ICS 35.080
CCS L00/09

# 团 体 标 准

T/ISC 0042—2024

# 软件安全开发能力评估技术规范

Technical specification for evaluating software security development capability

发布稿

2024 年 1 月 29 日发布 2024 年 2 月 28 日实施

中 国 互 联 网 协 会 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。

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。

本标准由中国互联网协会归口。

本文件起草单位：中国信息通信研究院、北京国舜科技股份有限公司、北京风行网安科技有限公司、深圳开源互联网安全技术有限公司、扬州数安技术有限公司、中国石油昆仑数智科技有限责任公司、中国民航信息网络股份有限公司、中邮信息科技(北京)有限公司、中国经济信息社、中国移动通信集团设计院有限公司、中国电力科学研究院有限公司、中建数字科技有限公司、北京航天绘景、OpenSDV汽车软件开源联盟、杭州默安科技有限公司、北京智精灵科技有限公司、北京德安信华科技有限公司、四川赛闯检测股份有限公司、成都信息工程大学、北京龙盾数据有限公司、网宿科技股份有限公司、北京微步在线科技有限公司、阿里巴巴集团、仁寿智仁智慧科技有限公司、四川仁恒智合科技有限公司、江苏大道云隐科技有限公司。

本文件主要起草人：蒋阿芳、马英轩、樊可欣、汤志刚、于伟杰、郭治文、张志强、王颉、张磊、王晓龙、滕征岑、张嵩、孙忠伟、杨京煜、王宇、翟冬梅、马德斌、陈长胜、马丽娜、吴新丽、王勇、王一村、肖秀琴、冯明杨、张玉雪、缪思薇、周亮、左海峰、段柯欣、贾大伟、张文君、申小旦、马永炼、滕召智、梁尧、李力宏、张坤、王晓宇、郝旭、方建康、周琼、冯丽、袁丽、马欣、秦元、黄莎琳、吕士表、杨志伟、童兆丰、娄珽、吴孟晴、党杜均、邓恒、黄圣超。

# 软件安全开发能力评估技术规范

## 1 范围

本标准中广义的软件包含支持组织业务的软件和应用系统软件（可简称应用系统），其中狭义的软件是指由组织开发，通过出售等模式供第三方使用的软件，应用系统软件是组织为满足某项业务的开展而开发，供组织自身使用。如果软件与应用系统并列时，指狭义软件，其他时候指广义的软件。

本标准规定软件安全开发过程中需求、设计、编码、测试、部署/发布、运维等各个阶段的安全实现要求，对软件安全开发过程能力提供评估标准及依据。

本标准规定软件及应用安全开发体系在不同等级中的实践活动要求，适用于组织机构自身的安全开发能力评估和过程改进，适用于第三方开展软件安全开发体系能力评估认证。

## 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，标注日期的引用文件，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 25069-2010 信息安全技术 术语

GB/T 29246-2017 信息技术 安全技术信息安全管理体系 概述和词汇

GB/T 19000-2016 质量管理体系 基础和术语

GB/T 20261-2020 信息安全技术 系统安全工程 能力成熟度模型

GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

## 3 术语和定义

GB/T 25069-2010、GB/T 29246-2017、GB/T 19000-2016、GB/T 20261-2020、GB/T 28458-2020、GB/T 24363-2009 界定的以及下列术语和定义适用于本文件。

### 3.1 软件生存周期 software life cycle

软件产品从构思开始到软件停止使用为止的时间周期。软件生存周期在组织中典型地包括：需求阶段、设计阶段、实现阶段、测试阶段、部署阶段或发布阶段、操作和维护阶段有时还包括销毁阶段。

### 3.2 安全开发 security development

识别软件生存周期中潜在的安全威胁，对信息和数据进行保护的一组技术状态管理活动。

### 3.3 保密性 confidentiality

使信息不泄漏给未授权的个人、实体、进程，或不被其利用的特性。

[来源：GB/T 25069-2010，2.1.1]

### 3.4 完整性 integrity

准确和完备的特性。

[来源：GB/T 29246-2017，2.40]

### 3.5 可用性 availability

已授权实体一旦需要就可访问和使用数据和资源的特性。

[来源：GB/T 25069-2010，2.1.20]

### 3.6 安全开发能力 security development capability

组织在组织建设、制度流程、技术工具以及人员能力等方面对安全开发的保障。

### 3.7 能力成熟度 capability maturity

对一个组织有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的水平。

### 3.8 能力成熟度模型 capability maturity model

对一个组织的能力成熟度进行度量的模型，包括一系列代表能力和进展的特征、属性、指示或模式。

### 3.9 安全过程 security process

用于实现某一安全目标的完整过程，该过程包含输入和输出。

### 3.10 基本实践 base practice

实现某一安全目标的安全开发相关活动。

### 3.11 基础实践 foundation practice

在评估中用于不能清晰界定属于某一安全过程域而重要且基础的安全开发相关活动。

### 3.12 评估 assessment

对于某一产品、系统或服务，对照某一标准，采用相应的评估方法，以建立合规性并确定其所做是否得到确保的验证。

### 3.13 过程 process

利用输入实现预期结果的相互关联或相互作用的一组活动。

[来源：GB/T 19000-2016，3.4.1]

### 3.14 基线 baseline

经过一个正式评审并通过的规约或产品，作为后续开发的基础。对其变更只有通过正式的变更控制规程方可进行。

[来源：GB/T 20261-2020，3.11]

### 3.15 威胁 threat

可能对系统或组织造成危害的不期望事件的潜在因素。

### 3.16 组件 component

在系统中，实现其部分功能的可识别区分的部分。

### 3.17 过程域 process area

实现同一安全目标的相关安全开发基本实践的集合。

### 3.18 网络安全漏洞 cyber security vulnerability

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。

[来源：GB/T 28458-2020，3.1]

### 3.19 应急响应 emergency response

组织为了应对突发／重大信息安全事件发生所做的准备，以及在事件发生后所采取的措施。

[来源：GB/T 24363-2009，3.4]

