ICS 35.020

L70

YD

中华人民共和国通信行业标准

YD/T 3764.6—20XX

[代替 YD/T]

研发运营一体化（DevOps）能力成熟度模型 第6部分：安全及风险管理

The capability maturity model of devops—Part 6 ： security risk management

（报批稿）

[点击此处添加本稿完成日期]

[××××]-[××]-[××]发布　　[××××]-[××]-[××]实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准是研发运营一体化（DevOps）能力成熟度模型系列标准之一。该系列标准的结构及名称如下:

——研发运营一体化（DevOps）能力成熟度模型 第1部分：总体架构

——研发运营一体化（DevOps）能力成熟度模型 第2部分：敏捷开发管理

——研发运营一体化（DevOps）能力成熟度模型 第3部分：持续交付

——研发运营一体化（DevOps）能力成熟度模型 第4部分：技术运营

——研发运营一体化（DevOps）能力成熟度模型 第5部分：应用设计

——研发运营一体化（DevOps）能力成熟度模型 第6部分：安全及风险管理

——研发运营一体化（DevOps）能力成熟度模型 第7部分：评估方法

——研发运营一体化（DevOps）能力成熟度模型 第8部分：系统和工具技术要求

本部分是第6部分：安全及风险管理

本部分按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：中国信息通信研究院、北京华佑科技有限公司、腾讯云计算（北京）有限责任公司、阿里巴巴（中国）有限公司、OPPO广东移动通信有限公司、奇安信科技集团股份有限公司、浙江蚂蚁小微金融服务集团股份有限公司、杭州安恒信息技术股份有限公司、北京金山云网络技术有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、普元信息技术股份有限公司、畅捷通信息技术股份有限公司、苏宁消费金融有限公司、中软国际科技服务有限公司

本部分主要起草人：牛晓玲、萧田国、刘凯铃、景韵、张嵩、赵锐、韩方、韩晓光、庄飞、李青、李滨、张祖优、武鑫、程岩、袁明坤、杨廷峰、毛茂德、陈雪秀、郑锐、王广清、郭雪、张娜、邸望春、王晓翔、侯大鹏、公丽丽、王永霞、程莹、张婷婷、叶林、周麟、王浏明、李明亮、王迪、李卜、熊昌伟、戚文平、顾黄亮、王云峰、马婷、李励立

研发运营一体化（DevOps）能力成熟度模型 第6部分：安全及风险管理

1 范围

本部分规定了IT软件或相关服务在采用研发运营一体化（DevOps）统一开发模式下，如何保障IT软件和相关服务的安全，进行风险管理。

本部分适用于具备IT软件研发交付运营能力的组织实施IT软件开发和服务过程的能力进行评价和指导；可供其他相关行业或组织进行参考；也可作为第三方权威评估机构衡量软件开发交付成熟的标准依据。

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，仅所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（包括所有的修改单）适用于本文件。

[1]GB/T 25069-2010 信息安全技术 术语

[2]GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

3 术语、定义及缩略语

3.1 术语及定义

下列术语和定义适用于本文件。

3.1.1

安全基线 security baseline

为了明确应用需要满足的最基本的安全防护能力而制定的一系列安全配置基准。

3.1.2

安全门限 security threshold

用于确定安全质量的最低可接受风险级别。

3.1.3

安全态势感知 security situation awareness

基于环境的、动态、整体地洞悉安全风险的能力,是以安全大数据为基础,从全局视角提升对安全威胁的发现识别、分析、响应处置能力的一种方式。

3.1.4

安全需求基线 security requirements baseline

经过攻击面分析及威胁建模，确定的满足软件安全风险管理的基本安全需求清单。

3.1.5

安全需求标准库 security requirements standard library

基于信息安全相关的国家法律、法规，行业监管要求，公司的策略与实践，以及信息安全业界的最佳实践，形成的安全的功能需求、功能性的安全需求以及非功能性安全需求的标准集合。

3.1.6

暴力破解 brute force attack

攻击者通过系统地组合所有可能性（例如登录时用到的账户名、密码），尝试所有的可能性破解用户的账户名、密码等敏感信息。

3.1.7

分布式拒绝服务攻击 distributed denial of service;DDoS

处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击，其中的攻击者可以有多个。拒绝服务指一种系统失去可用性的攻击。[GB/T 25069-2010]

