GA

# 中华人民共和国公共安全行业标准

GA/T 390 — 2002

# 计算机信息系统安全等级保护通用技术要求

Common technology requirement

in computer information system classified security protection

2002-07-18 发布　　2002-07-18 实施

中华人民共和国公安部　发布

# 目　　次

# 前　　言

GB17859-1999《计算机信息系统安全保护等级划分准则》作为我国计算机信息系统安全等级管理的重要标准，已于 1999 年 9 月 13 日发布。为促进安全等级管理的工作的正常有序开展，特制定一系列相关的标准，包括：

——计算机信息系统安全等级保护技术要求系列标准；

——计算机信息系统安全等级保护管理要求；

——计算机信息系统安全等级保护工程实施要求；

——计算机信息系统安全等级保护实施管理办法；

——计算机信息系统安全保护等级评测系列标准。

其中，计算机信息系统安全等级保护技术要求系列标准主要包括以下五个标准：

——GA ××1 — ×××× 计算机信息系统安全等级保护通用技术要求；

——GA ××2 — ×××× 计算机信息系统安全等级保护网络技术要求；

——GA ××3 — ×××× 计算机信息系统安全等级保护操作系统技术要求；

——GA ××4 — ×××× 计算机信息系统安全等级保护数据库管理系统技术要求；

——GA ××5 — ×××× 计算机信息系统安全等级保护应用系统技术要求。

《计算机信息系统安全等级保护通用技术要求》作为计算机信息系统安全等级保护技术要求系列标准的基础性标准，详细说明了计算机信息系统为实现 GB17859 所提出的安全等级保护要求应采取的通用的安全技术，以及为确保这些安全技术所实现的安全功能达到其应具有的安全性而采取的保证措施，并将 GB17859 对计算机信息系统五个安全保护等级每一级的要求，从技术要求方面进行详细描述。

本标准为本系列标准中其它标准提供了可供参考和引用的内容。

本标准分由中华人民共和国公安部信息系统安全标准化委员会提出。

本标准分由中华人民共和国公安部信息系统安全标准化委员会归口。

本标准起草单位：江南计算技术研究所。

本标准主要起草人：

# 引　　言

《计算机信息系统安全等级保护通用技术要求》是计算机信息系统安全等级保护技术要求系列标准的基础性标准，用以指导设计者如何设计和实现具有所需要的安全等级的计算机信息系统，主要从对计算机信息系统的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现《计算机信息系统安全保护等级划分准则》中每一个保护等级的安全要求应采取的安全技术措施，以及各安全技术要求在不同安全级中具体实现上的差异。

本标准首先对计算机信息系统安全等级保护所涉及的安全功能技术要求和安全保证技术要求做了比较全面的描述，然后按照GB17859五个安全等级的划分，对每一个安全等级的安全功能技术要求和安全保证技术要求做了详细描述。本标准参考的主要文件是：

——GB17859-1999 计算机信息系统安全保护等级划分准则；

——ISO/IEC 15408：1999 Information technology—Security techniques— Evaluation Criteria for IT Security ，Version 2.0。

# 计算机信息系统安全等级保护通用技术要求

## 1 范围

本标准规定了对计算机信息系统进行安全等级保护所需要的通用技术要求，并给出了每一个安全保护等级的不同技术要求。

本标准适用于按照《计算机信息系统安全保护等级划分准则》（以下简称《准则》）的安全等级保护要求所进行的计算机信息系统的设计和实现，按照《准则》安全等级保护的要求对计算机信息系统进行的测试、管理也可参照使用。

## 2 规范性引用文件

下列文件中的条款通过在本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。

GBJ45-82 高层民用建筑设计防火规定

GB9361-1988 计算机场地安全要求

GB17859—1999 计算机信息系统安全保护等级划分准则

TJ16-74 建筑设计防火规范

## 3 术语和定义

GB17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

**安全要素 security element**

《准则》中，各安全级所包含的安全内容的组成成份。其中有 10 个安全要素。每个安全要素在不同的安全级中可有不同的具体内容。

3.2

**安全功能策略（SFP） security function policy**

为实现安全要素所要求的功能，所采用的安全策略。

3.3

**安全功能 security function**

为实现安全要素的内容，正确实施相应安全功能策略所提供的功能。

3.4

**安全保证 security assurance**

为确保安全要素的安全功能达到要求的安全性目标所采取的方法和措施。

3.5

**可信计算基（TCB） trusted computing base**

计算机信息系统中保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境，并提供一个可信计算系统所要求的附加服务。

3.6

**TCB 安全策略（TSP） TCB security policy**

对 TCB 中的资源进行管理、保护和分配的一组规则。一个 TCB 中可以有一个或多个安全策略。

3.7

**TCB 安全功能（TSF） TCB security function-TSF**

正确实施 TCB 安全策略的全部硬件、固件、软件所提供的功能。每一个安全策略的实现，组成一个安全功能模块。一个 TCB 的所有安全功能模块共同组成该 TCB 的安全功能。

3.8

**TSF 控制范围（TSC） TSF scope of control**

TCB 的操作所涉及的主体和客体。

3.9

**用户标识 user identification**

用来标明用户的身份，确保用户在系统中的唯一性和可辨认性，一般用名称和用户标识符（UID）来标明系统中的一个用户。名称和标识符都是公开的明码信息。标识是有效实施其它安全策略（如：用户数据保护、安全审计等）的基础。通过为用户提供唯一标识，TCB 能使用户对自己的行为负责。

3.10

**用户鉴别 user authentication**

用特定信息对用户身份的真实性进行确认。用于鉴别的信息一般是非公开的、难以仿造的。常用的鉴别信息有：口令（俗称“密码”）信息、生物特征信息、智能 IC 卡信息等。用户鉴别是有效实施其它安全策略（如：用户数据保护、安全审计等）的基础。

3.11

**用户-主体绑定 user- subject binding**

用一定方法将指定用户的安全属性全部或部分地与为其服务的主体（如进程）相关联。

3.12

**主、客体标记 label of subject and object**

为主、客体指定敏感信息（安全属性）。这些标记信息是等级分类和非等级类别的组合，是实施强制访问控制的依据。

3.13

**可信信道 trusted channel**

为了执行关键的安全操作，在 TSF 与其它可信 IT 产品之间建立和维护的保护通信数据免遭修改和泄露的通信路径。

3.14

**可信路径 trusted path**

为实现用户与 TSF 之间的可信通信，在 TSF 与用户之间建立和维护的保护通信数据免遭修改和泄露的通信路径。

3.15

**故障容错 fault tolerance**

通过一系列故障处理措施，确保故障情况下 TCB 所提供的安全功能的有效性和可用性；

3.16

**服务优先级 priority of service**

通过对资源使用的有限控制策略，确保 TCB 中高优先级任务的完成不受低优先级任务的干扰和延误，从而确保 TCB 安全功能的安全性；

3.17

**资源分配 resource allocation**

通过对 TCB 安全功能控制范围内资源的合理管理和调度，确保 TCB 的安全功能不因资源使用方面的原因而受到影响。

3.18

**配置管理（CM） configuration management**

一种建立功能要求和规范的方法。该功能要求和规范是在 TCB 的执行中实现的。

3.19

**配置管理系统（CMS） configuration management system**

通过提供追踪任何变化，以及确保所有修改都已授权的方法，确保 TCB 各部分的完整性。

3.20

**保护框架（PP） protection profile**

详细说明计算机信息系统安全保护需求的文档，即通常的安全需求，一般由用户负责编写。

3.21

**安全目标（ST） security target**

阐述计算机信息系统安全功能及信任度的文档，即通常的安全方案，一般由开发者编写。

3.22

**TCB 安全管理 security management**

是指对与TCB安全相关方面的管理,包括对不同的管理角色和它们之间的相互作用(如能力的分离)进行规定,对分散在多个物理上分离的部件有关安全属性的传播、TSF 数据和功能的修改等问题的处理。

## 4 安全功能技术要求

### 4.1 物理安全

#### 4.1.1 环境安全

##### 4.1.1.1 中心机房的安全保护

###### 4.1.1.1.1 机房场地选择

a） 基本要求

——按一般建筑物的要求进行机房场地选择。

b） 较高要求

——避开易发生火灾和危险程度高的地区，如油库、和其它易燃物附近的区域；

——避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域；

——避开低洼、潮湿及落雷区域；

——避开强震动源和强噪声源区域；

——避开强电场和强磁场区域；

——避开有地震、水灾危害的区域；

——避免在建筑物的高层以及用水设备的下层或隔壁。

c） 严格要求

——避开易发生火灾和危险程度高的地区，如油库、和其它易燃物附近的区域；

——避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域；

——避开低洼、潮湿及落雷区域；

——避开强震动源和强噪声源区域；

——避开强电场和强磁场区域；

——避开有地震、水灾危害的区域；

——避免在建筑物的高层以及用水设备的下层或隔壁；

——避免靠近公共区域，如运输邮件通道、停车场或餐厅等。

#### 4.1.1.1.2 机房内部安全防护

a） 基本要求

——机房出入口应有专人负责，未经允许的人员不准进入机房；

——没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，磁铁、私人电子计算机或电设备、食品及饮料、香烟、吸烟用具等均不准带入机房。

b） 较高要求

——机房应只设一个出入口，另设若干紧急疏散出口，标明疏散线路和方向，并应有专人负责，未经允许的人员不准进入机房；

——可派专门的警卫人员对出入机房的人员进行管理，没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房；磁铁、私人电子计算机或电子设备、食品及饮料、香烟、吸烟用具等均不准带入机房；

——获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同；

——在机房中设有信息系统安全管理中心的，更应加强其安全防护，如进入不同区域时佩带有不同标记的证章、重要部位的出、入口设置电子锁、指纹锁等。

c） 严格要求

——机房应只设一个出入口，另设若干紧急疏散出口，标明疏散线路和方向，并应有专人负责，未经允许的人员不准进入机房；

——可派专门的警卫人员对出入机房的人员进行管理，没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房；磁铁、私人电子计算机或电子设备、食品及饮料、香烟、吸烟用具等均不准带入机房；

——机房内部应分区管理，一般分为主机区、数据处理操作区、辅助区等，应根据每个工作人员的实际工作需要，确定其能进入的区域；获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同；

——在机房中设有信息系统安全管理中心的，更应加强其安全防护，如进入不同区域时佩带有不同标记的证章、重要部位的出入、口设置电子锁、指纹锁等，必要时可设置摄像监视系统。

#### 4.1.1.1.3 机房防火

a） 基本要求

——建筑材料防火，要求机房和记录介质存放间，其建筑材料的耐火等级，应符合 TJ16 中规定的二级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16 中规定的三级耐火等级；

——区域隔离防火，要求机房布局要将脆弱区和危险区进行隔离，防止外部火灾进入机房，特别是重要设备地区，安装防火门、使用阻燃材料装修等；

——报警和灭火系统，要求设置火灾报警系统，由人来操作灭火设备，并对灭火设备的效率、毒性、用量和损害性有一定的要求。

b） 较高要求

——建筑材料防火，要求机房和重要的记录介质存放间，其建筑材料的耐火等级，应符合GBJ45 中规定的二级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16 中规定的二级耐火等级；

——区域隔离防火，要求机房布局要将脆弱区和危险区用防火墙进行隔离，防止外部火灾进入机房，特别是重要设备地区，安装防火门、使用阻燃材料装修等；

——报警和灭火系统，要求设置火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等，能对火灾放生的部位以声、光或电的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。

c） 严格要求

——建筑材料防火，要求机房和重要的记录介质存放间，其建筑材料的耐火等级，应符合GBJ45 中规定的一级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16 中规定的二级耐火等级；

——区域隔离防火，要求机房布局要将脆弱区和危险区用防火墙进行隔离，防止外部火灾进入机房，特别是重要设备地区，安装防火门、使用阻燃材料装修等；

——报警和灭火系统，要求设置火灾自动消防系统，能自动检测火情、自动报警，并自动却段电源和其他应急开关，自动启动事先固定安装好的灭火设备进行自动灭火。

#### 4.1.1.1.4 机房供、配电

a） 基本要求

——机房供电系统应将动力、照明用电与计算机系统供电线路分开，并配备应急照明装置；

——建立备用的供电系统，以备常用供电系统停电时启用。

b） 较高要求

——机房供电系统应将动力、照明用电与计算机系统供电线路分开，并配备应急照明装置；

——建立备用的供电系统，以备常用供电系统停电时启用；

——采用线路稳压器，防止电压波动对计算机系统的影响；

——采用有效措施，减少机房中电器噪声干扰，保证计算机系统正常运行；

——防止电源线干扰，包括中断供电、异常状态供电（指连续电压过载或过低）、电压瞬变、噪声（电磁干扰）以及由于核爆炸或雷击等引起的设备突然失效事件；

——设置电源保护装置，如金属氧化物可变电阻、硅雪崩二极管、气体放电管、滤波器、电压调整变压器、不间断电源（UPS）、避雷针和浪涌滤波器等。

c） 严格要求

——机房供电系统应将动力、照明用电与计算机系统供电线路分开，并配备应急照明装置；

——建立备用的供电系统，以备常用供电系统停电时启用；

——采用不间断供电电源，防止电压波动、电器干扰、断电等对计算机系统的影响；

——采用有效措施，减少机房中电器噪声干扰，保证计算机系统正常运行；

——防止电源线干扰，包括中断供电、异常状态供电（指连续电压过载或低电压）、电压瞬变、噪声（电磁干扰）以及由于核爆炸或雷击等引起的设备突然失效事件；

——设置电源保护装置，如金属氧化物可变电阻、硅雪崩二极管、气体放电管、滤波器、电压调整变压器、、避雷针和浪涌滤波器等；

——提供紧急情况供电，配置抵抗电压不足的设备，包括基本的 UPS、改进的 UPS、多级 UPS

和应急电源（发电机组）等。

#### 4.1.1.1.5 机房空调、降温

a） 基本要求

——应有必要的空调设备，使机房温度达到所需的基本要求。

b） 较高要求

——应有较完备的中央空调系统，保证机房温度的变化在计算机运行所允许的范围。

c） 严格要求

——应有完备的中央空调系统，保证机房各个区域的温度变化能满足计算机运行、人员活动和其它辅助设备的要求。

#### 4.1.1.1.6 机房防水与防潮

a） 基本要求

——水管安装，不得穿过屋顶和活动地板下，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；计算机设备应放在工作台上，并备有防水罩；

——对工作人员进行防水害教育，了解机房进水管关闭阀的准确位置，做到人人会用；

——采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。

b） 较高要求

——水管安装，不得穿过屋顶和活动地板下，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；

——对工作人员进行防水害教育，了解机房进水管关闭阀的准确位置，做到人人会用；

——采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透；

——安装对水敏感的检测仪表或元件，对机房进行防水检测、报警。

c） 严格要求

——水管安装，不得穿过屋顶和活动地板下，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施；

——对工作人员进行防水害教育，了解机房进水管关闭阀的准确位置，做到人人会用；

——采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透；

——安装对水敏感的检测仪表或元件，对机房进行防水检测、报警；

——机房应设有排水口，并购置水泵，以便迅速排出积水。

#### 4.1.1.1.7 机房防静电

a） 基本要求

——采用接地与屏蔽措施，使计算机系统有一套合理的接地与屏蔽系统；

——人员服装采用不易产生静电的衣料，工作鞋选用低阻值材料制作；

——控制机房温湿度，使其保持在不易产生静电的范围内。

b） 较高要求

——应采用接地与屏蔽措施，使计算机系统有一套合理的接地与屏蔽系统；

——人员服装采用不易产生静电的衣料，工作鞋选用低阻值材料制作；

——控制机房温湿度，使其保持在不易产生静电的范围内；

——机房地板从地板表面到接地系统的阻值，应保证防人身触电和产生静电；

——机房中使用的各种家具，工作台、柜等，应选择产生静电小的材料。

c） 严格要求

——应采用接地与屏蔽措施，使计算机系统有一套合理的接地与屏蔽系统；

——人员服装采用不易产生静电的衣料，工作鞋选用低阻值材料制作；

——控制机房温湿度，使其保持在不易产生静电的范围内；

——机房地板从地板表面到接地系统的阻值，应保证防人身触电和产生静电；

——机房中使用的各种家具，工作台、柜等，应选择产生静电小的材料；

——在硬件维修时，应采用金属板台面的专用维修台，以保护 MOS 电路；

——在机房中使用静电消除剂和静电消除器等，以进一步减少静电的产生。

#### 4.1.1.1.8 机房接地与防雷击

a） 基本要求

——应采用地桩、水平栅网、金属板、建筑物基础钢筋等构建接地系统，确保接地体良好的接地；

——设置信号地与直流电源地，应注意不造成额外耦合，保障去耦、滤波等的良好效果；

——设置避雷地，应以深埋地下、与大地良好相通的金属板作为接地点，至避雷针的引线则应采用粗大的紫铜条，或者使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连。

b） 较高要求

——应采用地桩、水平栅网、金属板、建筑物基础钢筋等构建接地系统，确保接地体良好的接地；

——设置信号地与直流电源地，应注意不造成额外耦合，保障去耦、滤波等的良好效果；

——设置避雷地，应以深埋地下、与大地良好相通的金属板作为接地点，至避雷针的引线则应采用粗大的紫铜条，或者使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连；

——设置安全防护地与屏蔽地，应采用阻抗尽可能小的良导体的粗线，以减小各种地之间的电位差；应采用焊接方法，并经常检查接地的良好，检测接地电阻，确保人身、设备和运行的安全。

c）严格要求

——应采用地桩、水平栅网、金属板、建筑物基础钢筋构建接地系统等，确保接地体良好的接地；

——设置信号地与直流电源地，应注意不造成额外耦合，保障去耦、滤波等的良好效果；

——设置避雷地，应以深埋地下、与大地良好相通的金属板作为接地点，至避雷针的引线则应采用粗大的紫铜条，或者使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连；

——设置安全防护地与屏蔽地，应采用阻抗尽可能小的良导体的粗线，以减小各种地之间的电位差，应采用焊接方法，并经常检查接地的良好，检测接地电阻，确保人身、设备和运行的安全；

——设置交流电源地线，交流供电线应有规范连接位置的三芯线，即相线、中线和地线，并将该“地线”连通机房的地线网，以确保其安全保护作用。

#### 4.1.1.1.9 机房电磁防护

a） 基本要求

——应采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；

——应采用屏蔽方法，对信号线、电源线进行电屏蔽，减少外部电器设备对计算机的瞬间干扰；

——应采用距离防护的方法，将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。

b） 较高要求

——应采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；

——应采用屏蔽方法，对信号线、电源线进行电屏蔽，减少外部电器设备对计算机的瞬间干扰；

——应采用距离防护的方法，将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方；

——应采用低辐射材料和设备，防止电磁发射泄露；

——应采用屏蔽方法，对重要设备进行电磁屏蔽，削弱外部电磁场对计算机设备的干扰，防止电磁信号的泄露；

——对磁带、磁盘等磁记录介质的保管存放，应注意电磁感应的影响，如使用铁制柜存放。

c） 严格要求

——应采用接地的方法防止外界电磁干扰和设备寄生耦合干扰；

——应采用屏蔽方法，对信号线、电源线进行电屏蔽，减少外部电器设备对计算机的瞬间干扰；

——应采用距离防护的方法，将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方；

——应采用低辐射材料和设备，防止电磁发射泄露；

——应采用屏蔽方法，对计算机机房进行电磁屏蔽，防止外部电磁场对计算机设备的干扰，防止电磁信号的泄露；

——对磁带、磁盘等磁介质设备的保管存放，应注意电磁感应的影响，如使用铁制柜存放。

### 4.1.1.2 通信线路的安全防护

a）基本要求

——应采取一定措施，预防线路截获，使线路截获设备难以工作；

——应有探测线路截获装置，及时发现线路截获事件并报警。

b）较高要求

——应采取有效措施，预防线路截获，使线路截获设备无法工作；

——应有探测线路截获装置，及时发现线路截获的事件并报警；

——应有定位线路截获装置，能发现线路截获窃取设备的准确位置。

c）严格要求

——应采取有效措施，预防线路截获，使线路截获设备无法工作；

——应有探测线路截装置，及时发现线路截获的事件并报警；

——应有定位线路截获装置，能发现线路截获窃取设备的准确位置；

——应有对抗线路截获装置，能阻止线路截获窃取设备的有效使用。

#### 4.1.2 设备安全

##### 4.1.2.1 设备的防盗和防毁

a） 基本要求

——计算机系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物；

——计算中心应安装防盗报警装置，防止夜间从门窗进入的盗窃行为。

b） 较高要求

——计算机系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物；

——计算中心应利用光、电、无源红外等技术设置机房报警系统，并有专人值守，防止夜间从门窗进入的盗窃行为；

——机房外部的网络设备，应采取加固防护等措施，以防止盗窃和破坏。

c） 严格要求

——计算机系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物；

——应利用闭路电视系统对计算机中心的各重要部位进行监视，并有专人值守，防止夜间从门窗进入的盗窃行为；

——机房外部的网络设备，应采取加固防护等措施，必要时安排专人看管，以防止盗窃和破坏。

##### 4.1.2.2 设备的安全可用

a） 基本要求

——支持计算机信息系统运行的所有设备，包括计算机主机、外部设备、网络设备及其它辅助设备等均应安全可用；

——应提供基本的运行支持，并有一定的故障恢复能力。

b） 较高要求

——支持计算机信息系统运行的所有设备，包括计算机主机、外部设备、网络设备及其它辅助设备等均应安全可用；

——应提供可靠的运行支持，并有一定的故障容错和故障恢复能力。

c） 严格要求

——支持计算机信息系统运行的所有设备，包括计算机主机、外部设备、网络设备及其它辅助设备等均应安全可用；

——应提供可靠的运行支持，并通过故障容错和故障恢复等措施，支持计算机信息系统实现不间断运行。

#### 4.1.3 记录介质安全

a） 基本要求

——存放有用数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取一定措施防止被盗、被毁和受损；

——应该删除和销毁的有用数据，应有一定措施，防止被非法拷贝。

b） 较高要求

——存放有用数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取一定措施防止被盗、被毁和受损；

——存放重要数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取有效措施，如建立介质库等，防止被盗、被毁和受损；

——系统中有很高使用价值或很高机密程度的重要数据，应采用加密等方法进行保护；
——应该删除和销毁的有用数据，应有一定措施，防止被非法拷贝；
——应该删除和销毁的重要数据，应采取有效措施，防止被非法拷贝；
——重要数据的销毁和处理，要有严格的管理和审批手续。

c） 严格要求
——存放有用数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取一定措施防止被盗、被毁和受损；
——存放重要数据和关键数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取有效措施，如建立介质库、异地存放等，防止被盗、被毁和发霉变质；
——系统中有很高使用价值或很高机密程度的重要数据，或者对系统运行和应用来说起关键作用的数据，应采用加密等方法进行保护；
——应该删除和销毁的有用数据，应有一定措施，防止被非法拷贝；
——应该删除和销毁的重要数据和关键数据，应采取有效措施，防止被非法拷贝；
——重要数据的销毁和处理，要有严格的管理和审批手续，而对于关键数据则应长期保存。

#### 4.1.4 安全管理中心安全

安全管理中心的物理安全应满足以下要求：

a） 管理中心设置在中心机房，以各种方式与计算机信息系统的各类安全机制相连接；

b） 除了按照一般的机房建设要求进行设计外，还应设置一些关卡，比如，严格的门卫制度和人员管理，必要时可安装闭路摄像监视系统。

### 4.2 运行安全

#### 4.2.1 风险分析

风险分析应按以下要求进行：

a） 以系统安全运行和信息安全保护为出发点，全面分析由于物理的、系统的、管理的、人为的和自　然的原因所造成的安全风险；

b） 通过对影响计算机信息系统安全运行的诸多因素的了解和分析，明确系统存在的风险，找出克服 这些风险的办法；

c） 对常见的风险（如：后门/陷阱门、拒绝使用、辐射、盗用、伪造、假冒、逻辑炸弹、破坏活动、超级处理、偷窃行为、搭线窃听以及计算机病毒等）进行分析，确定每类风险的程度；

d) 系统设计前和运行前应进行静态风险分析，以发现系统的潜在安全隐患；

e) 系统运行过程中应进行动态风险分析，测试、跟踪并记录其活动，以发现系统运行期的安全漏洞；

f) 系统运行后应进行综合性风险分析，并提供相应的系统脆弱性分析报告；

g) 采用风险分析工具，通过收集数据、分析数据、输出数据，确定危险的严重性等级，分析危险的可能性等方法进行风险分析，以便确定安全对策。

#### 4.2.2 系统安全性检测分析

计算机信息系统安全性检测分析应从以下方面进行：

a） 操作系统安全性检测分析，应从操作系统的角度，以管理员身份评估文件许可、文件宿主、网络服务设置、账户设置、程序真实性以及一般的与用户相关的安全点、入侵迹象等，从而检测和分析操作系统的安全性，发现存在的安全隐患。

b） 数据库管理系统安全性检测分析，应对支持计算机信息系统运行的数据库管理系统进行安全

性检测分析，要求通过扫描数据库系统中与鉴别、授权、访问控制和系统完整性设置相关的数据库管理系统特定的安全脆弱性，分析其存在的缺点和漏洞，提出补救措施。

c） 网络安全性检测分析，应采用侵袭模拟器，通过在网络设备的关键部位，用模拟侵袭的方法，自动扫描、检查并报告网络系统中存在的缺点和漏洞，提出补救措施，达到增强网络安全性的目的。

d） 防火墙安全性检测分析，应通过反复高速地逐个对防火墙和宿主系统上的数百个与安全性相关的因素进行测试，对其安全性进行检测分析，寻找其安全漏洞。

e） 电磁泄露检测分析，应对运行中的计算机信息系统环境进行电磁泄露检测，要求采用专门的检测设备，检查系统运行过程中由于电磁干扰和电磁辐射对计算机信息系统的安全性所造成的威胁，并提出补救措施。

#### 4.2.3 网络安全监控

网络安全监控应采用以下方法：

a) 设置分布式探测器实时监听网络数据流，监视和记录内、外部用户出入网络的相关操作，在发现违规模式和未授权访问时，报告网络安全监控中心。

b) 设置安全监控中心，对收到的来自分布式探测器的信息，根据安全策略进行分析，并作审计、报告、事件记录和报警等处理。监控中心应具有一定的远程管理功能，如对探测器实现远程参数设置、远程数据下载、远程启动等操作。安全监控中心还应具有实时响应功能，包括攻击分析和响应、误操作分析和响应、漏洞分析和响应以及漏洞形势分析和响应。

#### 4.2.4 安全审计

##### 4.2.4.1 安全审计的自动响应

安全审计 TSF 应按以下要求响应审计事件：

a） 实时报警的生成，当检测到可能有安全侵害事件时，生成实时报警信息；

b） 违例进程的终止，当检测到可能有安全侵害事件时，将违例进程终止；

c） 服务的取消，当检测到可能有安全侵害事件时，取消当前的服务；

d） 用户账号的断开与失效，当检测到可能有安全侵害事件时，将当前的用户账号断开，并使其失效。

##### 4.2.4.2 安全审计数据产生

安全审计 TSF 应按以下要求产生审计数据：

a） 为下述可审计事件产生审计记录：

——审计功能的启动和关闭；

——使用身份鉴别机制；

——将客体引入用户地址空间（例如：打开文件、程序初始化）；

——删除客体；

——系统管理员、系统安全员、审计员和一般操作员所实施的操作；

——其他与系统安全有关的事件或专门定义的可审计事件。

b） 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。

c） 对于身份鉴别事件，审计记录应包含请求的来源（例如：终端标识符）。

d） 对于客体被引入用户地址空间的事件及删除客体事件，审计记录应包含客体名及客体的安全级别。

e） 将每个可审计事件与引起该事件的用户相关联。

#### 4.2.4.3 安全审计分析

安全审计分析应包括：

a） 潜在侵害分析，应能用一系列规则去监控审计事件，并根据这些规则指出 TSP 的潜在侵害。这些规则包括：

——由已定义的可审计事件的子集所指示的潜在安全攻击的积累或组合；

——任何其它的规则。

b） 基于异常检测的描述，应维护用户所具有的质疑等级——历史使用情况，以表明该用户的现行活动与已建立的使用模式的一致性程度。当用户的质疑等级超过门限条件时，TSF 应能指出将要发生对安全性的威胁。

c） 简单攻击探测，应能检测到对 TSF 实施有重大威胁的签名事件的出现。为此，TSF 应维护指出对 TSF 侵害的签名事件的内部表示，并将检测到的系统行为记录与签名事件进行比较，当发现两者匹配时，指出一个对 TSF 的攻击即将到来。

d） 复杂攻击探测，在上述简单攻击探测的基础上，要求 TSF 应能检测到多步入侵情况，并能根据已知的事件序列模拟出完整的入侵情况，还应指出发现对 TSF 的潜在侵害的签名事件或事件序列的时间。