## 4 缩略语

下列缩略语适用于本文件。

BP：基本实践（Base Practice）

SSDCMM：软件安全开发能力成熟度模型（Software Secure Development Capability Maturity Model）

PA：过程域（Process Area）

DevOps：研发运营一体化（Development and Operations）

SAST：静态应用程序安全测试（Static Application Security Testing）

SCA：软件成分分析（Software Composition Analysis）

IAST：交互式应用程序安全测试（Interactive Application Security Testing）

## 5 安全开发体系评估模型

本标准适用于瀑布式以及敏捷开发模式

### 5.1 成熟度模型架构

SSDCMM 架构如图 1 所示。

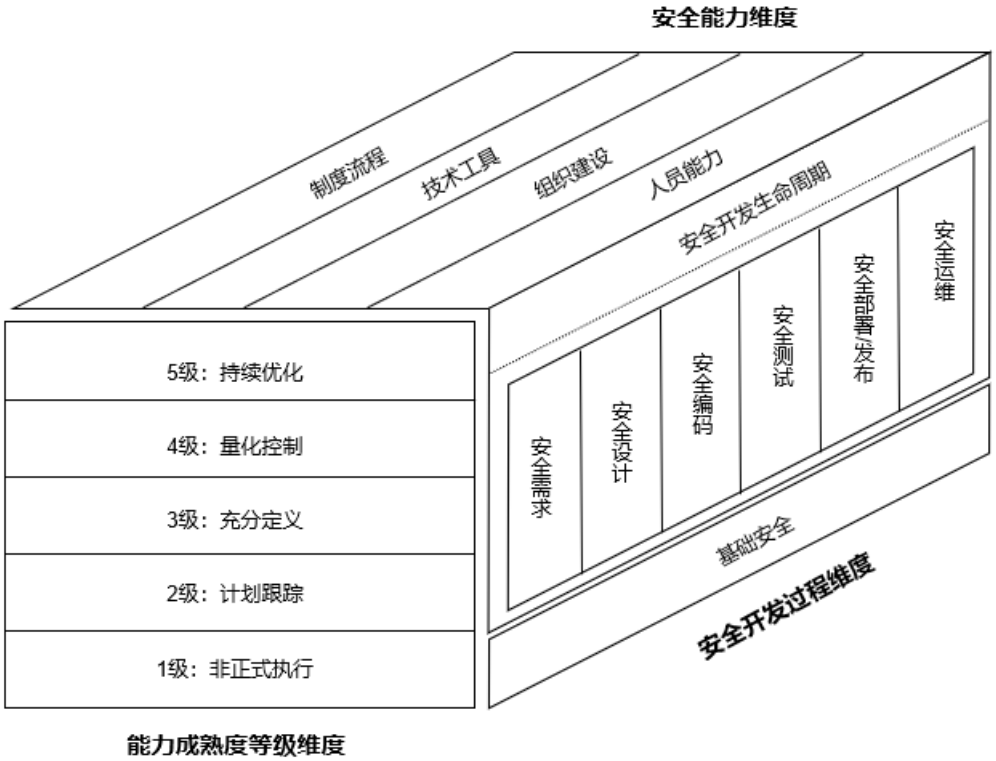

图 1 SSDCMM 架构图

SSDCMM 架构由以下三个维度构成：

a） 安全能力维度

安全能力维度明确了组织在安全开发领域应具备的能力，包括组织建设、制度流程、技术工具和人员能力。

b） 能力成熟度等级维度

安全开发能力成熟度等级划分为五级，具体包括：1 级是非正式执行级，2 级是计划跟踪级，3 级是充分定义级，4 级是量化控制级，5 级是持续优化级。

c） 安全开发过程维度

1） 安全开发过程包括开发生命周期安全过程和基础安全过程；

2） 开发生命周期安全过程具体包括：安全需求、安全设计、安全编码、安全测试、安全部署/发布、安全运维等 6 个阶段。

## 5.2 安全能力维度

### 5.2.1 能力构成

通过对组织各安全开发过程应具备安全能力的量化，进而评估每项安全过程的实现能力。

安全能力分为以下 4 个方面：

a） 组织建设：安全开发组织的设立、职责分配和沟通协作；

b） 制度流程：组织中安全开发领域的制度和流程，及执行；

c） 技术工具：通过技术手段和产品工具落实安全开发要求或自动化实现安全开发工作；

d） 人员能力：执行安全开发工作人员的安全意识及相关专业能力。

### 5.2.2 组织建设

从承担安全开发工作组织应具备的组织建设能力角度，根据以下方面进行能力等级区分：

a） 安全开发组织架构对组织业务的适用性；

b） 安全开发组织承担的工作职责的明确性；

c） 安全开发组织运作、沟通协调的有效性。

### 5.2.3 制度流程

从组织在安全开发制度流程的建设以及执行情况角度，根据以下方面进行能力等级区分：

a） 开发生命周期关键控制节点授权审批流程的明确性；

b） 相关流程制度的制定、发布、修订的规范性；

c） 制度流程实施的一致性和有效性。

### 5.2.4 技术工具

从组织用于开展安全开发工作的安全技术、应用系统和工具出发，根据以下方面进行能力等级区分：

a） 安全开发技术在开发全生命周期过程中的利用情况，应对开发全生命周期安全风险的能力；

b） 利用技术工具对安全开发工作的自动化支持能力，对安全开发制度流程固化执行的实现能力。

### 5.2.5 人员能力

从组织承担安全开发工作人员应具备的能力出发，根据以下方面进行能力等级区分：

a） 安全开发人员所具备的安全开发技能是否能够满足实现安全目标的能力要求（对安全开发相关业务的理解程度以及安全开发专业能力）；

b） 开发团队的安全意识以及对关键安全开发岗位员工安全开发能力的培养。

## 5.3 能力成熟度等级维度

组织的安全开发能力成熟度等级共分为 5 级，见表 1。

**表 1 安全开发能力成熟度等级共性特征**

| 安全开发能力成熟度等级 | 共性特征 | 说明 |
|---|---|---|
| **等级 1：非正式执行** | **执行 BP**：组织在安全开发过程中不能有效地执行相关工作，仅在部分软件和应用系统开发执行过程中根据临时的需求执行了相关工作，未形成成熟机制保证相关工作的持续有效进行，执行相关工作的人员未达到相应能力。所执行的过程称为“非正式过程” | 随机、无序、被动地执行开发安全过程，依赖于个人经验，无法复制 |
| **等级 2：计划跟踪** | a） **规划执行**：对开发安全过程进行规划，提前分配资源和责任。<br>b） **执行**：对开发安全过程进行控制，使用执行计划、执行基于标准和程序的过程，对安全开发过程实施配置管理。<br>c） **验证执行**：确认过程按预定的方式执行，验证过程的执行与计划是一致的。<br>d） **跟踪执行**：控制安全开发过程执行的进展，当过程实践与计划产生重大偏离时采取修正行动 | 在重要软件和重要应用系统的开发中，主动地实现了安全过程的计划与执行，但停留在“做”的阶段，对执行质量没有规范性要求，没有形成体系化 |
| **等级 3：充分定义** | a） **定义标准过程**：组织对标准过程进行制度化，为组织定义标准化的过程文档，为满足特定用途对标准过程进行裁剪。 | 在组织级别实现了安全过程的规范执行 |

| | | |
|---|---|---|
| | b） **执行已定义的过程：**充分定义的过程是可重复执行的，并使用过程执行的结果数据，对有缺陷的过程结果和安全实践进行核查。<br>c） **协调安全实践：**确定各技术团队之间、组织外部活动的协调机制 | |
| **等级 4：<br>量化控制** | a） **建立可测的安全目标：**为组织的安全开发建立可测量目标。<br>b） **客观地管理执行：**确定过程能力的量化测量，使用量化测量管理安全过程，并以量化测量作为修正行动的基础 | 建立了量化目标，安全过程可度量 |
| **等级 5：<br>持续优化** | a） **改进组织能力：**在整个组织范围内对规程的使用进行比较，寻找改进规程的机会，并进行改进。<br>b） **改进过程有效性：**制定处于持续改进状态下的规程，对规程的缺陷进行消除，并对规程进行持续改进 | 根据组织的整体目标，不断改进和优化安全过程 |

能力成熟度等级与 PA、BP、安全能力的关系如下：

a） 将组织在每个安全开发 PA 的能力成熟度划分为五级，针对每个等级下组织应具备的能力要求，从 4 个安全能力（组织建设、制度流程、技术工具及人员能力）提出具体的 BP；

b） 3 级要求应包含全部 4 个安全能力，其他等级要求可不包含完整的 4 个安全开发关键能力，并非每个安全开发 PA 的能力成熟度等级都包含完整的 4 个安全开发关键能力；

c） 对于每个安全开发 PA，高等级的能力要求应包括所有低等级能力要求。针对某一具体安全开发 PA，如果 5 级的能力要求中未涉及某一关键能力的内容，则默认应达到在 4 级的能力要求中的该关键能力的内容；如果 4 级的能力要求中依旧未涉及该关键能力，则默认应达到在 3 级的能力要求中该关键能力的内容，依此类推。

能力成熟度等级评估参考方法，参见附录 A。

能力成熟度等级评估流程和模型使用方法，参见附录 B。

## 5.4 安全开发过程维度

### 5.4.1 安全开发生命周期

安全开发生命周期分为以下 6 个阶段：

a） 安全需求：在软件开发的需求阶段，包括概略需求和详细需求阶段，根据业务需求提出安全要求的过程；

b） 安全设计：在软件开发的设计阶段，根据安全需求进行安全设计，满足安全要求的过程；

c） 安全编码：在软件开发的编码阶段，根据安全需求，参照安全设计，实现安全功能的过程；

d） 安全测试：在软件开发的测试阶段，验证安全需求是否满足的过程；

e） 安全部署/发布：对于应用系统软件，在软件部署阶段，按照安全需求，参照安全设计，进行安全配置的过程。对于通用软件，在软件发布阶段，按照安全需求，参照安全设计，对通用软件的默认配置进行安全配置的过程；

