ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 29830.2—2013/ISO/IEC TR 15443-2:2005

信息技术　安全技术
信息技术安全保障框架
第2部分:保障方法

Information technology—Security technology—A framework for IT security assurance—Part 2:Assurance methods

[ISO/IEC TR 15443-2:2005,IDT]

2013-11-12 发布　　2014-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/Z 29830《信息技术　安全技术　信息技术安全保障框架》分为以下3个部分：

——第1部分：综述和框架；

——第2部分：保障方法；

——第3部分：保障方法分析。

本部分为GB/Z 29830的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分采用翻译法等同采用ISO/IEC TR 15443-2:2005《信息技术　安全技术　信息技术安全保障框架　第2部分：保障方法》。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分主要起草单位：中国电子技术标准化研究院。

本部分的主要起草人：张明天、罗锋盈、王延鸣、陈星、杨建军。

引　言

本指导性技术文件的目的是，为了获得一个给定交付件满足其所指出的信息安全保障需求的信心，给出各种保障方法，并指导信息安全专业人员如何选择一个合适的保障方法（或组合一些方法）。本指导性技术文件审视了不同类型组织所提出的保障方法和途径，包括已批准的标准和事实标准。

为了达到这一目的，本指导性技术文件由以下7个方面内容组成：

a) 一个框架模型，用于定位现有的保障方法并给出它们之间的关系；

b) 一组保障方法以及对它们的描述和引用；

c) 特定保障方法的共性和个性的表达；

d) 现有保障方法的定性比较，其中尽可能进行定量比较；

e) 与当前保障方法关联的保障模式的标识；

f) 不同保障方法之间关系的描述；以及

g) 有关保障方法的应用、组合和认知的指导。

本指导性技术文件由3部分组成，对保障途径、分析和相互间的关系处理如下：

第1部分：综述和框架。概述了一些基础性概念，例如保障、保障框架等，并给出了安全保障方法的一般性描述。其目的是帮助理解本标准的第2部分和第3部分内容。第1部分针对信息安全管理人员和其他人员，其中包括负责开发安全保障程序、确定他们的交付件的安全保障、参加安全评估审计或参加其他保障活动的人员。

第2部分：保障方法。描述由不同类型的组织提出和使用的各种IT安全保障方法和途径，不论它们是被一般公认的、事实上被认可的或标准的；并把这些保障方法与第1部分的保障模型关联起来。重点是识别对保障有影响的保障方法的定性特征，在可能的地方，还将定义保障级别。该材料面向IT安全专业人员，帮助理解如何在产品或服务的特定的生存周期阶段中获得保障。

GB/Z 29830.2—2013使用定义在GB/Z 29830.1—2013中的术语和定义。

该部分应与GB/Z 29830.1—2013一并使用。

第3部分：保障方法分析。分析了各种保障方法的保障特征。这个分析有助于保障机构在确定每一种保障途径的相对值并确定保障途径，使这些途径提供最适合于运行环境的具体上下文的需求的保障结果。而且，这个分析还有助于保障机构运用保障方法的结果，实现交付件所预想的确信度。这部分材料面向的对象是那些必须选择保障方法和保障途径的IT安全专业人员。

GB/Z 29830.3—2013使用定义在GB/Z 29830.1—2013中的术语和定义。

该部分应与GB/Z 29830.1—2013一并使用。

本指导性技术文件分析了一些可能不为IT安全所专有的保障方法；然而，在指导性技术文件中所给出的指导将限于IT安全需求。只对IT安全领域提供相应的指导，并不期望这一指导对一般的质量管理、评估或IT符合性具有指导意义。

信息技术　安全技术
信息技术安全保障框架
第2部分:保障方法

1　范围

1.1　意图

GB/Z 29830的本部分收集了一些保障方法,其中还包括一些对整体ICT安全具有作用但不是专对ICT安全的保障方法。本部分概括了这些方法的目标,描述了它们的特征以及引用文件和标准等。

原则上,ICT安全保障的最终结果是对运行中的产品、系统或服务的保障。因此,最终的保障是应用于产品、系统或服务的生存阶段中每一种保障方法所得到的保障增量之和。大量可用的保障方法均提供了应用于一个给定领域的必要指导,以便获得公认的保障。

本部分使用GB/Z 29830.1—2013中的基本保障概念和术语,以一种概览的方式,对本部分中所收集的每一项保障方法进行分类。

通过使用这一分类,本部分指导ICT专业人员选择保障方法以及保障方法的可能组合,以适合于给定的ICT安全产品、系统或服务及其特定的环境。

1.2　适用领域

本部分以一种概括和概览的方式给出有关保障方法的指导。为了从本部分所收集的方法中获得一个量少的可用方法集合,应采用排除其中不适宜的方法这一方式从中选择之。

这一概括是描述性的,为支持分析理解原标准提供了基础。

本指导性技术文件预期读者包括:

a) 获取方(从供应方获取或取得系统、软件产品或服务的个人或组织);
b) 评价方(执行评价的个人或组织;例如,评价方可以是测试实验室、软件开发组织的一个品质部门、政府组织或用户);
c) 开发方(执行开发活动的组织或个人,包括需求分析、设计、以及软件生存周期过程期间的验收测试);
d) 维护方(执行维护活动的组织或个人);
e) 确认软件质量(授权测试)时的供应方(在获取方的合同中提供合同条款规定的系统、软件产品或软件服务的个人或组织);
f) 评估软件质量(验收测试)时的用户(使用软件产品来执行特定功能个人或组织);
g) 评估软件质量(授权测试)的安全官员或部门(对软件产品或软件服务执行系统检查的个人或部门)。

1.3　限制

本部分仅以一种综述的方式给出指导。为了更好地形成保障需求,GB/Z 29830.3提供了精化这一选择的指导,以便能够评审它们的可比较性和协作性。

支持保障途径验证并支持执行验证人员的规章制度,没有包含在本部分的范围中。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO 9000 质量管理体系 基础和术语(Quality management systems—Fundamentals and vocabulary)

ISO 9001 质量管理体系 需求(Quality management systems—Requirements)

ISO/IEC 9126-1 软件工程 产品质量 第一部分：质量模型(Software engineering—Product quality—Part 1:Quality model)

ISO/IEC 12207 软件生存周期过程(Information technology—Software life cycle processes)

ISO/IEC 13335-1 信息技术 安全技术 信息和通讯技术安全管理 第1部分：信息和通讯技术安全管理概念和模型(Information technology—Security techniques—Management of information and communications technology security—Part 1:Concepts and models for information and communications technology security management)

ISO/IEC 13335-2 信息技术 信息技术安全管理指南 第2部分：信息技术安全管理和规划(Information technology—Guidelines for the management of IT Security—Part 2:Managing and planning IT Security)

ISO/IEC 13335-3 信息技术 信息技术安全管理指南 第3部分：信息技术安全管理技术(Information technology—Guidelines for the management of IT Security—Part 3:Techniques for the management of IT Security)

ISO/IEC 13335-4 信息技术 信息技术安全管理指南 第4部分：安全措施的选择(Information technology—Guidelines for the management of IT Security—Part 4:Selection of safeguards)

ISO/IEC 13335-5 信息技术 信息技术安全管理指南 第5部分：网络安全管理指南(Information technology—Guidelines for the management of IT Security—Part 5:Management guidance on network security)

ISO/IEC 14598-1 信息技术 软件产品评估 第1部分：一般性概述(Information technology—Software product evaluation—Part 1:General overview)

ISO/IEC 15939 软件工程-软件测量过程(ISO/IEC 15939, Software engineering—Software measurement process)

ISO/IEC 15288 系统工程 系统生存周期过程(Systems engineering—System life cycle processes)

ISO/IEC 15408-1 信息技术 安全技术 信息技术安全评估准则 第1部分：简介与一般模型(Information technology—Security techniques—Evaluation criteria for IT security—Part 1:Introduction and general model)

ISO/IEC 15408-2 信息技术 安全技术 信息技术安全评估准则 第2部分：安全功能要求(Information technology—Security techniques—Evaluation criteria for IT security—Part 2:Security functional requirements)

ISO/IEC 15408-3 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障要求(Information technology—Security techniques—Evaluation criteria for IT security—Part 3:Security assurance requirements)

ISO/IEC 15504-1 信息技术 过程评估 第1部分：概念与术语(Information technology—Process assessment—Part 1:Concepts and vocabulary)

ISO/IEC 15504-2 信息技术 过程评估 第2部分:执行与评估(Information technology—Process assessment—Part 2:Performing and assessment)

ISO/IEC 15504-3 信息技术 过程评估 第3部分:评估执行指南(Information technology—Process assessment—Part 3:Guidance on performing an assessment)

ISO/IEC 15504-4 信息技术 过程评估 第4部分:过程改善和过程能力确定的使用指南(Information technology—Process assessment—Part 4: Guidance on use for process improvement and process capability determination)

ISO/IEC 15504-5 信息技术 软件过程评估 第5部分:评估模型及指标指南(Information technology—Software Process Assessment—Part 5:An assessment model and indicator guidance)

ISO/IEC 17799 信息技术 安全技术 信息安全管理导则(Information technology—Security techniques—Code of practice for information security management)

ISO/IEC 21827 信息技术 系统安全工程 能力成熟度模型(SSE-CMM®)[Information technology—Systems Security Engineering—Capability Maturity Model(SSE-CMM®)]

ISO/IEC 90003 软件工程 ISO 9001:2000应用于软件的指南(ISO/IEC 90003,Software engineering—Guidelines for the application of ISO 9001:2000 to computer software)

3 术语、定义和缩略语

GB/Z 29830.1—2013界定的术语、定义和缩略语适用于本文件。

4 方法概述和表达

GB/Z 29830.1为现有保障方法的分类提供了一个框架。本章列出并表达了ICT安全领域关注的并直接有关的一些可用保障方法。本章还根据下述框架对这些方法进行了分类:

a) 根据描述生存周期各方面的不同保障阶段:设计、实施、集成、验证、部署、传输或运行;

b) 根据不同保障途径:产品、过程或环境。

正如本指导性技术文件第1部分所指出的,保障方法可能涉及了一些组合的保障途径和保障阶段.为了进一步给出用户指导,在5.4中的概览表中表达了这一分类,并对以下两方面伴有相应的记忆符:

——ICT安全相关的单个方法,以及

——单个方法的实用性。

5 保障的生存周期阶段与图示符号

5.4中的概览表列出了后面要表达的、按生存周期阶段所分类的方法。而每一子节的标题重复了这一分类。

在该表2中,通过四列来图形化地表达所关注的不同生存周期阶段。为了这一意图并为了接近ISO/IEC 15288及ISO 9000中的概念,技术方面的生存周期过程被分为4个阶段,并使用以下字符来表示每列所代表的阶段:

——D 设计,包括利益攸关方需求定义过程,需求分析过程,体系结构设计过程和实现过程;

——I 集成,包括集成和验证过程;

——T 转化,包括复制、转移、部署和确认过程;

——O 运行,包括运行、维护和处置过程。

注1:一个给定的方法可能覆盖生存周期之外的阶段。在这种情况下,这一阶段没有给出相应的图形化表达。

注 2：生存周期过程 D-I-T-O 是一些可应用于特定 ICT 系统及其部件(即硬件，软件)的过程。生存周期过程的开发和改善是另一方面的问题，这一问题也可予以图形化地表达，但在此没有给出。在 ICT 安全中，这一方面的问题对于应用于 ICT 系统运行阶段的安全管理方法而言是特别重要的，例如 ISO/IEC 17799 和 BS 7799-2。这一方面问题的基本特性包括过程评估以及过程建档、过程开发、过程测量、过程改善和认证。这一方面问题与 D-I-T-O 是正交的。

5.1 保障途径与图示符号

5.4 中的概览表列出了以后要表达的、按其保障途径分类的保障方法。单个列出的每一子节标题重复了这一分类。方法所对应的保障途径类以符号表达之(参见表 1)：

——产品保障：以箭头中的黑体字符，表示生存周期阶段：⇒D⇒；

——过程保障：以灰色背景上的白色字符，表示生存周期阶段：D；

——环境保障：以左右两黑棒之间的字符，表示生存周期阶段：■ D ■。

表 1 框架中的保障方法—图示符号

章节	保障—阶段→ —途径↓	设计/实现	集成/验证	部署/转移	运行
	产品[/系统/服务][🔒]	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
	过程[🔒]	D	I	T	O
	环境[/组织/人员][🔒]	D	I	T	O

注 1：由于方法可能体现一个组合途径的特征，因此以上这些符号可以予以堆积，例如：一个覆盖过程保障和环境保障的方法，应是黑体字段的字母加上一个黑框。

注 2：一个给定的保障方法可能覆盖一个途径并或多或少地覆盖其他途径。这一可视化的概览表达是不适于表示一个给定方法覆盖不同保障途径的程度。

注 3：一个给定的保障方法可能覆盖一个仅是“边缘”的途径。在这种情况里，这一途径就没有在该符号化表示中给出。

5.2 实用性与符号表示

由于方法是大量的，因此按其状态为本部分的用户给出一些指导。5.4 中的概览表反映了这一状态，如下：

——当前相对广泛使用并且还在不断进行维护的方法，在该概览表中以粗字符表示；

——已失时效的、已被替代的、已被合并的或失掉实用性的方法，在该概览表中均以均匀细线字符表示。

注：有关实用性的符号表示，在单个列出的子节标题中没有予以重复。

5.3 安全相关性与符号表示

由于方法是大量的，因此按其 ICT 安全相关性为本部分的用户给出一些指导。5.4 中的概览表和运用了安全相关性的其他子节标题均反映了这一状态，如下：

——和 ICT 安全相关的方法，用符号“🔒”标记。

5.4 概览表

表 2 给出了已考虑的那些保障方法，并依据上述的第 1 部分的框架给出它们的分类。

表 2　框架中保障方法-概览

章节	保障—阶段→ —途径↓	设计/实现	集成/验证	部署/转移	运行
6.1	ISO/IEC 15408　信息技术安全评估准则	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.2	TCSEC　可信计算机系统评估准则	⇒D⇒	⇒I⇒		⇒O⇒
6.3	ITSEC/ITSEM　信息技术安全评估准则和方法学	⇒D⇒	⇒I⇒		⇒O⇒
6.4	CTCPEC　加拿大可信产品评估准则	⇒D⇒	⇒I⇒		
6.5	KISEC/KISEM　韩国信息安全评估准则和方法学	⇒D⇒	⇒I⇒		⇒O⇒
6.6	RAMP-维护阶段的评定	⇒D⇒	⇒I⇒		⇒O⇒
6.7	ERM　评估评定的维护(一般性的)	⇒D⇒	⇒I⇒		⇒O⇒
6.8	TTAP　可信技术评价程序	⇒D⇒	⇒I⇒		
6.9	TPEP　可信产品评估程序	⇒D⇒	⇒I⇒		
6.10	RUP Rational 统一过程®(RuP®)	⇒D⇒	⇒I⇒	⇒T⇒	
6.11	ISO/IEC 15288　系统生存周期过程	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.12	ISO/IEC 12207　软件生存周期过程	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.13	V-模型	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.14	ISO/IEC 14598　软件产品评价	⇒D⇒			⇒O⇒
6.15	X/Open 基线安全服务	⇒D⇒			
6.16	SCT 严格符合性测试		⇒I⇒		
6.17	ISO/IEC 21827　系统安全工程　能力成熟度模型(SSE-CMM®)	D	I	T	O
6.18	TCMM　可信任能力成熟度模型	D	I		
6.19	CMMI　集成化能力成熟度模型®	D	I	T	O
6.20	ISO/IEC 15504　软件过程评估	D	I	T	O
6.21	CMM　能力成熟度模型®(针对软件)	D	I		
6.22	SE-CMM®　系统工程能力成熟度模型®	D	I		
6.23	TSDM　可信任软件开发方法	D	I		
6.24	SDoC　提供方符合性声明	D			
6.25	SA-CMM®　软件需求能力成熟度模型®			T	
6.26	ISO 9000 系列　质量管理	D	I	T	O
6.27	ISO 13407　以人为中心的设计(HCD)	D			
6.28	开发者良源(一般情况)	D			
6.29	ISO/IEC 17025　鉴定保障	D	I		
6.30	ISO/IEC 13335　信息和通信技术安全管理(MICTS)		I	T	O