3.1.8

攻击面分析 attack surface analysis

程序任何能被用户或者其它程序所访问到的部分，这些暴露给用户的地方往往也是最可能被恶意攻击者攻击的地方。攻击面分析就是枚举所有访问入库、接口、协议以及可执行代码等的过程。

3.1.9

工作项 work item

项目研发过程中的需求、任务、缺陷等。

3.1.10

黑盒安全测试 black-box security test

也称为动态应用安全测试，在测试或运行阶段分析应用程序的动态运行状态。模拟黑客行为对应用程序进行动态攻击，分析应用程序的反应，从而确定该应用是否易受攻击。

3.1.11

红蓝对抗 reds vs. blues

攻守双方在实际环境中进行网络进攻和防御的一种网络安全攻防演练。

3.1.12

基础设施即代码 infrastructure as code

基于软件开发实践的基础设施自动化方法，强调系统及其配置的日常置备和变更具有一致性和可重复性。

3.1.13

金丝雀发布 canary release

可以降低在生产环境中引入新软件版本的风险的技术，先将新版本发布给小部分用户，逐渐发布到整体基础设施并且将新版本发布给所有用户。

3.1.14

蓝绿部署 blue-green deployment

可以保证系统在不间断提供服务的情况下上线的部署方式。

3.1.15

逆向攻击 reverse attack

对软件等进行逆向破解以进行黑客攻击的一种手段。

3.1.16

渗透测试 penetration test

以未经授权的动作绕过某一系统的安全机制的方式，检查数据处理系统的安全功能，以发行信息系统安全问题的手段。也成渗透性测试或逆向测试。[GB/T 25069-2010 信息安全技术 术语]

3.1.17

威胁建模 threat modeling

通过结构化的方法，系统的识别、评估产品的安全风险和威胁，并针对这些风险、威胁制定消减措施的一个过程。

3.1.18

研发安全运营一体化 DevSecOps

全新的安全及风险管理理念与模式，是指将安全内嵌到应用的全生命周期中，在这种模式下安全是每个人的责任。

3.1.19

资产 asset

对组织具有价值的任何东西。[GB/T 25069-2010]

3.1.20

资产动态感知 asset dynamic awareness

基于资产探测、自动化关联分析等手段，实现对资产变化的动态检测，实时感知设备、端口、服务等资产的变化。

3.1.21

资产风险管理 asset risk management

通过全面识别企业it资产，通过漏洞扫描、漏洞情报等手段及时识别资产的安全风险，并进行响应，实现资产风险的有效管理。

3.1.22

注入攻击 injection attacks

将不受信任的数据作为命令或查询的一部分发送到解析器时攻击手段，其本质是把用户输入的数据当做代码执行，如：SQL注入、XML注入、命令注入、CRLF注入等。

3.2 缩略语

下列缩略语适用于本文件。

API	应用程序编程接口	Application Programming Interface
CD	持续交付	Continuous Delivery
CI	持续集成	Continuous Integration
CSRF	跨站点请求伪造	Cross Site Request Forgery
IDE	集成开发环境	Integrated Development Environment
MTTR	平均修复时长	Mean Time To Repair
RASP	应用运行时自我保护	Runtime Application Self-Protection
SDK	软件开发工具包	Software Development Kit
XSS	跨站点脚本	Cross-Site Scripting

4 安全及风险管理

本标准规定了IT软件或相关服务在采用研发安全运营一体化（DevSecOps）的开发模式下，相比于传统开发模型发生变化，安全融入每个阶段过程，开发、安全、运营各部门紧密合作。DevSecOps强调在安全风险可控的前提下，帮助企业提升IT效能，更好地实现研发运营一体化。

安全及风险管理分级技术要求包括：控制通用风险、控制开发过程风险、控制交付过程风险、控制运营过程风险，如表1所示。

表 1 安全及风险管理分级技术要求

安全及风险管理			
控制通用风险	控制开发过程风险	控制交付过程风险	控制运营过程风险
组织建设和人员管理	需求管理	配置管理	监控管理
安全工具链	设计管理	构建管理	运营安全
基础设施管理	开发过程管理	测试管理	应急响应
第三方管理		部署与发布管理	运营反馈
数据管理			