f） 安全运维：在软件的广泛应用和应用系统软件的运行过程中，监控运行的安全状态，并及时响应的过程。

特定的软件安全开发所经历的生命周期由实际的业务所决定，可为完整的 6 个阶段或是其中的几个阶段。

### 5.4.2 安全开发PA体系

#### 5.4.2.1 PA体系

PA 体系分为开发生命周期安全过程和基础安全过程两部分，共包含 19 个 PA，如图 2 所示。

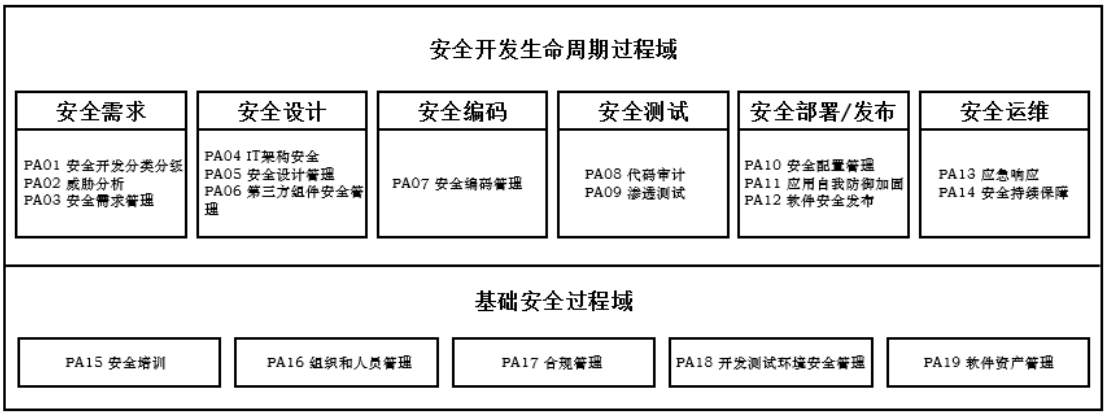


**图 2 安全开发 PA 体系**

开发生命周期安全过程域包括以下 6 个过程：

a） 安全需求的 PA（PA01~PA03）包括：安全开发分类分级、威胁分析、安全需求管理 3 个 PA；

b） 安全设计的 PA（PA04~PA06）包括：IT 架构安全、安全设计管理、第三方组件安全管理 3 个 PA；

c） 安全编码的 PA（PA07）包括：安全编码管理 1 个 PA；

d） 安全测试的 PA（PA08~PA09） 包括：代码审计、渗透测试 2 个 PA；

e） 安全部署/发布的 PA（PA10~PA12）包括：安全配置管理、应用自我防御加固、软件安全发布 3 个 PA；

f） 安全运维的 PA（PA13~PA14）包括：应急响应、安全持续保障 2 个 PA。

基础安全过程域（PA15~PA19）包括：安全培训、组织和人员管理、合规管理、开发测试环境安全管理、软件资产管理 5 个 PA。

#### 5.4.2.2 编码规则

安全开发 PA 编码规则如下：

a） 每个 PA 有对应的编号，分别采用递增的数值 01、02，...，表示。

**示例 1：**PA01，代表 PA“安全开发分类分级”。

b） 每个 PA 由一些 BP 组成。BP 用 BP.××.××来进行编号，第一组编码表示所在 PA 的序号，第二组编码表示具体 BP 的序号，具体 BP 的序号采用递增的数值 01，02，...，表示。

**示例 2：**BP.01.01 表示，过程域 PA01“安全开发分类分级”中的第一个 BP。

c） 对于每个 PA 的每个级别，需要同时满足本级别和所有低于该级别的 BP 的要求，才能达到本级别的能力水平，依此类推。

## 6 安全需求

### 6.1 PA01 安全开发分类分级

#### 6.1.1 PA描述

基于法律法规以及业务需求和信息系统特点等，确定组织内部的应用系统分类分级方法，在应用系统分类分级的基础上，基于一次开发项目中所涉及的信息系统、开发内容等，确定组织内部的开发项目分类分级方法，开发项目包括新建系统的项目和系统升级改造的项目，对所有的应用系统和开发项目进行分类分级。

#### 6.1.2 等级描述

##### 6.1.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

制度流程：组织未建立成熟稳定的系统和开发项目分类分级，仅根据临时需求或基于个人经验，对部分项目进行分类分级或单独处理（BP.01.01）。

##### 6.1.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队或项目管理团队人员负责相关系统和开发项目的分类分级（BP.01.02）；

b） 制度流程：应根据业务特性和外部合规要求，对相关系统项目（至少是重要项目）进行分类分级管理（BP.01.03）。

#### 6.1.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立负责系统和开发项目分类分级工作的管理岗位和人员，主要负责定义组织整体的系统和开发项目分类分级的原则（BP.01.04）。

b） 制度流程：

1） 应明确系统和开发项目分类分级原则、方法和操作指南（BP.01.05）；

2） 应对不同类别和级别的开发项目建立相应的安全管理和控制措施（BP.01.06）；

3） 应明确开发项目分类分级变更审批流程和机制，通过该流程保证对开发分类分级的变更操作及其结果符合组织的要求（BP.01.07）。

c） 技术工具：应在所有开发管理工具和安全开发工具中体现开发项目分类分级信息（BP.01.08）。

d） 人员能力：负责该项工作的人员应了解系统和开发项目分类分级的要求，能够识别哪些开发项目属于重要项目，进行重点管控（BP.01.09）。

#### 6.1.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

技术工具：

a） 应能自动化进行开发项目的分类分级，记录自动分类分级结果与人工审核后的分类分级结果之间的差异，定期分析改进分类分级标识工具，提升工具处理的准确度（BP.01.10）；

b） 应对开发项目分类分级的操作、变更过程进行日志记录和分析，定期通过日志分析等技术手段进行变更操作审计，开发项目分类分级可追溯（BP.01.11）。

#### 6.1.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

a） 制度流程：应定期评审开发项目分类分级的规范和细则，考虑其内容是否完全覆盖了当前的业务，并执行持续的改进优化工作（BP.01.12）；

b） 技术工具：应跟踪开发项目分类分级标识效果，持续改进开发项目分类分级的技术工具（BP.01.13）。

### 6.2 PA02 威胁分析

#### 6.2.1 PA描述

组织应在安全需求阶段，对业务系统执行威胁分析，从攻击者的视角出发识别潜在的威胁项，并针对威胁项进行风险评估，提出相应的消除、缓解措施，即安全需求。

### 6.2.2 等级描述

#### 6.2.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：组织未建立成熟的威胁建模方法论，在安全需求阶段仅凭个人经验由安全人员来执行威胁建模（BP.02.01）。

#### 6.2.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由安全人员和业务人员、系统架构人员共同来执行威胁建模，并针对相关的威胁项进行分析总结（BP.02.02）；

b） 制度流程：重要软件和重要应用系统开发应执行威胁建模（BP.02.03）。

#### 6.2.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a）组织建设：组织应明确执行威胁分析的开发团队和安全团队人员的角色和职责，负责制定统一的威胁建模和威胁分析的规范（BP.02.04）；

b）制度流程：应明确威胁建模和威胁分析的管理流程（BP.02.05）；

c）技术工具：应建立统一的威胁建模和威胁分析的系统和工具（BP.02.06）；

d）人员能力：负责该项工作的人员应了解威胁建模的内容和实施规范，具备对威胁项的分析能力，并能针对威胁项提供相应的消除缓解方案即安全需求（BP.02.07）。

#### 6.2.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

无进一步要求。

#### 6.2.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

技术方案：在业界分享相关威胁建模的方法论和工具最佳实践，成为行业标杆（BP.02.08）。

## 6.3 PA03 安全需求管理

### 6.3.1 PA描述

在组织的开发过程中需求环节，建立针对性的安全需求分析机制，分析组织内软件或应用系统软件的安全需求。

### 6.3.2 等级描述

#### 6.3.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：未建立成熟稳定的安全需求分析机制，仅根据临时需求或基于个人经验对个别系统开发进行了安全需求分析（BP.03.01）。

#### 6.3.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：开发部门应设置负责安全开发需求分析人员（BP.03.02）；

b） 制度流程：重要软件和重要应用系统开发应开展安全开发需求分析（BP.03.03）。

#### 6.3.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立负责安全开发需求分析的岗位和人员，负责对业务系统需求分析阶段开展安全需求分析工作，确保安全需求的有效制定和规范化表达（BP.03.04）。

b） 制度流程：

1） 应明确安全需求分析的流程和评审机制，明确安全需求文档内容要求（BP.03.05）；

2） 应依据国家法律、法规、标准等要求，分析软件或应用系统软件的安全合规性需求（BP.03.06）；

3） 应识别软件或应用系统软件面临的潜在威胁和自身潜在脆弱性，分析安全风险和消减攻击面的应对措施需求（BP.03.07）。

c） 技术工具：

1） 应建立承载安全需求分析活动的安全需求分析系统，该系统记录所有开发项目的安全需求分析结果，以保证对所有的安全需求分析过程的有效追溯（BP.03.08）；

2） 能够建立业务系统特点和使用场景与安全需求的自动关联性（BP.03.09）。

d） 人员能力：负责该项工作的人员应具有安全需求分析能力，对组织的安全需求管理有充分的理解，并通过培训实现各业务的需求分析人员对安全需求分析标准的一致性理解（BP.03.10）。

