

# 中华人民共和国国家标准

GB/T 18336.4—2024/ISO/IEC 15408-4:2022

部分代替 GB/T 18336.3—2015

## 网络安全技术 信息技术安全评估准则 第4部分：评估方法和活动的规范框架

Cybersecurity technology—Evaluation criteria for IT security—  
Part 4: Framework for specification of evaluation methods and activities

(ISO/IEC 15408-4:2022, Information security, cybersecurity and privacy  
protection Evaluation criteria for IT security—Part 4: Framework for  
specification of evaluation methods and activities, IDT)

2024-04-25 发布

2024-11-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会



目 次

前言 ..... III

引言 ..... V

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 评估方法和评估活动的一般模型 ..... 2

    4.1 概念和模型 ..... 2

    4.2 用派生方法制定评估方法和评估活动 ..... 3

    4.3 评估方法和评估活动描述中的动词用法 ..... 5

    4.4 评估方法和评估活动的描述公约 ..... 5

5 评估方法的结构 ..... 5

    5.1 概述 ..... 5

    5.2 评估方法的规范 ..... 6

6 评估活动的结构..... 10

    6.1 概述 ..... 10

    6.2 评估活动的说明 ..... 11

附录 NA（资料性） 缩略语 ..... 14

参考文献 ..... 15





## 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 18336《网络安全技术 信息技术安全评估准则》的第4部分。GB/T 18336 已经发布以下部分：

- 第1部分：简介和一般模型；
- 第2部分：安全功能组件；
- 第3部分：安全保障组件；
- 第4部分：评估方法和活动的规范框架；
- 第5部分：预定义的安全要求包。

本文件和 GB/T 18336.3—2024《网络安全技术 信息技术安全评估准则 第3部分：安全保障组件》、GB/T 18336.5—2024《信息安全技术 网络安全安全评估准则 第5部分：预定义的安全要求包》共同代替 GB/T 18336.3—2015《信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件》。

本文件部分代替 GB/T 18336.3—2015《网络技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件》。与 GB/T 18336.3—2015 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 增加了评估方法和评估活动的一般模型(见第4章)；
- 删除了保障范型(见 GB/T 18336.3—2015 年版的第5章)；
- 删除了安全保障组件(见 GB/T 18336.3—2015 年版的第6章)；
- 增加了评估方法的结构(见第5章)；
- 增加了评估活动的结构(见第6章)；
- 删除了评估保障级(见 GB/T 18336.3—2015 年版的第7章)；
- 删除了组合保障包(见 GB/T 18336.3—2015 年版的第8章)；
- 删除了 APE 类：保障轮廓评估(见 GB/T 18336.3—2015 年版的第9章)；
- 删除了 ASE 类：安全目标评估(见 GB/T 18336.3—2015 年版的第10章)；
- 删除了 ADV 类：开发(见 GB/T 18336.3—2015 年版的第11章)；
- 删除了 AGD 类：指导性文档(见 GB/T 18336.3—2015 年版的第12章)；
- 删除了 ALC 类：生命周期支持(见 GB/T 18336.3—2015 年版的第13章)；
- 删除了 ATE 类：测试(见 GB/T 18336.3—2015 年版的第14章)；
- 删除了 AVA 类：脆弱性评定(见 GB/T 18336.3—2015 年版的第15章)；
- 删除了 ACO 类：组合(见 GB/T 18336.3—2015 年版的第16章)。

本文件等同采用 ISO/IEC 15408-4:2022《信息安全、网络安全和隐私保护 信息技术安全评估准则 第4部分：评估方法和活动的规范框架》。

本文件做了下列最小限度的编辑性改动：

- 为与现有标准协调，将标准名称改为《网络安全技术 信息技术安全评估准则 第4部分：评估方法和活动的规范框架》；
- 增加资料性附录 NA“缩略语”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息安全测评中心、中国合格评定国家认可中心、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国电子科技集团公司第十五研究所、中贸促信息技术有限责任公司、北京邮电大学、中国航天系统科学与工程研究院、国家广播电视总局广播电视科学研究院、北京奇虎科技有限公司、国网新疆电力有限公司电力科学研究院、启明星辰信息技术集团股份有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、远江盛邦(北京)网络科技股份有限公司。

本文件主要起草人：石竑松、张宝峰、李凤娟、杨永生、许源、高金萍、刘昱函、林阳荟晨、王晨宇、陶小峰、王志远、刘佳、王峰、申永波、张屹、李明轩、张锦川、霍珊珊、孙俊、丁峰、吴大鹏、刘健、张益、权晓文、叶建伟、解伟、万晓兰、谢仕华、毕海英、贾炜、邓辉、王书毅、刘宏伟。

本文件于 2001 年首次发布为 GB/T 18336.3—2001,2008 年第一次修订,2015 年第二次修订,本次为第三次修订,部分代替 GB/T 18336.3—2015,编号为 GB/T 18336.4。

# 引 言

本文件的读者对象主要是采用 GB/T 18336—2024 的评估者和确认评估者行为的认证者,以及评估发起者、开发者、PP/ST 作者和其他对 IT 安全感兴趣的团体。

GB/T 18336 拟由五个部分构成。

- 第 1 部分:简介和一般模型。旨在对 GB/T 18336 进行整体概述,定义信息技术安全评估的一般概念和原则,并给出了评估的一般模型。
- 第 2 部分:安全功能组件。旨在建立一套可用于描述安全功能要求的功能组件标准化模板。这些功能组件按类和族的方式进行结构化组织,通过组件选择、细化、裁剪等方式构造出具体的安全功能要求。
- 第 3 部分:安全保障组件。旨在建立一套可用于描述安全保障要求的保障组件标准化模板。这些安全保障组件按类和族的方式进行结构化组织,定义针对 PP、ST 和 TOE 进行评估的准则,通过组件选择、细化、裁剪等方式构造出具体的安全保障要求。
- 第 4 部分:评估方法和活动的规范框架。旨在为规范评估方法和活动提供一个标准化框架。这些评估方法和活动包含在 PP、ST 及任意支持这些方法和活动的文档中,供评估者基于 GB/T 18336 的其他部分中描述的模型开展评估工作。
- 第 5 部分:预定义的安全要求包。旨在提供利益相关者通常使用的安全保障要求和安全功能要求的包,提供的包示例包括评估保障级(EAL)和组合保障包(CAP)。

针对信息技术(IT)产品的安全评估,GB/T 18336 提供了一套通用的安全功能及其保障措施要求,从而允许各个独立的 IT 产品的评估结果之间具有可比性。ISO/IEC 18045 为 GB/T 18336 中规定的一些保障要求提供了配套的方法。

本文件描述了一个框架,可用于从 ISO/IEC 18045 的工作单元派生评估活动,并将其分组为评估方法(EM)。评估活动或评估方法可能包含在 PP 和任何支持它们的文件中。当 PP、PP-配置、PP-模块、包或安全目标(ST)确定要使用特定的评估方法/评估活动时,ISO/IEC 18045 要求评估人员在确定评估者裁定时,遵循并报告相关的评估方法/评估活动。如 GB/T 18336.1 中所述,在某些情况下,评估授权机构能决定不批准使用特定的评估方法/评估活动;在这种情况下,评估授权机构能决定不按照 ST 所要求的评估方法/评估活动进行评估。