表 2（续）

章节	保障—阶段→ —途径↓	设计/实现	集成/验证	部署/转移	运行
6.31	BS 7799-2　信息安全管理系统　规格说明与使用指导				O
6.32	ISO/IEC 17799　信息安全管理实践指南				O
6.33	FR　缺陷修补（一般性）				O
6.34	IT 基线保护指南				⇒O⇒
6.35	渗透测试				⇒O⇒
6.36	人员认证（与安全无关）				O
6.37	人员认证（与安全有关）	D	I	T	O

5.5　表达方法学

第 6 章的意图是，对已识别的保障方法提供一个复审。因为许多保障方法有助于不同保障途径和保障，因此在这里表达的每一种保障方法均应具有自己的描述方式和角度。在这个阶段上没有提供比较。

在第 6 章的每个子节中，将为这一技术框架所标识的每一个保障方法，给出结构化的提纲。

每一个方法的标题都是一个说明性的名字，为了正确引用，每一种保障方法的名字尽可能完整和正式，并当合适引用时其名字尽可能是容易记忆的。

每一提纲分为以下几个部分：

——目的：有关方法的简要表征性意图；

——描述：方法的简短描述；

——源描述：指出/引用所涉及的委员会和/或组织，指出/引用该方法的文档和/或标准。

6　保障方法

6.1　ISO/IEC 15408　信息技术安全评估准则

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.1.1　目标

为 ICT 安全评估，提供一个协调的评估框架和详细的评估准则，适用于政府使用和一般性使用。

6.1.2　描述

通用准则（Common Criteria）的制定，代表了许多政府信息安全机构，该准则可作为独立评估 ICT 产品和系统的安全表现特性的方式。通用准则伴随着联合技术委员会（JTC 1）的第 27 分小组委员会及安全技术一起发展而来，公开发布为国际标准 ISO/IEC 15408。

通用准则分别考虑了安全保障中的安全功能，并详细描述了有助于增强开发信心——一个产品或系统满足其安全目的技术和功能。这些基本的、非排他的、特定保障技术和功能在 ISO/IEC 15408-3 中予以定义，是针对独立评估或验证所获得的保障，其意图是支持国家认证模式验证该评估准则的一致

应用。

在 ISO/IEC 15408-3 中,保障技术被分为称为类的一些不同的应用域。在每一个类中,标识了一些称为族的不同技术。每个族又依据应用该技术的严格程度,标识了一个或多个组件。每一个组件规约了所要求的准确动作和证据元素。

在 ISO/IEC 15408-3 中,定义了多个以互补方式一起工作的保障组件包。这些包称为评估保障等级(Evaluation Assurance Levels,Eals)。

为了支持这些准则的应用,通用准则方法学工作组开发了相应的方法,称为通用评估方法学(CEM),是通用准则项目的一部分。

6.1.3 源

参考第 2 章:ISO/IEC 15408-1;ISO/IEC 15408-2;ISO/IEC 15408-3。

注:ISO/IEC 15408 是该委员会的产品:

ISO/IEC JTC 1/SC 27/WG3 信息技术　安全技术　安全评估准则。

6.2 TCSEC　可信计算机系统评估准则

⇒D⇒	⇒I⇒		⇒O⇒

6.2.1 目的

对计算机系统产品所提供的安全进行评分或划分等级。

6.2.2 描述

可信计算机系统评估准则(Trusted Computer System Evaluation Criteria,TCSEC)是以前用于对计算机系统产品所提供的安全进行评分和划分等级的一组准则。现在,尽管有些评估仍继续使用,但新的评估不再使用 TCSEC。由于它的封面是橙色,因此 TCSEC 有时被称作“桔皮书”。

如果一个产品通过由可信产品评估程序(TPEP)或可信技术评价程序(TTAP)所进行的评估,且一个独立评估显示该产品具有某一等级的特征和保障,那么该产品就符合 TCSEC。

一个等级是一个评估系统要符合的可信任计算机系统评估准则(TCSEC)中一组特定需求。在 TCSEC 中存在 7 个等级,分别为 A1、B3、B2、B1、C2、C1 和 D,这 7 个等级的特征和保障是逐渐增强的。因此,评估为 B3 等级的系统与 B1 等级相比,具有更多的安全特征,并且就有关安全特征是否按预期的那样工作而言,具有更大的信心。一个高等级的需求总是一个低等级需求的超集,因此 B2 等级的系统满足 C2 等级的每一个功能要求,并且具有更高程度的保障。

依据可信计算机系统评估准则(TCSEC)(参见 TCSEC 准则 概念 FAQ,问题 11),以递减的特征和保障方式,对等级给出一个划分(见问题 1),即把 7 个等级划分为 4 个级类,即 A、B、C、D。这样,在 B 中一个等级上已评估的系统与 C 中一个等级上已评估的系统相比,就具有更多的安全特征,和/或有关安全特征是否按预期的那样工作具有更大的信心。尽管 TCSEC 的计算机安全子系统解释(Computer Security Subsystem Interpretation,CSSI)为不同 D 的评定规约了准则,但这些准则并没有反映在 TCSEC 本身中,它们对 D 级系统没有什么需求。一个未经评定的系统默认为是 D 级系统。

不同级类的需求是:

D 级类:最小保护——该级类留给那些经过评估但不满足更高级类需求的系统。

C1 级:自主安全保护——C1 级系统的可信计算基(Trusted Computing Base,TCB)通过提供用户和数据的分离,像名字那样满足自主安全要求。它加入了一些形式的可靠控制能力,在一个单个的基础上实施访问控制,即外表上允许用户保护项目信息或私有信息,并且防止其他用户意外地读取或销毁他

们的数据。期望 C1 级的环境是一种用户处理具有相同敏感程度数据的协同环境。

C2 级:受控的访问保护——与 C1 系统相比,该级类中的系统执行更细粒度的自主访问控制,通过登入规程、审计与安全相关的事件以及资源隔离,可单独核查用户的动作。

B1:打标记的安全保护(Labeled Security Protection)——B1 类系统要求类 C2 的所有特征。另外,还必须表达一个非正式陈述的安全策略模型、数据标记(例如,秘密或私密)以及命名主体和客体上的强制访问控制。还必须具有准确标记对外输出信息的能力。

B2 级:结构化保护——在 B2 级系统中,TCB 基于一个清晰定义并建档的正式安全策略模型,该模型要求将 B1 级系统中的自主访问控制和强制访问控制扩展到自动数据处理系统中的所有主体和客体。另外,还要强调隐蔽通道。该 TCB 必须细致地被结构化为关键保护元素和非关键保护元素。该 TCB 接口还应良好予以定义,并且其设计和实现可更容易进行全面的测试和更容易进行完整的评审。B2 级系统的身份鉴别机制被增强,以一种支持系统管理员和操作者功能的形式,提供了可信设施管理,并强加了更严格的配置管理控制。该系统是相对抗渗透的。

B3 级:安全域——B3 级的 TCB 必须满足参照监视器需求,它仲裁所有主体对客体的访问,可证明是否予以篡改的,且是足够小的以便进行分析和测试。其结果,TCB 被结构化,剔除对执行安全策略非基本的代码,并在 TCB 的设计和实现的期间,为了最小化它的复杂度,实施了充分的系统工程。B3 级的 TCB 支持安全管理员,为了指示安全相关事件,扩充了审核机制,并要求系统恢复规程。系统具有高度的抵渗透能力。

A1 级:已验证的设计——在 A 级中的系统,其功能等同于没有增加额外的体系结构特征或策略需求的 B3 级中的系统。在这一级中,系统特征的主要区别来自于正式的设计规格说明和验证技术所引发的分析,以及由于该 TCB 的正确实现所产生高等级的保障。这一保障是自然形成的,开始于一个正式的安全策略模型和一个正式的顶层设计规格说明(FTLS)。FTLS 是一种以形式化数学语言编写的系统顶层规格说明,允许(表明系统规格说明与其正式需求之对应的)定理予以假定和形式化证明。记住,对于 A1 级中系统所要求的 TCB 的扩展设计和开发分析,需要更严格的配置管理,并为安全地把系统分布在不同地点,需要建立相应的规程。该类系统支持系统安全管理员。

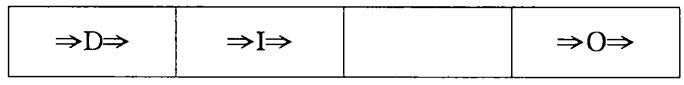
6.2.3 源

参考文献目录:

[45] 可信计算机系统评估准则(TCSEC),1985。

注:TESEC 及其解释和指南都有不同颜色的封面,有时被称为“彩虹系列”。TESEC 是美国国防部内部标准和产品。

6.3 ITSEC/ITSEM 信息技术安全评估准则和方法学



6.3.1 目的

为欧洲市场的 IT 安全评估提供一个评估准则框架和一种评估方法学。

6.3.2 描述

评估准则“信息技术安全评估标准(Information Technology Security Evaluation Criteria,ITSEC)”和评价手册“信息技术安全评价手册(Information Technology Security Evaluation Manual,ITSEM)”是通用准则(Common Criteria)和通用评估方法学(Common Evaluation Methodology)的先期文档。ITSEC 和 ITSEM 是在 20 世纪 90 年代早期,由 4 个欧洲国家(法国、德国、荷兰和英国)开发的。

ITSEC 的保障基于 TCSEC 中所引入的途径。但把 ITSEC 中的功能需求和保障需求予以分离，允许更大的灵活性。保障需求本身又分为有效性和正确性两个方面。有效性评价涉及了评价对象(Target of Evaluation，TOE)如下一些方面的考虑：

——TOE 执行的安全功能应对其安全威胁的适宜性；

——TOE 执行的安全功能和机制以相互支持的方式绑定在一起的能力，以及提供一种集成和有效整体的能力；

——TOE 执行的安全机制承受直接攻击的能力；

——TOE 构造中的已知安全脆弱性实际上是否能够危及 TOE 的安全；

——TOE 不可能以不安全的方式予以配置和使用，但 TOE 的管理员或终端用户应有理由地相信该 TOE 是安全的；

——TOE 运行中已知的安全脆弱性实际上是否能够危及 TOE 的安全。

保障有效性需求更多地关注那些方面，即评估人员必须使用所拥有的知识和经验来评价受评 IT 产品或系统中的安全途径是否合理。

ITSEC 的保障正确性要求更多地关注于一些方面，即确认与被评估产品或系统的 IT 安全相关的开发者的信息是正确的。

ITSEC 针对 TOE 构造和 TOE 运行，区分了它们之间的正确性需求。构建方面的准则覆盖了开发过程以及不同规格说明层，以高层的需求描述开始，这些需求可予实例化为体系结构设计，进一步，体系结构设计又可予实例化为详细设计和实现表示。由 ITSEC 所覆盖的开发环境，其构建方面是配置控制、编程语言和编译器，以及开发者安全(Developers Security)。

运行需求进一步划分为 4 个方面，即运行文档以及用户文档，管理文档，运行环境以及交付和配置，以及启动和操作。

ITSEC 的正确性需求以 6 个层次化的保障等级(E1～E6)予以表达。通过从一个等级到另一个等级增加需求，确保对 IT 产品和系统更为严格的评价。保障的有效性需求没有包括在这些保障等级中，但定义了由正确性评估所获得的、用于执行脆弱性分析的信息。

另外，ITSEC 还概括了评估等级与 TCSEC 类的关系。

ITSEM 基于 ITSEC，描述了根据这些准则如何来评估一个 TOE。ITSEM 的特定目的是，确保存在一个与 ITSEC 互补的、协调一致的评价方法集。

ITSEM 没有基于以前什么文档，是首次为应用 ITSEC 中的保障方法表达了如此多的基本信息，并且还间接地为用于 TCSEC 和 CTCPEC 中的保障方法表达了基本信息。

6.3.3 源

参考文献目录：

[40] 信息技术安全评估准则(ITSEC)，版本 1.2；

[41] 信息技术安全评估准则(ITSEM)，版本 1.0。

注：ITSEC/ITSEM 是欧盟委员会，通用信息协会理事会(Directorate General Information Society)的产品。该理事会可通过下面的网址访问：http://europa.eu.int/pol/infso/index_en.htm。

6.4 CTCPEC 加拿大可信产品评估准则

⇒D⇒	⇒I⇒		

6.4.1 目的

为评估软件、硬件产品或系统所提供的安全服务功能和保障，提供一种度量。

6.4.2 描述

加拿大可信产品评估准则(Canadian Trusted Product Evaluation Criteria,CTCPEC)的制定具有3个目的:

1) 为商用产品的评估提供一个可比的尺度;
2) 为可信计算机产品规格说明的开发提供基础;以及
3) 为可信产品采购的规约提供方法。

CTCPEC为可信处理,描述了以下两种类型的需求:

1) 特定的安全服务要求,以及
2) 保障要求。

考虑到产品之间一些特有的安全服务,CTCPEC规约了两组不同的需求:功能需求和保障需求。功能需求由机密性、完整性、可用性以及可核查性准则组成,而保障需求组由一些保障准则组成。

一些保障需求能使一个评估来确定所要求的特征是否给出,功能是否像预期的那样。这些准则应用于组成可信产品的一组部件,而单独应用于每一产品部件并不是必要的。因此,一个产品的一些部件可能是完全不可信的,而其他的一些部件可能单独地予以评估,其评估等级可能比该可信任产品的整体更高或更低。在高端的可信产品中,隔离的强度和仲裁机制致使该产品的许多部件可能是完全不可信的。