#### 6.3.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

a） 制度流程：应使用威胁驱动分析方法或模型，对业务系统的潜在威胁和自身潜在脆弱性能够有效、充分识别，确保安全需求的完备性和有效表达（BP.03.11）；

b） 技术工具：应能分析安全需求的有效性，统计安全需求中重要需求的使用频度，场景关联的准确性等（BP.03.12）。

#### 6.3.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

a） 制度流程：应持续优化安全开发需求分析，以保证符合组织发展战略和业务发展的实际需要（BP.03.13）；

b） 人员能力：负责该项工作的人员应具有应对新技术新场景的安全需求分析挖掘能力（BP.03.14）。

## 7 安全设计

### 7.1 PA04 IT架构安全

#### 7.1.1 PA描述

在设计 IT 架构时，从宏观层面设计系统的高可用架构、加解密架构、访问控制架构、通讯安全架构等安全内容，从而保证系统架构层面的安全性。

#### 7.1.2 等级描述

#### 7.1.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：未在组织上、流程上建立架构安全管理，仅根据临时需求或基于个人经验对架构进行安全设计和规划（BP.04.01）。

#### 7.1.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应有负责架构安全的人员（BP.04.02）；

b） 制度流程：应在架构管理的制度中明确架构安全的管理要求，关键业务的架构设计有专门的架构安全设计环节（BP.04.03）。

#### 7.1.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立负责架构安全的人员或团队（BP.04.04）；

b） 制度流程：应制定组织的架构安全规范，架构安全评审流程等（BP.04.05）；

c） 技术工具：应部署相关设备支撑安全架构设计，如加解密设备、统一用户登录平台等设备（BP.04.06）；

d） 人员能力：负责该项工作的人员应具有架构安全设计的能力，了解架构安全规范，能够根据不同业务制定有效的架构安全方案（BP.04.07）。

#### 7.1.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

无进一步要求。

#### 7.1.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

技术工具：应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.04.08）。

### 7.2 PA05 安全设计管理

#### 7.2.1 PA描述

为实现安全需求，建立对应的安全设计，保证组织内业务的安全需求实现的质量。

#### 7.2.2 等级描述

#### 7.2.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：组织未建立成熟稳定的安全设计机制，仅根据临时需求或基于个人经验对个别系统开发进行了安全设计（BP.05.01）。

#### 7.2.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：开发部门应设置负责安全开发设计人员（BP.05.02）；

b） 制度流程：重要软件和重要应用系统开发应开展安全开发设计（BP.05.03）。

#### 7.2.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立负责安全开发设计的岗位和人员，负责在软件设计阶段开展安全设计工作，确保软件设计安全，安全需求得到满足（BP.05.04）。

b） 制度流程：

1） 应明确安全设计的流程和评审机制，明确安全设计规范（BP.05.05）；

2） 安全设计除满足安全需求外，还应满足国家法律、法规、标准等未在安全需求中说明的要求，实现业务系统的安全合规性需求（BP.05.06）。

c） 技术工具：

1） 应建立安全设计管理系统，该系统记录所有项目的安全设计结果，以保证对所有的安全设计过程的有效追溯（BP.05.07）；

2） 能够建立组织的安全设计标准方案库，并建立安全需求与安全设计的自动关联性（BP.05.08）。

d） 人员能力：负责该项工作的人员应具有安全设计能力，对组织的安全设计管理有充分的理解，对组织的安全设计标准方案有充分的理解并能在安全设计中灵活应用，以及通过培训实现各业务的安全设计人员对安全设计标准的一致性理解（BP.05.09）。

#### 7.2.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

技术工具：应能分析安全设计有效性，统计标准安全设计方案的使用频度，安全需求与安全设计关联的准确性等（BP.05.10）。

#### 7.2.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

a） 制度流程：应持续优化安全设计规范，安全设计标准库，以保证符合组织发展战略和业务发展的实际需要（BP.05.11）；

b） 人员能力：负责该项工作的人员应具有应对新技术新场景的安全设计能力

（BP.05.12）。

### 7.3 PA06 第三方组件安全管理

#### 7.3.1 PA描述

在设计阶段对第三方组件的引入、使用进行安全管理，保证第三方组件的安全性。

#### 7.3.2 等级描述

##### 7.3.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

制度流程：组织未建立成熟稳定的第三方组件引入、使用的安全管理，仅根据临时需求或基于个人经验对个别第三方组件进行安全管理（BP.06.01）。

##### 7.3.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队相关人员负责第三方组件安全管理（BP.06.02）；

b） 制度流程：应明确第三方组件引入、使用的安全要求，并在重要软件和重要应用系统软件开发中有第三方组件的安全管控（BP.06.03）。

##### 7.3.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立第三方组件安全管理的岗位和人员，负责制定相关的第三方组件安全管理的制度，推动相关要求、流程的落地，并对具体业务或项目的第三方组件风险评估提供咨询和支持（BP.06.04）。

b） 制度流程：

1） 应明确组织的第三方组件的引入安全原则，引入和使用的流程（BP.06.05）；

2） 应在第三方组件引入时，对其风险进行评估，包括来源的合法性，软件许可的风险性，组件自身的脆弱性等（BP.06.06）。

c） 技术工具：

1） 应有第三方组件的检测工具（SCA），可以在合适时，验证系统中所包含的第三方组件符合安全设计中的第三方组件说明（BP.06.07）；

2） 应用第三方组件的风险检测工具（SCA），可以跟踪和检测第三方组件的漏洞和软件许可风险（BP.06.08）。

d） 人员能力：负责该项工作的人员应能够充分理解第三方组件的安全要求，并能够根据组织的软件开发特点，提出针对性的解决方案（BP.06.09）。

#### 7.3.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

a） 制度流程：应明确统计组织各软件和应用系统第三方组件的应用情况，第三方组件关联风险的覆盖率等工作流程（BP.06.10）；

b） 技术工具：应有工具实现跟踪和检测第三方组件的风险，统计第三方组件关联风险覆盖率（BP.06.11）。

#### 7.3.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

制度流程：应保持第三方组件安全管理持续优化，能持续跟踪第三方组件相关安全数据，并能迅速应用（BP.06.12）。

## 8 安全编码

### 8.1 PA07 安全编码管理

#### 8.1.1 PA描述

在编码阶段，建立组织的代码安全管理，保证编码自身的安全性，以满足安全需求和安全设计的要求。

#### 8.1.2 等级描述

#### 8.1.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：未在组织建立成熟稳定的开发编码环节安全管理机制，仅根据临时需求或基于个人经验考虑编码安全（BP.07.01）。

#### 8.1.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队人员根据软件开发特点和业务需求、安全需求、安全设计等，进行代码安全管控（BP.07.02）；

b） 制度流程：在重要软件和重要应用系统建设中应将代码安全管控作为必要的环节（BP.07.03）。

#### 8.1.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立编码安全管理岗位和人员，负责制定统一的安全管理要求和编码安全规范（BP.07.04）。

b） 制度流程：

1） 应明确编码安全的技术规范，编写编码安全指南指导开发团队安全编码（BP.07.05）；

2） 应明确编码环节中，开发团队的内部编码安全管控机制，明确编码安全的评审机制，利用内部交叉检查、外部代码审计等常规手段进行安全编码管控（BP.07.06）。

c） 技术工具：应利用技术工具实现对编码安全进行安全管理和监控，实现编码安全异常及时告警，可将该技术工具嵌入到编码工具和编译工具中（BP.07.07）。

d） 人员能力：负责该项工作的人员应了解编码安全的管控要求，能够开展编码安全质量评估工作（BP.07.08）。

#### 8.1.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

制度流程：应定期对组织整体编码安全质量进行分析，整理频繁出现的代码安全缺陷，更新安全编码规范，安全编码指南等文档（BP.07.09）。

#### 8.1.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

技术工具：

a) 将成熟、高质量的安全代码，抽象出来，独立化、组件化，建立相应的代码安全组件，以提升优质代码的重用率，提升代码安全质量和开发效率（BP.07.10）；

b) 考虑通过部分安全组件代码开源方式，在业界分享最佳实践，成为行业标杆（BP.07.11）。

## 9 安全测试

### 9.1 PA08 代码审计

#### 9.1.1 PA描述

以源代码或编译后代码为检测对象，进行代码安全检测和审计，以保证代码安全质量以及软件整体安全性。

#### 9.1.2 等级描述

##### 9.1.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：组织未建立成熟稳定的代码安全检测手段，仅根据临时需求或基于个人经验对个别系统的代码进行了安全检测（BP.08.01）。

