ICS 35.040
L 80

团 体 标 准

T/ISEAA 00*-202*

信息安全技术 网络安全等级保护 应用软件开发安全管理要求

Information security technology – Requirements of secure management on developing of application software for classified protection of cybersecurity

20XX -XX-XX 发布　　20XX -XX-XX 实施

中关村信息安全测评联盟 发布

目　　次

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。

本文件由中关村信息安全测评联盟提出并归口。

本文件起草单位：。

本文件主要起草人：。

引　言

为了进一步保证各类网络的应用安全，提升应用软件上线运行前的安全性，降低网络运行后的各类风险，尤其是开发数据安全所面临的风险，本文件将GB/T 22239-2019和GB/T 28448-2019的通用安全管理要求中关于软件开发的相关安全管理要求进一步细化和扩展，提出应用软件开发过程应遵循的安全管理要求和测评要求。

本文件是网络安全等级保护相关系列标准之一。

与本文件相关的标准包括：

——GB/T 22239 《信息安全技术 网络安全等级保护基本要求》

——GB/T 28448 《信息安全技术 网络安全等级保护测评要求》

——GB/T 38674 《信息安全技术 应用软件安全编程指南》

在本文件中，**加黑部分**表示较高等级中增加或增强的要求。

信息安全技术 网络安全等级保护应用软件开发安全管理要求

1 范围

本文件规定了应用软件开发过程的安全管理要求和测评要求，从提升软件开发安全的角度对开发过程安全提出相关管理要求。安全保护等级为第一至四级的等级保护对象适用于本文件，第五级的等级保护对象相关要求不在本文件描述。

本文件适用于应用软件开发机构、对软件开发过程具有安全管理需求的软件采购/使用机构以及第三方软件安全评估机构用于对应用软件开发过程进行监督管理和安全评估。

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。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

3 术语和定义

GB/T 22239-2019、GB/T 25069-2022、GB/T 30273—2013、GB/T 29246-2017界定的以及下列术语和定义适用于本文件。

3.1

应用软件 application software

专门解决应用问题的软件或程序。

注：应用软件不同于控制计算机本身的软件。

[GB/T 25069-2022，定义3.730]

3.2

基线 baseline

a)业已经过正式审核与同意，可用作下一步开发的基础，并且只有通过正式的修改管理过程方能加以修改的规格说明或产品；

b)在配置项目生存周期的某一特定时间内，正式指定或固定下来的配置标识文件和一组这样的文件。基线加上根据这些基线批准同意的改动构成了当前配置标识；

c)任何协议或在一给定时间赋予或固定的结果，如要变更，要求证明和批准。

[GB/T 11475-2006，定义 2.125]

3.3

软件开发周期 software development cycle

从决定开发一个软件产品开始到产品交付结束的时间周期。这个周期典型的包括需求阶段、设计阶段、实现阶段、测试阶段、有时还包括安装和验收阶段。

注：a)上列的阶段可以覆盖或者重复执行，取决于所用的软件开发方法。

b)此术语有时用于含义更长的时间周期，或者当软件不再由开发者增强而结束的时间周期或即整个软件生存周期(software life cycle)

[GB/T 11475-2006，定义 2.1483]

3.4

测试 testing

通过对测评对象按照预定的方法/工具使其产生特定的行为，获取证据以证明被测对象安全保障措施是否有效的一种方法。

[GB/T 30273—2013，定义 3.12]

3.5

验证 verification

通过提供客观证据，证实满足规定要求的行为。

Note 1 to entry: This could also be called compliance testing.

注：这也可被称为符合性测试。

[GB/T 29246—2017，定义 2.88]

3.6

威胁 threat

可能对系统或组织造成危害的不期望事件的潜在原由。

[GB/T 29246—2017，定义 2.83]

4 概述

4.1 软件开发周期安全管理框架

本文件从应用软件开发周期应遵循的安全管理要求角度提出测评要求，分为管理对象安全和管理过程安全两大方面。其中，管理对象安全主要包括安全管理制度、人员安全管理、环境安全管理、开发工具安全管理等内容；管理过程安全主要遵循应用软件开发周期各个环节(即，需求、设计、开发、测试、发布和交付等环节)提出的安全管理要求。整体安全管理框架如下图所示：