本文件还允许为扩展 SAR 定义评估活动,在这种情况下,评估活动的派生与为扩展 SAR 定义的等效行为元素和工作单元相关。如果本文件中引用 ISO/IEC 18045 或 ISO/IEC 15408-3 对 SAR 的使用(如定义评估活动的基本原理时),那么在扩展 SAR 的情况下,这种引用也将适用于为扩展 SAR 定义的等效行为元素和工作单元。

为简明起见,本文件指定了如何定义评估方法和评估活动,但本身没有规定评估方法或评估活动的实例。

在 GB/T 18336 的其他部分和 GB/T 30270—2024 中出现的下述注描述了在那些文件中关于粗体字和斜体字的使用。本文件没有使用那些惯例,但这里注仍被保留以与其他标准一致。

注:本文件在某些情况下使用粗体字和斜体字来区分术语和其余部分文本。族内组件之间的关系约定使用粗体突出显示,对所有新的要求也约定使用粗体字。对于分层的组件,当其要求被增强或修改,且超出了前一个组件的要求时,以粗体显示。此外,除了前面的组件之外,任何新的或增强的允许的操作使用粗体突出显示。约定使用斜体来表示具有精确含义的文本。对于安全保障要求,该约定也适用于与评估相关的特殊动词。



# 网络安全技术 信息技术安全评估准则

## 第 4 部分：评估方法和活动的规范框架

### 1 范围

本文件提供了一个标准化框架,用以规定客观的、可重复的和可重现的评估方法和评估活动。

本文件未规定如何评估、采用或维持评估方法和评估活动。这方面的内容由那些在其感兴趣的特定领域内提出评估方法和评估活动的相关方负责。

### 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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/IEC 15408-1 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 1 部分:简介和一般模型(Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 1: Introduction and general model)

注: GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第 1 部分:简介和一般模型(ISO/IEC 15408-1:2022,IDT)

ISO/IEC 15408-2 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 2 部分:安全功能组件(Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 2: Security functional components)

注: GB/T 18336.2—2024 网络安全技术 信息技术安全评估准则 第 2 部分:安全功能组件(ISO/IEC 15408-2:2022,IDT)

ISO/IEC 15408-3 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 3 部分:安全保障组件(Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 3: Security assurance components)

注: GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第 3 部分:安全保障组件(ISO/IEC 15408-3:2022,IDT)

ISO/IEC 18045 信息安全、网络安全和隐私保护 信息安全评估方法(Information security, cybersecurity and privacy protection IT security techniques—Methodology for IT security evaluation)

注: GB/T 30270—2024 网络安全技术 信息技术安全评估方法(ISO/IEC 18045:2022,IDT)

### 3 术语和定义

ISO/IEC 15408-1、ISO/IEC 15408-2、ISO/IEC 15408-3 以及 ISO/IEC 18045 界定的术语和定义适用于本文件。

注: 附录 NA 给出了本文件使用的缩略语。

4 评估方法和评估活动的一般模型

4.1 概念和模型

ISO/IEC 18045 定义了一组通用的工作单元,评估者通过执行这些工作单元对 ISO/IEC 15408-3 中定义的大多数保障类、族和组件做出裁定。ISO/IEC 15408-3 的安全保障要求(SAR)的结构与 ISO/IEC 18045 中的工作单元之间的关系在 GB/T 30270—202X 的第 9 章中进行了描述,并在图 1 中进行了总结。

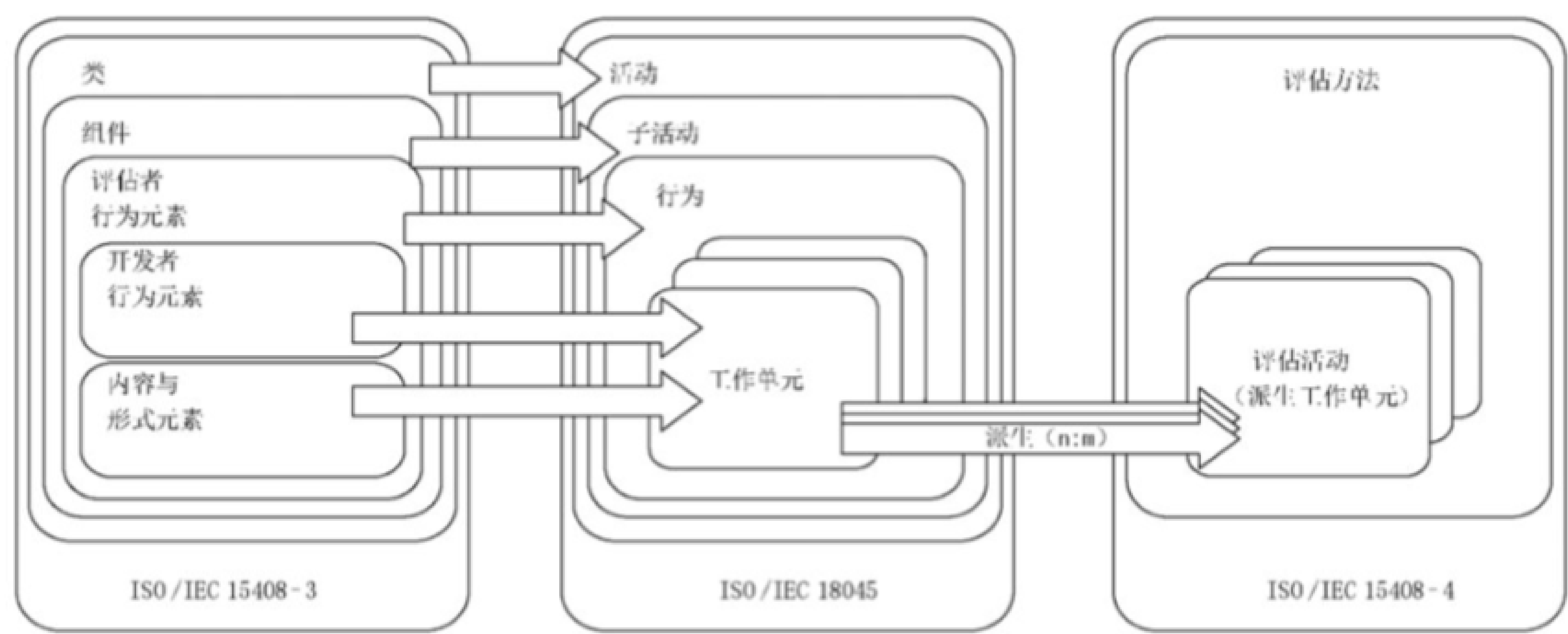


图 1 ISO/IEC 15408-3 和 ISO/IEC 18045 结构与本文档结构的对应关系

为了定义新的评估方法和评估活动,需要注意的是每个行为(在 ISO/IEC 15408-3 中代表一个评估者行为元素或隐含的评估者行为元素)在 ISO/IEC 18045 中表示为一组由评估者执行的工作单元。

本文件规定了从 ISO/IEC 18045 的通用工作单元派生出新的评估活动的方式,并将其组合成一种评估方法,用于特定的评估情景。这种评估情景的典型示例是特定 TOE 类型或特定技术类型。

示例 1:

TOE 类型:网络设备

技术类型:特定密码功能

如果要求评估方法和评估活动与特定的 PP、PP-模块、PP-配置一起使用,则 PP 或 PP-模块或 PP-配置应在其符合性声明中标识该要求。如果要求评估方法和评估活动与特定的包一起使用,那么包应在安全要求部分中标识该要求。如果 ST 声明的评估方法和评估活动是因其声称其符合 PP、PP-配置或包,则 ST 应识别其符合性要求中所使用的评估方法/评估活动(EM/EA)。在这些情况下,没有正式对 ISO/IEC 15408-4(PP、PP-模块、PP-配置和包的内容在 ISO/IEC 15408-1 中有更详细的描述)的符合性提出声明。

