ICS 35.020
L 09

GA

中华人民共和国公共安全行业标准

GA/T 388—2002

计算机信息系统安全等级保护操作系统技术要求

Operating system technology requirement in computer information system classified security protection

2002-07-15 发布　　2002-07-15 实施

中华人民共和国公安部　发布

目　　次

前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是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由以下标准和其他相关标准组成：

GA/T 390—2002　计算机信息系统安全等级保护通用技术要求；

GA/T 387—2002　计算机信息系统安全等级保护网络技术要求；

GA/T 388—2002　计算机信息系统安全等级保护操作系统技术要求；

GA/T 389—2002　计算机信息系统安全等级保护数据库管理系统技术要求。

本标准是计算机信息系统安全等级保护技术要求系列标准中的第3项。

本标准的附录A是资料性附录。

本标准由中华人民共和国公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：江南计算技术研究所。

本标准主要起草人：汪晓茵 、吉增瑞、徐良华、袁志平。

引　　言

本标准是计算机信息系统安全等级保护技术要求系列标准的重要组成部分，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操作系统，主要从对操作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 GB 17859—1999 中每一个保护等级的安全要求对操作系统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。

本标准按 GB 17859—1999 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。本标准中有关概念的说明见附录 A。本标准参考的主要文件已列在参考文献中。

计算机信息系统安全等级保护操作系统技术要求

1 范围

本标准规定了按照 GB 17859—1999 对操作系统进行安全保护等级划分所需要的详细技术要求。

本标准适用于按照 GB 17859—1999 的安全等级保护要求所进行的操作系统的设计和实现。对于按照 GB 17859—1999 安全等级保护要求对操作系统进行的测试、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可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全等级划分准则

GA/T 390—2002 计算机信息系统安全等级保护通用技术要求

3 术语和定义

GB 17859—1999 和 GA/T 390—2002 确立的术语和定义适用于本标准。

4 安全保护等级划分技术要求

4.1 第一级：用户自主保护级

4.1.1 安全功能

4.1.1.1 身份鉴别

身份鉴别应包括对用户的身份进行标识和鉴别。应按 GA/T 390—2002 中 6.1.3.1.1、6.1.3.1.2 的要求，设计操作系统的身份鉴别功能。本安全等级要求：

a) 应提供用户进入操作系统时的身份标识，并按以下要求进行设计：

——凡需进入操作系统的用户，应先进行标识(建立账号)。

——操作系统用户标识一般使用用户名和用户标识符(UID)。

b) 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，并在存储时有安全保护。

4.1.1.2 自主访问控制

应按 GA/T 390—2002 中 6.1.3.2 的要求，设计操作系统的自主访问控制功能。本安全等级要求：

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，并阻止非授权用户对客体共享。

b) 设置默认功能。当一个主体生成一个客体时，在该客体的访问控制表中相应地应具有该主体设置的默认值。

4.1.1.3 数据完整性

应按 GA/T 390—2002 中 6.1.3.3 的要求，设计操作系统的数据完整性功能，防止数据遭受非授权用户的修改、破坏或删除。本安全等级要求：

对操作系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能。

4.1.2 TCB 自身安全保护

4.1.2.1 TSF 保护

应按 GA/T 390—2002 中 6.1.4.1 的要求，设计操作系统的 TSF 保护。本安全等级要求：

a) 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的系统软件的一个子集，并应防止外部干扰和破坏，如修改其代码或数据结构。

c) 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d) 一个进程的虚地址空间至少应被分为两个段：用户空间和系统空间，两者的隔离应是静态的。驻留在内存中的操作系统应由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户模式下运行的进程对系统段进行写操作，而在系统模式下运行时，应允许进程对所有的虚存空间进行读、写操作。

e) 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义。

f) 应区分普通操作模式和系统维护模式。

4.1.2.2 资源利用

应按 GA/T 390—2002 中 6.1.4.2 的要求，设计操作系统的资源利用。本安全等级要求：

a) 应通过一定措施确保当系统出现某些确定的故障情况时，TSF 也能维持正常运行。

b) 应采取适当的策略，有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配。

c) 应按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，要求配额机制确保用户和主体将不会独占某种受控的资源。