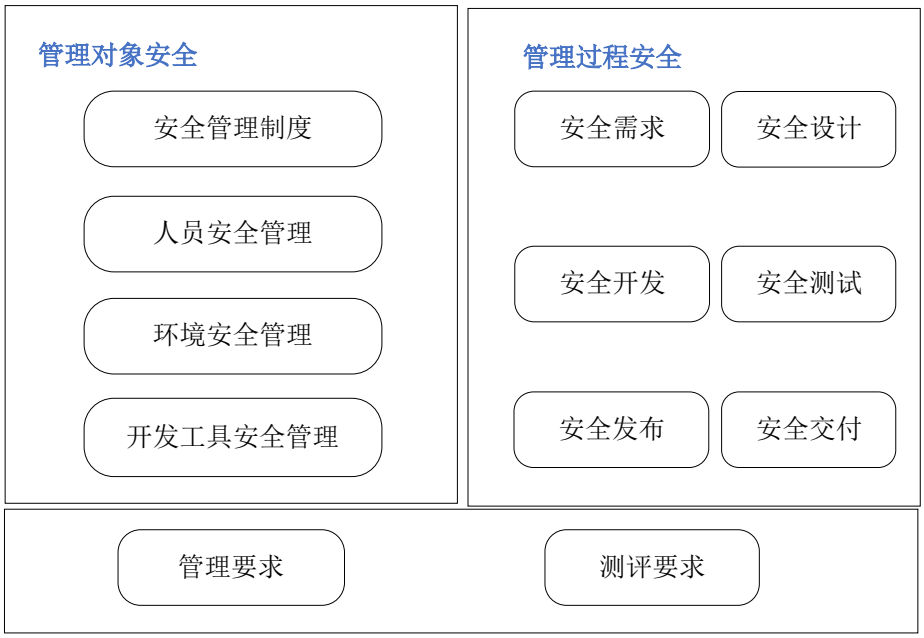

图1 应用软件开发周期安全管理框架图

其中，安全管理制度主要针对软件开发过程需遵循的各类管理制度、操作规范和记录表单等的制定、发布、执行、检查以及维护修订等生命周期关键活动进行规范；人员安全管理主要针对软件开发中涉及的各类岗位人员的设置、配备、任职、培训和离职等关键活动进行规范；环境安全管理主要针对各类开发环境、测试环境的安全隔离、访问控制以及各类数据备份管理等建设和运维活动进行规范；开发工具安全管理主要针对开发过程中涉及的各类工具的准入、使用以及回收等生命周期关键活动进行规范。开发过程安全管理主要针对软件开发全生命周期的需求、设计、开发、测试、发布和交付等环节的各类管理要求进行规范。

管理要求主要针对软件开发管理对象安全和管理过程安全提出相应的要求；测评要求则针对管理要求描述如何判断该要求项实现情况的测评方法，具体以测评单元为描述方法，每个测评单元包括测评指标、测评对象、测评实施和测评结果四个部分。

4.2 测评等级描述

测评等级分为基本级（LB）和增强级(LI)。安全保护等级为第二级及以下的安全保护对象，其应用软件开发过程的安全管理要求参考基本级（LB）管理要求；安全保护等级为第三级及以上的安全保护对象，其应用软件开发过程安全管理要求除基本级管理要求外，还需参考增强级管理要求(LI)。

5 安全管理要求

5.1 安全管理制度(SMS)

5.1.1 制定和发布

a) 应建立软件安全开发管理制度，明确软件开发各环节的安全管理要求和人员行为准则等；
b) 应制定安全开发操作指南和管理流程；
c) 应确保各类开发管理制度、操作指南、流程表单等正式发布。

5.1.2 执行和修订

a) 应定期开展软件开发安全管理制度执行情况检查；
b) 应定期对各类软件开发安全管理制度进行修订并更新。(LI)

5.2 人员安全管理(SSM)

5.2.1 岗位设置和人员配备

a) 应设立软件开发岗、测试岗、安全岗等岗位，并明确各岗位安全职责；
b) 应根据岗位需求配备相应岗位人员，安全岗位不得兼任。(LI)

5.2.2 人员任职

a) 应与各岗位人员签署保密协议，关键岗位人员签署岗位安全协议；(LI)
b) 应建立人员上岗前安全考核机制，未通过考核不得上岗。(LI)

5.2.3 人员培训

a) 应对各岗位人员开展管理制度宣贯、开发安全意识、保密教育等方面培训；
b) 应针对不同岗位制定不同培训计划，并进行培训考核。(LI)

5.2.4 人员离岗

a) 应及时终止离岗人员所有访问权限(包括但不限于代码库、软件开发文档等)，并取回全部资产。

5.2.5 第三方人员管理

a) 应制定第三方人员管理制度，至少涵盖人员进出管理、账号及权限管理、行为操作管理等内容。

5.3 环境安全管理(ESM)

5.3.1 环境建设管理

a) 应建立并使用专用的软件开发过程中涉及的研发、测试、发布等环境，并与外部环境进行必要的隔离；
b) 应建立软件开发过程中相关环境的资产清单，至少包括名称、版本、安装的软件组件、适用项目范围等信息；
c) 应建立软件开发过程中相关环境安全基线要求，包括但不限于软件组件更新规范、安全策略配置规范、入侵防范措施等；
d) 应建立软件开发过程中相关环境的配置操作手册，并依据手册进行配置。

5.3.2 环境运维管理

a) 应对软件开发过程中涉及的研发、测试、发布等环境建立明确的权限管控机制；
b) 应建立环境远程访问策略，确保外部通信接口或通道经授权后方可传输数据，并在使用结束后关闭接口或通道；
c) 应建立环境变更审批规范，明确在线开发、协同开发等事项的审批过程；
d) 应对软件开发核心代码及重要文档进行权限管理，并对重要操作进行日志记录；(LI)
e) 应定期离线备份环境配置文件、软件开发代码及重要文档等，并进行版本控制；(LI)
f) 应建立软件开发相关环境中敏感信息的保护机制，确保敏感信息不被泄露；(LI)
g) 应定期检查违反环境安全基线的行为，包括软件组件更新情况、安全策略配置情况、入侵防范措施配置情况等内容；(LI)

h) 应定期执行软件开发过程中相关环境的安全漏洞扫描，扫描类型包括但不限于主机扫描、容器扫描、端口扫描等，并对发现的问题及时进行处置。(LI)