PP、PP-配置、PP-模块或包可使用一种以上的评估方法或一系列独立的评估活动。

示例 2:

多种评估方法能被使用,为 PP 中使用的加密操作和安全信道协议分别定义了评估方法。

注:在精确符合的情况下,ISO/IEC 15408-1 不允许在 PP-配置中定义评估方法/评估活动(所使用的评估方法/评估活动包含在 PP 和 PP-模块中,而不包含在 PP-配置中)。



当 PP、PP-模块、PP-配置或包标识了要使用的特定评估方法/评估活动时,则需要使用一种标准化措辞来说明要求并引用要使用的评估方法/评估活动的定义。ST 应仅标识其声明符合性的 PP、PP-模块、PP-配置或包中所包含要求的评估方法和评估活动(即 ST 本身不应增加、修改或删除任何评估方法或评估活动)。ST 应包括其要求的所有评估方法/评估活动的标识(即包括任何 ST 声明符合性的 PP、PP-模块、PP-配置或包的要求),于是就形成了供 ST 的评估者和读者检查和参考的单一列表。

评估方法和评估活动可在要求它们的文件中定义(例如,作为 PP 的一部分),也可在外部的不同文件中定义,或两者的结合。虽然如上所述需要进行标识,但没有必要在其他文件中复制评估方法/评估活动的文本(例如,ST 不必包括其声明符合性的 PP 的评估方法/评估活动的全文)。

## 4.2 用派生方法制定评估方法和评估活动

一般来说,定义评估活动和评估方法可从 SAR 开始,目的是使其工作单元的某些或所有部分更加具体;也可从 SFR 开始,目的是定义与 SFR 相关的工作单元的具体方面。

从 SAR 开始时,流程指导如下。

- a) 标识 ISO/IEC 18045 相关的工作单元,从中派生出至少一个单独的评估活动或一组评估活动。
- b) 对于派生评估活动的每个工作单元:
  - 1) 根据 6.2 中所述的具体执行工作和评估准则定义新的评估活动(如有需要,包括 6.2.8 中所述的通过/不通过准则);
  - 2) 必要时将评估活动分组形成评估方法;
  - 3) 按照 5.2.10 和 6.2.10 所述,说明新的评估活动和评估方法的基本原理。

示例:

基本原理包括对开发者行为指南,以及派生它们的工作单元的内容和形式元素。

从 SFR 开始时,流程指导如下。

- a) 标识相关的 SFR。
- b) 标识针对特定 SFR 处理的 SAR(来自 ISO/IEC 15408-3 或扩展的 SAR 集,或两者),以及相应的 ISO/IEC 18045 工作单元。
- c) 根据 6.2 中所述的具体执行工作和评估准则定义新的评估活动(如有需要,包括 6.2.8 中所述的通过/不通过准则)。

示例:

评估活动能被定义为检查 TOE 概要规范(源自 ASE)中特定 SFR 的表述,检查指导性文件(源自 AGD)中 SFR 的表述情况,并对该 SFR 进行特定测试(源自 ATE)。

- d) 将受 SAR 影响的工作单元映射到新的评估活动。
- e) 按照 5.2.10 和 6.2.10 所述,说明新的评估活动和评估方法的基本原理。

尽管作者可选择从 SAR 或 SFR 开始,但需要注意的是,SAR 最终涵盖所有 SFR。在阐明 SAR 如何应用于特定 SFR 的细节时,从上述 SFR 开始是非常有用的技术,并且在描述其评估活动的同时呈现 SFR 也很有用。

可以不在工作单元和新的评估活动之间进行一对一映射,实际的对应关系记录在基本原理中(如 5.2.10 中所述)。派生可根据独立的工作单元或整个工作单元组进行,如图 2 所示。在图 2 的情况 a) 中,作者将每个工作单元从 ISO/IEC 18045 映射到相应的评估活动,而在情况 b) 中,作者对不同的工作单元和评估活动进行映射,但仍然处理一个活动的所有方面(即工作单元的集合)。

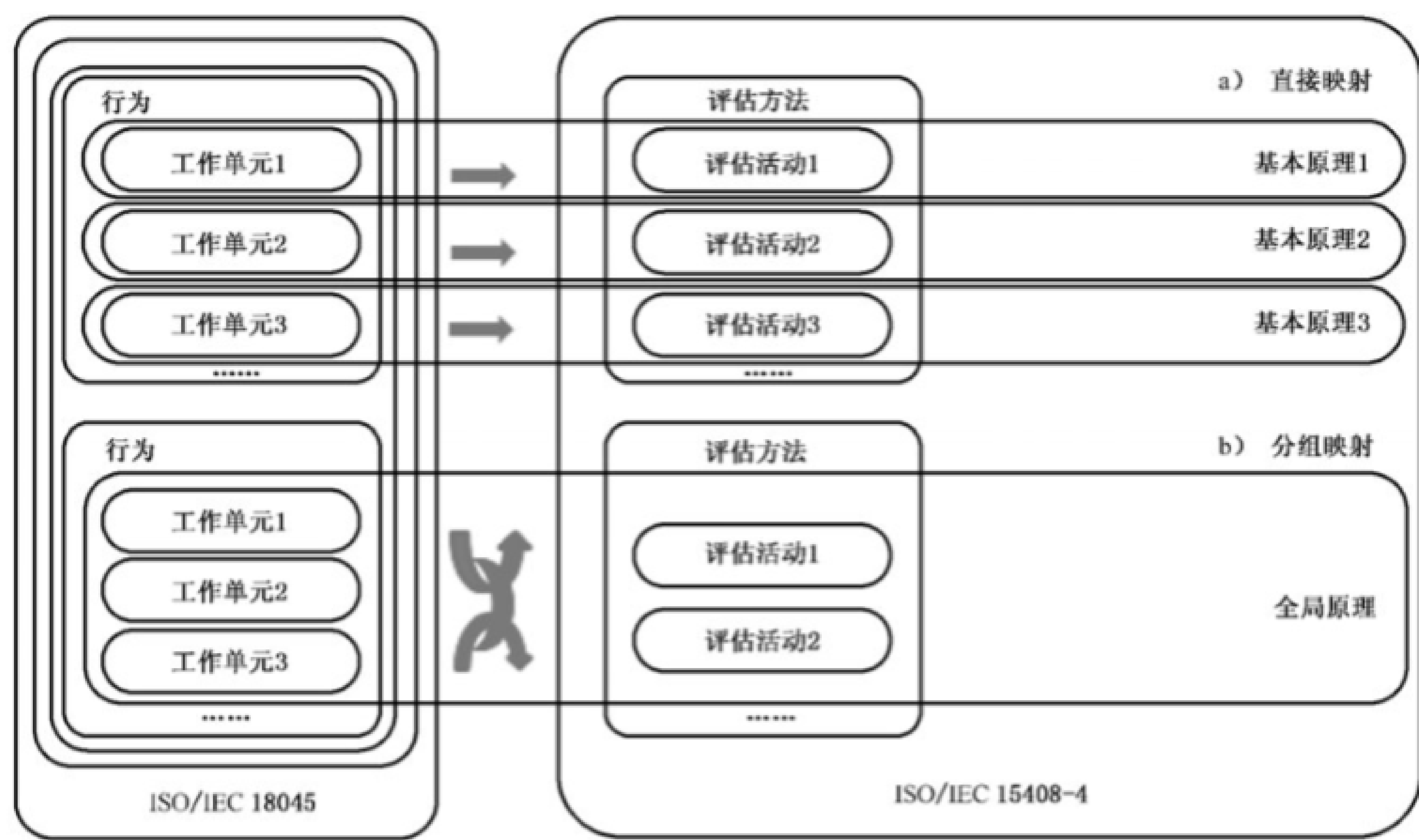


图 2 将 ISO/IEC 18045 映射到派生评估活动的替代方法

根据具体的工作单元和评估活动的内容,也有可能使用其他方法;即使工作单元和评估活动的数量相同,简单的一对一映射有时也不可行,因此在活动级别上的映射可能更合适。下面的示例中描述了一些更详细的映射情况。

