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 29830.3—2013/ISO/IEC TR 15443-3:2007

信息技术　安全技术
信息技术安全保障框架
第3部分:保障方法分析

Information technology—Security technology—A framework for IT security assurance—Part 3: Analysis of assurance methods

(ISO/IEC TR 15443-3:2007,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 3 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 15443-3:2007《信息技术　安全技术　信息技术安全保障框架　第 3 部分：保障方法分析》。

本部分做了下列编辑性修改：

——国际标准中的附录 D、附录 E 为资料性附录，转标时予以删除。

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、北京化工大学。

本部分主要起草人：王晶、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指导性技术文件的第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3部分:保障方法分析

1　范围

1.1　意图

GB/Z 29830的本部分的意图是:为保障机构选择合适类型的ICT(信息通信技术)保障方法提供指导,并为特定环境铺设分析特定保障方法的框架。

1.2　应用

本部分可使用户把特定保障需求和/或典型保障情况与一些可用的保障方法所提供的一般性表现特征相匹配。

1.3　适用领域

本部分的指导适用于具有安全需求的ICT产品和ICT系统的开发、实现及运行。

1.4　限制

安全需求可能是复杂的,保障方法是各式各样的,并且组织的资源和文化之间是有很大差异的。因此,本部分所给出的建议是定性的和概括性的,可能需要用户自己来分析第2部分中哪些方法最适合自己特定的交付件和组织的安全需求。

2　术语和定义

ISO/IEC TR 15443-1和ISO/IEC TR 15443-2界定的以及下列术语和定义适用于本文件。

2.1

资产　asset

对组织有价值的任何东西。

2.2

评估　assessment

系统化地检查一个实体有能力满足其规定需求的程度;当针对一个交付件时,评估是评价(evaluation)的同义词。

[ISO/IEC 14598-1]

2.3

评估方法　assessment method

为了确定一个交付件是否可以接受或发布,把特定文档化的评估准则应用于一个交付件的动作。

2.4

保障机构　assurance authority

受托对一个交付件的保障做出有关决定(即:选择、规格说明、接受、增强)的人和组织,其中,这些决

定最终可导致建立该交付件的信心。

注：在特定的模式和组织中，术语“保障机构”可以是不同的，例如“评价机构”。

2.5

保障管理者　assurance administrator

负责选择、实现或接受交付件的人。

2.6

保障目标　assurance goal

通过应用正式的和非正式的评估活动，要予满足的整个安全期望。

2.7

保障关注　assurance concern

保障机构的一个保障小组所追求的一般类型的保障目的。

注：在本部分中，使用“保障关注”的目的是，为给予保障指南的那组用户，建立相关的分析和结论。

2.8

交付件　deliverable

IT 安全产品、系统、服务、过程，或特别地作为保障评估对象的环境因素（即人员、组织）。

注 1：一种对象可以是 ISO/IEC 15408 中定义的保护轮廓（PP）或安全目标（ST）。

注 2：当用于 ISO 9000 标准族时，服务是一类产品和“产品和/或服务”。

注 3：就本部分的意图，并为了与 ISO 9000 中的用法类似，在整个文档中出现交付件的地方，一般均使用术语“产品”。

2.9

环境　environment

生存周期过程执行的环境（即人、支持设施和其他资源）及所关联的环境保障特征（如声誉、认证）。

注：在 ISO/IEC TR 15443 中，环境保障相对于产品保障和过程保障。

2.10

信息安全管理体系　information security management system；ISMS

整个管理体系的一部分，该部分基于风险途径，建立、实现、运行、监视、维护和改进信息安全。

[ISO/IEC 27001:2005，定义 3.7]

2.11

方法　method

为了获得可重复的结果，以系统化和可跟踪的样式，按计划执行某件事情的方式。

2.12

度量　metric

用于测量的定量化尺度和方法。

2.13

过程能力　process capability

一个过程达到所要求目标的能力。

2.14

产品　product

IT 安全产品、系统、服务。

注 1：针对本部分的意图，类似与 ISO 9000 有关产品一词的用法，在整个指导性技术文件中，术语“产品”将替代交付件这一术语。

注 2：“产品”等同于“交付件”。

2.15

残余风险　residual risk

风险处置之后仍然存在的风险。

2.16

风险评估　risk assessment

风险分析和评价的整个过程。

[ISO/IEC 指导 73:2002,定义 3.3.1]

注 1：风险评价是一个把估算的风险与给定的风险准则进行比较的过程，目的是为了确定风险的严重性。

注 2：就本部分的意图而言，风险评估、风险分析以及“威胁-风险-分析”概括地称为风险评估。

2.17

风险处置　risk treatment

为了修改风险，选择并实现按一定测度进行测量的过程。

2.18

安全　security

与定义、实现和维护保密性、完整性、可用性、抗抵赖性、可核查性、真实性和可靠性等有关的所有方面。

[ISO/IEC 13335-1:2004,定义 2.11]

2.19

安全目的　security objective

意在抵御已标识的威胁和/或满足已标识的组织安全策略和假定的陈述。

[ISO/IEC 15408-1:2005,定义 2.42]

2.20

安全策略　security policy

一个组织部门内的规则集，规定这一部门如何在其法律和文化的语境下使其资产的管理符合所描述的组织目的。

2.21

阶段　stage

交付件生存周期中一个由过程和活动组成的时段。

注：改编自 ISO/IEC 15288。

3　缩略语

下列缩略语适用于本文件。

COBIT：有关信息和相关技术的控制目的，一种 ISACA 的方法（Control Objectives for Information and related Technology，a method of ISACA）

DA：开发保障(Developmental Assurance)

IA：集成保障(Integration Assurance)

ISACA：信息系统审计与控制联盟(Information Systems Audit and Control Association)

ISSEA：信息系统安全工程联盟(International Systems Security Engineering Association)

OA：运行保障(Operation Assurance)

ST：安全目标(Security Target)

4 对保障的理解

保障的目的是为了提供一种信心，即一个产品在一个给定的语境中将安全运行。这一章针对其中一些有关的基本问题进行了相应的考虑，而在本部分的其余章节中，给出这些问题的详细分析和指导。

按本指导性技术文件的第1部分和第2部分中所给出的概念定义，这意味着产品满足一个给定的保障目标。这一目标必须以一种相当正式的方式予以建立。用户必须了解残余风险。

信心将是通过使用并解释保障结果而获得的，其中保障结果或是对应用的保障方法已经是可用的，或是通过应用保障方法而获取的。因此，保障方法需要很好地予以选择和使用。

大量方法是可使用的，并在本指导性技术文件的第2部分中给出了许多保障方法。有关这些方法的应用，在4.2中给出了其中一些基本说明。

用户的保障结果可以表达为各种各样的复杂程度。这一复杂性可以指导保障方法所关联的严格程度(参见4.2.1)、应用范围(参见4.2.2)，以及所涉及的生存周期阶段(参见4.2.3)。

特别注意的是，要对保障结果进行评估。为了获得较大信心，可能需要正式的评估或认证(参见4.3)。

4.1 保障目标的设置

保障目标应依赖于要满足的保障需求：

——产品供应商可能具有一些一般性的保障需求，其意图是为了满足多个用户(即产品、系统或服务的用户群)的特定需求；

——产品的用户一般都具有一些非常特殊的保障需求，这样的保障需求通常依赖于其组织的特定安全策略。

以下给出有关保障目标设置的说明，并把它联系到合适的保障供给和使用。

注1：在附录A.1的例子中，区分了硬件供应商、软件供应商、网络提供方、服务器运行方、内容提供方，以及用户方——企业。在这一例子中，明确指出供应商属于保障提供方，而用户组织属于得到保障一方——保障的用户，而其他的既是保障提供方又是得到保障的一方。

注2：一个组织可能需要把来自多个保障源的保障结果组合为一个一致的、复合的保障结果。这是一个重要方面，在本部分的5.3和6.2.3.1中将谈及。当多个保障结果可用于一个保障的用户，或当一个保障提供方打算使用两个或多个保障方法时，就出现了这一方面的问题。4.1.1和4.1.2通常与开发、集成期间的产品保障相联系的。这与保障关注的不同在第六章中进行讨论。

注3：重要的是，要理解一个产品的运行通常受控于用户组织的责任和监督，即使安全服务与服务提供方签订了子合同。因此，4.1.1和4.1.2并不直接可用于运行保障(OA)。

4.1.1 供给的保障

按照提供产品、系统或服务组织的商业观点，合适的保障方法应基于预期的用户或用户群及其组织规模和专业知识。必须按照这些不同来剪裁保障。特别地，如果是针对一个用户群，那么保障就必须具有充分的一般性。

通常，提供保障是应对市场的一个重要的因素或是涉及成本的一个重要的因素。因此，提供保障的组织就必须依据其成本考虑其效益。

由上可见，在做出提供保障这一决策的过程中，首先要标识以下两个步骤：

——用户为什么想要为保障买单；

——用户建立保障想要达到什么意图。

采用这些步骤，可以进一步导出客户的保障需求，并最终导出可用的保障方法，如图1所示。

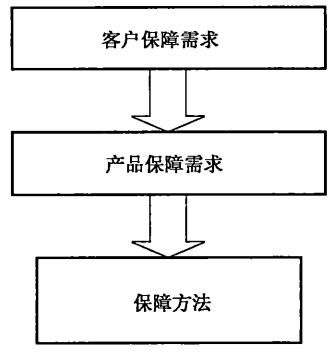

图 1　保障供给

其结果，保障通常可像表 1 所表达的那样予以供给。

表 1　供给的保障类型

供给的保障	针对的客户	客户的保障需求	要求的保障严格程度
已通过的保障	最终用户	内容标记； 对最终用户是有意义的并且是可认可的	低
市场上的保障	一般性的用户群	标签、标记、印记； 标记引用了一般的保障需要； 是以非常简洁的或封装的方式表达的对最终用户是有意义的并且是可认可的，即认可的“质量标签”	低
内部保障	内部客户	保障陈述的独有形式；为组织内部提供的，并基于信任	任意
外部保障	特定用户群	标记包含了扩展的论据和资料；可有受限地发行	高
小型组织的保障	小型组织	标签或商标； 期望通过简介来创建信任； 对最终用户是有意义的并且是可认可的，即认可的“质量标签”	中
大型组织的保障	大型组织	详细的保障陈述	高
强制性保障	特殊复杂的组织	证书或符合意图的陈述； 组织强制使用一定的保障格式甚至保障方法	高

客户的保障需求是以保障方法所提供的保障陈述形式标识的。

必须考虑具有支持作用的保障论据，特别是它们的保障严格程度（参见表 3）。多半保障方法产生多种类型的保障需求，并且保障严格程度依赖于相应的保障方法。因此，为了确保最终要满足用户的保障需求和最终的保障目标，必须认真组合所选择的保障方法。

4.1.2　保障的使用

用户的保障供给具有不同观点。从最终的保障机构的视角来说，用户的目的是获得信心，即特定产品满足他的特定保障目标，这一信心是对产品以及组织语境的整个安全期望，其中，该产品是在这一语

境下予以实现、部署和/或运行的。

理想上，保障目标是通过风险评估来建立的，或可能是由组织策略予以施加的。

信心可通过选择和应用正式的或非正式的评估活动来获得。这样的活动可以由供应商、系统集成方提供，或由用户执行，或用户指派特定人群按其要求执行。

保障的使用可以如同表 2 所表达的那样，该表还提供了可使用户建立最终信心的活动。

表 2　保障供给的使用

用户类型	要寻求的保障	用户保障的鉴别活动	相关的评估严格程度
特定用户	内容标记(labelling)	检测内容标记是否是有意义的，是否是认可的并可应用于已领悟的保障目标	低
一般用户	标签、标记、印记	检测内容标记是否是有含义的，是否是认可的并可应用于已领悟的保障目标	低
内部客户	保障陈述的专有形式	确认内部的信任，例如通过提出适当的问题	任意
特定用户群的成员	标记	确认标记的信任，例如通过提出有关其他成员或其他团体组织的问题	高
小规模的组织	标签或印记	检测内容标记是否是有意义的，是否是认可的并可应用于已领悟的保障目标。 认可的“质量标签”是完美的	中
大规模的组织	详细的保障陈述	通过组织专家已验证和确认陈述	高
特殊复杂的组织	认证或意图陈述合理	信任可由第三方评价和/或认证提供，至少通过保障提供者的声誉	高

4.1.3　残余风险

在其最基本的等级中，保障为用户提供了如下的信心，即“一个产品将按提供者所宣称的那样运行，而没有表现出不期望行为”。但是，保障与其他安全保证措施不一样，其本身并不提供任意附加的功能(安全机制)，因此保障不能抵御任何附加的脆弱性和威胁。

所有安全元素，特别是在与方法的使用相对独立的风险管理中，包括一些不确定性。不确定性来源于许多地方，例如不完全了解所有因素，不了解测量中的容错以及这些因素的外延等。在某些情况中，这样的不确定性可能很大，以至它表达了残余风险的主要因素。其他因素是目标运行环境的脆弱性以及安全机制的不完美。如果保障是严格的话，必然涉及安全特性和安全机制，这样就可减少与这些因素相关的不确定性，从而减少整个风险。

在一些确定的情况中，保障可能仅是一种减少不确定性的方式。如果没有增加任何新的安全机制的话，保障可以把风险减少到一个可接受的程度。在这一情况中，保障成本就可直接为安全的效益作出贡献。由上可见，保障的目标是减少风险。

4.2　保障方法的应用

保障方法具有一些可作为一些部件或一些方面的不同特性。为了提供有关如何选择一个或多个方法的指导，有必要以类似的形式，特征化地描述可在不同保障方法中发现的这些部件或这些方面。一个给定的保障方法可以包括一些一般性的保障特性，或可能关注一些特定的保障特性。

按着本指导性技术文件的第 1 部分和第 2 部分所描述的那些内容，通过评估：

——产品，或在该产品创建之后；
——过程，创建该产品期间所使用的过程；
——环境，实现产品的环境，即涉及的人员和组织；
一些方法就有可能达到(实现)一个产品的保障。