5.4 开发工具安全管理(TSM)

5.4.1 工具准入管理

a) 应根据软件所承载的数据重要性，制定并保存开发工具清单，至少包括工具信息、来源信息、重要程度、责任人等内容；
b) 应对工具准入建立审批程序，按照审批程序执行审批过程；
c) 应制定供应商选择策略和制度，并根据开发工具重要程度开展供应商评审，形成供应商清单；(LI)
d) 应制定开发工具的组件清单，记录并保留开发工具所用组件的基本信息。(LI)

5.4.2 工具使用管理

a) 应对重要开发工具进行登录用户身份标识和鉴别,身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
b) 应对重要开发工具建立权限策略管理机制；
c) 应记录并保存重要开发工具的操作日志，日志保存时间不少于为 6 个月；
d) 应对开发工具定期进行维护管理；
e) 应制定开发工具安全配置基线，依据基线定期进行安全配置检查；(LI)
f) 应对开发工具的安全风险进行持续跟踪；(LI)
g) 应建立内部可信工具资源库，确保工具来源可靠； (LI)
h) 应建立开发工具接入检测机制，能够发现非授权开发工具的非法接入行为。(LI)

5.4.3 工具回收管理

a) 应建立开发工具终止机制，在开发工具终止使用后对其中相关数据删除或销毁。

5.5 开发过程安全控制管理(PSM)

5.5.1 安全需求管理

a) 应通过分析软件利益相关者的实际需要，明确安全需求；
b) 应对安全需求进行合理性论证和审定；
c) 应在安全需求发生重大变更时进行合理性论证和审定，并进行版本控制；
d) 应确保安全需求至少涵盖合规性安全需求、业务安全需求、数据安全需求、技术架构安全需求以及供应链安全需求等。(LI)

5.5.2 安全设计管理

a) 应对软件设计文档进行安全审核；
b) 应建立软件安全设计基线，至少包括软件安全功能设计和软件功能安全防护设计等；
c) 应保证软件安全设计文档的完整性和可操作性；(LI)
d) 应对软件安全设计文档的修改、更新进行评审，并进行版本控制；(LI)
e) 应采用结构化的方法，系统的识别软件的威胁和风险，并针对威胁和风险制定消减策略。(LI)

5.5.3 安全开发管理

a) 应正式发布开发语言的安全编码规范；
b) 应持续维护安全编码规范；(LI)
c) 应依照安全编码规范进行安全开发；(LI)
d) 应以组件化的方式实现通用的软件安全需求；(LI)
e) 应制定开源组件安全管控制度，对开源组件的成熟度、漏洞风险等方面进行要求；(LI)
f) 应对应用软件准入的开源组件进行安全检查。(LI)

5.5.4 安全测试管理

a) 应制定安全测试管理制度，制度中至少应包含安全测试工作相关角色及其职责、安全测试工作流程、测试用例管理、测试结果管理等内容；
b) 应针对安全需求编写对应的安全测试用例；
c) 应对应用软件的代码、功能、组件等进行安全性测试；
d) 应具备主要安全测试基线自动核查能力；(LI)
e) 应在安全测试工作中不断更新完善安全测试用例；(LI)
f) 应对应用软件的 API 接口、业务逻辑等进行安全性测试。(LI)

5.5.5 安全发布管理

a) 应制定安全发布管理制度，至少应包含安全发布工作相关角色及其职责、安全发布工作流程等内容；
b) 应制定软件发布前的安全测试规范，并在发布工作中进行落地检查；
c) 应制定安全发布基线，并在安全发布过程中应用；（LI）
d) 应在发布环节对软件进行签名，确保软件后续使用过程中可被追溯。（LI）

5.5.6 安全交付管理

a) 应制定安全交付管理制度，制度中至少包含安全交付工作相关角色及其职责、安全交付工作流程、应用软件交付清单、软件物料清单等内容；
b) 应确保交付清单至少包括软件使用说明书、软件物料清单、开源组件清单、源代码安全分析报告、开源组件安全分析报告等技术资料。

6 安全测评要求

6.1 安全管理制度(SMS)

6.1.1 制定和发布

6.1.1.1 测评单元(LB-SMS-01)

该测评单元包括以下要求：
a) 测评指标：参见 5.1.1 a)。
b) 测评对象：软件安全开发管理制度文档
c) 测评实施:应核查软件安全开发管理制度是否涵盖人员、环境、工具以及开发过程，是否明确各类安全管理要求。
d) 测评结果:若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.1.1.2 测评单元(LB-SMS-02)

该测评单元包括以下要求：

a) 测评指标：参见 5.1.1 b)。

b) 测评对象：安全开发相关指南类和流程类文档。

c) 测评实施：

1) 应核查安全开发操作指南和流程文档是否涵盖源代码、设计文档、核心人员、重要基础设施等对象；

2) 应核查安全开发操作指南和流程文档是否明确执行过程和操作方法。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.1.1.3 测评单元(LB-SMS-03)

该测评单元包括以下要求：

a) 测评指标：参见 5.1.1 c)。

b) 测评对象：软件开发人员和各类文档发布证明材料。

c) 测评实施：

1) 应访谈软件开发人员是否知晓软件开发安全管理制度相关内容，在工作中是否执行；

2) 应核查发布证明材料是否通过正式有效的方式发布，如正式发文、领导签署、单位盖章等。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.1.2 执行和修订