注: 这些例子假设所描述的评估活动是由一个团体定义的,它能判断评估活动完整性基本原理的适用性。这些示例只关注映射的形式和结构,而不关注完整性基本原理的本质或接受程度。

示例 1:

对于既包括软件又包括硬件的 TOE 类型,额外的评估活动能被定义来处理制造环境及其过程。考虑到 ALC\_DVS 族,一种可能采用的方法是将已有的所有 ALC\_DVS 工作单元应用于软件开发环境,为每个相关的硬件和制造环节定义额外的评估活动。这些活动内容能包括将正常 ALC\_DVS 范围扩展到其他过程,如对开发环境中的硬件设计保护、从开发环境到制造环境的软件安全传输、制造场所的安全以及在等待交付时对成品的保护等。它们还能包括仅在制造环境中出现的与评估对象和过程相关的新的考虑,例如:

- 确认生产线上使用的固件来源的可靠性,获得自固件生成系统中的授权版本;
- 检查生产线 TOE 测试程序的配置管理;
- 确认在 TOE 上禁用测试或调试接口的进程正确且运行可靠;
- 检查在生产过程中用于向 TOE 输入密钥或证书的密钥管理系统,确认其物理和逻辑的安全性。

在此示例中,原始 ALC\_DVS.1.1E 操作被映射为包括所有新的评估活动,但另一种方法是为 ALC\_DVS.1.1E 的每个独立工作单元定义额外的评估活动,识别附加活动以覆盖该工作单元的制造环境。

示例 2:

如果将 AVA\_VAN.1 脆弱性分析应用于特定类型的 TOE,需要与使用的公共域脆弱性源保持一致,那么一种可能采用的方法是定义一个评估活动,该活动包括通过指定要使用的特定脆弱性源,搜索公共域脆弱性源的 AVA\_VAN 工作单元,甚至可能还需要进行特定的搜索,以及针对分析和测试得出的潜在脆弱性结果列表,以进行决策准则的选择。在此示例中,原始 AVA\_VAN.1-3 的工作单元映射到新的评估活动。

示例 3:

对于与集成电路等硬件一起使用的评估方法,评估活动能被定义来检查电路的架构,定义所需的输入,为评估者提供有关操作的特定详细信息以及通过电路接口可用的信息。这些所需输入的定义能明确相关接口,包括电路的物理接口、可执行编程指令和通信接口。

评估方法中的进一步评估活动能检查电路对物理探测的抵御,以防止操纵或破坏 TSF 特性。



对于测试活动,评估方法中的评估活动能被定义为一个所需的输入,该输入将电路设计呈现为渗透到电路各子系统的安全功能流程图。然后,评估者能使用该流程图来创建测试用例,并确认电路的测试覆盖率。

示例 4:

对于 TOE 类型,如提供加密验证固件更新的网络设备,评估活动能提供具体细节,说明如何要求评估者审查安全目标和指导性文档,以确认加密更新过程所需的特定特性。

其他评估活动能定义特定的测试用例,包括当前固件的验证、更新的可用性、获取更新、使用加密签名验证更新的来源,以及使用特定类型的无效更新,以测试 TOE 的验证功能。

4.3 评估方法和评估活动描述中的动词用法

如果一个动词在 ISO/IEC 15408-1 中有定义,那么评估活动的描述只能根据定义使用这些动词。备选动词可在评估方法中用于评估活动,前提是备选动词是在评估方法中定义的。任何此类动词的定义都应明确评估者的判断所涉及的程度(而不是简单的检查)。

示例:

包含协议自动测试生成的评估方法能定义一个动词“覆盖”,应用于协议参数中的枚举类型,以表示在可用参数长度内尝试所有已定义和未定义值的参数。然后,评估活动能被写成“评估者应覆盖 PaymentMode 字段”这样的形式。

本文件中使用的评估者行为动词,如 check(核查)、examine(检查)、report(报告)和 record(记录)等,其含义在 ISO/IEC 15408-1 中定义。

4.4 评估方法和评估活动的描述公约

下面的段落描述了 ISO/IEC 15408-3 和 ISO/IEC 18045 中使用的支持评估方法和评估活动描述一致性的约定。

所有的工作单元和子任务动词前面都有助动词“应”,动词和“应”都用斜体字体表示。只有在所提供的文本有强制性时才使用助动词“应”,因此它只能在工作单元和子任务中使用。这些工作单元和子任务包含了评估者为作出裁定而必需进行的强制性活动。

工作单元和子任务的指导文本进一步说明了如何在评估中应用工作单元和子任务。

5 评估方法的结构

5.1 概述

定义了一种评估方法及其组成的评估活动,以便在特定的评估情景中使用。例如,可为特定的技术领域定义单独的评估方法,从特定的功能到特定的产品类型,甚至在极端的情况下,对于一个特定的产品,当对产品的独特特性进行评估时,但又要求使用一个单独定义的方法来评估产品,该方法支持评估的可见性、可重复性和可复现性。

示例:

能定义单独评估方法的评估情景如下:

- 特定产品类型,如网络设备、智能卡、生物识别设备、移动设备;
- 被多种类型产品重用的特定安全功能,如加密功能、加密协议、数字证书验证、标识和鉴别方案。

一种评估方法包括一组单独的评估活动,以及评估活动如何共同满足与确定的评估情景相关目标的附加信息。

评估方法的描述包括:

- a) 确定负责定义和维护评估方法的实体;
- b) 评估方法的预期使用范围、标识评估方法中产生评估活动的目的、评估方法拟应用的评估情景,以及评估方法的任何已知限制或不打算涵盖的方面;
- c) 执行评估方法中所包含的评估活动所需的任何工具类型和/或评估者能力;

- d) 对报告应用评估方法的结果的要求；
- e) 对 ISO/IEC 18045（或等效的扩展 SAR）的评估方法中，评估活动所涉及的每个工作单元的识别；
- f) 识别任何可导出评估方法的扩展 SAR（如适用），并据此制定评估方法；
- g) 任何在描述评估活动中代替 ISO/IEC 15408-3 定义的动词使用的附加动词。

对内容的进一步说明，包括确定哪些内容元素是强制性的，以及如何在评估方法及其评估活动之间分配内容元素，详见 5.2 和 6.2。在表 1 中如果内容元素是可选的（如明确的评估者能力，或所需的工具类型），那么可从相关定义中简单地删除该部分，没有必要包括空白内容。

5.2 评估方法的规范

5.2.1 概述

评估方法根据 5.2.2~5.2.12 所确定的信息予以规定。除非 5.2.2~5.2.12 中对单个元素进行了说明，提供或呈现这些信息不需要特定的格式。在 5.2.2~5.2.12 中指定评估方法描述的目的是确保评估中使用的保障技术能够被明确识别，（在预期的情况下）评估方法的使用是恰当的，并支持一致的评估结果方式。