4.1.2.3 TCB 访问控制

应按 GA/T 390—2002 中 6.1.4.3 的要求，设计操作系统的 TCB 访问控制。本安全等级要求：

a) 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对用来建立会话的安全属性的范围进行限制。

b) 按多重并发会话限定中基本限定的要求，进行会话管理的设计。在基于基本标识的基础上，TSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数。

c) 按最小级会话建立机制，对会话建立的管理进行设计。

4.1.3 TCB 设计和实现

4.1.3.1 配置管理

应按 GA/T 390—2002 中 6.1.5.1 的要求，设计操作系统 TCB 的配置管理。本安全等级要求：

应具有基本的配置管理能力，即要求开发者所使用的版本号与所应表示的 TCB 样本完全对应。

4.1.3.2 分发和操作

应按 GA/T 390—2002 中 6.1.5.2 的要求，设计操作系统的 TCB 分发和操作。本安全等级要求：

a) 以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由最终用户考虑，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥作用。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激

活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按最新的系统版本来制作的。

4.1.3.3 开发

应按 GA/T 390—2002 中 6.1.5.3 的要求，进行操作系统 TCB 的开发。本安全等级要求：

a) 按非形式化功能说明、描述性高层设计、TSF 子集实现、TSF 内部结构模块化、描述性低层设计和非形式化对应性说明的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，二重/多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式储存，并以书面形式向用户提供关于软件所有权法律保护的指南。

4.1.3.4 指导性文档

应按 GA/T 390—2002 中 6.1.5.4 的要求，编制 TCB 的指导性文档。本安全等级要求：

a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南。

b) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等。

c) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。

4.1.3.5 生命周期支持

应按 GA/T 390—2002 中 6.1.5.5 的要求，设计操作系统的 TCB。本安全等级要求：

a) 按开发者定义生命周期模型进行开发。

b) 提供安全安装默认值。在未做特殊选择时，应按默认值安装安全机制。

c) 随同系统交付的全部默认用户标识号，在刚安装完时应处于非激活状态，并由系统管理员加以激活。

d) 操作文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

4.1.3.6 测试

应按 GA/T 390—2002 中 6.1.5.6 的要求，对操作系统的 TCB 进行测试。本安全等级要求：

a) 应通过一般功能测试和相符性独立测试，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试。所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

4.1.4 TCB 安全管理

应按 GA/T 390—2002 中 6.1.6 的要求，实现 TCB 的安全管理。本安全等级要求：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置等有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、身份鉴别、数据完整性和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试等所涉及的有

关内容设计 TCB 安全管理。

4.2 第二级：系统审计保护级

4.2.1 安全功能

4.2.1.1 身份鉴别

身份鉴别应包括对用户的身份进行标识和鉴别。应按 GA/T 390—2002 中 6.2.3.1.1 和 6.2.3.1.2 的要求，设计操作系统的身份鉴别功能。本安全等级要求：

a) 应提供用户进入操作系统时的身份标识，并按以下要求进行设计：
   ——凡需进入操作系统的用户，应先进行标识(建立账号)。
   ——操作系统用户标识应使用用户名和用户标识(UID)，并在操作系统的整个生命周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性。
b) 采用口令进行鉴别，并要求在每次用户登录系统时进行鉴别。口令应是不可见的，并在存储和传输时有安全保护。

4.2.1.2 自主访问控制

应按 GA/T 390—2002 中 6.2.3.3 的要求，设计操作系统的自主访问控制功能。在本安全等级要求：

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，并阻止非授权用户对客体的共享。
b) 设置默认功能。当一个主体生成一个客体时，在该客体的访问控制表中相应地具有该主体设置的默认值。
c) 有更细粒度的自主访问控制。对系统中的每一个客体，都应能够实现由客体的创建者以用户指定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。
d) 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。
e) 客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但是，不允许客体拥有者把该客体的控制权分配给其他主体。
f) 定义访问控制属性，并保护这些属性。主体的访问控制属性至少应有：读、写、执行等；客体的访问控制属性应包含可分配给主体的读、写和执行等权限。
g) 定义分配和修改主体和客体的访问控制属性的规则，并执行对主体和客体的访问控制属性的分配和修改，规则的结果应达到只有被授权的用户才允许访问一个客体。
h) 定义主体对客体的访问授权规则。该规则应基于主体对客体的访问控制属性，同时应指出主体和客体对这些规则应用的类型。