如果没有特别解释的话,这些保障需求可适用于整个谱系的电子数据处理产品,或适用于整个谱系的应用处理环境。

6.4.3 源

参考文献目录:

[31] 加拿大可信计算机产品评估准则(CTCPEC),版本3.0。

注:CTCPEC是一个国际标准,是通信安全组织(Communications Security Establishment,CSE)的产品。该组织可以通过下面的网址访问:http://www.cse-cst.gc.ca。

6.5 KISEC/KISEM 韩国信息安全评估准则和方法学

⇒D⇒	⇒I⇒		⇒O⇒

6.5.1 目的

为韩国的防火墙和入侵检测系统,提供了一个安全评估准则框架和安全评估方法学。

6.5.2 描述

评估准则"韩国信息安全评估准则(KISEC)"和评估方法学"韩国信息安全评估方法(KISEM)"开发于1998年,其3个目的是:

——为防火墙和入侵检测系统的安全功能评估,提供一个层次化的评定尺度;
——为规约采购中的可信防火墙和入侵检测系统提供一种方法;
——通过执行其自己的评估准则和方法学,积累有关IT安全评估的知识。

KISEC为7个评估等级(K1~K7)分别定义了相应的功能需求和保障需求。KISEC的每一个等级都有一组功能需求和保障需求,受评的防火墙或入侵检测系统都应符合这些需求。依赖产品类型,例如防火墙和入侵检测系统,KISEC有一些不同的功能需求。而保障需求公用于防火墙和入侵检测系统。

功能需求由识别和认证、完整性、安全审计、安全管理等组成。保障需求由开发、配置管理、测试、运行环境、指导文档和弱点分析等组成。

依据防火墙或入侵检测系统所实现了的安全功能以及保障需求的信心，可确定其特定的等级。以其安全功能性需求和保障需求，评估等级分为 7 个等级，K1 代表最低的等级，而 K7 代表最高的等级。

下面是每一评估等级的特征：

——等级 K1 必须满足最低水平的安全功能，例如系统管理员和安全管理的身份标识与鉴别等。而且，必须存在安全目标和功能规格说明。

——等级 K2 必须满足等级 K1 的需求，并且还能够创建和维护与安全相关活动的审计记录。另外，还必须给出体系结构设计文档；必须完成防火墙或入侵检测系统的脆弱性和误操作分析。

——等级 K3 必须满足等级 K2 的需求，还能够检测是否存在对存储于防火墙或入侵检测系统中的数据以及对传输的数据的任何改动。另外，还必须给出详细设计和配置管理文档。

——等级 K4 必须满足等级 K3 的所有需求，还必须提供标识和鉴别功能，以保护防火墙或入侵检测系统免遭重放攻击。另外，还必须提交源代码和/或硬件设计文档。

——等级 K5 必须满足等级 K4 的所有需求，还必须提供相互鉴别功能。另外，还要求给出防火墙或入侵检测系统安全策略的正式模型。功能规格说明、体系结构设计文档和详细设计文档必须以半形式化的方式编写。

——等级 K6 必须满足等级 K5 的需求。在该等级上，必须验证详细设计文档、源代码和/或硬件设计文档之间的一致性。

——等级 K7 必须满足等级 K6 的所有需求。在该等级上，必须以形式化的方式编写功能规格说明和体系结构设计文档，以保持与形式化的系统安全策略模型是同步的。

KISEM 是基于 KISEC 而构造的，描述了如何根据这些准则来评估防火墙和入侵检测系统。KISEM 的特定目的是，确保存在一组与 KISEC 互补的、协调一致的评估方法。

6.5.3 源

参考文献目录：

[50] 韩国信息安全评估准则(KISEC)；

[51] 韩国信息安全评估方法学(KISEM)。

注：KISEC/KISEM 是韩国信息安全机构(Korea Information Security Agency)的产品。该机构可以通过下面的网址联系：http://www.kisa.or.kr/。

6.6 RAMP 维护阶段的评定

⇒D⇒	⇒I⇒		⇒O⇒

6.6.1 目的

为把以前的 TCSEC 评定扩展到新版本，提供一个机制。

6.6.2 描述

建立维护阶段评定(Rating Maintenance Phase，RAMP)程序，是为了提供一个把以前计算机系统产品的 TCSEC 评定扩展到一个新版本的机制。RAMP 通过使用参加产品维护的人员，寻求减少维持一个评定所要求的评估时间和工作量，以便管理改变的过程并执行安全分析。因此，承担证明为 RAMP 所付出的工作量，这依靠那些系统维护的责任(即供应商和 TEF)，而不依靠一个评估组。

在 CC(信息技术安全评估通同准则)中,为了维护现有 EAL 等级给出一些需求。为了关注这些需求,类似于 RAMP 的程序目前正在开发中。

6.6.3 源

参考文献目录:

[32] 维护阶段评定程序(RAMP),版本 2,1995。

注:RAMP 是美国国家计算机安全中心(National Computer Security Center NCEC)的产品。

6.7 ERM 评估评定的维护(一般性的)

⇒D⇒	⇒I⇒		⇒O⇒

6.7.1 目的

在其生存周期和(或)时间周期之外,尤其是修改之后,延续已取得的保障。

6.7.2 描述

一旦已经取得系统的保障,但当其予以修改时,仍存在所要求的保障。为了维持系统在历经小的改动之后的保障,目前存在一些模式,以便维护所进行的评价(即,“认证”或“评定”)。

评估评定的维护(Evaluation Rating Maintenance),是评估阶段之后的那个评价阶段。这一术语之下的理解是,一系列维护评定的动作,评估符合该产品修订版本的可用需求,并允许列出这些版本。在 ERM 期间,供应商执行为了确定对产品的改变保持了早先取得的评定的大部分工作。

在一个 ERM 模式中,涉及了一些不同的实体(供应商、用户、认证组织),它们具有各自的责任。针对这一保障框架,这意味着称为“评估评定维护”的保障方法,极大地依赖于设计/开发阶段和运行保障阶段。

评估评定维护模式以各种不同的形式存在,通常由下面一些部分组成:

——可用需求:评估产品的需求。

——ERM 审计:基于一个合适的、具有代表性的样例,评审 RAMP 的证据,以确保只实施了已批准的改变,并执行了满意的安全分析。除了 VSA 执行所要求的 RAMP 审计之外,还可由安全分析组执行定期 RAMP 审计。

——ERM 计划:描述机制、规程和工具的供应商文档用于满足 RAMP 需求。在整个评定维护阶段中,都遵循评定维护计划中的规程。该评定维护计划由供应商提出,并作为评估过程的一部分而得以批准。在产品 RAMP 的进行期间,特别是在指派人员的标识中,该评定维护计划可以改变。

——安全分析:以符合可用需求的方式,检查提出的改变(或一组改变)是否支持原来产品及其后续发布的、以前已按 RAMP 维护的产品所具有的安全特征和保障。

通常,ERM 模式的操作者是:

——安全分析组:面向技术审核委员会,负责执行安全分析,并负责 RAMP 证据表达和保护的个体(例如,VSA,附加的评估人员)。

——技术评审委员会:提供高层评审资料,包括评估组的技术发现、结论和建议。技术审核委员会作为评估质量、一致性和一贯性的一个检查点。

在美国,ERM 已正式地成为 RAMP,用于 TPEP 和 ISO/IEC 21827(SSE-CMM)的评定。在英国,ERM 已正式成为 ITSEC 评定所基于的认证维护模式。

ISO/IEC 15408 评估准则承认 ERM，但把评估维护留给监视评估模式的国家机构。

6.7.3 源

关于美国评估维护模式，可参考 6.6。

关于英国评估维护模式，可参考文献：[44] 英国认证维护模式，发行版 1.0。

注：认证维护模式(Certificate Maintenance Scheme CMS)是以下认证机构的产品：
英国信息技术安全评估认证模式(UK IT Security Evaluation and Certification Scheme)。

6.8 TTAP 可信技术评价程序

⇒D⇒	⇒I⇒		

6.8.1 目的

建立、批准及监视商业评估服务机构。

6.8.2 描述

可信技术评价程序(Trust Technology Assessment Program，TTAP)是国家安全局(NSA)和国家标准和技术协会(NIST)共同工作成果，以便建立商用服务机构来执行可信产品评估。TTAP 将建立、批准并监视商业评估机构。该程序最初关注具有 CC(信息技术安全评估通同准则)所表征的特征和保障的产品。

在 TTAP 之下执行评估，组织必须被认可为一个 TTAP 评估机构(TTAP Evaluation Facility，TEF)。首先，想成为 TEF 的组织向 TTAP 监督委员会(TTAP Oversight Board)提出暂定状态的申请。如果被接受的话，该组织就被授权进行试用性评估，并被列入暂定的 TEF 列表。接着，暂定的 TEF 与供应商签订合同并进行可信产品的试用性评估。试用性评估之后，升格暂定状态成为可进行 TTAP 之下评估的 TEF。

TTAP 监督委员会应监视 TEF，以确保评估质量和评估的一致性。期望进行安全评估的信息技术产品的供应商应与一个 TEF 订立合同，并支付其产品评估的费用。一旦评估完成，产品将会被添加到国家安全局的评估产品列表中。

6.8.3 源

参考文献目录：

[28] 可信技术评估程序(TTAP)。

注：TTAP 是美国政府内部标准，同时也是国家安全监督委员会(Oversight Board c/o National Security Agency)的产品。

6.9 TPEP 可信产品评估程序

⇒D⇒	⇒I⇒		

6.9.1 目的

为了鼓励可信计算机产品的广泛可用性。

6.9.2 描述

依据可信产品评估程序(Trusted Product Evaluation Program,TPEP),供应商带着他们的商用成品(COTS)向 NSA 申请特定等级的信任等级的评估。评估者按着 TPEP,采用 TCSEC 及其解释,评价产品是否满足指定评定的需求。每一个季度,TPEP 评估结果发布在已评产品列表(EPL)中,该列表像第 4 章的信息系统安全产品和服务目录。

TPEP 的最终目的是,鼓励可信计算机产品对数据所有者和希望保护其敏感的和(或)保密信息的用户的广泛可用性。其他目的包括:

——确保满足最终用户操作需求的有用可信产品的可用性;

——提供可信产品,以便构造一个可信系统;

——提供有关如何使用可信产品的特定指导;

——提供有关安全特征互操作性方面的特定指导,以及有关被评产品的、与特定特征相关联的保障等级方面的具体指导;

——通过使用计算机以及国家与国防信息基础设施(National and Defense Information Infrastructures),培育一种开放和协作的业务关系。

6.9.3 源

参考文献目录:

[46] 可信产品评估程序(TPEP)。

注:TPEP 已被替换为可信技术评价程序。现在,已经不再使用可信计算机评估准则(TCSEC)来进行评估,参阅 TCSEC。

TPEP 是美国政府的一个内部标准,同时也是美国国家安全局(National Security Agency)的一个产品。

6.10 Rational 统一过程®(RUP®)

6.10.1 目的

提供一个完整的、已普遍的软件工程生存周期框架,包括环境、过程、活动、技术以及工具。

6.10.2 描述

Rational 统一过程®或 RUP®是一个商用成品的软件工程过程框架,由 Rational® 软件公司开发和维护。该框架持续不断地更新和改进,以反映当前经验并演化一些最佳实践。

与一些标准(例如 ISO 12207)不同,"空"框架 RUP 具有指导、过程、方法、技术、模版、工具和一些例子,据此可实例化一个具体的过程框架,并管理和改进之。

RUP 本身的设计和建档,如其产生的软件产品,采用了统一建模语言(Unified Modeling Language,UML)。RUP 的基础性对象模型是统一软件过程模型(Unified Software Process Model,USPM)。

从项目管理的角度上看,RUP 为开发组织内的任务和职责分配提供了一个结构化的途径。它强调极早地关注高风险问题,并允许随着项目的进展来精化需求,以助于在预期的进度和预算内满足用户需求的高质量软件。

RUP 的活动有效地使用了统一建模语言(UML)来创建和维护模型,并强调了模型的开发和维护-

通过计算机处理工具支持开发中软件系统丰富语意的表示。这些工具使大部分过程自动化，例如可视化建模、编程、测试和配置管理。

RUP 是一个可配置的过程框架，适用于小的开发团队和大的开发组织。它的过程体系结构为一个过程族提供了共性，并且在开发套件的支持下，该体系结构支持 RUP 的配置，以适应特定组织的要求。

RUP 融合了一些最佳实践，尤其是如下 6 个基本的最佳实践：

——交互地开发软件；

——管理需求；

——使用基于构件的体系结构；

——可视化的软件建模；

——验证软件质量；

——控制软件的改变。

从过程管理和改进的角度看，在项目层面上，RUP 符合 CMM 和 ISO/IEC 15504 的需求。如果正确实施的话，它对应于 CMM 组织成熟度 2 级或 3 级。因为软件过程予以良好的定义，并且在管理上对所有项目的技术进度都有很好的了解，因此 RUP 适合于较高等级的过程成熟度。

6.10.3 源

参考文献目录：

[52] 菲利普·克鲁奇顿，《Rational 统一过程》 简介。

注：Rational 为 IBM 公司软件集团旗下所有，RUP 是该软件品牌的产品。

可以通过以下网址联系 Rational：http://www.rational.com/rup/。

6.11 ISO/IEC 15288 系统生存周期过程

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.11.1 目的

为任何类型复杂技术系统的整个生存周期，提供生存周期模型、过程和活动。

6.11.2 描述

ISO/IEC 15288 系统生存周期过程(System Life Cycle Processes)，是 ISO 第一个处理由硬件、人机接口(human interface)和软件所组成的复杂系统的系统生存周期过程的标准。目前，这一 ISO/IEC 标准正在处于 FDIS(最终草稿国际标准)阶段，在 2002 年 10 月发布。

该指导性技术文件围绕人造系统的生存周期，时间跨度为：从系统概念到系统的退役。它为获取和支持系统产品和服务提供了相应的过程，而这些产品和服务是由一个或多个如下类型的系统部件：硬件、软件和人机接口配置而成的。这一框架还为系统的生存周期及其过程的评价和改善，提供了一些活动列表和条款。

在这一国际标准中的过程形成了一个全集，一个组织可以依据这一全集，构造适合该产品、服务类型以及市场的生存周期模型。一个组织可以根据其意图，通过剪裁条款来选择和应用一个合适的子集，以实现该组织的意图。

从质量观点上来说，相关的大部分过程是：质量管理过程，集成、验证和确认过程，以及项目规划、评价和控制过程。

这一国际标准可以以不同方式使用：

——一个组织可采用该标准来建立所希望的过程环境;其中的过程可通过训练有素的人员、利用特定的方法、规程、技术和工具等予以支持。组织应使用这一环境来管理它的项目,服务于项目生存周期阶段的进展。