度量与反馈改进			

5 研发运营一体化控制通用风险

在 DevOps 模式下，安全内建于开发、交付、运营过程中，通用风险覆盖三个过程中的共性安全要求，包括：组织建设和人员管理、安全工具链、基础设施管理、第三方管理、数据管理、度量与反馈改进，具体要求如表 2 所示。

5.1 组织建设和人员管理

组织建设和人员管理指组织在将安全内建到DevOps过程中时，需要建设对应的组织负责不同的安全职责与工作，需要建设组织级的安全文化以及对研发人员、测试人员、技术运营人员等进行安全管理，包括第三方机构和人员，实现每个人都为安全负责。

5.2 安全工具链

安全工具链，关注研发运营一体化过程中与应用相关的安全工具。安全工具链建设过程中，一方面，将安全左移研发过程(DevSec)，并强化运营过程安全（SecOps），实现将安全工具内嵌到DevOps全生命周期；另一方面，安全工具由人工化、单一化向自动化、多元化及智能化方向发展。

5.3 基础设施管理

基础设施作为应用的载体，包括基础资源层、操作系统层、应用中间件层等，基础设施的安全性、一致性、可靠性与稳定性为应用的安全及风险管理提供基础支撑。

5.4 第三方管理

第三方管理是指围绕应用安全对合作的第三方机构、人员、软件、服务进行安全管理，包括：接入控制、日常管理与监控、安全风险评估等，第三方机构包括：监管机构、供应商、合作伙伴等。

5.5 数据管理

数据管理是指在研发运营一体化过程中，对从采集、存储、传输、处理、交换到销毁的整个数据生命周期过程中涉及的各类数据进行安全及合规管理，利用制度、流程及工具等手段保护数据的机密性、完整性和可用性。[GB/T 37988-2019 5.4 6.1]

注： 关于数据安全生命周期及数据分类分级可以参考《信息安全技术 数据安全能力成熟度模型》。

5.6 度量与反馈改进

度量与反馈改进是指通过对应用的研发、交付、运营过程的安全风险进行度量、展示并反馈给团队处理和改进的机制。设立清晰可量化的安全度量指标模型并可视化展示度量数据，有助于团队共享

信息、识别改进方向并衡量改进效果。另外，设立及时有效的反馈机制，可以加快信息传递速率与准确性，有助于尽早地发现问题、分析问题、反馈问题、解决问题。度量与反馈改进可以保证整个团队内部安全信息获取的及时性和一致性，实现基于度量的持续改进。如表2所示：

表 2 研发运营一体化控制通用风险要求

级别	组织建设和人员管理	安全工具链	基础设施管理	第三方管理	数据管理	度量与反馈改进
1	有专职的安全管理岗位及人员。	具有漏洞扫描工具，如：Web 安全扫描工具、App 安全扫描工具、主机安全扫描工具等。	1） 生产环境的管理有安全管理规范与流程； 2） 生产环境具有安全基线。	具有第三方管理的安全规范与制度，明确人员管理、数据安全、服务器运维等安全要求。	数据管理具有基本的安全管理要求。	安全问题统计与报告以手工方式为主。
2	1) 有专门的安全管理团队与安全主管，如：安全部门等； 2) 有明确的组织内各角色的安全职责、权利和义务； 3) 研发人员、测试人员和技术运营人员的安全职责分离； 4) 有明确的团队间安全协作流程和规范。	1） 确保安全工具的有效性及安全性，具有一定的安全规范和要求，如：定期规则升级、软件补丁升级、工具版本升级等； 2） 具有应用安全自动化测试工具及安全配置加固工具，包括但不限于：源代码安全检测工具、黑盒安全测试工具、安全基线检查工具、主机安全扫描工具等； 3） 具有自动化漏洞扫描平	1） 基础设施的管理有安全规范与流程，如：云平台安全管理、中间件安全漏洞管理等； 2） 基础设施的管理有安全的工具系统； 3） 具有基础设施的安全基线； 4） 定期执行基础设施安全基线扫描，及时发现和处理安全风险。	1） 具有完善的第三方管理安全规范与制度，如：明确的第三方人员引入和办公场所出入规则、第三方服务的访问控制等； 2） 第三方合作须签署相应的安全协议； 3） 控制第三方软件的接入风险，包括但不限于：第三方开源软件、第三方商业软件等。	1） 数据管理具有安全管理要求，覆盖运营过程，如：制度、规范等； 2） 具有明确的数据分类分级方法，对生成或收集的数据进行分类分级标识，如：通过打标签的方式等； 3） 对于不同环境、类别及级别的数据具有安全管控机制，如：访问控制、数据加解密、数据脱敏等。	1） 仅在局部领域定义部分安全度量指标； 2） 安全度量报告以自动化方式生成和展示，团队成员可查看报告； 3） 基于度量识别的安全问题纳入系统管理，并定期反馈团队； 4） 团队定期实施改进并取得效果，如：每月/季度一次、应用上线前后等。