4.2.1.3 客体重用

应按 GA/T 390—2002 中 6.2.3.4 的要求设计操作系统的客体重用功能。本安全等级要求：

a) 应确保动态分配与管理的资源，在保持信息安全的情况下被再利用，主要包括：
   ——确保非授权用户不能查找使用后返还系统的记录介质中的信息内容；
   ——确保非授权用户不能查找系统现已分配给他的记录介质中以前的信息内容。
b) 在单用户系统中，存储器保护应防止用户进程影响系统的运行。
c) 在多用户系统中，存储器保护应保证系统内各个用户之间互不干扰。
d) 存储器保护应包括：
   ——对存储单元的地址的保护，使非法用户不能访问那些受到保护的存储单元；
   ——对被保护的存储单元的操作提供各种类型的保护。最基本的保护类型是“读/写”和“只读”。不能读/写的存储单元，若被用户读/写时，系统应及时发出警报或中断程序执行。

——可采用逻辑隔离的方法进行存储器保护，具体有：界限地址寄存器保护法、内存标志法、锁保护法和特征位保护法等。

4.2.1.4 审计

应按GA/T 390—2002中6.2.2.3的要求设计操作系统的审计功能。本安全等级要求：

a) 审计功能应与身份鉴别、自主访问控制等安全功能紧密结合。

b) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问。

c) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

d) 指出可记录的审计事件的最少类型，包括建立会话登录成功和失败，使用的系统接口，系统数据库管理的改变(改变用户账户属性、审计跟踪设置和分析、为程序分配设置用户ID、附加或改变系统程序或进程、改变日期和时间等)，超级用户命令改变用户身份、将某个客体引入某个用户的地址空间(如打开文件)、删除客体、系统管理员及系统安全管理员进行的操作等。当审计激活时应确保审计跟踪事件的完整性；应提供一个机制来显示当前选择的审计事件，这个机制的使用者应是有限的授权用户。

e) 每个事件的数据记录，应包括的信息有：事件发生的日期和时间、触发事件的用户、事件的类型、事件成功或失败等。对于身份识别和认证事件，应记录请求的源(如末端号或网络地址)；对于创建和删除客体的事件，应记录客体的名字和客体的安全属性。

f) 应提供一个受保护的打开和关闭审计的机制。该机制能选择和改变审计事件，并在系统工作时处于默认状态；该机制的使用应受到系统管理员的授权限制，系统管理员应能够选择一个或多个基于身份识别或客体属性的用户的审计活动；审计工具应能够授权个人使用、修改和删除审计；应提供对审计跟踪管理功能的保护，使之可以完成审计跟踪的创建、破坏、腾空和存档；系统管理员应能够定义超过审计跟踪极限的阈值；当存储空间被耗尽时，应能按管理员的指定决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

4.2.1.5 数据完整性

应按GA/T 390—2002中6.2.3.5的要求，设计操作系统的数据完整性功能。本安全等级要求：

a) 在对数据进行访问操作时，检查存储在存储介质上的用户数据是否出现完整性错误。操作系统对磁盘设备中存储的数据，可通过增加磁盘扫描程序实现以下功能：

——自动检查文件与磁盘表面是否完好；

——将磁盘表面的问题自动记录下来；

——随时检查、诊断磁盘上的错误。

b) 对操作系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能。

c) 对操作系统中处理的数据，应按回退的要求设计相应的TCB安全功能模块，进行异常情况的操作序列回退，以确保数据的完整性。

4.2.2 TCB自身安全保护

4.2.2.1 TSF保护

应按GA/T 390—2002中6.2.4.1的要求，设计操作系统的TSF保护。本安全等级要求：

a) 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的系统软件的一个子集，并应防止外部干扰和破坏，如修改其代码或数据结构。

c) 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d) 一个进程的虚地址空间至少应被分为两个段：用户空间和系统空间，两者的隔离应是静态的。

