GB

中国国家标准汇编

600

GB 30270~30280

（2013年制定）

中国标准出版社

中国国家标准汇编

600

GB 30270～30280

（2013 年制定）

中国标准出版社　编

中国标准出版社

北　京

图书在版编目(CIP)数据

中国国家标准汇编:2013 年制定.600:
GB 30270～30280/中国标准出版社编.—北京:
中国标准出版社,2014.9
ISBN 978-7-5066-7681-6

Ⅰ.①中… Ⅱ.①中… Ⅲ.①国家标准-
汇编-中国-2013 Ⅳ.①T-652.1

中国版本图书馆 CIP 数据核字(2014)第 187901 号

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 37.25 字数 1 138 千字
2014 年 9 月第一版 2014 年 9 月第一次印刷

*

定价 220.00 元

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。它在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2.《中国国家标准汇编》收入我国每年正式发布的全部国家标准，分为“制定”卷和“修订”卷两种编辑版本。

“制定”卷收入上一年度我国发布的、新制定的国家标准，顺延前年度标准编号分成若干分册，封面和书脊上注明“20××年制定”字样及分册号，分册号一直连续。各分册中的标准是按照标准编号顺序连续排列的，如有标准顺序号缺号的，除特殊情况注明外，暂为空号。

“修订”卷收入上一年度我国发布的、被修订的国家标准，视篇幅分设若干分册，但与“制定”卷分册号无关联，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样。“修订”卷各分册中的标准，仍按标准编号顺序排列(但不连续)；如有遗漏的，均在当年最后一分册中补齐。需提请读者注意的是，个别非顺延前年度标准编号的新制定的国家标准没有收入在“制定”卷中，而是收入在“修订”卷中。

读者配套购买《中国国家标准汇编》“制定”卷和“修订”卷则可收齐由我社出版的上一年度我国制定和修订的全部国家标准。

3.由于读者需求的变化，自1996年起，《中国国家标准汇编》仅出版精装本。

4.2013年我国制修订国家标准共1 979项。本分册为“2013年制定”卷第600分册，收入国家标准GB 30270～30280的最新版本。

中国标准出版社

2014年8月

目　　录

ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30270—2013/ISO/IEC 18045:2005

信息技术 安全技术 信息技术安全性评估方法

Information technology—Security technology—Methodology for IT security evaluation

(ISO/IEC 18045:2005,IDT)

2013-12-31 发布　　2014-07-15 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

信息技术 安全技术 信息技术安全管理指南

Information technology — Security techniques — Information technology security management guidelines

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准采用翻译法等同采用国际标准 ISO/IEC 18045:2005《信息技术　安全技术　信息技术安全性评估方法》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 18336—2008　信息技术　安全技术　信息技术安全性评估准则(ISO/IEC 15408:2005,IDT)。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位：中国信息安全测评中心、吉林信息安全测评中心、华中信息安全测评中心。

本标准主要起草人：李守鹏、吴世忠、黄元飞、李斌、刘晖、刘春明、郭颖、付敏、谭运猛、徐长醒、宋小龙、简余良、郭涛、甘杰夫、张宝峰、石竑松、杨永生、毕海英、高金萍、王峰、李凤娟、唐喜庆、曾华春。

引　言

本标准提出的信息技术(IT)安全性评估方法仅限于对 ISO/IEC 15408 中定义的 EAL1～EAL4 评估，不提供 EAL5～EAL7 及其他保证包的评估指南。

本标准的读者对象主要是采用 ISO/IEC 15408 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。

本标准并不能解决所有有关 IT 安全评估的问题，有些问题还需要进一步的解释。这些解释将由各评估体制决定如何处理，即便它们要遵从多方互认协议。可以由各体制处理的评估方法相关活动列表见附录 A。

本标准提出了依据 ISO/IEC 15408《信息技术　安全技术　信息技术安全性评估准则》进行信息技术安全评估时的评估方法，是 ISO/IEC 15408 的配套标准。