一般来说，评估方法的描述可能包括它所包含的单独评估活动的描述。这意味着评估方法描述的各个方面可从评估活动描述中推导出来。

图 3 说明了本文件中描述的评估方法的内容。它未定义描述评估方法的强制性结构。

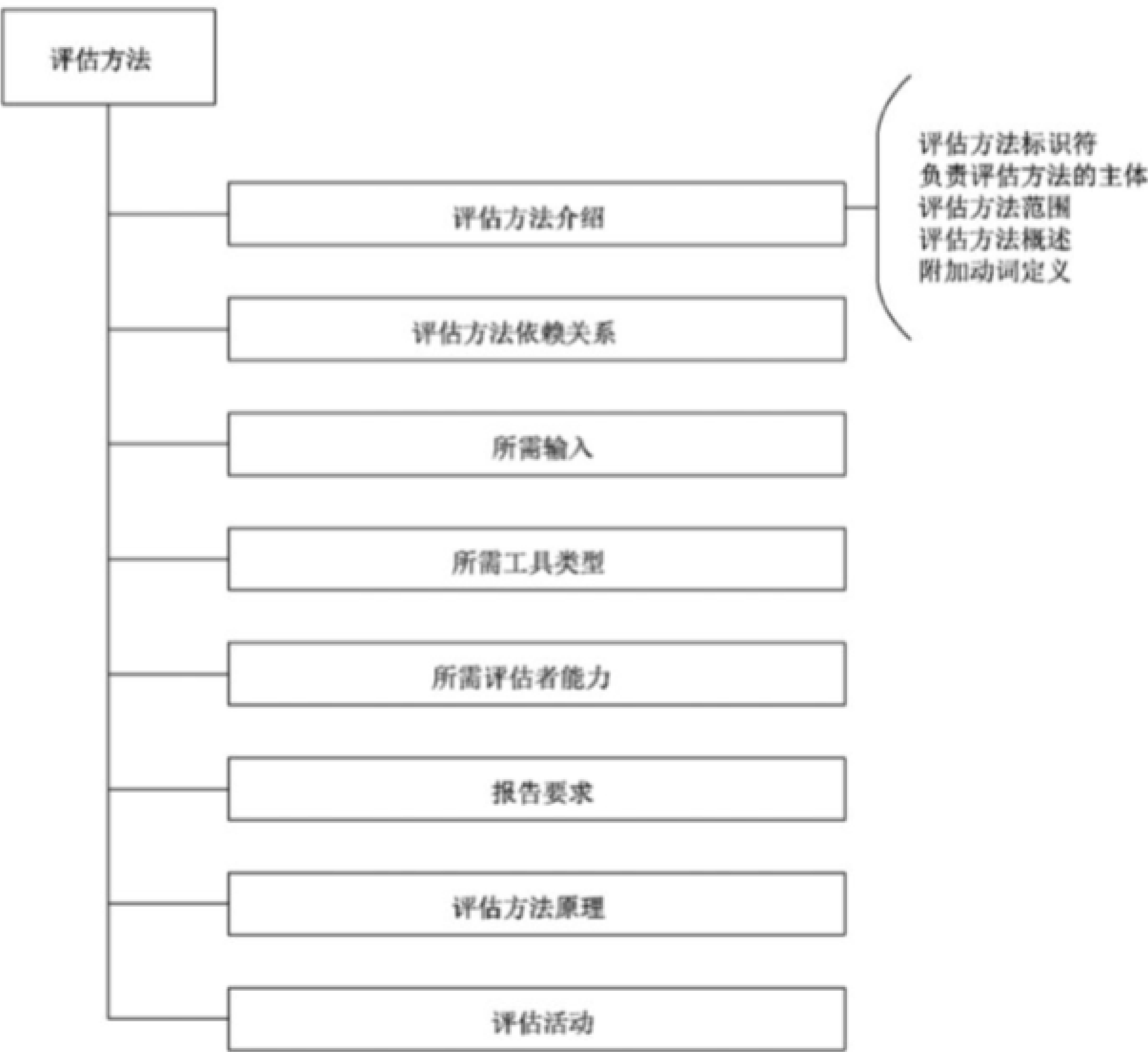


图 3 评估方法的内容

图 3 所示的内容在 5.2 和 6.2 中有更详细的描述，表 1 给出了指定评估方法和评估活动的强制的和可选的要求的总结。

表 1 评估方法(EM)和评估活动(EA)之间的内容对比

内容元素	评估方法	评估活动
标识符	强制的	强制的
责任主体	强制的	不适用
范围	强制的	不适用
依赖关系	在 EM 或 EA 级别上可选的	
需要的输入	在 EM 或 EA 级别上强制的	
所需的工具类型	在 EM 或 EA 级别上可选的	
需要的评估者能力	在 EM 或 EA 级别上可选的	
报告要求	在 EM 或 EA 级别上可选的	
基本原理	在 EM 或 EA 级别上强制的	
评估活动	强制的	不适用
附加动词的定义	可选的	不适用
目标	不适用	强制的
评估活动与 SFR、SAR 和其他评估活动相联系	不适用	可选的
评估策略	不适用	强制的
通过/不通过的准则	不适用	可选的

5.2.2 标识评估方法

评估方法的定义应包括唯一标识符,以便明确地识别在任何给定评估中应用的一组评估活动。宜在评估方法层面(而不只是在其所包含的评估活动层面)指定一个标识符,以反映评估方法是作为一个整体应用的事实,并受制于该层面的基本原理和定义的目的和目标。如果一组评估活动被组合成一种评估方法,那么只有当使用该评估方法中的一整套评估活动时,该评估方法才被认定为同一种评估方法,其基本原理与原评估方法中包含的相同。如果有必要将评估方法划分为评估活动的较小子集,则应为每个子集定义一个单独的评估方法,并具有其自身的理论基础。

示例 1:  
由包含评估方法的支持文件或 PP 文件的标题和版本号表示的唯一标识符。

示例 2:  
从注册的授权机构获得的标识符。

如 5.2.10 所述,一种评估方法可与另一种评估方法重叠(例如用于其他 PP 或 PP-模块)。在这种情况下,如果原评估方法的基本原理仍然成立(如 5.2.10 所述),则应使用原评估方法的标识符。然而,如果作为基本原理覆盖的一部分发生了改变,那么应使用在相关的 PP-模块、PP-配置或 PP 中定义的一个单独的标识符。这里的目的是确保在基本原理发生重大变更时使用不同标识符。

5.2.3 负责评估方法的实体

评估方法的定义应说明负责评估方法定义和维护的实体。

示例:  
责任实体的例子包括评估授权机构、标准机构、行业工作组或技术团体。

5.2.4 评估方法的范围

评估方法的定义应描述其范围,包括:

- a) 评估方法的目标,包括对保障目标的简要概述,以及评估方法内的评估活动如何实施这些目标的高级陈述。
- b) 要应用评估方法的评估情景。例如,可能描述一种 TOE 类型,如智能卡或网络设备,或一种功能,如使用特定算法和模式,应用于特定类型的数据传输和数据存储的加密功能。
- c) 任何已知的评估方法的局限性,或评估方法不打算涵盖的方面。