驻留在内存中的操作系统应由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户模式下运行的进程对系统段进行写操作，而在系统模式下运行时，应允许进程对所有的虚存空间进行读、写操作。

e) 提供设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义。

f) 应区分普通操作模式和系统维护模式。

g) 应防止一个普通用户从未经允许的系统进入维护模式，并应防止一个普通用户与系统内维护模式交互。从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。

h) 对备份或不影响 TCB 的常规的系统维护，不要求所有的系统维护都在维护模式中执行。

i) 当操作系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。

j) 执行系统所提供的实用程序，应(默认地)限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

k) 操作环境应为用户提供一个机制，来控制命令的目录/路径的查找顺序。

l) 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。并按失败保护中所描述的内容，实现对 TSF 出现失败时的处理。

m) 操作系统环境应控制和审计系统控制台的使用情况。

n) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密模式传送。

4.2.2.2 资源利用

应按 GA/T 390—2002 中 6.2.4.2 的要求，设计操作系统的资源利用。本安全等级要求：

a) 应通过一定措施确保当系统出现某些确定的故障情况时，TSF 也能维持正常运行，如系统应检测和报告系统的服务水平已降低到预先规定的最小值。

b) 应采取适当的策略，有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配。

c) 应按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，要求配额机制确保用户和主体将不会独占某种受控的资源。

d) 系统应确保在被授权的主体发出请求时，资源能被访问和利用。

e) 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。

f) 系统应提供维护状态中运行的能力，在维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。

g) 系统应以每个用户或每个用户组为基础，提供一种机制，控制他们对磁盘的消耗和对 CPU 的使用。

4.2.2.3 TCB 访问控制

应按 GA/T 390—2002 中 6.2.4.3 的要求，设计操作系统的 TCB 访问控制。本安全等级要求：

a) 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试，对用来建立会话的安全属性的范围进行限制。

b) 按多重并发会话限定中基本限定的要求，进行会话管理的设计。在基于基本标识的基础上，TSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数。

c) 按最小级会话建立机制，对会话建立的管理进行设计。

d) 在建立 TCB 会话之前，应认证用户的身份。登录机制不允许认证机制本身被旁路。

e) 成功登录系统后，TCB 应向用户显示以下数据：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——应显示口令到期的天数；

——成功或不成功的事件次数的显示可以用整数计数、时间戳列表等表述方法。

4.2.3 TCB 设计和实现

4.2.3.1 配置管理

应按 GA/T 390—2002 中 6.2.5.1 的要求设计配置管理。本安全等级要求：

a) 在配置管理能力方面应实现对版本号、配置项、授权控制等方面的要求。

b) 在 TCB 的配置管理范围方面，应将 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。

c) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

4.2.3.2 分发和操作

应按 GA/T 390—2002 中 6.2.5.2 的要求，设计操作系统的 TCB 分发和操作。本安全等级要求：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。

b) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程。

c) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制系统的方式，确认安全性会由最终用户考虑，所有安全机制都应以功能状态交付。

d) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

e) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

f) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的系统软件是严格按最新的系统版本来制作的。

4.2.3.3 开发

应按 GA/T 390—2002 中 6.2.5.3 的要求，进行操作系统 TCB 的开发。本安全等级要求：

a) 要求按非形式化功能说明、完全定义的外部接口、描述性高层设计、TSF 子集实现、TSF 内部结构模块化和层次化、描述性低层设计、非形式化对应性说明以及非形式化安全策略模型的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，二重/多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知