		台，具备多维度扫描工具组合扫描，具备周期性巡检机制； 4） 具有软件组成分析工具，包括但不限于：开源组件安全风险检测工具等。				
3	1） 同上，且需达到以下要求： 2） 有完善的安全管理体系与流程，如：参考行业的最佳实践和监管要求等； 3） 有高效的团队间安全协作机制，包括但不限于：虚拟安全小组、定期或不定期召开团队间会议、共同协作处理关键安全问题等； 4） 已建立安全专家组织，负责评审关键架构设计并建设安全、研发与运营团队的一体化规范等；	1） 同上，且需达到以下要求： 2） 具有安全需求管理工具，并在集成完成前进行代码安全检测； 3） 具有威胁建模及安全需求管理自动化平台； 4） 具有开源组件许可证合规检测工具； 5） 具有应用安全自动化测试工具及安全配置加固工具，并集成到研发运营一体化平台； 6） 具有统一的漏洞管理平台，对漏洞进行汇聚及集中	1） 同上，且需达到以下要求： 2） 具有统一的基础设施安全基线，包括但不限于：开发、测试、生产环境等； 3） 基础设施的管理采用基础设施即代码与自动化方式管理，实现管理低风险、可追溯、可审计； 4） 具有安全的开发环境与工具，包括但不限于：安全的开发工具、安全的开发配置、安全的CI/CD工具等； 5） 基础设施	1） 同上，且需达到以下要求： 2） 通过技术平台对第三方合作进行管理和监控，如：办公场所与机房人员出入、应用的访问和操作等； 3） 对于因第三方合作造成的安全事件、问题有应急响应措施； 4） 对第三方进行定期和按需的安全风险评估和审计，如：通过相关权威机构安全评测等。	1） 数据管理按数据生命周期进行管理，具有完善的安全管理要求及流程，包括但不限于制度、规范、流程、指南等； 2） 实现对数据分类分级的自动化标识、审核等，对于不同环境、类别及级别的数据具有自动化管控手段； 3） 具备自动化的数据安全相关管理工具，如：数据资产管理、数据脱敏、数据防泄漏等； 4） 具备数据使用过程的自动化监控和审	1） 建立跨领域、跨组织、端到端的安全度量指标体系并持续更新，具有部分预测性指标，如：漏洞修复率、安全问题MTTR、安全覆盖率等； 2） 具有安全度量平台，支持自动生成报告内容、分类分级展示、趋势展示、阈值设置与预警、按需定制、多种图表类型、订阅等； 3） 安全度量数据完整真实，数据时效性不低于T+1天，度量数据至少半年以