6.1.2.1 测评单元(LB-SMS-04)

该测评单元包括以下要求：

a) 测评指标：参见 5.1.2 a)。

b) 测评对象：安全开发主管和安全管理制度执行检查记录。

c) 测评实施：

1) 应访谈安全开发主管是否定期开展软件开发安全管理制度执行情况检查；

2) 应核查检查记录是否覆盖软件开发安全管理制度各方面。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.1.2.2 测评单元(LI-SMS-05)

该测评单元包括以下要求：

a) 测评指标：参见 5.1.2 b)。

b) 测评对象：安全开发主管和安全管理制度维护记录。

c) 测评实施：

1) 应访谈安全开发主管是否定期对管理制度的适用性进行检查维护；

2) 应核查是否具有软件开发安全管理制度维护更新记录。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.2 人员安全管理(SSM)

6.2.1 岗位设置和人员配备

6.2.1.1 测评单元(LB-SSM-01)

该测评单元包括以下要求：

a) 测评指标：参见 5.2.1 a)。
b) 测评对象：软件开发负责人、岗位人员名单和岗位职责说明文件。
c) 测评实施：
   1) 应访谈软件开发负责人是否明确设立开发岗、测试岗、安全岗等岗位；
   2) 应核查岗位人员名单是否明确各岗位人员；
   3) 应核查岗位职责说明文件是否明确各岗位安全职责。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.2.1.2 测评单元(LI-SSM-02)

该测评单元包括以下要求：
a) 测评指标：参见5.2.1 b)。
b) 测评对象：软件开发负责人和岗位人员名单。
c) 测评实施：
   1) 应访谈软件开发负责人各岗位人员是否配备齐全，安全岗位人员是否专职；
   2) 应核查岗位人员名单是否明确各岗位配备情况，安全岗是否未兼任开发岗或测试岗。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.2.2 人员任职

6.2.2.1 测评单元(LI-SSM-03)

该测评单元包括以下要求：
a) 测评指标：参见5.2.2 a)。
b) 测评对象：保密协议和岗位安全协议。
c) 测评实施：
   1) 应核查软件开发人员保密协议是否明确保密范围、保密责任、违约责任、有效期限和签字等内容；
   2) 应核查关键岗位人员安全协议是否明确关键岗位范围(如架构师、核心代码开发岗位等)、关键岗位安全责任和义务等内容。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.2.2.2 测评单元(LI-SSM-04)

该测评单元包括以下要求：
a) 测评指标：参见5.2.2 b)。
b) 测评对象：人员上岗前考核记录。
c) 测评实施：应核查人员上岗前考核记录是否涵盖安全意识及岗位安全技能。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.2.3 人员培训

6.2.3.1 测评单元(LB-SSM-05)

该测评单元包括以下要求：
a) 测评指标：参见5.2.3 a)。
b) 测评对象：应用软件安全开发涉及全员人员培训文档。
c) 测评实施：

1) 应访谈软件开发相关人员是否进行过安全意识、保密教育等培训；
2) 应核查是否具有相关培训记录，内容是否覆盖管理制度、安全意识、保密教育等方面。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.2.3.2 测评单元(LI-SSM-06)

该测评单元包括以下要求：

a) 测评指标：参见5.2.3 b)。
b) 测评对象：软件开发不同岗位人员、人员培训文档和考核文档。
c) 测评实施：
1) 应核查人员培训计划，是否根据不同岗位(如开发岗、测试岗、安全岗等)制定不同的培训计划；
2) 应核查是否根据培训计划具有相应的培训记录；
3) 应核查是否具有各岗位人员技能考核文档。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.2.4 人员离岗

6.2.4.1 测评单元(LB-SSM-07)

该测评单元包括以下要求：

a) 测评指标：参见5.2.4 a)。
b) 测评对象：软件开发负责人和人员离岗手续记录。
c) 测评实施：
1) 应访谈软件开发负责人，是否有离职/离岗人员，如有，是否已根据要求完成相关离岗手续；
2) 应核查是否具有离岗人员终止其各类资产(包括但不限于代码库、软件开发文档等)的访问权限、软硬件设备等登记记录。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.2.5 第三方人员管理

6.2.5.1 测评单元(LB-SSM-08)

该测评单元包括以下要求：

a) 测评指标：参见5.2.5 a)。
b) 测评对象：第三方人员管理制度相关文档。
c) 测评实施：
1) 应核查第三方人员管理制度是否包括第三方人员进出管理、账号及权限管理、行为操作管理等内容；
2) 应核查是否具有相关管理记录（如人员进出登记记录、账号审批记录等）。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3 环境安全管理(ESM)