用户。

e) 系统控制数据，如口令和密钥，不应在未受保护的程序或文档中以明文形式储存，并以书面形式向用户提供关于软件所有权法律保护的指南。

4.2.3.4 指导性文档

应按 GA/T 390—2002 中 6.2.5.4 的要求，编制 TCB 的指导性文档。本安全等级要求：

a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南，不应包括那些如果公开将会危及系统安全的任何信息。

b) 系统管理员文档应提供：

——关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程；

——一个单独的安装指南，详细说明设置系统的配置和初始化过程，提供一个新系统版本的安全设置和安装文档，包括对所有用户可见的安全相关过程、软件和数据文档的描述。

c) 安全管理员文档应提供：

——有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告；

——与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变用户的安全特征等；

——提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程、为检查能被目录文件所利用的磁盘剩余空间所推荐的过程；

——关于设置所有文件和目录的最低访问许可的建议；

——运行文件系统或磁盘完整性检测所做的建议；

——如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告），为灾害恢复计划所做的建议；

——描述普通侵入技术和其他威胁，并查出和阻止它们的内容。

d) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

4.2.3.5 生命周期支持

应按 GA/T 390—2002 中 6.2.5.5 的要求，设计操作系统 TCB 生命周期支持。本安全等级要求：

a) 应按开发者定义生命周期模型进行开发，并提供开发过程中的安全措施说明。

b) 所有安全软件应提供安全安装默认值。在未做特殊选择时，应按默认值安装安全机制。

c) 随同系统交付的全部默认用户标识号，在安装完时应处于非激活状态，并由系统管理员加以激活。

d) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

e) 如果系统含有加强安全性的硬件，那么管理员、最终用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

4.2.3.6 测试

应按 GA/T 390—2002 中 6.2.5.6 的要求，对操作系统的 TCB 进行测试。本安全等级要求：

a) 应通过一般功能测试和相符性独立测试、测试的范围分析、高层设计的测试，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试，包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。所有被发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

4.2.3.7 脆弱性评定

应按 GA/T 390—2002 中 6.2.5.7 的要求，对所开发的 TCB 进行脆弱性评定。本安全等级要求：

a) 从指南检查、TCB 安全功能强度评估和开发者脆弱性分析等方面进行脆弱性评定。

4.2.4 TCB 安全管理

应按 GA/T 390—2002 中 6.2.6 的要求，实现 TCB 的安全管理。本安全等级要求：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、身份鉴别、客体重用、审计、数据完整性和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、脆弱性评定等所涉及的有关内容设计 TCB 安全管理。

4.3 第三级：安全标记保护级

4.3.1 安全功能

4.3.1.1 身份鉴别

身份鉴别应包括对用户的身份进行标识和鉴别。应按 GA/T 390—2002 中 6.3.3.1.1 和 6.3.3.1.2 的要求，设计操作系统的身份鉴别功能。本安全等级要求：

a) 应提供用户进入操作系统时的身份标识，并按以下要求进行设计：

——凡需进入操作系统的用户，应先进行标识(建立账号)。

——操作系统用户标识应使用用户名和用户标识(UID)，并在操作系统的整个生命周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性。

b) 采用口令、智能 IC 卡、指纹、视网膜等进行鉴别，并要求在每次用户登录系统时进行鉴别。鉴别信息应在存储和传输时应按 GA/T 390—2002 中 6.3.3.8 的要求进行安全保护。

4.3.1.2 自主访问控制

应按 GA/T 390—2002 中 6.3.3.3 的要求，设计操作系统的自主访问控制功能。本安全等级要求：

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) 设置默认功能。当一个主体生成一个客体时，在该客体的访问控制表中相应地具有该主体的默认值。

c) 有更细粒度的自主访问控制，将访问控制的粒度控制在单个用户。对系统中的每一个客体，都应能够实现由客体的创建者以用户指定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。

d) 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。

e) 客体的拥有者应是唯一有权修改客体访问权限的主体，拥有者对其拥有的客体应具有全部控制权，但是，不允许客体拥有者把该客体的控制权分配给其他主体。

f) 定义访问控制属性，并保护这些属性。主体的访问控制属性至少应有：读、写、执行等；客体的访问控制属性应包含可分配给主体的读、写和执行等权限。

g) 定义分配和修改主体和客体的访问控制属性的规则，并执行对主体和客体的访问控制属性的分配和修改，规则的结果应达到只有被授权的用户才允许访问一个客体。

h) 定义主体对客体的访问授权规则。该规则应基于主体对客体的访问控制属性，授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型。