#### 4.2.4.4 安全审计查阅

安全审计查阅工具应具有：

a） 审计查阅，提供从审计记录中读取信息的能力，即要求 TSF 为授权用户提供获得和解释审计信息的能力。当用户是人时，必须以人类可懂的方式表示信息；当用户是外部 IT 实体时，必须以电子方式无歧义地表示审计信息。

b） 有限审计查阅，在上述审计查阅的基础上，审计查阅工具应禁止具有读访问权限以外的用户读取审计信息。

c） 可选审计查阅，在上述有限审计查阅的基础上，审计查阅工具应具有根据准则来选择要查阅的审计数据的功能，并根据某种逻辑关系的标准提供对审计数据进行搜索、分类、排序的能力。

#### 4.2.4.5 安全审计事件选择

应根据以下属性选择可审计事件：

a） 客体身份、用户身份、主体身份、主机身份、事件类型；

b） 作为审计选择性依据的附加属性。

#### 4.2.4.6 安全审计事件存储

应具有以下创建并维护安全的审计踪迹记录的能力：

a） 受保护的审计踪迹存储，要求审计踪迹的存储受到应有的保护，能检测或防止对审计记录的修改。

b） 审计数据的可用性确保，要求在意外情况出现时，能检测或防止对审计记录的修改，以及在发生审计存储已满、存储失败或存储受到攻击时，确保审计记录不被破坏。

c） 审计数据可能丢失情况下的措施，要求当审计跟踪超过预定的门限时，应采取相应的措施，进行审计数据可能丢失情况的处理。

d） 防止审计数据丢失，要求在审计踪迹存储记满时，应采取相应的防止审计数据丢失的措施，可选择“忽略可审计事件”、“阻止除具有特殊权限外的其他用户产生可审计事件”、“覆

盖已存储的最老的审计记录”和“一旦审计存储失败所采取的其它行动”等措施，防止审计数据丢失。

#### 4.2.4.7 网络环境安全审计与评估

在网络环境运行的计算机信息系统，TSF 应采用以下措施进行安全审计与评估：

a) 建立由安全审计中心（安全审计服务器）和分布在网络各个运行节点的审计代理程序组成的分布式安全审计系统，实现网络环境计算机信息系统安全审计与评估；
b) 安全审计代理程序为安全审计服务器提供审计数据；
c) 安全审计服务器实时收集各安全代理程序的审计信息，并进行记录分析与保存；
d) 设置跨平台的安全审计机制，对安全事件快速进行评估并作出响应，向管理人员提供各种能反映系统使用情况、出现的可疑迹象、运行中发生的问题等有价值的统计和分析信息；
e) 运用统计方法学和审计评估机制，给出智能化审计报告及趋向报告，达到综合评估系统安全现状的目的。

### 4.2.5 网络防病毒

计算机信息系统应采用以下病毒防治措施：

a） 严格管理，严格控制各种外来介质的使用，必须先杀毒，后使用；
b） 防杀结合，要求在所有病毒可能入侵的网络连接部位设置病毒扫描工具，拦截并杀除企图进入系统的病毒；
c） 整体防御，应设置病毒管理中心，通过对全系统的服务器、工作站和客户机，进行病毒防治的统一管理，注意新病毒和杀病毒软件的升级换代；扫描、检查病毒感染情况，并设置在线报警功能，一旦发现病毒，可由管理人员从管理中心予以解决；
d） 防管结合，应将防病毒与网络管理相结合，在网管所涉及的重要部位设置防病毒软件，在所有病毒能够进入的地方都采取相应的防范措施，防止病毒侵袭；
e） 多层防御，应采用实时扫描、完整性保护和完整性检验等不同层次的技术，将病毒检测、多层数据保护和集中式管理功能集成起来，提供全面的病毒防护功能，检测、发现和消除病毒，阻止病毒的扩散和传播。

### 4.2.6 备份与故障恢复

#### 4.2.6.1 备份

为了实现确定的恢复功能，必须在系统正常运行时定期地或按照某种条件实施相应的的备份。根据不同的恢复要求，应有以下形式的备份：

a） 用户自我信息备份，由用户自身有选择地备份重要信息；
b） 增量信息备份，由系统定时对新增信息进行备份；
c） 局部系统备份，对某些重要的局部系统进行定期备份；
d） 热备份，对系统的重要设备进行冗余设置，并在必要时能立即投入使用；
e） 全系统备份，定期对全系统的运行现场进行备份；
f） 主机系统远地备份，对于重要的计算机信息系统，设置主机系统的远地备份，以备主机系统不能正常运行时能在较短时间内启动，替代主机系统工作。

#### 4.2.6.2 故障恢复

应在上述备份功能的基础上提供过程和机制，确保在确定不减弱保护的情况下启动 TCB，并在运行中断后能在不减弱保护的情况下恢复计算机信息系统的运行。故障恢复包括：

a） 手动恢复，TCB 只提供以人工干预的方法使计算机信息系统返回到安全状态的机制。该机制

在计算机信息系统发生失败或服务中断后，使 TSF 进入维护方式，并提供以手工方法将 TCB 返回到一个保护状态的能力。

b） 自动恢复，应对至少一种类型的服务中断，在无人工干预的情况下能使计算机信息系统恢复到安全状态，对其它的服务中断可由手动恢复实现。

c） 无过分丢失的自动恢复，在进行自动恢复时，应确保在 TSC 内的 TSF 数据或客体无超过限定量的丢失。

d） 灾难性恢复，当发生地震、水灾、火灾等不可抗拒的自然灾害或由于人为原因造成系统灾难性故障时，能通过启动远地备份系统的主机系统，使计算机信息系统继续正常运行，提供不间断服务。

#### 4.2.7 计算机信息系统的应急计划和应急反应

在应急情况作出反应的应急计划应：

a） 具有各种安全措施，包括在出现各种安全事件时应采取的措施，这些措施是管理手段与技术手段的结合；

b） 设置正常备份机制，在系统正常运行时就通过各种备份措施为灾害和故障做准备；

c） 健全安全管理机构，建立健全的安全事件管理机构，明确人员的分工和责任；

d） 建立处理流程图，制定安全事件响应与处理计划及事件处理过程示意图，以便迅速恢复被安全事件破坏的系统。

### 4.3 信息安全

#### 4.3.1 标识和鉴别

##### 4.3.1.1 数据鉴别

要求 TSF 能提供一种鉴别信息真实性的方法（如数字签名），用这种方法，可以保证特定数据单元的有效性，进而可用其验证信息内容没有被伪造或篡改。数据鉴别包括：

a） 基本数据鉴别，要求 TSF 应具有保证客体信息内容真实性的能力。TSF 能提供确保客体表或信息类型表有效性的能力；TSF 能提供一个主体表，该主体表能对验证指定信息的有效性提供证据。

b） 伴有保证者身份的数据鉴别，要求 TSF 除具有基本数据鉴别功能外，还应具有确保主体身份真实性的能力。

##### 4.3.1.2 用户标识

a） 同步标识，应允许用户在被 TSF 标识之前，实施一定的动作，这些动作用来确定标识自己的条件（如生成标识符或在登录过程中请求输入需要的信息等），并要求 TSF 在允许任何以该用户的名义实施由其它 TSF 促成的动作之前，都要成功地标识该用户。

b） 动作前标识，TSF 应在允许任何代表该用户的其它 TSF 促成的动作之前，要求该用户应成功地标识自己。

##### 4.3.1.3 标识用户的身份鉴别

a） 同步鉴别，要求 TSF 应允许用户在被鉴别之前以该用户名义实施由 TSF 促成的某些动作。这些动作用来确定鉴别自己的条件（如生成口令或在登录过程中请求输入需要的信息等），并要求 TSF 在允许任何以该用户名义实施由其它 TSF 促成的动作之前，应成功地鉴别该用户。

b） 动作前鉴别，TSF 应在允许任何代表该用户的其它 TSF 促成的动作之前，要求对该用户的身份进行成功的鉴别。

c） 不可伪造鉴别，应检测并防止使用伪造或复制的鉴别数据。一方面，要求 TSF 应检测或防止由任何别的用户伪造的鉴别数据，另一方面，要求 TSF 应检测或防止当前用户从任何其它用户处复制的鉴别数据的使用。

d） 一次性使用鉴别，应能提供一次性使用鉴别数据操作的鉴别机制，即 TSF 应防止与已标识过的鉴别机制有关的鉴别数据的重用。

e） 多机制鉴别，应能提供不同的鉴别机制，用于鉴别特定事件的用户身份，并且 TSF 应根据所描述多种鉴别机制如何提供鉴别的规则，来鉴别任何用户所声称的身份。

f） 重新鉴别，应有能力规定需要重新鉴别用户的事件，即 TSF 应在需要重鉴别的条件表所指示的条件下，重新鉴别用户。例如，用户终端操作超时被断开后，重新连接时需要进行重鉴别。

g） 受保护的鉴别反馈，要求 TSF 在鉴别期间只有有限的反馈信息提供给用户，即当进行鉴别时，TSF 仅仅将反馈表提供给用户。

#### 4.3.1.4 鉴别失败处理

要求 TSF 为不成功的鉴别尝试次数（包括尝试数目和时间的阈值）定义一个值，以及明确规定达到该值时所应采取的动作。鉴别失败的处理应包括检测出现相关的不成功鉴别尝试的次数与所规定的数目相同的情况，并进行预先定义的处理。

#### 4.3.1.5 用户-主体绑定

在 TCB 安全功能控制范围之内，对一个已标识和鉴别的用户，为了要求 TSF 完成某个任务，需要激活另一个主体（如进程），这时，要求通过用户-主体绑定将该用户与该主体相关联，从而将用户的身份与该用户的所有可审计行为相关联。

### 4.3.2 信息交换的安全鉴别

#### 4.3.2.1 原发抗抵赖

应确保信息的发送者不能成功地否认曾经发送过该信息。这就要求 TSF 提供一种方法，来确保接收信息的主体在数据交换期间能获得证明信息原发的证据，而且该证据可由该主体或第三方主体验证。

原发抗抵赖分为：

a） 选择性原发证明，要求 TSF 具有为主体提供请求原发证据信息的能力。即 TSF 在接到原发者或接收者的请求时，能就传输的信息产生原发证据，证明该信息的发送由该原发者所为。

b） 强制性原发证明，要求 TSF 在任何时候都能对传输的信息产生原发证据。即 TSF 在任何时候都能就传输的信息强制产生原发证据，证明该信息的发送由该原发者所为。

#### 4.3.2.2 接收抗抵赖

应确保信息的接收者不能成功地否认对该信息的接收。这就要求 TSF 提供一种方法，来确保发送信息的主体在数据交换期间能获得证明该信息被接收的证据，而且该证据可由该主体或第三方主体验证。

接收抗抵赖分为：

a） 选择性接收证明，要求 TSF 具有为主体提供请求信息接收证据的能力。即 TSF 在接到原发者或接收者的请求时，能就接收到的信息产生接收证据，证明该信息的接收由该接收者所为。

b） 强制性接收证明，要求 TSF 总是对收到的信息产生接收证据。即 TSF 能在任何时候对收到的信息强制产生接收证据，证明该信息的接收由该接收者所为。

#### 4.3.3 隐密

##### 4.3.3.1 匿名

要求 TSF 应确保用户和/或主体集，不能确定与主体和/或操作和/或客体列表相关联的实际用户，并且要求 TSF 在对主体提供服务时，在对用户身份进行真实性鉴别的前提下不询问实际的用户名。

##### 4.3.3.2 假名

要求 TSF 应确保用户在使用资源或设备时，不暴露其真实名称，但仍能对该次使用负责，TSF 应确保用户和/或主体集，在对用户身份进行真实性鉴别时，不能确定与主体和/或操作和/或客体列表相关联的真实的用户名。

##### 4.3.3.3 不可关联性

一个用户可以多次使用资源和服务，但任何人都不能将这些使用联系在一起，要求 TSF 应确保用户和/主体不能确定系统中的某些操作是否由同一用户引起。

##### 4.3.3.4 不可观察性

用户在使用资源和服务时，其它人，特别是第三方不能观察到该资源和服务正在被使用，要求 TSF 应确保用户和/或主体，不能观察到由受保护的用户和/或主体对客体所进行的操作，还要求 TCB 为授权用户提供可观察性，即向授权用户提供观察资源和/或服务列表使用情况的能力。

#### 4.3.4 标记

##### 4.3.4.1 用户属性定义

要求TSF应对用户进行标记，即为用户指定安全属性。

##### 4.3.4.2 客体属性定义

要求TSF应对客体进行标记，即为客体指定安全属性。

#### 4.3.5 自主访问控制

##### 4.3.5.1 访问控制策略

要求 TSF 应按确定的自主访问控制安全策略进行设计，并按需要确定访问控制策略的控制范围，包括策略控制下的主体、客体，及由策略覆盖的被控制的主体与客体间的操作。可以有多个访问控制安全策略，但它们必须独立命名，且不能相互冲突。常用的自主访问控制策略为访问控制表访问控制，包括：目录表访问控制、存取控制表访问控制、访问控制矩阵访问控制、能力表访问控制等。

按访问控制的覆盖范围，自主访问控制策略分为：

a） 子集访问控制，要求 TSF 的每个确定的自主访问控制，TSF 应对其所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略。

b） 完全访问控制，要求 TSF 的每个确定的自主访问控制，TSF 应对其所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略。并要求 TSF 应确保 TSC 内的任意一个主体和任意一个客体之间的所有操作将至少被一个确定的访问控制 SFP 覆盖。

##### 4.3.5.2 访问控制功能

对于自主访问控制，要求 TSF 应明确指出采用一条命名的访问控制策略所实现的特定功能，说明策略的使用和特征，以及该策略的控制范围。与自主访问控制策略相对应，自主访问控制功能分为：

a） 子集访问控制，由相应子集访问控制策略实现的访问控制功能，实现对 TSF 所覆盖的主体、客体及其之间的操作的访问控制。

b） 完全访问控制，由相应的完全访问控制策略实现的访问控制功能，实现对 TSC 内的任意一个主体和任意一个客体之间的所有操作的访问控制的覆盖。

无论子集访问控制还是完全访问控制，TSF 应有能力提供：

——将在安全属性或命名的安全属性组的客体上，执行访问控制 SFP；

——将使用在受控客体上的受控操作所管理的受控主体和受控客体之间的访问规则，来决定受控主体与受控客体之间的操作是否被允许；

——将在基于安全属性的授权主体访问客体的附加规则的基础上，授权主体访问客体；

——将基于安全属性的拒绝主体对客体访问的规则，实现拒绝主体对客体的访问。

#### 4.3.6 强制访问控制

##### 4.3.6.1 访问控制策略

要求 TSF 应按确定的强制访问控制安全策略进行设计，并按需要确定访问控制策略的控制范围，包括策略控制下的主体、客体，及由策略覆盖的被控制的主体与客体间的操作。可以有多个访问控制安全策略，但它们必须独立命名，且不能相互冲突。按访问控制的覆盖范围，访问控制策略分为：

a） 子集访问控制，要求 TSF 的每个确定的基于安全属性的访问控制，TSF 应对属性所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略。

b） 完全访问控制，要求 TSF 的每个确定的基于安全属性的访问控制，TSF 应对属性所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略，并要求 TSF 应确保 TSC 内的任意一个主体和任意一个客体之间的所有操作将至少被一个确定的访问控制 SFP 覆盖。

常用的强制访问控制策略为多级安全模型。该模型要求 TCB 控制范围内的所有主体对客体的直接或间接的访问应满足：

——向下读原则——仅当主体安全级（安全属性）中的等级分类高于或等于客体安全级（安全属性）中的等级分类，且主体安全级（安全属性）中的非等级类别包含了客体安全级（安全属性）中的全部非等级类别，主体才能读该客体；

——向上写原则——仅当主体安全级（安全属性）中的等级分类低于或等于客体安全级（安全属性）中的等级分类，且主体安全级（安全属性）中的非等级类别包含于客体安全级（安全属性）中的非等级类别，主体才能写该客体。

##### 4.3.6.2 访问控制功能

要求 TSF 应明确指出采用一条命名的访问控制策略所实现的特定功能，说明策略的安全属性的使用和特征，以及该策略的控制范围。按访问控制的覆盖范围，访问控制策略分为：

c） 子集访问控制，要求 TSF 的每个确定的基于安全属性的访问控制，TSF 应对属性所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略。

d） 完全访问控制，要求 TSF 的每个确定的基于安全属性的访问控制，TSF 应对属性所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略，并要求 TSF 应确保 TSC 内的任意一个主体和任意一个客体之间的所有操作将至少被一个确定的访问控制 SFP 覆盖。

无论子集访问控制还是完全访问控制，TSF 应有能力提供：

——将在安全属性或命名的安全属性组的客体上，执行访问控制 SFP；

——将使用在受控客体上的受控操作所管理的受控主体和受控客体之间的访问规则，来决定受控主体与受控客体之间的操作是否被允许；

——将在基于安全属性的授权主体访问客体的附加规则的基础上，授权主体访问客体；

——将基于安全属性的拒绝主体对客体访问的规则，实现拒绝主体对客体的访问。

#### 4.3.7 用户数据保密性存储保护

应对存储在 TSC 内的用户数据进行保密性保护，包括：

a） 自主访问控制，应确保每一个用户的数据，不被该用户授权以外的任何用户或授权用户以任何未经授权的方式访问。

b） 强制访问控制，应确保系统中的数据，不被任何未经授权的用户或授权用户以任何未经授权的方式访问。

c） 数据加密存储，应对系统中的重要数据进行加密存放，确保除合法持有密钥者外，其余任何用户不能获得该数据。

#### 4.3.8 用户数据保密性传输保护

##### 4.3.8.1 TCB 内部数据传输保护

应对在 TSC 内传输的用户数据进行保密性保护，通过加密或其它方式保护数据在传输过程中不被泄露和窃取，包括：

a） 基本内部传输保护，要求 TCB 在对物理上分隔的部分（如内存与磁盘）间传递用户数据时，应执行访问控制安全功能策略（SFP），以防止信息的泄漏、篡改和丢失。

b） 属性分隔传输保护，要求除具有基本内部传输保护功能外，还应根据安全属性来分隔传输的数据，如，按属性有的数据需要进行加密保护。

##### 4.3.8.2 TSF 间用户数据传输保护

应对不同 TSF 之间，或不同 TSF 上的用户之间传递的用户数据，通过加密或其他方式保护数据在传输过程中不被泄露和窃取。

##### 4.3.8.3 向 TSC 之外输出数据的保护

当数据从 TSC 之内向其控制范围之外输出时，根据需要可以保留或不保留数据的安全属性和保护措施，包括：

a） 不带安全属性的用户数据输出，要求 TSF 在安全功能策略的控制下输出用户数据到 TSC 之外时，应执行合适的 SFP，并且由 TSF 所输出的用户数据不带有与数据相关的安全属性。

b） 带有安全属性的用户数据输出，要求 TSF 在 SFP 的控制下输出用户数据到 TSC 之外时，应执行相应的 SFP，且 TSF 所输出的用户数据应带有与数据相关的安全属性，并应确保安全属性与所输出的数据确切相关联。

##### 4.3.8.4 从 TSC 之外输入数据

当数据从 TSF 控制范围之外向其控制范围之内输入时，应有相应的安全属性和保护措施，以便输入的数据能受到保护，包括：

a） 不带安全属性的用户数据输入，TSF 应做到：

——在 SFP 控制下从 TSC 之外输入用户数据时，应执行访问控制 SFP；

——略去任何与从 TSC 之外输入的数据相关的安全属性；

——应执行附加的输入控制规则，为输入数据设置安全属性。

b） 带有安全属性的用户数据输入，TSF 应做到：

——在 SFP 控制下从 TSC 之外输入用户数据时，应执行访问控制 SFP；

——TSF 应使用与输入的数据相关的安全属性；

——TSF 应确保在安全属性和接收的用户数据之间提供了确切的联系；

——TSF 应确保对输入的用户数据的安全属性的解释与原安全属性的解释是一致的。

#### 4.3.9 用户数据完整性保护

##### 4.3.9.1 存储数据的完整性

应对存储在 TSC 内的用户数据进行完整性保护，包括：

a） 存储数据的完整性检测，要求 TSF 应对基于用户属性的所有客体，对存储在 TSC 内的用户数据进行完整性检测。

b） 存储数据的完整性检测和恢复，要求 TSF 应对基于用户属性的所有客体，对存储在 TSC 内的用户数据进行完整性检测,并且当检测到完整性错误时，TSF 应采取必要的恢复措施。

#### 4.3.9.2 传输数据的完整性

当用户数据在 TSF 和其它可信 IT 产品间传输时应提供完整性保护，包括：

a） 数据交换完整性检测，要求对被传输的用户数据进行检测，及时发现以某种方式传送或接收的用户数据被篡改、删除、插入或重用的情况发生。

b） 源数据交换恢复，要求由接收者 TCB 借助于源可信 IT 产品提供的信息，恢复被破坏的数据为原始的用户数据。

c） 目的数据交换恢复，要求由接收者 TCB 自己，无需来自源可信 IT 产品的任何帮助，即能恢复被破坏的数据为原始的用户数据。

#### 4.3.9.3 处理数据的完整性

对计算机信息系统中处理中的数据，应通过“回退”进行完整性保护，包括：

a） 基本回退，要求 TSF 应执行访问控制 SFP，以允许对客体列表上的指定操作的回退，并允许在回退可以实施的范围内进行回退操作。

b） 高级回退，要求 TSF 应执行访问控制 SFP，以允许对客体列表上的所有操作的回退，并允许在回退可以实施的范围内进行回退操作。

### 4.3.10 剩余信息保护

在对资源进行动态管理的系统中，客体资源（内存缓冲区、磁盘空间、进程空间、其它记录介质、寄存器、外部设备等）中的剩余信息不应引起信息的泄露。剩余信息保护分为：

a） 子集信息保护，要求对 TCB 安全控制范围之内的某个子集的客体资源，在将其分配给某一用户或代表该用户运行的进程时，应将其中的残留信息全部清除。

b） 完全信息保护，要求对 TCB 安全控制范围之内的所有客体资源，在将其从某一用户或代表该用户运行的进程回收时，应将其中的残留信息全部清除。

c） 特殊信息保护，对于某些需要特别保护的信息，应采用专门的方法对残留信息做彻底清除，如对剩磁的清除等。

### 4.3.11 隐蔽信道分析

#### 4.3.11.1 一般性的隐蔽信道分析

应通过对隐蔽信道的非形式化搜索，标识出可识别的隐蔽信道，并根据实际测量或工程估量确定每一个被标识信道的最大带宽；应对每个信息流控制策略都搜索隐蔽信道，并提供隐蔽信道分析的文档。分析文档应说明以下情况：

a) 标识出隐蔽信道并估计它们的容量；

b) 描述用于确定隐蔽信道存在的过程，以及进行隐蔽信道分析所需要的信息；

c) 描述隐蔽信道分析期间所作的全部假设；

d) 描述最坏的情况下对隐蔽信道容量进行估计的方法；

e) 为每个可标识的隐蔽信道描述其最大可能的利用情形。

#### 4.3.11.2 系统化的隐蔽信道分析

应通过对隐蔽信道的系统化搜索，标识出可识别的隐蔽信道，并以结构化、可重复的方式标识出隐蔽信道；应对每个信息流控制策略都搜索隐蔽信道，并提供隐蔽信道分析的文档。对分析文档的要

求与一般性隐蔽信道分析相同。

#### 4.3.11.3 彻底的隐蔽信道分析

应通过对隐蔽信道的穷举搜索，标识出可识别的隐蔽信道，并以结构化、可重复的方式标识出隐蔽信道；应提供额外的证据，证明对隐蔽信道的所有可能的搜索方法都已执行。对分析文档的要求与一般性隐蔽信道分析相同。

### 4.3.12 用户与 TSF 间可信路径

用户与 TSF 间的可信路径应：

a) 提供真实的端点标识，并保护通信数据免遭修改和泄露；

b) 允许 TSF 自身、本地用户或远程用户原发的经可信路径的通信；

c) 对原发用户的鉴别或需要可信路径的其它服务均使用可信路径；

d) 运用以 PKI 为基础的混合密码体制建立安全的可信路径。

### 4.3.13 密码支持

#### 4.3.13.1 密码分级

根据密码强度与信息系统安全等级匹配的原则，按照国家密码主管部门的密码分级配置，确定相应的密码分级如下：

a) 第一级：对应于《准则》用户自主保护级的安全要求，采用国家密码主管部门的一级密码配置，按照 4.3.13.2 条密钥管理和 4.3.13.3 条密码运算的要求，设置密码支持系统；

b) 第二级：对应于《准则》系统审计保护级的安全要求，采用国家密码主管部门的二级密码配置，按照 4.3.13.2 条密钥管理和 4.3.13.3 条密码运算的要求，设置密码支持系统；

c) 第三级：对应于《准则》安全标记保护级的安全要求，采用国家密码主管部门的三级密码配置，按照 4.3.13.2 条密钥管理和 4.3.13.3 条密码运算的要求，设置密码支持系统；

d) 第四级：对应于《准则》结构化保护级的安全要求，采用国家密码主管部门的四级密码配置，按照 4.3.13.2 条密钥管理和 4.3.13.3 条密码运算的要求，设置密码支持系统；

e) 第五级：对应于《准则》访问验证保护级的安全要求，采用国家密码主管部门的五级密码配置，按照 4.3.13.2 条密钥管理和 4.3.13.3 条密码运算的要求，设置密码支持系统。

#### 4.3.13.2 密钥管理

密钥是密码系统的关键组成部分，密钥在密码的整个生存周期内应进行严格管理。根据上述五级密码配置和管理办法，应对不同级别的密钥实施以下方面的不同管理：

a） 密钥产生，要求 TSF 能根据某个指定标准的特定的算法和密钥长度来产生密钥。

b） 密钥分配，要求 TSF 能根据某个指定标准的特定的分配方法来分配密钥。

c） 密钥访问，要求 TSF 能根据某个指定标准的特定的访问方法来访问密钥。

d） 密钥销毁，要求 TSF 能根据某个指定标准的特定的销毁方法来销毁密钥。

#### 4.3.13.3 密码运算

TSF 必须按照密码分级配置所确定的特定密码算法和指定长度的密钥进行密码运算，以确保密码运算功能的正确性和不同级别的密码运算的不同强度。典型的密码运算包括：数据加密和/或解密，数字签名的产生和/或验证，针对完整性的密码校验和的产生和/或校验和的检验，保密散列（信息摘要），密钥加密和/或解密，以及密钥协商等。

## 5 安全保证技术要求

### 5.1 TCB 自身安全保护

#### 5.1.1 安全运行测试

要求 TSF 在系统初始化期间、在正常运转下周期性地、应授权用户请求或在其它条件下应能运行一组与系统当前状态有关的测试套件，来验证由 TSF 所提供的安全假定的正确运行。

安全运行测试应包括：

f) 对基本平台的测试，主要指对硬件和固件环境（如内存条、数据路径、总线、控制逻辑、处理器寄存器、通信接口、控制台接口以及外围设备等）的测试；

g) 对软件的可装载测试，主要指对软件部件（如逻辑单元，计算单元等）的装载和强化测试，包括初始化和运行的正确确认。

#### 5.1.2 失败保护

应确保当 TSF 中所确定的失败类型出现时保存一个保护状态。该保护状态确保 TSF 从失败恢复时安全策略的正确性。

#### 5.1.3 输出 TSF 数据的可用性

应通过一系列规则，根据 TSF 数据类型列表的指示，在所定义的可用性度量范围内，确保 TSF 数据（如口令、密钥、审计数据或 TSF 的可执行代码）在 TSF 与远程可信 IT 产品之间传输时的可用性。