——一个组织中的项目为了提供产品或服务,可以使用该标准来选择、结构化、使用和执行已建立的环境元素。

——在供需关系中,通过合同或协议,该标准还可以用于选择、协商和执行该标准之外过程与活动。此外,这一模式还可以用于评价供需双方性能与协议的符合性。

该标准是由 ISO/IEC 19760 指南所支持的,该指南为一个标准,期望:

——作为 ISO/IEC 15288:系统生存周期过程的姊妹文档;

——给出该国际标准(ISO/IEC 15288)的实施指南。

该指南适用于规模大的或规模小的系统,适用于要求规模大或规模小的项目组的系统,适用于新的或遗产系统。该指南包括:1)一些连接,可连接到其他一些为了支持实施该国际标准(ISO/IEC 15288)以及为了评价实施有效性所需要的 ISO 文档,2)一些因素,即当实施该国际标准(ISO/IEC 15288)所要考虑的因素。

该指南对以下人员是有用的:

——一个组织中,实施该国际标准(ISO/IEC 15288)的人员;

——针对一个特定的系统,使用该国际标准(ISO/IEC 15288)的人员;或

——基于该国际标准(ISO/IEC 15288),编制组织或特定行业标准的人员。

适当时,可以针对系统的规模、项目的人员或系统类型,定制一些特定应用。在该国际标准的附录 A 中以及在该标准的第 4 章中,给出了相应的定制指导。但是,该指南没有提供也不期望提供该国际标准(ISO/IEC 15288)有关需求的基本理由。

6.11.3 源

参考第 2 章:ISO/IEC 15288。

参考文献目录:

ISO/IEC TR 19760 系统工程 有关 ISO/IEC 15288 指南

注:ISO/IEC 15288 是以下委员会的产品:

ISO/IEC JTC 1/SC 7/WG 7 信息技术 软件和系统工程 生存周期管理。

6.12 ISO/IEC 12207 软件生存周期过程

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.12.1 目的

为软件系统的整个生存周期提供生存周期模型、过程和活动。

6.12.2 描述

软件不论作为一个整体还是作为许多产品和系统的必要部分,其重要性就要求一个通用的国际性框架,以便规约有关软件过程、活动和任务的最佳实践。

ISO/IEC 12207 把软件生存周期期间可执行的活动分组为:

——基本过程(获取过程、供应过程、开发过程、运行过程、维护过程);

——支持过程(文档过程、配置管理过程、质量保证过程、验证过程、确认过程、联合评审过程、审核

过程、问题解决过程)；

——组织过程(管理过程、基础设施过程、改进过程、培训过程)。

每个过程详细说明了所包括的活动和任务，定义了相应的责任，还定义了活动/任务的输出。

必须注意，这一标准并没有隐含任意特定的生存周期模型。

ISO/IEC 12207 的过程形成了一个全面综合的集合。一个组织可以根据自己的意图，选择一个适合的子集来实现该意图。此外，为了适应软件产品的范围、规模、复杂度和紧要程度以及组织自身情况，可以选择并剪裁该标准的活动。

从质量的角度上看，相关的大部分过程是：质量保证过程、验证过程、确认过程、联合评审过程、审计过程和问题解决过程。另外，该标准突出了日常活动期间所进行的过程内部评估。

该标准的读者和使用者为：

——获取一个系统的组织，其中该系统包括软件或独立存在的软件产品。

——软件产品供应方。

——参与软件运行和维护的组织。

——针对 12207 的指南是一个标准，其中精化了在不同方式的语境中应用 ISO/IEC 12207 中应考虑的一些可应用的因素。该导则讨论了 3 个基本的生存周期模型，并且提供了定制的例子。该导则不提供 ISO/IEC 12207 所要求的基本原理。

——讨论了 3 个基本生存周期模型，并提供了一些剪裁的例子。

——该指南并不想提供有关 ISO/IEC 12207 需求的理由。

6.12.3 源

参考第 2 章：ISO/IEC 12207。

参考文献目录：

ISO/IEC TR 15271 信息技术 有关 ISO/IEC 12207 的指南

注：ISO/IEC 12207 是以下委员会的产品：

ISO/IEC JTC 1/SC 7/WG 7 信息技术 软件和系统工程 生存周期管理。

6.13 V-模型

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.13.1 目的

为软件开发中有关必须要做什么、如何来执行任务以及应使用什么工具，奠定一种一致的、绑定的方式。

6.13.2 描述

V-模型是一般的方向性指导系列(250，251 和 252)，描述了一种生存周期模型，其中包括一组规程、一组所应用的方法以及开发软件系统中所用工具在功能上的需求。该模型最初是为德国联邦国防(German Federal Armed Forces)部开发的。V-模型是一个得到国际认可的开发标准。

V-模型为开发任务定义了要采用的步骤以及要应用的方法，定义了所用工具应具有的功能特征。V-模型包括一个生存周期过程模型、方法的分配以及工具的功能需求。

其中的生存周期过程模型结构化为以下 3 部分：

第 1 部分：规章。这一部分包括要执行的步骤与结果(产品)和执行(活动)进行绑定的规定。

第 2 部分:相对权威机构的补充。一旦是为德国联邦国防领域和为民众联邦管理领域,则存在这一部分。该部分包括把该生存周期过程模型应用于这两个领域的指导。

第 3 部分:手册集。

这一部分包括一个处理一些特定主题(例如,ICT 安全或面向对象语言的使用)的手册集。

V-模型可作为合同的基础,作为指导的基础,作为参与方之间交流的基础。通过该文档的描述手段和术语条目,为客户、用户、合同方以及开发方之间的相互理解并减少摩擦奠定一个基础。

V-模型的条目在组织上是协调的,针对特定的技术开发过程,这些条目予以相应的限制。因此,V-模型不仅适宜作为公共管理中的开发标准,而且还适宜作为工业中的开发标准。

V-模型的使用不需支付许可费用,它不是专利,是一个不受复制保护的标准。

对于关键软件的生产而言,V-模型包括了一些必要的规则。通过应用 V-模型,管制开发过程的这些规定,满足目前有效的安全准则(ITSEC)。因此,为认证如此开发的软件带来极大的便利。

V-模型、方法标准(Methods Standard)和工具标准(Tool Standard),完全覆盖了功能性领域的软件开发、质量保障、配置管理和项目管理,提供了实际支持,是复杂的但却是灵活的和协调的,具有广泛的应用领域,并在变化控制委员会(Change Control Boar)的监管下得到公开的控制。控制委员会负责处理该标准的改进和纠正性变更。

变更控制委员会确保用户有关 V-模型必要的维护和修改过程的作用,该委员会大概每年与来自工业界和政府部门的代表聚会一次。依据有序的规程,变更控制委员会负责认真处理对 V-模型的所有变更请求。

6.13.3 源

参考文献目录:

[42] V-模型 IT 系统的开发标准,VM 1997。

注:V-模型是德国 BWB IT I 5 的产品。

6.14 ISO/IEC 14598 软件产品评价

⇒D⇒			

6.14.1 目的

为软件产品质量提供一种测量、评估和评价的方法。

6.14.2 描述

ISO/IEC 14598 基于 ISO/IEC 9216 的一般质量模型。因此,它为所有类型的软件产品的评价提供了一个框架,并指出软件产品测量和评估方法的需求。

ISO/IEC 14598 期望开发者、获取者使用之,特别是那些负责软件产品评估的独立评价者使用之。应用 ISO/IEC 14598 所产生的评估结果,可以被管理者和开发人员/维护人员用于度量与需求的符合性,并在必要的地方做出一些改进。评估结果还可被分析人员用于建立内部度量和外部度量之间的关系。通过研究和检查项目产品的质量信息,过程改进人员可使用评估结果来确定过程如何予以改进。

ISO/IEC 14598 是系列标准,给出了度量、评价和评估软件产品质量的方法。但是这些标准既没有描述评估软件生产过程的评估方法,也没有给出成本预测的方法。当然,软件产品质量的测量可用于软件生产过程的评估和成本预测。

ISO/IEC 14598 的评估过程流程如图 1 所示。

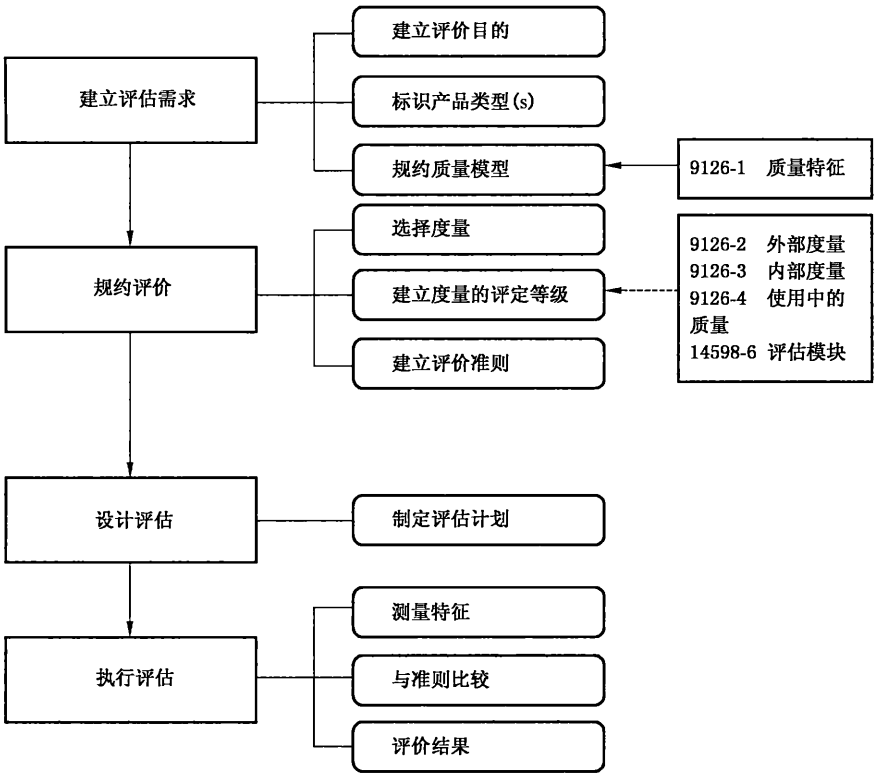


图 1 ISO/IEC 14598 评价过程的流程

6.14.3 源

参考第 2 章:ISO/IEC 9126-1;ISO/IEC 14598-1。

参考文献目录:

ISO/IEC TR 9126-2 软件工程 产品质量 第 2 部分:外部度量

ISO/IEC TR 9126-3 软件工程 产品质量 第 3 部分:内部度量

ISO/IEC TR 9126-4 软件工程 产品质量 第 4 部分:使用质量度量

ISO/IEC 14598-2 软件工程 产品评价 第 2 部分:规划及管理

ISO/IEC 14598-3 软件过程 产品评价 第 3 部分:开发者过程

ISO/IEC 14598-4 软件工程 产品评价 第 4 部分:获取者过程

ISO/IEC 14598-5 信息技术 软件产品评估 第 5 部分:评价者过程

ISO/IEC 14598-6 软件工程 产品评估 第 6 部分:评价模块文档

注:ISO/IEC 14598 是以下委员会的产品:

ISO/IEC JTC 1/SC 7/WG 7 信息技术 软件和系统工程 生存周期管理。

6.15 X/Open 基线安全服务

⇒D⇒			

6.15.1 目的

通过与第三方认证的 X/Open 标准的符合来提供保障。

6.15.2 描述

X/Open 授牌是一种不同类型的保障，它通过符合性测试、供应商担保以及商标（暗示着第三方控制）来提供保障。这一途径提供了保障，即通过提供文档化证据和第三方对标准的执行，系统将按供应商声称的那样执行。

X/Open 是一个创建开放标准的公司联盟，以提供一个开放系统环境，称为公共应用环境（Common Applications Environment，CAE）。这一环境提供应用程序和系统的互操作性和可移植性。符合 X/Open 标准的产品、系统和应用带有 X/Open 商标，以表示其符合它们的标准。

X/Open 授牌是一个规程，通过这一规程，供应商获得其产品符合一项或多项 X/Open 标准的认证证书。这个证书包括实际系统细节的符合性陈述以及测试证据，以支持供应商的声称。供应商产品的测试，可由供应商执行或由第三方执行；但测试实验室必须得到 X/Open 的批准。

X/Open 的安全解决方案是 X/Open 的基线安全服务（X/Open Baseline Security Services，XBSS）规格说明，该规格说明的开发是为了提供给购买者 X/Open 已授牌系统，具有如下保障：这样系统提供了已定义的最小等级的安全功能。XBSS 本质上是一个包括大多数安全功能需求和几个保障需求的 PP[保护轮廓（Protection Profile）]。该轮廓定义了产品必须提供的最低等级的安全功能。它还定义了一些特定的默认设置，其中需求是一些可供选择的安全项。一个系统若作为符合这一轮廓定义而进行注册，那么该系统就必须提供这一等级的安全或更高等级的安全。

任何满足已定义的安全等级的系统，当符合时均可予以授牌。实际系统（运行系统）的细节必须记录在符合性陈述中。X/Open 要求产品像 X/Open XBSS 规格说明那样，支持强制性的安全功能和默认的参数设置。

X/Open 不同于其他 3 个候选的 AA 方法学，因为它不关注开发保障。XBSS 规格说明包括一些主要的功能需求，而保障量是通过符合性测试、供应商担保以及 X/Open 商标来提供的。

6.15.3 源

参考文献目录：

[39] X/Open 基线安全控制（XBSS）；

[30] 开发品牌实践指导。

注：X/Open 品牌是开发标准组织（The Open Group）的产品，该组织总部在美国旧金山。可通过以下网址访问开发标准组织：http://www.opengroup.org/。

6.16 SCT 严格符合性测试

6.16.1 目的

测试安全功能。

6.16.2 描述

严格（安全）符合性测试[Strict（Security） Conformance Testing]定义了一种按照公开可用的规范（通常是标准）对安全系统进行测试的方法。为了强调测试的实施，以一种系统的方法设计了一些测试套件。驱动测试的开始点是一个抽象安全目标（abstract security target，AST），它编入在一个基础性的安全标准中。这提供了一种结构化测试套的手段，而且还提供了一个途径，使从利用安全功能和支持机制的安全要求到这些机制的测试更容易。对应于该基础性标准的抽象水平，在一个抽象层上撰写这些

测试。接着,针对特定的实现,参数化测试套件。这提供了一个优点,即允许进行一定量的抽象安全目标和对应的测试套件的预评估。这确保基本的覆盖程度,减少评估中准备证据的工作量,其中评估的主题是标准的实施。

SCT 是功能性测试而不是稳健性(robustness)测试。

6.16.3 源

参考文献目录:

[20] SCT 严格符合性测试。

注:SCT 是英国的国家物理实验室的产品。

可通过以下网址访问该实验室:http://www.npl.co.uk/。

6.17 ISO/IEC 21827 系统安全工程 能力成熟度模型(SSE-CMM®)

D	I	T	O

6.17.1 目的

改进组织的系统安全工程过程并产生具有能力保障的可交付件。

6.17.2 描述

ISO/IEC 21827 信息技术 系统安全工程 能力成熟度模型(SSE-CMM®)主要关注系统安全工程所要求的过程领域(PAs),称为工程 PA(Engineering PA)。ISO/IEC 21827 还包括支持在系统安全工程领域内所执行的项目的 PA,称为项目 PA,以及组织内所要求的 PA,整体上来支持系统安全工程 PA,称为组织 PA。

ISO/IEC 21827 强调系统安全工程 PA 及其活动。SSE-CMM 的 PA 能够根据组织的需求进行调整,并且 ISO/IEC 21827 的应用范围可以是一个特定的项目、一个组织部门或整个组织。

ISO/IEC 21827 适用于且可用于任何涉及信息和通信技术(ICT)安全的组织或关注 ICT 安全的组织。这些组织的范围可以从那些开发产品和/或集成产品(不管是安全产品还是非安全产品)的组织,到那些使用安全产品或提供安全服务的组织。因此,ISO/IEC 21827 可用于组织来改进他们的系统安全工程过程,以便按进度开发具有高质量的 ICT 安全产品或交付安全服务(例如:威胁和风险评价)。

SSE-CMM 是一个独特的模型,因为它详述了安全系统工程的安全工程需求,除此之外还提供了一些工程安全服务,这些均需开发环境满足之。另外,它包括了针对广泛开发领域的 PA,例如安全需求定义、系统测试、威胁和脆弱性分析。这与可信能力成熟度模型(TCMM)是不同的,TCMM 只规范了组织开发环境必须满足的需求。

为了描述组织的过程,并且为了度量组织对这些 PA 的执行,ISO/IEC 21827 包括 PA、基本实践(Base Practices,BP)、一般实践(Generic Practices,GP)和能力水平。PA 是由一组相关的 BP 组成的,BP 关注组织内特定过程活动,而 GP 是与组织整个过程的成熟度相关的。PAs、BPs、GPs 可以认为是指示与 ISO/IEC 21827 符合的需求和能力等级;不过,这些需求只涉及一个过程达到的最终结果,而不涉及如何达到这一结果,以便不干扰组织的运作模型。对每一个 PA 都指定一个能力等级,以表明与 ISO/IEC 21827 的符合等级;等级总有 5 级,从 0 级的"未执行"到 5 级的"持续改进"。该标准以图形表达方式,给出了一个评定轮廓,其中包含每一等级及其要执行的 PA,或作为组织整体上所达到的成熟度等级。评定组依据 SSE-CMM 评定方法学(SSAM),对该组织执行与 ISO/IEC 21827 的符合性鉴定,确定能力等级和评定轮廓。

能力等级表明一个组织所有可用的 PA(一组相关的实践)已经达到一个最小的能力等级。GP 是

一些特定的需求，适用于与整个 PA 成熟度和整个组织过程制度化有关的特定需求。后继的等级表明了该组织的整体过程成熟度和能力的改进，并有能力在整个组织中实施这些 PA。

等级说明描述了组织在每个 PA 的能力水平，表明了组织的强处和弱点。等级说明可用于指示组织必须在什么地方付出努力以改进它们的过程并实现下一个更高的能力水平。尽管这不是最初所预想的，等级说明能作为一个调配工具以要求组织在具体的 PA 上实现不同的能力水平而不是在所有的 PA 上实现一个能力水平。比如，一个调配说明可能指定在 PA1-5 上具有能力水平 2 并在 PA6-10 上具有能力水平 3。

ISO/IEC 21827 的 SSE-CMM 是一个连续模型，其在工业组织中更为灵活，因为可以只选择适用的 PA。不过，如果采用了阶段模型，比如 TCMM，那么比较不同组织的等级则会更为困难。

因为水平 1 的过程是随意的并且可能不完整；它是不充分的，所以一个组织应当在所有的 PA 上至少实现能力水平 2，以满足良好的安全。对于 SSE-CMM 模型，这意味着，组织应当规划并跟踪其自身的基本准则，并且在产品中发生错误时应进行纠正。这表明一个组织的过程是可重复的并且是一致的，从而可以产生一个可预测的并且一致的产品，而这是很重要的保障因素。

6.17.3 源

参考第 2 章：ISO/IEC 21827。

参考文献目录：

[24] 系统安全工程能力成熟度模型 模型描述(SSE-CMM 模型)，版本 2.0；

[25] 系统安全工程能力成熟度模型 评估方法(SSE-CMM 方法)，版本 2.0。

注 1：ISO/IEC 21827 是以下委员会的产品：

ISO/IEC JTC 1/SC 7/WG 3 信息技术 安全技术 安全评估准则。

注 2：ISO/IEC 21827 的基础文档由国际系统安全工程协会(International Systems Security Engineering Association，ISSEA)提供和维护。

可以通过下面的网址访问 ISSEA：http://www.issea.org。

6.18 TCMM 可信任能力成熟度模型

D	I		

6.18.1 目的

改进组织的软件安全保障和软件开发过程。

6.18.2 描述

可信任能力成熟度模型(Trusted Capability Maturity Model，TCMM)是一个开发阶段的安全软件保障标准，它基于 SEI 制定的 CMM 的基本原理和结构。尽管 TCMM 是一个特殊的 CMM，但它通过合并可信任软件开发方法(Trusted Software Development Methodology，TSDM)和 SEI CMM，产生了许多修正的关键过程领域(Key Process Areas，KPA)以及一个新的 KPA，即可信任软件开发(Trusted Software Development)。可信任软件开发包含了新的惯例，这些准则不适合于已有的 KPA。TCMM 只关注开发环境，面向组织的管理和组织活动；这与 ISO/IEC 21827(SSE-CMM)有极大的不同。TCMM 只适用于过程和系统。任何与 TOE 开发相关的过程都不在考虑范围。

TCMM 包括关键过程领域，一般惯例，以及描述组织过程和度量组织多好地执行与 ISO/IEC 21827 的 SSE-CMM 模型相似的 KPA 的能力水平。一个组织将被赋予一个能力水平，以指示其对某一水平的符合性。TCMM 共有 5 个水平，从水平 1 的初始的到水平 5 的优化的。水平 1 包含很少的 KPA，组

织具有随意的过程。

作为一个阶段模型，TCMM 能力水平形成了一系列阶段，每一个阶段有一个水平（水平 1 除外），其包括了唯一的一组相关的 KPA。与连续模型不同，组织必须满足所有的 KPA 才能达到一个能水平。不过，这些阶段有助于组织关注改进它们的过程，并清晰地给出了如何提升到下一水平的途径。这些阶段使得需求和比较更为容易，因为每一个阶段的 KPA 保持不变。作为一个阶段模型，TCMM 与 CC 相似；不过，TCMM 只限制于开发环境安全，而 CC 集中关注 TOE。

6.18.3 源

参考文献目录：

[26] 可信任能力成熟度模型，版本 2.0；

也可以参考文献[27]，[48]。

注：TCMM 由（美国）国家安全局（NSA）和软件工程协会（SEI）共同制定，TCMM 从未发布，因为 NSA 的随后决定只支持其所赞助的两个提案中的一个。

6.19 CMMI 集成化能力成熟度模型®

D	I	T	O

6.19.1 目的

为组织的过程及其能力的改善提供指导，以便管理产品和服务的开发、获取和维护。

6.19.2 描述

集成化能力成熟度模型®（Capability Maturity Model® Integration，CMMI SM）提供了一个改进组织的过程，以及提升其管理产品和服务的开发、需求和维护的能力的指导。CMM®集成 SM 把经过证明的实践放在一个结构当中，该结构有助于评估组织的成熟度及过程域能力、有助于确定改善的优先次序，有助于指导这些改善的实施。

CMMI 产品套件（CMMI Product Suite）源于一个框架，该框架可产生多个集成模型、评价进程和一个评定方法。随着新的资料添加到该框架，将会有更多的集成模型和支持资料，覆盖更多的业务领域。

目前，如下的模型是可用的：

——CMMI-SE/SW 针对系统工程和软件工程的集成模型；

——CMMI-SE/SW/IPPD 针对系统工程、软件工程、以集成产品和过程的开发模型；

——CMMI-SE/SW/IPPD/SS 针对系统工程、软件工程、集成产品和过程开发、以及供应源模型。

在 CMMI 的工作可以用来支持过程和产品的改进，减少冗余并减少运用分离的单独模型时的不一致性。CMMI 的目的是运用集成了多个准则（比如在系统开发中不可分割的系统工程和软件工程）的模型提高效率、投资回报、以及有效性。

CMMI 项目的概念是改进 CMM®技术在软件工程的成功应用之外在更为广泛的领域的可用性。

CMMI 项目的概念号召使用共同技术、共同组件、以及构建能力成熟度模型的规则，通过减少多个领域的用户所需的培训和过程改进的支出，使得能力成熟度可用。随着概念的发展，CMMI 采用比较明智的做法，限制 CMMI 项目的最初的范围为几个最需要的领域当中，直到概念得到验证。工业和政府部门选择软件工程、系统工程和集成产品开发的 CMM，用于最初的概念验证阶段。CMMI 产品套件被设计为在领域上和生存周期上都具有扩展能力。如今，在需求方面的扩展工作已经展开，诸如安全系统工程方面的也将可能被包括。扩展的决定将基于最初发布的成功、用户社区的需要和支持、以及有开

发的参与者。

CMMI 和来源模型(软件 CMM,集成产品开发模型,以及 EIA/IS 731,即系统工程成熟模型)覆盖了一样的生存周期。

CMMI 框架设计用于容纳额外的领域,而且可以根据用户社区的需要增加领域。目前,增加领域的过程在 CMMI 的操作概念(CONOPS)文档中进行描述。

CMMI A-Spec 要求 CMMI 产品套件与 ISO/IEC 15504 一致和兼容,并且该框架能容纳额外的准则,但是并没有具体制定是何种领域。到目前为止,已经加入了供应者来源准则。

6.19.3 源

参考文献目录:

[35] 集成化能力成熟度模型®中系统工程和软件工程的集成模型,CMMI-SE/SW 版本 1.1;

[36] CMMISM 系统工程/软件工程/集成产品和过程开发,版本 1.1,阶段式表述;

[37] CMMISM 系统工程/软件工程/集成产品和过程开发/供应商来源,版本 1.1,阶段式表述。

注:CMMI 是软件工程协会(Software Engineering Institute)的产品。

可以通过以下网址访问该协会:http://www.sei.cmu.edu。

6.20 ISO/IEC 15504 软件过程评估

D	I	T	O

6.20.1 目的

根据 ISO/IEC 12207 为评价软件生存周期过程的概念和过程提供一个框架。该框架与 ISO/IEC 15939 的过程度量一致。

6.20.2 描述

ISO/IEC 15504 与 CMM 一致。ISO/IEC 15504 采用了过程维度和能力维度。基本准则被划分成组织、管理、工程、客户-供应者和支持几个部分。ISO/IEC 15504 根据下面的开发过程规范了组织的能力等级:

L0	不完整的过程
L1	经执行的过程
L2	经管理的过程
L3	经确立的过程
L4	可预测过程
L5	优化的过程

ISO/IEC 15504 的等级基于对具体过程实例的评价。ISO/IEC 15504 支持所有类型的评价,其适用于自我评价和独立评价,还适用于连续的评价和离散的评价。

ISO/IEC 15504 水平 3 等级意味着成功的 ISO 9000 认证。

6.20.3 源

参考第 2 章:ISO/IEC 15504-1;ISO/IEC 15504-2;ISO/IEC 15504-3;ISO/IEC 15504-4;ISO/IEC TR 15504-5。

注：ISO/IEC 15504 是以下委员会的产品：

ISO/IEC JTC 1/SC 7/WG 10　信息技术　软件和系统工程　过程评价。

6.21　CMM　能力成熟度模型®（针对软件）

D	I		

6.21.1　目的

判断软件过程的成熟度以及改进一个组织在这些过程的成熟度。

6.21.2　描述

软件的能力成熟度模型(Capability Maturity Model for Software)描述了根本的软件过程成熟度的原理和惯例，用于帮助组织改进它们的软件过程的成熟度，使软件过程从随意的、无序的过程发展为一个成熟的、有序的软件过程。

CMM 按 5 个成熟度水平组织：

水平 1—初始的：该软件过程具有随意的、有时甚至有混乱的特征，该水平定义了很少的过程，其成功依赖于个人的努力和行为。

水平 2—可重复的：该水平确立了基本的项目管理过程，以跟踪成本、进度以及功能。采用相似的应用程序，项目可以重复获得已取得的成功，因为必需的过程秩序是到位的。

水平 3—已定义的：该水平的管理活动和工程活动的软件过程都是有文档的、标准化的，并且已集成在组织的标准软件过程中。所有的项目都采用一个经认可的和经定制的组织标准软件过程，进行软件的开发和维护。

水平 4—受管理的：该水平收集了软件过程和产品质量的详细测量。软件过程和产品都数量化地进行理解和控制。

水平 5—优化的：通过来自于过程、先导性的创新思想和技术的数量化反馈，使得能够进行连续的过程改进。

随着组织在这 5 个水平的增进，可预测性、有效性和组织软件过程的控制也确信可以得到提升。虽然不严格，但是经验证据都支持这一信条。

除了水平 1，每一个成熟度水平都可分解成几个关键的过程领域，这些领域表明了在提升软件过程时组织所应当关注的。

水平 2 的关键过程领域集中关注软件项目与确立基本的项目管理控制有关的方面，即要求的管理、软件项目规划、软件项目跟踪和监督、软件子合同管理、软件质量保障，以及软件配置管理。

水平 3 的关键过程领域涉及项目和组织两方面的问题，因为组织确立人事结构，对所有的项目间的软件工程和管理过程进行制度化。这些问题是：组织过程关注，组织过程定义、培训程序、集成软件管理、软件产品工程、组间合作、以及对等审查。

水平 4 的关键过程领域集中关注确立对软件过程和正在创建的软件产品的数量化理解，即数量化过程管理和软件质量管理。

水平 5 的关键过程领域涉及组织和项目必须处理的问题，以实施连续的、可测量的软件过程的改进等问题。这些问题包括缺陷预防（Defect Prevention）、技术变化管理（Technology Change Management）、以及过程变化管理(Process Change Management)。

每一个关键过程领域，都根据其对有助于满足目标的关键惯例来进行叙述。关键惯例描述了对关键过程领域的实施和制度化影响最大的基础结构和活动。

6.21.3 源

参考文献目录：

[34] 软件的能力成熟度模型。

注：CMM 是软件工程协会(Software Engineering Institute)的产品。

可以通过下面的网址访问该协会：http://www.sei.cmu.edu。

6.22 SE-CMM® 系统工程能力成熟度模型®

D	I		

6.22.1 目的

改进系统工程过程。

6.22.2 描述

系统工程能力成熟度模型®(Systems Engineering Capability Maturity Model®，SE-CMM®)，描述了确保优良的系统工程所必须有的组织系统工程过程的主要元素。