	5） 针对研发人员、测试人员和技术运营人员开展专项的安全技能培训； 6） 在IT组织内进行安全意识教育和培训，提升团队成员安全能力，建立安全文化。	的管理，实现自动化漏洞扫描、漏洞修复通知推送、提供漏洞验证，支持漏洞按照种类与风险级别等维度进行统计、分析、展示； 7） 具有统一的资产风险管理平台，能对应用相关的资产进行风险监控及管理； 8） 具有自动化的安全测试平台； 9） 具备自主集成外部安全工具的能力，如：安全自动化测试平台集成多种黑盒安全扫描工具等。	具备良好的抗攻击与灾备容错能力，能有效地实现多方联防联控； 6） 基础设施支持低风险的应用发布方式。		计机制。	上； 4） 基于度量识别的安全问题可自动化反馈给团队的工作项管理平台； 5） 度量反馈的安全问题纳入研发迭代的待办事项列表； 6） 基于度量分析安全问题库，反馈针对性的安全建议，如：历史共性安全缺陷等。
4	1） 同上，且需达到以下要求： 2） 有高级别的安全管理组织，履行组织级的安全治理职责，如：重大风险的审阅和处置策略的决策等；	1） 同上，且需达到以下要求： 2） 应用集成安全SDK，具有包括但不限于密钥安全、资源操作安全、运行时自我防护能力等，同时具备	1） 同上，且需达到以下要求： 2） 具有统一的基础设施管理平台； 3） 基础设施的管理具有部分智能化安全能力，如：支持秒级容灾容	1） 同上，且需达到以下要求： 2） 通过自动化的技术平台对第三方进行安全管理、监控和应急响应，如：第三方安全评级与风险监控系统	1） 同上，且需达到以下要求： 2） 具备数据流转的自动化追踪和溯源能力； 3） 具备数据安全风险监控系统，对数据使用过程中的	1） 同上，且需达到以下要求： 2） 建立基于分级评价的完整安全度量体系，如：能力成熟度模型等； 3） 具有安全度量平台，支

	3） 有完善的安全专家团队，如：数据安全、网络安全等； 4） 有常态化的安全文化建设，如：完善的培训机制等。	统一安全管控平台； 3） 具备全网资产动态感知平台，构建资产安全风险画像，实时感知企业资产的风险变化； 4） 具备自主研发安全工具的能力，如：自研基于流量的 web 安全扫描器等； 5） 持续运营和改进安全工具，提升安全工具效能，包括但不限于安全策略持续调优、安全工具的能力提升等。	错切换、安全风险问题自动处置等。	等； 3） 通过自动化方式对第三方进行实时的安全风险评估与审计。	风险进行自动化的识别、监控、告警和处置。	持成熟度展示； 4） 团队持续改进，提升安全能力的成熟度； 5） 团队基于度量反馈主动持续改进，全面提升安全效能，如：漏洞修复率、误报率等指标的改善等； 6） 识别有效改进，并作为企业级安全知识扩展到整个组织。
5	1） 同上，且需达到以下要求： 2） 具有行业影响力的安全专家团队，能有效对行业进行贡献； 3） 具有安全组织建设与安全人员管理的持续改进机制。	1） 同上，且需达到以下要求： 2） 具备智能化软件安全开发全生命周期管理平台，智能化威胁建模、智能化安全测试及智能化的安全风险评估； 3） 具备智能化应用安全态	1） 同上，且需达到以下要求： 2） 基础设施管理具备全面的智能化安全能力，能够自动化发现、分析和修复环境问题，及时发现并处置安全威胁。	1） 同上，且需达到以下要求： 2） 通过智能化的技术平台对第三方进行安全管理、监控和应急响应； 3） 通过智能化方式对第三方进行实时的安全风险评估	1） 同上，且需达到以下要求： 2） 具备智能化数据安全风险管理能力，实现对数据安全风险的态势感知，实现数据安全风险的智能化预测和处置。	1） 同上，且需达到以下要求： 2） 持续改进安全指标体系与安全度量平台，支持深度智能化、支持业务决策等。

		势感知平台，智能化资产安全风险感知及处置，智能化应用安全威胁感知及防护。		与审计。		

6 研发运营一体化控制开发过程风险

从应用的开发过程开始实施安全风险管理工作，可以保障进入交付过程的代码是安全的，降低后续交付、运营中的安全风险，保障研发运营一体化的整体安全，包括：需求管理、设计管理和开发过程管理，具体要求如表3所示。

6.1 需求管理

需求管理是指将安全工作左移到应用生命周期的源头，在应用的需求阶段即进行安全风险控制，定义安全需求并采取有效的措施和手段，从而控制开发过程的安全风险。安全需求既要包括功能性的安全需求，如：认证、授权、安全日志与审计等；又要包括非功能性安全需求，如：健壮性、可用性、可靠性等。