4.3.1.3 标记

应按 GA/T 390—2002 中 6.3.3.4 的要求，设计标记功能。本安全等级要求：

a) 应采用标记的方法为操作系统 TCB 安全功能控制范围内的主体和客体设置敏感标记。这些敏感标记构成多级安全模型的属性库。操作系统主、客体的敏感标记应以默认方式生成或由安全员进行建立、维护和管理。

b) 当信息从 TCB 控制范围之内向 TCB 控制范围之外输出时，可带有或不带有敏感标记；当信息从 TCB 控制范围之外向 TCB 控制范围之内输入时，应通过标记标明其敏感标记。

4.3.1.4 强制访问控制

应按 GA/T 390—2002 中 6.3.3.5 的要求，设计强制访问控制功能。本安全等级要求：

a) 应由专门设置的系统安全员统一管理操作系统中与强制访问控制等安全机制有关的事件和信息，并将系统的常规管理、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，按职能分割原则分别授予它们各自为完成自己所承担任务所需的权限，并形成相互制约关系。

b) 强制访问控制应与用户身份鉴别、标记等安全功能密切配合，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，对客体的控制范围涉及操作系统内部的存储、处理和传输过程。

c) 运行于网络环境的分布式操作系统，应统一实现强制访问控制功能。

d) 运行于网络环境的多台计算机系统上的网络操作系统，在需要进行统一管理时，应考虑各台计算机操作系统的主、客体安全属性设置的一致性，并实现跨网络的 TCB 间用户数据保密性和完整性保护。

4.3.1.5 客体重用

应按 GA/T 390—2002 中 6.3.3.6 的要求，设计操作系统的客体重用功能。本安全等级要求：

a) 应确保动态分配与管理的资源，在保持信息安全的情况下被再利用，主要包括：

——确保非授权用户不能查找使用后返还系统的记录介质中的信息内容；

——确保非授权用户不能查找系统现已分配给他的记录介质中以前的信息内容。

b) 在单用户系统中，存储器保护应防止用户进程影响系统的运行。

c) 在多用户系统中，存储器保护应保证系统内各个用户之间互不干扰。

d) 存储器保护应包括：

——对存储单元的地址的保护，使非法用户不能访问那些受到保护的存储单元；

——对被保护的存储单元的操作提供各种类型的保护。最基本的保护类型是“读/写”和“只读”。不能读/写的存储单元，若被用户读/写时，系统应及时发出警报或中断程序执行；

——可采用逻辑隔离的方法进行存储器保护，具体有：界限地址寄存器保护法、内存标志法、锁保护法和特征位保护法等。

4.3.1.6 审计

应按 GA/T 390—2002 中 6.3.2.4 的要求，设计操作系统的审计功能。本安全等级要求：

a) 审计功能应与身份鉴别、自主访问控制、标记、强制访问控制及完整性控制等安全功能紧密结合。

b) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问。

c) 能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

d) 指出可记录的审计事件的最少类型，包括建立会话登录成功和失败，使用的系统接口，系统数据库管理的改变(改变用户账户属性、审计跟踪设置和分析、为程序分配设置用户 ID、附加或改变系统程序或进程、改变日期和时间等)，超级用户命令改变用户身份、将某个客体引入某个用户的地址空间(如打开文件)、删除客体及计算机操作员、系统管理员与系统安全管理员进程的操作等。当审计激活时应确保审计跟踪事件的完整性；应提供一个机制来显示当前选择的审计事件，这个机制的使用者应是有限的授权用户。

e) 每个事件的数据记录，应包括的信息有：事件发生的日期和时间、触发事件的用户、事件的类型、事件成功或失败等。对于身份识别和认证事件，应记录请求的源(如末端号或网络地址)；对于创建和删除客体的事件，应记录客体的名字和客体的安全属性。

f) 应提供一个受保护的打开和关闭审计的机制。该机制能选择和改变审计事件，并在系统工作时处于默认状态；该机制的使用应受到系统管理员的授权限制，系统管理员应能够选择一个或多个基于身份识别或客体属性的用户的审计活动；审计工具应能够授权个人监察和浏览审计数据，同时数据应得到授权的使用、修改和删除；应提供对审计跟踪管理功能的保护，使之可以完成审计跟踪的创建、破坏、腾空和存档；系统管理员应能够定义超过审计跟踪极限的阈值；当存储空间被耗尽时，应能按管理员的指定决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