##### 9.1.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队相关人员负责对代码安全进行安全检测（BP.08.02）；

b） 制度流程：重要软件和重要应用系统开发应建立代码安全检测方案（BP.08.03）。

##### 9.1.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立负责代码安全检测岗位和人员，负责制定统一的代码安全检测要求和代码安全检测规范（BP.08.04）。

b） 制度流程：

1） 应明确对代码安全检测的内容以及技术规范，明确代码安全评审的要求（BP.08.05）；

2） 应明确代码安全检测的流程节点（BP.08.06）。

c） 技术工具：

1） 应采用自动和人工审计相结合的方法或手段对代码进行静态代码安全检测（SAST）（BP.08.07）；

2） 对于 WEB 应用型软件，应采用自动插桩技术，检测软件的安全脆弱性（IAST）（BP.08.08）。

d） 人员能力：负责该项工作的人员应了解代码安全检测的内容和技术规范，具备对检测结果的研读和分析、判断能力（BP.08.09）。

##### 9.1.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

a） 技术工具：应建立综合的代码质量安全分析统计能力，能够分析代码万行缺陷率，缺陷种类量等安全指标（BP.08.10）；

b） 人员能力：负责该项工作的人员应充分理解代码安全检测的要求，可以持续优化代码检测规则和工具（BP.08.11）。

#### 9.1.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

技术工具：在业界分享代码检测、代码检测工具、代码检测规则的最佳实践，成为行业标杆（BP.08.12）。

### 9.2 PA09 渗透测试

#### 9.2.1 PA描述

组织通过模拟黑客攻击的方式，对软件进行综合性的安全测试，以降低软件可能存在的安全缺陷，提升业务系统的安全性。

#### 9.2.2 等级描述

#### 9.2.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：未在系统上线前建立成熟稳定的模拟攻击测试机制，仅根据临时需求或基于个人经验考虑了个别系统的模拟攻击测试（BP.09.01）。

#### 9.2.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应组织人员对系统进行模拟攻击测试（BP.09.02）；

b） 制度流程：应明确重要软件和重要应用系统必须进行模拟攻击测试（BP.09.03）；

c） 人员能力：负责模拟攻击测试工作的人员理解模拟攻击的要求，能够进行有效的模拟攻击测试（BP.09.04）。

#### 9.2.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立负责模拟攻击测试的安全管理岗位和人员，负责制定模拟攻

击的规则和提供技术能力，并推动在组织内落地执行（BP.09.05）。

b） 制度流程：

1） 应明确模拟攻击测试的测试内容，测试技术规范（BP.09.06）；

2） 应明确模拟攻击测试的流程节点（BP.09.07）；

3） 应明确模拟攻击测试的安全评审的要求，包括清晰的安全质量通过标准（BP.09.08）。

c） 技术工具：

1） 应采用自动和人工模拟攻击相结合的方式和手段，检测主机、操作系统、数据库系统、中间件系统等的安全性（BP.09.09）；

2） 应采用自动和人工模拟攻击相结合的方式和手段，检测应用系统的安全性，包括用户权限认证、访问控制、网络通讯安全等（BP.09.10）；

3） 应采用自动和人工模拟攻击相结合的方式和手段，检测应用系统的业务逻辑安全性，防止数据泄露以及其他业务风险（BP.09.11）。

d） 人员能力：负责模拟攻击测试的人员应能够充分理解模拟攻击测试的流程和要求，并根据模拟攻击的结果执行相应的风险评估，从而提出实际的解决方案（BP.09.12）。

#### 9.2.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

技术工具：应对软件和应用系统软件的脆弱性长期跟踪，持续统计系统的漏洞数量和种类（BP.09.13）。

#### 9.2.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

a） 制度流程：组织应及时跟进模拟攻击测试的结果，定期评估现有安全开发的能力，及时调整相应的技术规范和管控措施（BP.09.14）；

b） 在业界分享原创的模拟攻击最佳实践，成为行业标杆（BP.09.15）。

## 10 安全部署/发布

### 10.1 PA10 安全配置管理

#### 10.1.1 PA 描述

在应用软件发布或应用系统部署时，对配置项进行安全检查，保证缺省配置的安全性，从而保证软件或应用系统软件的初始安全性。

### 10.1.2 等级描述

#### 10.1.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：未在组织建立成熟稳定的配置安全管理，仅根据临时需求或基于个人经验在个别场景考虑了配置安全风险（BP.10.01）。

#### 10.1.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队的相关人员负责配置安全控制（BP.10.02）；

b） 制度流程：应明确重要软件发布或重要应用系统软件部署的安全配置和审核流程（BP.10.03）；

c） 人员能力：负责配置安全工作的人员应基本理解配置安全的要求（BP.10.04）。

#### 10.1.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立相关岗位人员，负责组织的软件配置安全，并对负责配置的人员进行安全培训（BP.10.05）。

b） 制度流程：

1） 应明确软件发布或应用系统软件部署的配置安全审核制度，审核配置方案是否符合安全要求（BP.10.06）；

2） 应审核正式发布版本或正式部署版本的配置与最后测试版本配置的差异性，必须保证配置的安全性不低于最后测试版本（BP.10.07）；

3） 应审核配置方案中的配置项完整性，防止配置缺失而影响系统安全性（BP.10.08）。

c） 技术工具：应在发布/部署流程管控中具备配置安全审核的内容，并对配置方案存储、审核（BP.10.09）。

d） 人员能力：负责配置安全管理的人员应充分理解配置安全管理的制度和流程，并能够根据实际配置方案，评估配置的风险（BP.10.10）。

#### 10.1.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

无进一步要求。

#### 10.1.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

无进一步要求。

### 10.2 PA11 软件/应用自我防御加固

#### 10.2.1 PA描述

组织在部署和发布阶段，在软件或应用系统的部分构成（包括变形形式，如编译后的执行文件、二级制代码等）暴露在外部的情况下，应对其安全性进行加固，防止软件内部逻辑、敏感信息的泄露，增强系统的安全性。

#### 10.2.2 等级描述

##### 10.2.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：组织未建立成熟稳定的软件/应用自我防御加固方案，仅根据临时需求或基于个人经验对个别系统进行了自我防御加固（BP.11.01）。

##### 10.2.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a) 组织建设：应由开发团队或运维团队相关人员负责对应用实施应用自我防御加固（BP.11.02）；
b) 制度流程：重要软件和重要应用系统开发应建立明确的软件/应用自我防御加固方案（BP.11.03）。

##### 10.2.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a) 组织建设：组织应在开发团队或者安全团队设立负责应用自我防御加固的岗位和人员，负责制定统一的软件和应用自身安全加固要求和规范（BP.11.04）。
b) 制度流程：
   1） 应明确对软件/应用自身安全加固的技术规范，实施要求（BP.11.05）；
   2） 应明确自我防御加固在部署或发布过程中的流程节点（BP.11.06）。
c) 技术工具：应具备代码安全加固工具进行代码安全加固，包括代码混淆、可执行文件加固、APP 加固等（BP.11.07）。

d) 人员能力：负责该项工作的人员应了解软件/应用自身安全加固的内容和技术规范，具备对检测结果的研读和分析、判断能力（BP.11.08）。

#### 10.2.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

人员能力：负责该项工作的人员应充分了解软件/应用自身安全加固的原理，可以持续优化安全加固方案和规则（BP.11.09）。

#### 10.2.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

技术工具：在业界分享软件/应用安全加固的最佳实践，成为行业标杆（BP.11.10）。

### 10.3 PA12 软件安全发布

#### 10.3.1 PA描述

在应用软件发布时，采取必要手段，加强发布环节的安全控制，从而保证软件发布后的初始安全性。

#### 10.3.2 等级描述

#### 10.3.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：未在组织建立成熟稳定的发布安全管理，仅根据临时需求或基于个人经验在个别场景考虑了软件发布安全风险（BP.12.01）。

#### 10.3.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队或运维团队的相关人员负责软件发布安全控制（BP.12.02）；

b） 制度流程：应明确重要软件发布时的审核流程（BP.12.03）；

c） 人员能力：负责软件发布安全工作的人员应基本理解软件安全发布的要求（BP.12.04）。

#### 10.3.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立相关岗位人员，负责组织的软件发布安全，并对负责软件发布的人员进行安全培训（BP.12.05）。

b） 制度流程：

1） 应明确电子签名的审核制度，审核电子签名方式是否符合发布渠道要求，软件主体是否满足电子签名的要求（BP.12.06）；

2） 应明确软件发布的安全审核制度，审核发布方案是否符合安全要求，所选择的发布渠道是否安全可靠，是否充分利用发布渠道的安全机制（BP.12.07）；

3） 应审核正式发布版本与最后测试版本配置的差异性，是否采取必要的电子签名，必须保证发布版本的安全性不低于最后测试版本（BP.12.08）；

4） 应审核发布方案中的配置项完整性，保证充分利用发布渠道的安全机制（BP.12.09）。

c） 技术工具：应使用成熟安全的发布渠道，或者使用自建的发布工具，自建的发布工具应该已经通过充分的安全评审（BP.12.10）。

d） 人员能力：负责发布安全的人员应充分理解发布安全管理的制度和流程，并能够根据实际情况，评估发布的风险（BP.12.11）。

#### 10.3.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

无进一步要求。

#### 10.3.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

无进一步要求。

## 11 安全运维

### 11.1 PA13 应急响应

#### 11.1.1 PA描述

建立针对已发布的软件或已部署的应用系统软件的应急响应体系，对各类安全事件进行及时响应和处置。

#### 11.1.2 等级描述

##### 11.1.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：未在组织建立成熟稳定的应急响应机制，仅根据临时需求或基于个人经验对个别安全事件进行应急处理（BP.13.01）。

