专题讲座

信息安全测评标准

王 宏
北京信息安全测评中心

内 容

- 信息安全标准化体系
- 信息安全测评标准发展
- 标准TCSEC、GB 17859
- 标准ISO 15408、GB/T 18336
- 标准DB11/T 171

《党政机关信息系统安全测评规范》

信息安全标准化体系

1　标准化组织简介
2　信息安全标准分类
3　信息安全基础标准
4　信息安全技术标准
5　安全测评标准简介

1 标准化组织简介（部分）

1）国际标准化组织（ISO）
　5000多
2）Internet 体系结构委员会（IAB）
　IETF、IRTF，RFC1421-1424，RFC1510 ...
3）国家标准委员会
　美国国家标准协会（ANSI）等等
4）美国国家标准技术研究所（NIST）
　FIPS PUB、SPEC PUB，DES、FIPS PUB 140-1、
　CC、EES、FPKI、GKMI、AES
5）美国国防部（DoD、NCSC）
　TCSEC、Rainbow系列
6）国际电信联盟（ITU）
　X.400，X.500
7）电气和电子工程师学会（IEEE）
　P1363

2 信息安全标准分类

1）安全体系结构和框架标准：设计其它类标准的基础、参考

2）安全技术标准：广泛适用的技术规范，与分层、具体应用无关

3）层安全协议标准：各层独立于应用的协议规范

4）具体应用安全标准

5）安全管理标准

6）安全测评标准

低层安全协议：TLSP，NLSP，SDE，IPSEC，TLS

高层安全标准：ASN.1、通用高层安全标准GULS

3 信息安全基础标准

把安全性加入OSI体系结构

（1）安全体系结构

（2）安全框架标准

（1）安全体系结构

国际标准ISO 7498-2

OSI安全体系结构不是实现的标准，而是如何设计标准的标准。

关于：术语，安全服务和安全机制的定义，各种安全服务在OSI各层中的位置，作为OSI基本参考模型的补充。

（1）安全体系结构－－基本安全服务

安 全 服 务	安 全 服 务
认证 对等实体认证 数据起源认证	完整性 可恢复的连接完整性 不可恢复的连接完整性 选择字段的连接完整性 无连接完整性 选择字段的无连接完整性
访问控制	
机密性 连接机密性 无连接机密性 选择字段机密性 业务流机密性	非否认 数据起源的非否认 传递过程的非否认

安全审计

（1）安全体系结构－－安全机制

实现安全服务的基本安全机制　　其他安全机制

- 加密
- 数字签名
- 访问控制
- 数据完整性
- 认证交换
- 业务流填充
- 路由控制
- 公证

- 可信功能模块
- 安全标签
- 事件检测
- 安全审计追踪
- 安全恢复

（1）安全体系结构－－服务分层配置

服务 \ 分层	1	2	3	4	5	6	7
对等实体认证			√	√			√
数据起源认证			√	√			√
访问控制服务			√	√			√
连接机密性	√	√	√	√		√	√
无连接机密性		√	√	√		√	√
选择字段机密性						√	√
业务流机密性	√		√				√
可恢复的连接完整性				√			√
不可恢复的连接完整性			√	√			√
选择字段的连接完整性							√
无连接完整性			√	√			√
选择字段的无连接完整性							√
数据起源的非否认							√
传递过程的非否认							√

（2）安全框架标准

详细论述OSI安全体系结构指出的基本安全主题，包括认证、访问控制、机密性、完整性、非否认性、安全审计。

框架标准对整个标准化进程的贡献是给出了一些概念、术语、模型作为其他标准的基础。

框架标准是制定标准的标准，而不是实现的标准。

（2）安全框架标准——通用概念

安全策略：限定对象与安全相关的活动之规则集。

安全机构：对安全策略的实现负责，使用安全策略限制其他实体的活动。

安全区域：对象在进行安全相关活动时，安全权威机构根据安全策略进行管理。

安全交互规则：安全域之间交互的规则。

3 信息安全基础标准——小结

OSI安全体系结构和框架标准，作为“标准的标准”有以下两个实际用途：

1）为设计可实现的安全标准提供指南；

2）为以后的标准的术语提供参考源。

4 信息安全技术标准

（1）密码算法

（2）封装和数字签名

（3）实体认证

（4）密钥管理

（5）安全标签

（6）其他安全技术标准

（1）密码算法

NIST两次征集密码算法标准：DES、AES

ISO政策：不进行密码算法的标准化。

算法的注册程序标准化

ISO/IEC 9979标准制定了密码算法注册服务的程序，注册机构分配唯一的标识符（ASN.1）。

算法的工作模式标准化

FIPS PUB 81：DES工作模式的标准

ISO 8372（1987）：64位加密算法的工作模式

ISO 10116（1991）：n位加密算法的工作模式

（2）封装和数字签名

消息认证码

ISO 9797（通用MAC标准，支持DES之外的算法）

带附录的数字签名

GB/T 17902

具有消息恢复功能的数字签名

ISO 9796

(3) 实体认证

基于对称密码技术的实体认证

ISO/IEC 9798-2

基于公钥密码技术的实体认证

ISO/IEC 9798-3

(4) 密钥管理

ISO 8732 银行-密钥管理（批发）

FIPS PUB 171 政府应用

ISO/IEC 11770 密钥管理标准（—2 对称技术、—3 公钥技术），密钥分发

ISO 11568 不限于DES，引入公钥技术

ISO 11166 金融服务—基于公钥算法的密钥管理

（5）安全标签

在网络中，安全标签主要用于路由控制—数据报，消息，或连接所带的标签将决定它是否被允许到达或通过某网络。

美国联邦政府和Internet团体为开放式系统中的政府应用规定了标准标签格式。

IP安全选项（GOSIP、DoD IPSO、CIPSO）

ISO/IEC 8473

（6）其他安全技术标准

PKIX、SPKI

S/MIME 、Open PGP

EDIFACT、SET

S-HTTP

Kerberos

PKCS

（7）安全测评标准简介

- 安全测评需求
- 公正的产品测评的组织，制定独立的产品测评标准
- 产品的认可或产品的证书
- 安全测评标准适用方：产品开发商（供应方）、购买者（客户）、测评者
- 安全测评已成为专门领域

（7）安全测评标准简介——标准

- DoD准则
- CC通则
- 党政机关信息系统安全测评规范
- 密码设备的评估准则

（7）安全测评标准简介－密码设备的评估

- FIPS PUB 140-1
- FIPS PUB 140-2 (NIST 1999)