评估活动能被定义为专门适用于一个或多个 SFR。当评估方法包括此类 SFR 特定的评估活动时,应在其范围内的一个子部分中,确定评估方法所定义的单个 SFR 以及定义 SFR 的位置(例如 ISO/IEC 15408-2 或保护轮廓中定义的扩展 SFR)。对于 ISO/IEC 15408-2 中未定义的扩展 SFR,位置的标识尤其重要,因为相同的 SFR 名称可能在不同的来源中使用,以引用具有不同内容的 SFR(如果评估方法不针对任何特定 SFR,则不需要本部分)。

同样,评估活动可能被定义为专门适用于一个或多个扩展的 SAR(即在 ISO/IEC 15408-3 中未定义的 SAR)。当评估方法包括此类评估活动时,应在其范围内的一个子部分中,确定相关的扩展 SAR 及其定义的位置(如在 PP 中)。与扩展的 SFR 一样,位置的标识尤其重要,因为相同的 SAR 名称可能在不同的来源中使用,以引用具有不同内容的 SAR(如果评估方法不适用于任何扩展的 SAR,则不需要本部分)。

注:评估方法完整性的基本原理(见 5.2.10)能为评估方法的使用范围提供进一步的信息。

5.2.5 依赖关系

评估方法的定义应描述对其他评估方法、评估活动或 ISO/IEC 18045 中某些通用措施的依赖关系。

示例:

一种评估方法依赖于从 ISO/IEC 15408-3 或 ISO/IEC 18045 中某些其他开发者行为元素或从某些行为中获得的信息。

依赖关系可在评估方法层面上进行确认,或者在评估方法中包含的单独评估活动层面上进行确认。

5.2.6 来自开发者或其他实体的必要输入

评估方法的定义应确定执行评估活动所需的任何开发者输入。这可在评估方法层面上进行,也可在评估方法中包含的单独评估活动层面上进行。输入的描述也可参照 ISO/IEC 15408-3 中定义的用于派生评估活动的通用 SAR 的定义(或处理扩展 SAR 的等效通用定义)。

示例:

处理媒介加密 TOE 的评估方法的输入时,能定义针对密钥层次结构的特定细节进行描述的要求。

5.2.7 所需工具类型

如果评估活动需要任何工具类型,那么这些工具类型应被列为评估方法定义的一部分。工具类型可在评估方法层面上进行标识,或者在评估方法中包含的单独评估活动层面上进行标识。

5.2.8 评估者需要的能力

评估方法可确认评估活动所需的特定评估者能力(见参考文献[4])。如果确认了具体的评估者的能力,那么可在评估方法层面进行,也可在评估方法中所包含的单独评估活动层面(或两者的结合)进行。

### 5.2.9 报告要求

评估方法的描述可包括报告要求的描述。此描述可在评估方法层面、单独评估活动层面或在这两者中进行。

示例 1:

评估方法层面能给出一般的报告要求,但有些评估活动也需要特别的观察、论证或对具体问题的回答。

任何所陈述的报告要求,应保持与 ISO/IEC 18045 中对评估技术报告的要求,以及与进行评估所需的任何其他标准相一致。

示例 2:

ISO/IEC 17025 是进行评估所需的另一个标准的例子。

报告要求可规定 ISO/IEC 18045 中所述的评估技术报告(ETR)中包含的报告,但也可规定其他输出报告的内容。

示例 3:

能为公共发布和限制范围发布(如开发商、评估者和评估授权机构)定义单独的报告。

如果以这种方式定义了多个报告,那么评估方法的报告要求(包括单独评估活动的报告要求)就可在每个输出报告中指定要报告的方面。

如果评估方法不需要报告或报告细节,而是需要在其派生的工作单元中给出(或者是评估活动中规定了的所有额外的报告要求),则不需要本部分。

### 5.2.10 评估方法的基本原理

应在 ISO/IEC 18045 的原本工作单元中给出一个理由,表明评估方法中评估活动的推导是适当的。(在扩展 SAR 的情况下,则引用 ISO/IEC 18045 中的工作单元,而不是引用扩展 SAR 的相关方法定义中的工作单元)。这可在评估方法层面或在单独评估活动层面提出。如果评估方法中所包含的评估活动没有按照 6.2.10 所述的单独基本原理,则评估方法应包括 ISO/IEC 18045 中对工作单元进行评估活动的推导基本原理。这一基本原理可能包括解释为什么要根据特定技术或 TOE 类型的评估范围和深度,对工作单元进行重制。基本原理应进一步说明,其所包含的评估活动如何涉及 ISO/IEC 15408-3 所适用的行为元素的所有方面。它还应证明,就拟应用评估方法的评估情景而言,处理行为元素或工作单元的方式是完备的。

如果评估活动是从扩展的 SAR 中得到的,基本原理应证明评估活动与扩展 SAR 的工作单元描述相符(ISO/IEC 18045 中定义的用于评估扩展组件定义的方法(ISO/IEC 15408-3 中的 APE\_ECD, ACE\_ECD 和 ASE\_ECD 族)要求将工作单元作为扩展 SAR 定义的一部分)。

基本原理可在适当的情况下被认定是为评估情景所作的具体假设。

当不同的安全要求源被组合在一起时,例如 PP-模块与 PP-配置中的基本 PP 一起使用时,每个来源的评估活动(例如,每个基本 PP/PP-模块的评估活动和 PP-配置的每个组成部分的评估活动)将被组合并应用于最终的 TOE。作为组合的一部分,一种评估方法可能会被另一种评估方法所叠加,但必需对由该叠加所作的任何更改进行说明,以便仍然能够给出所产生评估方法的基本原理。当来自不同来源的多个评估活动的范围相同时,就存在叠加。叠加的原因是,当两个部件一起使用时,便于使最终的评估方法更具体地针对 TOE,如在本例中,部件是一个基本 PP 和一个 PP-模块,但也可能出现其他情况,例如当一个包在 PP 中使用时,为 PP 定义的更具体的评估方法叠加到为包定义的更通用的评估方法上。

注:虽然在默认情况下,评估活动适用于生成的整个 TOE,但评估方法或评估活动的定义能定义其应用的限度。

例如,能专门为在某个安全通道协议的背景下使用的加密操作定义评估活动;当在保护存储数据的情景下使用时,这些评估活动将不适用于相同的加密操作。



示例：

在网络设备 TOE 的基本 PP 中能定义一种评估方法，包括 TOE 支持的通用安全通道的评估活动。PP-模块能使用特定的安全通道类型（例如指定特定的操作或特定的协议），为网络设备上的某些远程管理操作进行定义。然后，PP-模块的评估活动将会叠加基本 PP 的评估方法，这意味着 PP-模块的评估活动取代了 PP-模块中涉及的特定远程管理活动的基本 PP 评估活动（其他安全通道的能力仍将受制于基本 PP 的评估方法中的评估活动）。

叠加效果是对底层评估方法做了以下一个或多个更改：

- a) 底层评估活动可能被删除——通常这是因为该评估活动不再相关（例如，一个 PP-模块删除了一个基本 PP 的 SFR 中的一些可用选择值）；
- b) 底层评估活动可能通过添加更多的具体细节（这可能使活动更严格）来细化——通常情况下，这将反映评估情景中的额外细节（例如，细节是通过功能包添加到 PP 情景中的）；
- c) 定义附加评估活动——这将反映额外的评估情景（例如，由功能包添加到 PP 情景的附加细节，或在 PP-配置中添加的附加 SAR）。