6.3.1 环境建设管理

6.3.1.1 测评单元(LB-ESM-01)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.1 a)。
b) 测评对象：软件开发负责人和网络拓扑图文档。
c) 测评实施：
   1) 应访谈软件开发负责人是否建立及使用专用的软件开发过程中涉及的研发、测试、发布等环境；
   2) 应核查专用环境与外部环境之间是否采取必要的隔离措施。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3.1.2 测评单元(LB-ESM-02)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.1 b)。
b) 测评对象：资产清单文档。
c) 测评实施：应核查资产清单是否包括名称、版本、安装的软件组件、适用项目范围等信息。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.3.1.3 测评单元(LB-ESM-03)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.1 c)。
b) 测评对象：软件开发环境安全基线文档。
c) 测评实施：应核查软件开发环境安全基线文档是否明确软件组件更新规范、安全配置策略、入侵防范措施等要求。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.3.1.4 测评单元(LB-ESM-04)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.1 d)。
b) 测评对象：操作规程类文档。
c) 测评实施：应核查软件开发环境配置操作手册是否明确配置操作步骤等内容。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.3.2 环境运维管理

6.3.2.1 测评单元(LB-ESM-05)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.2 a)。
b) 测评对象：管理制度类文档。
c) 测评实施：应核查相关管理制度中是否对研发、测试、发布等环境的权限管控机制进行要求。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.3.2.2 测评单元(LB-ESM-06)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.2 b)。

b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施：
   1) 应核查相关管理制度中是否明确各类环境远程访问的策略要求；
   2) 应核查是否具有外部通信接口或通道等远程访问方式的相关授权审批记录；
   3) 应核查授权开通的外部通信接口或通道是否在使用结束后关闭。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3.2.3 测评单元(LB-ESM-07)

该测评单元包括以下要求：
a) 测评指标：参见 5.3.2 c)。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施：
   1) 应核查管理制度中是否明确在线开发、协同开发等事项执行审批的过程；
   2) 应核查相关事项是否具有审批执行记录。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3.2.4 测评单元(LI-ESM-08)

该测评单元包括以下要求：
a) 测评指标：参见 5.3.2 d)。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施：
   1) 应核查管理制度中是否明确软件开发的核心代码及重要文档的权限管理要求；
   2) 应核查是否具有对软件核心代码或重要文档的操作日志。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3.2.5 测评单元(LI-ESM-09)

该测评单元包括以下要求：
a) 测评指标：参见 5.3.2 e)。
b) 测评对象：开发负责人和记录表单类文档。
c) 测评实施：
   1) 应访谈开发负责人是否定期离线备份环境配置文件、软件开发代码及重要文档等；
   2) 应核查是否具有环境配置文件、软件开发代码及文档等重要数据的备份记录，并核查记录中是否对备份数据进行了版本控制。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3.2.6 测评单元(LI-ESM-10)

该测评单元包括以下要求：
a) 测评指标：参见 5.3.2 f)。
b) 测评对象：管理制度类文档和记录表单类文档。
c) 测评实施：
   1) 应核查软件开发环境敏感信息保护制度，是否明确对账号、软件开发代码及文档、数据库表结构、安全漏洞等敏感信息的保护要求；
   2) 应核查是否具有防止敏感信息泄露的监测或保护手段。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3.2.7 测评单元(LI-ESM-11)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.2 g)。
b) 测评对象：开发负责人和记录表单类文档。
c) 测评实施：
   1) 应访谈开发负责人是否定期检查违反环境安全基线的行为；
   2) 应核查是否具有定期检查违反环境安全基线的记录，包括软件组件更新情况、安全策略配置情况、入侵防范措施配置情况等内容。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.3.2.8 测评单元(LI-ESM-12)

该测评单元包括以下要求：

a) 测评指标：参见 5.3.2 h)。
b) 测评对象：开发负责人和记录表单类文档。
c) 测评实施：
   1) 应访谈开发负责人是否定期执行软件开发过程中相关环境的安全漏洞扫描，扫描类型包括但不限于主机扫描、容器扫描、端口扫描等；
   2) 应核查是否具有环境的安全漏洞扫描记录及问题处置记录。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4 开发工具安全管理(TSM)

6.4.1 工具准入管理

6.4.1.1 测评单元(LB-TSM-01)

该测评单元包括以下内容：

a） 测评指标：参见5.4.1 a)。
b） 测评对象：开发负责人和开发工具清单。
c） 测评实施：
   1) 应核查开发工具清单，是否包含唯一标识、类型、名称、版本、来源（官方网站、第三方下载站点、供应商等）、IP地址、重要性等级以及对应的安全责任人等内容；
   2) 应核查开发工具清单是否与目前使用的开发工具一致；
   3) 应核查是否根据开发工具承载的数据重要性进行工具重要程度判定。
d） 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.1.2 测评单元(LB-TSM-02)

该测评单元包括以下内容：

a) 测评指标：参见5.4.1 b)。
b) 测评对象：开发工具管理制度和开发工具准入审批记录。
c) 测评实施：
   1） 应核查开发工具管理制度中是否明确要求对工具准入建立审批程序；
   2） 应核查是否具有工具准入审批记录。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.1.3 测评单元(LI-TSM-03)

该测评单元包括以下内容：

a) 测评指标：参见5.4.1 c)。

b) 测评对象：供应商管理制度、供应商评审记录和供应商清单。

c) 测评实施：

1） 应核查供应商管理制度是否明确供应商选择等相关要求；

2） 应核查供应商评审记录，是否根据开发工具重要程度针对质量、环境和安全、地理政治和道德、准时交付等风险因素进行识别和评估；

3） 应核查是否具备供应商清单。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.1.4 测评单元(LI-TSM-04)