（7）安全测评标准简介－FIPS 140-2

- 四个安全级别
- 十一个要求

（7）安全测评标准简介－FIPS 140-2

- 级别1：最低的安全级别。
- 为密码模块指定基本的安全要求（如，加密算法是经过NIST认可的）。在密码模块中没有要求物理安全机制作为产品-等级装备的要求。安全级别1允许在通用目的的PC中用软件执行密码功能。

（7）安全测评标准简介－FIPS 140-2

- 级别2：增加明显的防窜挠外壳、封条或防撬锁等要求来改进密码模块的物理安全。
- 明显的防窜挠外壳或封条被放置到一个密码模块上使得外壳或封条在对模块中的明文密钥和其它关键安全参数（CSPs）进行物理访问时就会被破坏。
- 最小的安全级别2要求基于角色的认证，其中密码模块认证操作员是否是假定的特定角色，并执行相应的服务集合。
- 安全级别2允许在多用户的分时系统使用软件密码，但所使用的操作系统需满足要求：满足通用准则（CC）中的控制式访问保护轮廓（CAPP）所描述的功能要求；满足CC中的评估保证级别EAL2。

（7）安全测评标准简介－FIPS 140-2

- 级别3：除了明显的防窜挠要求外，如果覆盖物被除掉或门被打开，任何未保护的关键安全参数（CSPs）都被清零。
- 安全级别3要求基于身份的认证。密码模块认证操作员的身份和检查被认证的操作员是否是授权的假定的特定角色，并执行对应的服务集合。
- 安全级别3要求输入和输出CSPs的数据端口与其他的数据端口在物理上分开。
- 安全级别3允许在多用户分时系统中使用软件密码，但所使用的操作系统需满足要求：满足CAPP中描述的功能要求和可信通路（FTP_TRP.1）功能要求；满足CC中的评估保证级别EAL3和具有非形式化的TOE的安全政策模型（ADV_SPM.1）的保证要求。

（7）安全测评标准简介－FIPS 140-2

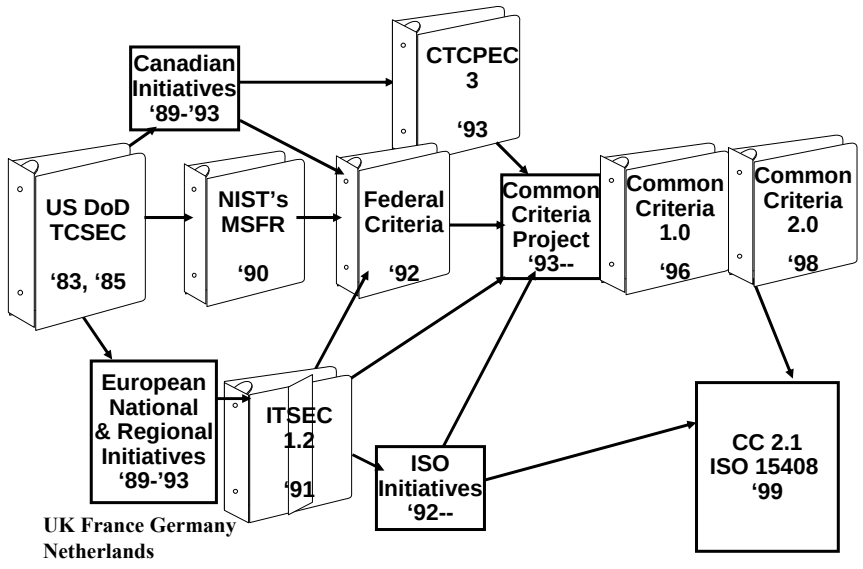
- 级别4：最高级别的安全性。
- 物理安全在密码模块周围提供可以检测察觉从任何方向试图渗透的保护封套。（检测到破坏后所有的关键安全参数被清零。）
- 安全级别4也保护密码模块对抗由于环境的条件或波动外部电压和温度带来的影响。
- 安全级别4允许在多用户分时系统中使用软件密码，但所使用的操作系统需满足要求：满足级别3的功能要求；满足EAL4和形式化的TOE安全策略模型（ADV_SPM.3），隐通道分析（AVA_CCA.1）和模块化（ADV_INT.1）保证要求。