4.2.1 保障严格性

由保障方法所提供的严格性，通常规定了它的使用，如表3所示。

表3 保障的严格程度

严格程度	使用
1	简单的“批准的保障印记”
2	有关保障的符合程度陈述
3	支持所宣称保障的详细事实
4	支持所宣称保障并可验证的详细事实
5	对一般受众(例如，董事会)的表达，并得到认可
6	对安全专业受众的表达，并受到已授权受众的认可

注1：除了必须考虑表达强度之外，还要考虑该表达的支持论据的强度。在特殊的情况中，可应用一些限制和约束。
注2：当把一些已评估部件的保障，组合到一个可部署的系统中时，度量可能是重叠的和/或可能存在一些“空隙”问题。
注3：本指导性技术文件的第2部分没有提供有关评估严格性的评定。

4.2.2 应用范围

所获得的保障还可能由于保障途径关注点的范围而有变化，参见表4。

表4 保障途径应用范围

保障途径	保障方法的关注点	应用范围
产品	产品、系统或服务的特性，以便确定该产品或系统的保障	产品或系统的某些方面
		产品或系统的所有方面
过程	组织针对一个特定产品或系统所使用的开发过程，以便确定该产品或系统的保障	开发的某些方面
		开发的所有方面
	组织针对所有产品或系统所使用的开发过程	开发的某些方面
		开发的所有方面
环境	执行该任务所雇用的人员	人员的资质
		声誉
	组织	组织为关注后来发现的问题，采取的演示式动作，以及这些动作的速率
		声誉

4.2.3 应用与生存周期

本指导性技术文件的第1部分基于ISO/IEC 15288采用了一种阶段式模型。每一生存周期阶段对应一个环境中应用到一个产品的过程。每一过程由一个活动集组成，并使用该环境的资源。

应用每一阶段的过程和过程活动，一个产品、系统或服务交付件在其生存周期得以处理。

本指导性技术文件的第1部分引入了一个框架，该框架允许表征要予评估的产品类型、保障途径和保障阶段。

一直存在一些要予强调的问题。本指导性技术文件本部分将扩展在本指导性技术文件第1部分所建立的概念框架，以便允许做进一步分析。

本部分中，将通过增加概念/规约阶段来增强生存周期阶段式模型(参见表5)。

基于许多标准，本指导性技术文件给出对应“概念/规格阶段”的过程。然而相互分离的生存周期阶段通常不一定以这些过程为前提。目前只有几个保障方法为这一生存周期阶段提供了良好定义的相关过程和活动，即公认的需求工程原理。

在本部分中，增加“概念和或规约阶段”的理由是，ICT安全要求对产品安全特征的高内聚和低耦合规约的产生，应予特别的注意，并要增加适当的工作。为了适于ICT安全领域，现有几个保障方法已为这一生存周期阶段提供了良好定义的过程和活动。

在这一增强的模型中，使用表5中的5列来表达不同的生存周期阶段。并且，为了接近ISO/IEC 15288的概念，把技术上的生存周期过程分组到五个阶段中，每一列代表一组过程，并缩写为一个字符：

C：概念，引导建立安全设计需求，其中可包括一个整体上的体系结构；

D：设计，包括利益有关方功能需求定义过程、需求分析过程、体系结构设计过程和实现过程；

I：集成，包括集成过程和验证过程；

T：转移：包括复制过程、转移过程、部署过程和确认过程；

O：运行，包括运行过程、维护过程和销毁过程。

表5 生存周期保障模型

保障阶段 → 保障途径 ↓	概念/规格说明	设计/执行	集成/验证	开发/转移	运行
产品	⇒C⇒	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
过程	C	D	I	T	O
环境	C	D	I	T	O

在本指导性技术文件的第1部分中，开发了以下三个概念：

——产品保障，由于保障可能关注过程的结果——产品，从而出现产品保障。

——过程保障，由于组织及其用户通常关注正应用于产品的过程，即他们或相当严格地或不大严格地规约应用于产品的过程，或经常或强或弱地改进这些过程。因此，保障可能关注应用于产品的过程，而不是关注产品本身，从而出现过程保障。

——环境保障，由于过程的执行需要一个环境，其中涉及人、设施和其他资源等。因此，保障可能关注处理一个产品的环境，而不是产品或过程，从而出现环境保障。

注：在本指导性技术文件中，没有细化生存周期途径的范围及其过程和活动，但是为了更细腻地对保障方法进行比较，必要时可能对它们进行细化。

4.2.4 生存周期过程管理

生存周期阶段C-D-I-T-O由可应用于特定ICT交付件及其构件(如硬件、软件、服务)的过程组成。

在关注质量和改进的情况中，这些过程及其活动可从属于过程管理。过程管理本身又是一个过程，该过程不是在项目层面上执行，而是在组织层面上执行。因此，过程管理是一个组织方面的过程，独立于一个特定的项目。

但是，只有当这些过程被 IT 管理人员或被 ICT 项目的产品开发人员重复执行时，过程管理才会有意义。

在本部分中，通过增加过程管理(作为另一维度)来增强本指导性技术文件的第 1 部分中的生存周期过程模型。

在 ICT 安全中，这一维度对于运行阶段中应用于 ICT 系统的安全管理方法尤为重要，例如在 ISO/IEC 27002 及其关联的 ISO/IEC 27001 的情况中。

过程管理涉及生存周期过程的开发、使用和改进，主要包括。

——过程定义，包括过程开发及建档；

——过程的重复使用；

——过程评估和测量；

——过程改进。

过程可以从属于第三方的认证。

与这些步骤相关联的过程/活动数量，对应于一个进展(progression)，并依赖(dependency)：

——如果没有已制定的和建档的过程，就不存在重复使用；

——如果没有过程的重复使用，就不存在过程评价和测量；

——如果没有过程评价和/或测量，就不存在过程改进；

——如果没有过程评价和/或测量，最终就不存在认证。

当改进导致过程及其文档的改变时，过程管理就可能被认为是一个不断改进的循环模型，如图 2 所示。

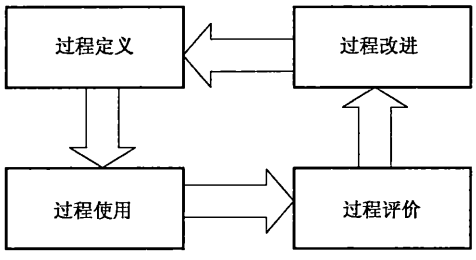

图 2　生存周期过程管理

注 1：为了获得过程的可测量性，这些只能按照文档所述的那样予以使用。过程管理是第 2 维度的过程，与 C-D-I-T-O 阶段这一维度的过程是正交的。如果一个保障方法提供了过程保障，那么这就意味着应用于一个产品的过程就从属于过程管理。如果一个方法的保障阶段用灰色表示(参考表 6，第 2、4、6、7 单元格)，那么该方法就提供了过程管理。

注 2：产品开发和过程开发非常类似，因此很容易引起混淆。它们必须予以区分和分离。

4.2.5　生存周期特性的累积

相对于生存周期特性，方法并不是十分完备的。然而生存周期特性可以予以累计，这可以表征一个方法的完美性，但又表征一个方法的复杂性。

在本指导性技术文件的第 1 部分中，规约了一些值得重视的、表现为一个保障方法的保障途径。这些保障途径可用符号表达为：

——产品保障:在箭头中间以黑体字符显示生存周期阶段,例如:⇒D⇒

——过程保障:在阴影中以白色字符显示生存周期阶段,例如:

——环境保障:在左右两个黑棒之间的字符,显示生存周期阶段,例如:■D■

这些途径可以予以累积,如表 6 所示。其中,对于一个给定的保障方法以及值得重视的生存周期阶段,给出了级别(7)这一有意义的可能性。

通过部件数目可以看出,等级 7 是最完备的一个级别,而且通过术语、过程和结果,等级 7 至少表达了综合性以及与希望一致等优点。这特别会影响培训及成本。

注:综合性并不意味着最完备的方法对一种特定的保障情况而言必然是最好的。方法的好与不好,必须要考虑它的其他方面,例如严格性、详细程度以及所关联的成本等。

表 6 保障途径

级别	产品保障	过程保障	环境保障	生存周期阶段 X 图示
1	√			⇒X⇒
2		√		X
3			√	X
4	√	√		⇒X⇒
5	√			⇒X⇒
6		√	√	X
7	√	√	√	⇒X⇒

4.3 保障结果的评估

对于那些提供保障的产品、过程和环境而言,其安全相关特性存在于它们最初的格式声明中,这一声明是由原单位(通常是该交付件、服务或环境的生产者)做出的。为了验证这些声明的保障,可能需要评估相应的保障结果,或可能需要认证之。

可以建立一个保障评估模型。该模型定义了一系列通用的、可应用于这一技术报告中所提及的任意保障方法的步骤。

这一保障质量模型,需要:

——人员、评估者或团体,对应用的准则进行验证;

——评估规则、准则和/或方法学,它们是一个评估的基础;

——认证,授权审计人员,和/或依据评估规则完成相应的评估过程;

——评估结论,给出该评估的结果。

这一类完整的模型通常称为一个保障模式。

4.3.1 评估员

产品安全保障特性的评估,可以由产品的用户进行。这涉及一些专门的知识。为了节省时间和成本,这一评估可聘请有经验的第三方进行。

由于第三方是相对独立的这一简单事实,因此第三方的评估可进一步增强保障。

注:有关人员保障应当认证该评估者的资格是否是可接受的。

4.3.2 评估准则和方法学

为了使评估是可重复的,评估规则需要文档化,并需要与方法学互补。

注：在人员评估中，被评估的交付件是一个人。

4.3.3 评估证据

对所有评估方法而言，其共性是它们的评估结果一般是基于证据的。证据是由一些陈述给出的，并一般采用文档形式。

证据证明了过程中的动作以及计划和规程，均按安全策略和安全概念各自有效地执行。这些内容必须予以评审，并且如果需要的话，还要按规定的方式予以修正。

该文档最重要的需求是：

——稳定性(文档必须反映实际情况)；

——完整性(所有关注的问题必须建立相应的文档)；

——细节的充分程度；

——配置控制和完整性控制(对文档的未授权改变)。

在保障方法的详细分析中，将进一步探索这一文档的需求和可比性问题。

4.3.4 评估结论

定量或定性的评估结果必须予以规约。这可以以最简单的形式：通过/失败；而更详细的结果通常采用一种评定格式，例如一些不同的等级，其中包括一个对应于“失败”的评定。

与某些其他技术领域不同，安全具有不断演进的特征。这是因为交付件的复杂性，新的安全缺陷可能出现；这是因为威胁环境，新的威胁可能需要予以抵御。

4.3.5 评估维护

一旦做完了一个评估，就必须定期地提出问题，或按由事件触发的时间间隔提出相应的问题。评估维护是为了确保所赋予的安全保障结果或评定的时效性。

注：在人员保障中，这可能意味着不断进行人员培训，人员的定期再评估或再认证。

4.4 例子

保障机构——一个供应商，按 ISO/IEC 15408 评估准则构造了一个可信系统，满足一般性的需求。评估服务机构的评价人员评估该供应商的系统，以确保该系统符合这些一般性需求，并符合 ISO/IEC 15408。

为了再现性，该评估机构应用 ISO/IEC 18045(评估方法学)，并发布适当的批准评定。

按通用准则(CC)互认协议，评估人员和评估服务机构得到国家认证认可机构的认可。

国家认证认可机构发布证书，给出该评价结果以及获得的评定。

这一认证可能需要对评价进行维护，以确保该产品的更新并没有危及最初的评定。

5 保障的比较、选择和组合

本部分的意图是，为保障机构在选择合适的 ICT 保障方法方面提供指导，以获得给定的保障目标，即满足组织的安全策略。这一指导将有助于保障机构来确定：

——哪一种保障途径将提供最适合保障机构需要的保障结果；

——每一种保障途径相对应的值最适合保障机构的特定语境；

——如何处理复杂交付件(即不同硬件构件、软件构件、安全服务、环境方面或它们的组合)的保障。

5.1 保障途径的选择

保障可以通过使用不同的方法获得不同的保障等级。在这一节中，以得失攸关的角度，采用一对一

比较方式，比较如下每一保障途径（不是方法）：

——产品保障与过程保障；

——过程保障与环境保障；

——产品保障与环境保障。

这三种途径对应表 6 中前三个条目。比较的目标是为了了解如何以一般方式来选择其中一种保障途径。

注：对应表 6 条目 4～7 的组合途径将在 5.2 中讨论。

5.1.1 产品保障与过程保障

产品保障关注有关产品的每一个定义，而过程保障关注在一给定数目的生存周期阶段中应用于该产品的过程。

在产品保障中，其声明是：该产品的特征和性能已予以深入细致地评估、测试或确认，以至该产品获得期望的可信等级。产品保障的这一等级是所用准则（什么要予以评估）和相应保障方法学（如何验证符合该准则）的一个函数。

在过程保障中，其假定是：组织用于设计、开发、生产和/或运行一个产品的过程，具有可预测的、可重复的结果，并由此产生一个具有所建保障的产品。

但是，在生产人员所使用的过程中，即使是最可信的用户，也不能保证他们就一个给定的产品均正确、有效地应用了这些过程。换言之，对于一个高等级保障的产品而言，产品保障（或评估）是必要的。

在产品保障中，每一产品必须分别予以评估，这样整个成本就随着开发的产品数目而不断增加。

然而，从制造商的观点来看，如果用户对制造商的过程保障是满意的，即所使用的过程符合可信赖的过程质量标准，那么就可以避免类似的或等同的产品的重复评估。给出过程保障方法的益处是，组织除了维护其认证而进行必要的定期评估之外，可以不必进行其他附加的评估，生产不同的产品。

这一比较仅对保障方法的可比的有效性、深度和正确性是成立的，并通过称为更客观的第三方所提供的信任就可有理由证明是可能的。

另外，当组合使用这两个途径时，还必须考虑一些相互协调的问题。例如，实现适当过程保障的制造商应耗费一定的资源，为其通过过程保障的过程而实现的产品进行产品评估。

5.1.2 过程保障与环境保障

过程保障关注产品特定生存周期阶段中所应用的每一过程的定义，而环境保障关注资源以及使用这些资源的语境。

对使用环境资源的一个产品的信任，来自于对该组织和/或其人员以及其他应用于该产品的资源的信任。这一信任可以通过对有关人员和/或组织所使用的标准或好的专业实践之认证来提供，最低的信任等级是主管该产品的人员或组织的声誉。