信息技术　安全技术
信息技术安全性评估方法

1　范围

本标准描述了在采用 ISO/IEC 15408《信息技术　安全技术 信息技术安全性评估准则》所定义的准则和评估证据进行评估时，评估者应执行的最小行为集，是 ISO/IEC 15408 的配套标准。

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(包括所有的修改版)适用于本文件。

ISO/IEC 15408(所有部分)　信息技术　安全技术　信息技术安全性评估准则(Information technology—Security techniques—Evaluation criteria for IT security)

3　术语和定义

下列术语和定义适用于本文件。

3.1

行为　action

ISO/IEC 15408-3 的评估者行为元素。这些行为在 ISO/IEC 15408-3 保证组件中要么是直接声明为评估者行为，要么是间接从开发者行为(隐含的评估者行为)中导出。

3.2

活动　activity

ISO/IEC 15408-3 保证类的施用。

3.3

核查　check

通过简单比较形成一个裁定。评估者不一定必须具备专门技能。使用此动词的语句描述了需要核查的内容。

3.4

评估交付件　evaluation deliverable

评估者或监督者为执行一个或多个评估或评估监督活动所必需的，由发起者或开发者提交的所有资源。

3.5

评估证据　evaluation evidence

真实的评估交付件。

3.6

评估技术报告　evaluation technical report

由评估者编写并呈交给监督者、以文档形式记录总体裁定及其理由的报告。

3.7

检查 examine

评估者通过采用专业技能分析形成一个裁定。使用此动词的语句表明哪些是分析对象以及对象的哪些属性。

3.8

解释 interpretation

对 ISO/IEC 15408 中的要求、本标准中的要求或体制要求的一种澄清或详述。

3.9

方法 methodology

用于 IT 安全性评估的原则、程序和过程组成的体系。

3.10

观察报告 observation report

在评估过程中由评估者编写的用于澄清或标识一个问题的报告。

3.11

总体裁定 overall verdict

评估者发布的关于评估结果是“通过”还是“不通过”的决定。

3.12

监督裁定 oversight verdict

根据评估监督活动的结果，监督者发布的认可或否决总体裁定的决定。

3.13

记录 record

记录过程、事件、观察结果、所了解事项以及结果的书面描述。该描述需足够详细，以便评估过程中执行的工作能够重现。

3.14

报告 report

将评估结果和支持性材料纳入到评估技术报告或观察报告。

3.15

方案 scheme

评估管理机构制定的一套规则，这套规则定义了评估环境，包括 IT 安全评估所需的准则和方法。

3.16

子活动 sub-activity

ISO/IEC 15408-3 中一个保证组件的施用。本标准不处理保证族，因为评估子活动只用到保证族中的单个保证组件。

3.17

追溯 tracing

两个实体集合之间的简单定向关系，表明第一个集合中的哪些实体与第二集合中的哪些实体相对应。

3.18

裁定 verdict

评估者发布的关于 ISO/IEC 15408 中一个评估者行为元素、保证组件或类是“通过”“不通过”，还是“待定”的一项决定。

3.19

工作单元 work unit

评估工作的最小组成部分。每个评估方法行为由一个或多个工作单元组成，这些工作单元按照ISO/IEC 15408中“证据的内容和形式元素”或“开发者行为元素”组织到评估方法行为中。在本标准中，工作单元的呈现顺序与导出它们的ISO/IEC 15408元素的呈现顺序相同。工作单元用形如“4：ALC_TAT.1-2”的符号标识，其中第一个数字“4”表示EAL等级，字符串ALC_TAT.1表示ISO/IEC 15408组件(即本标准的子活动)，最后一个数字“2”代表这是子活动ALC_TAT.1的第二个工作单元。

4 缩略语

下列缩略语适用于本文件。

ETR：评估技术报告(Evaluation Technical Report)

OR：观察报告(Observation Report)