#### 5.1.4 输出 TSF 数据的保密性

应保护 TSF 数据（如口令、密钥、审计数据或 TSF 的可执行代码）在 TSF 与远程可信 IT 产品之间传输时，不被未经授权的泄露。

#### 5.1.5 输出 TSF 数据的完整性

应保护 TSF 数据（如口令、密钥、审计数据或 TSF 的可执行代码）在 TSF 与远程可信 IT 产品之间传输时，不被未授权者修改，包括：

a） TSF 间修改的检测，在假定知道远程可信 IT 产品所使用的机制的情况下，TSF 应提供在所定义的修改度量范围内检测 TSF 与远程 IT 产品之间传输的所有 TSF 数据被修改的能力。

b） TSF 间修改的检测与改正，在上述 TSF 间修改的检测的基础上，如果检测到修改时，能按修改类型将所有被修改的数据改正过来。

#### 5.1.6 TCB 内 TSF 数据传输

TSF 数据在 TCB 内的分离部分间传输时应受到保护，包括：

a） 内部 TSF 数据传输的基本保护，要求 TSF 应对 TCB 的分离部分间传输的 TSF 数据进行保护，使其在传输过程中不被泄露或修改。

b） TSF 数据传输分离，在对 TCB 内部的分离部分间传输数据时，要求 TSF 将用户数据与 TSF 数据进行分离，以保护 TSF 数据在 TCB 的分离部分间传输时不被泄露或修改。

c） TSF 数据完整性保护，要求 TSF 对在 TCB 的分离部分间传输的 TSF 数据时，能检测出所传输的 TSF 数据被修改、替换、重排序、删除等完整性错误，并能采取规定的措施进行改正。

#### 5.1.7 物理安全保护

##### 5.1.7.1 物理攻击的被动检测

应对可能危及 TSF 安全的物理篡改提供明确的检测手段，并提供判断 TSF 设备或 TSF 要素是否已被物理篡改的能力。篡改检测是被动的，授权用户必须激活安全管理功能或用手动方式检查，以确定篡改是否发生。

#### 5.1.7.2 物理攻击的自动报告

应对可能危及TSF安全的物理篡改提供明确的检测手段，并提供判断TSF设备或TSF要素是否已被物理篡改的能力。对需主动检测的TSF设备或TSF要素，TSF应监视这些设备和要素，并当其发生物理篡改时，自动报告给指定用户。

#### 5.1.7.3 物理攻击抵抗

应提供自动检测并抵制对TSF设备或TSF要素的物理篡改，使TSP不受损害。对某些形式的威胁，TSF不仅有必要监测到它们，更要以使设备受到保护的策略自动回应物理篡改，真正地抵制或阻止这些攻击。比如，根据保密性策略的要求，对于存储在某类存储介质上的信息，使其处于不可写的状态，从而保护其上的信息不被篡改。

### 5.1.8 可信恢复

应在确定不减弱保护的情况下启动TCB，并在TSF运行中断后能在不减弱保护的情况下恢复运行。可信恢复包括：

a） 手动恢复，应允许TCB只提供以人工干预的方法返回到安全状态的机制。为此，在TCB发生失败或服务中断后，TSF应进入维护方式，该方式将提供以手工方法将TCB返回到一个保护状态的能力。

b） 自动恢复，对至少一种类型的服务中断，要求TSF应确保使用自动化过程使TCB返回到一个安全状态，对其它的服务中断可由手动恢复实现。

c） 无过分丢失的自动恢复，在进行自动恢复时，不允许被保护的客体有过分的丢失。即在实现上述自动恢复时，应确保在TSC内的TSF数据或客体无超过限量的丢失。

d） 功能恢复，要求TSF应确保TCB安全功能或者被成功完成，或者对指定的情况恢复到一致的和安全的状态。

### 5.1.9 重放检测

应能检测出确定实体（如消息、服务请求、服务响应、会话等）的重放,从而实现有效地避免重放攻击，并在检测到重放要求时，应执行操作列表所指示的操作。

### 5.1.10 参照仲裁

对一个给定的SFP，其所实现的访问监视器和/或前端过滤器应是“始终被激活的”，并正确、成功地执行，从而使SFP强制执行的所有行动都要由TSF加以确认，即要求TSF对TSP具有不可旁路性和防篡改性。

### 5.1.11 域分离

a） TSF域分离，应为自身执行维护一个安全域，以防止不可信主体的干扰和篡改，并进行TSC内主体安全域之间的强行分离。域分离的具体要求如下：

——通过将TSF的安全域（“保护域”）的资源与该域外的主体及不受约束的实体分离开，使得保护域外的实体不能观察或修改保护域内的TSF数据或TSF编码；

——域间的传输是受控的，不能随意地进入或退出保护域；

——按地址传到保护域的用户或应用参数，根据保护域的地址空间进行确认，而按值传到保护的域的用户或应用参数则根据保护域所期望的值进行确认；

——除了由TSF控制的共享部分外，每个主体有不同的安全域。

b） SFP域分离，应按SFP对TSF的域进一步细分：一个SFP的确定集合是一个域，TSF的其余部分是一个域，TCB内的非TSF部分是一个域，并且要求：

——TSF的未隔离部分应对自身的执行维护一个安全域，以防止不可信主体的干扰和篡改；

——TSF 应对 TSC 内主体的安全域之间作强行分离；

——TSF 应对 TCB 中与访问控制 SFP 有关的部分，维护一个自身执行的安全域，以防止被 TCB 内非 TSF 部分的干扰和篡改。

#### 5.1.12 状态同步协议

在分布式系统中，应通过 TSF 采取的某些安全措施，确保分布式的两部分之间在完成与安全有关的活动后，状态保持同步。状态同步协议包括：

a） 简单的可信回执，要求数据接收者给出简单回执，即 TSF 收到来自另一 TSF 发出的传输数据时应提供确认（回执），以表明其成功地接收到了未经修改的 TSF 数据。

b） 相互的可信回执，要求交换数据的双方相互给出回执。即 TSF 收到来自另一 TSF 发出的传输数据时应提供确认（回执），以表明其成功地接收到了未经修改的 TSF 数据；并且另一 TSF 在收到该确认（回执）后应证实其已收到这一确认。这为交换数据的双方知道已成功地完成了数据传输提供了进一步的信任。

#### 5.1.13 时间戳

应为 TSF 自身的应用提供可靠的时间戳，即应有可靠的计时系统。

#### 5.1.14 TSF 间的 TSF 数据的一致性

在分布式或复合式系统环境下，TSF 与别的可信 IT 产品交换 TSF 数据（如：SFP 属性、审计信息、标识信息等）时，应提供确保 TSF 间数据一致性的能力，即 TSF 应提供对 TSF 数据类型列表所列数据一致性解释的能力，对别的可信 IT 产品的 TSF 数据的解释，应使用该 IT 产品的 TSF 所确定的规则。

#### 5.1.15 TCB 内 TSF 数据复制的一致性

应确保对 TCB 内部 TSF 数据复制的一致性，，当出现包含复制的 TSF 数据的 TCB 部分断开时，TSF 应确保在重建连接后，在处理任何与 TSF 数据复制的一致性相关请求前，实现被复制的 TSF 数据的一致性。

#### 5.1.16 TSF 自检

应提供对 TSF 正确操作的自测试能力。这些测试可在启动时进行，或周期性地进行，或在授权用户要求时进行，或当某种条件满足时进行，同时应提供对 TSF 数据和可执行代码的完整性验证的能力。

#### 5.1.17 资源利用

##### 5.1.17.1 故障容错

应通过一定措施防止由于 TCB 失效引起的资源能力的不可用，确保即使出现故障情况，TSF 也能维持正常运行，如在电力中断或通信中断时，TCB 将继续执行关闭程序的操作。故障容错机制有主动和被动两种。在主动机制下，特定的功能在故障发生时将会被激活，如火警即是一种主动机制，当 TSF 检测到火情时可以将操作切换到备份系统上；在被动机制下，TCB 被设计为能自动处理故障，如多处理器的多数表决系统，当其中的某一个处理器失效时并不影响 TCB 的正常运行，当然需要检测出失效的处理器以便更换。

故障容错分为：

a） 降级故障容错，要求在确定的故障情况下，TSF 能继续正确运行指定的功能。这种功能往往是实现一些善后操作，如在安全状态保留失败的情况下，TSF 能按能力列表所列功能运行。这是一种强制性的安全功能策略，要求在出错情况下 TCB 能继续规定的正确操作，因而要求系统必须在故障发生后通过降低能力保持一个安全的状态。这类故障的例子有计算机房进水、电力短时间中断、CPU 或主机瘫痪、软件错误或缓冲区溢出等。

b） 受限故障容错，对标识的故障事件，TSF 能继续正确运行原有功能。这就要求 TCB 必须采取

有效措施来对抗指定的故障。如在安全状态保留失败的情况下，能运行所有 TCB 的功能。

#### 5.1.17.2 服务优先级

应通过控制用户和主体对 TSC 内资源的使用，使得高优先级任务的完成总是不受低优先级任务的干扰和影响，这些资源包括处理类资源和通信类资源等。服务优先的机制可以是被动的也可以是主动的。前者以调度方式实现，后者以中断方式实现。服务优先级分为：

a） 有限服务优先级，将服务优先级的控制范围限定在 TSC 内的某个资源子集，要求 TSF 对与该资源子集有关的主体定义优先级，并指出对何种资源使用该优先级。如果一个主体准备对由服务优先级控制的资源进行操作，那么其访问和/或访问时间将取决于该主体的优先级、当前正在对该资源进行操作的主体的优先级以及等待进行该操作的队列中的主体的优先级。

b） 全部服务优先级，服务优先级的控制范围应包括 TSC 内的全部资源，要求 TSC 内的所有资源都服从服务优先机制，并对相关的主体定义优先级。如果一个主体准备对一个可共享的 TSC 内的资源进行操作，那么其访问和/或访问时间将取决于该主体的优先级、当前正在对该资源进行操作的主体的优先级以及等待进行该操作的队列中的主体的优先级。

#### 5.1.17.3 资源分配

应通过控制用户和主体对资源的占用，使得不因不恰当地占有资源而出现拒绝服务情况。这里的重点是对资源的分配，而不关心其使用。

资源分配的控制方法分为：

a） 最大限额，应确保用户和主体不会超过某一数量或独占某种受控资源。安全保护框架（PP）应规定所要求的最大资源分配限额的受控资源（如处理器、磁盘空间、内存、传输带宽）清单。

b） 最小和最大限额，除确保上述最大限额的受控资源分配外，还应确保用户和主体至少获得最小规定的资源。

### 5.1.18 TCB 访问控制

应提供控制用户与 TCB 建立会话的功能。用户会话的建立包括创建一个或多个主体（如进程），这些主体在 TCB 中代表用户执行操作，并具有相应用户的安全属性。TCB 访问控制包括：

a） 可选属性范围限定，应提供 TCB 会话建立时限制用户可能选择的会话安全属性的范围要求，以及用户可能要绑定到的主体（如进程）。这些限制取决于访问方法、访问的地址或端口、及访问时间（如一日的某些时间、一周的某些天等）。PP 应为 TSF 规定有关要求，以便基于环境条件对授权用户的安全属性的域设置限制。例如，可允许一个用户在正常的工作时间内建立一个“秘密会话”，而在非正常工作时间该用户就只能建立“不分级的会话”。

b） 多重并发会话限定，应对同一用户在一个时间段内可能的并发会话次数进行限制，包括多重并发会话的基本限定和每位用户多重并发会话的属性限定。前者提供了对 TCB 内所有用户并发会话数的限制要求，以便有效地使用 TCB 资源，后者在前者的基础上，提供了对每一个用户并发会话次数的限制要求，这种限制是基于有关用户的安全属性做出的。

c） 会话锁定，应提供交互式会话的 TSF 原发的和用户原发的锁定和解锁能力及 TSF 原发终止能力，以便对交互式会话在进入非活动周期后对终端进行锁定或结束会话。TSF 原发终止提供在用户静止“一段时间”以后，由 TSF 终止该用户会话的能力。为了激活终端，必须在开锁前执行规定的事件（如再次鉴别）等。TSF 原发的会话锁定是指在指定的用户静止周期时间以后，由 TSF 原发的交互会话的锁定。用户原发锁定是指在指定的用户静止期以后，由用户原发的交互会话锁定，该功能提供用户锁定和解锁自己的交互会话的能力。在用户的静止期超

过规定的值时，通过以下方式锁定该用户的交互式会话：

——在显示设备上清除或涂抹，使当前的内容不可读；

——取消会话解锁之外的所有用户数据的存取/显示的任何活动；

——在会话解锁之前再次鉴别。

d） TCB 访问标记，要求在对用户进行标识和鉴别之前，TSF 应提供对使用 TCB 的用户显示警告信息的能力，TSF 还应提供缺省的 TCB 访问标记，以便为建立 TCB 的访问标记做准备，且该标记应先于会话的对话建立之前显示。

e） TCB 访问历史，要求 TSF 可在一次会话成功建立的基础上，显示该账户上一次会话成功建立的日期、时间、方法和位置等信息，或显示该账户上一次会话建立不成功的日期、时间、方法和位置等信息，以及从最后一次成功的会话建立以来不成功的尝试次数。用户应能够复查这些信息，也可以放弃这些信息，并且在没有给用户提供访问历史信息的机会的情况下，不能从用户界面上抹去该信息的。

f） TCB 会话建立，要求 TSF 应根据属性允许或拒绝该次会话的建立。这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级、角色中的成员资格），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。这种限制能防止在正确监控措施未实施时，用户执行某些未授权操作，从而提供一定的操作性保护。

#### 5.1.19 可信路径/信道

##### 5.1.19.1 TSF 间可信信道

应在 TSF 与远程可信 IT 产品之间提供一条通信信道，并提供真实的端点标识，以及保护信道数据免遭修改和泄露，同时要求允许由 TSF 或远程可信 IT 产品原发的经可信信道的通信，还要求 TSF 支持由可信信道的各种功能列表原发的经可信信道的通信。

##### 5.1.19.2 用户与 TSF 间可信路径

应在 TSF 与本地用户或远程用户之间提供一条可信的信息传输路径。该可信路径应提供真实的端点标识，保护通信数据免遭修改和泄露；TSF 应允许由 TSF 自身、本地用户或远程用户原发的经可信路径的通信，还应对原发用户的鉴别或需要可信路径的其它服务均使用可信路径。

### 5.2 TCB 设计和实现

#### 5.2.1 配置管理

##### 5.2.1.1 配置管理自动化

应通过配置管理（CM）自动化增加 CM 系统的有效性，使所设计的 TCB 不易受人为错误或疏忽的影响。这里的 TCB 是就纯软件而言的，通过引进自动化的 CM 来协助 TCB 配置项的正确生成，并确定 TCB 与其以前版本之间的变化及将来版本的改变。

CM 自动化分为：

a） 部分 CM 自动化，应确保 TCB 的实现表示是通过自动方式控制的，从而解决复杂实现或众多合作者合作开发，以及在开发过程中多种变化情况所出现的人工难以解决的问题，并确保这些变化是已授权的行为所产生的。部分 CM 自动化要求：

——TCB 的开发者所使用的 CM 系统应通过所提供的自动方式来确保 TCB 的实现表示只能进行已授权的变化，并能提供自动方式来支持 TCB 的生成；

——开发者所提供的 CM 计划应描述 CM 系统中所使用的自动工具，并说明如何使用这些工具。

b） 完全 CM 自动化，除了与上述部分 CM 自动化有相同的内容外，还能自动确定 TCB 版本间的

变化，并标识出哪个配置项会因其余配置项的修改而受到影响。

#### 5.2.1.2 配置管理能力

应确保 TCB 在提交用户运行之前是正确和完备的，所有配置项不会缺少，并能防止对 TCB 配置项进行未授权的增加、删除或修改。

配置管理能力的设计应满足以下要求：

a） 版本号，要求开发者所使用的版本号与所应表示的 TCB 样本应完全对应，没有歧义。

b） 配置项，要求配置项应有唯一的标识，从而对 TCB 的组成有更清楚的描述。这些描述与部分 CM 自动化的要求相同。

c） 授权控制，要求开发者用对 TCB 的唯一引用作为其标签，从而使 TCB 的使用者明确自己使用的是哪一个样本；控制机制使 TCB 不会受到未经授权的修改，从而确保 TCB 的完整性。为此，授权控制要求：

——CM 计划应描述系统是如何使用的，并说明运行中的 CM 系统与 CM 计划的一致性；

——CM 文档应足以说明在 CM 系统下有效地维护了所有的配置项；

——CM 系统应确保对配置项只进行授权修改。

d） 生成支持和验收过程，要求在上述版本号、配置项、授权控制的基础上确认对配置项的任何生成和修改都是由授权者进行的。为此，CM 系统应支持 TCB 的生成，验收计划应描述用来验收修改过的或新建的配置项的过程，并作为 TCB 的一部分。

e） 进一步的支持，要求集成过程有助于确保由一组被管理的配置项生成 TCB 的过程是以授权的方式正确进行的，并要求 CM 系统有能力标识用于生成 TCB 的主拷贝的材料，这有助于通过适当的技术，以及物理的和过程的安全措施来保持这些材料的完整性。为此，CM 的进一步支持要求：

——CM 文档除应包括配置清单、CM 计划外，还应包括一个验收计划和集成过程，集成过程应描述在 TCB 制作过程中如何使用 CM 系统；

——CM 系统应要求将一个配置项接收到 CM 中的不是该配置项的开发者；

——CM 系统应明确标识组成 TSF 的配置项；

——CM 系统应支持所有对 TCB 修改的审计，至少应包括操纵者、日期、时间等信息；

——CM 系统应有能力标明用于生成 TCB 主拷贝的所有材料；

——CM 文档应阐明 CM 系统与开发安全方法相联系的使用，并只允许对 TCB 作授权的修改；

——CM 文档应阐明集成过程的使用能够确保 TCB 的生成是以授权的方式正确进行的；

——CM 文档应阐明 CM 系统足以确保负责将某配置项接收到 CM 中的不是该配置项的开发者；

——CM 文档应能证明接收过程对所有配置项的修改都提供了充分而适当的复查。

#### 5.2.1.3 配置管理范围

应通过确保 CM 系统跟踪所有必须的 TCB 配置项来保证这些配置项的完整性。

对 CM 范围的要求包括以下内容：

a） TCB 配置管理范围，要求将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档、CM 文档等置于 CM 之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此要求：

——开发者所提供的 CM 文档应展示 CM 系统至少能跟踪上述 CM 之下的内容；

——文档应描述 CM 系统是如何跟踪这些配置项的；

——文档还应提供足够的信息证明达到所有要求。

b） 问题跟踪配置管理范围，除 TCB 配置管理范围描述的内容外，要求特别强调对安全缺陷的跟踪。

c） 开发工具配置管理范围，除问题跟踪配置管理范围所描述的内容外，要求特别强调对开发工具和相关信息的跟踪。

#### 5.2.2 分发和操作

##### 5.2.2.1 分发

应通过系统控制、分发工具和分发过程确保接收方所收到的 TCB 产品正是发送者所发送的，且没有任何修改，主要目标是在分发过程中能够检测和防止对 TCB 的任何修改。

a） 分发过程，应将 TCB 或其部分的分发以文档形式提供给用户，分发文档应描述给用户分发 TCB 的各版本时用以维护安全所必须的所有过程，并按该过程进行分发。

b） 修改检测，要求除按分发过程的要求进行 TCB 的分发外，分发文档还应：

——描述检测修改的方法和技术，或者描述开发者的主拷贝与用户收到的版本之间的任何差异；

——描述用来检测试图伪装成开发者向用户发送产品的方法。

c） 修改防止，要求在修改检测的基础上，分发文档应描述如何防止修改的方法和技术。

##### 5.2.2.2 操作（安装、生成和启动）

应确保在开发者所期望的安全方式下进行安装、生成和启动，将处于配置控制下的 TCB 的实现表示安全地转换为用户环境下的初始操作。对于不同的 TCB，安装、生成和启动会有不同的情况，如智能卡的所有安装、生成和启动都在开发者一方进行，而纯软件的 TCB 则以软件形式分发，其安装、生成和启动都在 TCB 的拥有者一方进行。安装、生成和启动过程可以以独立的文档进行描述，也可以与其它管理员文档一起描述。

a） 安装、生成和启动过程，要求开发者以文档形式提供对 TCB 安全地进行安装、生成和启动的过程进行说明，并确保最终生成了安全的配置。

b） 日志生成，要求文档应描述建立日志的过程，该日志包含了用以生成 TCB 的生成选项，从而能够明确决定 TCB 是何时及如何产生的。

#### 5.2.3 开发

##### 5.2.3.1 功能设计

根据要求的形式化程度和所提供的 TSF 外部接口的详细程度，功能设计分为：

a） 非形式化功能设计，应使用非形式化风格来完备地描述 TSF 及其外部接口，功能设计应当是内部一致的，并且使用所有外部 TSF 接口的目的与方法，适当的时候，还要提供结果例外情况和错误信息的细节。

b） 完全定义的外部接口，除上述非形式化功能设计的要求外，功能设计还应包括 TSF 是完备地表示的基本原理。

c） 半形式化功能设计，应使用半形式化风格来完备地描述 TSF 及其外部接口，必要时可由非形式化、解释性的文字来支持。其余要求与上述相同。

d） 形式化功能设计，应使用形式化风格来描述 TSF 及其外部接口，必要时由非形式化、解释性的文字来支持。其余要求与上述相同。

##### 5.2.3.2 高层设计

应通过对 TSF 的每个结构单元的功能及其相互关系的描述，实现 TCB 的安全功能要求。根据所要求的形式化程度和所提供的接口说明的详细程度，高层设计分为：

a） 描述性高层设计，要求：

——说明应是非形式化的、内在一致的，并应通过单元来描述TSF的结构；

——应描述每一个单元所提供的安全功能，标识TSF要求的任何基础性的硬件、固件和/或软件，并且通过支持这些硬件、固件或软件所实现的保护机制，来提供TSF功能表示；

——应标识TSF单元的所有接口，并标明TSF单元的哪些接口是外部可见的。

b） 安全加强的高层设计，除上述描述性高层设计要求外，还应当描述 TSF 单元所有接口的使用目的与方法，并提供例外情况和错误信息的细节，以及描述如何将 TCB 分离成 TSP 加强单元和其它单元。

c） 半形式化高层设计，要求高层设计的表示应是半形式化的，并对 TSF 单元提供所有结果的完整细节。其余要求与安全加强的高层设计相同。

d） 半形式化高层解释，除上述要求外，还要求高层设计应当证明所标识的分离方法，包括任何保护机制，是足以确保从非 TSP 加强功能中将 TSP 加强功能清晰而有效地分离出来，并应证明 TSF 机制足以实现在高层设计中标识的安全功能。

e） 形式化高层设计，要求高层设计的表示应是形式化的，其余要求与半形式化高层解释相同。

#### 5.2.3.3 实现表示

应以源代码、固件或硬件等来表述 TSF 的具体符号表示，从而可以获得 TSF 内部的详细工作情况。根据完备性和所提供的实现表示的结构，实现表示分为：

a） TSF 子集实现，实现表示应无歧义地定义一个详细级别的 TSF，无须进一步的设计就能生成，并且实现表示应当是内在一致的。

b） TSF 完全实现，应为整个 TSF 提供实现表示，并应描述各部分之间的关系。其余要求同上。

c） TSF 的结构化实现，实现表示应是构造较小的，且易于理解。其余要求与 TSF 完全实现相同。

#### 5.2.3.4 TSF 内部结构

应采用模块化、层次化、策略加强机制的复杂度最小化，以及 TSF 中非 TSF 加强功能性的数目最小化进行 TSF 的内部结构设计，从而简化 TSF 的设计，达到可分析的程度。根据模块的数量和复杂性要求，TSF 内部结构分为：

a） 模块化，应以模块化方法设计和构建 TSF，并避免设计模块之间出现不必要的交互。为此要求：

——结构化描述应当标识 TSF 模块，并应描述每一个 TSF 模块的目的、接口、参数和影响；

——结构化描述应当描述 TSF 设计是如何使独立的模块间避免不必要的交互作用。

b） 复杂性降低，除上述对模块化的要求外，还要求结构化描述应当以分层的方式设计和构建 TSF，使设计层次之间的交互作用最小化。为此要求：

——在设计和构建 TSF 时，应使 TSF 部分的复杂度最小化，以加强访问控制策略；

——结构化描述应当标识 TSF 模块，并应指明 TSF 的哪些部分是加强访问控制策略的；

——结构化描述应描述分层结构，并说明如何使交互作用最小化；

——结构化描述应描述加强访问控制策略的TSF部分是如何被构建的，从而使其复杂性降低。

c） 复杂性最小化，除上述复杂性降低要求外，还要求开发者应当设计和构建 TSF，使得整个 TSF 的复杂性最小化。为此要求：

——在设计和构建 TSF 时，应使 TSF 部分的复杂度最小化，使加强访问控制略“简单到足以进行分析”；

——应确认那些目的与 TSF 无关的功能都已从 TSF 中排斥出去；

——结构化描述应证明 TSF 中的任何非 TSP 加强模块的包含关系。

#### 5.2.3.5 低层设计

应对 TSF 的每一个模块描述它的目的、功能、接口、依赖性和所有 TSP 加强功能的实现。根据低层设计所要求的形式化程度和接口说明所要求的详细程度，低层设计分为：

a） 描述性低层设计，要求 TSF 低层设计应满足：

——低层设计的表示应是非形式化的，内在一致的，并以模块术语描述；

——低层设计应描述每一个模块的目的；

——低层设计应以所提供的安全功能和对其它模块的依赖性术语定义模块间的相互关系；

——低层设计应描述如何提供每一个 TSP 加强功能；

——低层设计应标识 TSF 模块的所有接口，标识 TSF 模块的哪些接口是外部可见的，以及描述 TSF 模块所有接口的目的与方法，必要时，应提供影响、例外情况和错误信息的细节；

——低层设计应描述如何将 TCB 分离成 TSP 加强模块和其它模块。

b） 半形式化低层设计，除上述描述性低层设计要求外，要求低层设计应当是半形式化的，并在必要时提供所有结果的完备细节、例外情况和错误信息。

c） 形式化低层设计，除上述半形式化低层设计要求外，要求低层设计的表示应当是形式化的。

#### 5.2.3.6 表示的对应性

各种 TSF 表示，如功能设计、高层设计、低层设计、实现表示等相邻表示之间在相应严格程度上应具有对应性。根据各种 TSF 表示之间的对应性所需的形式化程度，表示的对应性分为：

a） 非形式化对应性说明，应在所提供的 TSF 表示的所有相邻对之间提供其对应性分析，即对所提供的 TSF 表示的每个相邻对，分析应当阐明，较为抽象的 TSF 表示的所有相关安全功能应当在较不抽象的 TSF 表示中得到正确而完备地细化。

b） 半形式化对应性说明，除上述非形式化对应性要求外，还要求对所提供的 TSF 表示的每个相邻对，当两者的各部分至少都是以半形式化来描述时，表示部分之间的对应性阐明也应是半形式化的。

c） 形式化对应性说明，除上述半形式化对应性要求外，还要求：

——对那些形式化规定的表示的相应部分，应严格证明其对应性；

——对所提供的 TSF 表示的每个相邻对，当其中一个表示是半形式化规定，而另一个表示至少是半形式化规定时，表示部分之间的对应性阐明也应是半形式化的；

——对于所提供的 TSF 表示的每个相邻对，如果两者的各部分都是形式化规定的，表示部分之间的对应性的证明也应是形式化的。

#### 5.2.3.7 安全策略模型化

通过开发基于 TSP 策略的安全策略模型，并建立功能设计、安全策略模型和 TSP 策略之间的对应性的方法，确保功能设计中的安全功能实施 TSF 中的策略。根据 TSF 模型，以及该模型与功能设计之间对应性所要求的形式化程度，安全策略模型化分为：

a） 非形式化 TCB 安全策略模型，要求 TSP 模型应阐明功能设计与 TSP 模型之间的对应性，并满足：

——TSP 模型应是非形式化的，并描述所有可以模型化的 TSP 策略的规则与特征；

——TSP 模型应包括一个基本原理，阐明该模型对所有可模型化的 TSP 策略来说，是与其一致的、完备的；

——TSP 模型和功能设计之间的对应性阐明应说明，所有功能设计中的安全功能对于 TSP 模

型来说是与其一致的、完备的。

b） 半形式化 TCB 安全策略模型，除上述非形式化 TCB 安全策略模型的要求外，要求所提供的 TSP 模型应是半形式化的，并且当功能设计至少是半形式化时，TSP 模型与功能设计之间的对应性的阐明也应是半形式化的。

c） 形式化 TCB 安全策略模型，除上述半形式化 TCB 安全策略模型的要求外，要求所提供的 TSP 模型应是形式化的，并且当功能设计是形式化时，TSP 模型与功能设计之间的对应性证明也应是形式化的。