##### 11.1.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：已发布的软件和已部署的重要应用系统应设立负责安全事件管理和应急响应的岗位和人员（BP.13.02）；

b） 制度流程：已发布的软件和已部署的重要应用系统应明确安全事件管理和应急响应的策略和具体方案（BP.13.03）。

##### 11.1.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设立专职负责安全事件管理和应急响应的岗位和人员（BP.13.04）。

b） 制度流程：

1） 应明确安全事件管理和应急响应工作管理制度和流程，定义安全事件类型，明确不同类别事件的处置流程和方法（BP.13.05）；

2） 应明确安全事件应急预案，定期开展应急演练活动（BP.13.06）。

c） 技术工具：应建立统一的安全事件管理系统（BP.13.07）。

d） 人员能力：负责该项工作的人员应具备安全事件的判断能力，熟悉安全事件应急响应措施（BP.13.08）。

##### 11.1.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

技术工具：安全事件管理系统应能够基于分析的内容评估安全响应的效率，包括平均响应时长，最高响应时长，分类安全事件的平均响应时长、最高响应时长等，可作为应急响应流程和预案的提升依据（BP.13.09）。

##### 11.1.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

制度流程：安全事件管理和应急响应机制应随着组织实际情况不断调整、更新和完善，并定期对组织人员开展流程培训和宣贯（BP.13.10）。

## 11.2 PA14 安全持续保障

### 11.2.1 PA 描述

组织对已发布的软件，持续跟踪其风险，发现新的软件安全缺陷后，通过发布新的版本或配置方案对安全缺陷进行补救;对已部署的应用系统软件,组织监控运行安全,跟踪主机、操作系统、数据库系统、中间件系统、应用系统的安全缺陷，发现缺陷后通过修改配置，系统升级或打补丁方式保证应用系统安全性。

### 11.2.2 等级描述

#### 11.2.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：组织未建立成熟稳定的安全持续保障机制，仅根据临时需求或基于个人经验考虑安全持续保障（BP.14.01）。

#### 11.2.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 制度流程：相关部门对已发布的软件或已部署的应用系统实施安全持续保障活动，包括主动的漏洞收集，主动发起的漏洞检测活动，对发生安全事件具备反应的能力和流程（BP.14.02）；

b） 技术工具：有技术工具去发现运行时系统的安全缺陷（BP.14.03）。

#### 11.2.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织内应设立负责安全持续保障的岗位和人员，负责安全持续保障制度和流程的制定，负责漏洞等安全缺陷的跟踪和发现，协调资源，推动制度和流程的落地（BP.14.04）。

b） 制度流程：

1） 组织应明确安全持续保障的日常管理制度和工作流程（BP.14.05）；

2） 组织应明确系统升级和补丁更新的工作流程（BP.14.06）；

3） 组织应明确漏洞发现和处置的工作流程（BP.14.07）。

c） 技术工具：

1） 应采用自动和人工模拟攻击相结合的方式和手段，在保证不影响应用系统工作的前提下，检测主机、操作系统、数据库系统、中间件系统等的安全性（BP.14.08）；

2） 应采用自动和人工参与相结合的方式和手段，跟踪软件相关第三方组件的安全性，发现是否有新出现的安全漏洞（BP.14.09）；

3） 应有对已发布软件或已部署应用系统软件的漏洞和安全脆弱性进行管理的系统，登记漏洞，跟踪漏洞的处置，实现漏洞和安全脆弱性的持续管理（BP.14.10）。

d） 人员能力：负责该项工作的人员应充分了解安全持续保障的管理制度和工作流程，能够在发现漏洞和安全脆弱性时评估其风险而确定应对方案（BP.14.11）。

#### 11.2.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

a） 制度流程：组织应定期对已发布的软件或已部署的应用系统软件安全性进行量化评估，评估新风险和需要调整的控制措施（BP.14.12）；

b） 技术工具：能够统计已发布的软件或已部署的应用系统软件的漏洞数量、漏洞种类等数据，为后续安全管控能力提升提供技术支持（BP.14.13）。

#### 11.2.2.5 等级 5 ：持续优化

该等级的安全开发能力要求描述如下：

技术工具：在业界分享原创的漏洞发现，成为行业标杆（BP.14.14）。

## 12 基础安全

### 12.1 PA15 安全培训

#### 12.1.1 PA描述

组织应通过传授安全意识和技能来提高组织和人员的安全意识和防范能力，培训的内容包括国家最新的安全政策和法规，近期重大软件安全事件，新的安全管理制度和监督机制等内容。安全培训可以有效降低组织对软件安全认知的交流成本，提升人员的安全技能。

#### 12.1.2 等级描述

#### 12.1.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：组织未在任何部门中设立固定的安全意识和技能培训人员，仅根据团队个人的经验水平传授安全意识和技能的相关知识，由个别人员临时承担了安全培训的工作（BP.15.01）。

#### 12.1.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：

1） 应由相关业务部门人员负责完成人力资源管理策略中的安全培训要求（BP.15.02）；

2） 重要软件和重要应用系统开发小组应接受安全培训（BP.15.03）。

b） 制度流程：

1） 应对安全培训进行制度性管理，对培训内容、频率、考核制度做出要求，培训应配有相应签到、考试等制度性要求（BP.15.04）；

2） 应该针对不同人员角色进行针对性培训，对于管理人员、开发人员、负责人等做出不同程度的培训和考核方式（BP.15.05）。

c） 人员能力：应配备专业的安全意识培训人员，该人员对培训内容负责，并且在组织内部有一定的权力保障培训的制度性执行（BP.15.06）。

#### 12.1.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：

1） 人力资源部门与安全培训部门的人员能够进行有效配合，对培训考核的结果做出清晰的要求（BP.15.07）；

2） 组织应建立组织层面专职的安全培训部门（或团队）和岗位（BP.15.08）。

b） 制度流程：

1） 应明确重要岗位人员的安全开发培训计划，并在重要岗位转岗、岗位升级等环节对相关人员开展培训（BP.15.09）；

2） 组织对重要岗位人员的安全开发培训计划需要具备吸收外部资源在开发安全方面的知识与能力，合理安排人员参与第三方组织的开发安全专业培训，保证参与第三方培训人员的合理占比（BP.15.10）；

3） 安全培训部门对于组织内部的软件安全实施情况有制度性的调查安排，清楚组织内部的软件安全开发现状，并定期有相应报告产出（BP.15.11）；

4） 能定期总结安全经验知识库，对过往组织内外发生的安全事件进行复盘总结，并融入到安全培训的内容之中（BP.15.12）。

c） 技术工具：应通过技术工具实现部分培训内容的自动化和可拓展化，便于培训内容在组织内传播（BP.15.13）。

d） 人员能力：培训组织人员能够了解当前开发安全现状和对应的培训要求，培训讲师具备充分的安全培训水平（BP.15.14）。

#### 12.1.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

组织建设：

a） 应对安全培训的运行效果能以量化指标的形式进行定期衡量，建立考核、培训内容整改、个人绩效挂钩等一系列相应量化体系建设，并形成多维度的安全能力评估打分，受培训学员能清晰看到自身量化能力水平（BP.15.15）；

b） 应不断引入外部专家参与培训，对内部安全培训内容进行相关更新，以确保培训内容的时效性（BP.15.16）。

#### 12.1.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

组织建设：应能够持续迭代优化组织的安全培训的内容、培训组织方式、培训组织，根据培训人员的反馈和组织内部要求不断优化，针对不同能力水平的培训对象实现定制化培训，能适应整体业务安全要求所带来的安全培训要求（BP.15.17）。