信息安全测评标准发展

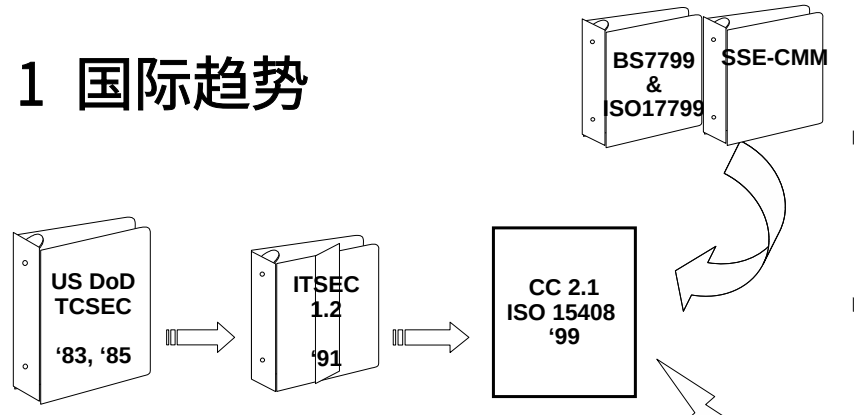
1 国际趋势

2 国内趋势

1 国际趋势



1 国际趋势

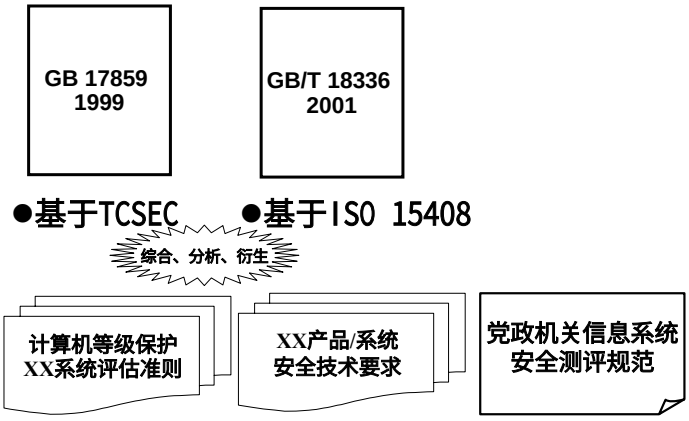


- ●可信系统
- ●主要面向单机系统、OS
- ●安全性：访问控制、保密、审计

- ●保护轮廓PP
- ●安全性：较全面

- ●IT安全“字典”
- ●产品、系统，适应网络发展
- ●安全功能、保证要求集
- ●评估保证级
- ●CC—PP—ST

2 国内趋势



标准TCSEC、GB 17859

1 橘皮书：可信计算机系统评估准则
2 红皮书：网络环境、数据库
3 国标：GB 17859

1 橘皮书

（1）概述
（2）分级要求

（1）概述

- 可信计算机系统评估准则（TCSEC）
- 橘皮书的重点在于提供对敏感信息的机密性保护
- 橘皮书主要被用于操作系统评估

（1）概述

- 系统安全六个方面：
  （1）安全策略：系统实施的安全策略；
  （2）标识：访问控制标志与客体相联系；
  （3）识别：单独的主体必须被识别；
  （4）责任：审计信息必须被有选择地保存和保护起来，使影响安全的行为可以被追踪；
  （5）保证：计算机系统必须包括硬件/软件机制，这些机制能够独立地评估以确定系统能否执行上述四项要求；
  （6）持续的保护：能够执行这些基本需求的可信机制，必须被连续地保护以抵御篡改和未授权的修改。

（1）概述

- 两大部分：

  第一部分详细地说明了对计算机系统安全等级的划分准则，这种划分完全建立在人们对敏感信息保护的信心基础上。

  第二部分讨论了此准则开发的基本目标、基本原理和美国政府的政策。它也为开发者提供了关于隐通道，安全测试和强制（多级）访问控制的实现指南。

（2）分级要求

- 四个等级七个级别：

  D，C，B，A

  D，C1，C2，B1，B2，B3，A1

（2）分级要求－－D

- D级：

（最小保护）

经评估的系统无法达到较高的安全级别，不具备安全特征。

（2）分级要求－－C1

- C1级：

（自主安全保护）

用户和数据分离，满足自主需求。各种控制能力组合成一体，每一个实体独立地实施访问控制能力。用户能够保护个人信息和防止其它用户读和破坏，但还不足以保护系统中的敏感信息。

（2）分级要求－－C2

- C2级：

（控制访问保护）

比C1级系统更细粒度的自主访问控制。使用户通过登录程序、安全相关事件的审计和资源隔离等措施单独地为他们的行为负责。客体重用的规定，确保存储信息再分配时，不会泄露给一个新的用户。C2级可视作处理敏感信息所需的最低安全级别。

（2）分级要求－－B1

- B1级：

（基于标签的安全保护）

首个需要强制访问控制支持的级别。系统必须对主要数据结构加载敏感度标签。系统必须给出有关安全策略模型、数据标签和大量主体客体之间的出入控制的非形式陈述。系统必须具备精确标识输出信息的能力。

（2）分级要求－－B2

- B2级：

(结构化保护)

TCB必须是被建立在一个形式的安全策略模型上。在B1级系统中所采用的自主式和强制式访问控制被扩展到B2级系统中的所有客体和主体。在这一级别上还特别强调了隐通道分析。TCB必须被特别地结构化，授权机制被加强。需要有特殊化系统管理员和操作员功能以及严格的配置管理控制能力。

（2）分级要求－－B3

- B3级：

(安全域)

TCB必须监控所有客体到主体的访问，必须是防窜扰的，必须足够小以便于分析和测试。对系统结构作了进一步限制，要求支持安全管理员功能，将审计机制扩充到信号的安全相关事件，需要可信系统恢复过程。

（2）分级要求－－A1

- A1级：
  （验证设计）
  采用安全策略的形式模型。功能上等价于B3级。然而，形式设计规范和验证技术必须贯穿于整个开发过程。存在一个可信的分发系统。

2 红皮书

- TCSEC的可信计算机网络注释（TNI）
- TCSEC的可信计算机数据库注释（TDI）
- 彩虹（Rainbow）系列
- 红皮书第一部分为桔皮书应用于网络环境的指南。为网络产品指定安全级别的基础，包括从局域网到广域网的计算机。
- 第二部分描述附加的安全服务。如，认证、非否认和网络管理。可为安全产品给出定性的安全性估计。

3 国标GB 17859

- 本质上等同于TCSEC
- 舍弃D、A1级，划分为五级
- 第一级
- 第二级
- 第三级
- 第四级
- 第五级

标准ISO 15408、GB/T 18336

1 欧洲ITSEC
2 西方六国CC、国际标准ISO 15408
3 国标GB/T 18336

1 欧洲ITSEC

（1）概述

（2）分级简介

（1）概述

- 英国用于商业安全产品的绿皮书
- 法国的蓝-白-红书
- 德国的国家准则
- 法国、德国、荷兰和英国 信息技术安全评测准则（ITSEC），由欧洲共同体委员会发布。
- ITSEC目标是适用于更多的产品、应用和环境，为评估产品和系统提供一致的方法。在安全特征和安全保证之间提供了明显的区别。不特别限定功能要求。

（2）分级简介－－功能级

- 五个功能级别：
- F-C1，F-C2，F-B1，F-B2，F-B3
- 与TCSEC的对应

（2）分级简介－－保证级

- 七个评估级别：

E0级：不充分的保证。
E1级：有安全目标和对体系结构设计的非形式描述。功能测试。
E2级：还对详细的设计有非形式的描述。功能测试的证据必须被评估。有配置控制系统和认可的分配过程。
E3级：要评估与安全机制相对应的源代码和/或硬件设计图。还要评估测试这些机制的证据。
E4级：有支持安全目标的安全策略的基本形式模型。用半形式的格式说明安全加强功能、体系结构和详细设计。
E5级：在详细的设计和源代码和/或硬件设计图之间有紧密的对应关系。
E6级：必须正式说明安全增强功能和体系结构设计，使其与安全策略的基本形式模型一致。

2 西七CC、国际标准IS015408

(1) 背景
(2) 概述
(3) 安全功能
(4) 安全保证
(5) 评估保证级

(1) 背景

- 加拿大可信计算机产品评估准则（CTCPEC）：在安全功能与保证分离方面更进了一步。为四类功能类定义了不同的准则：机密性、完整性、可用性和审计，再加上一个保证类。每类分子类，每个子类定义了评估级别。
- 美国联邦准则(FC)：扩展访问控制，涉及完整性和可用性方面，定义了不同的保护轮廓来适应不同环境的安全要求。增加了对商用环境。
- ISO/IEC 15408 通用安全评价准则（CC）Common Criteria for IT security Evaluation ：美、荷、法、德、英、加