#### 5.2.4 指导性文档

##### 5.2.4.1 管理员指南

应描述设置、维护和管理 TCB 的正确方式和方法，最大限度地保证 TCB 安全运行。管理员指南应帮助管理员理解 TCB 所提供的安全功能，包括要求管理员应采取的紧急安全措施和应提供的紧急安全信息。

管理员指南应包括以下内容：

a） 描述安全管理员可使用的管理功能和接口；

b） 描述如何以安全的方式管理 TCB；

c） 说明在安全处理环境中管理员可获取的功能和权限的警告；

d） 描述所有与安全操作有关的用户行为的假设；

e） 描述所有受安全管理员控制的安全参数；

f） 描述每一种与管理功能有关的安全相关事件，包括改变安全功能所控制的实体的安全特性；

g） 描述与安全管理员有关的系统环境的所有安全要求。

##### 5.2.4.2 用户指南

应描述 TSF 提供的安全功能，安全功能使用的命令和指导方针，包括警报信息说明等。用户指南提供了关于 TCB 的使用和可信度的测量的假设基础，这样非恶意的用户、应用提供者和其他使用 TCB 外部接口的人员都能理解 TCB 安全操作并自觉执行。在许多情况之下，用户指南可以适当地对两类不同用户提供单独的文档：一类是一般的操作员用户，另一类是使用软硬件接口的应用程序员和/或硬件设计员。

用户指南应包含以下内容：

a） 描述非安全管理员用户可用的功能和接口；

b） 描述用户可获取的安全功能和接口的用法；

c） 说明在安全处理环境中用户可获取的功能和权限的警告；

d） 阐明安全操作中用户应负的责任，包括在安全环境中能找到的用户行为的假设；

e） 描述与用户有关的系统环境的所有安全要求。

#### 5.2.5 生命周期支持

##### 5.2.5.1 开发安全

应采用的物理上、程序上、人员上以及其它方面的安全措施保护 TCB 开发环境的安全，包括开发场地的物理安全和对开发人员的选择；应采取适当的防护措施来消除或降低 TCB 开发所面临的安全威胁。

根据所要求的安全措施的充分性，开发安全分为：

a） 安全措施的说明，要求提供的开发安全文件中应包括以下内容：

——描述在 TCB 的开发环境中，为保护 TCB 设计和实现的机密性和完整性，在物理上、程序

上、人员上以及其它方面必要的安全措施；

——提供在 TCB 的开发和维护过程中执行安全措施的证据。

b） 安全措施的充分性，除安全措施说明的要求外，开发安全文件中所提供的在 TCB 的开发和维护过程中执行安全措施的证据应能证明安全措施对维护 TCB 的保密性和完整性提供了必要的保护。

#### 5.2.5.2 缺陷纠正

应跟踪和纠正 TCB 的缺陷，并提供缺陷信息和纠正缺陷所采取的策略和过程。根据缺陷纠正的范围不断扩大和缺陷纠正策略的严格性程度不断提高，缺陷纠正分为：

a） 基本缺陷纠正，要求缺陷纠正程序文档中应：

——描述用以跟踪所有 TCB 版本里已被报告的安全缺陷的过程；

——描述所提供的每个安全缺陷的性质和效果，以及缺陷纠正的情况；

——标识每个安全缺陷所采取的纠正措施；

——描述为 TCB 用户的纠正行为所提供的信息、纠正和指导的方法。

b） 缺陷报告，除基本缺陷纠正要求外，还要求缺陷报告应：

——记录缺陷纠正的过程，制定用来接受用户对于安全缺陷的报告和纠正这些缺陷的要求的措施；

——描述用以跟踪所有 TCB 版本里已报告的安全缺陷的过程；

——已报告的安全缺陷的处理过程应确保所有已知缺陷都已被纠正，并将纠正办法告知用户；

——已报告的安全缺陷的处理过程应提供防范机制，确保为纠正这些安全缺陷所引进的纠正方法不会带来新的缺陷。

c） 系统缺陷纠正，除缺陷报告要求外，应为用户有关 TCB 的安全问题的报告和查询指明一个或多个特别联系点，还应包括这样一个过程，它负责及时将安全缺陷报告及其相应的纠正自动分发给可能受到这种安全缺陷影响的注册用户。

#### 5.2.5.3 生命周期定义

应在 TCB 的生命周期内建立 TCB 开发和维护的模型。为了确保 TCB 能满足它所有的安全功能要求，并提高 TCB 的整体质量，一个标准的生命周期模型应是为某些专家组(例如学科专家、标准化实体等)所认可的模型；一个可测量的生命周期模型应是带有算术参数和/或测量 TCB 开发特性的度量(例如源码复杂性度量)。生命周期模型应包括用于开发和维护 TCB 的过程、工具和技术。这个模型所涉及的内容包括设计方法、复查过程、项目管理控制、转换控制过程、测试方法和接收过程。

根据生命周期模型的标准化、可测性，以及对其符合性不断提高的要求，生命周期定义包括：

a） 开发者定义的生命周期模型，要求开发者应建立用于开发和维护 TCB 的生命周期模型。该模型应对 TCB 开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护 TCB 的模型。

b） 标准生命周期模型，要求开发者应建立标准化的、用于开发和维护 TCB 的生命周期模型。该模型应对 TCB 开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护 TCB 的模型，解释选择该模型的原因，解释如何用该模型来开发和维护 TCB，以及阐明与标准化的生命周期模型的相符性。

c） 可测量的生命周期模型，要求开发者应建立标准化的、可测量的、用于开发和维护 TCB 的生命周期模型，并用此模型来衡量 TCB 的开发。该模型应对 TCB 开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护 TCB 的模型，包括针对该模型衡量

TCB 开发所需的算术参数和/或度量的细节。生命周期定义文档应解释选择该模型的原因，解释如何用该模型来开发和维护 TCB，阐明与标准化的可测量的生命周期模型的相符性，以及提供利用标准化的可测量的生命周期模型来进行 TCB 开发的测量结果。

#### 5.2.5.4 工具和技术

应明确定义用于开发、分析和实现 TCB 的工具，如编程语言、文档、实现标准以及其它支持 TCB 运行的程序库等，无需进一步检验就可以使用。

根据实现标准、实现的文档描述和范围要求的不同，工具和技术分为：

a） 明确定义的开发工具，要求开发者应标识用于开发 TCB 的工具，并且所有用于实现的开发工具都必须有明确定义。开发者应文档化已选择的依赖实现的开发工具的选项，并且开发工具文档应明确定义实现中每个语句的含义，以及明确定义所有基于实现的选项的含义。

b） 遵照实现标准-应用部分，除明确定义的开发工具的要求外，要求开发者应描述所应用部分的实现标准。

c） 遵照实现标准-所有部分，除遵照实现标准-应用部分的要求外，要求开发者应描述 TCB 所有部分的实现标准。

### 5.2.6 测试

#### 5.2.6.1 范围

应表明所标识的测试范围如何象功能设计中描述的那样与 TSF 相一致。这里不需要开发者覆盖 TSF 的各个方面，但有必要考虑其不足之处。测试范围包括：

a） 范围的证据，要求开发者通过提供相应的证据表明 TSF 已经按照功能要求进行了测试。开发者所提供的测试范围的证据应当表明测试文档中所标识的测试与功能设计中所描述的 TSF 之间的对应性。

b） 范围分析，要求开发者通过提供对应性分析表明 TSF 已经以系统的方法针对功能规范进行了测试。为此要求：

——开发者所阐明的已标识的测试应包括在功能设计中描述的所有安全功能的测试；

——开发者所提供的范围分析应当表明测试文档中所标识的测试与功能设计中所描述的 TSF 之间的对应性；

——测试范围的分析应当阐明功能设计中所描述的 TSF 和测试文档所标识的测试之间的对应性是完备的。

c） 严格的范围分析，除上述范围分析要求外，还要求测试范围的分析应当严格地阐明功能设计所标识的 TSF 的所有外部接口已经被完备测试过了。

#### 5.2.6.2 测试深度

测试的级别应适合所要求的安全级别，达到所要求的详细程度。

根据 TSF 表示所提供的从高层设计到实现表示不断增加的细节，测试的深度分为：

a） 高层设计测试，要求用“单元”描述对 TSF 高层设计的测试。TSF 单元提供 TSF 内部工作的一个高层描述。以阐明缺陷为目的的单元级别的测试保证了该单元已正确实现。开发者所提供的测试深度分析应阐明测试文档中所标识的测试足以表明该 TSF 的行为是与高层设计一致的。

b） 低层设计测试，要求用“模块”描述对 TSF 低层设计的测试。TSF 模块提供 TSF 内部工作的低层描述。以阐明缺陷为目的的模块级别的测试确保 TSF 的模块已经正确实现。开发者所提供的测试深度分析应阐明测试文档中所标识的测试足以表明该 TSF 行为是与高层设计和低层

设计一致的。

c） 实现表示测试，应确保该 TSF 已正确实现。要求开发者所提供的测试深度分析应阐明测试文档中所标识的测试足以表明该 TSF 是根据高层设计、低层设计和实现表示而运作的。

#### 5.2.6.3 功能测试

应展示 TSF 满足安全保护框架（PP）所要求的安全功能，保证 TSF 至少能够满足安全功能的要求。测试过程应提供测试程序和测试工具的使用说明书，包括测试环境，测试条件，测试数据参数和值。测试过程还应该显示如何从输入中得到测试结果。

功能测试包括：

a） 一般功能测试，要求开发者阐明所有的安全功能按照规定运作。为此要求：

——开发者所提供的测试文档应包括测试计划、测试过程描述，预期的测试结果和实际测试结果；

——测试计划应标识要测试的安全功能，描述要达到的测试目标；

——测试过程描述应标识要执行的测试，并描述每个安全功能的测试概况，包括对其它测试结果的顺序依赖性；

——期望的测试结果应当表明成功测试运行后的预期输出；

b） 顺序的功能测试，除满足一般功能测试要求外，还要求测试文档应包含测试过程中对顺序依赖性的分析。

#### 5.2.6.4 独立性测试

应由评估者或一个有专业知识的团体支持的独立实验室或消费者组织实施测试。这种测试需要与其它保证行为的表现相一致的对于 TCB 的理解。独立性测试可以采用全部或部分重复开发者功能测试的形式，也可采用讨论开发者功能测试的形式，来拓宽开发者测试的深度或广度，或者是测试对 TCB 都适用的公用领域中明显的安全性弱点。这些行为是互补的，并且对于每个 TCB 功能都可制定一个适当的组合计划。这个组合计划考虑了测试结果的可用性和适用范围，以及 TSF 的功能复杂度。一个测试计划要开发到与其他安全保护要求的级别一致的程度，并象更高的安全保护所要求的那样，包括更多样本的重复测试，更多的由评估者实施的正面和反面功能测试。

根据测试文档、测试支持和评估者测试的数目，独立性测试分为：

a） 相符性独立测试，应表明安全功能是按照规定运作的。要求开发者应提供用于测试的 TCB，并且该 TCB 要与测试相适应。

b） 抽样独立性测试，要求通过选择和重复测试开发者测试的一个抽样，表明安全功能按规范运作。开发者应提供能有效重现开发者测试的必需资料，包括可由机器阅读的测试文档、测试程序等。评估者应拥有开发者提供的有用的测试结果以补充测试过程。要求开发者所提供的用于测试的 TCB 应与测试相一致，并提供一个与开发者的 TSF 功能测试中使用的资源相等的集合。

c） 完全独立性测试，应通过重复所有开发者的测试来表明所有安全功能按规定执行。除了要求评估者应执行测试文档内的所有测试，以验证开发者的测试结果外，其余要求与抽样独立性测试。

### 5.2.7 脆弱性评定

#### 5.2.7.1 隐蔽信道分析

应确定并标识出 TCB 中非预期的信号通道的存在性，及其潜在的容量。通道容量的估计是基于非形式化的工程度量和实际的测量。隐蔽信道分析所基于的假设可以包括处理器速度、系统或网络配置、

内存大小和缓存大小等。

隐蔽信道分析是建立在 TCB 的实现、管理员指南、用户指南以及完整定义的外部接口等基础上的。隐蔽信道分析可以是一般性的，也可以是系统化的，或者是严格的，其要求如下：

a） 一般性的隐蔽信道分析，应通过对隐蔽信道的非形式化搜索，标识出可标识的隐蔽信道，为此要求：

——对每个信息流控制策略都应搜索隐蔽信道，并提供隐蔽信道分析的文档；

——分析文档应标识出隐蔽信道并估计它们的容量；

——分析文档应描述用于确定隐蔽信道存在的过程，以及进行隐蔽信道分析所需要的信息；

——分析文档应描述隐蔽信道分析期间所作的全部假设；

——分析文档应当描述最坏的情况下对通道容量进行估计的方法；

——分析文档应当为每个可标识的隐蔽信道描述其最坏的利用情形。

b） 系统化的隐蔽信道分析，应通过对隐蔽信道的系统化搜索，标识出可标识的隐蔽信道。为此，要求开发者以结构化、可重复的方式标识出隐蔽信道。除上述一般性隐蔽信道分析要求外，还要求分析文档提供证据证明用于标志隐蔽信道的方法是系统化的。

c） 彻底的隐蔽信道分析，应通过对隐蔽信道的穷举搜索，标识出可标识的隐蔽信道。为此，要求开发者提供额外的证据，证明对隐蔽信道的所有可能的搜索方法都已执行。其具体要求与系统化隐蔽信道分析要求相同。

#### 5.2.7.2 防止误用

应防止对 TCB 以不安全的方式进行使用或配置而不为人们所察觉。为此，应使对 TCB 的无法检测的不安全配置和安装，操作中人为的或其它错误造成的安全功能解除、无效或者无法激活，以及导致进入无法检测的不安全状态的风险达到最小。要求提供指导性文档，以防止提供冲突、误导、不完备或不合理的指南。指导性文档应满足以下要求：

a） 指南检查，要求指导性文档应：

——包括安装、生成和启动过程、非形式化功能设计、管理员指南和用户指南等；

——明确说明对 TCB 的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果，以及对于保持安全操作的意义；

——是完备的、清晰的、一致的、合理的，应列出所有目标环境的假设，并列出所有外部安全措施（包括外部过程的、物理的或人员的控制）的要求。

b） 分析确认，在指南检查的基础上，应文档化指导性文档，并要求分析文档应阐明指导性文档是完备的。

c） 对安全状态的检测和分析，在分析确认的基础上，还应进行独立测试，以确定管理员或用户在理解指导性文档的情况下能基本判断 TCB 是否在不安全状态下配置或运行。

#### 5.2.7.3 TCB 安全功能强度

应通过对安全机制的安全行为的合格性分析或统计的分析结果，以及为克服脆弱性所付出的努力得到 TCB 安全功能强度的说明。为了对安全功能强度进行评估，应对安全目标中标识的每个具有 TCB 安全功能强度声明的安全机制进行 TCB 安全功能强度的分析，证明该机制达到或超过安全目标要求所定义的最低强度，并证明该机制达到或超过安全目标要求所定义的特定功能强度。

#### 5.2.7.4 脆弱性分析

应能够发现缺陷的威胁。这些缺陷会导致对资源的非授权访问，对 TCB 安全功能的影响或改变，或者干涉其它授权用户的权限。根据不断增加的严格性，脆弱性分析分为：

a） 开发者脆弱性分析，应确定明显的安全脆弱性的存在，并确认在所期望的 TCB 环境下所存在的脆弱性不会被利用。为此，应通过搜索用户能违反 TSP 的明显途径，文档化 TCB 明显的脆弱性分布。对所有已标识的脆弱性，文档应说明在所期望的 IT 环境中无法利用这些脆弱性。

b） 独立脆弱性分析，评估者通过独立穿透测试，确定 TCB 可以抵御的低级攻击能力攻击者发起的穿透性攻击。为此，除满足开发者脆弱性分析要求外，还要求所提供的文档应当证明对于具有已标识脆弱性的 TCB 可以抵御明显的穿透性攻击。评估者则应进一步实施独立的脆弱性分析，并在此基础上实施独立的穿透性测试，以确定在所期望环境下额外标识的脆弱性的可利用性。

c） 中级抵抗力，在独立脆弱性分析的基础上，要求所提供的证据应说明对脆弱性的搜索是系统化的。评估者则应确定可以抵御中级攻击能力攻击者发起的对 TCB 的穿透性攻击。

d） 高级抵抗力，在中级抵抗力的基础上，要求所提供的分析文档应表明该分析完备地表述了 TCB 的脆弱性。评估者则应确定可以抵御高级攻击能力攻击者发起的对 TCB 的穿透性攻击。

### 5.3 TCB 安全管理

#### 5.3.1 TSF 功能的管理

应允许授权用户对 TSF 中的安全功能行为进行控制管理。为此，应允许授权用户使用规则或指定的可管理条件，管理 TSF 中的功能行为，有限制地提供授权用户对功能表所列功能进行行为判断、行为使能、行为不能或修改的能力，从而使授权用户能够建立和控制 TCB 的安全操作。这些管理典型地分为:

a) 与相应的 TCB 的访问控制、可查性和鉴别控制相关的功能的管理；

b) 与可用性的控制相关的功能的管理；

c) 与一般的安装和配置有关的功能的管理；

d) 与路径控制和 TCB 资源维护有关的功能的管理。

#### 5.3.2 安全属性的管理

应允许特定用户管理标识的安全属性。在没有专门指定某个值为安全属性时，用缺省值（默认值）作为安全属性值。 缺省值在参数初始过程中获得。

PP 应列出安全属性所适用的访问控制 SFP 表，并规定对指定安全属性的操作，规定哪些用户能“创建”、查询、修改安全属性，修改缺省值，删除整个安全属性或定义他们自己的操作，或执行的其他操作。

安全属性的管理包括：

a） 管理安全属性，应通过执行访问控制 SFP，有限制地提供标识的授权用户对由安全属性表所表示的安全属性进行查询、修改、删除、修改缺省值或其它操作的能力。

b） 安全的安全属性，应确保安全属性只接受安全的值，即确保分配给安全属性的值，其安全状态是有效的，从而保证任何可以接受的安全属性的组合处在一个安全的状态中。“安全”的定义应在 TCB 指南和 TSP 模型中给出。PP 应提供安全值的清晰定义和认为它们安全的理由。安全的安全属性包含了对安全属性的赋值要求。其赋值应使 TCB 保持安全的状态。“安全”的定义应由 TCB 的开发者在有关文档中给出。例如：如果一个用户账号已经创建，它应该有一个有效的口令。

c） 静态属性初始化，应为相关客体安全属性提供缺省值，并确保安全属性的缺省值适用于许可的或受限的情况。如果存在一种机制允许在创建时指定许可，一个新客体在创建时会有不同的安全属性。PP 应列出安全属性所适用的访问控制 SFP 表，并选择访问控制属性的缺省值是

否是受限的、许可的还是其它。

### 5.3.3 TSF 数据的管理

应对 TSF 数据进行管理。例如，作为 TSF 数据的审计跟踪信息，应规定谁能读、删除或创建审计跟踪。TSF 数据管理包括：

a） 管理 TSF 数据，应允许授权用户管理 TSF 数据的值，当没有专门指定某个值时，用在参数创建过程中提供的缺省值作为默认值。PP 应规定对指定 TSF 数据的操作，规定授权用户能清除、查询、修改 TSF 数据，修改默认值，或整个删除 TSF 数据。“清除”TSF 数据意味着 TSF 数据的内容被取消,但是该实体本身还保留在系统内。PP 还应规定授权用户能够执行的其他操作（如“创建” TSF 数据），规定能被授权用户操作的 TSF 数据，规定可以被管理的缺省值，以及规定哪个用户被允许操作 TSF 数据。

b） TSF 数据界限的管理，应规定对 TSF 数据的限制，以及当超过这些限制时所要采取的行动。例如，允许定义对审计记录大小的限制，以及规定当这些限制被超越时，所要采取的行动。PP 应规定受限的 TSF 数据及其限制值（如用户登录数），并应规定允许哪些用户修改 TSF 数据的界限及如何修改界限，还应规定对 TSF 数据所规定的限制被超过时，所要采取的行动（如通知授权用户和生成审计记录等）。

c） 安全的 TSF 数据，应确保分配给 TSF 数据的值，其安全状态是有效的，即要求所赋值应使 TCB 保持在安全的状态中。“安全”的定义由 TCB 的开发者在有关文档中给出，并说明认为它们安全的理由。

### 5.3.4 安全角色的定义与管理

应通过对用户给以不同的角色配置，确定这些角色的安全管理能力，其中包括：

a） 安全角色的定义，应能维护标识的授权角色，并把用户与该角色关联起来，应明确定义并识别不同的角色。通常系统应该区分客体的拥有者、管理员和其它用户。具有较高安全保护等级的系统要求将安全员、审计员和系统管理员进行明确定义。PP 应规定对安全而言用户可能拥有又被系统识别的角色。

b） 安全角色的限制，应能维护标识的授权角色，并把用户与该角色关联起来，同时应确保不同的角色满足不同的条件，并规定角色详细说明及控制角色之间关系的规则。通常系统应明确实体的拥有者、管理员和其它用户所受的限制。具有较高安全保护等级的系统应按“最小授权原则”明确安全员、审计员和系统管理员所受的限制。PP 应规定能被系统识别的角色，并规定控制角色赋值的条件。例如，“一个帐号的用户不能同时具有审计员和管理员角色，或具有助理角色的用户也必须具有拥有者角色等。”

c） 安全角色的担任，应向 TSF 明确提出担任某角色的请求。PP 应规定要求成为特定角色（如审计者和管理员等）的请求。

### 5.3.5 安全属性终止

应有对标识的授权用户按支持有效期的安全属性表的规定实施有效期的能力，并在超过了指定的有效期后，能根据活动表的规定采取必要的动作。PP 应提供支持终止的安全属性清单（如，用户的安全许可证），规定允许修改 TSF 中安全属性的角色，提供在每个安全属性到达终止期时所要采取的行动的清单（例如，当用户安全许可证到期时，将它设置为 TCB 上最低级别的许可证或作“立即撤消”处理）。

### 5.3.6 安全属性撤消

应对 TSC 内标识的授权角色，有限制地提供其撤消与用户、主体、客体、及其它附加资源相关联

的安全属性的能力，定义对 TCB 内各种实体安全属性的撤消，规定对撤消权限的要求，并对撤消规则有详细的说明。例如，撤消可能发生在用户下次登录时、下次试图打开该文件时或在某一固定时间段内。对具有时限授权的安全属性，TSF 应能够在超过指定的安全属性有效期后将其撤消。PP 应规定是否有从用户、主体、客体或其它任何由 TSF 提供的资源中撤消安全属性的能力。对从 TSF 提供的资源中撤消安全属性的情况，应进一步用细化操作定义该资源。PP 还应规定允许修改 TSF 功能的角色，并规定撤消规则。

## 6 安全保护等级划分要求

本章按《准则》对各个安全保护等级的不同要求，分别从安全功能和安全保证两方面，对其技术要求作详细描述。表 1 计算机信息系统安全保护等级安全功能技术要求，给出了每一个安全保护等级应达到的安全功能技术要求；表 2 计算机信息系统安全保护等级安全保证技术要求，给出了每一个安全保护等级应达到的安全保证技术要求。