5 概述

5.1 本标准的组织

第6章定义了本标准中使用到的一些约定。

第7章描述了不需要做出裁定的通用评估任务，这些任务没有映射到ISO/IEC 15408评估者行为元素。

第8章定义了保护轮廓(PP)评估。

第9章定义了安全目标(ST)评估。

第10章～第13章定义了为完成EAL1～EAL4评估而需要的最小评估努力，并提供了完成评估的方法和手段指南。

第14章定义了缺陷纠正评估活动。

附录A提出了一些基本评估技术，用于为评估结果提供技术性证据。

6 文档约定

6.1 行文方式

ISO/IEC 15408中每个元素相对于族中所有组件都保持其标识符的最末一个数字不变，本标准则不同，当ISO/IEC 15408中的评估者行为元素从一个子活动变换到另一个子活动时，本标准可引入新的工作单元，因此，尽管工作单元没有改变，工作单元标识符的最末一个数字可以改变。例如，一个附加的工作单元，其标记为4：ADV_FSP.2-7被添加到EAL4，后续的FSP工作单元顺序号偏移了一位，此时工作单元3：ADV_FSP.1-8对应于工作单元4：ADV_FSP.2-9，这样表示虽然他们的编号不再直接对应但却是相同的要求。

任何不需要直接从ISO/IEC 15408要求中导出的特定方法论评估工作称为*任务*或*子任务*。

6.2 动词用法

在所有工作单元和子任务动词前都加以助动词“应”，并且动词和“应”都用***粗斜体***表示。只有当规定的条文是强制要求的时，才使用助动词“应”。为了得出裁定，评估者应执行工作单元和子任务中包含的强制活动。

工作单元和子任务附带的指导性条文给出了如何在一个评估中使用 ISO/IEC 15408 语句的进一步解释。描述方法是标准化的，也就是说助动词的用法与 GB/T 1.1 的约定是一致的，即：助动词“宜”表示强烈推荐该方法，“可”表示允许使用该方法但不是首选的（助动词“应”只用在工作单元或子任务中）。

动词“核查”“检查”“报告”和“记录”在本标准中有确定的意义，在使用时请参见第 3 章的定义。

6.3 通用评估指南

适用于多个子活动的指导性材料被集中到一个地方。适用性很广泛（跨越活动和 EAL）的一些指导性条文已统一放在附录 A 中。在各个活动的简介部分已提供了适合于该活动中多个子活动的指南。如果指南只适合某单一的子活动，则它在子活动中进行描述。

6.4 ISO/IEC 15408 和本标准结构间的关系

ISO/IEC 15408 结构（即类、族、组件和元素）与本标准的结构之间有直接的关系。图 1 说明了 ISO/IEC 15408 结构的类、组件和评估者行为元素对应本标准的活动、子活动和行为之间的关系。另外，有些评估方法工作单元可以从 ISO/IEC 15408 的“开发者行为元素”和“证据的内容和形式元素”中得出。如图 1。