4.3.1.7 数据完整性

应按 GA/T 390—2002 中 6.3.3.7 的要求，设计操作系统的数据完整性功能。本安全等级要求：

a) 应为操作系统 TCB 安全功能控制范围内的主体和客体设置完整性标签(IL)，并建立完整性保护策略模型，来保护信息在存储、传输和处理过程中的完整性。

b) 在对数据进行访问操作时，检查存储在存储介质上的用户数据是否出现完整性错误，并在检测到完整性错误时进行恢复。可通过密码支持系统所提供的完整性功能，对加密存储的数据进行完整性保护。操作系统对磁盘设备中存储的数据，可通过增加磁盘扫描程序实现以下功能：

——自动检查文件与磁盘表面是否完好；

——将磁盘表面的问题自动记录下来；

——随时检查、诊断和修复磁盘上的错误；

——修复扇区交错和扇区流失；

——将数据移到好的扇区；

——可增加硬盘数据备份和修复程序，将硬盘中的数据压缩、备份，并在必要时恢复。

c) 在操作系统内部进行的数据传输，如进程间的通信，应提供保证数据完整性的功能。完整性标签应随数据一起流动，系统应保证低完整性的数据不能插入、覆盖到高完整性的数据。

d) 对操作系统中处理的数据，应按回退的要求设计相应的 TCB 安全功能模块，进行异常情况的操作序列回退，以确保数据的完整性。系统应保证在处理过程中不降低数据完整性的级别。

4.3.2 TCB 自身安全保护

4.3.2.1 TSF 保护

应按 GA/T 390—2002 中 6.3.4.1 的要求，设计操作系统的 TSF 保护。本安全等级要求：

a) 系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的系统软件的一个子集，并应防止外部干扰和破坏，如修改其代码或数据结构。

c) 操作系统应进行分层设计，对操作系统程序和用户程序要进行隔离。

d) 一个进程的虚地址空间至少应被分为两个段:用户空间和系统空间,两者的隔离应是静态的。驻留在内存中的操作系统应由所有进程共享。用户进程之间应是彼此隔离的。应禁止在用户模式下运行的进程对系统段进行写操作,而在系统模式下运行时,应允许进程对所有的虚存空间进行读、写操作。

e) 提供设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前,应对用户和管理员的安全策略属性应进行定义。

f) 应区分普通操作模式和系统维护模式。

g) 应防止一个普通用户从未经允许的系统进入维护模式,并应防止一个普通用户与系统内维护模式交互。从而保证在普通用户访问系统之前,系统能以一个安全的方式进行安装和配置。

h) 对备份或不影响 TCB 的常规的系统维护,不要求所有的系统维护都在维护模式中执行。

i) 当操作系统安装完成后,在普通用户访问之前,系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。

j) 执行系统所提供的实用程序,应(默认地)限定于对系统的有效使用,只允许系统管理员修改或替换系统提供的实用程序。

k) 操作环境应为用户提供一个机制,来控制命令的目录/路径的查找顺序。

l) 系统应提供一个实用程序来校验文件系统和磁盘的完整性。此实用程序应由操作系统自动执行。

m) 系统应为系统管理员提供一种机制,来产生安全参数值的详细报告。

n) 在 TCB 失败或中断后,进程应保证保护文本以最小的损害得到恢复。并按失败保护中所描述的内容,实现对 TSF 出现失败时的处理。系统因故障或其他原因中断后,应有一种机制去恢复系统。系统应提供在管理维护状态中运行的能力,管理维护状态只能被系统管理员使用,各种安全功能全部失效。

o) 操作系统环境应控制和审计系统控制台的使用情况。

p) 系统应能识别由通信渠道接收的信息的来源者,所有待确认的数据应能从进入点被安全地传送到确认系统,如口令不应由公共的或共享的网络以明文发送,可使用数据加密设备或通过加密信道用加密模式传送。