6.2 设计管理

设计管理关注开发过程中应用架构与设计过程中的安全风险控制。通过攻击面分析、威胁建模等手段，识别应用潜在的安全风险和威胁，制定措施消除或减少威胁、规避风险，确保应用的安全性。

6.3 开发过程管理

开发过程管理指对编码过程中的安全风险进行管理，通过引入安全编码规范与检测机制降低源代码中的安全风险。如表3所示：

表 3 研发运营一体化控制开发过程风险要求

级别	需求管理	设计管理	开发过程管理
1	需求包含基本的安全内容。	具有基础的安全设计规范，包括但不限于：身份认证、访问控制、加密等。	具有项目级安全编码规范。
2	1） 需求包含安全内容，并纳入团队整体的需求清单； 2） 分析项目涉及的法律法规和行业规范要求，并制定合规	1） 同上，且需达到以下要求： 2） 基于风险级别及业务优先	具有团队级安全编码规范，对于不同类型编码语言具有相应的安全编码指南。

	和安全需求基线，如：个人隐私风险等； 3） 针对安全需求具有相应的用例，并明确验收标准，如：安全需求清单等； 4） 针对不同技术栈，制定相应的安全需求。	级等对应用进行分级； 3） 制定和发布标准化的安全性功能，如：统一认证接入等； 4） 安全设计中具有基础的威胁建模的分析方法； 5） 基于应用分级，针对应用开展安全设计评审，并交付安全设计方案。	
3	1） 同上，且需达到以下要求： 2） 具有持续更新的安全需求标准库和管理平台，包括但不限于：法律法规、行业监管要求、公司的安全策略以及业界最佳实践等； 3） 针对应用场景特点，制定相应的安全需求与用例，如：Web 应用安全、移动应用安全等； 4） 安全需求与其他功能性需求同步开展测试，由测试团队和安全团队联合负责。 5） 安全需求既要包括功能性需求，如：认证、授权、安全日志与审计等，又要包括非功能性需求，如：健壮性、可用性、可靠性等。	1） 具备完善的安全设计规范，如：标准化 API 接口安全规范、标准化互联网应用安全架构等； 2） 具备标准化且安全的技术栈，如：中间件、框架和公共库等； 3） 安全设计中具有完善的威胁建模的分析方法； 4） 针对高风险应用，开展安全设计、攻击面分析与威胁建模，交付安全设计方案； 5） 在安全设计过程中，对共性安全解决方案进行持续积累，促进形成标准化的安全设计规范。	1） 具有组织级安全编码规范，并持续更新，规范包括但不限于：安全编码指南、安全示例代码、不推荐的函数列表、安全门限等； 2） 代码提交前，进行源代码安全检测，如：采用 IDE 安全检测插件等； 3） 代码提交前，对开源组件的安全风险及合规进行检测。
4	1） 同上，且需达到以下要求： 2） 针对具体的业务逻辑风险，制定相应的安全需求与用例； 3） 具有自动化的安全需求管	1） 同上，且需达到以下要求： 2） 具备标准化的威胁建模方法和工具； 3） 具备标准化的安全功能组件，如：安全加固 SDK、安全	1） 同上，且需达到以下要求： 2） IDE 集成源代码安全检测插件，实现安全编码规范的自动化检查。

	理平台，如：基于业务场景自动推荐安全需求等。	软键盘、CSRF-token 组件、XSS 过滤器等。	
5	1） 同上，且需达到以下要求： 2） 具有智能化的安全需求管理平台，包括：多渠道需求自动化收集与分析等； 3） 具有完善的安全需求自动化验证能力。	1） 同上，且需达到以下要求： 2） 具备智能化的威胁建模平台，智能化进行威胁建模并输出安全设计方案。	1） 同上，且需达到以下要求： 2） 编码工具具有智能化识别安全问题并提供解决方案的能力。

7 研发运营一体化控制交付过程风险

交付过程是指从代码提交到应用发布给用户使用，安全交付是将安全内建到交付过程中，包括：配置管理、构建管理、测试管理、部署与发布管理，具体要求如表4所示。

7.1 配置管理

配置管理是指在持续交付过程中，所有与项目相关的产物，以及它们之间的关系都被定义、修改、存储和检索的过程。配置管理保证了应用交付过程中所有交付产物的完整性，一致性和可追溯性。安全的配置管理是控制交付过程风险的基础，是保障持续交付正确性的前提，主要包括：源代码及相关脚本、依赖组件、发布制品、应用配置、环境配置等的安全管理。