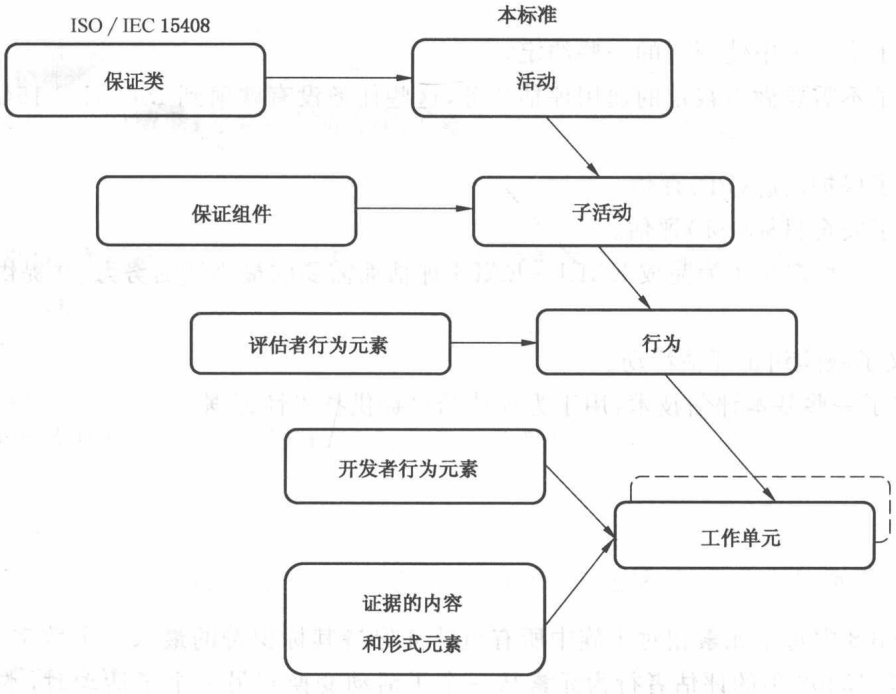

图 1 ISO/IEC 15408 与本标准结构间的映射

6.5 评估者裁定

评估者是对否满足 ISO/IEC 15408 的要求给予裁定而不是本标准的要求。要给予裁定的最小 ISO/IEC 15408 结构是评估者行为元素（明显的或隐含的）。作为执行相应评估方法行为及其组成工作单元的结果，每个 ISO/IEC 15408 评估者行为元素均被赋予一个裁定。最后给出 ISO/IEC 15408-1 的 6.3 所述的评估结果。

本标准认可三种互相排斥的裁定情形：

a） 通过：评估者完成了 ISO/IEC 15408“评估者行为元素”，并确定接受评估的 PP、ST 或 TOE 的

要求得到满足。通过评估的条件在相关行为的组成工作单元中给定；

b) 待定：评估者未完成与 ISO/IEC 15408 评估者行为元素相关的一个或多个评估方法行为工作单元；

c) 不通过：评估者完成了 ISO/IEC 15408 评估者行为元素并确定接受评估的 PP、ST 或 TOE 未满足要求。

所有的裁定最初都是“待定”，直到被赋予“通过”或“不通过”裁定为止。

当且仅当所有组成部分的裁定都为“通过”，总体裁定才为“通过”。如图 2 所示，如果某个评估者行为元素的裁定为“不通过”，则相应保证组件、保证类的裁定和总体裁定都为“不通过”。