（2）概述

- 主要分两大部分：安全功能要求、安全保证要求
- 功能与保证分离，面向组件，仅对保证定级
- 衍生保护轮廓（PP）和安全目标（ST）来评估具体的产品和系统
- PP面向安全环境：威胁，假设，安全策略，IT环境安全要求
- PP构造安全目的、要求的基本原理，映射关系

（2）概述

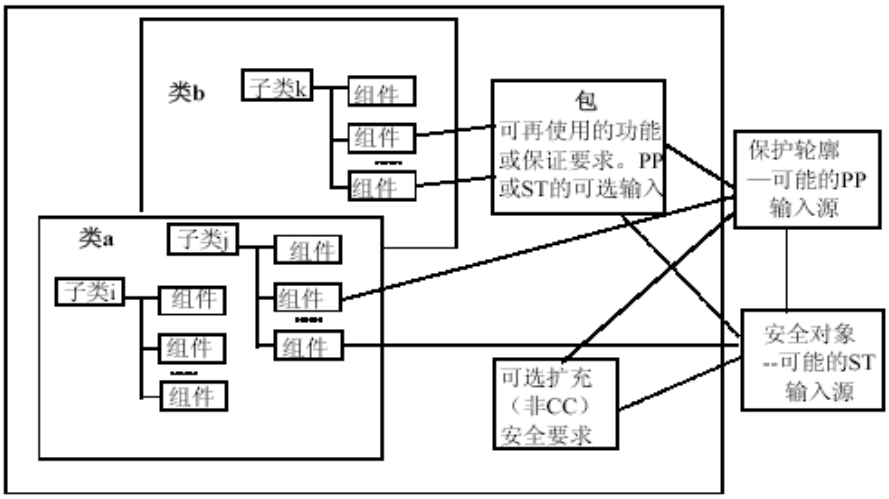


图 5.6　要求的组织和结构

(3) 安全功能

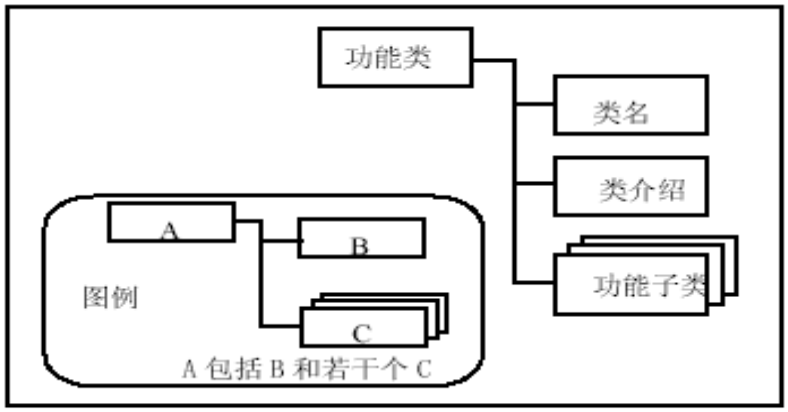


图3.1　功能类结构

(3) 安全功能

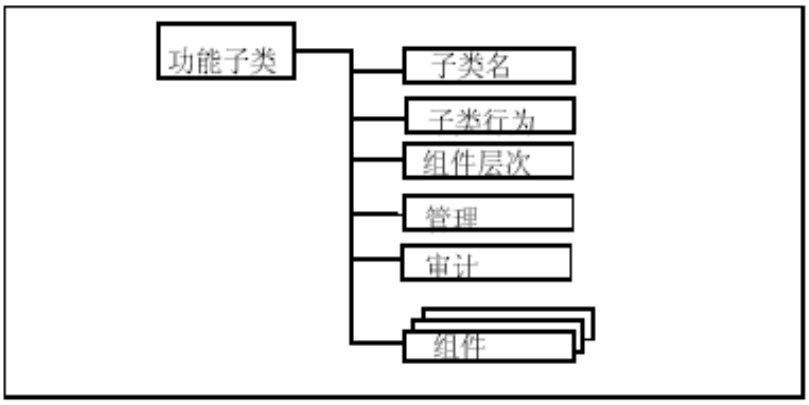


图3.2　功能子类结构

(3) 安全功能

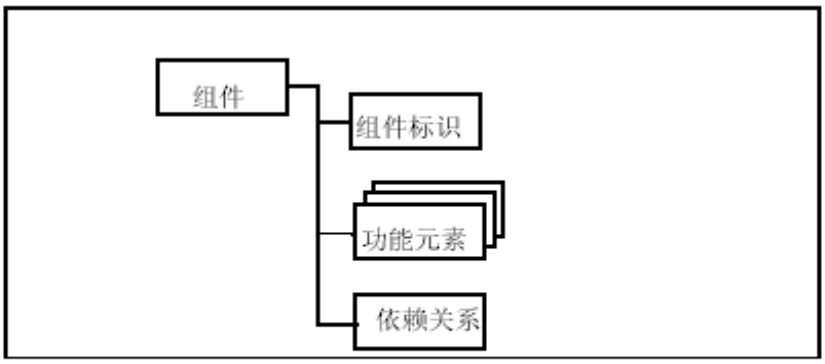


图3.3 功能组件结构

(3) 安全功能

- 允许的功能组件操作：
  - 反复
  - 赋值
  - 选择
  - 细化

（3）安全功能

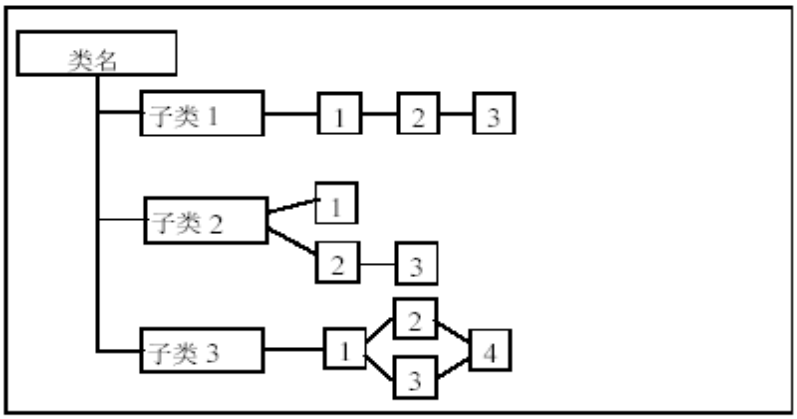


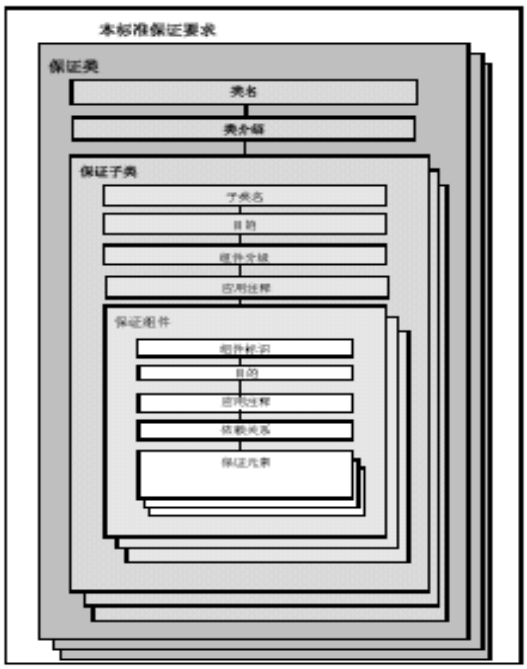
图3.4　示范类分解图

（3）安全功能

11个功能类：

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

(4) 安全保证



(4) 安全保证

保证类	保证子类	缩写名称
ACM 类：配置管理	CM 自动化	ACM_AUT
	CM 能力	ACM_CAP
	CM 范围	ACM_SCP
ADO 类：交付和运行	交付	ADO_DEL
	安装、生成和启动	ADO_IGS
ADV 类：开发	功能规范	ADV_FSP
	高层设计	ADV_HLD
	实现表示	ADV_IMP
	TSF 内部	ADV_INT
	低层设计	ADV_LLD
	表示对应性	ADV_RCR
	安全策略模型	ADV_SPM
AGD 类：指导性文档	管理员指南	AGD_ADM
	用户指南	AGD_USR
ALC 类：生命周期支持	开发安全	ALC_DVS
	缺陷纠正	ALC_FLR
	生命周期定义	ALC_LCD
	工具和技术	ALC_TAT
ATE 类：测试	覆盖范围	ATE_COV
	深度	ATE_DPT
	功能测试	ATE_FUN
	独立性测试	ATE_IND
AVA 类：脆弱性评定	隐蔽信道分析	AVA_CCA
	误用	AVA_MSU
	TOE 安全功能强度	AVA_SOF
	脆弱性分析	AVA_VLA

（5）评估保证级

- 七个评估保证级别：
- EAL1 功能测试
- EAL2 结构测试
- EAL3 系统地测试和检查
- EAL4 系统地设计、测试和复查
- EAL5 半形式化设计和测试
- EAL6 半形式化验证的设计和测试
- EAL7 形式化验证的设计和测试

(5)评估保证级

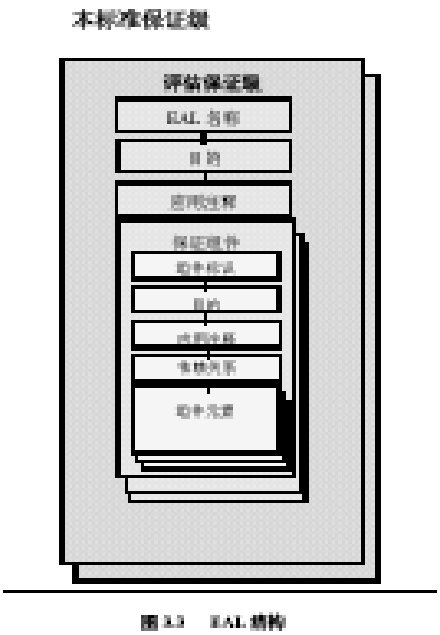