表 1　计算机信息系统安全保护等级安全功能技术要求

| 安全功能技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 4.1 物理安全 | * | * | * | * | * |
| 4.1.1 环境安全 | * | * | * | * | * |
| 4.1.1.1 中心机房的安全保护 | * | * | * | * | * |
| 4.1.1.1.1 机房场地选择 | * | * | * | * | * |
| a）基本要求 | * | * | | * | * |
| b）较高要求 | | | * | * | * |
| c）严格要求 | | | | * | * |
| 4.1.1.1.2 机房内部安全防护 | * | * | * | * | * |
| a）基本要求 | * | * | | * | * |
| b）较高要求 | | | * | * | * |
| c）严格要求 | | | | * | * |
| 4.1.1.1.3 机房防火 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.1.1.4 机房供配电 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.1.1.5 机房空调降温 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.1.1.6 机房防水与防潮 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.1.1.7 机房防静电 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.1.1.8 机房接地与防雷击 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.1.1.9 机房电磁防护 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 1　计算机信息系统安全保护等级安全功能技术要求（续 1）

| 安全功能技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 4.1.1.2 通信线路的安全防护 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.2 设备安全 | * | * | * | * | * |
| 4.1.2.1 设备的防盗和防毁 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.2.2 设备的安全可用 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.3 记录介质安全 | * | * | * | * | * |
| a）基本要求 | * | * | | | |
| b）较高要求 | | | * | | |
| c）严格要求 | | | | * | * |
| 4.1.4 安全管理中心安全 | | | * | * | * |
| 4.2 运行安全 | * | * | * | * | * |
| 4.2.1 风险分析 | * | * | * | * | * |
| 4.2.2 系统安全性检测分析 | * | * | * | * | * |
| a）操作系统安全性检测分析 | * | * | * | * | * |
| b）数据库管理系统安全性检测分析 | * | * | * | * | * |
| c）网络安全性检测分析 | | * | * | * | * |
| d）防火墙安全性检测分析 | | | * | * | * |
| e）电磁泄露检测分析 | | | * | * | * |
| 4.2.3 网络安全监控 | | | * | * | * |
| a）设置分布式探测器 | | | * | * | * |
| b）设置安全监控中心 | | | * | * | * |
| 4.2.4 安全审计 | | * | * | * | * |
| 4.2.4.1 安全审计的自动响应 | | * | * | * | * |
| a）实时报警的生成 | | * | * | * | * |
| b）违例进程的终止 | | | * | * | * |
| c）服务的取消 | | | | * | * |
| d）用户帐号的断开与失效等 | | | | | * |
| 4.2.4.2 安全审计数据产生 | | * | * | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 1　计算机信息系统安全保护等级安全功能技术要求（续 2）

| 安全功能技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 4.2.4.3 安全审计分析 | | * | * | * | * |
| a）潜在侵害分析 | | * | * | * | * |
| b）基于异常检测的描述 | | | * | * | * |
| c）简单攻击探测 | | | | * | * |
| d）复杂攻击探测 | | | | | * |
| 4.2.4.4 安全审计查阅 | | * | * | * | * |
| a）审计查阅 | | * | * | * | * |
| b）有限审计查阅 | | * | * | * | * |
| c）可选审计查阅 | | | * | * | * |
| 4.2.4.5 安全审计事件选择 | | * | * | * | * |
| 4.2.4.6 安全审计事件存储 | | * | * | * | * |
| a）受保护的审计踪迹存储 | | * | * | * | * |
| b）审计数据的可用性确保 | | | * | * | * |
| c）在审计数据可能丢失情况下的措施 | | | | * | * |
| d）防止审计数据丢失 | | | | | * |
| 4.2.4.7 网络环境安全审计与评估 | | | * | * | * |
| 4.2.5 网络防病毒 | * | * | * | * | * |
| a）严格管理 | * | * | * | * | * |
| b）防杀结合 | * | * | * | * | * |
| c）整体防御 | | | * | * | * |
| d）防管结合 | | | | * | * |
| e）多层防御 | | | | * | * |
| 4.2.6 备份与故障恢复 | * | * | * | * | * |
| 4.2.6.1 备份 | * | * | * | * | * |
| a）用户自我信息备份 | * | * | * | * | * |
| b）增量信息备份 | * | * | * | * | * |
| c）局部系统备份 | | * | * | * | * |
| d）热备份 | | * | * | * | * |
| e）全系统备份 | | | * | * | * |
| f）主机系统远地备份 | | | | * | * |
| 4.2.6.2 故障恢复 | * | * | * | * | * |
| a）手动恢复 | * | * | * | * | * |
| b）自动恢复 | | | * | * | * |
| c）无过分丢失的自动恢复 | | | | * | * |
| d）灾难性恢复 | | | | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 1　计算机信息系统安全保护等级安全功能技术要求（续 3）

| 安全功能技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 4.2.7 计算机信息系统的应急计划和应急反应 | | * | * | * | * |
| a）具有各种安全措施 | | * | * | * | * |
| b）设置正常备份机制 | | * | * | * | * |
| c）健全安全管理机构 | | | * | * | * |
| d）建立处理流程图 | | | | * | * |
| 4.3 信息安全 | * | * | * | * | * |
| 4.3.1 标识和鉴别 | * | * | * | * | * |
| 4.3.1.1 数据鉴别 | | | * | * | * |
| a）基本数据鉴别 | | | * | | |
| b）伴有保证者身份的数据鉴别 | | | | * | * |
| 4.3.1.2 用户标识 | * | * | * | * | * |
| a）同步标识 | * | * | * | * | * |
| b）动作前标识 | | * | * | * | * |
| 4.3.1.3 标识用户的身份鉴别 | * | * | * | * | * |
| a）同步鉴别 | * | * | * | * | * |
| b）在任何动作之前鉴别 | | * | * | * | * |
| c）不可伪造鉴别 | | | * | * | * |
| d）一次性使用鉴别 | | | * | * | * |
| e）多机制鉴别 | | | | * | * |
| f）重鉴别 | | | | * | * |
| g）受保护的鉴别反馈 | | | | * | * |
| 4.3.1.4 鉴别失败 | * | * | * | * | * |
| 4.3.1.5 用户-主体绑定 | * | * | * | * | * |
| 4.3.2 信息交换用户的身份鉴别 | | * | * | * | * |
| 4.3.2.1 原发抗抵赖 | | * | * | * | * |
| a）选择性原发证明 | | * | * | | |
| b）强制性原发证明 | | | | * | * |
| 4.3.2.2 接收抗抵赖 | | * | * | * | * |
| a）选择性接收证明 | | * | * | | |
| b）强制性接收证明 | | | | * | * |
| 4.3.3 隐密 | | | | * | * |
| 4.3.3.1 匿名 | | | | * | * |
| 4.3.3.2 假名 | | | | * | * |
| 4.3.3.3 不可关联性 | | | | * | * |
| 4.3.3.4 不可观察性 | | | | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 1　计算机信息系统安全保护等级安全功能技术要求（续 4）

| 安全功能技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 4.3.4 标记 | | | * | * | * |
| 4.3.4.1 用户属性定义 | | | * | * | * |
| 4.3.4.2 客体属性定义 | | | * | * | * |
| 4.3.5 自主访问控制 | * | * | * | * | * |
| 4.3.5.1 访问控制策略 | * | * | * | * | * |
| a）子集访问控制 | * | * | * | | |
| b）完全访问控制 | | | | * | * |
| 4.3.5.2 访问控制功能 | * | * | * | * | * |
| a）子集访问控制 | * | * | * | | |
| b）完全访问控制 | | | | * | * |
| 4.3.6 强制访问控制 | | | * | * | * |
| 4.3.6.1 访问控制策略 | | | * | * | * |
| a）子集访问控制 | | | * | | |
| b）完全访问控制 | | | | * | * |
| 4.3.6.2 访问控制功能 | | | * | * | * |
| a）子集访问控制 | | | * | | |
| b）完全访问控制 | | | | * | * |
| 4.3.7 用户数据保密性存储保护 | * | * | * | * | * |
| a）自主访问控制 | * | * | * | * | * |
| b）强制访问控制 | | | * | * | * |
| c）数据加密存储 | | | * | * | * |
| 4.3.8 用户数据保密性传输保护 | * | * | * | * | * |
| 4.3.8.1 TCB 内部数据传输保护 | * | * | * | * | * |
| a）基本内部传输保护 | * | * | * | * | * |
| b）属性分隔传输保护 | | * | * | * | * |
| 4.3.8.2 TSF 间用户数据传输保护 | * | * | * | * | * |
| 4.3.8.3 向 TSC 之外输出数据 | | | * | * | * |
| a）不带安全属性的用户数据输出 | | | * | | |
| b）带有安全属性的用户数据输出 | | | | * | * |
| 4.3.8.4 从 TSC 之外输入数据 | | | * | * | * |
| a）不带安全属性的用户数据输入 | | | * | * | |
| b）带有安全属性的用户数据输入 | | | | * | * |
| 4.3.9 用户数据完整性保护 | | * | * | * | * |
| 4.3.9.1 存储数据的完整性 | | * | * | * | * |
| a）存储数据的完整性检测 | | * | | | |
| b）存储数据的完整性检测和恢复 | | | * | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 1　计算机信息系统安全保护等级安全功能技术要求（续 5）

| 安全功能技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 4.3.9.2 传输数据的完整性 | * | * | * | * | * |
| a）数据交换完整性检测 | * | * | * | * | * |
| b）源数据交换恢复 | | | * | | |
| c）目的数据交换恢复 | | | | * | * |
| 4.3.9.3 处理数据的完整性 | | * | * | * | * |
| a）基本回退 | | * | * | | |
| b）高级回退 | | | | * | * |
| 4.3.10 剩余信息保护 | | * | * | * | * |
| a）子集信息保护 | | * | * | | |
| b）完全信息保护 | | | | * | * |
| c）特殊信息保护 | | | | | * |
| 4.3.11 隐蔽信道分析 | | | | * | * |
| 4.3.11.1 一般性的隐蔽信道分析 | | | | * | |
| 4.3.11.2 系统化的隐蔽信道分析 | | | | | * |
| 4.3.11.3 彻底的隐蔽信道分析 | | | | | * |
| 4.3.12 用户与 TSF 间可信路径 | | | | * | * |
| 4.3.13 密码支持 | * | * | * | * | * |
| 4.3.13.1 密码分级 | * | * | * | * | * |
| a）第一级 | * | | | | |
| b）第二极 | | * | | | |
| c）第三级 | | | * | | |
| d）第四级 | | | | * | |
| e）第五级 | | | | | * |
| 4.3.13.2 密钥管理 | * | * | * | * | * |
| a）密钥产生 | * | * | * | * | * |
| b）密钥分配 | * | * | * | * | * |
| c）密钥访问 | * | * | * | * | * |
| d）密钥销毁 | * | * | * | * | * |
| 4.3.13.3 密码运算 | * | * | * | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 2　计算机信息系统安全保护等级安全保证技术要求

| 安全保证技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 5.1 TCB 自身安全保护 | * | * | * | * | * |
| 5.1.1 安全运行的测试 | * | * | * | * | * |
| 5.1.2 失败保护 | * | * | * | * | * |
| 5.1.3 输出 TSF 数据的可用性 | | | * | * | * |
| 5.1.4 输出 TSF 数据的保密性 | | | * | * | * |
| 5.1.5 输出 TSF 数据的完整性 | | | * | * | * |
| a）TSF 间修改的检测 | | | * | | |
| b）TSF 间修改的检测与改正 | | | | * | * |
| 5.1.6 TCB 内 TSF 数据传输 | * | * | * | * | * |
| a）内部 TSF 数据传输的基本保护 | * | * | * | * | * |
| b）TSF 数据传输分离 | | | * | * | * |
| c）TSF 数据完整性保护 | | | * | * | * |
| 5.1.7 物理安全保护 | * | * | * | * | * |
| 5.1.7.1 物理攻击的被动检测 | * | * | * | | |
| 5.1.7.2 物理攻击的自动报告 | | | * | * | * |
| 5.1.7.3 物理攻击抵抗 | | | | * | * |
| 5.1.8 可信恢复 | | | | | * |
| a）手动恢复 | | | | | * |
| b）自动恢复 | | | | | * |
| c）无过分丢失的自动恢复 | | | | | * |
| d）功能恢复 | | | | | * |
| 5.1.9 重复检测 | | | * | * | * |
| 5.1.10 参照仲裁 | | | * | * | * |
| 5.1.11 域分离 | | | * | * | * |
| a）TSF 域分离 | | | * | | |
| b）SFP 域分离 | | | | * | * |
| 5.1.12 状态同步协议 | | | * | * | * |
| a）简单的可信回执 | | | * | | |
| b）相互的可信回执 | | | | * | * |
| 5.1.13 时间戳 | * | * | * | * | * |
| 5.1.14 TSF 间的 TSF 数据的一致性 | | | * | * | * |
| 5.1.15 TCB 内 TSF 数据复制的一致性 | | | * | * | * |
| 5.1.16 TSF 自检 | * | * | * | * | * |
| 5.1.17 资源利用 | * | * | * | * | * |
| 5.1.17.1 故障容错 | * | * | * | * | * |
| a）降级故障容错 | * | * | * | * | * |
| b）受限故障容错 | | | * | * | * |
| 5.1.17.2 服务优先级 | * | * | * | * | * |
| a）有限服务优先级 | * | * | | | |
| b）全部服务优先级 | | | * | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 2　计算机信息系统安全保护等级安全保证技术要求（续 1）

| 安全保证技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 5.1.17.3 资源分配 | * | * | * | * | * |
| a）最大限额 | * | * | | | |
| b）最小和最大限额 | | | * | * | * |
| 5.1.18 TCB 访问控制 | * | * | * | * | * |
| a）可选属性范围限定 | * | * | * | * | * |
| b）多重并发会话限定 | * | * | * | * | * |
| c）会话锁定 | | | * | * | * |
| d）TCB 访问标签 | | | * | * | * |
| e）TCB 访问历史 | | * | * | * | * |
| f）TCB 会话建立 | * | * | * | * | * |
| 5.1.19 可信路径/信道 | | | | * | * |
| 5.1.19.1 TSF 间可信信道 | | | | * | * |
| 5.1.19.2 用户与 TSF 间可信路径 | | | | * | * |
| 5.2 TCB 设计和实现 | * | * | * | * | * |
| 5.2.1 配置管理 | * | * | * | * | * |
| 5.2.1.1 配置管理自动化 | | | * | * | * |
| 1）部分 CM 自动化 | | | * | * | |
| 2）完全 CM 自动化 | | | | | * |
| 5.2.1.2 配置管理能力 | * | * | * | * | * |
| a）版本号 | * | * | * | * | * |
| b）配置项 | | | * | * | * |
| c）授权控制 | | | * | * | * |
| d）生成支持和验收过程 | | | | * | * |
| e）进一步的支持 | | | | * | * |
| 5.2.1.3 配置管理范围 | | * | * | * | * |
| a）TCB 配置管理范围 | | * | * | * | * |
| b）问题跟踪配置管理范围 | | | * | * | * |
| c）开发工具配置管理范围 | | | | * | * |
| 5.2.2 分发和操作 | * | * | * | * | * |
| 5.2.2.1 分发 | * | * | * | * | * |
| a）分发过程 | * | * | * | * | * |
| b）修改检测 | | | * | * | * |
| c）修改防止 | | | | * | * |
| 5.2.2.2 操作（安装、生成和启动） | * | * | * | * | * |
| a）安装、生成和启动过程 | * | * | * | * | * |
| b）日志生成 | | * | * | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 2　计算机信息系统安全保护等级安全保证技术要求（续 2）

| 安全保证技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 5.2.3 开发 | * | * | * | * | * |
| 5.2.3.1 功能设计 | * | * | * | * | * |
| a）非形式化功能设计 | * | * | * | | |
| b）完全定义的外部接口 | | * | * | * | |
| c) 半形式化功能设计 | | | | * | |
| d）形式化功能设计 | | | | | * |
| 5.2.3.2 高层设计 | * | * | * | * | * |
| a）描述性高层设计 | * | * | | | |
| b）安全加强的高层设计 | | | * | | |
| c）半形式化高层设计 | | | | * | |
| d）半形式化高层解释 | | | | * | |
| e）形式化高层设计 | | | | | * |
| 5.2.3.3 实现表示 | * | * | * | * | * |
| a）TSF 子集实现 | * | * | | | |
| b）TSF 完全实现 | | | * | | |
| c）TSF 的结构化实现 | | | | * | * |
| 5.2.3.4 TSF 内部结构 | * | * | * | * | * |
| a）模块化 | * | * | * | * | * |
| b) 复杂性降低 | | * | * | | |
| c）复杂性最小化 | | | | * | * |
| 5.2.3.5 低层设计 | * | * | * | * | * |
| a）描述性低层设计 | * | * | * | | |
| b）半形式化低层设计 | | | | * | |
| c）形式化低层设计 | | | | | * |
| 5.2.3.6 表示的对应性 | * | * | * | * | * |
| a）非形式化对应性说明 | * | * | * | | |
| b）半形式化对应性说明 | | | | * | |
| c）形式化对应性说明 | | | | | * |
| 5.2.3.7 安全策略模型化 | | * | * | * | * |
| a）非形式化 TCB 安全策略模型 | | * | * | | |
| b）半形式化 TCB 安全策略模型 | | | | * | |
| c）形式化 TCB 安全策略模型 | | | | | * |
| 5.2.4 指导性文档 | * | * | * | * | * |
| 5.2.4.1 管理员指南 | * | * | * | * | * |
| 5.2.4.2 用户指南 | * | * | * | * | * |
| 5.2.5 生命周期支持 | | * | * | * | * |
| 5.2.5.1 开发安全 | | * | * | * | * |
| a）安全措施的说明 | | * | * | * | * |
| b）安全措施的充分性 | | | | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 2　计算机信息系统安全保护等级安全保证技术要求（续 3）

| 安全保证技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 5.2.5.2 缺陷纠正 | | | * | * | * |
| a）基本缺陷纠正 | | | * | | |
| b）缺陷报告 | | | | * | |
| c）系统缺陷纠正 | | | | | * |
| 5.2.4.3 生命周期定义 | * | * | * | * | * |
| a）开发者定义的生命周期模型 | * | * | | | |
| b）标准生命周期模型 | | | * | * | |
| c）可测量的生命周期模型 | | | | | * |
| 5.2.5.4 工具和技术 | | | * | * | * |
| a）明确定义的开发工具 | | | * | * | * |
| b）遵照实现标准-应用部分 | | | | * | |
| c）遵照实现标准-所有部分 | | | | | * |
| 5.2.6 测试 | * | * | * | * | * |
| 5.2.6.1 范围 | | * | * | * | * |
| a）范围的证据 | | * | * | * | * |
| b）范围分析 | | * | * | | |
| c）严格的范围分析 | | | | * | * |
| 5.2.6.2 测试深度 | | * | * | * | * |
| a）高层设计测试 | | * | * | * | * |
| b）低层设计测试 | | | * | * | * |
| c）实现表示测试 | | | | * | * |
| 5.2.6.3 功能测试 | * | * | * | * | * |
| a）一般功能测试 | * | * | * | | |
| b）顺序的功能测试 | | | * | * | * |
| 5.2.6.4 独立性测试 | * | * | * | * | * |
| a）相符性独立测试 | * | * | * | * | * |
| b）抽样独立性测试 | | | * | * | * |
| c）完全独立性测试 | | | | | * |
| 5.2.7 脆弱性评定 | | * | * | * | * |
| 5.2.7.1 隐蔽信道分析 | | | | * | * |
| a）一般性的隐蔽信道分析 | | | | * | |
| b）系统化的隐蔽信道分析 | | | | * | |
| c）彻底的隐蔽信道分析 | | | | | * |
| 5.2.7.2 防止误用 | | * | * | * | * |
| a）指南检查 | | * | * | * | * |
| b）分析确认 | | | * | * | * |
| c）对安全状态的检测和分析 | | | | * | * |
| 5.2.7.3 TCB 安全功能强度评估 | | * | * | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

表 2　计算机信息系统安全保护等级安全保证技术要求（续 4）

| 安全保证技术要求 | 安全保护等级 | | | | |
|---|---|---|---|---|---|
| | 用户自主保护级 | 系统审计保护级 | 安全标记保护级 | 结构化保护级 | 访问验证保护级 |
| 5.2.7.4 脆弱性分析 | | * | * | * | * |
| a）开发者脆弱性分析 | | * | * | * | * |
| b）独立脆弱性分析 | | | * | * | * |
| c）中级抵抗力 | | | | * | * |
| d）高级抵抗力 | | | | | * |
| 5.3 TCB 安全管理 | * | * | * | * | * |
| 5.3.1 TSF 功能的管理 | * | * | * | * | * |
| 5.3.2 安全属性的管理 | | | * | * | * |
| a）管理安全属性 | | | * | * | * |
| b）安全的安全属性 | | | * | * | * |
| c）静态属性初始化 | | | * | * | * |
| 5.3.3 TSF 数据的管理 | | | * | * | * |
| a）管理 TSF 数据 | | | * | * | * |
| b）TSF 数据界限的管理 | | | * | * | * |
| c）安全的 TSF 数据 | | | | * | * |
| 5.3.4 安全角色的定义与管理 | * | * | * | * | * |
| a）安全角色的定义 | * | * | * | * | * |
| b）安全角色的限制 | | | * | * | * |
| c）安全角色的担任 | | | * | * | * |
| 5.3.5 安全属性终止 | | | * | * | * |
| 5.3.6 安全属性撤消 | | | * | * | * |
| 注：“*”号表示具有该要求。 | | | | | |

以下对每一安全保护等级的具体技术要求分别进行描述。其中**加粗宋体**表示所描述的内容在该级中第一次出现。

## 6.1　第一级　用户自主保护级

### 6.1.1　物理安全

**应按照 4.1 条中环境安全、设备安全及记录介质安全所描述的基本要求，进行计算机、网络的硬件及相关环境的设计。**

### 6.1.2　运行安全

#### 6.1.2.1　风险分析

**应按照 4.2.1 条所描述的要求，结合所要设计的计算机信息系统的安全需求，明确用户自主保护级的计算机信息系统安全设计所要解决的问题。**

#### 6.1.2.2　系统安全性检测分析

**应按照 4.2.2 条操作系统安全性检测分析和数据库安全性检测分析的要求，运用有关工具，检测所选用的操作系统和数据库系统的安全性，并结合计算机信息系统系统的安全要求加以改进。**

#### 6.1.2.3　网络防病毒

**应按照 4.2.5 条严格管理和防杀结合的要求，选择合适的病毒防杀产品，实现计算机信息系统的病毒防治。**

6.1.2.4 备份与故障恢复

应按照 **4.2.6.1** 条用户自我信息备份和增量备份的要求，设计备份功能，按照 **4.2.6.2** 条手动恢复的描述，设计恢复功能，以便在计算机信息系统发生故障时进行必要的恢复工作。

6.1.3 信息安全

6.1.3.1 用户标识

应按照 **4.3.1.2** 条同步标识的描述，设计用户标识功能。一般以用户名和用户标识符（UID）来标识一个用户，确保在一个计算机信息系统中用户名和用户标识符的唯一性，并由此确保用户的唯一性和可区别性。

6.1.3.2 用户鉴别

应按照 **4.3.1.3** 条同步鉴别的描述，设计标识用户的身份鉴别功能，并按照 **4.3.1.4** 条和 **4.3.1.5** 条的要求进行进行鉴别失败和用户主体-绑定的处理。

鉴别应确保用户身份的真实性。本级要求：

a) 采用口令进行鉴别，并在每次用户登录系统时进行鉴别。口令应是不可见的，并在存储时按 4.3.13 条密码支持第一级的要求进行保护。

b) 对跨网络的远程用户，当口令在网上传输时应进行适当的保护。

c) 对以浏览方式进入系统的非注册用户，应设置特殊的用户身份，并与访问控制相结合，严格控制其对写操作的执行。

6.1.3.3 自主访问控制

应按照 **4.3.5.1** 条子集访问控制策略所描述的要求，并按照 **4.3.5.2** 条子集访问控制功能所描述的要求，设计和实现所需要的自主访问控制功能。

目前常用的自主访问控制策略，按照主体与客体的关系，即客体为主体的拥有者/同组/其它，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定主体对客体的访问权限。

本安全级中，无论采用何种访问控制策略所实现的自主访问控制功能，都要求能够：

a) 允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取敏感信息。

b) 对访问是跨网络的情况，可以设计成一个跨网络的 TCB，也可以设计成两个 TCB。前者对传输中的数据保护应按照 4.3.8.1 条基本内部传输保护的要求进行设计；后者对传输中的数据保护则应按照 4.3.8.2 条所描述的要求进行设计，并根据 4.3.13 条密码支持第一级的要求保证数据在通过网络传输时的保密性和完整性。

c) 对访问是非注册用户，如通用浏览器的情况，应重点考虑对其写访问的严格控制。

6.1.3.4 数据完整性

a) 传输数据完整性保护，应按照 4.3.9.2 条数据交换完整性检测的要求，采用 4.3.13 条密码支持第一级所提供的功能，设计相应的 TCB 安全功能模块，对经过网络在两个 TCB 间传输的用户数据进行完整性保护。本级要求 TCB 提供监视用户数据完整性的功能，即能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警。

6.1.4 TCB 自身安全保护

6.1.4.1 TSF 保护

应提供与 TSF 机制的完整性和管理有关的保护，也应提供与 TSF 数据的完整性有关的保护。本级中，TSF 保护的设计应：

a) 按 5.1.1 条所描述的内容，实现在系统初始化期间对 TSF 安全假定的正确运行的测试；

b) 按 5.1.2 条所描述的内容，实现对 TSF 出现失败时的处理；

c) 按 5.1.6 条内部 TSF 数据传输的基本保护所描述的要求，实现对 TSF 数据的传输保护；

d) 按 5.1.7 条物理攻击的被动检测所描述的要求，实现对 TCB 的物理安全保护；

e) 按 5.1.13 条时间戳的要求，为 TCB 的运行提供可靠的时间戳支持；

f) 按 5.1.16 条的要求，实现 TSF 在启动时的自检。

6.1.4.2 资源利用

应通过故障容错、服务优先级和资源分配来增强 TCB 自身的安全性。

在本级中，资源利用的设计应：

a) 按 5.1.17.1 条降级故障容错的要求，实现 TCB 对指定故障的处理；

b) 按 5.1.17.2 条有限服务优先级的要求，进行 TCB 资源的管理和分配；

c) 按 5.1.17.3 条最大限额的要求，进行 TCB 资源的管理和分配。

6.1.4.3 TCB 访问控制

应通过对会话安全属性、多重并发会话限定、会话锁定、TCB 访问标签、TCB 访问历史和会话建立的管理，来确保 TCB 自身的安全性。

本级中，TCB 访问控制的设计应：

a) 按 5.1.18 条可选属性范围限定的要求，对用以建立会话的安全属性的范围进行限制；

b) 按 5.1.18 条多重并发会话限定的要求，进行会话管理的限定；

c) 按 5.1.18 条 TCB 会话建立所描述的要求，实现对会话建立管理的设计。

6.1.5 TCB 设计和实现

6.1.5.1 配置管理

应按照 5.2.1 条的要求进行设计。本级要求具有基本的配置管理能力，即按照 5.2.1.2 条版本号的要求，使用户所使用的版本号与 TCB 样本完全一致。

6.1.5.2 分发和操作

应以文档形式提供对 TCB 安全地进行分发以及安装、生成和启动的过程进行说明。具体要求为：

a) 按 5.2.2.1 条分发过程的要求编制说明；

b) 按 5.2.2.2 条安装、生成和启动过程所描述的要求编制说明。

6.1.5.3 开发

应按照 5.2.3 条所描述的对开发的要求进行 TCB 设计。本级要求：

a) 按 5.2.3.1 条非形式化功能设计的要求进行功能设计；

b) 按 5.2.3.2 条描述性高增设计的要求进行高层设计；

c) 按 5.2.3.3 条 TSF 子集实现的要求进行实现表示设计；

d) 按 5.2.3.4 条模块化的要求进行内部结构设计；

e) 按 5.2.3.5 条描述性低层设计的要求进行低层设计；

f) 按 5.2.3.6 条非形式化对应性的要求进行对应性设计。

6.1.5.4 指导性文档

应按照 5.2.4 条对管理员指南和用户指南的要求设计文档。本级要求根据上述配置管理、分发和操作、开发以及测试等方面的要求提供管理员指南和用户指南。

6.1.5.5 生命周期支持

应按照 5.2.5 条所描述的要求进行 TCB 设计。本级要求按 5.2.5.3 条开发者定义的生命周期模型所描述的要求进行 TCB 的开发设计。

6.1.5.6 测试

**应按照 5.2.6 条所描述的要求对所开发的 TCB 进行测试。本级要求按照 5.2.6.3 条一般功能测试的要求和 5.2.6.4 条相符性独立测试的要求进行测试。**

6.1.6 TCB 安全管理

**应根据本级中安全功能技术要求所涉及的物理安全、运行安全、信息安全和安全保证技术要求所涉及的 TCB 自身安全与 TCB 设计和实现等有关内容，按照 5.3 条 TCB 安全管理所描述的要求，设计 TCB 安全管理。本级应按以下要求制定相应的操作、运行规程和行为规章制度：**

**a) 5.3.1 条 TSF 的功能管理的要求；**

**b) 5.3.4 条安全角色的定义所描述的要求。**

6.2 第二级 系统审计保护级

6.2.1 物理安全

应按照 4.1 条中环境安全、设备安全及记录介质安全所描述的基本要求，进行计算机、网络的硬件及相关环境的设计。

6.2.2 运行安全

6.2.2.1 风险分析

应按照 4.2.1 条所描述的要求，结合所要设计的计算机信息系统的安全需求，明确**系统审计保护级**的计算机信息系统安全设计所要解决的问题。

6.2.2.2 系统安全性检测分析

应按照 4.2.2 条对操作系统安全性检测分析、数据库安全性检测分析和**网络安全性检测分析**的要求，运用有关工具，检测所选用的操作系统、数据库管理系统和**网络系统**的安全性，并结合计算机信息系统系统的安全要求对其安全性加以改进。

6.2.2.3 审计

**应按照 4.2.4 条对审计的要求进行设计。本级的审计主要是提供可查性，要求对审计功能的设计应与用户标识与鉴别、自主访问控制、客体重用、数据完整性等安全功能的设计紧密结合，按照审计功能设计的总要求和各安全功能技术要求中的具体审计要求来进行。本级要求：**

**a) 按 4.2.4.1 条实时报警的生成的要求，设计自动响应功能；**

**b) 按 4.2.4.2 条的要求产生审计数据；**

**c) 按 4.2.4.3 条潜在侵害分析的要求进行审计分析设计；**

**d) 按 4.2.4.4 条审计查阅和有限审计查阅的要求进行安全审计查阅设计；**

**e) 按 4.2.4.5 条的要求提供对审计事件的选择；**

**f) 按 4.2.4.6 条受保护的审计踪迹存储的要求来保存审计事件。**

6.2.2.4 网络防病毒

应按照 4.2.5 条网络防病毒中严格管理和防杀结合的要求，选择合适的病毒防杀产品实现计算机信息系统的病毒防杀工作。

6.2.2.5 备份与故障恢复

应按照 4.2.6.1 条有关用户自我信息备份、增量备份、**局部系统备份和热备份**的要求，设计备份功能，按照 4.2.6.2 条手动恢复的描述，设计恢复功能，以便在计算机信息系统发生故障时进行必要的恢复工作。