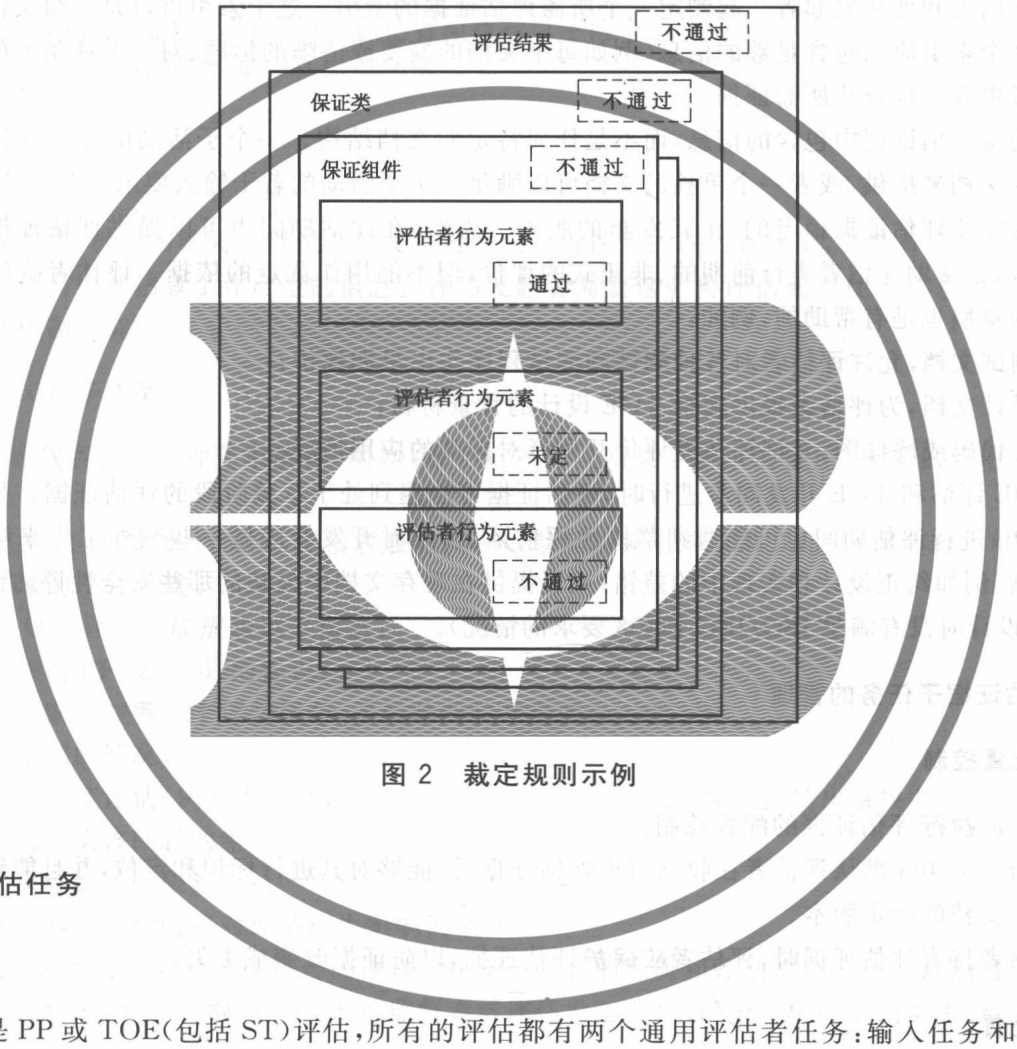

图 2 裁定规则示例

7 通用评估任务

7.1 简介

不管是 PP 或 TOE(包括 ST)评估，所有的评估都有两个通用评估者任务：输入任务和输出任务。这两个任务与评估证据的管理和报告的产生有关，本章对其进行了描述。每一个任务由一些适用于所有 ISO/IEC 15408 评估(PP 或 TOE 评估)的标准化的子任务组成。

尽管 ISO/IEC 15408 没有专门强制要求这些评估任务，但是本标准在其需要的地方进行了强制要求。不同于本标准中其他章节描述的活动，本章的这些任务没有与之关联的裁定，因此不能映射到 ISO/IEC 15408 评估者行为元素，执行它们就是为了遵守本标准。

7.2 评估输入任务

7.2.1 目的

本任务的目的是确保评估者能够获得正确版本的评估证据，且证据得到了充分保护。否则，就不能保证评估的技术精确性，也不能保证评估结果的可重复性和可再现性。

7.2.2 应用注释

提供所有必需的评估证据是评估发起者的责任。然而，大多数评估证据很可能是由开发者（代表评估发起者）产生和提供的。因为保证要求适用于整个 TOE，所以要使 TOE 组成部分的所有产品有关的评估证据对评估者都是可用的。这种评估证据的范围和所需内容不依赖开发者对每个产品（即 TOE 的组成部分）的控制水平。例如，如果要求高层设计，则 ADV_HLD“高层设计”要求将适用于所有子系统（即 TSF 的组成部分）。此外，需要采用核查程序的保证要求（例如 ALC_CAP“CM 能力”和 ALC_DEL“交付”）将适用于整个 TOE（包括来自其他开发者的任何部分）。