图 3.3 EAL 结构

(5)评估保证级

表 7.1 评估保证级汇总

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

3 国标GB/T 18336

- 等同采用ISO 15408三部分
- 第一部分：
- 第二部分：
- 第三部分：
- 安全技术要求：《XXX防火墙安全技术要求》
  《路由器安全技术要求》
  《网络代理服务器安全技术要求》
  《政务公开网站通用安全技术要求》

标准DB11/T 171

1 概述
2 安全定级准则
3 安全技术要求
4 安全管理要求
5 安全测评工作

1 概述

- 以往的安全测评针对产品的居多，如何对集成的信息网络系统进行安全测评，是一个备受关注、富有挑战性的课题
- DB11/T 171党政机关信息系统安全测评规范，从党政机关信息系统的信息资产价值和威胁分析出发，落实“安全等级保护”思想
- 吸纳GB/T 18336和ISO 17799的优点
- 主要分两大部分：安全技术要求、安全管理要求
- 安全技术要求分四个层次：网络系统层、操作系统层、公共应用平台层、党政应用系统层
- 安全管理要求分10个大项：共121个安全管理要素

2 安全定级准则——基线

等级	系统处理的信息价值	应对攻击/威胁描述
I	系统所处理的信息为一般信息。该单位的信息系统所管理、控制和处理的信息资产，在遭到攻击和破坏时，系统安全、人员生命财产、部门业务以及单位利益基本不会受到影响或损害极小。	系统需应对的主要是用户的误操作、非恶意行为，以及意外事件。
II	处理信息为日常政务信息。该单位的信息系统所管理、控制和处理的信息资产，在遭到攻击和破坏时，会对系统安全、人员生命财产、部门业务以及单位利益带来小的损失或破坏。	系统需应对的主要是有限资源和能力的个体恶意攻击、犯罪。
III	处理信息为日常政务信息。该单位的信息系统所管理、控制和处理的信息资产，在遭到攻击和破坏时，会对系统安全、人员生命财产、部门业务以及单位利益带来一定损失或破坏。	系统需应对的主要是国内犯罪团伙的攻击行为、跨地区犯罪、内外勾结犯罪。这些攻击或犯罪行为可以进行长期的策划，并有一定的资金、人力和技术资源可以利用。
IV	处理信息包含有重要的政务信息。该单位的信息系统所管理、控制和处理的信息资产，在遭到攻击和破坏时，会对系统安全、人员生命财产、部门业务以及单位利益带来严重的影响或损失。	系统需应对的主要是大型国际商业机构的商业间谍、国际恐怖团体、国际犯罪团伙的攻击行为。这些集团能够实施跨国界的集团犯罪，所能利用的资源丰富。一些大型的国际性信息技术商业机构，不仅拥有强大的计算能力，而且可能是党政机关信息系统硬件、软件和系统的提供商。
V	处理信息包含有关键政务信息。该单位的信息系统及其所管理、控制和处理的信息资产，在遭到攻击和破坏时，会对系统安全、人员生命财产、部门业务以及单位利益带来非常严重的损失或破坏。	系统需应对的是国家级的攻击行为、可调动国家资源实施的信息系统攻击。攻击者组织精良、资源充足，甚至可以不计经济代价。