依据所提供的应用细节之可比程度，环境保障的有效性一般低于过程保障。事实上，组织或人员均可能具有把过程应用于一个产品的一般性知识和能力。但并没有证明这些过程已经文档化，已经予以评估或已经予以认可。

环境保障是最低的保障形式，容易获得。可能存在一些情况，如下所述，对于这些情况而言，只有环境保障才是实际可用的保障或是可承担得起的保障：

——承担不起过程保障或产品保障成本的小型组织；或

——供应商不允许或不提供过程保障或产品保障的现成商品（COST）。

5.1.3 产品保障与环境保障

依据以上的讨论，可以证明保障也存在一个“进展”问题，即如果产品保障是不可“进入的”话，那么

过程保障就是“下一个较好的”保障；进而，如果过程保障是不可“进入的”的话，那么剩下的可能性就是环境保障。

5.1.4 结论

在不承认所给保障途径具有可比性的条件下，其结论可表达为：

——应为最高的保障需求选择产品保障；

——通过相关过程的质量保障，过程保障提供了有据的、最合算的保障；

——对于规模不大的组织，或在产品和/或其生产者不可能进行过程评估和/或产品评估的情况下，必须选择环境保障。

一般而言，可陈述为(参见图 3)：

——提升严格性的产品保障，局限于复杂性相对较低的交付件的开发保障。而

——环境保障主要适于运行保障，其中系统相对复杂而保障相对不太严格。

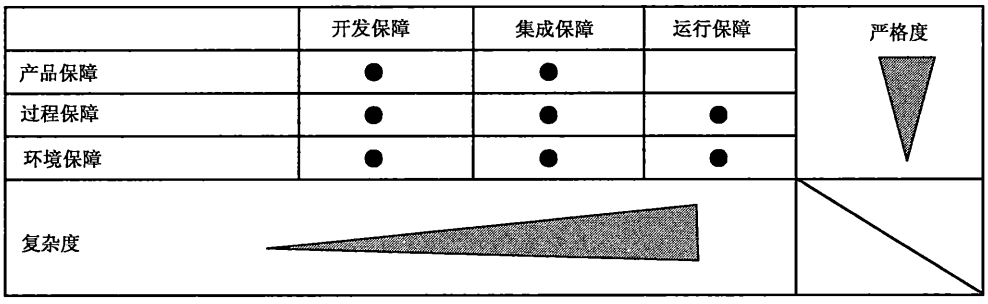

图 3 可用方法

5.2 保障方法的组合

不可避免地，许多用户将涉及多个保障方法：或可能涉及 ISO/IEC 15408 和 ISO 9000，或可能涉及 ISO/IEC 15408 和 ISO/IEC 21827。

本指导性技术文件提供一种结构，使用这一结构可记录所涉及的这些保障方法的证据/经验。本指导性技术文件提供一些概念和一种通用语言，以此可描述方法和途径之间的相互影响和相互作用，从而有助于探索可能的组合。

通过从正在使用的保障途径之外的其他保障途径中接受一些保障元素，即从一些不同的保障途径中组合保障特性的能力，将有助于达到产品和系统的保障。

例如，如果一个组织已通过 ISO/IEC 21827 等级 3 的认证，那么就可承认该组织在 ISO/IEC 15408 的模式中，而没有必要让该组织重新提交已为另一保障途径而提交的证据。另外，这还有助于认可人员的工作，因为他们在确定整个系统保障中将具有一些现在可采纳的附加证据。

通过保障方法的比较，可以了解有关保障组合途径的潜在限制。当该组合保障途径基于不同属性时，这一了解关系到如何灵活地交叉这些保障特性。

从不同的角度和在不同的范围内寻求安全的方法，可以针对具有不同意图的不同用户或不同的组织部门。在本指导性技术文件中，没有一种方法可以被认为是一种“综合”安全的方法，即保护现有的 IT 系统合适地抵御了所有相关的威胁。因此在大多数情况下，有必要协同地使用一些方法的组合。

如果 IT 供应商和用户以伙伴关系一起努力的话，一个 IT 系统就可达到一种最理想的安全程度。

在附录 C 中给出了一些显示保障方法组合方面的例子。

5.3 保障方法的比较

可使用两种基本途径来比较第 2 部分中所列出的那些保障方法的相关价值。

——特性矩阵;或

——成对比较(一对一比较)。

如果必须对三个以上复杂条目进行相互比较的话(参见图 4),那么就比较这些条目所具有的共性。随着条目的增多,就越可证明这一途径是不可否认的。当然,必要条件是在这些方法中相似性的数量是有一定规模的。

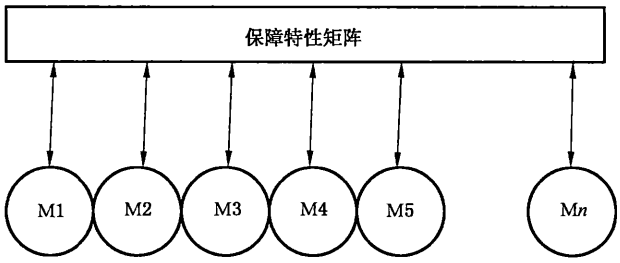

图 4 矩阵比较原理

就矩阵比较的意图而言,必须开发一张保障特性表。因此这一途径的挑战是,建立一张最理想的特性表,适于勾画方法的主要区别。

保障方法的矩阵比较仅由一张表组成,描述并评定每一单个的方法。定量的测量或分等可以简化该结果的表达。为了从这些基准标记的结果中进行选择,提供指导的一种合适的方式是准备一些图形化的概览检测表。

为了做出以下两方面的非正式决策,一是使用哪一种保障方法,二是有从一种特定保障方法中所产生的保障结果的价值,矩阵比较分析检查特定保障方法的组合。

依据感兴趣团体的类型,例如产品制造商、大型组织等,可以把这样的矩阵比较剪裁为一些特定的关注域。

在本部分中的第 6 章中,定义了三种保障关注,并给出了相应的选择指导。

例如在 A.1 中,针对所选方法给出了一种整个特性的概括性矩阵比较。

5.3.1 一对一比较

有关条目的一种更详细的比较,可以使用一个自定义的列表:增加一些条目或删除一些条目,以适应成队选择的条目,并必须研究进一步的细节。

然而,随着要比较方法的数目增加,一对一比较的数目会按 n 和 2 的二项式系数地增加,其中 n 是方法的数目,例如 6 个条目就会有 15 个单独的比较条款。因此,本部分没有给出这种类型的比较。

这种类型的比较留给用户,用户可以基于第 2 部分列举的描述和列在那里的引用文件进行这样的比较。用户还可以从这样大量的一对一的比较中作出一个总结,从而得出结论。

5.3.2 保障特性矩阵

保障特性是保障的实际源,并且可予以适当的度量。这些度量包括成本以及各种可定量方面,如严格程度、可靠性、可重复性、效率等。

何种保障方法是目前保障问题的正确方法,以及应如何应用之?要回答这个问题,必须了解保障方法所能带来的益处及其相关的成本。换言之,为了更容易地进行比较,必须表征那些对保障价值具有作用的保障特征。

5.4 关注的保障特性

为了对已建立的保障方法进行比较,开发了许多特征化的保障特性。本部分的目标是,帮助用户决

定哪一个方法或哪些方法的组合对他/她的特定情况是有帮助的。

表 7 中的保障特性是一些具有一般性的、最基本的保障特性，并在附录 B 中以这些特性为基础，分析了一些保障方法。

在 A.1 中，以总结的形式表达了这些方法的一般指向。依据这些表，可以总结出一个方法在一个特定的语境下的适合性和不可适用性。

另一方面可能是应用保障方法所要求的时间问题。

注：有关方法的源和更多的信息，可参阅本指导性技术文件的第 2 部分。

表 7　比较的关键方面

方面	描述
保障目标	方法是否提供了保障目标的定义？ 根据什么方法可导出这一目标？ 这一保障目标如何达到？
目标读者	该方法强调哪方面保障(即保障关注)？ 该方法针对何种公司？以及其内容指向该企业中哪些角色？
特性	该方法的意图涉及什么？ 它包括哪些方法学上的基本元素？ 该方法如何应用于通用的企业结构？ 如何把该方法映射到一个特定的应用情况？
多功用性	应用方法的工作量和成本之间的关系是什么？ 可以处理调研中什么规模和复杂性的对象？ 这可以予以控制吗？例如，通过应用不同的详细层
适时性	方法的当前版本反映了最新技术了吗？ 如果有必要进行有规律更新的话，那么这如何予以确保呢？
完备性	有关问题中关注点的准则，是否由一个封闭的(closed)、详尽的条目类别所组成，或只是被所选择的方面所覆盖？ 该相关的准则类别适合什么样的安全等级安全？
实施成本/工作量	当把一组 IT 安全准则应用到一个典型场景时，必须期望什么样的工作量和成本？
工具支持	是否存在工具来支持用户应用所关注的方法？
密码学上的要求	所关注的 IT 安全准则集是否包含有关密码学上的规程和算法的供给和指导？
评估与认证	对于该方法而言，是否存在一个鉴定和/或认证系统？ 该方法适合于产品或整个解决方案吗？
声誉和认可	成功评估和认证的影响，即潜在顾客或管理机构的满意度，或至少作为补充测试的一个基础。 模式成熟到什么程度？ 市场接受的及其驱动力是什么？

5.4.1 保障目标

为了获得可接受的风险等级，保障机构的任务是，批准准确的保障以及要收集的保障证据数量和质量。这意味着对预期的环境而言，残余风险不应超过利益攸关方（例如一个组织）可接受的风险，并且残余风险可以被利益攸关方所接受。

为了建立对保障结果的信心，保障机构必须用一种合理的方式断定这一结果，证实交付件在实施安全策略中按所要求的那样运行，提供所要求的功能。信心程度应是保障过程和利益攸关方个人感觉程度的一个直接结果。

因此，必须了解用于创建保障结果的过程和标准，包括保障证据的定义、收集和评审。通过用于开发、组合和维护保障证据的方法，可以收集这样的证据。

保障目标可以基于风险评估、安全策略、基线或保护轮廓（PP）。

进行保障特性“保障目标”的比较，可以回答以下问题：

——该方法是否提供了保障目标的定义？

——在该方法中是什么可导出这一目标？

——如何达到这一保障目标？

当一个方法没有提供“保障目标”时，或如果这一目标不对应保障机构的需求时，可取的办法是，使用风险评估来建立保障目标，或对已提议的保障目标进行有效性验证。其中为了反映产业和管理中的实践，必要时可扩充已提议的保障目标。

注 1：可能需要确保风险评估本身，例如通过评估交付风险评估的人员之经验、培训程度以及/或其他认证（即人员受训的地方）等。保障目标可以规定预期的保障方法必须拥有的一些特性，和/或规定所做出的有关保障表达的方式，这样就可减少可获取保障的方法数目。

注 2：在现有的一些 IT 安全标准和技术报告中，表达了一些相关的概念和过程，如 ISO/IEC 13335、ISO/IEC 27002、ISO/IEC 21827 和 ISO/IEC 15408。

5.4.2 目标读者

本指导性技术文件的本部分已经进行了必要的剪裁，以便针对第 6 章中说明的 3 种典型情况给出相应的指导。这一保障特性将显示以下三种类别：

开发保障：ICT 产品的开发，例如针对一个安全目的；

集成保障：获得和/或组合一些产品成为一个 ICT 系统，例如，满足一个安全策略；

ICT 系统的运行保障，例如，满足给定的组织安全策略。

另外，开发保障、集成保障和运行保障可以回答以下问题：

——该方法是针对哪些公司的？

——其内容直接涉及企业内的哪些角色？

——该方法如何应用于一般性的企业结构？

5.4.3 特性

在本指导性技术文件的第 1 部分、第 2 部分的定义中和在 6.1 中，已对保障途径予以详细解析。

另外，这些内容可以回答以下问题：

——该方法如何应用于一般性的企业结构？

——该方法所关注的意图是什么？

——它主要包括什么方法学方面的元素？

注：有关选择可用于一个特定保障目标的保障途径的指导，请参见 5.1。

5.4.4 多功用性

复用一个评价中一些部分的可能性，允许分摊一个产品的工作成本，例如在以后类似产品的评估中。在独一产品的情况下，例如不是当前交付件家族或未来交付件家族中的一个产品，针对一个特定的版本，必须拨付相应的成本。

另外，这些条目可以回答以下问题：

——应用的工作量和成本之间的关系是什么？

——可以处理什么规模或复杂度的受调查对象？

——这是可以控制的吗？例如应用不同水平的细致程度。

5.4.5 适时性

这些条目可以回答以下问题：

——方法的当前版本反映了最新技术吗？

——如果按规定进行必要更新的话，如何确保这一更新？

——市场接受及其驱动力是什么？

另外，这些条目还可以回答以下问题：

——有关问题中关注点的准则，是否由一个封闭的、详尽项的目录所组成，或覆盖的仅是那些所选择的方面？

——什么样的安全等级适合该相关的准则目录？

5.4.6 完备性

该条目可回答以下问题：

——该方法是否关注了安全目的，具有一个封闭的、详尽项的目录或仅涉及所选择的那些方面？

——该方法适于什么样的安全等级？

5.4.7 实施成本/工作量

该条款可回答以下问题：

当把一组给定 IT 安全准则应用到一个典型场景时，期望必须是什么样的工作量和成本？

保障特性是实际的保障源，并可局限于一些适当的度量。它们包括成本以及各种定量方面，如严格程度、可靠性、可重复性、效率等。

何种保障方法是目前保障问题的正确方法以及如何应用呢？要回答这个问题，必须了解保障方法所能带来的益处及其相关的成本。也就是说，在已经标识了备选的保障方法之后，必须度量并比较对其价值具有作用的评估特征。

