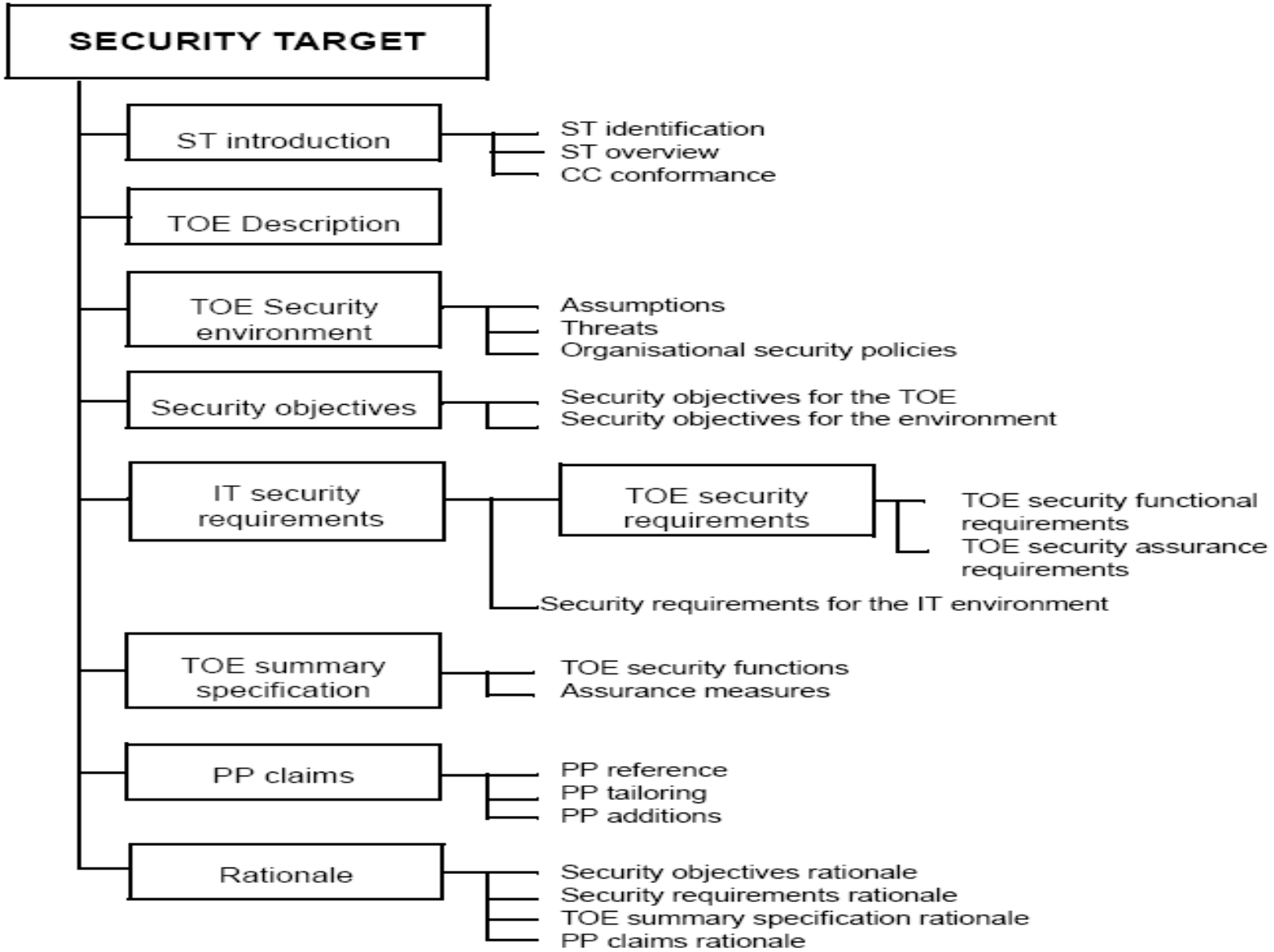
保护规范(Protection Profiles，PP)