3 安全技术要求——进阶表

安全技术要求组件		I	II	III	IV	V
安全审计自动响应	FAU_ARP.1		√	√	√	√
安全审计数据产生	FAU_GEN.1	√	√	√	√	√
	FAU_GEN.2	√	√	√	√	√
安全审计分析	FAU_SAA.3		△	△		
	FAU_SAA.4		△	△	√	√
安全审计查阅	FAU_SAR.1	√	√	√	√	√
	FAU_SAR.2	√	√	√	√	√
	FAU_SAR.3			√	√	√
安全审计事件选择	FAU_SEL.1	√	√	√	√	√
安全审计事件存储	FAU_STG.1	√	√			
	FAU_STG.2			√	√	√
	FAU_STG.3	√	√			
	FAU_STG.4			√	√	√

3 安全技术要求－－进阶表

安全技术要求组件		I	II	III	IV	V
原发抗抵赖	FCO_NRO.1			○	√	√
接收抗抵赖	FCO_NRR.1			○	√	√

3 安全技术要求－－进阶表

安全技术要求组件		I	II	III	IV	V
访问控制策略	FDP_ACC.1		√	△	△	
	FDP_ACC.2			△	△	√
访问控制功能	FDP_ACF.1		√	√	√	√
数据鉴别	FDP_DAU.1		√	√	√	√
	FDP_DAU.2			√	√	√
向 TSF 控制范围之外输出	FDP_ETC.1			√	√	√
	FDP_ETC.2		√	√	√	√
从 TSF 控制范围之外输入	FDP_ITC.1		√	√	√	√
	FDP_ITC.2		√	√	√	√
TOE 内部传输	FDP_ITT.1	√				
	FDP_ITT.2		√	√	√	√
	FDP_ITT.3	√				
	FDP_ITT.4				√	√
残余信息保护	FDP_RIP.1			√	√	√
存储数据的完整性	FDP_SDI.1			√	√	√
	FDP_SDI.2		√	√	√	√

3 安全技术要求－－进阶表

安全技术要求组件		I	II	III	IV	V
鉴别失败	FIA_AFL.1	√	√	√	√	√
用户属性定义	FIA_ATD.1	√	√	√	√	√
秘密的规范	FIA_SOS.1	√	√	√		
	FIA_SOS.2				√	√
用户鉴别	FIA_UAU.1	△	△	√	√	√
	FIA_UAU.3			△	△	△
	FIA_UAU.4			△	△	△
	FIA_UAU.5	△	△	√	√	√
	FIA_UAU.6	△	△	√	√	√
	FIA_UAU.7	△	△	√	√	√
用户标识	FIA_UID.1	√	√	√	√	√
	FIA_UID.2			√	√	√
用户_主体绑定	FIA_USB.1	√	√	√	√	√

3 安全技术要求－－进阶表

安全技术要求组件		I	II	III	IV	V
失败保护	FPT_FLS.1		√	√	√	√
输出 TSF 数据的可用性	FPT_ITA.1	√	√	√	√	√
输出 TSF 数据的保密性	FPT_ITC.1	√	√	√	√	√
输出 TSF 数据的完整性	FPT_ITI.1	√	√	√	√	√
TOE 内 TSF 数据传输	FPT_ITT.1	√				
	FPT_ITT.2		√	√	√	√
可信恢复	FPT_RCV.1	√	√	√		
	FPT_RCV.2				√	√
状态同步协议	FPT_SSP.1			√		
	FPT_SSP.2				√	√
时间戳	FPT_STM.1		√	√	√	√

3 安全技术要求－－进阶表

安全技术要求组件		I	II	III	IV	V
容错	FRU_FLT.1	√	√	√	√	√
	FRU_FLT.2			√	√	√
服务优先级	FRU_PRS.1		√	√	√	√
资源分配	FRU_RSA.1		√		√	√
	FRU_RSA.2			√	√	√
可选属性范围限定	FTA_LSA.1		√	√	√	√
多重并发会话限定	FTA_MCS.1	√	√	√	√	√
会话锁定	FTA_SSL.1	√	√	√	√	√
	FTA_SSL.2		√	√	√	√
	FTA_SSL.3				√	√
TOE 访问旗标	FTA_TAB.1	√	√	√	√	√
TOE 访问历史	FTA_TAH.1	√	√	√	√	√
TOE 会话建立	FTA_TSE.1	√	√	√	√	√
TSF 间可信信道	FTP_ITC.1		√	√	√	√

3 安全技术要求－－II细表

安全技术要求组件		网络系统层	操作系统层	公共平台层	应用系统层
安全审计自动响应	FAU_ARP.1	√	√		
安全审计数据产生	FAU_GEN.1	√	√	√	
	FAU_GEN.2	√	√	√	
安全审计分析	FAU_SAA.3	△			
	FAU_SAA.4	△			
安全审计查阅	FAU_SAR.1	√	√	√	
	FAU_SAR.2	√	√	√	
安全审计事件选择	FAU_SEL.1	√	√	√	
安全审计事件存储	FAU_STG.1	√	√	√	
	FAU_STG.3	√	√	√	
访问控制策略	FDP_ACC.1		√		√
访问控制功能	FDP_ACF.1		√		√
数据鉴别	FDP_DAU.1				√
向 TSF 控制范围之外输出	FDP_ETC.2				√
从 TSF 控制范围之外输入	FDP_ITC.1				√
	FDP_ITC.2				√
TOE 内部传输	FDP_ITT.2				√
存储数据的完整性	FDP_SDI.2				√

3 安全技术要求—II细表

安全技术要求组件		网络系统层	操作系统层	公共平台层	应用系统层
鉴别失败	FIA_AFL.1	√	√	√	√
用户属性定义	FIA_ATD.1	√	√	√	√
秘密的规范	FIA_SOS.1		√	√	√
用户鉴别	FIA_UAU.1	△	△	△	△
	FIA_UAU.5	△	△	△	△
	FIA_UAU.6	△	△	△	△
	FIA_UAU.7	△	△	△	△
用户标识	FIA_UID.1		√		
用户_主体绑定	FIA_USB.1	√	√	√	√
失败保护	FPT_FLS.1	√	√	√	√
输出 TSF 数据的可用性	FPT_ITA.1	√	√	√	√
输出 TSF 数据的保密性	FPT_ITC.1	√	√	√	√
输出 TSF 数据的完整性	FPT_ITI.1	√	√	√	√
TOE 内 TSF 数据传输	FPT_ITT.2	√	√	√	√
可信恢复	FPT_RCV.1	√	√	√	√
时间戳	FPT_STM.1			√	
容错	FRU_FLT.1	√	√		
服务优先级	FRU_PRS.1	√	√	√	√
资源分配	FRU_RSA.1	√	√	√	√
可选属性范围限定	FTA_LSA.1				√
多重并发会话限定	FTA_MCS.1		√	√	√
会话锁定	FTA_SSL.1		√		√
	FTA_SSL.2		√		√
TOE 访问旗标	FTA_TAB.1		√		√
TOE 访问历史	FTA_TAH.1		√		√
TOE 会话建立	FTA_TSE.1	√	√	√	√
TSF 间可信信道	FTP_ITC.1	√	√	√	√