评估是一种保障增量，它的获取是以时间、人员和大量成本为代价的。

因此，保障机构必须论证使用这样评价的价值。

保障是有成本的，因此就可涉及保障价值这一问题。

在确定保障途径的价值中，十分重要的是要考虑评估机构的特定语境。依据满足保障机构的特定工作需要，可预测这一价值，但必须对应于保障需要，并特别注意接受该保障最终用户。

在多个备选保障是可用的情况下，必须建立保障方法的相对价值。

组织的安全策略或文化可能会影响保障的形式。这一形式是由组织愿意为此支付多少资金或由其他如政治法令或规定等相应的准则予以支配的。从这些因素中可以捕获到保障的用户为什么愿意为保障支付，以及他们希望把这些支付的保障用在什么地方。

注：在考虑保障方法时，第一步可能是要标识用户为什么愿意为保障支付以及用户需要保障的意图。这可以消除

其他的保障方法，并且还可极大地影响可达到的保障目标。

5.4.8 工具支持

该条目可回答以下问题：

——在应用所涉及的方法中，是否存在可支持用户的工具？

5.4.9 加密问题

该条目可回答以下问题：

——所关注的一组 IT 安全准则是否包含有关加密规程和算法的规定和指导？

5.4.10 评估与认证

如果进行了保障结果的评估和/或得到某一认可的认证模式的认证的话，就可达到更大的保障增量。

这一保障特性条目可回答以下问题：

——对于该方法，是否存在鉴别和(或)认证系统？

——该方法适合于产品或整个解决方案吗？

——它是否依赖于独立的评价者给出认证呢？或评估认证是由一个团体或一个组织给出的吗？

——认证团体本身经过评估和认证吗？认证规则是什么？

——存在相互承认的协议吗？

——什么影响成功评估和认证？（即满足顾客或管理人员的潜在性，或至少作为补充测试基础的价值。）

——模式的成熟程度？

注：在附录 A 中，给出方法及其关联的认证模式。

5.4.11 信赖与认可

方法的信赖及其可能关联的模式，对用户接受的结果具有很大的影响。

通过市场宣传，可信联盟支持，或通过政府的接受、甚至鼓励或要求，可建立方法的可信赖性。

对整个用户而言，必须了解有关方法的国际标准。

6 指导

任何有效的指导都要求抽象、简单和集中。为了减少基本可用的方法数量，本部分分析了三种典型的情况。这些情况称为“保障关注”，并定义为：

——开发保障：ICT 产品的开发，通常针对一个安全目的；

——集成保障：把一些产品集成到一个 ICT 系统中，通常满足一些安全目的或策略；

——运行保障：一个 ICT 系统的运行，通常满足一个给定的安全策略。

每一个关注是各不相同的，各自具有自己的特殊性和问题。

通过使用本指导性技术文件的第 1 部分中的生存周期和保障途径概念，结合本指导性技术文件的第 2 部分的内容，并用 4.2.3 中的概念/规格说明予以扩展，这样就可容易地把保障关注这一概念予以可视化的(参见图 5)。

理解各种不同的保障方法和途径，将允许一个保障机构来确定适合于业务需求和保障关注的方法，其中要牢记的一个重要方面是保障的最终目标，即达到利益攸关方有关所使用方法的信心。

由于安全需求的复杂性、保障方法的多功用性以及组织资源和文化之间的差异，在本部分中所给出

的建议只能是定性的、概括性的。

本部分中所给出的指导将集中于几个方法，就开发保障、集成保障和运行保障这 3 个保障关注而言，这几个方法已被证明并被广泛接受。

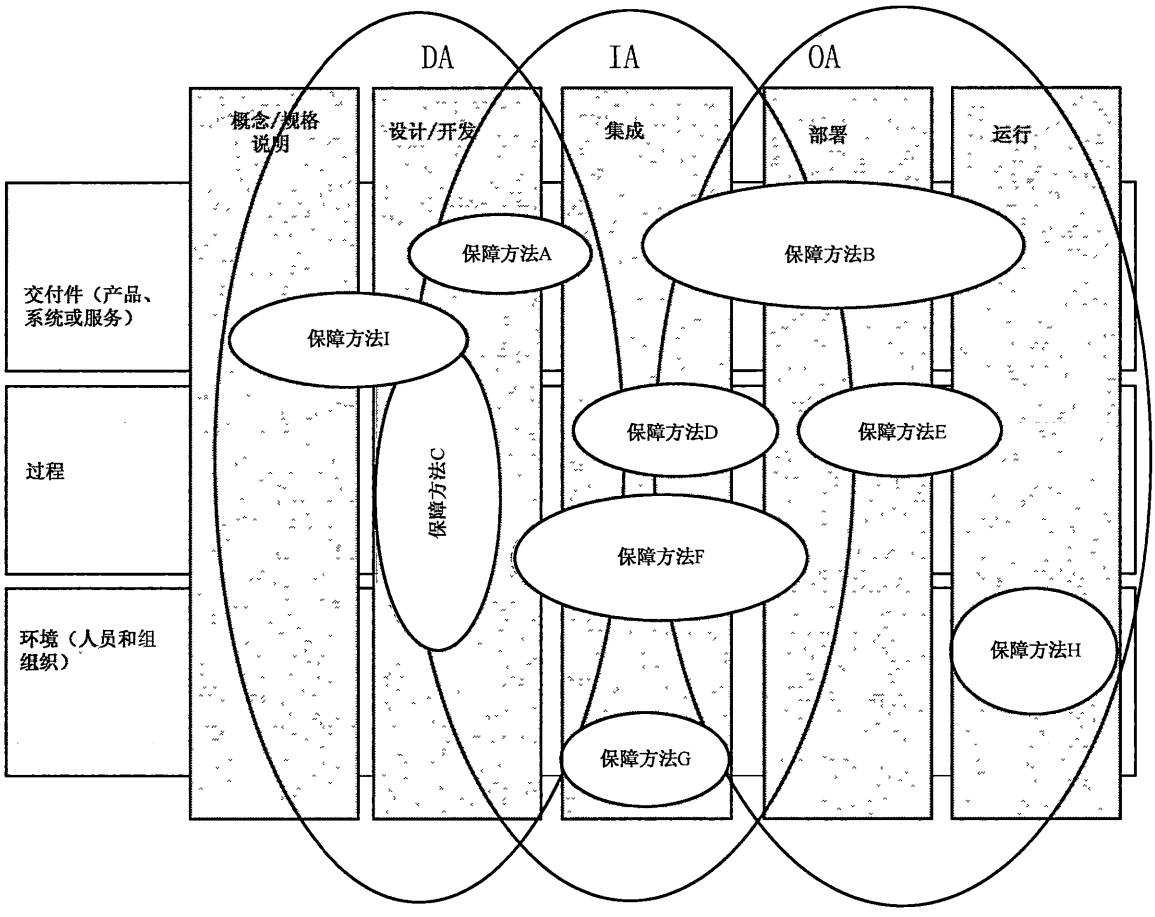

图 5　保障关注

6.1　开发保障(DA)

当在开发一个产品、系统或服务时，可以应用开发保障(DA)。理想地，开发是：

——以一个概念开始的；

——把概念演化为一个规格说明，接之计划开发过程；

——按规约的声明实现一个产品；成功地演示产品所规约的特征；最后在指定的环境中确认其特征。

可以规约保障需求，并可选择适于 DA 需求的保障方法。

6.1.1　保障目标

DA 的保障目标必须予以定义。可选地，可选择/组合可用的方法，如为一个概念阶段提供相应的方法，以便按其要求的精化，定义安全目的。

在 DA 中，安全目的可以是：

——在独一产品情况下，安全目的是一个安全策略；

——在市场化的产品情况下，安全目的是通用于指定用户群的一般性的安全目的。

6.1.2 可用的方法

在 A.2 中给出了一些 DA 可用的保障方法。通过使用第 2 部分，可以选择其他保障方法。

A.2 中的可用方法为 ISO/IEC 15408、ISO/IEC 19790、ISO/IEC 21827、ISO/IEC 27001，以及 ISO/IEC 9000。这些方法的主要方面在附录 B 中给出。

6.1.3 主要问题

对于高的保障需求，必须评估产品安全功能的强度和正确性。因此，所选择的方法就必须包含（或引用，或要补充）确保这些方面的评估过程。

6.1.3.1 强度验证

强度验证是为了确保关键机制，如加密、散列、口令算法等可抵御攻击，特别是蛮力攻击。

6.1.3.2 正确性验证

正确性验证是为了确保从功能需求到系统使用的开发过程步骤均得以正确地进行。因此，正确性验证涉及低层设计（包括实现）是否符合高层设计的评估。这一活动并不关注威胁或涉及的安全目的，而仅关注是否进行了正确的开发。正确性验证与质量验证或质量保证功能紧密相关。

正确性验证是一个过程：证实系统是否符合规格说明，证实低层设计合规格说明是否符合高层设计。这包括检测与需求规格说明的符合性，并可直接检测需求规格说明是否以一种方式给出；正确性验证还既包括测试规程，以及形式化、非形式化的设计分析和验证技术。可应用于正确性验证的严格程度将依赖于不同设计层的精确和无歧义的表达。形式化分析和验证技术需要高精确度的设计表达，从而限制了可用的设计描述方法。特别地，如果想要对系统的正确性获得高的确信度，设计就必须不能存在歧义性。

6.2 集成保障（IA）

当把大量不同的原始产品及其保障结果集成到一个系统中时，通常需要应用集成保障（IA）。

许多产品是一些已成型的、已被证明具有可用保障结果的商业产品，但按用户的期望，这些结果经常是不可使用的。因此，在多数情况中，用户作为一个可部署系统的最终保障机构，必须管理一种复杂的保障状态。

市场上开发一个系统的系统集成方，在这里通常被认为他们仅提供所部署系统的一部分。因此，这一集成方面临的情况并不是十分复杂的，除非负责整个系统的任务。

复杂的集成情况一般要求附加一些其他安全产品或增加一些测量，其目的是，对应所要求的保障目标，实现丢失的保障等级。

复杂的集成情况一般要求附加一些其他安全产品或增加一些测量，以此创建亏缺的可用保障。这一亏缺必须填充，以便达到给定的保障目的。

抽象的或复杂的保障结果，可能必须在运行中予以确认，以便达到必要的信心。

注：在本指导性技术文件中没有涉及系统组合及其保障：尽管每个子系统在测试时可能满足其功能和安全需求，但整个组合系统不一定功能正确和/或安全。组合保障问题可能需要附加的系统测试和验证。

6.2.1 保障目标

IA 的保障目标必须定义。该保障目标可以是：

——在独一系统的情况中：系统安全策略或保护轮廓（PP）；

——在市场化系统的情况中：适用于指定用户群的一般性通用安全目的，可能以 PP 形式；

——在非常复杂的用户系统情况中:事先存在的组织安全策略。

可选地,可选择/组合一些可选的方法,例如提供概念阶段,允许按要求的精化来定义安全目的。

6.2.2 可用的方法

在 A.2 中给出了一些 IA 可用的保障方法。通过使用本指导性技术文件的第 2 部分,也可以选择其他保障方法。

A.2 中的可用方法为 ISO/IEC 21827 以及 ISO/IEC 9000。

注:当前的 ISO/IEC 19791 可增加到可用 IA 的方法列表中。但是,在本指导性技术文件中没有提供相关的指导。

6.2.3 主要问题

6.2.3.1 组合方法的使用

市场上复杂产品的集成方,对应具有一定严格程度和完备性的保障目的,可能需要应用多个保障方法,以便获得相应的保障结果。

通常,该集成方应自由地选择可用的保障方法。有关当前和未来产品的即时成本和未来成本,将影响这一选择,以及客户的期望和市场因素。

这样产生的保障包应是所选方法结果的组合。

方法的选择可以基于该方法的保障特性分析,如在本指导性技术文件的第 2 部分中所表达的。本部分的目标是比较这些方法的主要特性(feature),这些特性对实现集成方的需要具有正面和负面作用。

6.2.3.2 各种保障结果使用

IA 意味着要把多个产品(通常是一批产品)作为部件集成到最后可运行的和/或可部署的系统,并把各产品的保障集成到这一系统的保障包中。

为了创建这一保障包,集成方需要:

——编辑事先存在的、来自多个源的相同或类似方法的保障;

——转换并调和源于不同保障方法的保障;

——解释不确定的保障结果;

——集成以上所有结果。

该保障结果应需要在建立安全目的的情况和在以后保障评价执行情况下的语境中予以评审。

必须明确地给出限制条件,以避免该包所提供的保障不当地用于不期望的目的。

最终的保障结果应必须是有信心的,即在所关注的情况下使用,“该系统就是安全的”。

6.2.3.3 保障的比较和集成

有关集成系统保障结果的高确信度,与综合理解每一个保障部件的保障过程构成基本元素是有关的,这些保障过程构成元素包括:

——导引保障的输入;

——与保障方法相关的理由和概念;

——所关联的保障结果。

如果把每一保障方法认为是一个“黑盒子”,只通过输入和以后输出的评估来比较保障结果,那么只能获得不大的信心。

如果只考虑它们本身所具有的保障结果,那么只能获得最低的信心。然而,这对于小型组织或对于低资产风险的系统而言,可能是唯一的选择。

6.2.3.4 保障结果的组合

大多数保障结果是不可直接比较的，但必须予以排序。

方法或是严格的或是不太严格的，这样就有相关的一些保障结果：

——严格的保障方法一般基于一种特定的方法学，产生可测量的、可重复的结果，尽管这些结果可能是经验的，并是该保障方法本身所独有的；

——不大严格的保障方法通常缺少一种特定的方法学，不可能重复相同的结果。这样的结果（例如所估算的组织声誉）可以被认为是“模糊的”、主观的。

仅当保障结果来自严格保障方法的情况下，组合结果才能“浓缩”为调整后的尺度。大多数严格方法包括某些形式的保障尺度，尽管该尺度仅可能包含一个单序，即“通过或失败”这一结果。通过分析，可以标识严格保障方法尺度之间的一个关注点或相关性，并在适当调整之后组合这些结果。

当保障结果来自不大严格保障方法并混杂一些来自严格方法的结果的情况下，组合结果就可能是很复杂的，并具有一定的感性和主观性，因此这样的组合结果是具有质疑的或具有问题的。