此外，SE-CMM 给出了实际系统的工程惯例与这些主要要素比较的参考。SE-CMM 在 1993 年 8 月开始制定，其制定是为了响应工业界要求协助整理与发布一个与 CMM 类似的模型，该模型可用于系统工程的连续性。SE-CMM 制定的工作由包括 SEI 在内的多个组织协作进行。

现在，该领域的当前工作属于 CMMI 的部分。

6.22.3 源

参考文献目录：

[21] 系统工程能力成熟度模型(SE-CMM 模型)，版本 1.1；

[22] 系统安全工程能力成熟度模型，评估方法(SSE-CMM 模型)，版本 2.0。

注：SE-CMM® 是软件工程协会(Software Engineering Institute)的产品。

可以通过下面的网址访问该协会：http://www.sei.cmu.edu。

6.23 TSDM 可信任软件开发方法

D	I		

6.23.1 目的

通过给管理政策(Management Policy)、环境控制和管理，以及软件工程分配信任等级提供保障。

6.23.2 描述

可信任软件开发方法(Trusted Software Development Methodology，TSDM)在 20 世纪 80 年代中期由战略防御倡议办公室(Strategic Defense Initiative Office，SDIO)制定，通过加强开发过程以增强软件的保障。

由于所提出的 SDIO 项目的预期规模(数百万行代码)过大，典型的软件错误密度将使得系统不起作用，分析表明改进开发过程能减少软件错误率。

为了确定潜在的弱点，软件开发过程的每一个特征都进行了检查。分析的结果形成了 25 条信任

准则。

在1993年7月2日的TSM报告中，TSDM定义了信任准则。其中还包括每条准则的基本原理，信任准则的符合性要求以及可适用信任类别的识别。此外，该文档确定了一系列关联的要求，这些要求描述了与信任准则中类似的活动，并对信任准则提供了一系列的有用引用文献。

25条TSDM信任准则可以按如下的4个领域进行分组，并且关联到一般软件开发过程：

——管理政策(信任准则1～6)；

——环境控制(信任准则7～10)；

——环境管理(信任准则11～14)；

——软件工程(信任准则15～25)。

每一个信任准则适用5个TSDM水平进行度量：

——T1(最低信任)；

——T2(中等信任)；

——T3(首选的)；

——T4(恶意的攻击)；

——T5(理想的)。

TSDM提出了软件/信息保障(IA)的度量方法。一个具体程序的软件开发计划(Software Development Plan，SDP)要求执行可接受的TSDM准则。这是因为SDP将会获得TSDM的符合性方法，以及软件工程团队的风险分析的初步结果。

能力评估。另外，十分重要的是要理解运用软件工程分析标准[比如软件工程协会(Software Engineering Institutes，SEI)的能力成熟度模型(CMM)]如何确定和跟踪TSDM的符合性。要求具备这样的知识，能估计为软件工程团队成员提供TSDM培训的程序的成本。最后，还需要软件重用的知识以及度量标准的收集。

注：为了集成CMM和TSDM，已经组成了一个来自于(美国)国防部的以及软件工程协会的团队，该团队最终制定可信任能力成熟度模型，作为执行可信任软件评估的基础。参阅6.18。

6.23.3 源

参考文献目录：

[29] 可信任的软件方法(卷1和卷2)；

[47] 一种可信任的软件开发方法。

6.24 SDoC 提供方符合性声明

D			

6.24.1 目的

供应者负责对产品、过程或服务与标准化文档的一致性的声明和证明。

6.24.2 描述

该方法利用供应者一致性声明(SDoC)正规化了开发者对产品的承诺。对于IT安全系统，该声明将包括系统的安全一致性声明。安全功能所要求的结构和内容以及保障方面应定义在卖主和终端用户的指南中。

在IT产品的许多方面已经有多种SDoC机制，而且SDoC在欧洲的电磁兼容(Electromagnetic Compatibility，EMC)以及低压指令(Low Voltage Directive，LVD)产品已经强制执行。不过，对于其他

的情形，比如 ISO 9000，软件质量，人体工程学，环境保护，德国安全认证标志等，SDoC 则是自愿的。

安全一致性方面的声明至今还未得到考虑；不过，大多数的供应者都在为最终用户所未见的安全功能方面进行了大量的规范、设计、测试/保障、以及文档工作，而其他的则只进行了最低限度的测试。供应者对于安全方面充分的声明将会增加终端用户选择可信任产品的透明性和可比性。

而且，SDoC 的 IT 安全一致性声明使得供应者和最终用户更加关注 IT 安全。受“进入市场的时间(time to market)”的驱动，现在比过去已经有更多的商业实体，而这将在成本更优和自愿的基础上进一步提高 IT 产品的安全。

相关的 ISO/IEC 标准规定了支持文档的框架的一般准则。正如 ISO/IEC 17050 定义的，利用支持文档可以加强、促进以及提高供应者一致性声明的确信度。

6.24.3 源

参考文献目录：

ISO/IEC 17024　一致性评定　对个人进行认证操作的组织的一般要求；

ISO/IEC 17025　实验室测试及校准能力的一般要求；

ISO/IEC 17050-1　一致性评定　供应者一致性声明　第一部分：一般要求。

注：SDoC 是以下委员会的产品：

ISO/CASCO WG 24　一致性评定声明　供应商一致性声明及其支持文档。

6.25 SA-CMM® 软件需求能力成熟度模型®

		T	

6.25.1 目的

基准化和改进软件需求过程。

6.25.2 描述

软件需求能力成熟度模型®(Software Acquisition Capability Maturity Model®，SA-CMM®)用于基准化和改进软件需求过程。该模型与软件能力成熟度模型(Capability Maturity Model for Software，SW-CMM)具有相同的体系结构，但是其特别强调需求问题以及负责规划和管理软件需求支出的个人与团体的需求。每一个成熟度水平表明一个需求过程的能力，并且一个成熟度水平有多个关键过程领域(Key Process Areas，KPAs)见表 3。每一个 KPA 都有其目的、一般的特征和组织惯例，这些特征和组织习惯可以用来制度化一般的惯例。在国防部(Department of Defense，DOD)与其他的联邦机构、SEI、工业界、以及需求专家的共同努力下，这些组织最早开发、样品测试、规划了 SA-CMM 的实施。由于近期陆军、海军、空军、以及其他的联邦机构对软件需求过程建模进行了大量的工作，该软件能力成熟度模型组合了这些工作最好的部分，对这些工作进行了提炼，并采用已确立的 SW-CMM 作为体系结构模型。

表 3 SA-CMM® 关键过程领域

水　平	集中关注点	关键过程领域
5　优化的	连续过程改进	需求创新管理 连续过程改进
4　数量化的	数量化管理	数量化的需求管理 数量化的过程管理

表 3（续）

水　平	集中关注点	关键过程领域
3　定义的	过程标准化	培训程序 需求风险管理 合同执行管理 项目执行管理 用户要求 过程定义和维护
2　可重复的	基本项目管理	转换到支持 评估 合同跟踪和监视 项目管理 要求订立和管理 请求 软件需求规划
1　初始的	胜任的人员	

6.25.3　源

参考文献目录：

[38]　软件需求能力成熟度模型®(SA-CMM®)，版本 1.03。

注：SA-CMM®是软件工程协会(Software Engineering Institute)的产品。

可以通过下面的网址访问该协会：http://www.sei.cmu.edu。

6.26　ISO 9000 系列　质量管理

6.26.1　目的

为组织提供质量管理框架并对其成功实施质量管理进行认证。

6.26.2　描述

ISO 9000 是一个质量保障标准，其包括了 20 个高水平保障的条款，一个组织在取得 ISO 9000 登记之前应当满足这些要求。ISO 9000 最初为制造业组织设计，其也适用于软件开发组织，不过要求进行许多解释。因此，增加了 ISO 9000-3 指南，它是 ISO 9001 关于软件开发、供应和维护的指南，用于解决应用 ISO 9001 于软件的困惑和困难。ISO 9000-3 包括 22 个条款，明确针对软件开发；并且这 22 条与 ISO 9001 的 20 个条款相对应。尽管 ISO 9000-3 的条款更具体地针对软件，这些条款经进一步解释能足够地适用于组织，不过这些条款未涉及信息技术安全。应注意，ISO 9000-3 指南仅限制于软件；而 ISO 9001 和 CC 在适用于软件产品和系统之外还适用于硬件。

ISO 9000 的符合性，通过独立的审核人员检查一个组织的质量手册和过程，并对职员的面试来实现。ISO 9000 认证只授予合适的组织，比如一个公司。这有别于 ISO/IEC 21827(SSE-CMM)，ISO/IEC 21827 可以对一个公司或一个组织内的单立的小组或项目进行评价。

ISO 9001 比 CC 的要求涵括了更大的范围，从概念到产品的退役。这意味着，把 ISO 9001 登记看

成为一个节省评估时间的途径的组织必须实现一个质量体系，该体系比 CC 评估涵盖更多的领域。为取得 ISO 9001 的这部分额外的工作可以不作证明。

重要的是要注意到 ISO 9000-3 只是指导，组织必须满足 ISO 9001 要求以实现登记。

6.26.3 源

参考第 2 章：ISO 9000；ISO 9001；ISO/IEC 90003(ISO 9000-3 的修订版)。

注 1：ISO 9000 和 ISO 9001 是委员会 ISO TC 176 质量管理和质量保障及以下分会的产品：

ISO TC 176/SC 1 质量管理和质量保障 概念和术语；

ISO TC 176/SC 2 质量管理和质量保障 质量体系；

ISO TC 176/SC 3 质量管理和质量保障 支援技术。

注 2：ISO/IEC 90003 是以下委员会的产品：

ISO/IEC JTC 1/SC 7/WG 18 信息技术 软件和系统工程 质量管理。

6.27 ISO 13407 以人为中心的设计(HCD)

D			

6.27.1 目的

通过以人为中的设计，取得更可使用的、可培训的、可支持的产品，以减少与系统运作相关联的安全风险。

6.27.2 描述

交互系统的 ISO 13407 以人为中心的设计过程是由 ISO TC 159/SC 4/WG 6 制定的标准，其解释了通过使交互系统生存周期更加以人为中心所能获得的好处，并揭示了使生存周期以人为中心所要求的过程。该标准中的以人为中心的生存周期过程模型是 ISO 13407 中描述的以人为中心过程的结构化和正规化定义。ISO 13407 适用于软件过程评价和改进的专家以及那些熟悉或参与过程建模的人员。

该文档中叙述的模型采用了过程评价模型中的通用格式。这些模型描述了一个组织应当执行以实现既定技术目标的过程。模型中的这些过程按照 ISO 15504 软件过程评价所定义的格式进行描述。尽管采用过程评价模型的主要目的是为了度量一个组织多好地执行了模型所涵盖的过程，这些模型还能用于描述什么是设计和发展有效的组织和工程过程所要求的。

基于 ISO 13407 的可用成熟模型 UMM 描述了 7 个过程，每一个均由一组基本的惯例定义。该文档定义了基本的惯例。对于每一个过程都给定了一组工作产品。在 ISO/IEC 15504 中，提供了一个对 ISO/IEC 15504 的评价过程成熟度的总结，还列出了采用模型的概要，提供了一个记录表格，并描述了如何使用该表格，提供了如何把基本准则映射到 SPICE、CMM 和 SE-CMM 中的过程。ISO 13407 的过程模型与 ISO/IEC 15504 的一致。

就系统和软件开发人员而言，采用以人为中的方法能提供一个更可使用的、可培训的和可支持的产品，并具有更大的客户满意度。以人为中心的设计可减少系统运作相关联的风险。以人为中心的设计在生存周期的早期阶段要求更多的投资，但是人们已经发现其不仅减少了服务成本还减少了开发成本。以人为中的过程尤其减少了不可预测的要求改变并减少了返工和安装风险。

以人为中心的方法的目的是提醒开发人员和交互系统的所有者，系统是用于使用而不仅仅是交付和购买。以人为中的过程允许开发人员和所有者分析系统运行时将会如何表现，并可以度量系统的质量和使用的保障。以人为中的过程考虑了使用的环境，即交互系统使用的整个环境。以人为中心的过程涉及了采用软件和硬件部件的整个系统。以人为中心的系统给用户权利，激发用户学习，其益处包括产量的增加、产品质量的提升、支持和培训的减少以及运行保障的提升。

6.27.3 源

参考第 2 章:ISO/IEC 15504-1。

参考文献目录:

ISO 13407 交互系统的以人为中心的设计过程。

注:ISO 13407 是以下委员会的产品:

ISO TC 159/SC 4/WG 6 人类工程学 人-系统交互的人类工程学 交互系统的以人为中心的设计过程。

6.28 开发者良源(一般情况)

D			

6.28.1 目的

应用先前的经验和成功的等级作为安全软件的质量的指示。

6.28.2 描述

系谱是一种确定证据的可接受程度的方法,该方法基于对证据的创建者的识别,即个人/组织已经具有开发、维护、运行或审查安全产品和系统的成功的等级(比如,跟踪记录)。系谱可基于个人的识别或基于创建证据的组织。而且,系谱可基于个人/组织的角色分类为创建者、评估者或证明者。

系谱可在 IT 安全社区内得到正式化。不管是否得到正式化,系谱是目前正在使用信息的一个渠道,虽然是一种更不正式的"信任"基础,因为许多产品/系统的选择是基于产品/系统的开发者或集成者来进行的。

在一些地方,要进行严肃的考虑的是开发者的保障。这涉及开发者进行内部测试和评价,并基于公司内部程序做出一些保障声明。开发者的保障分数不能给出与独立的第三方的测试一样水平的保障,但是一些组织认为确定一种机制承认可信任的开发者能够满足许多商业要求。

6.28.3 源

参考文献目录:[43]

注:"开发者系谱"的正式定义出现在以下的过程保障方法中:例如 CMM(6.21),ISO/IEC 15504(6.20),人员认证(6.36 和 6.37)和提供方符合性声明(6.24)。

6.29 ISO/IEC 17025 鉴定保障

D	I		

6.29.1 目的

鉴定保障的目的是确保所有评估过程和结果的一致性,以符合相关标准并确保客观和中立。

6.29.2 描述

确保所有评估过程和结果的一致性、遵照相关标准和确保客观和中立,这些组成了鉴定保障的基础。鉴定保障过程要求评估人员提供与条件和资格要求的符合性证明。

根据 ISO/IEC 17025,鉴定的要求如下:

1) 与 ISO/IEC 17025 相关部分的符合性(包括胜任整个 IT 安全领域的证据);