3 安全技术要求－－III细表

安全技术要求组件		网络系统层	操作系统层	公共平台层	应用系统层
安全审计自动响应	FAU_ARP.1	√	√		
安全审计数据产生	FAU_GEN.1	√	√	√	
	FAU_GEN.2	√	√	√	
安全审计分析	FAU_SAA.3	△			
	FAU_SAA.4	△			
安全审计查阅	FAU_SAR.1	√	√	√	
	FAU_SAR.2	√	√	√	
	FAU_SAR.3	√	√	√	
安全审计事件选择	FAU_SEL.1	√	√	√	
安全审计事件存储	FAU_STG.2	√	√	√	
	FAU_STG.4	√	√	√	
原发抗抵赖	FCO_NRO.1				○
接收抗抵赖	FCO_NRR.1				○

3 安全技术要求——细表

安全技术要求组件		网络系统层	操作系统层	公共平台层	应用系统层
访问控制策略	FDP_ACC.1	△	△	△	
	FDP_ACC.2	△	△	△	√
访问控制功能	FDP_ACF.1	√	√	√	√
数据鉴别	FDP_DAU.1			√	√
	FDP_DAU.2		√		
向 TSF 控制范围之外输出	FDP_ETC.1	√	√	√	
	FDP_ETC.2				√
从 TSF 控制范围之外输入	FDP_ITC.1	√	√	√	√
	FDP_ITC.2			√	√
TOE 内部传输	FDP_ITT.2				√
残余信息保护	FDP_RIP.1		√	√	√
存储数据的完整性	FDP_SDI.1			√	
	FDP_SDI.2				√
鉴别失败	FIA_AFL.1	√	√	√	√
用户属性定义	FIA_ATD.1	√	√	√	√
秘密的规范	FIA_SOS.1		√	√	√
用户鉴别	FIA_UAU.1	√	√	√	√
	FIA_UAU.3	△	△	△	△
	FIA_UAU.4	△	△	△	△
	FIA_UAU.5	√	√	√	√
	FIA_UAU.6	√	√	√	√
	FIA_UAU.7	√	√	√	√
用户标识	FIA_UID.1		√		
	FIA_UID.2			√	√
用户_主体绑定	FIA_USB.1	√	√	√	√

3 安全技术要求——细表

安全技术要求组件		网络系统层	操作系统层	公共平台层	应用系统层
失败保护	FPT_FLS.1	√	√	√	√
输出 TSF 数据的可用性	FPT_ITA.1	√	√	√	√
输出 TSF 数据的保密性	FPT_ITC.1	√	√	√	√
输出 TSF 数据的完整性	FPT_ITI.1	√	√	√	√
TOE 内 TSF 数据传输	FPT_ITT.2	√	√	√	√
可信恢复	FPT_RCV.1	√	√	√	√
状态同步协议	FPT_SSP.1			√	√
时间戳	FPT_STM.1			√	
容错	FRU_FLT.1			√	
	FRU_FLT.2	√	√		
服务优先级	FRU_PRS.1	√	√	√	√
资源分配	FRU_RSA.2	√	√	√	√
可选属性范围限定	FTA_LSA.1				√
多重并发会话限定	FTA_MCS.1		√	√	√
会话锁定	FTA_SSL.1		√		√
	FTA_SSL.2		√		√
TOE 访问旗标	FTA_TAB.1		√		√
TOE 访问历史	FTA_TAH.1		√		√
TOE 会话建立	FTA_TSE.1	√	√	√	√
TSF 间可信信道	FTP_ITC.1	√	√	√	√

4 安全管理要求——进阶表

共121个要素

安全管理要求项目		安全管理要素	系统安全类别				
			I	II	III	IV	V
安全策略	信息安全策略	信息安全策略文件	基本	√	√	√	√
		评审和评价			√	√	√
组织的安全	信息安全管理基础	信息安全管理专题会议	基本	√	√	√	√
		信息安全协调		√	√	√	√
		信息安全职责的分配		√	√	√	√
		信息处理设施的授权过程			√	√	√
		专家信息安全建议		√	√	√	√
		组织之间的合作		√	√	√	√
		信息安全的独立评审			√	√	√
	第三方访问的安全	标识第三方访问的风险		√	√	√	√
		第三方合同中的安全要求		√	√	√	√
	外包	外包合同中的安全要求	基本	√	√	√	√

4 安全管理要求—进阶表

安全管理要求项目		安全管理要素	系统安全类别				
			I	II	III	IV	V
资产分类控制	资产的可核查性	资产清单	基本	√	√	√	√
	信息分类	分类指南	基本	√	√	√	√
		信息标记和处理		√	√	√	√
人员安全	工作设定和人力资源的安全	工作职责中的安全	基本	√	√	√	√
		人员筛选和策略		√	√	√	√
		保密协议		√	√	√	√
		聘用期限和条件		√	√	√	√
	用户培训	信息安全教育和培训	基本	√	√	√	√
	对安全事故和故障的响应	报告安全事故	√	√	√	√	√
		报告安全弱点	√	√	√	√	√
		报告软件故障	√	√	√	√	√
		从事故中学习	√	√	√	√	√
		纪律处理	√	√	√	√	√
物理和环境的安全	安全区域	物理安全周边	基本	√	√	√	√
		物理入口控制		√	√	√	√
		区域的安全保护		√	√	√	√
		在安全区域工作		√	√	√	√
		隔离的交接区域			√	√	√
	设备安全	设备安置和保护	基本	√	√	√	√
		电源		√	√	√	√
		布线安全		√	√	√	√
		设备维护		√	√	√	√
		离开建筑物的设备的安全		√	√	√	√
		设备安全处置和重用			√	√	√
	一般控制	清理桌面和清空屏幕策略			√	√	√
		财产的移动		√	√	√	√