该测评单元包括以下内容：

a） 测评指标：参见5.4.1 d)。

b） 测评对象：开发工具组件清单。

c） 测评实施：

1） 应核查是否具有所使用的工具组件清单；

2） 应核查组件清单是否包括其相关组件的组件名称、组件唯一标识、组件版本、组件来源、组件引用方式、知识产权等信息。

d） 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2 工具使用管理

6.4.2.1 测评单元(LB-TSM-05)

该测评单元包括以下内容：

a) 测评指标：参见5.4.2 a)。

b) 测评对象：重要开发工具。

c) 测评实施：

1） 应核查代码管理工具（如Git、Subversion等）、构建工具（如Maven、Gradle、NPM等）、持续集成/部署工具（如Jenkins、Travis CI、GitLab CI 等）等重要开发工具用户在登录时是否采用了身份鉴别措施；

2） 应核查用户列表确认用户身份标识是否具有唯一性；

3） 应核查用户配置信息是否不存在空口令用户；

4） 应核查用户鉴别信息是否具有复杂度要求并定期更换。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2.2 测评单元(LB-TSM-06)

该测评单元包括以下内容：

a) 测评指标：参见5.4.2 b)。

a) 测评对象：重要开发工具。

b) 测评实施：

1） 应访谈开发负责人是否制定重要开发工具使用的权限策略管理机制；
2） 应核查重要开发工具的权限策略是否满足最小权限原则。

c） 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2.3 测评单元(LB-TSM-07)

该测评单元包括以下内容：

a） 测评指标：参见5.4.2 c)。
b） 测评对象：开发工具的日志审计记录。
c） 测评实施包括以下内容：
1） 应核查开发工具是否开启日志审计功能；
2） 应核查日志保存时间是否不少于6个月。
d） 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2.4 测评单元(LB-TSM-08)

该测评单元包括以下内容：

a） 测评指标：参见5.4.2 d)。
b） 测评对象：开发负责人和开发工具管理制度。
c） 测评实施：
1） 应访谈开发负责人是否对开发工具进行定期维护；
2） 应核查是否具有开发工具的维护记录（如版本更新记录、规则更新记录和补丁安装记录等）；
d） 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2.5 测评单元(LI-TSM-09)

该测评单元包括以下内容：

a） 测评指标：参见5.4.2 e)。
b） 测评对象：重要开发工具。
c） 测评实施：
1） 应访谈开发负责人是否建立重要开发工具安全基线并定期进行安全配置检查；
2） 应核查重要开发工具安全配置检查记录，检查结果显示重要开发工具配置是否符合安全基线要求；
d） 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2.6 测评单元(LI-TSM-10)

该测评单元包括以下内容：

a） 测评指标：参见5.4.2 f)。
b） 测评对象：开发负责人和工具安全事件处置记录。
c） 测评实施：
1） 应访谈开发负责人是否建立开发工具漏洞或威胁情报的持续跟踪和应急处置机制；
2） 应核查是否具有开发工具安全事件处置记录。
d） 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2.7 测评指标(LI-TSM-11)

该测评单元包括以下内容：

a) 测评指标：参见5.4.2 g)。

b) 测评对象：开发工具管理制度、开发工具清单和可信工具资源库。

c) 测评实施：

1） 应核查开发工具管理制度是否明确工具从可信路径下载、从可信资源库获取等要求；

2） 应核查是否建立可信工具资源库；

3） 应核查开发工具清单是否均从可信工具资源库下载。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.4.2.8 测评单元(LI-TSM-12)

该测评单元包括以下内容：

a) 测评指标：参见5.4.2 h)。

b) 测评对象：工具检测记录。

c) 测评实施：应核查是否具有开发工具非法接入检测记录。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.4.3 工具回收管理

6.4.3.1 测评单元(LB-TSM-13)

该测评单元包括以下要求：

a) 测评指标：参见5.4.3 a)。

b) 测评对象：开发负责人、开发管理制度和记录表单类文档。

c) 测评实施：

1） 应访谈开发负责人是否建立开发工具终止机制；

2） 应核查开发管理制度是否明确开发工具使用终止后对数据的相关管理手段；

3） 应核查是否具有在开发工具终止使用后对登录信息、源代码、数据库表结构、产品相关技术文档、漏洞信息等重要信息进行删除或销毁的记录。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5 开发过程安全控制管理(PSM)

6.5.1 安全需求管理

6.5.1.1 测评单元(LB-PSM-01)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.1 a)。

b) 测评对象：需求负责人、安全需求文档及确认记录。

c) 测评实施：

1) 应访谈安全需求负责人，安全需求是否考虑了软件的投资者、使用者、供应者等相关方的需求、期望和约束条件的关联性和一致性；

2) 应核查安全需求文档，查看所有安全需求是否清晰明确的表达唯一的含义，并得到软件的投资者、使用者、供应者等相关方认可。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.1.2 测评单元(LB-PSM-02)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.1 b)。

b) 测评对象：安全需求负责人和论证评审记录。

c) 测评实施：

1) 应访谈安全需求负责人是否对安全需求文档进行论证和评审；

2) 应核查是否具有对需求文档的论证和评审记录。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.1.3 测评单元(LB-PSM-03)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.1 c)。