6.2.3.5 保障结果的组合

特别地，当面临一些来自不大严格方法的结果且组合有困难时，保障结果可以以一种有根据的方式予以组合。

组合保障结果的基本原则是，确保：

——收集支持性的保障结果；

——所收集的所有支持性保障结果有助于形成或增强所期望的组合结果；

——没有一种保障可严重弱化其他保障的作用。

在否定性保障结果的情况中，就有关一个保障源或其他源的使用，必须做出有根据的决定。这可能是困难的，除非所使用的根据与该结果紧密相关并了解之。

保障组合应受限于一个准确的期望用法和意图。这一限制应明确描述，以便避免该保障包不当地用于不期望的意图，如图 6 所示。

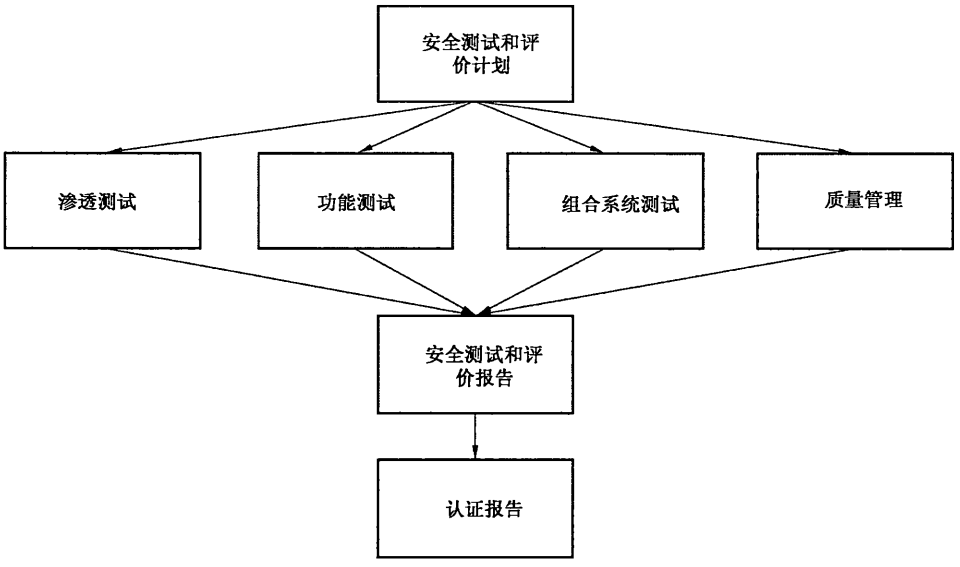

图 6 系统测试和评价

6.2.3.6 保障确认

IA 可能包括 ICT 产品从供应商到用户的过渡性保障，即从开发/集成到运行的过渡保障。

保障确认活动的意图是：在系统表明符合其规格说明之后，标识其尚存的关键性安全问题。

安全需求可以作为高等级的目的予以规约，这样的目的不总是可直接转换为精确的工程需求，因此通过一般性的正确性验证活动不能表明与其符合性。

保障确认仅是证明安全功能有效性的手段，并涉及系统的副作用，或一些没有涉及或不适合的方面。

保障确认通常包括脆弱性评估、渗透测试、隐蔽通道分析、安全功能强度分析、无效使用分析、失效假定确认和健壮测试等。

6.3 运行保障(OA)

OA 出现在使用一个 ICT 系统的地方，其中在一种定义了一般性安全环境中(包括人员和设施)，主动进行 ICT 安全管理。

保障机构通常面对一个可运行的系统，支持组织的业务操作。许多产品是现成可用的，并在大多数情况中，保障机构必须管理一个复杂的保障情况。因此，任何指导必须考虑附贴于每一部件的大量事先存在的保障特性或一些不确定的保障特性。这一情况一般要求附加一些安全产品或要求增加一些度量，以便按所要求的保障目标弥补其中缺失的保障。

6.3.1 保障目标

OA 的保障目标必须予以定义。可选地，可选择/组合可用的方法，如为一个概念阶段提供相应的方法，以便按其要求的精化，定义安全目的。

在 OA 中，安全目的可以是：

——在大型组织的情况中，安全目的是一安全策略；

——在小型组织的情况中，安全目的是适用于指定用户群的通用安全目的，例如一个基线；

——在任意其他特定情况中，安全目的是通过风险分析所获得的安全目的。

为了满足实际需求(即需要不同硬件、软构件、安全服务、环境等方面或这些项的组合)，运行阶段的保障指导需要适合由多个项组成的复杂系统。

6.3.2 可用的方法

在附录 A.2 中给出 OA 一些可用的保障方法。通过使用第 2 部分，可以选择其他保障方法。

附录 A.2 中的可用方法为：ISO/IEC 27001、COBIT、IT 基线手册以及 ISO/IEC 9000。

这些方法的主要方面已在附录 B 中详细给出。

6.3.3 主要问题

6.3.3.1 安全域

可能涉及大量安全域，其中某些安全域具有遗传特质，但一直频繁使用(参见表 8)。这些安全域可

能具有安全目的和度量目录。必须要做的是,确保按当前的风险分析,覆盖这些安全域。

表 8 安全域

安全域
行政管理上和组织上的安全
人员安全
物理和环境安全
硬件安全
软件安全
运行安全
沟通安全
传送安全
密码安全
辐射安全
网络安全

6.3.3.2 安全管理域

表 9 给出了扩展所列安全域的一个例子。按表 9 可以对一些可用的方法作一映射,以检测是否准确详细地覆盖了所要求的安全域。

表 9 安全管理特性

域	COBIT 域	过程
规划和组织	P01	定义战略性 IT 规划
	P02	确保符合外部需求
	P03	管理人力资源
	P04	沟通管理目标和方向
	P05	管理 IT 投资
	P06	确定技术方向
	P07	定义 IT 组织和关系
	P08	定义信息架构
	P09	评价风险
	P010	管理项目
	P011	管理质量
需求和实现	AI1	管理改变
	AI2	安装和鉴定系统
	AI3	获取并维护技术基础设施
	AI4	开发和维护规程
	AI5	获取并维护应用软件
	AI6	标识自动化方案

表 9（续）

域	COBIT 域	过程
交付和支持	DS1	管理运行
	DS2	管理支持设施
	DS3	管理数据
	DS4	管理问题和事件
	DS5	管理配置
	DS6	帮助并忠告客户
	DS7	用户教育和培训
	DS8	标识并分配成本
	DS9	确保系统安全
	DS10	确保持续性服务
	DS11	管理性能和能力
	DS12	管理第三方服务
	DS13	定义并管理服务水平
监视	M1	提供独立审计
	M2	获得独立评价
	M3	评价内部控制精度
	M4	监视过程

6.3.3.3 运行保障成熟度

一个组织安全策略的实施，可能需要进行必要的成熟度测量。表 10 给出了 OA 成熟度等级的一个例子。OA 成熟度的认证将增加保障的值。

表 10 整个 OA 的成熟度

OA 成熟度等级	描述
1	存在所有特定的或一般性的策略
2	特定的或一般性的风险已予管理并接受
3	度量已予定义、实现并管理
4	度量已予评估、修订和维护
5	度量和维护已予认可

附 录 A
（资料性附录）
列表比较

本附录的内容是根据可以公开获得的材料予以改编的。

A.1 方法及其针对的目标

为了标识一些可选方法，给出一个概括性的方法列表。该列表突出表征保障方法的如下方面（见图 A.1）：

——它们是否更集中于技术方面或组织方面；

——它们是否更可使用于产品或系统；

——它们是否更针对供应商或用户。

表 A.1 方法和目标用户群

关键词 P:首要目标群体 S:次要目标群体 X:其他组织		ISO/IEC 15408	ISO/IEC 19790	ISO/IEC 21827	ISO/IEC 13335	ISO/IEC 27001、ISO/IEC 27002	IT安全基线保护	COBIT	ISO 9000
公司类型	硬件供货商		P	P	S		S		X
	软件供货商		P	P	S	S	S		X
	网络提供方		S	P	S	S		S	X
	服务器操作人员		S	P	S	P	P		X
	内容提供方			P	S	P	P		X
	企业用户		S	S	P	P	P	P	X
公司内部角色	管理部门				P	P	S	P	P
	项目管理部门		P	P	P	P	P	P	P
	信息安全官		P	P	P	P	P	S	S
	IT 管理部门		S	P	P	P	P	P	S
	管理员		S			S	P	S	S
	审计员				S	S	S	P	S

基本认证模式

为了保障结果的评估，一些保障方法是与认证模式相关联的，参见表 A.2。

表 A.2 基本认证模式

保障途径	评估准则	评估方法	人员和/或设备合格评定	评估模式
产品	ISO/IEC 15408	ISO/IEC 18045	合格评定?	国际互认的国家认证实体
过程	ISO/IEC 21827	SSAM	SSO	国家/国际认证实体,例如:ISSEA
环境(IT 运行)	ISO/IEC 27001		ISO/IEC 27006	
环境(组织)	ISO 9000		国家/国际认证实体	国家/国际认证实体

A.2 可用的保障方法

针对用户的关注(开发保障,集成保障以及运行保障),附录 B 中给出的保障方法及其对应的保障途径如表 A.3 所示。

表 A.3 可用保障方法

	可发保障	集成保障	运行保障
产品保障	ISO/IEC 15408 ISO/IEC 19790		
过程保障	ISO/IEC 21827	ISO/IEC 21827	ISO/IEC 27001 COBIT IT 基线
环境保障	ISO/IEC 27001 ISO 9000	ISO/IEC 27001 ISO 9000	ISO/IEC 27001 ISO 9000

附 录 B
（资料性附录）
所选方法的保障特性

本附录的内容是根据已公开可用的材料予以改编的。

B.1 ISO/IEC 15408

ISO/IEC 15408 源于通用准则(CC),并与 CC 是紧密相关的。有关 ISO/IEC 15408 方法学的基本内容已在它的第 1 部分中予以描述。

在 ISO/IEC 15408 中,在“评估对象”(TOE)中定义了评估边界。这一 TOE 是非常认真定义的,并表达了一个产品的安全功能。

TOE 并不一定描述了一个完整的产品。但为了可读性和简单性,在这一节中把 TOE 称为“产品”。

B.1.1 保障目标

ISO/IEC 15408 允许在独立的安全评估之间进行比较。为此,该标准针对一组产品的安全功能和安全评估期间应用于这些产品的保障度量,提供了一个通用需求集。该评估过程可建立以下问题的确信度:这些产品的安全功能以及应用于这些 IT 产品的保障度量满足这些需求。该评估结果可以帮助用户确定这些 IT 产品是否实现了它们的安全要求。

ISO/IEC 15408 作为一种指导,可用于一组具有 IT 安全功能产品的开发、评估和/或生产。

该标准强调了信息保护,免遭未授权的泄露、修改和不可使用。与这三类安全失效相关的保护种类,分别称为保密性、完整性和可用性。该标准还可以应用于这三类 IT 安全之外的其他方面。该标准可用于人为活动所引发的风险(恶意的或其他),并可用于非人为活动所引发的风险。ISO/IEC 15408 可应用于 IT 的其他领域,但并没有声称在这些领域的能力。

ISO/IEC 15408 可应用于硬件中、软件中或固件中所实现的 IT 安全功能。

B.1.2 目标受众

关注 TOE 安全特性评估的人群有三种,即用户、开发人员和评估人员。他们被认为是 ISO/IEC 15408的基本用户。

B.1.2.1 用户

用户可能使用评估结果来帮助他们决定一个产品是否满足其安全要求。这些安全要求通常被定义为风险评估结果和策略方向。用户还可能使用评估结果来比较不同的产品。该标准为用户,特别是为感兴趣的用户群和用户团体,给出了一种独立实现的、称为 PP 的结构,其中表达了他们的特定安全需求。

B.1.2.2 开发人员

该标准期望支持评估人员准备并帮助他们进行产品评价,帮助标识这些产品要满足的安全需求。这些需求包含在独立实现的、称为 ST 的构造中。这一 ST 可能基于一个或多个 PP(以前讨论过的用户安全需求)。

因此,该标准可以用于确定支持证据的责任和动作,而这些证据必须按这些需求来支持产品的评

价。该标准还定义了这样证据的内容和表达。

B.1.2.3 评估人员

ISO/IEC 15408 包含评估人员当形成有关产品是否符合他们安全需求的断言时所使用的准则。ISO/IEC 15408 描述了一组一般评估人员所承担的动作，以及执行这些动作所涉及的安全功能需求(SFR)。**注意**，ISO/IEC 15408 没有规约执行这些动作所遵循的规程。

B.1.2.4 其他群体

该标准还可以作为参考资料用于所有关注或承担 IT 安全责任的组织，其中可以获得益处的一些组织包括：

——系统管理员和系统安全官员；
——审计员，包括内部审计和外部审计；
——安全架构人员以及负责产品安全特性规约的设计人员；
——负责接受用于一个特定环境中 IT 解决方案的认证人员；
——负责要求并支持一个评价的评价出资方；以及
——负责管理并监督 IT 安全评价程序的评价机构。

B.1.3 特性

通过在开发、评估和运行过程期间所采取的动作，可以获得 IT 安全的信心。产品是通过 ST 予以规约的。设计信息是通过非形式化、半形式化和形式化等形式提供的。

在 ISO/IEC 18045 通用评估方法学(CEM)的条款中，提供了有关保障的详细测试指导，其目的是为了确保一致地执行一个评价，提供可重复的结果。

在 ISO/IEC 15408 范围之外形成了一些正式的评估模式，以便管理和监督由独立测试组织所做的评价活动。

B.1.4 多功用性

ISO/IEC 15408 给出了一组功能需求和保障需求，这些需求可被用户选择以适应他们的需要。ISO/IEC 15408 包含 7 个预先定义的保障包，即 EAL1～EAL7，以便支持用户的选择和市场认知。

B.1.5 适时性

一组安全保障方法是相对稳定的并且是很少予以修改。以前的安全准则(TCSEC，ITSEC 等)已被 ISO/IEC 15408 所替代，第一个版本发布于 1999 年，当前版本发布于 2005 年。