建议评估者和评估发起者一起制定一个所需评估证据的索引。这个索引可以是一组文件参考资料的集合。这个索引应当包含足够的信息（例如每个文档的摘要或清晰的标题、对所关注条款的标记），以方便评估者更容易地查找所需证据。

需要的是评估证据中包含的信息，而不是任何特定的文档结构。一个子活动的评估证据可以通过一些不同的文档来提供，或者一个单独的文档可以满足一个子活动的若干输入要求。

评估者需要评估证据稳定的、正式发布的版本。当然，在评估期间也可以提供评估证据草稿。例如，草稿可用于帮助评估者进行前期的、非正式的评价，但不能用作裁定的依据。评估者查阅以下特定评估证据的草稿也是有帮助的，例如：

a) 测试文档，允许评估者对各种测试和测试程序作出早期评价；

b) 设计文档，为评估者提供理解 TOE 设计的背景材料；

c) 源代码或硬件图，允许评估者评价开发者对标准的应用情况。

在 TOE 评估和 TOE 开发同步进行时，评估证据可能遇到处于草稿阶段的评估证据。另外对已开发好的 TOE 进行评估期间也可能遇到草稿性评估证据，此时开发者应做一些额外工作来解决评估者提出的问题（例如纠正设计和实现中的差错）或者提供在现存文档中欠缺的那些安全性评估证据（例如，TOE 最初设计时没有满足 ISO/IEC 15408 要求的情况）。

7.2.3 评估证据子任务的管理

7.2.3.1 配置控制

评估者***应执行***评估证据的配置控制。

ISO/IEC 15408 默认评估者在收到每项评估证据后，能够对其进行标识和定位，并且能够确定评估者是否拥有文档的特定版本。

当评估者持有评估证据时，评估者***应保护***评估证据，以防证据改变或丢失。

7.2.3.2 处置

在评估结束时，评估方案需要控制评估证据的处置。应当用以下一种或几种方式处置评估证据：

a) 归还评估证据；

b) 存档评估证据；

c) 销毁评估证据。

7.2.3.3 保密性

在评估过程中，评估者可能接触到评估发起者和开发者的一些商业性敏感信息（例如 TOE 设计信息、专门工具），还可能接触到一些国家级敏感信息。评估发起者可能希望要求评估者维护评估证据的保密性。在保持与评估体制协调一致的前提下，评估发起者和评估者可以协商增加其他要求。

保密性要求会在许多方面影响评估工作，包括对评估证据的接收、处理、存储和处置。

7.3 评估输出任务

7.3.1 目的

本条的目的是描述观察报告(OR)和评估技术报告(ETR)。评估体制可能还需要其他评估者报告(例如有关单个工作单元的报告),或者还要求在 OR 和 ETR 中包含其他信息。本标准并不排除在这些报告中加入其他信息,因为本标准只规定了最少的信息内容。

为满足评估结果的可重复性和可再现性原则,评估结果报告应保持一致性。一致性涵盖 ETR 和 OR 中所报告信息的类型和数量。不同评估间 ETR 和 OR 的一致性由监督者负责。

为使报告内容达到本标准的要求,评估者应执行以下两个子任务:

a) 编写 OR 子任务(如果评估需要的话);

b) 编写 ETR 子任务。

7.3.2 应用注释

在本标准中,没有明确要求提供有关支持再评估和再使用的评估者证据,也没有确定有关为协助再评估或再使用而由评估者工作产生的信息。评估发起者需要这些再评估或再使用信息时,应当向当前所处的评估体制咨询。