2) 经证明在技术上胜任评估的一个具体领域(如果适用,多个领域)。

因此，鉴定过程由基本鉴定(符合条款 1 的要求)和至少一个许可过程(符合条款 2 的要求)组成。鉴定还可以通过额外的评估领域的许可过程进行增补见表 4。

表 4　鉴定过程

许可领域 1	许可领域 2	许可领域 3
与 ISO/IEC 17025 一致的基本鉴定		

在受鉴定方和操作者的鉴定协议的授权下，自然个人或合法个人可进行评估设施的操作；前提条件是，这些评估设施不参与待评估产品的开发、制造或市场。因此，原则上，这不排除鉴定所谓的卖主实验室的可能。

作为鉴定过程的基础，欧洲标准 ISO/IEC 17025 规范了测试实验室(包括校准实验室，不管参与的部门)的技术能力的一般准则。它用于测试实验室及其鉴定团体，并可用于其他相关团体认可测试实验室的能力。这一组准则在应用于 IT 特定的安全部门需要进行增补。

注：应按照 15408 共同准则，应用满足 ISO/IEC 17025 的且经鉴定的和许可的评估设施，进行独立的第三方评估。

6.29.3　源

参考文献目录：

ISO/IEC 17024　一致性评估　对个人实施认证机制的一般要求；

ISO/IEC 17025　测试和校准实验室的能力的一般要求。

注：ISO 13407 是以下委员会的产品：

ISO/CASCO WG 24　一致性评价委员会　评价和鉴定。

6.30　ISO/IEC 13335　信息和通信技术安全管理(MICTS)

	I	T	O

6.30.1　目的

为管理提供评价和管理安全风险的一般指导。

6.30.2　描述

信息和通信技术安全管理(MICTS)ISO/IEC 13335 由一系列的标准和标准组成，为信息和通信技术(ICT)安全的管理给出了指导，而不是解决方法。在组织内部负责 ICT 安全的个人能采用 ISO/IEC 13335 中的材料来满足他们的具体要求。ISO/IEC 13335 的主要目的是：

1)　定义和描述与 ICT 安全管理相关的概念；

2)　确定 ICT 安全管理和一般的 ICT 管理的关系；

3)　给出若干个可用于解释 ICT 安全的模型；以及

4)　提供 ICT 安全管理的一般指导。

MICTS 描述了风险评价和风险管理背后的基本概念，包括基本术语以及评价和管理风险的整体过程。

MICTS 的制定可用于整体地管理信息安全问题，处理诸如技术的、实体的、过程的和管理的控制等问题。MICTS 不仅为辅助组织开发和改进其信息安全体系结构提供基础，它还着眼于组织间建立共同性。

MICTS 为管理 IT 安全提供了一个框架。它讨论了信息技术安全管理的高层次概念，并介绍风险分析和管理的一般要求和技术。风险管理过程定义在 MICTS 的第 2 部分，它要求实施合适的控制，并

且建议从一些标准中选择具体的控制方法，比如从 ISO/IEC 17799 或 IT 基线保护指南中选择控制方法。

MICTS 目前正处于修订的过程中，而且其中的部分将从标准中转变为国际标准。一旦该过程完成，MICTS 将冠名为“信息和通信技术安全管理(Management of information and communications technology security)”，包括如下的部分：

第 1 部分：信息和通信技术安全管理的概念和模型；

第 2 部分：信息和通信技术安全风险管理技术。

ISO/IEC 13335 的第 1 部分(2004)将代替目前的 ISO/IEC TR 13335 第 1 部分(1996)和第 2 部分(1997)，它也包括了 ISO/IEC TR 13335 第 5 部分(2001)。

ISO/IEC 13335 的第 2 部分将代替目前的 ISO/IEC TR 13335 第 3 部分(1998)和第 4 部分(2000)。

ISO/IEC TR 13335 的下面部分将保留，并且冠名为“信息技术安全管理指南”(Guidelines for the management of information technology security)：

第 3 部分：信息技术安全管理技术；

第 4 部分：安全措施的选择；

第 5 部分：网络安全管理指导。

6.30.3 源

参考第 2 章：ISO/IEC 13335-1；ISO/IEC TR 13335-2；ISO/IEC TR 13335-3；ISO/IEC TR 13335-4；ISO/IEC TR 13335-5；ISO/IEC 17799。

参考文献目录：

[33] 信息技术基础保护手册。

注 1：ISO/IEC 13335 是以下委员会的产品：

ISO/IEC JTC 1/SC 27/WG 1 信息技术 安全技术 要求 安全服务和指南

注 2：在本标准发布之时，ISO/IEC 13335 正处于大幅的修订，包括结构调整和名称的改变。原先冠名为“信息技术安全管理指南”，ISO/IEC 13335 现在的名称为“信息和通信技术安全管理”，缩写为“MICTS”。

6.31 BS 7799-2 信息安全管理系统 规格说明与使用指导

			O

6.31.1 目的

确立创建和管理一个有效的信息安全管理系统(Information Security Management System，ISMS)的要求。

6.31.2 描述

BS 7799-2 详细叙述了实施 BS 7799-1 中确立的“安全控制”所需的要求。根据一个公司的部分或全部的需求，可对 BS 7799-1 进行定制。BS 7799-2 与 BS 7799-1 一起，清楚地说明了定义、实施、运行、文档撰写、监视、审查、维护和改进信息安全管理系统(ISMS)的要求。

BS 7799-2 考虑了组织的整体商业风险，定义了充分且合适的安全控制以保护信息财产，并给顾客和利益方带来确信度。这可以维护和增进一个组织的竞争力度、现金流、利润、合法性和商业前景。

为此目的，一个组织必须确定和管理它的许多活动，以有效地运作。任何一组利用资源的活动都可以视为一个过程，都应当进行管理。一个过程把输入转化为结果。一个过程的结果经常形成为下一个过程的输入。

在一个组织内部应用系统的过程，确定这些过程以及这些过程的互动，包括这些过程的管理，统称

为“过程方法”。BS 7799-2 采用过程方法，鼓励它的用户强调下面条款的重要性：

a) 理解商业信息安全要求以及确立信息安全政策和目标的需求；

b) 在一个组织的整体商业风险环境下实施和运作控制；

c) 监视和审查 ISMS 的性能和有效性；

d) 基于目标度量的连续改进。

BS 7799-2 的根本过程模型是“计划-实行-检查-纠正(PDCA)”模型，它考虑了确立、实施、操作、监视、维护和改进组织 ISMS 的有效性等方面。

6.31.3 源

参考文献目录：

[53] BS 7799-2:2002 信息安全管理系统 规范及应用指导。

注 1：BS 7799-2 是英国标准协会(British Standards Institution BSI)的产品。

可以通过以下网址联系 BSI:www.bsi-global.com。

注 2：BS 7799-2 在新西兰和澳大利亚发布为国内标准：AS/NZS 7799-2:2003，参考(www.standards.com.au)。

6.32 ISO/IEC 17799 信息安全管理实践指南

			O

6.32.1 目的

给出一个框架，典型地在组织水平上，使得公司能开发、实施和度量有效的安全管理惯例。

6.32.2 描述

ISO/IEC 17799 是一个关于信息安全管理的最佳实践的国际标准。在被 ISO 和 IEC 通过公开可用规范快速跟踪过程(Publicly Available Specification fast-track process)采纳之前，它最早是英国标准 BS 7799。它最初的制定，是为了响应工业界、政府和商业对一个共同框架的需求，因为共同的框架使得公司能够开发、实施和度量有效的安全管理实践，还为公司之间的贸易带来确信度。基于领先的英国的和国际的商业的最佳信息安全惯例，该标准受到了国际上的广泛赞誉。

ISO/IEC 17799 是优良的信息安全管理的实践指南。相关的 BS 7799-2:1999 标准是信息安全管理规范，它用于管理系统要求规范，依据该规范可对组织进行符合性评价以及后续的认证。BS 7799-2 已经在其他国家也作为国内标准进行发布。

ISO/IEC 17799 适用于任何信息，不论信息所储存或传输的媒介或信息所处的位置。每一个企业都需要一个系统，以系统的方式管理它的信息风险，而该标准给出了可用的最佳控制的指导。为了确保整个过程的价值，十分重要的是要利用风险评价过程选择合适的控制和目标，并且运用正确水平的控制。下面列出在 ISO/IEC 17799 中定义的控制，它们定义工业界优良的安全实践的基线，且被广为接受：

——信息安全政策；

——安全组织；

——财产分类和控制；

——个人安全；

——物理的和环境安全；

——计算机和网络管理；

——系统访问控制；

——系统开发和维护；

——商业连续性规划；

——符合性。

6.32.3 源

参考第 2 章:ISO/IEC 17799。

参考文献目录:

[53] BS 7799-2:2002 信息安全管理系统 规范及应用指导。

注:ISO/IEC 17799 是以下委员会的产品:

ISO/IEC JTC 1/SC 27/WG 1 信息技术 安全技术 要求、安全服务和指南。

6.33 FR 缺陷补救(一般性)

			O

6.33.1 目的

当产品在部署或运行时,获得有利的瑕疵/缺陷信息并进行补救。

6.33.2 描述

当产品在部署或运行时,瑕疵和缺陷将会引发信息系统的故障和/或遭到攻击。在这个阶段必须进行若干的活动:

——操作人员必须使系统处于安全状态,比如采用故障入侵检测系统,用最新的补丁进行更新,或通过临时限制系统的功能。

——操作人员必须向适当的地方汇报遭到的攻击和缺陷,比如,开发人员,急救中心、管理员、用户。

——开发人员必须为产品和系统提供后盾,为所有潜在的相关用户提供迅速有效的咨询,开发和发布补丁以补救安全瑕疵/缺陷。应当使用一个安全的软件分发系统。

所有的职责都应当正规化,比如,开发人员对产品和服务的承诺,及时地纠正程序缺陷,解决用户的问题以及承诺一旦某一个使用问题得到解决将为所有的用户发布补丁。

缺陷补救通常认为是独立于评估等级维护(Evaluation Rating Maintenance)的。

补丁是纠正软件错误和缺陷的程序,是一种最常用的堵塞已知的安全缺陷的方法。不过,安装卖主提供的安全补丁不是一个完美的安全解决方法:

——首先,频繁的补丁将迅速地使管理员不知所措,因为他们还肩负其他的管理任务。

——其次,即使组织安装了所有最新的补丁,一些新的攻击还可能继续,比如通过因特网。

——当一个新的缺陷被发现并公布在因特网上,在新的补丁发布和安装之前,大量的网络将马上变得极其脆弱。在一个有效的补丁准备好以对抗新的攻击之前,几个星期或几个月可能已经过去,这使得服务器为攻击大开方便之门。

——组织机构能通过监视关于威胁或常见攻击的安全咨询,了解对新补丁需要。这些安全咨询由不同的组织提出,通常意味着需要一个补丁或解决方案来弥补被发现的弱点。

——缺陷修复活动通常包含在方法内,例如 ISO/IEC 15408 或者 CMM。

6.33.3 源

注:安全咨询的来源是卡耐基·梅隆紧急响应团队(Carnegie Mellon Emergency Response Team),访问网址是 http://www.cert.org。

注:对特定的用户组,特定的来源可能存在,比如美国联邦政府的访问网址是:http://www.us-cert.gov/federal/。

6.34 IT 基线保护指南

6.34.1 目的

为在一般组织机构的 IT 系统提供一组实用的安全方法,使 IT 系统足够地和充分地满足保护要

求，并且这些要求能升级为更高的保护要求。

6.34.2 描述

通过合适地应用组织的、人事的、基础结构的及技术的标准安全方法，IT 基线保护可用于使 IT 系统达到一个安全水平，使得 IT 系统能足够地和充分地满足一般组织的保护要求，并且可作为要求较高保护程度的 IT 应用的基础。因此，IT 基线保护指南(IT Baseline Protection Manual)推荐把要素编入典型的 IT 配置、威胁环境和组织设置的安全措施组件中。

为准备该指南，德国信息安全机构(German Information Security Agency, Bundesamt für Sicherheit in der Informations technik-BSI)基于通常公用的威胁和弱点所假定风险场景；为对抗这些威胁，制定了一组结构化的方法，这些方法经常地更新。因此，用户只需要确信受推荐的方法是一致的并且充分地实施了。由于实施过程以一种核对表的方式进行组织，这使得能够以一种经济的方式实现一般 IT 安全保护要求。

组织的系统安全政策可能引用 IT 基线保护指南的一般方法，因此，IT 基线保护成为满足一般保护要求的方法的协议基础。

然而，被基线保护所采用的一般途径不能立即应用于要求高水平保障的 IT 系统。因此原则上，在要求高水平保护的 IT 应用中，必须确信在执行 IT 基线保护的基础上还进行了独立的安全分析。这将在 IT 基线保护方法之外，为选择和(或)制定额外的或质量上更有效的方法带来更具体的结果。而这带来了成本/有效性比值方面的上升。

为了实现全面的 IT 基线保护，只进行一次系统安全政策的制定是不够的，即使是基于 IT 基线保护指南。相反地，要求循环地设计、实施和监视 IT 安全方法，并且这些过程可能为安全漏洞所触发。这个任务具有基本的重要性，必须由机构/公司的管理层发起。为了支持这个任务，指南提出了一个行动方案。

6.34.3 源

参考文献目录：

[33] 信息技术基础保护手册。

注：信息技术基础保护手册是德国信息安全机构 BSI 的产品。

可以通过以下网址访问 BSI：http://www.bsi.bund.de/english/index.htm。

6.35 渗透测试

			⇒O⇒

6.35.1 目的

通过尝试克服安全措施来测试已实施的安全功能的有效性。

6.35.2 描述

渗透测试用于分析安全功能的有效性。渗透测试在成功地完成正确性测试之后进行。渗透测试涉及了产品正确但仍不安全的问题。

渗透测试的目的是检测产品的弱点。弱点又可划分成为构造性弱点和操作性弱点。可能的弱点是恶意部分或者隐蔽渠道。弱点可能立即出现在启动时或者出现在后期被特殊的输入所激发行动时。后面这种情形使具有良好规划的系统在运行时的任何时候都可能遭到攻击。弱点可能是在一般运行时不执行且在正确性测试时不能被触及的隐藏装置、功能、模块或库等。产品中所有的这些的部分都应当标记为潜在危险的。大多数弱点由稀少的和不可预知的(大多是隐秘的)输入激发。

应基于产品的安全分析来规范渗透测试计划和渗透测试过程。安全分析是对弱点的确认但未进行渗透测试。测试计划规范了测试过程应当包括的攻击。攻击是对弱点的尝试利用。渗透测试即是绕开产品安全特征的尝试。渗透即成功地利用了弱点。

渗透测试中的黑箱策略即是特洛伊木马检测、关键性输入产生和断言监视。关键性输入的产生策略包括输入流的截取,输入缓冲溢出、在输入中附加垃圾、输入恶意命令及张力测试。白箱策略即是对粗劣说明的、过时的和没有文档的代码覆盖,错误注入和基于代码的断言的监视。

6.35.3 源

参考文献目录:

[49] 入侵检测技术实践。

6.36 人员认证(与安全无关)