b) 测评对象：安全需求负责人、安全需求文档和论证评审记录。

c) 测评实施：

1) 应访谈安全需求负责人是否对需求变更进行论证和评审，包括但不限于合规性需求变更、架构变化导致的安全需求变更、业务功能变化导致的安全需求变更等；

2) 应核查是否具有需求变更的论证和评审记录；

3) 应核查安全需求文档是否具有版本管理记录。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.1.4 测评单元(LI-PSM-04)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.1 d)。

b) 测评对象：安全需求文档

c) 测评实施：

1) 应核查安全需求文档是否涵盖软件使用地区的相关法律规定和行业约束等合规性安全需求；

2) 应核查安全需求文档是否涵盖软件业务的安全需求；

3) 应核查安全需求文档是否涵盖了技术架构以及相关组件的安全需求；

4) 应核查安全需求文档是否涵盖了业务敏感数据、系统敏感数据，以及个人隐私数据等数据安全需求；

5) 应核查安全需求是否涵盖第三方软件/组件、开发过程和发布过程的安全需求。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.2 安全设计管理

6.5.2.1 测评单元(LB-PSM-05)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.2 a)。

b) 测评对象：各类安全设计文档和记录表单。

c) 测评实施：应核查是否具有对软件设计文档进行安全审核的记录，包括但不限于架构设计、功能设计、权限设计、日志设计等。

d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.5.2.2 测评单元(LB-PSM-06)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.2 b)。

b) 测评对象：安全设计文档

c) 测评实施：

1) 应核查安全设计文档是否具有安全功能设计，包括但不限于认证功能、权限控制功能、日志审计功能、访问控制功能等；

2) 应核查安全设计文档是否具有软件功能的安全防护设计，包括但不限于输入输出的防护，会话功能的防护、集成接口的防护、文件传输的防护等。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.2.3 测评单元(LI-PSM-07)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.2 c)。

b) 测评对象：安全设计文档和使用指南。

c) 测评实施：

1) 应核查安全设计文档是否涵盖所有的安全需求；

2) 应核查安全设计文档或相关文档是否指出了实现设计目标的执行过程和操作方法。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.2.4 测评单元(LI-PSM-08)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.2 d)。

b) 测评对象：安全设计文档和论证评审记录。

c) 测评实施：

1) 应核查是否具有安全设计文档变更的论证和评审记录；

2) 应核查安全设计文档是否具有版本管理记录。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.2.5 测评单元(LI-PSM-09)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.2 e)。

b) 测评对象：各类安全设计文档和记录表单。

c) 测评实施：

1) 应核查安全设计文档中是否对软件的总体结构进行分解，并对数据流或业务流进行分析；

2) 应核查安全设计文档是否对软件可能存在的威胁进行识别、记录和评估；

3) 应核查安全设计文档是否明确安全威胁的消减策略。

d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.3 安全开发管理

6.5.3.1 测评单元(LB-PSM-10)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.3 a)。
b) 测评对象:开发人员和安全编码规范文档。
c) 测评实施:
   1) 应访谈开发人员是否了解相关开发语言的安全编码规范；
   2) 应核查是否具有不同开发语言的安全编码规范文档。
d) 测评结果:若测评实施均为肯定,则此项测评指标测评结果为符合,否则为不符合或部分符合。

6.5.3.2 测评单元(LI-PSM-11)

该测评单元包括以下要求：
a) 测评指标：参见 5.5.3 b)。
b) 测评对象:安全编码规范文档更新记录。
c) 测评实施:应核查是否具有安全编码规范文档持续更新记录。
d) 测评结果:若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.5.3.3 测评单元(LI-PSM-12)

该测评单元包括以下要求：
a) 测评指标：参见 5.5.3 c)。
b) 测评对象：安全编码规范实施检查记录。
c) 测评实施：应核查是否具有安全编码规范实施记录。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.5.3.4 测评单元(LI-PSM-13)

该测评单元包括以下要求：
a) 测评指标：参见 5.5.3 d)。
b) 测评对象：安全组件设计及使用说明文档、安全组件清单。
c) 测评实施:
   1) 应核查安全组件设计及使用说明文档内容是否覆盖通用安全需求，如合规性安全需求、业务安全需求、数据安全需求、技术架构安全需求、供应链安全需求等，并且具有对应安全需求设计实现描述，组件概要设计、组件接口调用参数、组件调用示例等内容；
   2) 应核查是否具有安全组件清单。
d) 测评结果:若测评实施均为肯定,则此项测评指标测评结果为符合,否则为不符合或部分符合。

6.5.3.5 测评单元(LB-PSM-14)

该测评单元包括以下要求：
a) 测评指标：参见 5.5.3 e)。
b) 测评对象:开源组件安全管控制度文档及实施记录。
c) 测评实施:
   1) 应核查是否制定开源组件安全管控制度，明确开源组件成熟度要求、漏洞风险管理等内容；
   2) 应核查是否具有根据开源组件安全管控制度的实施记录，如允许使用的开源组件白名单、准入记录等。
d) 测评结果:若测评实施均为肯定,则此项测评指标测评结果为符合,否则为不符合或部分符合。

6.5.3.6 测评单元(LI-PSM-15)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.3 f)。
b) 测评对象：开源组件安全检查记录。
c) 测评实施：应核查是否具有开源组件相关检查记录，如针对漏洞、许可协议的检查等。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.5.4 安全测试管理