6.2.2.6 应急计划与应急反应

**应按照 4.2.7 条具有各种安全措施和设置正常备份机制的要求，结合系统审计保护级对计算机信**

**息系统安全的具体要求，设计和制定应急计划和应急措施，明确计算机信息系统出现各种情况时应采取的措施。**

6.2.3 信息安全

6.2.3.1 用户标识

应按照 4.3.1.2 条有关同步标识和**动作前标识**的描述，设计用户标识功能。一般以用户名和用户标识符（UID）来标识一个用户，确保在一个计算机信息系统中用户名和用户标识符的唯一性。**这种唯一性应在计算机信息系统的整个生命周期内都有效，即使一个用户的帐号已被删除，他的用户名和标识符也不能再使用，**并由此确保用户的唯一性和可区别性。

6.2.3.2 用户鉴别

应按照 4.3.1.3 条同步鉴别和**在任何动作之前鉴别**的描述，设计标识用户的身份鉴别功能，并按照 4.3.1.4 条鉴别失败和 4.3.1.5 条的有关要求进行相关问题的处理。

鉴别应确保用户身份的真实性。本级要求：

a) 采用口令进行鉴别，并在每次用户登录系统时进行鉴别。口令应是不可见的，并在存储和**传输时按 4.3.13 条密码支持第二级的要求进行**保护。

b) 对跨网络的远程用户，当口令在网上传输时应按 **4.3.13 条密码支持第二级**的要求进行保护。

**c) 在以交换方式引起信息流动时，TCB 应提供通信双方身份的真实性和双方对信息交换行为的不可抵赖性。对信息的发送方，TCB 应按 4.3.2.1 条选择性原发证明的要求进行设计；对信息的接收方，TCB 应按 4.3.2.2 条选择性接收证明的要求进行设计。这种安全通信的抗抵赖功能应以 PKI 为基础的 CA 认证系统作为可信第三方来支持。CA 系统所采用的密码算法应按 4.3.13 条密码支持第二级的要求进行设计。**

6.2.3.3 自主访问控制

应按照 4.3.5.1 条子集访问控制策略所描述的要求，并按照 4.3.5.2 条子集访问控制功能所描述的要求，设计和实现所需要的自主访问控制功能。

目前常用的自主访问控制策略，按照主体与客体的关系，即客体为主体的拥有者/同组/其它，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定主体对客体的访问权限。

**在本安全级中**，要求无论采用何种访问控制策略所实现的访问控制功能，都能够：

a) 允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取敏感信息。

**b) 有更细粒度的自主访问控制，即对 TSC 内的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。**

**c) 要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。**

d) 对访问是跨网络的情况，可以设计成一个跨网络的 TCB，也可以设计成两个 TCB。前者对传输中的数据保护应按照 4.3.8.1 条基本内部传输保护的要求进行设计；后者对传输中的数据保护则应按照 4.3.8.2 条所描述的要求进行设计，根据 **4.3.13 条密码支持第二级的要求**保证数据在通过网络传输时的保密性和完整性。

e) 对访问是非注册用户，如通用浏览器的情况，应重点考虑对其写访问的严格控制。

6.2.3.4 客体重用

**应按照 4.3.10 条子集信息保护的要求进行设计。这里的客体主要是指存放信息的介质，如内存、外存（主要指磁盘）、软盘、可擦写光盘等。而客体重用则着重考虑这些存储介质作为计算机系统资源被动态分配时，应确保曾经在介质中存放过的信息不因这种动态分配而遭泄露。本级要求对 TSC 内的存储资源进行重新分配时，确保其残留信息全部被清除。**

6.2.3.5 数据完整性

a) **存储数据完整性保护，应按照 4.3.9.1 条完整性检测的要求，通过 4.3.13 条密码支持第二级所提供的功能，采用自主完整性策略设计相应的 TCB 安全功能模块，对存储在 TCB 安全控制范围内的用户数据进行完整性保护。本级要求在适当的时候检测存储在 TCB 控制范围之内的用户数据是否出现完整性错误，并进行报警。**

b) 传输数据完整性保护，应按照 4.3.9.2 条数据交换完整性检测的要求设计相应的 TCB 安全功能模块，对经过网络在两个 TCB 间传输的用户数据进行完整性保护。本级要求 TCB 能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警，**还要求通过 4.3.13 条密码支持第二级所提供的功能，对加密传输的数据进行传输数据的完整性检验。**

c) **处理数据完整性保护，应按照 4.3.9.3 条基本回退的要求设计相应的 TCB 安全功能模块，通过在各种异常情况的事务回退，以事务的完整性确保数据的完整性。**

6.2.4 TCB 自身安全保护

6.2.4.1 TSF 保护

应提供与 TSF 机制的完整性和管理有关的保护，也应提供与 TSF 数据的完整性有关的保护。

本级中，TSF 保护的设计应：

a) 按 5.1.1 条所描述的内容，实现在系统初始化期间对 TSF 安全假定的正确运行的测试；

b) 按 5.1.2 条所描述的内容，实现对 TSF 出现失败时的处理；

c) 按 5.1.6 条内部 TSF 数据传输的基本保护所描述的相关内容的要求，实现对 TSF 数据的传输保护；

d) 按 5.1.7 条物理攻击的被动检测所描述的要求，实现对 TCB 的物理安全保护；

e) 按 5.1.13 条时间戳的要求，为 TCB 的运行提供可靠的时间戳支持；

f) 按 5.1.16 条 TSF 自检的相关要求，实现 TSF 在启动时的自检。

6.2.4.2 资源利用

应通过故障容错、服务优先级和资源分配来增强 TCB 自身的安全性。

在本级中，资源利用的设计应：

a) 按 5.1.17.1 条降级故障容错的要求，实现 TCB 对指定故障的处理；

b) 按 5.1.17.2 条有限服务优先级的要求，进行 TCB 资源的管理和分配；

c) 按 5.1.17.3 条最大限额的要求，进行 TCB 资源的管理和分配。

6.2.4.3 TCB 访问控制

应通过对会话安全属性、多重并发会话限定、会话锁定、TCB 访问标签、TCB 访问历史和会话建立的管理，来确保 TCB 自身的安全性。

本级中，TCB 访问控制的设计应：

a) 按 5.1.18 条可选属性范围限定的要求，对用以建立会话的安全属性的范围进行限制；

b) 按 5.1.18 条多重并发会话限定的要求，进行会话管理的限制；

c) **按照 5.1.18 条 TCB 访问历史所描述的要求，实现对会话管理的设计；**

d) 按 5.1.18 条 TCB 会话建立所描述的要求，实现对会话建立管理的设计。

6.2.5 TCB 设计和实现

6.2.5.1 配置管理

应按照 5.2.1 条配置管理的要求进行设计。本级配置管理应满足：

a) 5.2.1.2 条版本号的要求，使用户所使用的版本号与 TCB 样本完全一致；

**b) 5.2.1.3 条 TCB 配置管理范围的要求；**

c) **将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及 CM 文档等置于 CM 之下。**

6.2.5.2 分发和操作

应以文档形式提供对 TCB 安全地进行分发以及安装、生成和启动的过程进行说明。具体要求为：

——按 5.2.2.1 条分发过程的要求编制说明；

——按 5.2.2.2 条安装、生成和启动过程及**日志生成**所描述的要求编制说明。

6.2.5.3 开发

应按照 5.2.3 条所描述的对开发的要求进行 TCB 设计。本级要求：

a) 按 5.2.3.1 条非形式化功能设计和**完全定义的外部接口**的要求进行功能设计；

b) 按 5.2.3.2 条描述性高层设计的要求进行高层设计；

c) 按 5.2.3.3 条 TSF 子集实现的要求进行实现表示设计；

d) 按 5.2.3.4 条模块化和**复杂性降低**的要求进行内部结构设计；

e) 按 5.2.3.5 条描述性低层设计的要求进行低层设计；

f) 按 5.2.3.6 条非形式化对应性的要求进行对应性设计；

g) **按 5.2.3.7 条非形式化 TCB 安全策略模型**的要求进行安全策略模型设计。

6.2.5.4 指导性文档

应按照 5.2.4 条所描述的对指导性文档的要求进行文档设计。本级要求根据上述配置管理、分发和操作、开发以及测试等方面的要求提供管理员指南和用户指南，**要求文档还应包括生命周期支持和脆弱性评定等方面的内容。**

6.2.5.5 生命周期支持

应按照 5.2.5 条生命周期支持所描述的要求进行 TCB 设计。本级应满足:

**a) 5.2.5.1 条安全措施的要求；**

b) 5.2.5.3 条开发者定义的生命周期模型所描述的要求。

6.2.5.6 测试

应按照 5.2.6 条所描述的有关要求对所开发的 TCB 进行测试。本级应满足：

**a) 5.2.6.1 条范围的证据和范围的分析的要求；**

**b) 5.2.6.2 条高层设计测试的要求；**

c) 5.2.6.3 条一般功能测试的要求；

d) 5.2.6.4 条相符性独立测试的要求。

6.2.5.7 脆弱性评定

**应按照 5.2.7 条所描述的要求对所开发的 TCB 进行脆弱性评定。本级评定应按照：**

**a) 5.2.7.2 条指南检查的要求；**

**b) 5.2.7.3 条 TCB 安全功能强度评估的要求；**

**c) 5.2.7.4 条开发者脆弱性分析的要求。**

6.2.6 TCB 安全管理

应根据本级中安全功能技术要求所涉及的物理安全、运行安全、信息安全和安全保证技术要求所涉及 TCB 自身安全与 TCB 设计和实现的有关内容，按照 5.3 条 TCB 安全管理所描述的有关要求，设计 TCB 安全管理。本级应按以下要求制定相应的操作、运行规程和行为规章制度：

a) 5.3.1 条 TSF 的功能管理的要求；

b) 5.3.4 条安全角色的定义所描述的要求。

## 6.3 第三级 安全标记保护级

### 6.3.1 物理安全

应按照 4.1 条中环境安全、设备安全及记录介质安全中的**较高要求**，进行计算机、网络的硬件及相关环境的设计,**并按照 4.1.4 条安全管理中心安全的要求，设计和制定对安全管理中心的物理安全要求。**

### 6.3.2 运行安全

#### 6.3.2.1 风险分析

应按照 4.2.1 条所描述的要求，结合所要设计的计算机信息系统的安全需求，明确**安全标记保护级**的计算机信息系统安全设计所要解决的问题。

#### 6.3.2.2 系统安全检测分析

应按照 4.2.2 条有关操作系统安全性检测分析、数据库管理系统安全性检测分析、网络安全性检测分析、**防火墙安全性检测分析和电磁泄露检测分析**的描述，运用有关工具，检测所选用的操作系统、数据库管理系统和网络系统的安全性，以及电磁泄露情况，并结合计算机信息系统系统的安全要求对其安全性加以改进。

#### 6.3.2.3 网络安全监控

**应按照 4.2.2 条设置分布式探测器和设置安全监控中心的描述，设计计算机信息系统的安全监控功能。**

#### 6.3.2.4 审计

应按照 4.2.4 条安全审计所描述的对审计的要求进行设计。审计主要提供可查性，要求对审计功能的设计应与用户标识与鉴别、自主访问控制、**标记、强制访问控制、客体重用、数据完整性**等安全功能的设计紧密结合，按照审计功能设计的总要求和各安全功能技术要求中的具体审计要求来进行。本级要求：

a) 按 4.2.4.1 条实时报警的生成和**违例进程的终止**的要求，设计自动响应功能；

b) 按 4.2.4.2 条的要求产生审计数据；

c) 按 4.2.4.3 条潜在侵害分析和**基于异常检测的描述**的要求进行审计分析设计；

d) 按 4.2.4.4 条的审计查阅、有限审计查阅和**可选审计查阅**的要求进行安全审计查阅设计；

e) 按 4.2.4.5 条要求提供对审计事件的选择；

f) 按 4.2.4.6 条受保护的审计踪迹存储和**审计数据的可用性确保**的要求来保存审计事件；

**g) 按 4.2.4.7 条网络环境安全审计与评估的要求，对计算机信息系统的安全性进行审计与评估。**

#### 6.3.2.5 网络防病毒

应按照 4.2.5 条有关严格管理、防杀结合和**整体防御**的要求，选择合适的病毒防杀产品实现计算机信息系统的病毒防杀工作。

#### 6.3.2.6 备份与故障恢复

应按照 4.2.6.1 条有关用户自我信息备份、增量备份、局部系统备份、热备份和**全系统备份**的要求，

设计备份功能，按照 4.2.6.2 条手动恢复**和自动恢复**的描述，设计恢复功能，以便在计算机信息系统发生故障时进行必要的恢复工作。

#### 6.3.2.7 应急计划与应急反应

应按照 4.2.7 条具有各种安全措施、设置正常备份机制和**健全安全管理机构**的要求，结合安全标记保护级对计算机信息系统安全的具体要求，设计和制定应急计划和应急措施，明确计算机信息系统出现各种情况时应采取的措施。

### 6.3.3 信息安全

#### 6.3.3.1 用户标识

应按照 4.3.1.2 条有关同步标识和动作前标识的描述，设计用户标识功能。一般以用户名和用户标识符（UID）来标识一个用户，确保在一个计算机信息系统中用户名和用户标识符的唯一性。这种唯一性应在计算机信息系统的整个生命周期内都有效，即使一个用户的帐号已被删除，他的用户名和标识符也不能再使用，并由此确保用户的唯一性和可区别性。

#### 6.3.3.2 用户鉴别

应按照 4.3.1.3 条有关同步鉴别、在任何动作之前鉴别、**不可伪造鉴别和一次性使用鉴别**的描述，设计标识用户的身份鉴别功能；**按照 4.3.2.1 条选择性原发证明和 4.3.2.2 条选择性接收证明的描述设计信息交换用户的身份鉴别功能，**并按照 4.3.1.4 条和 4.3.1.5 条的有关要求进行相关问题的处理。

鉴别应确保用户的真实性。本级要求：

a) 在以请求访问方式引起信息流动时，除采用口令进行鉴别，并在每次用户登录系统时对请求者的身份进行鉴别外，**要求有更加严格的身份鉴别，如采用智能 IC 卡、人体生物特征（指纹、视网膜）等特殊信息进行身份鉴别，并在每次用户登录系统之前进行鉴别。**口令应是不可见的，并在存储时**按 4.3.13 条密码支持第三级的要求进行**保护。**智能 IC 卡身份认证应以密码技术为基础进行进行设计。**

b) 对跨网络的远程用户，当口令在网上传输时应按 **4.3.13 条密码支持第三级的要求进行**保护。

c) 在以交换方式引起信息流动时，要求 TCB 应提供通信双方身份的真实性和双方对信息交换行为的不可抵赖性。对信息的发送方，TCB 应按 4.3.2.1 的选择性原发证明的要求进行设计；对信息的接收方，TCB 应按 4.3.2.2 条的选择性接收证明进行设计。这种安全通信的抗抵赖功能应以 PKI 为基础的 CA 认证系统作为可信第三方来支持。CA 系统所采用的密码算法应**按 4.3.13 条密码支持第三级的要求进行设计。**

#### 6.3.3.3 自主访问控制

应按照 4.3.5.1 条子集访问控制策略所描述的要求，并按照 4.3.5.2 条子集访问控制功能所描述的要求，设计和实现所需要的自主访问控制功能。

目前常用的自主访问控制策略，按照主体与客体的关系，即客体为主体的拥有者/同组/其它，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定主体对客体的访问权限。

在本安全级中，要求的无论采用何种访问控制策略所实现的访问控制功能，都能够：

a) 允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取敏感信息。

b) 有更细粒度的自主访问控制，即对 TSC 内的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行

任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。

c) 要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

d) 对访问是跨网络的情况，可以设计成一个跨网络的 TCB，也可以设计成两个 TCB。前者对传输中的数据保护应按照 4.3.8.1 条基本内部传输保护的要求进行设计；后者对传输中的数据保护则应按照 4.3.8.2 条所描述的要求进行设计，根据 **4.3.13 条密码支持第三级的要求**保证数据在通过网络传输时的保密性和完整性，**并按照 4.3.1.1 条基本数据鉴别的要求进行设计，以确保传输数据的真实性。**

e) 对访问是非注册用户，如通用浏览器的情况，应重点考虑对其写访问的严格控制。

6.3.3.4 标记

**应按照 4.3.4.1 条用户属性定义、4.3.4.2 条客体属性定义及 5.3.2 条安全属性管理、5.3.5 条安全属性终止和 5.3.6 条安全属性撤消所描述的的要求进行设计。通常，主体（用户）的安全属性在用户建立注册帐户后由系统安全员通过 TCB 所提供的安全员界面进行标记，而客体的安全属性则在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员进行标记。TCB 应提供这种标记方式。本安全级要求：**

a) **当信息从 TCB 控制范围之内向 TCB 控制范围之外输出时，应带有安全属性，应按照 4.3.8.3 条带有安全属性的用户数据输出的要求进行设计；**

b) **当信息从 TCB 控制范围之外向 TCB 控制范围之内输入时，可不带有安全属性，应按照 4.3.8.4 条不带安全属性的用户数据输入的要求进行设计。**

6.3.3.5 强制访问控制

**应按照 4.3.6.1 条子集访问控制策略所描述的要求，选择所需的访问控制策略，并按照 4.3.6.2 条子集访问控制功能所描述的要求，设计和实现所需要的强制访问控制功能。**

a) **三权分立。应由专门设置的系统安全员统一管理计算机信息系统中与该访问控制有关的事件和信息。为了防止由于系统管理人员或特权用户的权限过于集中所带来的安全隐患，应将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，并按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，还应在三者之间形成相互制约的关系。**

b) **安全模型。强制访问控制当前常用的安全策略模型是多级安全模型。该模型将 TSC 内的所有主、客体成分通过标记方式设置安全属性（等级和范畴），这些安全属性共同组成属性库，作为访问控制的基本数据。该模型并按由简单保密性原则确定的规则——从下读、向上写，根据访问者主体和被访问者客体的安全属性，实现主、客体之间每次访问的强制性控制。也可以设置某些补充规则以满足专门的需要。**

c) **控制范围。强制访问控制应与用户身份鉴别、标记、审计等安全功能要素密切配合，使系统对用户的安全控制包含从用户进入系统到退出系统的全过程。本级要求的对客体的控制范围仅涉及信息系统内部的存储、处理和传输过程，而不包括将信息进行输入、输出操作的过程。**

d) **多计算机环境或分布式环境。对于网络环境的多计算机系统或分布式系统，TCB 的设计可以采用两种方法。一种方法是设计统一的 TCB（对分布式系统），另一种方法是设置多个 TCB（对多计算机系统）。在分布式系统环境，强制访问控制功能的 TCB 的设计应考虑跨网络的情况，一般应在分布式控制中心设置 TCB 安全功能模块，统一实现强制访问控制功能。如果 TCB 的功能需要延伸到其它部位，则应设计跨网络的 TCB。这时，除按常规要求设计 TCB 外，还需**

**要按 4.3.8.1 条基本数据传输保护和属性分隔传输保护的要求，实现跨网络的 TCB 信息传输的保护。对运行于网络环境的多台计算机系统上的信息系统，强制访问控制功能的 TCB 的设计，一般在每一台计算机系统内设计一个完整的 TCB，并在需要时按 4.3.8.2 条 TSF 间用户数据保密性传输保护和 4.3.9.2 条完整性检测和源数据交换恢复的要求实现跨网络的 TCB 间通信的保护。另外，还必须统一考虑各台计算机系统的主、客体安全属性的设置。同时，采用 4.3.13 条密码支持第三级以及 4.3.1.1 条基本数据鉴别的要求，保证数据在通过网络传输时的保密性、完整性和真实性。**

#### 6.3.3.6 客体重用

应按照 4.3.10 条子集信息保护的要求进行设计。这里的客体主要是指存放信息的介质，如内存、外存（主要指磁盘）、软盘、可擦写光盘等。而客体重用则着重考虑这些存储介质作为计算机系统资源被动态分配时，应确保曾经在介质中存放过的信息不因这种动态分配而遭泄露。本级要求对 TSC 内的存储介质进行重新分配时，确保其残留信息全部被清除。

#### 6.3.3.7 数据完整性

应对计算机信息系统中存储、传输和处理过程中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

a） 存储数据完整性保护，应按照 4.3.9.1 条**完整性检测和恢复**的要求，设计相应的 TCB 安全功能模块，对存储在 TCB 安全控制范围内的用户数据进行完整性保护。本级要求在适当的时候检测存储在 TCB 控制范围之内的用户数据是否出现完整性错误，并进行报警，**还要求在检测到完整性错误时采取必要的恢复措施。本级中，要求通过 4.3.13 条密码支持第三级所提供的功能，对加密存储的数据进行存储数据的完整性检验**。

b） 传输数据完整性保护，应按照 4.3.9.2 条数据交换完整性检测**和源数据交换恢复**的要求设计相应的 TCB 安全功能模块，对经过网络在两个 TCB 间传输的用户数据进行完整性保护。本级要求 TCB 能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警，**还要求通过 4.3.13 条密码支持第三级所提供的功能，对加密传输的数据进行传输数据的完整性检验。**

c） 处理数据完整性保护，应按照 4.3.9.3 条基本回退的要求设计相应的 TCB 安全功能模块，通过在各种异常情况的事务回退，以事务的完整性确保数据的完整性。

### 6.3.4 TCB 自身安全保护

#### 6.3.4.1 TSF 保护

TSF 保护应提供与 TSF 机制的完整性和管理有关的保护，也应提供与 TSF 数据的完整性有关的保护。

本级中，TSF 保护的设计应：

a） 按 5.1.1 条所描述的内容，实现在系统初始化期间、**在正常运转时周期性、应授权用户请求或在其它条件下**，对 TSF 安全假定的正确运行的测试；

b） 按 5.1.2 条所描述的内容，实现对 TSF 出现失败时的处理；

**c） 按 5.1.3 条所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的可用性保护；**

**d） 按 5.1.4 条所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的保密性保护；**

**e） 按 5.1.5 条 TSF 间修改的检测的要求，实现对两个 TCB 之间的 TSF 数据传输的完整性性保护；**

f） 按 5.1.6 条内部 TSF 数据传输的基本保护、**TSF 数据传输分离保护和 TSF 数据完整性保护**所描述的要求，实现对 TSF 数据的传输保护；

g) 按 5.1.7 条物理攻击的被动检测、**物理攻击的自动报告**的要求，实现对 TCB 的物理安全保护。

**h) 按 5.1.9 条所描述的要求，实现对指定实体的重复检测，及出现重复检测的处理；**

**i) 按 5.1.10 条的要求进行设计，确保实现 TCB 安全功能的访问监视器和/或前端过滤器是“始终被激活的”；**

j) **按 5.1.11 条 TSF 域分离的要求进行设计，确保 TCB 安全功能不受不可信主体的干扰和篡改；**

**k) 按 5.1.12 条简单的可信回执的要求进行设计，确保在分布式系统中实现的 TCB 安全功能保持同步状态；**

l) 按 5.1.13 条时间戳的要求，为 TCB 的运行提供可靠的时间戳支持；

**m) 按 5.1.14 条 TSF 间的 TSF 数据一致性要求进行设计，确保在分布式系统中或复合式系统环境下交换的 TSF 数据的一致性；**

**n) 按 5.1.15 条 TCB 内 TSF 数据复制的一致性要求进行设计，确保在跨网络的环境下 TCB 的各部分间的 TSF 数据复制的一致性；**

o) 按 5.1.16 条 TSF 自检的要求，实现 TSF 在系统初始化期间、**在正常运转时周期性、应授权用户请求或在其它条件下进行**的自检。

#### 6.3.4.2 资源利用

应通过故障容错、服务优先级和资源分配来增强 TCB 自身的安全性。

在本级中，资源利用的设计应：

a) 按 5.1.17.1 条降级故障容错**和受限故障容错**的要求，实现 TCB 对指定故障的处理；

b) 按 5.1.17.2 条**全部服务优先级**的要求，进行 TCB 资源的管理和分配；

c) 按 5.1.17.3 条**最小**与最大限额的要求，进行 TCB 资源的管理和分配。

#### 6.3.4.3 TCB 访问控制

应通过会话安全属性、多重并发会话的限定、会话的锁定、TCB 访问标签、访问历史和会话建立的管理，来确保 TCB 自身的安全性。

本级中，TCB 访问功能的设计应：

a) 按 5.1.18 条可选属性范围限定的要求，对用以建立会话的安全属性的范围进行限制；

b) 按 5.1.18 条多重并发会话限定的要求，实现对会话管理的限制；

**c) 按 5.1.18 条会话锁定所描述的要求，实现对会话管理的设计；**

**d) 按 5.1.18 条 TCB 访问标签所描述的要求，实现对会话管理的设计；**

e) 按 5.1.18 条 TCB 访问历史所描述的要求，实现对会话管理的设计；

f) 按 5.1.18 条 TCB 会话建立所描述的要求，实现对会话建立管理的设计。

### 6.3.5 TCB 设计和实现

#### 6.3.5.1 配置管理

应按照 5.2.1 条配置管理的要求进行设计。本级配置管理应满足：

a) **5.2.1.1 条部分 CM 自动化的要求；**

b) 5.2.1.2 条版本号、**配置项和授权控制**的要求；

c) 5.2.1.3 条 TCB 配置管理范围和**问题跟踪配置管理范围**的要求；

d) 将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下。

#### 6.3.5.2 分发和操作

应以文档形式提供对 TCB 安全地进行分发以及安装、生成和启动的过程进行说明。具体要求为：

a) 按 5.2.2.1 条分发过程和**修改检测**的要求编制说明；

b) 按 5.2.2.2 条安装、生成和启动过程及日志生成所描述的要求编制说明。

#### 6.3.5.3 开发

应按照 5.2.3 条所描述的对开发的要求进行 TCB 开发。本级要求：

a) 按 5.2.3.1 条非形式化功能设计和完全定义的外部接口的要求进行功能设计；

b) 按 5.2.3.2 条**安全加强的高层设计**的要求进行高层设计；

c) 按 5.2.3.3 条 **TSF 实现**的要求进行实现表示设计；

d) 按 5.2.3.4 条模块化和复杂性降低的要求进行内部结构设计；

e) 按 5.2.3.5 条描述性低层设计的要求进行低层；

f) 按 5.2.3.6 条非形式化对应性说明的要求进行表示的对应性设计；

g) 按 5.2.3.7 条非形式化 TCB 安全策略模型的要求进行安全策略模型的设计。

#### 6.3.5.4 指导性文档

应按照 5.2.4 条所描述的对指导性文档的要求进行设计。本级要求根据上述配置管理、分发和操作、开发以及测试等方面的要求提供管理员指南和用户指南，还要求文档应包括生命周期支持和脆弱性评定等方面的内容。

#### 6.3.5.5 生命周期支持

应按照 5.2.5 条生命周期支持所描述的要求进行设计。本级 TCB 设计应满足：

a) 5.2.5.1 条安全措施的要求；

**b) 5.2.5.2 条基本缺陷纠正的要求；**

**c) 5.2.5.3 条标准生命周期模型的要求；**

d) 5.2.5.4 条明确定义的开发工具所描述的要求。

#### 6.3.5.6 测试

应按照 5.2.6 条所描述的有关要求对所开发的 TCB 进行测试。本级测试应满足：

a) 5.2.6.1 条范围的证据和范围的分析的要求；

b) 5.2.6.2 条高层设计测试和**低层设计测试**的要求；

c) 5.2.6.3 条一般功能测试**和/或顺序功能测试**的要求；

d) 5.2.6.4 条相符性独立测试和**抽样独立性测试**的要求。

#### 6.3.5.7 脆弱性评定

应按照 5.2.7 条所描述的要求对所开发的 TCB 进行脆弱性评定。本级评定应按照：

a) 5.2.7.2 条指南检查和**分析确认的要求；**

b) 5.2.7.3 条 TCB 安全功能强度评估的要求；

c) 5.2.7.4 条开发者脆弱性分析和**独立脆弱性分析**的要求。

### 6.3.6 TCB 安全管理

应根据本级中安全功能技术要求所涉及的物理安全、运行安全、信息安全和安全保证技术要求所涉及 TCB 自身安全与 TCB 设计和实现的有关内容，按照 5.3 条 TCB 安全管理所描述的有关要求，设计 TCB 安全管理要求。**本级要求将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限。同时，他们之间应形成相互制约的关系。**

