# 国家信息安全测评

# 信息技术产品分级评估
# 业务白皮书


版本：5.1



2017 年 12 月

# 目　录

# 1 引言

信息技术产品分级评估是指依据国家标准 GB/T 18336—2015《信息技术 安全技术 信息技术安全评估准则》，综合考虑产品的预期应用环境，通过对信息技术产品的整个生命周期，包括技术、开发、管理、交付等部分进行全面的安全性评估和测试，验证产品的保密性、完整性和可用性程度，确定产品对其预期应用而言是否足够安全，以及在使用中隐含的安全风险是否可以容忍，产品是否满足相应评估保障级的要求。

# 2 目的和意义

信息技术产品分级评估的目的是促进高质量、安全和可控的 IT 产品的开发，分级评估具体的目的和意义包括：

1）深层次排除产品的信息安全隐患；

2）帮助用户选择安全可靠的信息产品；

3）有助于在涉及国家安全的信息安全领域中加强产品的安全性和可控性；

4）促进信息技术产业的稳步成熟和信息技术产品市场规范化。

# 3 业务范围

具有安全功能的信息技术产品，如：防火墙、IDS/IPS、智能卡、芯片、USBKey、扫描器、安全审计、数据库、操作系统等。

目前受理的级别包括：EAL1、EAL2、EAL3、EAL4、EAL5、EAL6、EAL7 及相应增强级，如 EAL3+、EAL4+、EAL5+。

# 4 业务特点

## 4.1 国家权威，国际认可

测评中心多年来依据国家授权对外开展测评业务，出具的测评报告具有权威性。测评中心依据国标 GB/T 18336—2015 开展分级评估业务，该标准等同采用国际标准 ISO/IEC 15408，所采用的评估方法均为国际通用方法，具备国际认可基础。

### 4.2 公平公正，客观规范

测评中心是第三方的独立测评机构，不代表任何商业组织的利益，出具的测评报告以事实为依据，以公平、公正为准则。测评活动严格按照质量体系相关要求执行，实事求是，确保测评的一致性和完整性。

### 4.3 测评专业，技术领先

测评中心是国内最早开展产品分级评估业务的专业职能机构，长期以来从事信息技术产品分级评估工作，拥有专业的评估队伍、一流的测试环境和丰富的评估技术手段。掌握国内外对信息技术产品的最新研究成果和发展趋势，测评技术达到国内领先水平。