			O

6.36.1 目的

确保职员在系统运行阶段能够完成其任务。

6.36.2 描述

人员认证是提供人才保障和人才保障维护的组织管理过程(也即提供并保障持续的认证教育)。

人员认证包含保障可应用的 ICT 教育、资格和经验,还包括保障身体能力,心理稳定性和个人的廉正。在 ICT 操作中,尤其需要考虑安全因素。ICT 安全领域的经历对认证是一个补充并且可以代替其中的部分。

现在有多种 ICT 认证,它们在 ICT 系统中可以提供一定程度的安全保障。

ICT 认证的职员,他们的雇主,同事和客户普遍反映他们的能力和创造力有了提高。另一方面,认证能够提供额外的 ICT 可信度,这也有助于职员的事业发展。

ICT 认证可以由以下人员管理:

——关注 ICT 操作需求的雇主;

——关注 ICT 产品和服务的制造商;

——关注市场或顾客需求的第三方。

注:人员认证的国际标准在其他技术领域已经存在,但在 ICT 领域还没有被广泛引入。

大型企业和政府可能有许多内部的 ICT 认证标准,这些标准可能建立在职员手册的应用部分。

由于大型企业的广泛推广,ICT 产品认证已经成为计算机行业衡量开发能力的标准,认为有这些标准的人是专业人员。例如:

——MCSE(微软认证系统工程师);

——ODBA(甲骨文数据库管理员);

——CNA(网威认证管理员);

——CNE(网威认证工程师);

——Cisco Certification(思科认证)。

在技术快速发展的领域,第三方的 ICT 认证已经成为一种新的教育方式,它授予证书而非学位。这种教育手段在不为政府注意或控制下挑战着高等教育。一项调查显示,在 ICT 领域,80%的就业条款上包含教育要求而非大学学历。

第三方 ICT 认证的目标是跟进和确保特定领域最新的知识和技术,许多评估或认证机构及它们的认证都是国际通用的。

第三方提供的 ICT 认证有：

——A+®认证(美国计算机行业协会 CompTIA)；

——计算机专业人员认证机构；

——全国通信系统工程师协会。

下面，以计算机科技行业相关的 A+®认证作为 ICT 认证的一个例子来进行说明。

A+®认证需要通过两个考试，这些考试用来衡量是入门级别的 IT 专业人员还是有超过 500 个小时实际经验的 IT 服务技术人员：

——A+“核心硬件”考试：侧重于和 Intel 兼容的电脑硬件上的操作，包括：

- 1.0 操作系统基础；
- 2.0 安装，配置和升级；
- 3.0 诊断和故障排除；
- 4.0 网络。

——A+“操作系统技术”考试：侧重在微软 DOS/Windows 环境下的操作，包括：

- 1.0 安装，配置和升级；
- 2.0 诊断和故障排除；
- 3.0 预防维护；
- 4.0 主板/处理器/内存；
- 5.0 打印机；
- 6.0 基本网络。

——培训材料用于学习和考试的参考。

6.36.3 源

认证信息和认证服务可以从证书的发起者和管理者那里获取。

注：美国计算机行业协会(CompTIA)总部在美国，在澳大利亚、新西兰、比荷卢、加拿大、日本、新加坡、南非、英国和斯堪的纳维亚均设有分部。

可以通过以下的网址联系 CompTIA：http://www.comptia.org/。

6.37 人员认证(与安全有关)

D	I	T	O

6.37.1 目的

通过认证管理员、操作员和审计人员保障运行安全。

6.37.2 描述

ICT 安全人员认证是人员认证(参阅 6.36)的一个特定方面，它保证了职员的安全意识。安全人员认证确保职员接受如下要求的安全教育和培训：

——提供必要的知识和信息，使得具有安全功能的质量性能；

——增进对信息安全程序政策和要求以及信息安全程序对国家安全的重要性的理解；

——灌注和维持对安全要求和知识威胁的持续的理解；

——辅助提升职员支持程序目标的较高程度的动机。

现在有许多安全认证提供不同程度的安全保障，包括：

——注册信息安全经理(CISM)™；

——系统安全认证专员(SSCP)™；

——注册信息系统审计师(CISA)™；

——安全专家认证(CPP)；
——DoD CIO 认证程序(包括安全和保障胜任)；
——全球信息保障认证(GIAC)信息安全初步；
——全球信息保障认证(GIAC)水平一　安全初步；
——全球信息保障认证(GIAC)水平二　对象领域模块；
——全球信息保障认证(GIAC)安全工程师。

下面,以 CISSP 作为安全认证的例子进行说明。

CISSP 认证用于认可对信息安全国际标准的理解和公共知识体系(Common Body of Knowledge, CBK)的理解。认证可以提升专业人员的职业并提供增强的信息安全声誉。

CISSP 认证考试由 250 个多项选择问题组成。投考者有 6 个小时来完成考试。考试涵括了关于共同知识体系的 CISSP 信息系统安全的 10 个领域：

——访问控制系统和方法；
——应用程序和系统开发；
——事业延续性规划；
——加密；
——法律、调查和道德规范；
——运作安全；
——物理安全；
——安全框架和模型；
——安全管理准则；
——电信、网络和因特网安全。

6.37.3　源

认证信息和认证服务可以从证书的发起者和管理者那里获取。

注：CISSP 是国际信息系统安全认证联盟[(ISC)2]颁发的证书。
可以通过以下网址访问(ISC)2：https://www.isc2.org/。

参 考 文 献

[1] ISO/IEC TR 9126-2 Software engineering—Product quality—Part 2:External metrics

[2] ISO/IEC TR 9126-3 Software engineering—Product quality—Part 3:Internal metrics

[3] ISO/IEC TR 9126-4 Software engineering—Product quality—Part 4:Quality in use metrics

[4] ISO 13407 Human-centred design processes for interactive systems

[5] ISO/IEC 14598-2 Software engineering—Product evaluation—Part 2:Planning and management

[6] ISO/IEC 14598-3 Software engineering—Product evaluation—Part 3:Process for developers

[7] ISO/IEC 14598-4 Software engineering—Product evaluation—Part 4:Process for acquirers

[8] ISO/IEC 14598-5 Information technology—Software product evaluation—Part 5:Process for evaluators

[9] ISO/IEC 14598-6 Software engineering—Product evaluation—Part 6:Documentation of evaluation modules

[10] ISO/IEC TR 15271 Information technology—Guide for ISO/IEC 12207

[11] ISO/IEC 17024 Conformity assessment—General requirements for bodies operating certification of persons

[12] ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories

Note: EN ISO 17025 is identical to CEN/CENELEC EN ISO 17025

Note:ISO/IEC 17025 replaces ISO Guide 25 and CEN/CENELEC EN 45001

[13] ISO/IEC 17050-1 Conformity assessment—Supplier's declaration of conformity—Part 1:General requirements

[14] ISO/IEC 17050-2 Conformity assessment—Supplier's declaration of conformity—Part 2:Supporting documentation

[15] ISO/IEC TR 19760 Systems engineering—Guide for ISO/IEC 15288(System Life Cycle Processes)

[16] ISO/IEC 25000 Software Engineering—Software Product Quality Requirements and Evaluation (SQuaRE)—Guide to SquaRE(presently FCD)

[17] ISO/IEC 25020 Software and System Engineering—Software quality requirements and evaluation (SQuaRE)—Quality measurement—Measurement reference model and guide(presently CD)

[18] ISO/IEC 25021 Software and System Engineering—Software Product Quality Requirements and Evaluation(SQuaRE)—Measurement Primitives(presently CD)

[19] ISO/IEC 25030 Software engineering—Software quality requirements and evaluation (SQuaRE)—Quality requirements(presently CD)

[20] SCT.Strict Conformance Testing NPL Report,March 1997.(National Physical Laboratory, Teddington,Middlesex TW11 OLW,UK)

[21] A Systems Engineering Capability Maturity Model(SE-CMM Model),Version 1.1 (CMU/SEI-95-MM-003),November 1995.Software Engineering Institute,Carnegie Mellon University,Pittsburgh,PA 15213-3890,USA

Note:The model may be available as

http://www.sei.cmu.edu/pub/documents/95.reports/pdf/mm003.95.pdf

[22] A Description of the Systems Engineering Capability Maturity Model Appraisal Method (SE-CMM Method), Version 1.1 A (CMU/SEI-96-HB-004), March 1996. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA

Note: The model may be available as

http://www.sei.cmu.edu/pub/documents/96.reports/pdf/hb004.96.pdf

[23] Capability Maturity Model® for Software (SW-CMM®) v1.1 National Technical Information Service (NTIS), US Department of Commerce, Springfield, VA 22161, USA

[24] System Security Engineering Capability Maturity Model, Model Description (SSE-CMM Model), Version 2.0 April 1, 1999 ISSEA, 13873 Park Center Road, Suite 200, Herndon, VA 20171, USA.

Note: The latest version is available at http://www.sse-cmm.org/model/model.asp

[25] System Security Engineering Capability Maturity Model, Appraisal Methodology (SSE-CMM Method), Version 2.0 April 16, 1999. ISSEA, 13873 Park Center Road, Suite 200, Herndon, VA 20171, USA.

Note: The latest version is available at http://www.sse-cmm.org/org/org.asp

[26] Trusted Capability Maturity Model, Version 2.0 NSA, June 20, 1996 (unreleased US Government document)

[27] A Tailoring of the CMM for the Trusted Software Domain Kitson, David H in Proceedings of the Seventh Annual Software Technology Conference. Salt Lake City, Utah, April 9-14, 1995

[28] Trust Technology Assessment Program (TTAP)

Note: Information may be available at http://www.radium.ncsc.mil/tpep/ttap/index.html

[29] Trusted Software Methodology (volumes 1 and 2) SDI-S-SD-91-000007, June 17, 1992. US Dept. of Defense, Strategic Defense Initiative Organization, Washington, D.C.

[30] Practical Guide to the Open Brand Ref. X981. The Open Group, 44 Montgomery, Street, Suite 960, San Francisco, CA 94104-4704, USA

Note: The guide may be available as http://www.opengroup.org/publications/catalog/x981.htm

[31] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0 (NITSM 8/93 and CID 09/19), 1993. Communications Security Establishment, P.O. Box 9703, Terminal, Ottawa, Ontario K1G 3Z4, Canada

[32] Rating Maintenance Phase Program (RAMP), Doc Vers. 2, 1995 NCSC-TG-013-95, Library No. S-242,047, National Computer Security Center (NCSC), 9800 Savage Road, Fort George G. Meade, Maryland 20755-6000, USA

Note: The document may be available as http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-013.2.html

[33] IT Baseline Protection Manual ISBN 3-88784-915-9. Bundesanzeiger-Verlag, Postfach 10 05 34, 50455 Koln, Germany.

Note: Up-to-date versions of this manual may also be available on-line at http://www.bsi.bund.de/english/index.htm

[34] Capability Maturity Model for Software CMU/SEI-91-TR-24, August 1991, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890.

Note: The document may be available as http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr24.93.pdf

[35] Capability Maturity Model® Integration for the systems engineering and software engi-

neering integrated model, CMMI-SE/SW Version 1.1 Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890.

Note: The document may be available as http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02tr001.pdf

[36] CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development, Version 1.1, Staged Representation CMMI-SE/SW/IPPD, V1.1, Staged, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890.

Note: The document may be available as http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02tr004.pdf

[37] CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Staged Representation CMMI-SE/SW/IPPD/SS, V1.1, Staged, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.

Note: The document may be available as http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02tr011.pdf.

[38] Software Acquisition Capability Maturity Model® (SA-CMM®), Version 1.03 March 2002. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.

Note: The document may be available as http://www.sei.cmu.edu/publications/documents/02.reports/02tr010.html

[39] X/Open Baseline Security Services(XBSS) Document Number C529, ISBN 1-85912-136-5, December 1995. The Open Group, 44 Montgomery, Street, Suite 960, San Francisco, CA 94104-4704, USA.

Note: The document may be available at http://www.opengroup.org/publications/catalog/c529.htm

[40] Information Technology Security Evaluation Criteria (ITSEC), version 1.2 Office for Official Publications of the EC, June 1991. Document may be obtained by: http://www.cordis.lu/infosec/src/crit.htm

[41] Information Technology Security Evaluation Manual(ITSEM), version 1.0 Office for Official Publications of the EC, September 1993. Document may be obtained by: http://www.cordis.lu/infosec/src/crit.htm

[42] V-Model—Development Standard for IT Systems, VM 1997 IABG, Einsteinstraße 20, D-85521 Ottobrunn, Germany. Document may be obtained by: http://www.v-modell.iabg.de/ENGL

[43] A Head Start on Assurance in Proceedings of an Invitational Workshop on Information Technology(IT) Assurance and Trustworthiness, March 21-23, 1994, NISTIR 5472. National Security Agency, 9800 Savage Road, Suite 6740, Ft. Meade, MD 20755-7640, USA.

[44] UK Certificate Maintenance Scheme, Issue 1.0 31 July 1996, Certification Body, PO Box 152, Cheltenham, Glos GL52 5UF, UK.

Note: The document may be available as http://www.cesg.gov.uk/site/iacs/itsec/media/formal-docs/uksp16p2.pdf

[45] Trusted Computer System Evaluation Criteria(TCSEC), 1985 DOD 5200.28-STD, Library No. S225, 711, US Dept. of Defense. Document may be obtained by: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html.

[46] Trusted Product Evaluation Program(TPEP) Information may be obtained by: http://www.radium.ncsc.mil/tpep/process/procedures.html

[47] A Trusted Software Development Methodology J.Watson and E.Amoroso, in Proc.13th Natl.Computer Security Conf, Oct.1990, pp.717-727.

[48] Insider Threat Mitigation Report in Final Report of the Insider Threat Integrated Process Team, IPT April 24, 2000.Insider Threat Integrated Process Team, Department of Defense, USA.

[49] State of the Practice of Intrusion Detection Technologies CMU/SEI-99-TR-028 ESC-TR-99-028, January 2000. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.

Note: The document may be available as http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf

[50] Korea Information Security Evaluation Criteria(KISEC) Ministry of Information and Communication, Republic of Korea, February 1998.

[51] Korea Information Security Evaluation Methodology(KISEM) Ministry of Information and Communication, Republic of Korea, November 1998.

[52] Philippe Kruchten, The Rational Unified Process—An Introduction Addison-Wesley-Longman, Reading, MA, USA

[53] BS 7799-2:2002 Information security management systems—Specification with guidance for use BSI(British Standards Institution), Customer Services, 389 Chiswick High Road, London W4 4AL, United Kingdom

中华人民共和国
国家标准化指导性技术文件
信息技术 安全技术
信息技术安全保障框架
第2部分:保障方法
GB/Z 29830.2—2013/ISO/IEC TR 15443-2:2005
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.25 字数 84 千字
2014年4月第一版 2014年4月第一次印刷
*
书号:155066·1-48741 定价 45.00元

GB/Z 29830 2-2013