7.3.3 编写 OR 子任务

OR 为评估者提供一种要求解释(例如,需要监督者说明某个要求的使用)或确认评估中某个问题的机制。

在裁定为"不通过"的情况下,评估者***应提供***OR,以反映评估的结果。此外,评估者也可以使用 OR 作为表达需求的一种方式。

对每个 OR,评估者***应报告***以下信息:

a) 被评估 PP 或 TOE 的标识;

b) 该观察是在哪一个评估任务/子活动期间产生的;

c) 观察到的情况;

d) 严重程度评估(例如失败裁定、阻碍评估进展、需要在评估完成前给出解决办法);

e) 负责解决该问题的组织;

f) 解决问题的时限建议;

g) 问题解决失败时将对评估产生影响的估计。

OR 报告的目标读者及处理报告的流程取决于该报告的性质和评估体制。评估体制可根据所要求的信息和分发对象的不同(例如,OR 要给监督者或评估发起者)来区分 OR 的不同类型,或者定义附加类型。

7.3.4 编写 ETR 子任务

7.3.4.1 目的

评估者***应提供***一份 ETR,以给出裁定的技术依据。

ETR 可能包含开发者或评估发起者的专有信息。

本标准定义了 ETR 的最少内容要求,评估体制还可以指定其他内容和结构要求。例如,评估体制可以要求 ETR 中包含某些介绍性材料(例如免责声明和版权声明条款)。

ETR 的读者需要被假定为熟悉信息安全常规概念、ISO/IEC 15408、本标准、评估方法以及 IT。

ETR 支持监督者作出监督裁定,但是不能期望 ETR 提供监督需要的所有信息,并且该文档也无法提供必要证据供评估体制确认评估是否依据相关标准执行,这已超出本标准范围,应当用其他监督方式

来满足。

7.3.4.2 PP 评估的 ETR

本条描述 PP 评估的 ETR 所需要的最少内容。ETR 的内容如图 3 所示，在构建 ETR 文档的结构大纲时，可以此图作为指南。

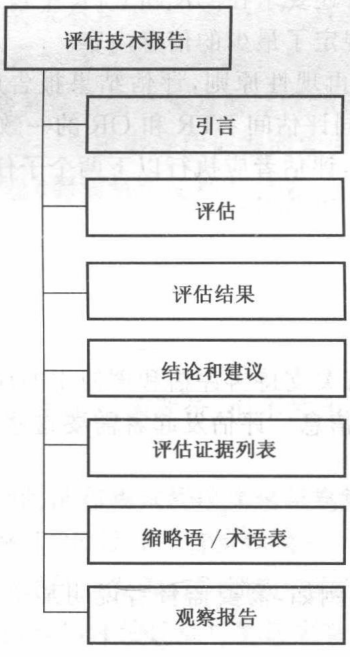

图 3 PP 评估的 ETR 信息内容

7.3.4.2.1 引言

评估者***应报告***评估体制的标识。

评估体制标识(例如标志)是明确地标识负责评估监督的评估体制信息。

评估者***应报告***ETR 配置控制标识。ETR 配置控制标识包含标识 ETR 的信息(例如，名称、日期、版本号)。

评估者***应报告***PP 配置控制标识。PP 配置控制标识(例如，名称、日期、版本号)用于标识出所评估的 PP，以便监督者核查评估者是否给出了正确的裁定。

评估者***应报告***开发者的身份。PP 开发者的身份用以标识出谁负责产生该 PP。

评估者***应报告***评估发起者的身份。评估发起者的身份用以标识出谁负责向评估者提供评估证据。

评估者***应报告***评估者的身份。评估者的身份用以标识出谁执行评估并且对评估裁定负责。

7.3.4.2.2 评估

评估者***应报告***所使用的评估方法、技术、工具和标准，注明在评估 PP 时所使用的评估准则、方法和解释。

评估者***应报告***所有对评估的限制、对评估结果处理的限制以及在评估期间所做的对评估结果有影响的假设。评估者可在报告中加入与法律法规、组织机构、保密性等相关的信息。

7.3.4.2.3 评估结果

评估者***应***针对组成 APE 活动的每个保证组件，***报告***其所作出的裁定及相应的基本原理，作为执行相应评估方法行为及其组成工作单元的结果。

基本原理应使用 ISO/IEC 15408、本标准、相关解释以及经过检查的评估证据来证明评估裁定是正