6.5.4.1 测评单元(LB-PSM-16)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.4 a)。
b) 测评对象：安全测试管理制度。
c) 测评实施：应核查安全测试管理制度中是否包含安全测试工作相关角色及其职责、安全测试工作流程、测试用例管理、测试结果管理等内容。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.4.2 测评单元(LB-PSM-17)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.4 b)。
b) 测评对象：安全测试用例文档或安全测试用例库。
c) 测评实施：
   1) 应核查是否具有安全测试用例文档或安全测试用例库；
   2) 应核查安全测试用例是否与安全需求相对应，是否覆盖了全部的安全需求。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.4.3 测评单元(LB-PSM-18)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.4 c)。
b) 测评对象：安全性测试报告。
c) 测评实施：应核查安全性测试报告是否包含了代码、功能、组件等方面内容。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.4.4 测评单元(LI-PSM-19)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.4 d)。
b) 测评对象：具备安全测试基线自动核查能力的工具或功能，安全测试基线自动核查记录。
c) 测评实施：
   1) 应核查是否具有主要安全测试基线自动核查能力的工具或功能；
   2) 应核查是否具有安全测试基线自动核查记录。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.4.5 测评单元(LI-PSM-20)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.4 e)。
b) 测评对象：安全测试用例更新记录。
c) 测评实施：应核查安全测试用例文档或安全测试用例库是否具有更新记录。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.5.4.6 测评单元(LI-PSM-21)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.4 f)。
b) 测评对象：安全性测试报告。
c) 测评实施：应核查安全性测试报告中是否包含了 API、业务逻辑等方面内容。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合。

6.5.5 安全发布管理

6.5.5.1 测评单元(LB-PSM-22)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.5 a)。
b) 测评对象：安全发布制度文档。
c) 测评实施：应核查软件安全发布管理制度是否包含安全发布工作相关角色及其职责、安全发布工作流程等内容。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.5.2 测评单元(LB-PSM-23)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.5 b)。
b) 测评对象：软件发布前的安全基线规范文档和规范实施的检查记录。
c) 测评实施：
   1) 应核查是否具有软件发布前的安全基线规范文档；
   2) 应核查是否具有依照规范开展安全测试工作的检查记录。
d) 测评结果:若测评实施均为肯定,则此项测评指标测评结果为符合,否则为不符合或部分符合。

6.5.5.3 测评单元(LI-PSM-24)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.5 c)。
b) 测评对象：安全发布基线文档和安全发布过程中针对安全发布基线的验证记录。
c) 测评实施：
   1) 应核查是否具有安全发布基线文档；
   2) 应核查是否具有安全发布基线的验证记录。
d) 测评结果:若测评实施均为肯定,则此项测评指标测评结果为符合,否则为不符合或部分符合。

6.5.5.4 测评单元(LI-PSM-25)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.5 d)。
b) 测评对象：软件签名规范文档和软件签名记录。
c) 测评实施：
   1) 应核查是否具有软件签名规范文档，包括但不限于开发方实体信息、软件名称信息、软件版本信息、软件摘要信息等；
   2) 应核查是否具有软件签名记录。
d) 测评结果：若测评实施均为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.6 安全交付管理

6.5.6.1 测评单元(LB-PSM-26)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.6 a)。
b) 测评对象：安全交付管理制度文档。
c) 测评实施：应核查软件安全交付管理制度中是否包含安全交付工作流程、应用软件交付清单、软件物料清单等内容。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

6.5.6.2 测评单元(LB-PSM-27)

该测评单元包括以下要求：

a) 测评指标：参见 5.5.6 b)。
b) 测评对象：交付物。
c) 测评实施：应核查交付清单中是否包含必要的技术资料、软件使用说明书、软件物料清单、开源组件清单、源代码安全分析报告、开源组件安全分析报告等。
d) 测评结果：若测评实施为肯定，则此项测评指标测评结果为符合，否则为不符合或部分符合。

7 其他

略。

参 考 文 献

[1] GB/T 38674-2020 信息安全技术 应用软件安全编程指南

[2] GB/T 25069-2022 信息安全技术 术语

[3] GB/T 30998-2014 信息技术 软件安全保障规范

[4] NIST Special Publication 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

附　录　A 测评单元编号说明

A.1　测评单元编码规则

测评单元编号为三组数据，格式为XX—XXX—XX，各组含义和编码规则如下：

第1组由2位组成，代表该测评单元的级别，其中第1位为字母L，第2位为字母B或I，字母B代表基本级，字母I代表增强级。

第2组由3位组成，分别为：SMS代表安全管理制度， SSM代表人员安全管理，ESM代表环境安全管理，TSM代表开发工具安全管理，PSM代表开发过程安全控制管理。

第3组由2位数字组成，分别代表该安全要求在此测评单元中的顺序编号。

示例：测评单元编号为LB-TSM-01，代表其为开发工具安全管理的基本级的第一个测评单元。

A.2　专用缩略语

下列专用缩略语适用于本标准。

SMS：安全管理制度(Security Management System)

SSM：人员安全管理(Stuff Security Management)

ESM：环境安全管理(Environment Security Management)

TSM：开发工具安全管理(Tool Security Management)

PSM：开发过程安全控制管理(Process Security Management)