本级应按以下要求制定相应的操作、运行规程和行为规章制度：

a) 5.3.1 条 TSF 的功能管理的要求；

b) 5.3.2 条管理安全属性、安全的安全属性和静态属性初始化的要求；

c) 5.3.3 条管理 TSF 数据、TSF 数据界限的管理的要求；

d) 5.3.4 条安全角色的定义、安全角色的限制、安全角色的担任的要求；

e) 5.3.5 条安全属性终止的要求；

f) 5.3.6 条安全属性撤消的要求。

### 6.4 第四级 结构化保护级

#### 6.4.1 物理安全

应按照 4.1 条中有关环境、设备及数据和介质安全中所叙述的**严格要求**，进行计算机、网络的硬件及相关环境的设计,并按照 4.1.4 条安全管理中心安全的要求，设计和制定对安全管理中心的安全要求。

#### 6.4.2 运行安全

##### 6.4.2.1 风险分析

应按照 4.2.1 条所描述的要求，结合所要设计的计算机信息系统的安全需求，明确**结构化保护级**的计算机信息系统安全设计所要解决的问题。

##### 6.4.2.2 网络安全检测分析

应按照 4.2.2 条有关操作系统安全性检测分析、数据库管理系统安全性检测分析、网络安全性检测分析、防火墙安全性检测分析和电磁泄露检测分析的描述，运用有关工具，检测所选用的操作系统、数据库管理系统和网络系统的安全性，以及电磁泄露情况，并结合计算机信息系统系统的安全要求对其安全性加以改进。

##### 6.4.2.3 网络安全监控

应按照 4.2.2 条设置分布式探测器和设置安全监控中心的描述，设计计算机信息系统的安全监控功能。

##### 6.4.2.4 审计

应按照 4.2.4 条安全审计所描述的对审计的要求进行设计。审计主要提供可查性，要求对审计功能的设计应与用户标识与鉴别、自主访问控制、标记、强制访问控制、客体重用、数据完整性、**隐蔽信道分析和可信路径**等安全功能的设计紧密结合，按照审计功能设计的总要求和各安全功能技术要求中的具体审计要求来进行。本级要求：

a) 按 4.2.4.1 条实时报警的生成、违例进程的终止和**服务的取消**的要求，设计自动响应功能；

b) 按 4.2.4.2 条安全审计数据产生的要求产生审计数据；

c) 按 4.2.4.3 条潜在侵害分析、基于异常检测的描述和**简单攻击探测**的要求进行审计分析设计；

d) 按 4.2.4.4 条审计查阅、有限审计查阅和可选审计查阅的要求进行安全审计查阅设计；

e) 按 4.2.4.5 条安全审计事件选择的要求提供对审计事件的选择；

f) 按 4.2.4.6 条受保护的审计踪迹存储、审计数据的可用性确保**和在审计数据可能丢失情况下的措施**的要求进行保存审计事件设计；

g) 按 4.2.4.7 条网络环境安全审计与评估的描述,对计算机信息系统的安全性进行审计与评估。

##### 6.4.2.5 网络防病毒

应按照 4.2.5 条网络防病毒中有关严格管理、防杀结合、整体防御、**防管结合和多层防御**的要求，选择合适的病毒防杀产品实现计算机信息系统的病毒防杀工作。

##### 6.4.2.6 备份与故障恢复

应按照 4.2.6.1 条有关用户自我信息备份、增量备份、局部系统备份、热备份、全系统备份和**主机**

**系统远地备份**的要求，设计备份功能，按照 4.2.6.2 条手动恢复、自动恢复、**无过分丢失的自动恢复以及灾难性恢复**的描述，设计恢复功能，以便在计算机信息系统发生故障时进行必要的恢复工作。

6.4.2.7 应急计划与应急反应

应按照 4.2.7 条具有各种安全措施、设置正常备份机制、健全安全管理机构和**建立处理流程图**的要求，结合结构化保护级对级计算机信息系统安全的具体要求，设计和制定应急计划和应急措施，明确计算机信息系统出现各种情况时应采取的措施。

6.4.3 信息安全

6.4.3.1 用户标识

应按照 4.3.1.2 条有关同步标识和动作前标识的描述，设计用户标识功能。一般以用户名和用户标识符（UID）来标识一个用户，确保在一个计算机信息系统中用户名和用户标识符的唯一性。这种唯一性应在计算机信息系统的整个生命周期内都有效，即使一个用户的帐号已被删除，他的用户名和标识符也不能再使用，并由此确保用户的唯一性和可区别性。

6.4.3.2 用户鉴别

应按照 4.3.1.3 条有关同步鉴别、在任何动作之前鉴别、不可伪造鉴别、一次性使用鉴别、**多鉴别机制、重鉴别和受保护的鉴别反馈**的要求，以及 4.3.1.5 条、**4.3.3 条所描述的要求，**设计标识用户的身份鉴别功能；按照 4.3.2.1 条**强制性原发证明**和 4.3.2.2 条**强制性接收证明**的描述设计信息交换用户的身份鉴别功能；按照 4.3.1.4 条和 4.3.1.5 条的有关要求进行相关问题的处理。

鉴别应确保用户的真实性。本级要求：

a) 在以请求访问方式引起信息流动时，除采用口令进行鉴别，并在每次用户登录系统时对请求者的身份进行鉴别外，要求有更加严格的身份鉴别，如采用智能 IC 卡、人体生物特征（指纹、视网膜）等特殊信息进行身份鉴别，并在每次用户登录系统之前进行鉴别。口令应是不可见的，并在存储时按 **4.3.13 条密码支持第四级**的要求进行保护。智能 IC 卡身份认证应以密码技术为基础进行进行设计。对跨网络的远程用户，当口令在网上传输时应按 **4.3.13 条密码支持第四级**的要求进行保护。

b) 在以交换方式引起信息流动时，要求 TCB 应提供通行双方身份的真实性和双方对信息交换行为的不可抵赖性。对信息的发送方，TCB 应按 4.3.2.1 条**强制性原发证明**的要求进行设计；对信息的接收方，TCB 应按 4.3.2.2 条**强制性接收证明**进行设计。这种安全通信的抗抵赖功能应以 PKI 为基础的 CA 认证系统作为可信第三方来支持。CA 系统所采用的密码算法应**按 4.3.13 条密码支持第四级的要求进行设计。**

**c) 在某些情况下，除了要求确保用户身份的唯一性和真实性外，还要求对某些用户的身份进行特别保护，使其不被其他用户发现或滥用。实现这种要求，应按照 4.3.3 条匿名、假名、不可关联性和不可观察性的要求进行 TCB 的设计。**

6.4.3.3 自主访问控制

应按照 4.3.5.1 条**完全访问控制策略**所描述的要求，并按照 4.3.5.2 条**完全访问控制功能**所描述的要求，设计和实现所需要的自主访问控制功能。

目前常用的自主访问控制策略，按照主体与客体的关系，即客体为主体的拥有者/同组/其它，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定主体对客体的访问权限。

在本安全级中，**要求将自主访问控制扩展到计算机信息系统的所有主体与客体，**要求无论采用何种访问控制策略所实现的访问控制功能，都能够：

a) 允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取敏

感信息。

b) 有更细粒度的自主访问控制，即对 TSC 内的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。

c) 要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

d) 对访问是跨网络的情况，可以设计成一个跨网络的 TCB，也可以设计成两个 TCB。前者对传输中的数据保护应按照 4.3.8.1 条基本内部传输保护的要求进行设计；后者对传输中的数据保护则应按照 4.3.8.2 条所描述的要求进行设计，根据 **4.3.13 条密码支持第四级的要求**保证数据在通过网络传输时的保密性和完整性，并按照 4.3.1.1 条基本数据鉴别的要求进行设计，以确保传输数据的真实性。

e) 对访问是非注册用户，如通用浏览器的情况，应重点考虑对其写访问的严格控制。

#### 6.4.3.4 标记

应按照 4.3.4.1 条用户属性定义、4.3.4.2 条客体属性定义及 5.3.2 条安全属性管理、5.3.5 条安全属性终止和 5.3.6 条安全属性撤消所描述的的要求进行设计。通常，主体（用户）的安全属性在用户建立注册帐户后由系统安全员通过 TCB 所提供的安全员界面进行标记，而客体的安全属性则在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员进行标记。TCB 应提供这种标记方式。本级要求：

a) 当信息从 TCB 控制范围之内向 TCB 控制范围之外输出时，应带有安全属性，按照 4.3.8.3 条带有安全属性的用户数据输出的要求进行设计；

b) 当信息从 TCB 控制范围之外向 TCB 控制范围之内输入时，**可以带有安全属性也可以不带有安全属性**，应按照 4.3.8.4 条不带安全属性**和/或带有安全属性**的用户数据输入的要求进行设计。

#### 6.4.3.5 强制访问控制

应按照 4.3.6.1 条**完全访问控制策略**所描述的要求，选择所需的访问控制策略，并按照 4.3.6.2 条**完全访问控制**的要求，设计和实现所需要的强制访问控制功能。

a) 三权分立。应由专门设置的系统安全员统一管理计算机信息系统中与该访问控制有关的事件和信息。为了防止由于系统管理人员或特权用户的权限过于集中所带来的安全隐患，应将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，并按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，还应在三者之间形成相互制约的关系。

b) 安全模型。强制访问控制当前常用的安全策略模型是多级安全模型。该模型将 TSC 内的所有主、客体成分通过标记方式设置安全属性（等级和范畴），这些安全属性共同组成属性库，作为访问控制的基本数据。该模型并按由简单保密性原则确定的规则——从下读、向上写，根据访问者主体和被访问者客体的安全属性，实现主、客体之间每次访问的强制性控制。也可以设置某些补充规则以满足专门的需要。

c) 控制范围。**在本级中，要求将强制访问控制扩展到计算机信息系统中的所有主体与客体。**强制访问控制应与用户身份鉴别、标记、审计等安全功能要素密切配合，使系统对用户的安全

控制包含从用户进入系统到退出系统的全过程。本级要求的对客体的控制范围仅涉及信息系统内部的存储、处理和传输过程，而不包括将信息进行输入、输出操作的过程。**还包括将信息进行输入、输出操作的过程，即无论信息以何种形式存在，都应有一定的安全属性与其相关联，并按强制访问控制规则对其进行控制。**

d) 多计算机环境或分布式环境。对于网络环境的多计算机系统或分布式系统，TCB 的设计可以采用两种方法。一种方法是设计统一的 TCB（对分布式系统），另一种方法是设置多个 TCB（对多计算机系统）。在分布式系统环境，强制访问控制功能的 TCB 的设计应考虑跨网络的情况，一般应在分布式控制中心设置 TCB 安全功能模块，统一实现强制访问控制功能。如果 TCB 的功能需要延伸到其它部位，则应设计跨网络的 TCB。这时，除按常规要求设计 TCB 外，还需要按 4.3.8.1 条基本数据传输保护和属性分隔传输保护的要求，实现跨网络的 TCB 信息传输的保护。对运行于网络环境的多台计算机系统上的信息系统，强制访问控制功能的 TCB 的设计，一般在每一台计算机系统内设计一个完整的 TCB，并在需要时按 4.3.8.2 条 TSF 间用户数据保密性传输保护和 4.3.9.2 条数据交换完整性检测和**目的数据交换恢复**的要求实现跨网络的 TCB 间通信的保护。另外，还必须统一考虑各台计算机系统的主、客体安全属性的设置。同时，采用 **4.3.13 条密码支持第四级**以及 4.3.1.1 条**伴有保证者身份的数据鉴别**的要求，保证数据在通过网络传输时的保密性、完整性和真实性。

#### 6.4.3.6 客体重用

应按照 4.3.10 条**完全信息保护**的要求进行设计。这里的客体包括存放信息的介质，如内存、外存（主要指磁盘）、软盘、可擦写光盘，以及寄存器、高速缓存等可读写的硬件设备。而客体重用则应考虑这些存储介质作为计算机系统资源被动态分配时和**在对资源进行回收时**，应确保曾经在介质中存放过的信息不因这种动态分配和回收而遭泄露。

#### 6.4.3.7 数据完整性

应对计算机信息系统中存储、传输和处理过程中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

a） 存储数据完整性保护，应按照 4.3.9.1 条完整性检测和恢复的要求，设计相应的 TCB 安全功能模块，对存储在 TCB 安全控制范围内的用户数据进行完整性保护。本级要求 TCB 在适当的时候检测存储在 TCB 控制范围之内的用户数据是否出现完整性错误，并进行报警，还要求在检测到完整性错误时采取必要的恢复措施。本级中，要求通过 **4.3.13 条密码支持第四级**所提供的功能，对加密存储的数据进行存储数据的完整性检验。

b） 传输数据完整性保护，应按照 4.3.9.2 条数据交换完整性检测和**目的数据交换恢复**的要求设计相应的 TCB 安全功能模块，对经过网络在两个 TCB 间传输的用户数据进行完整性保护。本级要求 TCB 能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警，还要求通过 **4.3.13 条密码支持第四级**所提供的功能，对加密传输的数据进行传输数据的完整性检验。

c） 处理数据完整性保护，应按照 4.3.9.3 条**高级回退**的要求设计相应的 TCB 安全功能模块，通过在各种异常情况的事务回退，以事务的完整性确保数据的完整性。

#### 6.4.3.8 隐蔽信道分析

**应根据实际测量和工程估算，分析系统中存在的隐蔽信道，并采取相应措施进行防范。本级要求按照 4.3.11.1 条一般性隐蔽信道分析的要求进行隐蔽信道分析。**

6.4.3.9 可信路径

**要求按 4.3.12 用户与 TSF 间可信路径所描述的要求进行设计。在对用户进行初始登录和/或鉴别时，TCB 应在它与用户之间建立一条安全的信息传输通路。**

6.4.4 TCB 自身安全保护

6.4.4.1 TSF 保护

TSF 保护应提供与 TSF 机制的完整性和管理有关的保护，也应提供与 TSF 数据的完整性有关的保护。

本级中，TSF 保护的设计应：

a) 按 5.1.1 条安全运行测试所描述的内容，实现在系统初始化期间、在正常运转时周期性、应授权用户请求或在其它条件下，对 TSF 安全假定的正确运行的测试；
b) 按 5.1.2 条失败保护所描述的内容，实现对 TSF 出现失败时的处理；
c) 按 5.1.3 条输出 TSF 数据的可用性所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的可用性保护；
d) 按 5.1.4 条输出 TSF 数据的保密性所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的保密性保护；
e) 按 5.1.5 条 **TSF 间修改的检测与改正**所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的完整性性保护；
f) 按 5.1.6 条内部 TSF 数据传输的基本保护、TSF 数据传输分离保护和 TSF 数据完整性保护所描述的要求，实现对 TSF 数据的传输保护；
g) 按 5.1.7 条物理攻击的被动检测、物理攻击的自动报告和**物理攻击抵抗**所描述的要求，实现对 TCB 的物理安全保护；
h) 按 5.1.9 条重复检测所描述的要求，实现对指定实体的重复检测，及出现重复检测的处理；
i) 按 5.1.10 条参照仲裁所描述的要求进行设计，确保实现 TCB 安全功能的访问监视器和/或前端过滤器是“始终被激活的”；
j) 按 5.1.11 条 **SFP 域分离**所描述的要求进行设计，确保 TCB 安全功能不受不可信主体的干扰和篡改；
k) 按 5.1.12 条**相互的可信回执**的要求进行设计，确保在分布式系统中实现的 TCB 安全功能保持同步状态；
l) 按 5.1.13 条时间戳的要求，为 TCB 的运行提供可靠的时间戳支持；
m) 按 5.1.14 条 TSF 间的 TSF 数据一致性要求进行设计，确保在分布式系统中或复合式系统环境下交换的 TSF 数据的一致性；
n) 按 5.1.15 条 TCB 内 TSF 数据复制的一致性要求进行设计，确保在跨网络的环境下 TCB 的各部分间的 TSF 数据复制的一致性；
o) 按 5.1.16 条 TSF 自检的要求，实现 TSF 在系统初始化期间、在正常运转时周期性、应授权用户请求或在其它条件下进行的自检。

6.4.4.2 资源利用

应通过故障容错、服务优先级和资源分配来增强 TCB 自身的安全性。

在本级中，资源利用的设计应：

a) 按 5.1.17.1 条降级故障容错和受限故障容错的要求，实现 TCB 对指定故障的处理；
b) 按 5.1.17.2 条全部服务优先级的要求，进行 TCB 资源的管理和分配；

c) 按 5.1.17.3 条资源分配中最小与最大限额的要求，进行 TCB 资源的管理和分配。

#### 6.4.4.3 TCB 访问控制

TCB 所实现的安全功能，一般都是有用户激发的。用户通过建立与 TCB 的会话来实现与 TCB 的交互。TCB 访问控制就是用来对会话进行管理的机制。这种管理机制从会话安全属性、多重并发会话的限定及会话的锁定，到 TCB 访问标签、访问历史和会话建立的管理，来确保 TCB 自身的安全性。

本级中，TCB 访问控制的设计应：

a) 按 5.1.18 条可选属性范围限定的要求，对用以建立会话的安全属性的范围进行限制；

b) 按 5.1.18 条多重并发会话限定的要求，实现对会话管理的限定；

c) 按 5.1.18 条会话锁定所描述的要求，实现对会话管理的设计；

d) 按 5.1.18 条 TCB 访问标签所描述的要求，实现对会话管理的设计；

e) 按 5.1.18 条 TCB 访问历史所描述的要求，实现对会话管理的设计；

f) 按 5.1.18 条 TCB 会话建立所描述的要求，实现对会话管理的设计。

#### 6.4.4.4 可信路径/信道

**在一个 TCB 中，可以有多个 TSF，它们之间需要进行数据交换；用户为实现某种安全功能，也需要与 TSF 进行数据交换。为此，TCB 应：**

**a) 按 5.1.19.1 条 TSF 间可信信道的要求进行数据交换的设计；**

**b) 按 5.1.19.2 条用户与 TSF 间可信路径的要求进行数据交换的设计。**

### 6.4.5 TCB 设计和实现

#### 6.4.5.1 配置管理

应按照 5.2.1 条配置管理的要求进行设计。本级配置管理应满足：

a) 5.2.1.1 条部分 CM 自动化的要求；

b) 5.2.1.2 条版本号、配置项、授权控制及**生成支持和验收过程**的要求；

c) 5.2.1.3 条 TCB 配置管理范围、问题跟踪配置管理范围和**开发工具配置管理范围**的要求；

d) 将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下。

#### 6.4.5.2 分发和操作

应以文档形式提供对 TCB 安全地进行分发以及安装、生成和启动的过程进行说明。具体要求为：

a) 按 5.2.2.1 条分发过程、修改检测和**修改防止**的要求编制说明；

b) 按 5.2.2.2 条安装、生成和启动过程及日志生成所描述的要求编制说明。

#### 6.4.5.3 开发

应按照 5.2.3 条所描述的对开发的要求进行 TCB 开发。本级要求：

a) 按 5.2.3.1 条完全定义的外部接口和**半形式化功能设计**的要求进行功能设计；

b) 按 5.2.3.2 条**半形式化高层设计**的要求进行高层设计；

c) 按 5.2.3.3 条 **TSF 的结构化实现**的要求进行实现表示设计；

d) 按 5.2.3.4 条模块化和**复杂性最小化**的要求进行内部结构设计；

e) 按 5.2.3.5 条**半形式化低层设计**的要求进行低层；

f) 按 5.2.3.6 条**半形式化对应性说明**的要求进行表示的对应性设计；

g) 按 5.2.3.7 条**半形式化 TCB 安全策略模型**的要求进行安全策略模型的设计。

#### 6.4.5.4 指导性文档

应按照 5.2.4 条所描述的对指导性文档的要求进行设计。本级要求根据上述配置管理、分发和操

作、开发以及测试等方面的要求提供管理员指南和用户指南，要求文档还应包括生命周期支持和脆弱性评定等方面的内容。

#### 6.4.5.5 生命周期支持

应按照 5.2.5 条生命周期支持所描述的要求进行设计。本级 TCB 设计应满足：

a) 5.2.5.1 条安全措施和**安全措施的充分性**的要求；

b) 5.2.5.2 条基本缺陷纠正的要求；

c) 5.2.5.3 条标准生命周期模型的要求；

d) 5.2.5.4 条明确定义的开发工具和**遵照实现标准-应用部分**所描述的要求。

#### 6.4.5.6 测试

应按照 5.2.6 条测试中所描述的有关要求对所开发的 TCB 进行测试。本级测应满足：

a) 5.2.6.1 条范围的证据和**严格的范围分析**的要求；

b) 5.2.6.2 条高层设计测试、低层设计测试和**实现表示测试**的要求；

c) 5.2.6.3 条**顺序的功能测试**的要求；

d) 5.2.6.4 条相符性独立测试和抽样独立性测试的要求。

#### 6.4.5.7 脆弱性评定

应按照 5.2.7 条所描述的要求对所开发的 TCB 进行脆弱性评定。本级评定应按照：

**a) 5.2.7.1 条一般性的隐蔽信道分析和/或系统化的隐蔽信道分析的要求；**

b) 5.2.7.2 条指南检查、分析确认及**对安全状态的检测和分析**的要求；

c) 5.2.7.3 条 TCB 安全功能强度评估的要求；

d) 5.2.7.4 条开发者脆弱性分析、独立脆弱性分析和**中级抵抗力**的要求。

### 6.4.6 TCB 安全管理

应根据本级中安全功能技术要求所涉及的物理安全、运行安全、信息安全和安全保证技术要求所涉及 TCB 自身安全与 TCB 设计和实现的有关内容，按照 5.3 条 TCB 安全管理所描述的有关要求，设计 TCB 安全管理要求。本级要求将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限。同时，他们之间应形成相互制约的关系。

本级应按以下要求制定相应的操作、运行规程和行为规章制度：

a) 5.3.1 条 TSF 的功能管理的要求；

b) 5.3.2 条管理安全属性、安全的安全属性和静态属性初始化的要求；

c) 5.3.3 条管理 TSF 数据、TSF 数据界限的管理和**安全的 TSF 数据**的要求；

d) 5.3.4 条安全角色的定义、安全角色的限制、安全角色的担任的要求；

e) 5.3.5 条安全属性终止的要求；

f) 5.3.6 条安全属性撤消所描述的要求。

## 6.5 第五级 访问验证保护级

### 6.5.1 物理安全

要求 TCB 的设计者按照 4.1 条中有关环境、设备及数据和介质安全中所叙述的严格要求，进行计算机、网络的硬件及相关环境的设计,并按照 4.1.4 条安全管理中心安全的要求，设计和制定对安全管理中心的安全要求。

### 6.5.2 运行安全

#### 6.5.2.1 风险分析

应按照 4.2.1 条描述的要求，结合所要设计的计算机信息系统的安全需求，明确**访问验证保护级**的计算机信息系统安全设计所要解决的问题。

#### 6.5.2.2 系统安全性检测分析

应按照 4.2.2 条有关操作系统安全性检测分析、数据库管理系统安全性检测分析、网络安全性检测分析、防火墙安全性检测分析和电磁泄露检测分析的描述，运用有关工具，检测所选用的操作系统、数据库管理系统和网络系统的安全性，以及电磁泄露情况，并结合计算机信息系统系统的安全要求对其安全性加以改进。

#### 6.5.2.3 网络安全监控

要求 TCB 的设计者按照 4.2.2 条设置分布式探测器和设置安全监控中心的描述，设计计算机信息系统的安全监控功能。

#### 6.5.2.4 审计

应按照 4.2.4 条安全审计所描述的对审计的要求进行设计。审计主要提供可查性，这就要求对审计功能的设计应与用户标识与鉴别、自主访问控制、标记、强制访问控制、客体重用、数据完整性、隐蔽信道分析、可信路径和**故障恢复**等安全功能的设计紧密结合，按照审计功能设计的总要求和各安全功能技术要求中的具体审计要求来进行。本级要求：

a) 按 4.2.4.1 条实时报警的生成、违例进程的终止、服务的取消和**用户帐号的断开与失效**的要求，设计自动响应功能；
b) 按 4.2.4.2 条安全审计数据产生的要求产生审计数据；
c) 按 4.2.4.3 条潜在侵害分析、基于异常检测、简单攻击探测和和**复杂攻击探测**的要求进行审计分析设计；
d) 按 4.2.4.4 条审计查阅、有限审计查阅和可选审计查阅的要求进行安全审计查阅设计；
e) 按 4.2.4.5 条安全审计事件选择的要求提供对审计事件的选择；
f) 按 4.2.4.6 条受保护的审计踪迹存储、审计数据的可用性确保、在审计数据可能丢失情况下的措施和**防止审计数据丢失**的要求进行保存审计事件设计；
g) 按 4.2.4.7 条网络环境安全审计与评估的描述，对计算机信息系统的安全性进行审计与评估。

#### 6.5.2.5 网络防病毒

要求 TCB 的设计者按照 4.2.5 条网络防病毒中有关严格管理、防杀结合、整体防御、防管结合和多层防御的要求，选择合适的病毒防杀产品实现计算机信息系统的病毒防杀工作。

#### 6.5.2.6 备份与故障恢复

要求 TCB 的设计者按照 4.2.6.1 条有关用户自我信息备份、增量备份、局部系统备份、热备份、全系统备份和主机系统远地备份的要求，设计备份功能，按照 4.2.6.2 条手动恢复、自动恢复、无过分丢失的自动恢复以及灾难性恢复的描述，设计恢复功能，以便在计算机信息系统发生故障时进行必要的恢复工作。

#### 6.5.2.7 应急计划与应急反应

应按照 4.2.7 条具有各种安全措施、设置正常备份机制、健全安全管理机构和建立处理流程图的要求，结合访问验证保护级对计算机信息系统安全的具体要求，设计和制定应急计划和应急措施，明确计算机信息系统出现各种情况时应采取的措施。

### 6.5.3 信息安全

#### 6.5.3.1 用户标识

应按照 4.3.1.2 条有关同步标识和动作前标识的描述，设计用户标识功能。一般以用户名和用户标识符（UID）来标识一个用户，确保在一个计算机信息系统中用户名和用户标识符的唯一性，这种唯一性应在计算机信息系统的整个生命周期内都有效，即使一个用户的帐号已被删除，他的用户名和标识符也不能再使用，并由此确保用户的唯一性和可区别性。

#### 6.5.3.2 用户鉴别

应按照 4.3.1.3 条有关同步鉴别、在任何动作之前鉴别、不可伪造鉴别、一次性使用鉴别、多鉴别机制、重鉴别和受保护的鉴别反馈的要求，以及 4.3.1.5 条用户-主体绑定、4.3.3 条隐秘所描述的要求，设计标识用户的身份鉴别功能；按照 4.3.2.1 条强制性原发证明和 4.3.2.2 条强制性接收证明的描述设计信息交换用户的身份鉴别功能，并按照 4.3.1.4 条鉴别失败和 4.3.1.5 条用户-主体绑定的有关要求进行相关问题的处理。

鉴别应确保用户的真实性。本级要求：

a) 在以请求访问方式引起信息流动时，除采用口令进行鉴别，并在每次用户登录系统时对请求者的身份进行鉴别外，要求有更加严格的身份鉴别，如采用智能 IC 卡、人体生物特征（指纹、视网膜）等特殊信息进行身份鉴别，并在每次用户登录系统之前进行鉴别。口令应是不可见的，并在存储时按 **4.3.13 条密码支持第五级**的要求进行保护。智能 IC 卡身份认证应以密码技术为基础进行进行设计。对跨网络的远程用户，当口令在网上传输时应按 **4.3.13 条密码支持第五级**的要求进行保护。

b) 在以交换方式引起信息流动时，要求 TCB 应提供通行双方身份的真实性和双方对信息交换行为的不可抵赖性。对信息的发送方，TCB 应按 4.3.2.1 条的强制性原发证明的要求进行设计；对信息的接收方，TCB 应按 4.3.2.2 条的强制性接收证明进行设计。这种安全通信的抗抵赖功能应以 PKI 为基础的 CA 认证系统作为可信第三方来支持。CA 系统所采用的密码算法应按 **4.3.13 条密码支持第五级**的要求进行设计。

c) 在某些情况下，除了要求确保用户身份的唯一性和真实性外，还要求对某些用户的身份进行特别保护，使其不被其他用户发现或滥用。实现这种要求，应按照 4.3.3 条隐秘中匿名、假名、不可关联性和不可观察性所描述的要求进行 TCB 的设计。