一个特殊的情况是，对一个底层评估活动进行改变，以对应一个相关的 SAR 的增强，通常情况下，这种行为在 PP-配置中的体现是使用更高层级的 SAR 替代现有的 SAR。在这种情况下，根据层级结构，更高层级的 SAR 中的新内容，可能像 b) 中那样添加细节，也可能像 c) 中那样添加进一步的评估活动。

由此产生的评估方法的基本原理，可能基于在原始评估方法基本原理中已经对叠加部分做了考虑（即，在原始评估方法定义中已经包括了叠加部分的基本原理），或者更具体的评估方法（例如 PP-模块）可能包括单独的基本原理，处理其对原始评估方法的影响（例如，基本 PP）。如果叠加的评估方法（例如 PP-模块）包含单独的基本原理，则应表明所产生的评估方法保留了叠加评估方法的相关方面，并考虑到了组合部分的使用环境。对于组合使用 PP 的情况，同样的原则适用：要么原始评估方法根据应用它的情景描述所允许的变化，要么由此产生的叠加评估方法处理对基本原始评估方法的影响。

如 ISO/IEC 15408-1 所述，叠加评估活动的基本原理可是一个单独的部分，也可作为保障基本原理或安全要求基本原理的一部分。

5.2.11 附加动词的定义

如 4.3 所述，可在评估活动规范中使用 ISO/IEC 15408-1 中定义的备选动词，但任何此类备选动词应定义为包含评估活动的评估方法的一部分。并应明确评估者的判断（相对于简单的检查）所涉及的程度。

5.2.12 评估活动集

评估方法中包含的评估活动应使用第 6 章中定义的结构来定义。

6 评估活动的结构

6.1 概述

在单独评估活动的层次上，规范的重点在于确保评估活动有一个明确的目标，明确的通过/不通过的准则（如果需要的话），以及确认对其他评估活动的任何依赖关系。这是为了支持对评估的理解，从而保证在每次评估中一致地应用该活动。

如 5.2 所述和表 1 所总结的，评估活动的一些具体细节可在评估方法层面或独立评估活动层面列入。

评估的内容可能以各种格式给出，包括仅由测试或分析活动的简短叙述性描述组成的格式（例如，确认用户文档描述了用于协议的凭据的安全生成）。此外，一些评估活动可分组在一起，并将内容元

素作为一个整体进行描述,而不是为每个单独的评估活动重复描述。评估活动的每个内容元素在 6.2.1~6.2.10 中有更详细的描述,表 1 中总结了每个元素的强制和可选状态。

6.2 评估活动的说明

6.2.1 评估活动的唯一标识

评估活动应在其源文件中进行唯一标识。源文件本身应进行唯一标识。如果评估活动被分组到一个评估方法中,那么除了整个评估方法的一个标识符外,还定义了单独评估活动标识符(见 5.2.2)。

6.2.2 评估活动的目的

应说明开展评估活动的目的。这可参照 6.2.3 中讨论的 SFR 和 SAR 以及 6.2.8 中的通过/不通过的准则来说明,然而,同样重要的是,目的陈述要有助于评估者了解变更评估活动以适应特定 TOE 的灵活性和局限性。

6.2.3 评估活动与 SFR、SAR 和其他评估活动有关

如果评估活动与特定 SFR 相关(还可能与另一个文档中的 SFR 特定实例,例如包、PP 或 PP-模块相关),则应将其标识为评估活动定义的一部分。

示例:

评估活动能与特定 PP 中陈述的 SFR 相关,并部分完成赋值,以限制能用于符合性 ST 中的可接受值。

同样,应确认与特定 SAR 的关系[这可通过从原始 SAR 的工作单元推导的基本原理来实现(见 5.2.10 和 6.2.10),除非需要提供关于该关系的附加信息]。

如果一项评估活动依赖于另一项评估活动的完成,则依赖性和其他评估活动应作为依赖性评估活动定义的一部分加以识别(依赖性可在评估方法的层面上进行识别,或在单独评估活动的层面上进行识别)。

6.2.4 来自开发者或其他实体的必要输入

如 5.2.6 所述,还可规定评估活动所需输入的格式和内容的附加细节。这种附加的细节通常用于支持精确的规范评估活动及通过/不通过准则(这可在评估方法层面上进行,也可在单独评估活动的层面上进行)。

如果评估活动除了派生它的工作单元中定义的输入之外不需要其他输入,那么这个部分是不需要的。

6.2.5 所需工具类型

如果执行评估活动需要任何工具类型来完成该活动,那么这些工具类型应被定义为评估活动定义的一部分。工具类型的定义应包括足够的细节,从而能够获得工具或重新创建该类型的工具,以便能够根据评估活动描述及其通过/不通过准则进行评估活动时,保持一致性(这可在评估方法层面上进行,也可在单独评估活动层面上进行)。

如果评估活动不需要特定的工具类型,除了那些在派生它的工作单元中给出的或隐含的工具类型,那么这个部分是不需要的。

6.2.6 评估者需要的能力

如 5.2.8 所述,评估方法可确定其评估活动所需的具体评估者能力(见参考文献[4])。如果确定了具体的评估者的能力,那么可在评估方法层面进行,也可在评估方法中所包含的单独评估活动层面进行(或两者结合)。

### 6.2.7 评估策略

评估活动的这一部分应提供如何执行该活动的指导和细节。根据评估活动的内容,它包括:

- a) 如何评估来自开发者或其他实体的关于评估活动完整性的输入;
- b) 如何使用所需的所有工具类型(可能包括工具校准或安装的指南);
- c) 执行评估活动步骤的指导。

对大多数评估活动来说,为适应特定技术留出一些空间是很重要的。在评估策略的精确规定和这种适应的允许空间之间找到正确的平衡,对于确保客观和可重复的结果很重要,对于得到有意义的结果也很重要。当开发者在如何实现功能要求方面具有更大的灵活性时,评估活动定义需要留出更多空间来使评估适应不同的潜在实现。在这些情况下,评估策略宜提供关于如何执行特定于 TOE 的细化和调整的一般指导,而不是详细说明评估者必需执行的行为的每个细节。一般来说,评估活动的偏差/改进(即忽略评估活动中要求的内容)是不允许的。

评估策略可能由评估者必需执行的几个阶段组成,在这种情况下,这些阶段应与每个阶段的预期结果一起进行规定。有些阶段可能取决于前几个阶段的结果,在这种情况下,评估策略还应规定,如果其中一个阶段没有产生预期的结果,说明评估者还需要做什么。这种情况的示例是返回到一个带有修改过的输入的前一个阶段,终止评估活动,指明该活动的结果是什么,或者继续进行另一个阶段。

根据评估情景的需要和评估活动本身的性质,评估策略可以是简短的,并可构成评估活动一般描述的一部分(例如,如何进行特定测试或分析活动的描述)。

### 6.2.8 通过/不通过准则

评估活动本身允许定义相关准则,评估者用其确定评估活动证明 TOE 是否满足了相关要求。在某些情况下,依赖于评估活动所产生的原始工作单元的描述可能是合适的,但在其他情况下,评估活动的作者可能需陈述更具体的准则,这是必要或有益的。最终,通过/不通过的准则涉及确定是否满足评估活动(见 6.2.2)的目的陈述。如果评估活动规定了单独的通过/不通过的准则,那么这些准则在不同的评估中执行评估活动,宜尽可能提高结果的一致性。以这种方式对特定的准则做出明确的陈述,尽可能减少不同的评估者在给出相同证据的情况下,对评估活动得出不同结论的机会。因此,一般来说,通过/不通过的准则宜尽量具体。