4 安全管理要求—进阶表

安全管理要求项目		安全管理要素	系统安全类别				
			I	II	III	IV	V
通信和操作管理	操作规程和职责	文件化的操作规程	基本		√	√	√
		操作变更控制			√	√	√
		事故管理规程			√	√	√
		责任分离		√	√	√	√
		开发和运行设施分离		√	√	√	√
		外部设施管理		√	√	√	√
	系统规划和验收	能力规划		√	√	√	√
		系统验收			√	√	√
	防止恶意软件	控制恶意软件	基本	√	√	√	√
	内务处理	信息备份		√	√	√	√
		操作员日志			√	√	√
		故障记录		√	√	√	√
	网络管理	网络控制		√	√	√	√
	媒体处置和安全	可移动媒体的管理		√	√	√	√
		媒体的处置		√	√	√	√
		信息处置规程			√	√	√
		系统文件的安全		√	√	√	√
	信息和软件的交换	信息和软件交换协定		√	√	√	√
		运输中的媒体安全		√	√	√	√
		电子邮件的安全		√	√	√	√
		电子办公系统的安全		√	√	√	√
		公开可用系统		√	√	√	√
		信息交换的其他形式			√	√	√

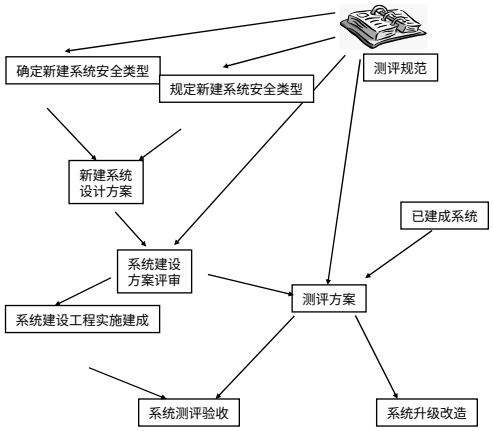
4 安全管理要求—进阶表

安全管理要求项目		安全管理要素	系统安全类别				
			I	II	III	IV	V
访问控制	访问控制的业务要求	策略和业务要求		√	√	√	√
		访问控制规则		√	√	√	√
	用户访问管理	用户注册		√	√	√	√
		特权管理			√	√	√
		用户口令管理		√	√	√	√
		用户访问权利的评审		√	√	√	√
	用户职责	口令使用		√	√	√	√
		无人值守的用户设备		√	√	√	√
	网络访问控制	使用网络服务的政策		√	√	√	√
		强制路径		√	√	√	√
		外部连接的用户鉴别		√	√	√	√
		节点鉴别		√	√	√	√
		远程诊断端口保护	基本	√	√	√	√
		网络分离			√	√	√
		网络连接控制		√	√	√	√
		网络路由选择控制		√	√	√	√
		网络服务的安全		√	√	√	√
	操作系统访问控制	自动化终端标识		√	√	√	√
		终端登录规程		√	√	√	√
		用户标识和鉴别		√	√	√	√
		口令管理系统		√	√	√	√
		系统实用程序的使用	基本		√	√	√
		保护用户的强制报警		√	√	√	√
		终端超时		√	√	√	√
		连接时间的限定			√	√	√
	应用访问控制	信息访问限制	基本	√	√	√	√
		敏感系统隔离		√	√	√	√
	对系统访问和使用的监视	事件记录			√	√	√
		对系统使用的监视		√	√	√	√
		时钟同步			√	√	√
	移动计算和远程工作要求	移动计算		√	√	√	√

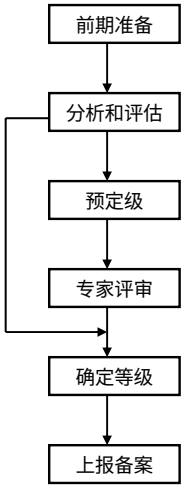
4 安全管理要求—进阶表

安全管理要求项目		安全管理要素	系统安全类别				
			I	II	III	IV	V
系统开发和维护	系统的安全	安全要求分析和规范			√	√	√
	应用系统的安全	输入数据确认	基本	√	√	√	√
		内部处理的控制		√	√	√	√
		报文鉴别		√	√	√	√
		输出数据确认			√	√	√
	系统文件的安全	运行软件的控制	基本	√	√	√	√
		系统测试数据的保护		√	√	√	√
		源程序库的访问控制		√	√	√	√
	开发和支持过程的安全	变更控制规程		√	√	√	√
		运行系统变更的技术评审		√	√	√	√
		软件包变更的限制			√	√	√
		隐蔽信道和特洛伊代码		√	√	√	√
		外包的软件开发		√	√	√	√
业务连续性管理	业务连续性管理的各方面	业务连续性管理过程	基本	√	√	√	√
		业务连续性和影响分析			√	√	√
		制定和实施连续性计划			√	√	√
		业务连续性计划框架			√	√	√
		全周期业务连续性计划			√	√	√
符合性	符合法律要求	可用法律的标识	基本	√	√	√	√
		知识产权（IPR）		√	√	√	√
		保护组织的记录			√	√	√
		防止滥用信息处理设备		√	√	√	√
		密码控制的规章			√	√	√
		证据的收集			√	√	√
	安全策略和技术符合性的评审	符合安全策略	基本	√	√	√	√
		技术符合性检验			√	√	√
	系统审核考虑	系统审核控制	基本	√	√	√	√
		系统审核工具的保护			√	√	√

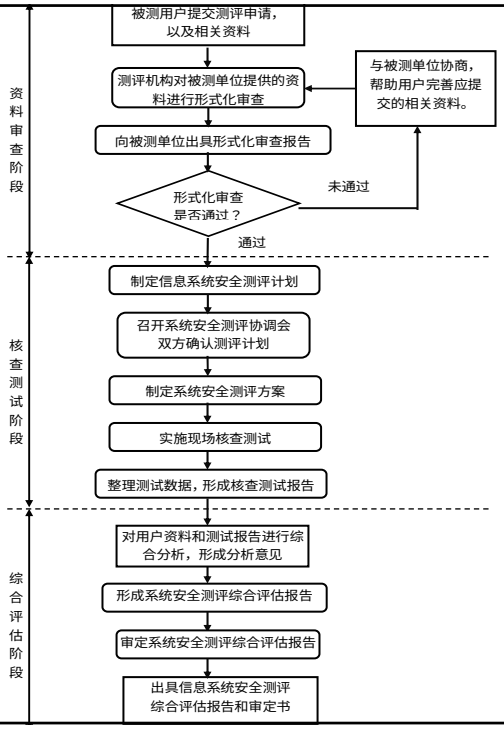
5 安全测评工作——规范使用



5 安全测评工作——定级方法



5 安全测评工作—流程



FAQ

谢 谢 ！

wanghong@bjtec.org.cn