### 12.2 PA16 组织和人员管理

#### 12.2.1 PA 描述

通过建立组织内部负责安全开发工作的职能部门及岗位，以及对人力资源管理过程中各环节进行安全管理，防范组织和人员管理过程中存在的安全开发风险。

#### 12.2.2 等级描述

#### 12.2.2.1 等级 1 ：非正式执行

该等级的安全开发能力描述如下：

组织建设：组织未在任何部门中设立固定的安全开发管理人员，仅根据临时需求或基于个人经验，由个别人员临时承担了业务的安全开发工作（BP.16.01）。

#### 12.2.2.2 等级 2 ：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：

1） 应由相关业务部门人员负责人力资源管理中安全要求（BP.16.02）；

2） 重要软件和重要应用系统开发应具有安全开发岗位和人员，以实现对安全开发风险的有效管理（BP.16.03）。

b） 制度流程：

1） 重要软件和重要应用系统开发应对重要岗位候选者从法律法规、行业道德准则等层面执行背景调查（BP.16.04）；

2） 应与所有涉及开发活动的人员签订安全责任协议和保密协议（BP.16.05）。

c） 人员能力：负责重要软件和重要应用系统安全开发职能的人员，应能够充分了解目前安全开发在组织整体业务目标中的要求和定位（BP.16.06）。

#### 12.2.2.3 等级 3 ：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：

1） 人力资源部门与安全开发部门的人员应能够进行有效配合（BP.16.07）；

2） 组织应建立组织层面专职的安全开发职能部门（或团队）和岗位并在职能岗位设计时考虑了职责分离的原则（BP.16.08）；

3） 应建立组织内部的监督管理职能部门，负责对组织内部的需求、设计、开发、测试、部署或发布等行为进行安全监督（BP.16.09）；

4） 应指定安全开发的安全需求、安全设计、安全测试、安全部署/发布、安全运维的责任部门（BP.16.10）；

5） 应明确组织层面承担人员安全开发培训管理职责的岗位和人员，负责对安全开发培训需求的分析及落地方案的制定和推进（BP.16.11）。

b） 制度流程：

1） 应明确安全开发相关部门或岗位的要求，明确其工作职责，以及职能部门之间的协作关系和配合机制（BP.16.12）；

2） 应明确安全开发追责机制，定期对责任部门和安全岗位组织安全检查，形成检查报告（BP.16.13）；

3） 应明确针对开发合作方的安全管理制度，并要求签署保密协议，定期对合作方人员行为进行安全审查（BP.16.14）；

4） 应明确重要岗位人员的安全开发培训计划，并在重要岗位转岗、岗位升级等

环节对相关人员开展培训（BP.16.15）。

c） 技术工具：应通过技术工具自动化实现安全开发相关的人力资源管理流程（BP.16.16）。

d） 人员能力：

1） 负责组织和人员管理的人员应充分理解人力资源管理流程中可对安全风险进行把控的环节（BP.16.17）；

2） 应开展针对员工入职过程中的安全开发教育，通过培训、考试等手段提升其整体的安全开发意识水平（BP.16.18）。

#### 12.2.2.4 等级 4 ：量化控制

该等级的安全开发能力要求描述如下：

组织建设：

a) 应对安全开发职能的运行效果以量化指标的形式进行定期衡量，并根据量化结果优化调整数据职能岗位的设置（BP.16.19）；

b) 应定期评估在当前组织职能架构下，安全开发职能岗位与开发、运维岗位之间的关系是否平衡（BP.16.20）。

#### 12.2.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

a） 组织建设：应能够持续优化组织的安全开发职能设置，以实现整体业务目标的优化（BP.16.21）；

b） 制度流程：应能够持续优化组织和人员管理的相关流程，以保证符合业务发展的实际情况（BP.16.22）。

### 12.3 PA17 合规管理

#### 12.3.1 PA描述

跟进组织需符合的法律法规和行业监管要求，以保证组织业务的发展不会面临合规风险。

#### 12.3.2 等级描述

#### 12.3.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：未在组织建立成熟稳定的安全开发合规工作，仅根据临时需求或基于个人经验在个别业务中考虑了安全开发合规要求（BP.17.01）。

#### 12.3.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由业务部门和开发团队相关人员负责安全开发合规管理（BP.17.02）；

b） 制度流程：重要软件和重要应用系统开发应通过识别安全开发合规要求，将合规要求更新至重要软件和重要应用系统开发相关的制度流程中，并在重要环节中设置相应的管控措施（BP.17.03）；

c） 人员能力：负责该项工作的人员应基本理解安全开发的合规要求，并可基于业务实际情况制定和推进安全开发合规方案（BP.17.04）。

#### 12.3.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：应在组织层面设立了专职负责安全开发合规的岗位和人员，负责明确安全开发合规需求，制定安全开发合规的技术规范和管理制度、流程，推进其在组织开发过程中执行（BP.17.05）。