实现分析文档的特定通过/不通过准则的方法,包括通过对特定特征的存在或不存在来表述准则,例如,通信堆栈的详细配置或执行环境的故障触发器集的存在,通过“是/否”的回答来规范“封闭性”的问题(可能会通过其他“开放性”问题的答案来得到支持)。

实现特定测试通过/不通过准则的方法是用特定的可见结果来表达准则,比如观察信道上成功的通信,或者接收到指示通道设置失败的错误消息,或者观察到内存访问/设置的错误消息。像“TOE 删除数据”这样描述的短语通常不建议使用,因为不清楚这个删除是如何由评估者决定的;更好的描述是“TOE 返回到‘无法找到文件’的错误”或“评估者使用〈命名接口调用〉并确认文件不在返回的文件列表中”。另一种表述评估活动的特定通过/不通过准则的方法是确定是否符合已标识的标准中的特定条款,或与参考模型或示例集进行比较,如 ISO/IEC 18045 中的攻击潜在模型或为某些 IT 产品类型定义的特定攻击潜在模型。

然而,人们也认识到,准则通常需要考虑到不同 TOE 之间的实现细节的差异。因此,通过/不通过的准则也可根据评估活动的目的来描述(见 6.2.2)。

如果评估活动不需要得出通过/不通过的裁定,除了派生它的工作单元中给出的那些裁定,则这部分是不需要的。



### 6.2.9 报告要求

如 5.2.9 所述,可为评估活动指定报告的具体要求(在 ETR 中,也可能在其他产出物中)——这些要求可在评估方法层面或单独评估活动层面上说明。在这个层面上,报告的定义要求通常是通过记录特定问题的答案、结论的基本原理或对特定测试结果的清晰描述,来支持通过/不通过判断的可见性和可重复性。需要特别注意的是,如果通过/不通过准则预期要求评估者做出判断,那么报告的要求应包括对涉及作出判断和得出通过/不通过结论的特定原因的记录。

如果评估活动不需要报告或报告的详细信息,只需要派生它的工作单元中给出的那些要求,那么这个部分是不需要的。

### 6.2.10 评估活动的基本原理

评估活动应包括其从 ISO/IEC 18045 中的一个或多个工作单元(或扩展 SAR 的等效工作单元定义)推导的论证。该论证可包含的解释是,为何一定要针对特定技术或 TOE 类型评估的范围和深度来评估工作单元。评估方法(见 5.2.10)和评估活动层面的基本原理相结合,应证明评估方法涉及 ISO/IEC 15408-3 所适用的行为元素的所有方面。此外,组合的基本原理应描述如何从原始的行为元素或工作单元推导出的结论,以确保相对于评估活动拟应用的评估情景而言,评估活动是完整的。

注:基本原理能识别并证明某些方面不适用于其特定的评估情景。

如果评估活动定义的通过/不通过准则与它所派生的工作单元不同,则论证时应提供新准则的可行性和有效性的理由。

基本原理可在适当的情况下被认定是为评估情景所作的具体假设。

基本原理可在评估方法层面或在单独评估活动层面提出。

附 录 NA  
(资料性)  
缩 略 语

- EA:评估活动(Evaluation Activities)
- EM:评估方法(Evaluation Method)
- ETR:评估技术报告(Evaluation Technical Report)
- IT:信息技术(Information Technology)
- PP:保护轮廓(Protection Profile)
- SAR:安全保障要求(Security Assurance Requirement)
- SFR:安全功能要求(Security Functional Requirement)
- ST:安全目标(Security Target)
- TOE:评估对象(Target of Evaluation)

参 考 文 献

[1] GB/T 18336.5—2024 网络安全技术 信息技术安全评估准则 第 5 部分:预定义的安全要求包

[2] GB/T 30270—2024 网络安全技术 信息技术安全评估方法

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

[4] ISO/IEC 19896-3 IT security techniques—Competence requirements for information security testers and evaluators—Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

---









中 华 人 民 共 和 国  
国 家 标 准

网络安全技术 信息技术安全评估准则  
第 4 部分：评估方法和活动的规范框架  
GB/T 18336.4—2024/ISO/IEC 15408-4:2022

\*

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

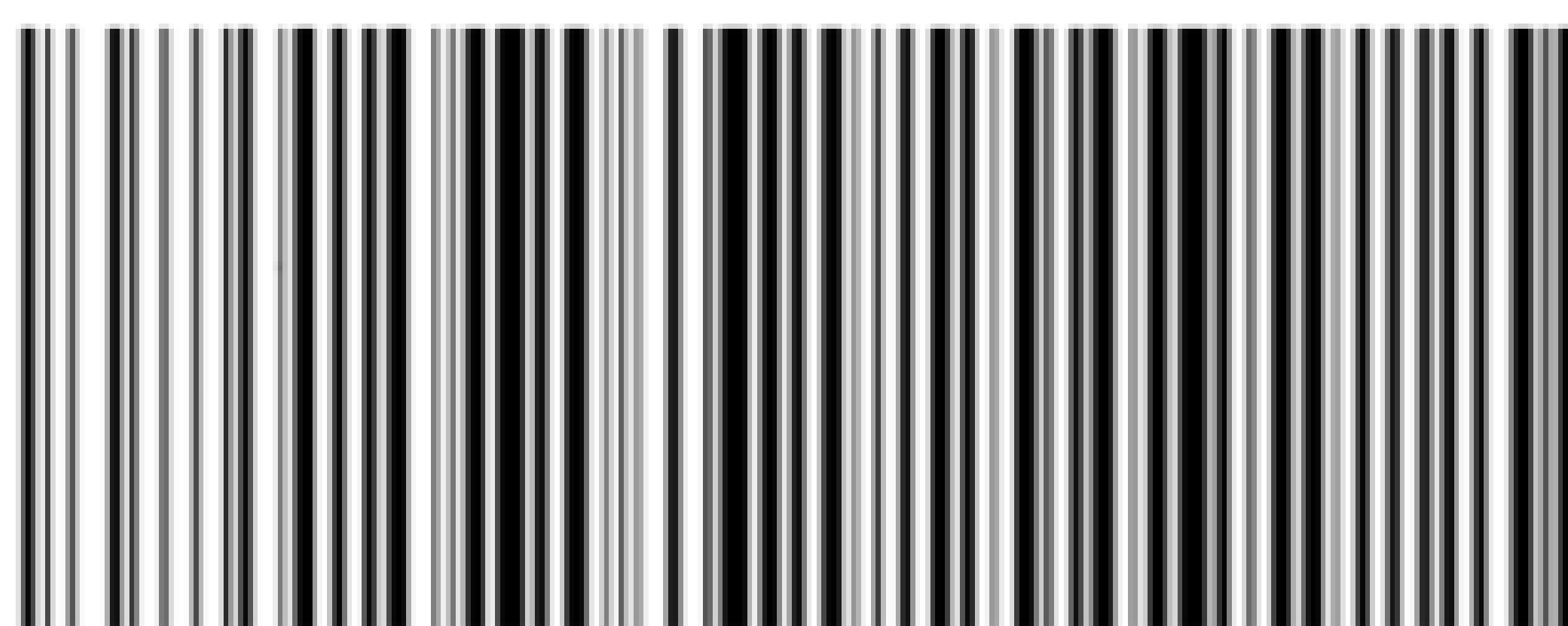
服务热线：400-168-0010

2024 年 4 月第一版

\*

书号：155066 • 1-75506

版权专有 侵权必究



GB/T 18336.4-2024