7.2 构建管理

构建管理是指从软件代码到可运行程序之间的过程管理，安全的构建过程管理可提升应用的发布制品安全性，可靠且可重复的构建过程有利于安全问题的避免和版本变更追溯，构建的安全管理主要包括构建工具、构建环境、构建脚本等的安全。

7.3 测试管理

测试管理在应用投入生产运行之前，对安全需求进行验证，尽可能地发现并排除应用中的安全缺陷，从而提高软件的安全质量。安全需求既要包括功能性的安全需求，如：认证、授权、安全日志与审计等；又要包括非功能性安全需求，如：健壮性、可用性、可靠性等。

7.4 部署与发布管理

部署与发布管理是指在实现软件价值向最终用户的交付的同时，通过安全的流程与规范、设置安全检查点等方式保证部署与发布过程的安全，如表4所示：

表 4 研发运营一体化控制交付过程风险要求

级别	配置管理	构建管理	测试管理	部署与发布管理
1	配置管理具有项目级安全管理规范。	构建管理有安全检查清单。	安全测试以手工为主。	应用的部署与发布具有基础的安全检查点。
2	1） 配置管理具有团队级安全管理规范，如：配置管理安全检查清单等； 2） 对源代码、依赖组件、发布制品、数据库变更脚本、应用配置进行安全管理并有源代码提交安全门限，如：定期的源代码安全扫描、开源组件的引入规范、代码访问授权控制等。	1） 构建管理有安全管理规范； 2） 具有安全的构建工具； 3） 构建脚本与配置内容的变更有审核机制。	1） 在交付过程中，有明确的安全测试的要求，安全测试结果作为发布的前置条件； 2） 采用主流的安全工具进行安全测试和合规扫描，如：黑盒安全测试工具、静态代码安全扫描工具等； 3） 开发测试环境不直接使用生产数据，采用公开数据、构造出的测试数据或经过脱敏后的生产数据； 4） 基于安全需求，制定相应的安全测试用例，并进行验证测试； 5） 安全测试用例和非安全性测试用例进行统一管理。	1） 应用的部署与发布有安全流程与规范； 2） 应用的部署与发布有明确的安全检查点，如：漏洞扫描报告等。
3	1） 配置管理有组织级全面的安全管理规范，如：配置数据访问策略、工具平台备份恢复方案、开源管理规范等； 2） 对源代码、依赖组件、发布制品、数据库变更脚本、环境	1） 同上，且需达到以下要求： 2） 具有安全的构建工具平台与环境，包括但不限于：环境一致性、环境隔离、数据隔离等； 3） 提交构建中集成	1） 具有完善的安全测试流程和规范，安全测试结果作为发布的前置条件； 2） 安全测试结果具有明确的质量门限，如：高危漏洞数量不能大于 0 等；	1） 应用的部署与发布有完备的安全流程与规范，如：安全回退、备份机制、应用发布安全指南等； 2） 应用的部署与发布过程采用自动化的安全控制方式，并嵌入到 DevOps 流水线