b） 制度流程：

1） 应明确组织所有的外部合规要求并形成清单，能够定期通过跟进监管机构合规要求动态对该清单进行更新，同时将其拆分发送给相关方以进行宣贯（BP.17.06）；

2） 应依据相关法律法规及行业监管要求，建立组织统一的安全开发制度和管控措施（BP.17.07）。

c） 技术工具：应建立安全开发合规资料库，相关人员可以通过该资料库查询合规要求（BP.17.08）。

d） 人员能力：负责该项过程的人员应具备对安全开发合规要求的解读和分析能力（BP.17.09）。

#### 12.3.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

技术工具：应量化组织整体的合规情况，并将合规结果通过图形化方式上报给管理层，以保证管理层对组织整体的合规情况得到有效了解（BP.17.10）。

#### 12.3.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

组织建设：应设置专门的合规岗位，该岗位负责与监管机构对接，跟进监管机构的合规要求动态，并参与合规制度流程的前期制定（BP.17.11）。

## 12.4 PA18 开发测试环境安全管理

### 12.4.1 PA描述

通过建立安全的开发测试环境，保证应用软件和应用系统的开发在安全环境中开发，从而保证应用软件和应用系统的安全。

### 12.4.2 等级描述

#### 12.4.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：未建立独立的开发测试环境，仅根据临时需求或基于个人经验，保护开发时环境安全（BP.18.01）。

#### 12.4.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队负责对开发测试环境安全进行管理（BP.18.02）。

b） 制度流程：

1） 应明确独立开发测试环境的准入制度（BP.18.03）；

2） 应保证重要软件和重要应用系统开发位于独立的开发测试环境（BP.18.04）。

c） 人员能力：相关人员应充分了解独立开发测试环境安全的相关信息（BP.18.05）。

#### 12.4.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设置开发测试环境管理岗位和人员，负责管理制度的制定和落地推动（BP.18.06）。

b） 制度流程：

1） 应明确严格的开发测试环境独立制度和准入制度（BP.18.07）；

2） 应明确开发测试环境与其他环境的数据、文件、代码导入、导出的管理制度（BP.18.08）；

3） 应明确开发测试环境的代码安全管理制度（BP.18.09）；

4） 应明确开发测试环境安全的审计制度（BP.18.10）。

c） 技术工具：

1） 应通过技术工具实现开发测试环境与其他网络的逻辑隔离或物理隔离（BP.18.11）；

2） 应通过技术工具实现对开发测试环境与其他环境数据、文件、代码导入、导出的审计（BP.18.12）；

3） 应有工具检测开发测试环境中私自搭建的外部通路（BP.18.13）；

4） 应通过代码管理工具实现代码访问安全控制（BP.18.14）。

d） 人员能力：负责安全开发测试环境安全的人员应了解安全管理需求，对数据、文件、代码的导入导出能够评估风险（BP.18.15）。

#### 12.4.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

技术工具：应能统计开发测试环境中的安全违规数据，包括非法外联、非法文件导出等违规频度数据，支持管理提升决策（BP.18.16）。

#### 12.4.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

无进一步要求。

### 12.5 PA19 软件资产管理

#### 12.5.1 PA描述

通过建立针对组织软件资产的有效管理手段，实现统一的管理要求。

#### 12.5.2 等级描述

#### 12.5.2.1 等级1：非正式执行

该等级的安全开发能力描述如下：

组织建设：未建立成熟稳定的软件资产管理，仅根据临时需求或基于个人经验，针对个别软件资产进行管理（BP.19.01）。

#### 12.5.2.2 等级2：计划跟踪

该等级的安全开发能力要求描述如下：

a） 组织建设：应由开发团队负责对软件资产进行管理（BP.19.02）；

b） 制度流程：重要软件和重要应用系统应制定软件资产登记制度，建立软件资产清单，明确软件资产管理的相关方（BP.19.03）；

c） 人员能力：相关人员应充分了解所管理软件资产的相关信息（BP.19.04）。

#### 12.5.2.3 等级3：充分定义

该等级的安全开发能力要求描述如下：

a） 组织建设：组织应设置软件资产管理岗位和人员，对组织的软件资产进行统一管理，负责软件资产管理规范的制定和落地推动（BP.19.05）。

b） 制度流程：

1） 应在组织层面建立软件资产安全管理制度（BP.19.06）；

2） 应明确软件资产登记机制，确保组织内部重要的软件资产已有明确的管理者或责任部门（BP.19.07）；

3） 应明确软件资产的版本变更管理制度（BP.19.08）。

c） 技术工具：

1） 应通过技术工具执行软件资产的登记，实现对软件资产的自动属性标识（BP.19.09）；

2） 应建立软件资产版本变更管理工具，并能够及时更新软件资产版本相关信息（BP.19.10）；

3） 应通过技术工具实现对软件资产的漏洞和脆弱性进行跟踪和管理（BP.19.11）。

d） 人员能力：负责统一管理组织软件资产的人员应了解组织内部软件资产的管理需求，能够建立适用于组织业务实际情况的管理制度（BP.19.12）。

#### 12.5.2.4 等级4：量化控制

该等级的安全开发能力要求描述如下：

技术工具：应能统计软件资产的风险情况，合规情况，支持软件资产管理的调整（BP.19.13）。

#### 12.5.2.5 等级5：持续优化

该等级的安全开发能力要求描述如下：

无进一步要求。

# 附 录 A

**（资料性附录）**

**能力成熟度等级评估参考方法**

组织机构的安全开发能力成熟度等级取决于各个安全开发PA的能力成熟度等级。各个安全开发PA的成熟度等级取决于该PA中的BP对于目标等级的满足情况。

本标准不对评级方法做具体限定，表 A.1 给出一种综合判定参考方法，供评估人员参考。

**表 A.1 PA评估表**

| 过程域 | 是否适用 ，如果不适用 ，给出说明 | 评估小结 | 评估等级 | 修正因子 | 修正后等级 |
|---|---|---|---|---|---|
| PA（X） | 是/否 | | 1~5 | 05~1.5 | 1~5 |
| … | | | | | |
| 综合等级评定 | | | | | 1~5 |

**注 1 ：**基于组织机构业务场景和安全开发风险，可对开发生命周期各阶段安全（PA01~PA15）进行适用性判断。

**注 2 ：**基于安全开发行业专家经验和组织机构对某一PA安全开发风险的接受程度，可对等级结果进行修订，修订因子不超过 05~1.5 区间范围，修正后向下取整。

**注 3 ：**组织机构综合安全开发等级评定，可以采用“木桶原理”、“90%达标”等方式。

# 附 录 B

（资料性附录）

## 能力成熟度等级评估流程和模型使用方法

### B.1 能力成熟度等级评估流程

安全开发能力成熟度等级的评估从组织建设、制度流程、技术工具和人员能力 4 个关键能力展开。通过对各项安全过程所需具备安全能力的评估，可评估组织在每项安全过程的实现能力属于哪一等级。

能力成熟度等级评估要素如下：

a） 对能力成熟度等级的详细评估流程如下：

1） 确定模型适用范围：分析需要保护的开发资产及业务范围，确定模型使用或评估范围；

2） 确定能力成熟度级别目标：分析组织机构安全开发风险，确定能力成熟度等级建设目标；

3） 选取安全 PA：针对组织机构的开发相关的业务现状，选取适当的安全开发 PA。例如，对于有的组织机构而言，不存在第三方组件的处理，则无需选择第三方组件的 PA；

4） 执行 BP：依据标准对各等级安全开发 BP 要求，从 4 个关键能力进行落地和不断改进提升；

5） PA 安全评估：基于选择的安全 PA 范畴，针对各项安全 PA 对组织机构的安全开发实践情况进行现状的调研和分析。确定该 PA 的等级，参见表 A.1；

6） 确定组织机构整体等级：结合所有 PA 的等级，确定组织机构整体的安全开发能力成熟度等级，对安全开发能力进行持续建设和改进。

b） 其中，对 4 个关键能力的评估方法如下：

1） 组织建设：评估是否具有开展工作的专职/兼职岗位、团队或人员，其工作职责是否通过规范要求或其他手段得到确认和保障；

2） 制度流程：检查是否有关键安全开发领域的制度规范和流程及其在组织机构内的落地执行情况；

3） 技术工具：检查组织机构内的各项安全技术手段、通过产品工具固化安全要求或自动化的安全作业的实施运作情况；

4） 人员能力：执行安全开发工作的人员是否经过专业的技能和安全意识教育培训。

c） SSDCMM 的评估所采用的方式与基线风险评估的方式类似，可以包括但不限于以

下几种手段：

1） 人员访谈：通过访谈的方式与被评估方进行交流、讨论等活动，获取相关证据，了解有关信息；

2） 文档审核：由被评估方输入与安全开发相关的文档材料（如安全开发的方针政策、制度规范流程、培训教育材料、以及相关的设计方案、配置说明、运行记录和其他配套表单），评估小组审核相关的文档材料是否已涵盖完整开发生存周期的 PA 和控制项；

3） 配置检查：根据被评估方提供的技术材料，登录相关的系统工具平台，检查配置是否与材料保持一致，对文档审核内容进行核实；

4） 工具测试：利用技术工具对系统工具进行测试，验证是否符合安全开发成熟度模型特定等级的技术能力要求；

5） 旁站式验证：评估人员在现场通过实地观察人员行为、技术设施和环境状况判断人员的安全意识、业务操作、管理程序等方面的安全情况。

### B.2 能力成熟度模型使用方法

由于各组织机构在业务规模、业务对开发的依赖性以及组织机构对安全开发工作定位等方向的差异，组织机构对模型的使用应“因地制宜”。

组织机构使用 SSDCMM 的闭环如图 B-1 所示。

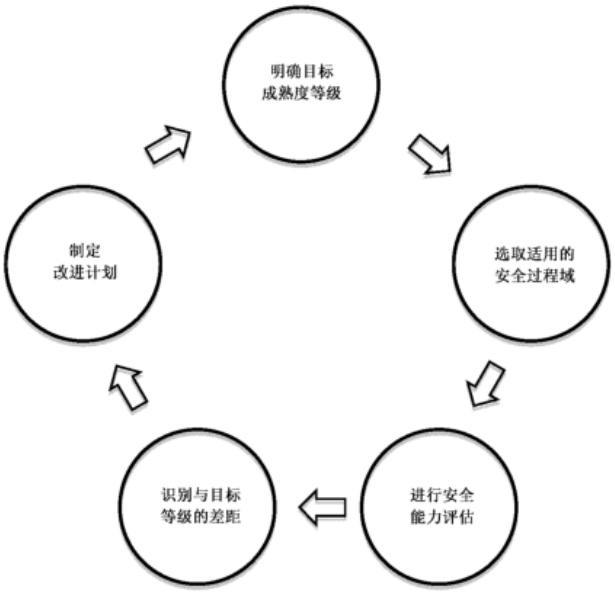


**图 B-1 推荐的成熟度模型使用步骤**

使用模型时，组织机构应首先明确其安全开发能力的目标成熟度等级。根据对组织机构整体的安全开发能力成熟度等级的定义，见 5.3，组织机构可以选择适合自己业务实际情

况的安全开发能力成熟度等级目标。本标准定义的安全开发能力成熟度等级中，3 级目标适用于所有具备安全开发保障需求的组织机构作为自己的短期目标/长期目标，具备了 3 级的安全开发能力则意味着组织机构能够针对安全开发的各方面风险进行有效的控制。然而，对于业务中开发规模较小的组织机构而言，其安全开发保障的需求整体较弱，因此其短期目标可先定位为 2 级，待达到 2 级的目标之后再进一步提升到 3 级的能力。

在确定目标成熟度等级的前提下，组织机构根据开发生命周期所覆盖的业务场景挑选适用于组织机构的安全开发 PA。

最后，组织机构基于对成熟度模型内容的理解，识别安全开发能力现状并分析与目标能力等级之间的差异，在此基础上进行安全开发能力的整改提升计划。而伴随着组织机构业务的发展变化，组织机构也需要定期复核、明确自己的目标成熟度等级，然后开始新一轮目标达成的工作。

# 参 考 文 献

[1] GB/T 29246-2017 信息技术 安全技术信息安全管理体系 概述和词汇

[2] GB/T 31497-2015 信息技术 安全技术 信息安全管理 测量（ISO / IEC27004 ：2009，IDT）

[3] GB/T 19000-2016 质量管理体系 基础和术语

[4] GB/T 20261-2006 信息技术系统安全工程能力成熟度模型

[5] GB/T 25069-2010 信息安全技术 术语

[6] GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范

[7] GB/T 30271-2013 信息安全技术 信息安全服务能力评估准则

[8] GB/T 22081-2016 信息技术安全技术信息安全控制实践指南（ISO/IEC27002 ：2013[3]，IDT）

[9] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

[10] ISO / IEC 21827 ： 2008 Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model（SSE-CMM）