4.3.2.2 资源利用

应按 GA/T 390—2002 中 6.3.4.2 的要求,设计操作系统的资源利用。本安全等级要求:

a) 应通过一定措施确保当系统出现某些确定的故障情况时,TSF 也能维持正常运行,如系统应检测和报告系统的服务水平已降低到预先规定的最小值。

b) 应采取适当的策略,有限服务优先级提供主体使用 TSC 内某个资源子集的优先级,进行 TCB 资源的管理和分配。

c) 应按资源分配中最大限额的要求,进行 TCB 资源的管理和分配,要求配额机制确保用户和主体将不会独占某种受控的资源。

d) 系统应确保在被授权的主体发出请求时,资源能被访问和利用。

e) 当系统的服务水平降低到预先规定的最小值时,应能检测和发出报告。

f) 系统应提供维护状态中运行的能力,在维护状态下各种安全性能全部失效,系统只允许由系统管理员使用。

g) 系统应以每个用户或每个用户组为基础,提供一种机制,控制他们对磁盘的消耗和对 CPU 的使用。

h) 系统应提供软件及数据备份和复原的过程,在系统中应加入再启动的同步点,以便于系统的复原。

i) 操作系统应能提供用户可访问的系统资源的修改历史记录。

j) 系统应提供能用于定期确认系统正确操作的机制和过程，这些机制或过程应涉及系统资源的监督、硬件和固件单元的正确操作、对可能在全系统内传播的错误状态的检测以及超过用户规定的门限的通讯差错的检测等内容。

4.3.2.3 TCB 访问控制

应按 GA/T 390—2002 中 6.3.4.3 的要求，设计操作系统的 TCB 访问控制。本安全等级要求：

a) 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试，对用来建立会话的安全属性的范围进行限制。

b) 按多重并发会话限定中基本限定的要求，进行会话管理的设计。在基于基本标识的基础上，TSF 应限制系统的并发会话的最大数量，并应利用默认值作为会话次数的限定数。

c) 按最小级会话建立机制，对会话建立的管理进行设计。

d) 在建立 TCB 会话之前，应认证用户的身份，不允许认证机制被旁路。

e) 成功登录系统后，TCB 应向用户显示以下数据：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——应显示口令到期的天数；

——成功或不成功的事件次数的显示可以用整数计数、时间戳列表等表述方法。

f) 在规定的未使用时限后，系统应断开会话或重新认证用户，系统应提供时限的默认值。

g) 系统应提供锁定用户键盘的机制，键盘开锁过程应要求验证用户。

h) 当用户认证过程不正确的次数达到系统规定的次数时，系统应退出登录过程并终止与用户的交互。

i) 系统应提供一种机制，能按时间、进入方式、地点、网络地址或端口等条件规定哪些用户能进入系统。

4.3.3 TCB 设计和实现

4.3.3.1 配置管理

应按 GA/T 390—2002 中 6.3.5.1 的要求，进行配置管理设计。本安全等级要求：

a) 在配置管理自动化方面要求部分的配置管理自动化。

b) 在配置管理能力方面应实现对版本号、配置项、授权控制等方面的要求。

c) 在 TCB 的配置管理范围方面，应将 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，要求实现对配置管理范围内的问题，特别是安全缺陷问题进行跟踪。

d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保未危及系统的安全。在软件配置管理系统中，应包含从源码产生出系统新版本、鉴定新生成的系统版本和保护源码免遭未授权修改的工具和规程。通过技术、物理和保安规章三方面的结合，可充分保护生成系统所用到的源码免遭未授权的修改和毁坏。

4.3.3.2 分发和操作

应按 GA/T 390—2002 中 6.3.5.2 的要求，设计操作系统的 TCB 分发和操作。本安全等级要求：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程；