## 5 业务实施

### 5.1 证据需求

根据业务内容的要求，申请方需提交的证据包括：

- 分级评估申请书
- 分级文档（注：见《分级文档编写指南》）
- 评估对象（TOE）
- 实现安全功能的源代码（注：EAL4 级及以上需此项）

### 5.2 业务流程

业务流程如下图 1 所示：

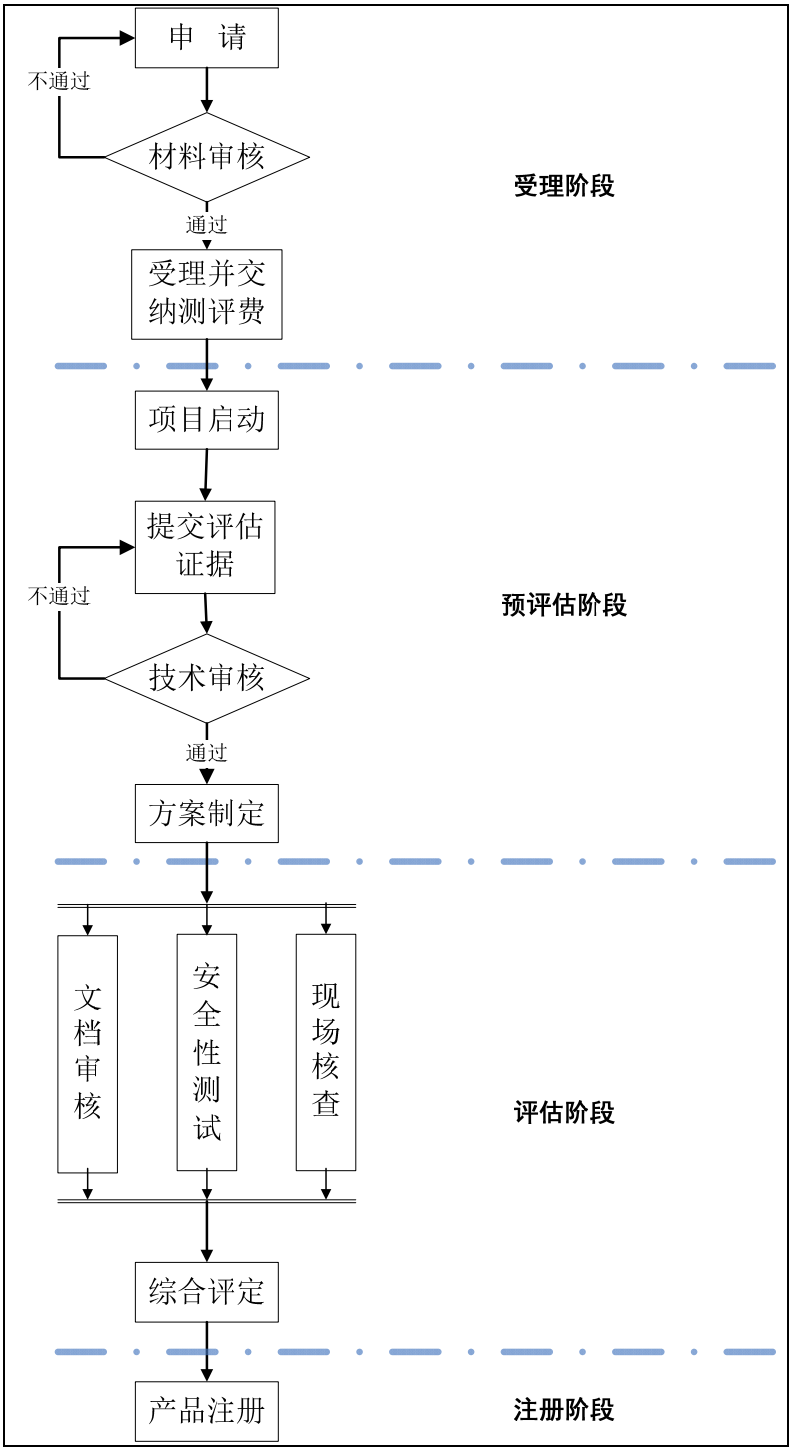


图 1 业务流程图

信息技术产品分级评估流程主要分为受理阶段、预评估阶段、评估阶段、注册阶段等四个阶段。

1） 受理阶段

申请方向测评中心提出分级评估申请。由受理人员对申请方提交的申请书进行审核。如果未通过审核，受理部门会根据提交材料的实际情况提出反馈意见，

申请方应根据反馈意见进行补充或修改。通过审核后，执行受理审批流程，申请方签订测评协议、交纳测评费用。

2） 预评估阶段

受理完成后，申请方应提交符合测评要求的产品。确认收到产品后，评估组人员通知申请方评估工作正式启动，并将需申请方配合的相关事宜一并告知，同时，评估组人员先对文档材料进行技术审核，来判定提交的材料内容是否符合要求。如果未通过审核，评估人员会根据提交材料的实际情况提出反馈意见，申请方应根据反馈意见进行补充或修改，并提交修改后的文档。通过审核后，评估组人员根据申请的级别制定评估方案。

3） 评估阶段

评估方案制定完成后，评估组人员根据方案，严格遵照评估进度开展评估工作，必要时可要求申请方提供技术支持，及配合完成有关操作。评估中出现的属于申请方的问题，评估组出具观察报告交由申请方签字确认。

在测评过程中如发现被测产品存在技术问题，申请方可选择进行回归测试或者主动放弃合同权益。如进行回归测试，则申请方在收到回归测试通知单后应及时反馈。回归测试需要申请方承担额外的费用，具体费用根据发现问题的复杂或难易程度等核算工作量来收取。

评估组人员根据各评估内容的评估结果，进行综合评定，并出具评估技术报告，该报告将作为产品是否通过分级评估的直接依据。

评估报告交由专家评审组进行评审，通过后进入下一阶段。

4） 注册阶段

通过评估的产品，测评中心对其进行注册及颁发证书，并将结果公布于测评中心的网站和杂志。

证书有效期为 3 年，在证书有效期届满前，由申请方向测评中心重新提出分级评估申请。通过评估的产品，测评中心将为其颁发新的证书。

## 5.3 评估内容

评估内容主要包括评估活动、安全性测试、现场核查共三个方面。

1）评估活动主要包括：

- 安全目标评估
- 开发活动评估
- 指导性文档评估
- 生命周期支持评估，包括配置管理、交付、开发安全、生命周期定义等
- 测试评估

- 脆弱性评定评估

GB/T 18336—2015第3部分对各个保障级别所需的文档内容有严格的要求，随着分级评估保障级别的增加，所需提交的文档所包含的内容就越全面，同时对每个文档内容的要求也越高。

2）安全性测试主要包括：

- 独立性测试：为了验证被评估产品所提供的安全功能是否能够正确实现，评估者从申请方提供的测试文档中抽取一定数量的测试用例，并经重新设计后来完成对安全功能的验证性测试操作。
- 穿透性测试：评估者通过实施穿透性测试，验证被评估产品在预期环境下是否存在明显的可被利用的脆弱性，从而威胁产品及其保护资产的安全。
- 安全性能测试：对于存在性能测试需求的产品，评估者参考RFC2544、RFC3511等标准和规范，对被评估产品实施安全性能测试。

3）现场核查主要包括：

- 核查配置管理、交付、开发安全。现场核查的形式包括文档证据审查、实际环境审查以及与有关人员交流。EAL3级（含）以上分级评估将进行现场核查。现场核查约在评估过程进行至70%左右时进行。

## 5.4 评估时间

评估开始时间为申请方接到项目启动通知单的时间，评估结束时间为信息安全实验室出具评估技术报告的时间。

一般情况下，常规信息技术产品的评估参考时间如下：

- EAL1：20个工作日
- EAL2：40个工作日
- EAL3：60个工作日
- EAL4：90个工作日
- EAL5：120个工作日

## 5.5 评估费用

根据申请的保障级别、产品的复杂程度等方面核定工作量，确定评估费用。

## 5.6 业务输出

分级评估业务的输出：评估技术报告、测评证书。