B.1.6 完备性

完备性是在 ST 中予以规约的。

B.1.7 实现成本/工作量

为逐渐增大保障的一个准则，规约了相应的成本/工作量。

为一个评估所耗费的时间长短，可能依赖于一些因素，包括：

——复用以前工作的能力；
——开发组织的成熟度；
——产品的成熟度，以及实验室的经验；
——所采用的评价策略。

正式评价的成本包括：

——模式费(各模式是不同的)；

——实验费(各实验室是不同的)；

——相互交流的内部工作以及评价人员所要求的最小修改；

——ST 开发。

另外还有：

——几乎需要由开发人员来编制的一些文档；

——评价过程一般不涉及产品中的脆弱性，但这些脆弱性需要予以纠正，其范围从最小到非常严重。

B.1.8 工具支持

在商业市场上仅存在几个可用的工具。一些支持文档是可用的，例如 ISO/IEC 15446“PP 和 ST 生成指南”。

B.1.9 密码问题

正式的评价并不包括所选密码算法的质量评估。但是，所选算法的实现是否正确是可评估的。

B.1.10 评估与认证

为满足 ISO/IEC 15408 的需求，使用合适方法学的评价可由测试实验室予以承担。例如，使用由 CC 管理委员会所规约的评价模式；该实验室必须按 ISO/IEC 17025 予以认证，并且测试结果是发布了一个确认报告并授予一个认证许可证。这样的认证结果是由认可认证机构(国家模式)签署的并在国际上发布。

更详细的信息可参见 http://www.commoncriteriaportal.org。

B.1.11 可信赖性和认可

ISO/IEC 15408 是国际标准，对应 CC 开发委员会发布的 CC 标准。

ISO/IEC 15408 以及 CC 均被认可并具有很强的可信赖性。

B.2 ISO/IEC 19790

B.2.1 保障目标

“加密模块安全要求”，最初由美国国家标准和技术研究院(National Institute of Standards and Technology，NIST)发布为“联邦信息处理标准(FIPS)140-2”，着眼于加密模块的规范。1995 年 7 月，NITS 与加拿大通信安全机构(Communication Security Establishment，CSE)一起，创立了相关的加密模块检验程序(Cryptographic Module Verification Program，CMVP)。该程序通过测试，在 FIPS 140-2 中补充了“FIPS 140-2 实施指南文档”和“FIPS 140-2 派生测试需求”，用于支持和解释测试和检验过程的标准。

CMVP 的网址是 http://csrc.nist.gov/cryptval。

在国家实验室自愿认可程序(National Voluntary Laboratory Accreditation Program，NVLAP)和加拿大标准理事会(Standards Council of Canada)的认可下，实验室对这个标准进行了符合性测试。到目前为止，NVLAP 授权了在美国、英国和德国的 12 个实验室。CMVP 复审了符合性测试的结果，在复审通过后，对测试的加密模块进行生效并颁发了验证证书。现在，650 个以上的证书已经为 1 000 个以上的验证模块所拥有。

FIPS 140-2 要求的一个子集于 2006 年作为国际标准 ISO/IEC 19790 发布。

B.2.2 目标受众

ISO/IEC 19790 可用于加密模块，FIPS 140-2 则被美国政府强制用于每个模块。其他组织或者政府也明确了它的使用规范。

B.2.3 特性

该保障方法使用一致性测试途径，主要应用在下面 11 个领域：

a) 加密模块；
b) 端口和接口；
c) 角色、服务和身份认证；
d) 有限状态机模型；
e) 物理安全；
f) 系统环境；
g) 密码密钥管理；
h) 自测试；
i) 保障设计；
j) 缓解其他攻击。

B.2.4 多功能性

不同的测试域构成了一个四层的 1-4，每一层在另一层之上。ISO/IEC 19790 根据一个特定的加密模块进行测试，如果有些东西进行了修改，测试就要重新进行。CMVP 对多种维护验证的方法提供了规划指导，这些方法根据变化的性质来提供及时和成本有效验证维护（见图 B.1）。

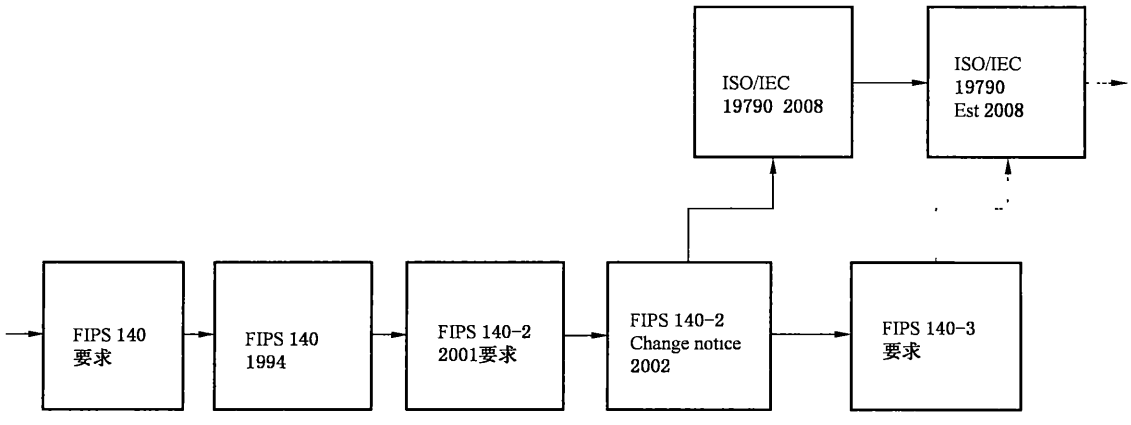

图 B.1 测试需求演进

B.2.5 适时性

B.2.6 完备性

一致性测试要保证加密模块尽可能符合加密模块的规范（ISO/IEC 19790）。

派生测试需求（Derived Test Requirements，DTR）和补充规范（Implementation Guidance，IG）用来保证测试的完备性和再现性。

B.2.7 实施的成本/工作量

ISO/IEC 19790 验证的成本包括以下因素：

a) 验证组织的成本(比如 NIST CMVP 成本回收)；

b) 测试实验室成本；

c) 内部劳动成本，如按照验证流程，提供测试要求的二次修改以及撰写规范文档。

由于验证范围较小，ISO/IEC 19790 测试比 ISO/IEC 15408 评估要省时。ISO/IEC 19790 测试的持续时间由以下因素决定：

a) 开发组织的成熟度；

b) 实验室的经验；

c) 验证机构的制约；

d) 产品的成熟度；

e) 一致性评估。

B.2.8 工具支持

在商业市场上仅存在几个可用的工具。NIST 提供的支持文档和工具箱在以下网址上可用：http://csrc.nist.gov/cryptval。

B.2.9 密码问题

该保障方法专门为加密模块(包括算法)定义。安全模块要获得批准，必须在加密算法验证程序(Cryptographic Algorithm Validation Program，CAVP)下得到独立的验证和认证。同时，NIST 为 NVLAP 认证测试实验室提供算法测试工具。

B.2.10 评估和认证

NIST 与 CSE 合作，引入了北美的鉴定机制——CMVP。

B.2.11 可信赖性和认可

ISO/IEC 19790 来源于 FIPS 140-2，美国政府通过国家标准局(NIST)公布了它的规范。为了保护敏感的非加密数据，该规范要求安全产品中嵌入加密设备。加密模块通过了一致性测试和其他程序要求后才被认证。

B.3 ISO/IEC 21827

B.3.1 保障目标

ISO/IEC 21827 的目标是为组织使用者定义的系统安全工程过程提供保障。

B.3.2 目标受众

该保障方法涵盖开发保障和集成保障，因此目标读者包括开发者和集成商。

B.3.3 特性

该保障方法使用过程保障途径。

B.3.4 多功用性

ISO/IEC 21827 重点强调了和过程成熟度有关的五个能力等级，由组织根据其首要目标决定。

B.3.5 适时性

ISO/IEC 21827 由前期 ISSEA 在 1994 到 2001 年间的工作成果发展而来。2001 年，ISO/IEC 根据 ISSEA 的“公共可用规范”(Publicly Available Specification)发布了 ISO/IEC 21827。2005 年，该标准开始进行修订，2007 年修订完成。

B.3.6 完备性

ISO/IEC 21827 涵盖了五个等级的能力要求，包括各个方面的安全工程准则。ISO/IEC 21827 的结构按过程的实践组织起来，允许用户根据过程灵活运用在自身的组织结构中。

B.3.7 实施的努力/成本

ISO/IEC 21827 评估的主要成本发生在第一次项目中。额外的项目中使用相同的方法的成本是该初始成本的一部分。可以通过使用内部评价者，减少这个成本。通常，不需要提供具体的文档。

如果投入了必需的人工(work-force)，该评价过程会很短，持续 2 到 3 周。

B.3.8 工具支持

有许多电子表格工具可用于追踪评估和总结的结果，并给出这些结果。

B.3.9 密码问题

无特殊要求。

B.3.10 评估和认证

培训和资格认定系统都可以评估本方法。

B.3.11 声誉和认可

ISO/IEC 21827 机制通过评估团队(Appraisal Team)规定了评估。

SSE-CMM 支持组织(SSE-CMM Support Organization，SSO)提供了专业的 ISO/IEC 21827 评估疏导员(facilitator)和团队，帮助组织评估它们的安全工程能力。其提供下面的服务：

a) ISO/IEC 21827 评估疏导(Appraisal Facilitation)；

b) ISO/IEC 21827 评估；

c) ISO/IEC 21827 后续审计；

d) 安全工程过程改进计划(Security Engineering Process Improvement Plan)。

与 ISO/IEC 15408 或者 ISO/IEC 19790 相反，ISO/IEC 21827 没有官方的、政府的、代理来保障该机制。

B.4 ISO/IEC 13335

B.4.1 保障目标

该保障由以下部分组成：

ISO/IEC 13335-1 发布为“技术报告”(Technical Report，1996 年、1997 年和 1998 年分别发布了第

1 部分、第 2 部分和第 3 部分，2000 年和 2001 年分别发布了第 4 部分和第 5 部分）。第 1 部分为“IT 安全的概念和模型”，定义了与 IT 安全和基本方面（威胁、风险、弱点，等等）以及过程（如应急计划、风险评估、提高认识）相关的基本术语。该部分面向组织内的责任经理和安全官员。第 2 部分，“IT 安全管理和规划”为 IT 安全过程的设计及其集成在现有企业的过程提供了信息，并建议了一个 IT 安全组织。第 3 部分，“IT 安全管理技术”提炼了 IT 安全过程的步骤，并为能用于此目的的方法和技术提供信息。最后，第 4 部分，“安全措施的选取”提供了针对某种风险，该选择何种安全设施何以及如何处理的信息，比如，如何为一个组织确定合理水平的基线保护。第 5 部分，“网络安全管理指导”提供了在没有特定解决方案的情况下的安全管理建议。

ISO/IEC 13335 的第二版分别修订成两部分的国际标准：ISO/IEC IS 13335-1 在 2004 年发布，它取代了 1996 年的 ISO/IEC TR 13335-1 和 1997 年的 ISO/IEC TR 13335-2。ISO/IEC IS 13335-2 将取代 ISO/IEC TR 13335-3 和 ISO/IEC TR 13335-4。ISO/IEC TR 13335-5（网络管理）将融合进ISO/IEC 18028-1。

该保障将把 ISO/IEC IS 13335-2 更名为 ISO/IEC IS 27005。

B.4.2 目标受众

该保障方法涵盖了运行保障。

其主要的目标群体是企业或组织内的管理者，这些人直接参与 IT 安全过程的规划或实施，为此，根据它们的相关性每一部分都有不同：

——第 1 部分针对管理委员会级别的管理者，尤其是那些负责企业范围的 IT 安全程序（programme）的人；

——第 2 部分针对那些负责企业内的 IT 系统的管理者，或者那些负责领域与 IT 的使用紧密相关的人；

——第 3 和第 4 部分针对所有那些在项目的生存周期的各个阶段里不得不处理 IT 安全的人。

这些技术报告可以为所有的机构使用，不管它们的最初的结构。不过，这些报告针对的是考查、修改（如果需要）必需的 IT 安全过程的结构。为此，所提供的信息独立于现有结构的复杂度以及目标安全水平。

B.4.3 特性

该保障方法使用环境保障途径。标准的各个部分都没有规定具体的过程和解决方案，但是，这些部分包括了如何运用这些内容以适应企业的建议，并建议了什么方法和模型是可用的。这些文档不用于度量 IT 安全水平，并且不以任何方式显示与标准的一致性。

B.4.4 多功能性

在原则上，这些报告通常不得不适应于机构及其 IT 基础结构或项目的具体的特殊性，并且这些报告也是可适应的。该标准的不同部分，为从管理委员会级别到项目级别的人都提供了建议。实际上，这些过程和流程只能在中等规模或者大规模的机构中完全实施。然而，作为指南，这些报告具有普遍的使用性。

B.4.5 适时性

ISO/IEC IS 13335 近期已经发布或正在发布中，不过，在可预见的将来，ISO/IEC IS 13335 的本质内容不大可能要求更新。

B.4.6 完备性

这些报告关于组织和 IT 安全过程的构件的描述是完整的。但是它们只为这些过程的定义和组织

内的结构给出了指导，并没有规范 IT 安全水平，因为这个水平的确定只发生在该保障方法所创建的组织和过程内。

B.4.7 实施的成本/工作量

在企业内引入和维护 IT 安全过程的成本依赖于现有的组织结构，并且不能在管理委员之间进行规定。相同考虑还适用于 ISO/IEC 27002。

B.4.8 工具支持

该保障方法的工具支持并不显得有利。关于 IT 安全管理形式的管理决定不依赖于度量标准。

B.4.9 密码过程

密码在措施水平上进行考虑。该保障方法未规范密码过程的要求；相反地，尤其是在密钥管理方面，引用了 ISO/IEC 11770-1。

B.4.10 鉴定和认证

不提供认证，而且它显得不合适进行认证。

B.4.11 信誉和认可

认可为国际准标准。

B.5 ISO/IEC 27001 和 ISO/IEC 27002

B.5.1 保障目标

ISO/IEC 27001 和 ISO/IEC 27002 的目的，是为信息安全管理的“最佳惯例”提供需求。ISO/IEC 27002为信息安全控制提供指导，而 ISO/IEC 27001 明确了信息安全管理系统的要求。