#### 6.5.3.3 自主访问控制

应按照 4.3.5.1 条完全访问控制所描述的要求，并按照 4.3.5.2 条完全访问控制功能所描述的要求，设计和实现所需要的自主访问控制功能。

目前常用的自主访问控制策略，按照主体与客体的关系，即客体为主体的拥有者/同组/其它，可以用访问控制表及其相应的访问规则所组成的访问控制策略，确定主体对客体的访问权限。

在本安全级中，要求将自主访问控制扩展到计算机信息系统的所有主体与客体，要求无论采用何种访问控制策略所实现的访问控制功能，都能够：

a) 允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取敏感信息。

b) 有更细粒度的自主访问控制，即对 TSC 内的每一个客体，都应能够实现由客体的创建者（用户）以用户指定方式或默认方式确定其对该客体的访问权限，而别的同组用户或非同组的用户和用户组对该客体的访问权则应由创建者用户授予，并将访问控制的粒度控制在单个用户，做到只有授权用户才能对该客体实施所授权的访问，而阻止那些非授权的用户对该客体进行

任何访问，也阻止授权用户以非授权的操作形式对该客体进行访问。

c) 要求自主访问控制能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

d) 对访问是跨网络的情况，可以设计成一个跨网络的 TCB，也可以设计成两个 TCB。前者对传输中的数据保护应按照 4.3.8.1 条基本内部传输保护的要求进行设计；后者对传输中的数据保护则应按照 4.3.8.2 条所描述的要求进行设计，根据 **4.3.13 条密码支持第五级的要求**保证数据在通过网络传输时的保密性和完整性，并按照 4.3.1.1 条基本数据鉴别的要求进行设计，以确保传输数据的真实性。

e) 对访问是非注册用户，如通用浏览器的情况，应重点考虑对其写访问的严格控制。

#### 6.5.3.4 标记

应按照 4.3.4.1 条用户属性定义、4.3.4.2 条客体属性定义及 5.3.2 条安全属性管理、5.3.5 条安全属性终止和 5.3.6 条安全属性撤消所描述的的要求进行设计。通常，主体（用户）的安全属性在用户建立注册帐户后由系统安全员通过 TCB 所提供的安全员界面进行标记，而客体的安全属性则在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员进行标记。TCB 应提供这种标记方式。

本安全级要求：

a) 当信息从 TCB 控制范围之内向 TCB 控制范围之外输出时，应带有安全属性，按照 4.3.8.3 条带有安全属性的用户数据输出的要求进行设计；

b) 当信息从 TCB 控制范围之外向 TCB 控制范围之内输入时，可以带有安全属性也可以不带有安全属性，应按照 4.3.8.4 条不带安全属性和/或带有安全属性的用户数据输入的要求进行设计。

#### 6.5.3.5 强制访问控制

应按照 4.3.6.1 条完全访问控制策略所描述的要求，选择所需的访问控制策略，并按照 4.3.6.2 条完全访问控制功能所描述的要求，设计和实现所需要的强制访问控制功能。

a) 三权分立。应由专门设置的系统安全员统一管理计算机信息系统中与该访问控制有关的事件和信息。为了防止由于系统管理人员或特权用户的权限过于集中所带来的安全隐患，应将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，并按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，还应在三者之间形成相互制约的关系。

b) 安全模型。强制访问控制当前常用的安全策略模型是多级安全模型。该模型将 TSC 内的所有主、客体成分通过标记方式设置安全属性（等级和范畴），这些安全属性共同组成属性库，作为访问控制的基本数据。该模型并按由简单保密性原则确定的规则——从下读、向上写，根据访问者主体和被访问者客体的安全属性，实现主、客体之间每次访问的强制性控制。也可以设置某些补充规则以满足专门的需要。

c) 控制范围。在本级中，要求将强制访问控制扩展到计算机信息系统中的所有主体与客体。强制访问控制应与用户身份鉴别、标记、审计等安全功能要素密切配合，使系统对用户的安全控制包含从用户进入系统到退出系统的全过程。本级要求的对客体的控制范围仅涉及信息系统内部的存储、处理和传输过程，而不包括将信息进行输入、输出操作的过程。还包括将信息进行输入、输出操作的过程，即无论信息以何种形式存在，都应有一定的安全属性与其相关联，并按强制访问控制规则对其进行控制。

d) 多计算机环境或分布式环境。对于网络环境的多计算机系统或分布式系统，TCB 的设计可以采用两种方法。一种方法是设计统一的 TCB（对分布式系统），另一种方法是设置多个 TCB（对多计算机系统）。在分布式系统环境，强制访问控制功能的 TCB 的设计应考虑跨网络的情况，一般应在分布式控制中心设置 TCB 安全功能模块，统一实现强制访问控制功能。如果 TCB 的功能需要延伸到其它部位，则应设计跨网络的 TCB。这时，除按常规要求设计 TCB 外，还需要按 4.3.8.1 条基本数据传输保护和属性分隔传输保护的要求，实现跨网络的 TCB 信息传输的保护。对运行于网络环境的多台计算机系统上的信息系统，强制访问控制功能的 TCB 的设计，一般在每一台计算机系统内设计一个完整的 TCB，并在需要时按 4.3.8.2 条 TSF 间用户数据保密性传输保护和 4.3.9.2 条数据交换完整性检测和目的数据交换恢复的要求实现跨网络的 TCB 间通信的保护。另外，还必须统一考虑各台计算机系统的主、客体安全属性的设置。同时，采用 **4.3.13 条密码支持第五级**以及 4.3.1.1 条伴有保证者身份的数据鉴别的要求，保证数据在通过网络传输时的保密性、完整性和真实性。

#### 6.5.3.6 客体重用

应按照 4.3.10 条完全信息保护和**特殊信息保护**的要求进行设计。这里的客体包括存放信息的介质，如内存、外存（主要指磁盘）、软盘、可擦写光盘，以及寄存器、高速缓存等可读写的硬件设备。而客体重用则应考虑这些存储介质作为计算机系统资源被动态分配时和在对资源进行回收时，应确保曾经在介质中存放过的信息不因这种动态分配和回收而遭泄露。**对于存放某些特殊信息的资源，要求在对其释放时应采取特别的信息檫除手段进行残留信息的清除。**

#### 6.5.3.7 数据完整性

应对计算机信息系统中存储、传输和处理过程中的信息采取有效措施，防止其遭受非授权用户的修改、破坏或删除。

a） 存储数据完整性保护，应按照 4.3.9.1 条完整性检测和恢复的要求，设计相应的 TCB 安全功能模块，对存储在 TCB 安全控制范围内的用户数据进行完整性保护。本级要求 TCB 在适当的时候检测存储在 TCB 控制范围之内的用户数据是否出现完整性错误，并进行报警，还要求在检测到完整性错误时采取必要的恢复措施。本级中，要求通过 **4.3.13 条密码支持第五级**所提供的功能，对加密存储的数据进行存储数据的完整性检验。

b） 传输数据完整性保护，应按照 4.3.9.2 条数据交换完整性检测和目的数据交换恢复的要求设计相应的 TCB 安全功能模块，对经过网络在两个 TCB 间传输的用户数据进行完整性保护。本级要求 TCB 能检测出被传输的用户数据被篡改、删除、插入和重用等情况发生，并进行报警，还要求通过 **4.3.13 条密码支持第五级**所提供的功能，对加密传输的数据进行传输数据的完整性检验。

c） 处理数据完整性保护，应按照 4.3.9.3 条**高级回退**的要求设计相应的 TCB 安全功能模块，通过在各种异常情况的事务回退，以事务的完整性确保数据的完整性。

#### 6.5.3.8 隐蔽信道分析

应根据实际测量和工程估算，分析系统中存在的隐蔽信道，并采取相应措施进行防范。本级要求按照 **4.3.11.2 条系统化隐蔽信道分析和 4.3.11.3 条彻底的隐蔽信道分析**的要求进行隐蔽信道分析。

#### 6.5.3.9 可信路径

要求按 4.3.12 条用户与 TSF 间可信路径所描述的要求进行设计。在对用户进行初始登录和/或鉴别时，TCB 应在它与用户之间建立一条安全的信息传输通路。

### 6.5.4 TCB 自身安全保护

TCB 自身安全保护是指为实现 TCB 的安全功能所应采取的内部措施，包括 TSF 保护、资源利用和 TCB 访问等方面的内容。

#### 6.5.4.1 TSF 保护

TSF 保护应提供与 TSF 机制的完整性和管理有关的保护，也应提供与 TSF 数据的完整性有关的保护。

本级中，TSF 保护的设计应：

a) 按 5.1.1 条描述的内容，实现在系统初始化期间、在正常运转时周期性、应授权用户请求或在其它条件下，对 TSF 安全假定的正确运行的测试；
b) 按 5.1.2 条描述的内容，实现对 TSF 出现失败时的处理；
c) 按 5.1.3 条输出 TSF 数据的可用性所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的可用性保护；
d) 按 5.1.4 条输出 TSF 数据的保密性所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的保密性保护；
e) 按 5.1.5 条 TSF 间修改的检测与改正所描述的要求，实现对两个 TCB 之间的 TSF 数据传输的完整性性保护；
f) 按 5.1.6 条内部 TSF 数据传输的基本保护、TSF 数据传输分离保护和 TSF 数据完整性保护所描述的要求，实现对 TSF 数据的传输保护；
g) 按 5.1.7 条物理攻击的被动检测、物理攻击的自动报告和物理攻击抵抗所描述的要求，实现对 TCB 的物理安全保护；
h) **按 5.1.8 条手动恢复、自动恢复、无过分丢失的自动恢复、功能恢复所描述的要求，以手动或自动方式实现对 TCB 运行中断时的恢复；**
i) 按 5.1.9 条重复检测所描述的要求，实现对指定实体的重复检测，及出现重复检测的处理；
j) 按 5.1.10 条参照仲裁所描述的要求进行设计，确保实现 TCB 安全功能的访问监视器和/或前端过滤器是“始终被激活的”；
k) 按 5.1.11 条 SFP 域分离所描述的要求进行设计，确保 TCB 安全功能不受不可信主体的干扰和篡改；
l) 按 5.1.12 条相互的可信回执的要求进行设计，确保在分布式系统中实现的 TCB 安全功能保持同步状态；
m) 按 5.1.13 条时间戳的要求，为 TCB 的运行提供可靠的时间戳支持；
n) 按 5.1.14 条 TSF 间的 TSF 数据一致性要求进行设计，确保在分布式系统中或复合式系统环境下交换的 TSF 数据的一致性；
o) 按 5.1.15 条 TCB 内 TSF 数据复制的一致性要求进行设计，确保在跨网络的环境下 TCB 的各部分间的 TSF 数据复制的一致性；
p) 按 5.1.16 条 TSF 自检的要求，实现 TSF 在系统初始化期间、在正常运转时周期性、应授权用户请求或在其它条件下进行的自检。

#### 6.5.4.2 资源利用

应通过故障容错、服务优先级和资源分配来增强 TCB 自身的安全性。

在本级中，资源利用的设计应：

a) 按 5.1.17.1 条降级故障容错和受限故障容错的要求，实现 TCB 对指定故障的处理；

b) 按 5.1.17.2 条全部服务优先级的要求，进行 TCB 资源的管理和分配；

c) 按 5.1.17.3 条最小与最大限额的要求，进行 TCB 资源的管理和分配。

#### 6.5.4.3 TCB 访问控制

TCB 所实现的安全功能，一般都是由用户激发的。用户通过建立与 TCB 的会话来实现与 TCB 的交互。TCB 访问控制就是用来对会话进行管理的机制。这种管理机制从会话安全属性、多重并发会话的限定及会话的锁定，到 TCB 访问标签、访问历史和会话建立的管理，来确保 TCB 自身的安全性。

本级中，TCB 访问控制的设计应：

a) 按 5.1.18 条可选属性范围限定的要求，对用以建立会话的安全属性的范围进行限制；

b) 按照 5.1.18 条多重并发会话限定的要求，实现对会话管理的设计；

c) 按照 5.1.18 条会话锁定所描述的要求，实现对会话管理的设计；

d) 按照 5.1.18 条 TCB 访问标签所描述的要求，实现对会话管理的设计；

e) 按照 5.1.18 条 TCB 访问历史所描述的要求，实现对会话管理的设计；

f) 按照 5.1.18 条 TCB 会话建立所描述的要求，实现对会话管理的设计。

#### 6.5.4.4 可信路径/信道

在一个 TCB 中，可以有多个 TSF，它们之间需要进行数据交换；用户为实现某种安全功能，也需要与 TSF 进行数据交换。为此，要求 TCB 应：

a) 按 5.1.19.1 条 TSF 间可信信道的要求进行数据交换的设计；

b) 按 5.1.19.2 条用户与 TSF 间可信路径的描述进行数据交换的设计。

### 6.5.5 TCB 设计和实现

#### 6.5.5.1 配置管理

应按照 5.2.1 条配置管理的要求进行设计。本级配置管理应满足：

a) 5.2.1.1 条**完全 CM 自动化**的要求；

b) 5.2.1.2 条版本号、配置项、授权控制及生成支持和验收过程的要求；

c) 5.2.1.3 条 TCB 配置管理范围、问题跟踪配置管理范围和开发工具配置管理范围的要求；

d) 将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下。

#### 6.5.5.2 分发和操作

应以文档形式提供对 TCB 安全地进行分发以及安装、生成和启动的过程进行说明。具体要求为：

a) 按 5.2.2.1 条分发过程、修改检测和修改防止的要求编制说明；

b) 按 5.2.2.2 条安装、生成和启动过程及日志生成所描述的要求编制说明。

#### 6.5.5.3 开发

应按照 5.2.3 条所描述的对开发的要求进行 TCB 开发。本级要求：

a) 按 5.2.3.1 条**形式化功能设计**的要求进行功能设计；

b) 按 5.2.3.2 条**形式化高层设计**的要求进行高层设计；

c) 按 5.2.3.3 条 TSF 的结构化实现的要求进行实现表示设计；

d) 按 5.2.3.4 条模块化和复杂性最小化的要求进行内部结构设计；

e) 按 5.2.3.5 条**形式化低层设计**的要求进行低层；

f) 按 5.2.3.6 条**形式化对应性说明**的要求进行表示的对应性设计；

g) 按 5.2.3.7 条**形式化 TCB 安全策略模型**的要求进行安全策略模型的设计。

#### 6.5.5.4 指导性文档

TCB 应按照 5.2.4 条所描述的对指导性文档的要求进行设计。本级除要求根据上述配置管理、分发和操作、开发以及测试等方面的要求提供管理员指南和用户指南外，要求文档还应包括生命周期支持和脆弱性评定等方面的内容。

#### 6.5.5.5 生命周期支持

应按照 5.2.5 条生命周期支持所描述的要求进行设计。本级 TCB 的设计应满足：

a) 5.2.5.1 条安全措施和安全措施的充分性的要求；

b) 5.2.5.2 条**系统缺陷纠正**的要求；

c) 5.2.4.3 条**可测量的生命周期模型**的要求；

d) 5.2.5.4 条明确定义的开发工具和**遵照实现标准-所有部分**所描述的要求。

#### 6.5.5.6 测试

应按照 5.2.6 条所描述的有关要求对所开发的 TCB 进行测试。本级测试应满足：

a) 5.2.6.1 条范围的证据和严格的范围分析的要求；

b) 5.2.6.2 条高层设计测试、低层设计测试和实现表示测试的要求；

c) 5.2.6.3 条顺序的功能测试的要求；

d) 5.2.6.4 条相符性独立测试和抽样独立性测试的要求。

#### 6.5.5.7 脆弱性评定

应按照 5.2.7 条所描述的要求对所开发的 TCB 进行脆弱性评定。本级评定应按照：

a) 5.2.7.1 条**彻底的隐蔽信道分析**的要求；

b) 5.2.7.2 条指南检查、分析确认及对安全状态的检测和分析的要求；

c) 5.2.7.3 条 TCB 安全功能强度评估的要求；

d) 5.2.7.4 条脆弱性分析中开发者脆弱性分析、独立脆弱性分析和**高级抵抗力**的要求。

### 6.5.6 TCB 安全管理

应根据本级中安全功能技术要求所涉及的物理安全、运行安全、信息安全和安全保证技术要求所涉及 TCB 自身安全与 TCB 设计和实现的有关内容，按照 5.3 条 TCB 安全管理所描述的有关要求，设计 TCB 安全管理要求。本级要求将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限。同时，他们之间应形成相互制约的关系。

本级应按以下要求制定相应的操作、运行规程和行为规章制度：

a) 5.3.1 条 TSF 的功能管理的要求；

b) 5.3.2 条管理安全属性、安全的安全属性和静态属性初始化的要求；

c) 5.3.3 条管理 TSF 数据、TSF 数据界限的管理和安全的 TSF 数据的要求；

d) 5.3.4 条安全角色的定义、安全角色的限制、安全角色的担任的要求；

e) 5.3.5 条安全属性终止的要求；

f) 5.3.6 条安全属性撤消所描述的要求。

# 附 录 A

（规范性附录）

## 标准概念说明

### A.1 组成与相互关系

信息安全是指信息的保密性、完整性和可用性（含可控性，不可否认性，互操作性等）。计算机信息系统安全包括计算机信息系统的安全运行和运行中的计算机信息系统的信息安全。根据计算机信息系统安全等级保护的总体要求，计算机信息系统安全要求的具体内容应从五个安全层面、三个安全特性和五个安全等级进行考虑。其相互关系如图 A.1 所示。

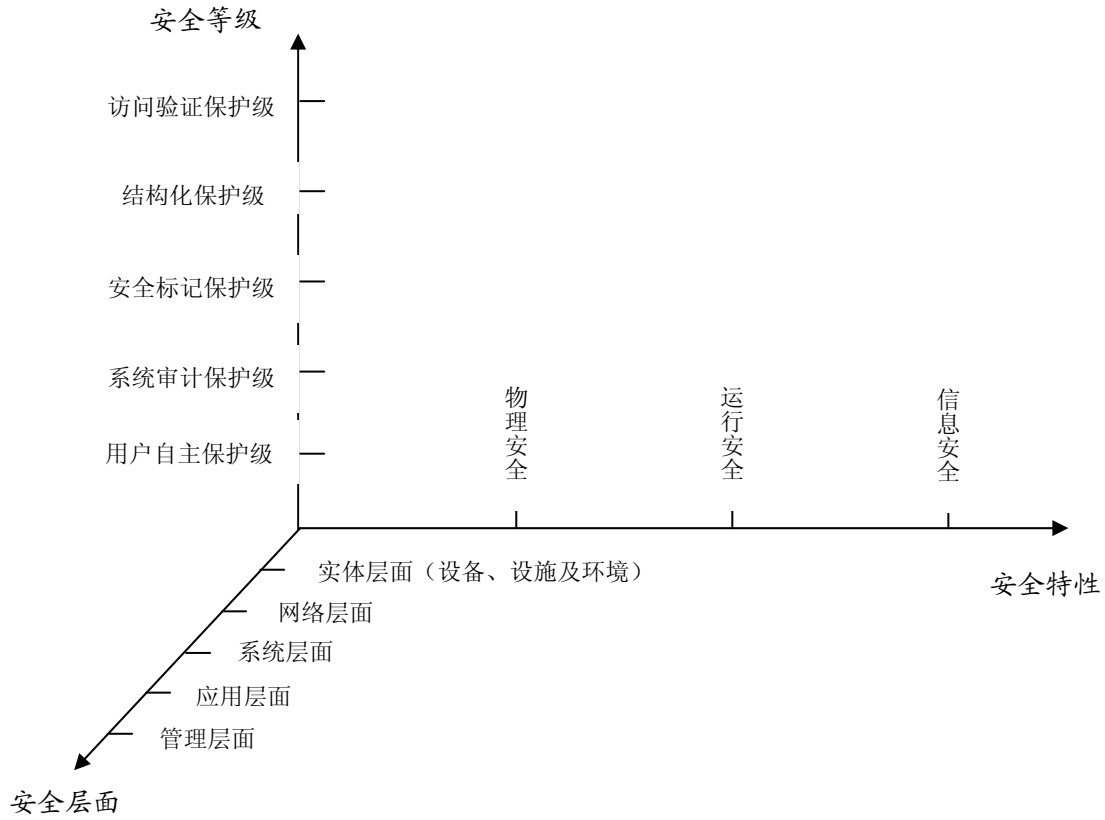


图 A.1 《通用技术要求》的组成与相互关系

图中五个层面是指：

a) 实体层面：硬件系统（含设备、设施、介质及环境等）；

b) 系统层面：操作系统、数据库系统（含运行和信息）；

c) 网络层面：网络系统（含运行和信息）；

d) 应用层面：应用系统（含运行和信息）；

e) 管理层面：系统安全管理（含物理安全、运行安全和信息安全的管理）。

三个安全特性是指：

a) 物理安全（含安全功能和安全保证）；

b) 运行安全（含安全功能和安全保证）

c) 信息安全（含安全功能和安全保证）。

五个等级则是指《计算机信息系统安全保护等级划分准则》所规定的等级。

本标准从物理安全、运行安全和信息安全三个方面对计算机信息系统安全等级保护五个层面所涉及的安全功能技术要求和安全保证技术要求做详细说明，并在此基础上，以《准则》五个等级划分的要求为基础，对每一个等级的安全功能技术要求和安全保证技术要求分别做详细说明。

物理安全主要描述实体层面所涉及的硬件系统及其环境的安全；运行安全则包括系统层面、网络层面和应用层面所涉及的操作系统、数据库系统、网络系统和应用系统的运行安全；信息安全则包括系统层面、网络层面和应用层面所涉及的操作系统、数据库系统、网络系统和应用系统的信息安全；管理层面所涉及的与技术密切相关的物理安全、运行安全和信息安全的管理，作为安全保证的内容，在 TCB 安全管理中描述，有关行政管理方面的内容另有专门标准。

安全保证是为确保安全功能达到应有的目标而采取的措施。本标准从 TCB 自身安全、TCB 安全设计和 TCB 安全管理三个方面对安全保证技术要求进行描述。

### A.2 关于安全等级的划分

一个计算机信息系统可能包含多个操作系统和多个数据库系统，以及多个独立的网络产品，网络系统也可能十分复杂。操作系统的安全、数据库系统的安全、网络系统的安全以及独立网络产品的安全，都可以单独作为一个独立的安全产品看待，只是他们的复杂程度不同而已。在对一个复杂的计算机信息系统的安全保护等级进行划分时，通常需要对构成这个计算机信息系统的操作系统、网络系统、数据库系统和独立的网络产品的安全性进行全面考虑，选用所需要的安全保护等级的安全产品，并按木桶原理综合分析，确定对该计算机信息系统安全保护等级的划分。

### A.3 关于主体、客体

在一个计算机信息系统中，每一个实体成分都必须或者是主体，或者是客体，或者既是主体又是客体。

主体是一个主动的实体，它包括用户、用户组、终端、主机或进程。系统中最基本的主体应该是用户。系统中的所有事件要求，几乎全是由用户激发的。进程是系统中最活跃的实体，用户的所有事件要求都要通过进程的运行来处理。在这里，进程作为用户的客体，同时又是其访问对象的主体。

客体是一个被动的实体，它可以是按照一定格式存储在一定记录介质上的数据信息，也可以是运行于某一网络节点上的进程。系统中最终的客体应该是记录介质及其信息。系统中的另一类实体，如进程，有着双重身份。当一个进程运行时，它必定为某一用户服务——直接或间接地处理该用户的事件要求。于是，该进程成为该用户的客体。系统中运行的任一进程，总是直接或间接为某一用户服务。这种服务关系可以构成一个服务链，最原始的主体是用户，最终的客体则是一定记录介质上的信息。

用户进程是固定为某一用户服务的，它在运行中代表该用户对客体资源进行访问，其权限应与所代表的用户相同（通过用户-主体绑定实现）。系统进程是动态的为所有用户提供服务的，因而它的权限是随着服务对象的变化而变化的,这就需要将用户的权限与为其服务的进程的权限动态地相关联(通过用户-主体绑定实现)。

### A.4 关于TCB、TSF、TSP、SFP及其相互关系

TCB、TSF、TSP、SFP 是《通用技术要求》中的重要的概念。在计算机信息系统中，TCB（可信计算基）是构成一个安全的计算机信息系统的所有安全保护装置的组合体。一个 TCB 可以包含多个 TSF（TCB 安全功能模块）,每个 TSF 是一个或多个 SFP（安全功能策略）的实现。TSP（TCB 安全功能策略）

是这些 SFP 的总称，构成一个安全域，以防止不可信主体的干扰和篡改。实现 TSF 有两种方法，一种是设置前端过滤器，另一种是设置访问监督器。两者都是在一定硬件基础上通过软件实现确定的安全策略，并提供所要求的附加服务。在网络环境下，一个 TCB 可能跨网络实现，构成一个物理上分散、逻辑上统一的分布式 TCB。

### A.5 关于引起信息流动的方式

在计算机信息系统中，引起信息流动的方式可以分为两类。一类是请求访问方式，另一类是信息交换方式。请求访问方式主要出现在以客户/服务器模式运行的系统中。在这种方式中，客户方作为主体向服务器方（客体）发出访问请求，由服务器进程代替客户进程实现对指定数据进行访问操作。这种访问操作一般包括读操作、写操作、运算处理操作或其组合操作。

信息交换方式则主要出现在以网络连接的各个计算机节点之间的数据交换。欲交换数据的双方首先需建立连接，经确认身份后方可进行数据交换。发送方用户作为主体通过运行发送进程将要发送的数据通过网络传送到接收方，接收方的相应进程作为客体接收该数据，并作为主体对该数据进行处理或按指定格式记录到某种记录介质上。

### A.6 关于密码技术

密码技术已成为当今计算机信息系统安全保护的关键技术。在不同安全保护等级中所采用的不同安全策略，应选取不同配置的密码技术作为构成信息安全保护的重要机制，或将密码技术与系统安全技术相结合，组成统一的安全机制。TSF 可以利用密码功能来满足一些特定的安全要求。这里主要是指由密码系统提供的以下支持：标识与鉴别、抗抵赖、传输数据加密保护、存储数据加密保护、传输数据的完整性保护、存储数据的完整性保护等。各个安全等级密码技术的具体配置由国家密码主管部门决定。

### A.7 关于安全计算机信息系统的开发方法

开发一个安全的计算机信息系统可以有两种途径。一种是从头设计；另一种是对原有系统进行加固。

从头设计是指开发一个完整的新系统。这时，需要将计算机信息系统的信息处理功能与所需要的安全功能一起考虑，在实现信息处理功能的同时构建安全的运行环境。用这种途径所实现的系统核心部分往往就是一个按安全功能要求实现的 TCB。随着信息处理功能的扩展，TCB 的安全功能的控制范围随之扩展，直到信息处理功能全部实现。

对原有计算机信息系统进行加固，是当前常见的增强通用计算机信息系统安全性的方法。这种方法往往只能采用增加外部安全控制模块来实现前端过虑器或访问监督器，其所能实现的安全功能会受到某些限制。比如，要用加固的方法实现一个结构化的 TCB 设计是十分困难的。因此，采用加固方法目前所能达到的安全保护等级一般最高为第三级。

无论采用哪一种途径，计算机信息系统的安全性设计都应当以构建安全子系统的方法实现。

# 参　考　文　献

1. GB 50174-1993 电子计算机机房设计规范

2. ISO/IEC 15408-1：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part1:Introduction and general model Part 1:Introduction and general model, Version 2.0

3. ISO/IEC 15408-2：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part2:Security functional requirements Part2:Security functional requirements, Version 2.0

4. ISO/IEC 15408-3：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part3:Security assurance requirements Part3:Security assurance requirements, Version 2.0