- 基本原理
  - 安全目标基本原理，论证了安全目标可追溯到所有的假设、威胁以及组织策略。
  - 安全需求基本原理，论证了产品或者系统的需求、环境的需求可追溯到相应的安全 目标，并且这些需求满足相应的安全目标。

ST — Security Targets

ST — Security Targets

- ST针对一个具体的产品或系统的一组安全需求和规范，用户特定产品的或者系统的评估基础。
- ST是开发者、评估者和用户达成对产品或系统一致认识的基础。
- ST 可供管理、市场、采购、安装、配置、操作和使用人员使用。


SECURITY TARGET
ST introduction
ST identification
ST overview
CC conformance
TOE Description
TOE Security environment
Assumptions
Threats
Organisational security policies
Security objectives
Security objectives for the TOE
Security objectives for the environment
IT security requirements
TOE security requirements
TOE security functional requirements
TOE security assurance requirements
Security requirements for the IT environment
TOE summary specification
TOE security functions
Assurance measures
PP claims
PP reference
PP tailoring
PP additions
Rationale
Security objectives rationale
Security requirements rationale
TOE summary specification rationale
PP claims rationale

ST —— 简介

- ST标识：用于标识该ST和产品的名称和描述性的信息。
- ST概述：ST的概括性叙述，使得产品或系统的潜在用户可以了解该产品或系统是否是他们所需要的。
- CC 的一致性声明：
  - ST与PP的一致性。
  - 第二部分一致性。
  - 第二部分扩展一致性。
  - 第三部分一致性（只用EAL保障性包）。
  - 第三部分增强一致性（EAL保障性包和第三部分的保障性需求）。
  - 第三部分扩展一致性。

ST —— 产品或系统描述

- 产品或系统的描述，帮助用户理解安全需求。
- 产品或系统的物理或逻辑的边界。
- 作为产品或系统的评估的参考依据。
- 产品或系统适应的应用环境。

ST —— 产品或系统安全环境

- 使用环境以及用户的假设
  - 产品或系统的使用方法，财产的价值，使用时的可能受到的限制。
  - 用户、物理方面的因素。
- 对要保护的资源的威胁
  - 包括威胁的动因、攻击的类型、作为攻击目标的资源。
- 产品或系统必须遵守的安全策略
  - 解释产品或系统必须遵守的安全策略，这些策略与安全目标的对应关系。

ST —— 安全目标

- 产品或系统的安全目标
  - 必须能追溯到特定的威胁和组织安全策略。
- 环境安全目标
  - 必须能追溯到产品或系统没有完全对抗的各种威胁。
  - 必须能追溯到产品或系统没有完全碰到的各种组织策略或假设。

ST —— 安全需求

- 安全功能需求
  - 来自CC的安全功能。
  - 新增的安全功能需求。
- 安全保障需求
  - 它建立在EAL的基础上。
  - 在EAL的基础上增加CC中其它安全保障需求。
  - 新增其它的详细的安全保障需求。
  - 需要的环境方面的安全需求。

ST —— 产品或系统的总结性声明

- 安全功能的定义。
- 这些安全功能是如何满足安全功能需求的描述。
- 安全保障措施的定义。
- 这些安全保障措施如何满足安全保障需求的描述。

ST —— PP声明

- 声明产品或系统遵守的一个或多个PP。
- 对每一个声明遵守的PP陈述其解释说明与证明材料。

ST —— 原则和理由

- 安全目标的基本原理：论证安全目标追溯到所有的假设、威胁以及组织策略。
- 安全需求的基本原理：论证产品或系统的需求、环境的需求可以追溯到相应的安全目标，并且这些需求可以满足安全目标。
- 产品或系统的总结性声明的基本原理：展示产品或系统安全功能和安全保障措施是如何满足安全需求的。
- PP声明基本原理：阐述ST的安全目标与安全需求与声明的PP的相关项的区别。