考虑的主要内容有计划、实施、操作和提高信息安全管理系统。其他相关的内容有识别和风险评估，以及选择合适的控制目标并进行控制。

B.5.2 目标受众

ISO/IEC 27001 和 ISO/IEC 27002 针对各种规模的企业和机构，但不针对私人用户。此外，该标准可以用于审计和认证行业的服务公司。

该标准的目标受众有：

a) 负责确保信息足够安全的管理人员；

b) 负责选择和实施 IT 安全措施的人员，比如 IT 安全官员、IT 领导人；

c) 负责监视的人员，比如内部和外部的审计人员；

d) 外部的股东，比如依赖组织信息安全措施的客户或供应商；

e) 信息安全管理系统认证机构。

标准的适应性很大程度上取决于组织的结构。以管理为导向的方法与不限制适用到特定技术系统或系统类型。

B.5.3 特性

该保障方法使用了过程保障方法，主要有以下步骤：

a) 建立信息安全管理系统；
b) 实施和运行信息安全管理系统；
c) 监控和审查信息安全管理系统；
d) 维护和改进信息安全管理系统。

ISO/IEC 27001 覆盖了和这些步骤相关的文档、管理责任、内部信息安全管理系统审计、信息安全管理系统的管理审查以及信息安全管理系统的改进的要求。

基于 ISO/IEC 27002，ISO/IEC 27001 包含了控制信息安全风险方式的要求。

该标准可以用在多个方面。首先，ISO/IEC 27002 可用作有关规范的具体指导的参考，也可用于个人控制。其次，ISO/IEC 27001 可用于实施一个顶尖的信息安全管理系统。再次，ISO/IEC 27001 和 ISO/IEC 27002 联合起来可用于实施一个可被独立认证机构认证的信息安全管理系统。

B.5.4 多功能性

ISO/IEC 27001 和 ISO/IEC 27002 可明确用于任何规模的机构，也可用于机构的各个可识别的子部门。如果一个机构有多个信息安全管理系统，它们覆盖了不同的范围（比如覆盖机构的不同子部门），将不能自动得知整个信息系统的安全性。但是，如果知道每个信息安全管理系统的文档，也可以判断和决定信息安全的方法是否符合整体目标。

B.5.5 适时性

ISO/IEC 27001 和 ISO/IEC 27002 是成熟的、完整的标准。与修改 ISO/IEC 标准的常规方法一致，该标准计划进行规律的更新，这些更新也会保持一致性。

B.5.6 完备性

ISO/IEC 27001 和 ISO/IEC 27002 主要面向组织管理严密的（top-down）途径，并且主要包括一般的标准安全措施。这些措施涵盖了目前所有的相关的领域。该标准不包括任何面向产品的措施，以及只是高度聚合的面向技术的措施，因为通常这些措施最多包括只是中等数量的细节。

一般情况下，ISO/IEC 27001 和 ISO/IEC 27002 不局限于一个具体的安全水平；但该标准所建议的措施却是针对基线安全途径，并且这些措施经过修改后只适合于较高到最高的安全水平。然而，面向管理的途径也为这些安全水平提供了支持。

如果 ISO/IEC 27002 中的控制项有排除的理由，ISO/IEC 27001 可以允许排除，比如说这些控制项与范围内的活动无关，或者如果相关的安全风险不需要处理。为了适合更小的企业，该标准可以进行修改。

B.5.7 实施的成本/工作量

由于该标准对组织措施的强调，使得实施所要求的努力严重依赖于机构的一般的组织质量。没有很好地组织的机构相比于组织一般或过度组织要求更多的努力。

基线安全途径通常使得不需要付出额外的成本就可以使用企业现存的措施，从而以一种最优的方式增加安全水平。

进行分析的努力很大程度上由风险分析的范围确定。风险分析类型的选择对于所要求的努力的量有主要的影响。

ISO/IEC 27001 认证的成本与 ISO 9000 认证具有相同的量级。

值得注意的是，认证的成本需要从实施信息安全管理系统中独立出来考虑。这样的成本依赖于组织的规模、所采取活动的本质以及遇到的威胁。一般不可能对这些成本作出一般化的评价。

典型地，评估要跨越一段时间，因为实施 ISMS 的不同方面或者矫正问题时有一些间隙。典型地，

评估跨越 3 到 12 个月的时间。

B.5.8 工具支持

ISO/IEC 27001 和 ISO/IEC 27002 可以得到工具的支持。使用特定的工具,ISO/IEC 27001 可用于风险评估,还可以对所需的文档和记录进行改进和维护,以及对目标用不同实施控制进行比较。

B.5.9 密码过程

ISO/IEC 27002 中的加密,规定了加密控制和密钥管理实践上的方针。由于标准的本质,该标准未对具体的产品进行建议。

B.5.10 鉴定和认证系统

ISO/IEC 27001 已经发展到允许独立认证机构进行认证。ISMS 的独立认证有效期为几年(通常是 3 年)。在此期间,每 6 到 12 个月要进行一次监制审计。如果不符合的地方很严重,同时/或者没有及时纠正,认证就要被撤销。最近正在改进中的 ISO/IEC 27006,规定了认证机构被认可的要求。

B.5.11 声誉和认可

许多国家的和区域性的认证服务提供独立的保障,即 ISO/IEC 27001 认证机构遵循合理的过程、雇佣有能力的职员并得到一致的结果。这些鉴定机构包括了是英国的 UKAS,以及澳大利亚和新西兰的 JASANZ。

国家的和区域性的认证服务,通过类似于欧洲认证合作(European Co-operation on Accreditation,EA)和国际认证论坛(International Accreditation Forum,IAF)的团体的成员关系在国际间进行合作。这些区域性的和国际性的协会确保国际间认证活动的一致性。

B.6 IT 基线保护指南

B.6.1 保障目标

IT 基线保护指南(IT Baseline Protection Manual)提供了标准的安全措施,着眼于为 IT 系统确立预先确定水平的安全。该水平还作为具有更严格安全要求的领域的起点。为此,IT 基线保护指南包括了下列每一个领域的一系列标准的安全措施:基础设施结构(infrastructure)、组织、职员、硬件和软件、通信和应变规划。其中的途径涵盖了下面的活动:IT 结构分析、保护要求的评价、建模、基本的安全检查、增补安全分析以及 IT 安全措施的实施。

B.6.2 目标受众

该保障方法涵盖了运行保障,以及 IT 服务环境中的产品保障和集成保障。

IT 基线保护指南基本上针对所有规模的机构和企业,但是不针对私人用户。为了更清楚地向负责的雇员指明标准的安全措施,其每一个安全措施的文本都以谁负责发起和实施所讨论的安全措施的信息为开始。对于每一种情况,都指明了机构或企业内的一个或者多个角色。这些角色的例子是 IT 部门的头领、IT 安全官员、人力资源、消防官员、管理者和 IT 用户。

基于 IT 基线保护指南中主要处理的典型的构件,该指南对于在因特网上创建内容或提供内容的服务提供商尤为有用,但是对于纯粹的网络提供商用处则更少。因为 IT 基线保护指南中包括大量的 IT 安全要求,该文档也适合于硬件产品或者软件产品的卖主。然而,软件开发只是略带提到。管理员可以在 IT 基线保护指南中找到全面而详细的技术信息。

由于 IT 基线保护指南遵循考虑典型的 IT 构件的一般途径,它很大程度上独立于企业结构。它适

用于采用了标准的 IT 系统和 IT 应用程序并且安全要求大体上是正规的所有领域。它只包含了有限的具有更高安全要求的 IT 安全措施。

B.6.3 特性

该保障方法使用了过程保障,但在需要考虑运行中的更新时,该保障方法包括了产品保障要素。IT 基线保护指南本质上是面向构件的。取决于所考虑的 IT 环境的构件,用户可从 IT 基线保护指南中选择合适的章节(或“模块”),并用于 IT 环境的建模。其保障途径分成为 5 个层次:更高层次方面、基础设施、IT 系统、网络和应用。

层次 1,更高层次方面涵盖了不能固定于单独的 IT 或基础设施构件的 IT 安全方面,但是这些方面影响较大的领域,甚至是整个 IT 环境。

B.6.4 多功能性

由于 IT 基线保护指南着眼于所考虑的 IT 环境的构件,应用该方面所涉及的努力和成本很大程度依赖于所考虑的 IT 环境的同质性(homogeneity)。IT 基线保护指南的途径包括了一个机制,把相同的构件分为一组,从而没有必要为这些要素单独处理。然而,如果 IT 环境根本不是同质的,那么最坏的情况是努力和成本与构件(IT 系统、IT 应用程序等)的数量成正比。

B.6.5 适时性

每隔两年,IT 基线保护指南进行审查和扩展。为了适应技术内容的发展,这是特别有必要的。基于 IT 基线保护指南的注册用户确定的要求,提供额外的材料。

B.6.6 完备性

IT 基线保护指南包括一般的标准安全措施,还包括具体产品和具体技术的标准安全措施。一般的措施涵盖了 IT 安全所有的重要方面,比如,组织和应变规划。由于 IT 部分不计其数的不同的产品和解决方案,不可避免地,具体的产品和具体的技术的措施只能涵盖最一般使用的构件。

IT 基线保护指南主要面向具有“正常的”安全要求的信息、IT 应用程序和 IT 系统的保护。如果安全要求比这个更高,IT 基线保护指南的标准安全措施需要通过另外的措施进行增补。

B.6.7 实施的成本/工作量

由于标准安全措施面向正常的安全要求,一般不要求成本巨大的服务或昂贵的安全或者基础设施构件。所以,实施这些措施的主要成本是组织的努力和劳动成本。还必须考虑执行 IT 基线保护的分析所要求的努力。这很大程度地依赖于所考虑的 IT 环境的同质性。对于一个中等规模的企业,应当规划至少 3 个月的工作。

B.6.8 工具支持

IT 基线保护指南得到途径(BSI IT 基线保护工具)和内容(USEIT-BSI 工具安全 UNIX 管理)方面的工具支持。

对这些工具的更进一步的开发适应于 IT 基线保护指南的延续。在市场上,还有其他适应于 IT 基线保护指南的途径或者内容的 IT 安全工具。

B.6.9 密码过程

与其他建议类似,使用密码过程的建议也是适应于标准的安全要求。该指南包括了对密码术的基本概念的介绍、使用加密机制的一般建议以及具体产品的建议。

B.6.10 鉴定和认证

目前，正在制定一个鉴定机制，使得权力机构和企业有可能证明它们已经成功实施了 IT 基线保护的事实，这对于外部世界有益。设想有 3 个水平：自我声明的“准入水平(entry-level)”、自我声明的“更高水平”以及实际的 IT 基线保护认证。后者专门由独立的认证权力机构承认。

在 IT 基线保护指南的每一个章节里，清楚地说明了每一个鉴定水平要求何种措施。计划于 2001 年底之前完成鉴定机制。

B.6.11 声誉和认可

IT 基线保护指南是在德国和英国内部可用的国家标准。

B.7 COBIT

B.7.1 保障目标

IT 的密集使用于支持和处理商业相关的业务，使得建立对环境的适当控制变得紧迫。COBIT(信息及其相关技术的控制目标，Control Objectives for Information and Related Technology)由信息系统审计和控制协会(Information Systems Audit and Control Association，ISACA，http://www.isaca.org)制定，作为测试这种限制环境风险发生的控制的完整性有效性的方法。

B.7.2 目标受众

这个保障方法涵盖运行保障。

COBIT 区分下面的目标群体：

a) 管理——当权衡风险和控制措施带来的投资时，进行管理支持；

b) 用户——用于改进的评价的可靠性，以及监视由内部或者由第三方提供的 IT 服务；

c) 测试者——用于测试证据的目标辩护，或者用于建议公司和内部控制的操作；

d) 过程的所有者或哪些负责 IT 的人——支持他们的工作。

COBIT 能用作为独立于内部结构或者企业的法律形式的面向过程的方法。

B.7.3 特性

该保障方法使用环境保障途径。

当使用 COBIT 时，用户一开始就确定何种 IT 过程与具体的情形相关。对于所选取的 IT 过程的每一个控制目标，必须权衡现有的措施能满足要求的程度。

COBIT 区分了 7 个不同的商业要求，并把它们分成为质量、安全和规律性三组：

a) IT 的质量——由所执行的过程的效力和经济决定——在准则、效力和效率中再生；

b) 安全要求的机密性、完整性和可用性等反映在 COBIT 中；

c) COBIT 使用可靠性准则，确保财务报表的可靠性(财务报表要求)以及该准则遵守了内部和外部标准的法律要求。

根据 COBIT，IT 支持的商业过程基于下面的 IT 资源：

a) 数据：广义上的外部的和内部的数据要素；

b) 人工的和程序化的流程的整体称为应用程序；

c) 技术包括硬件、操作系统、数据库管理系统、网络、通信应用程序等；

d) 财产：所有用于容纳和支持信息系统的资源；

e) 职员：与规划、组织、需求、符合性、信息系统和服务的支持和监视相关的知识、意识和生产力。

IT 资源应当以一种受控的方式进行规划、开发、实施、运行和监视。在 COBIT 中，定义了 34 个关键过程，这些过程在决定 IT 管理的成功中扮演重要的角色。这些 IT 资源下的 IT 过程能分成为 4 组主要的领域，形成一个完整的生存周期：

a) 规划和组织；

b) 需求和实施；

c) 运行和支持；

d) 监视。

对于 34 个关键的 IT 过程，COBIT 列出了大致 200 个核心任务。每一个核心任务都指定了必需的 IT 资源；并且基于（质量、安全和规律性的分类）的要求，定义了控制目标。

B.7.4 多功能性

由于 COBIT 的矩阵结构，用户有可能只考虑单独的领域或过程和/或从 7 个商业要求中选择一个子集（比如只选择安全要求机密性、完整性和可用性）。

B.7.5 适时性

COBIT 由信息系统审计和控制基金会（Information Systems Audit and Control Foundation）制定于 1996。在 1998 年，它被扩充并全部重新制定。第 2 个版本为使用 COBIT 提供了材料和软件。第 3 个版本（2000 年发布）发布为“开放标准”。

B.7.6 完备性

COBIT 给出了记录面向 IT 的且附随的过程的方法。相关联的控制目标的定义独立于技术，并且能用于不同的系统环境。然而，为了创建安全概念，必需增加额外的具体系统的措施。

COBIT 针对典型企业的安全利益，考虑了公司基本利益（内部信息和过程的完整性和机密性）的维持以及法令法规（数据的隐私保护、财务报表）的遵守。

COBIT 没有固定的安全水平，面向的是企业目标。

B.7.7 实施的成本/工作量

在 COBIT 下一个中等规模的企业的所有控制目标的完整分析不应当超过一个工作月。

B.7.8 工具支持

COBIT 的使用得到下面工具的支持，其中：

——“COBIT 顾问”，来自新西兰惠灵顿的 Methodware Limited；

——“COBIT 自我评价”，来自于美国认证培训协会（Certification Training Institute，CTI，USA）。

COBIT 的第 2 个版本还包括了有用的背景信息，有助于进行材料的应用和陈述。

COBIT 本身为检查（具体的安全措施）的实施提出了例子。使用这些例子，可以评价单独的控制目标被满足的程度。然而，COBIT 的用户（比如，审计组织）通常使用他们自己的评估机制。

B.7.9 密码过程

COBIT 把密码过程引用为适合于信息的保护和真实性的检验的措施。关于这一点，COBIT 涵盖了对法律要求的遵守，而且，涵盖了加密数据的法律效力方面。

B.7.10 鉴定和认证

在实际意义上不存在 COBIT 认证。然而，该方法通常被许多审计组织使用在账目的年度审计，以

测试 IT 控制环境。IT 测试的结果反馈在年度账的审计报告中。

B.7.11 声誉和认可

COBIT 是一个受国际上主要的会计公司支持的标准。

B.8 ISO 9000

B.8.1 保障目标

ISO 9000 系列的目标是定义一个测试方法，在其中可以规范质量管理系统的要求，且组织必须对该质量管理系统备有证明文件以证明它具有满足客户要求的能力，并使得该能力能被内部的和外部的视察者评价。还要检查组织中的 IT 环境是否满足客户的要求且适应商业目标。

该标准的目的不是暗示质量管理系统的一致性。组织里的质量管理系统的设计和实施受它的目标、客户要求、提供的产品或服务以及过程的影响。

B.8.2 目标受众

该保障方法在相对高层次上涵盖了任何组织内的环境保障。

ISO 9000 中包括的要求是高层次的，并且独立于具体的工业的或经济的部门。它们适用于任何类型和任何规模的组织。

这里，过程的文档有助于组织实现一致性，定义接口以及向每个雇员解释工作常规。

由于集成在管理过程中，该标准的结构 100%可直接适用于企业。该标准适合于 IT 结构用于支持内部过程和/或客户要求的所有领域。而且，由于它们是高于一切的，它们可以应用于所有产品或服务类别，以及每一个工业的或经济的部门。它们还独立于组织的类型和规模。

B.8.3 特性

该保障方法使用环境保障途径。

该标准中包含的要求不强迫企业改变他们的质量管理系统的结构或者强迫他们根据该标准的结构调整他们的文档。

组织的质量管理系统的过程的文档应当以一种适合于他们自己的活动的方式进行确立。

企业的 IT 支持文档集成在质量管理系统的过程环境中，因此，只能在其他管理过程的上下文中才可见。

这里，IT 用于支持内部过程和顾客要求，并且始终应当视作为一个接口。其功能性方面只作为组织其他的备有证明文件的管理过程的函数而存在。

B.8.4 多功能性

由于 ISO 9000 系列标准的 IT 独立于其他管理过程，因此测试所涉及的努力的量依赖于文档的一致和其他过程的功能性。如果生产过程或服务过程或根据客户的要求的 IT 部分非常复杂，那么测试方法将更为深入。不过，由于 IT 过程不可能从其他管理过程中隔离开来，测试的量仍旧是按比例的恒定的(proportionally constant)。

B.8.5 适时性

ISO 9000 中所包含的要求相对稳定并甚少修改。

然而，它们有规律地进行审查，以确保它们是最新的且是可用的。因此，比如，ISO 技术委员会(ISO Technical Committee)发布了一个名为 ISO 9000:2000 的新版本的标准。修订后的版本的标题中

不再含有词语“质量保障”,标准适用的修订领域也是如此。这使得实现满足要求和连续改进的能力的关键之处变得更为清楚。而且,其结果更适合于 ISO 14000 系列标准和环境管理系统。

B.8.6 完备性

质量管理系统的要求主要用于通过满足客户的要求(作为最低要求,通过应用这些要求、连续改进这些要求并且防止错误)实现客户的满意度。因此,这里只有备有证明文件的过程内的 IT 环境的功能性能得到保障。所以,并不宣称对技术本身进行审查,但是宣称对组织内的功能性(比如,偶然性概念、数据隐私保护官员的约见)进行审查。

B.8.7 实施的成本/工作量

把 IT 环境集成在过程环境的相关联费用相对较低。如果所关注的是内部过程和客户要求,那么这里一般不会要求任何成本密集型的服务或安全构件。这里,成本的最大部分反映了劳动和组织把过程集成在过程环境和定义接口的努力。

由于该 IT 过程不能独立于 ISO 9000 文档的整体考虑,对这个子领域要求的努力进行估计是几乎不可能的。

B.8.8 工具支持

这里,何种工具应当集成以便进行支持,很大程度依赖于企业。

所有在市场上可用的工具都可以考虑。

B.8.9 密码过程

与所有其他 IT 环境的过程一样,ISO 9000 适应于组织的商业活动,并适用于该组织的客户要求。因此可能会有较大的差别。

B.8.10 鉴定和认证

按照 ISO 9000:2000 的测试和认证由受鉴定的、独立的团体进行,测试的结果要通过认证的发布来文档化。在许多国家,多个组织可以进行这些认证的发布和发表。

B.8.11 声誉和认可

可能是得到最为广泛认可的国际标准。

附 录 C
（资料性附录）
保障方法的组合

本附录的内容是根据已公开可用的材料予以改编的。

硬件和软件的制造商必须提供具有适于预期目的和设想的运行环境的安全功能产品。按着系统化途径，所建立的保障方法（如 ISO/IEC 15408 和 ISO/IEC 19790）应为此而应用。

就用户而言，必须采取一些步骤，以确保实现了对整个方案的安全运行所必要的一些协调的措施，这包括有效的 IT 安全管理以及适合组织的、职员的和技术的 IT 安全措施。对于这些方面，可应用诸如 ISO/IEC 13335、ISO/IEC 27002 和 IT 基线保护指南等方法。

ISO/IEC 15408 中介绍的 PP 可以作为制造商和用户之间的桥梁。PP 可以能帮助用户准确表达有关安全特征和产品功能的需求。对于制造商而言，他们可以规约一个特定产品所涉及的 PP，并通过一个认证来支持这样的宣称。

经常使用如附录 C 中所给出的方法组合。

C.1 ISO/IEC 15408＋IT 基线保护手册

IT 基线保护手册以及 ISO/IEC 的一些部分可以用于组合。应用在 IT 基线保护手册中所列的标准的安全保证措施，将产生整个系统的基本保护，覆盖了 IT 安全管理以及构件层上的技术措施。但就一般而言，似乎在保护需求的评估期间或在可比的安全分析期间，特殊的安全要求或需求在已建立的一些部分中，单独使用 IT 基线保护手册不可能充分地予以保护。在这里，可以使用 PP 来表明安全需求，并用于选择适当的、尽可能通过合适认证的、并提供必要安全功能的产品。以这一方式，通过组合使用 IT 基线保护手册和 ISO/IEC 15408，就可达到一种合适的 IT 安全水平。

C.2 ISO/IEC 27002＋IT 基线保护

ISO/IEC 27002 关注信息安全的管理，并提供面向过程的途径。其主要的内容是一系列一般性的“最佳实践”措施。为了保护整个解决方案免遭相关的威胁，这些一般性的措施必须通过特定的、有关要采用的动作之上的技术指导以及有关安全措施的技术指导，置入到相关的实践中。在这里，IT 基线保护手册可以提供有用的帮助。IT 基线保护手册包括一系列源自组织、人员、基础设施和技术等领域的详细建议。因此，ISO/IEC 27002 和 IT 基线保护手册的组合可以产生一个严格分离 IT 安全控制和实际实现的途径。另外，在这一场景下，在具有特殊安全要求的子领域情况中，也从 ISO/IEC 15408 和（或）PP 那里得到帮助。

C.3 ISO/IEC 27001＋ISO/IEC 27002

ISO/IEC 27001 规约了信息安全管理体系的需求。基于 ISO 指导 62 和 ISO/IEC 17021，存在相应的认证标准。该途径可应用于完全不同的企业和组织。它允许信息安全管理活动集成为基于其他 ISO 标准化管理系统的管理体系。

针对安全管理的所有生存周期阶段，该标准规约了一些可访问的需求。在组织目的的语境下，可评估文档化的过程。可评估相关的记录，以确定是否遵循这些过程，是否达到期望的结果。管理体系需求包括当其没有达到所要求的结果时的纠正动作和预防动作。与 ISO/IEC 27001 的符合性需要予以管

理，通过扮演一个主动领导角色，提供准确的资源，并确保人员予以很好的培训，以便证实对信息安全管理的承诺。

ISO/IEC 27001 需要使用 ISO/IEC 27002 中规约的一些控制，作为处置不可接受风险的基础。

C.4 ISO/IEC 27002＋ISO 9000

ISO 9000 规约了质量管理体系的需求，并定义了相应的测试方法。该途径可应用于完全不同的企业和组织；但是，该途径没有考虑任何信息安全方面问题。其中所规约的所有内容是一个测试，看组织内的 IT 环境是否满足客户需求，是否适合业务目的。为了覆盖信息安全领域，可使用 ISO/IEC 27002，作为关注信息安全管理的补充。

特别地，ISO/IEC 27002 还包括涉及开发过程的措施，从而使这两个标准相互补充。但仍必要列举相关需求，并把这些需求置如实践中，使 ISO 9000 和 ISO/IEC 27002 像似针对管理层。

C.5 COBIT＋IT 基线保护

IT 基线保护是针对技术系统的保护，而 COBIT 着眼于管理的基本目的。由于企业的内部组织结构往往是针对任务的而不是针对技术的，所以经常容易使用 COBIT 向单个组织部门指派任务。另一方面，COBIT 只产生必要的 IT 安全管理机制的需求，却没有规约任何特定的技术措施。两种途径的组合可以为特定企业 IT 安全概念的创建产生一种有效率的途径。为此，根据 COBIT 可挑选一些基本的业务过程，并确定它们的安全需求。创建一个技术轮廓（把 IT 系统指派给业务过程），接着，IT 基线保护途径就是一种为实现相关安全需求来拟定特定措施的有用方式。

所描述的场景应当简单地把它看作为是一些有效组合安全准则集合的方式的例子。在一个特定应用情况中，其他途径可能是更合适的。例如，如果主要考虑审计问题，那么就可使用 COBIT 途径；如果关注点主要是加密规程，那么 ISO/IEC 19790 就是一种合适的途径。

参 考 文 献

[1] ISO/IEC 17025:1999 General requirements for the competence of calibration and testing laboratories(ISO/IEC 17025 replaces guide 25 and is identical to ISO/IEC EN 45001)

[2] ISO/IEC 17024 Personnel assessment (the document refers to assuring personnel)

[3] ISO/IEC Guide 61 General requirements for assessment and accreditation of certification/registration bodies

[4] ISO/IEC Guide 65 General requirements for bodies operating product certification systems

[5] ISO/IEC Guide 67 On the fundamentals of product certification

[6] ISO/IEC Guide 70 First, second and third party certification

[7] Cohen, Aaron. Review of ISO assurance approaches. The First Annual International Systems Security Engineering Conference. San Antonio, Texas, February 3-4, 2000

[8] AAWG, Task 1 Report, Draft Version 0.9. ISO/IEC 15408 Project: Assurance approaches working group(report: AAWG-97/037, annex A: AAWG-97/038). August 1997

[9] EN 45001 General criteria for the operation of testing laboratories(CEN/CENELEC)

[10] EN 45013 General criteria for certification bodies operating certification of personnel (CEN/CENELEC)

[11] FIPS 140-1 Security requirements for cryptographic modules

[12] U.S. Department of Commerce. National Institute of Standards and Technology, January 11, 1994

[13] FIPS PUB 31: Guidelines For Automatic Data Processing Physical Security And Risk Management

[14] IT Baseline Protection Manual Standard. Security Safeguards Standards, BSI/GISA, October 2000

[15] Example: Philippe Kruchten, The Rational Unified Process—An Introduction, Addison—Wesley—Longman, Reading, MA, USA

[16] Susanne Rohrig. Using process models to analyse IT security requirements, thesis, faculty of economics. university of Zurich, Switzerland, March 2003

[17] A Guide To Risk Assessment And Safeguard Selection For Information Technology Systems, January 1996, CSE, The ITS Publications Section, (613) 991-7514/7468 or http://www.cse.dnd.ca

[18] A Guide to Certification and Accreditation for Information Technology Systems (MG-4), January 1996, CSE, The ITS Publications Section, (613) 991-7514/7468 or http://www.cse.dnd.ca

[19] COBIT® MAPPING-Overview of International IT Guidance, IT Governance Institute, January 2004, IT Governance Institue, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 USA, (847) 590 7491 or http://www.itgi.org

[20] A Comparative Study of IT Security Criteria. Initiative D21

[21] Fiona Pattinson. Comparing ISO 17799:2000 with SSE CMM V2, 2002

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 3 部分：保障方法分析
GB/Z 29830.3—2013/ISO/IEC TR 15443-3:2007
*
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 85 千字
2014 年 5 月第一版　2014 年 5 月第一次印刷
*
书号：155066·1-48742　定价　45 00 元

GB/Z 29830.3-2013