	配置脚本等进行安全管理和统一变更管理，并有自动化安全管理机制，如：开源组件的自动化安全扫描、源代码安全规范、源代码与制品可追溯等； 3） 对高风险代码进行人工代码安全评审，并有自动化机制辅助评审； 4） 制品及相关配置有安全检查以及相应的防篡改机制； 5） 使用代码保护机制保护知识产权和关键信息及算法，提升逆向攻击和漏洞发现难度，如：互联网应用等； 6） 制品入库前进行自动化安全检查。	轻量级代码及依赖组件安全扫描； 4） 具有安全可靠的构建工具平台与运维保障机制。	3） 具备完善的端到端安全测试工具链进行安全测试和合规扫描，覆盖主要的安全测试类型，包括但不限于：黑盒安全测试工具、静态代码安全扫描工具、开源组件安全扫描工具、容器安全扫描工具等安全测试工具； 4） 在流水线中集成自动化安全测试，安全测试结果自动化反馈研发处理； 5） 引入人工渗透测试，如：针对业务逻辑、越权等漏洞进行人工测试； 6） 具备自动化安全测试结果汇总展示能力； 7） 持续优化安全测试策略，具备机制持续降低误报率与漏报率。	中，如：自动检查漏洞扫描报告、自动化SQL执行等； 3） 应用在各个环境中的部署与发布过程采用统一且安全的自动化工具与过程； 4） 应用的部署与发布具备强制的安全质量门限机制，阻断不安全应用发布上线； 5） 应用的部署与发布具有低风险发布机制，如：蓝绿部署、金丝雀发布等。
4	1） 同上，且需达到以下要求： 2） 对于配置管理内容变更进行自动化的安全管理； 3） 建立软件资产安全风险库，如：源代码、开源组件、配置库、发布版本等的安全风险。	1） 同上，且需达到以下要求： 2） 构建过程可自动识别安全风险并推荐可执行的策略。	1） 同上，且需达到以下要求： 2） 具有集中的漏洞聚合及管理平台，对不同的安全测试结果进行聚合及关联分析，如：源代码安全漏洞和黑盒安全测试漏洞进行上下文关联分析等； 3） 可以基于不同应	1） 同上，且需达到以下要求： 2） 应用的部署与发布有完备的安全流程与规范，可以针对不同的业务或场景进行分类分级管理； 3） 应用的部署与发布的安全管理流程、工具进行持续改进。

			用场景进行智能化安全风险决策； 4） 定制化安全测试工具和脚本进行深度安全测试，如：对API进行定制化的安全测试、修改开源工具提高渗透测试效率等； 5） 定期进行高阶安全评估，如：引入红蓝对抗机制等。	
5	1） 同上，且需达到以下要求： 2） 具有智能化的配置管理平台，可智能修复代码等配置内容的安全问题。	1） 同上，且需达到以下要求： 2） 具有智能化识别安全风险的构建工具平台。	1） 同上，且需达到以下要求： 2） 安全测试完全自动化与智能化，并内嵌到开发与交付过程中，无需人工干预； 3） 智能化优化安全测试策略。	1） 同上，且需达到以下要求： 2） 应用的部署与发布风险控制全面实现自动化和智能化，如：基于安全风险等级的智能化部署决策、无需人工干预等。

8 研发运营一体化控制技术运营过程的安全风险

技术运营过程是指应用发布给用户后的过程，将安全内建于运营过程中，通过监控、运营、响应、反馈等实现技术运营的安全风险闭环管理，包括：安全监控、运营安全、应急响应、运营反馈，具体要求如表5所示。

8.1 安全监控

安全监控是指在运营过程中对应用网络、运行状态等进行监控，识别攻击行为、发现安全问题和风险。

8.2 运营安全

运营安全是指对技术运营过程中的配置管理、变更管理等进行安全管理，通过安全监控分析、安全检测、安全缺陷识别、处理与跟踪等方式降低或消除安全问题对生产运营过程带来的影响。

8.3 应急响应

应急响应识别企业潜在安全危机和风险，针对运营过程中的安全事件、风险进行响应、跟踪和处置，及时消减风险和影响，保障业务连续性。应急响应涉及预案与流程机制建立的要求、应急演练的要求、事件管理的要求、人员与团队的要求、响应指标要求、自动化要求。

8.4 运营反馈

运营反馈关注安全信息的动态性、实时性、整体联动性，通过对应用研发、交付、运营全流程中的安全漏洞、缺陷和事件信息的获取并向“左”（即向上游）反馈，实现DevSecOps全过程的及时、有效反馈，实现DevSecOps闭环管理，如表5所示

表 5 研发运营一体化控制运营过程风险要求

级别	安全监控	运营安全	应急响应	运营反馈
1	在运营监控中实现基础的安全监控。	运营过程具备基础的安全管理规范，包括但不限于：变更管理安全审核机制等。	1） 具有基础的安全应急响应机制与流程； 2） 基于事件、风险的影响情况和严重程度进行分级、分类。	1） 具备基础的安全问题反馈机制； 2） 定期收集运营过程中的安全问题，并进行反馈。

2	1） 具有安全监控管理要求，包括流程、制度、策略、组织、措施； 2） 具有专有的安全监控机制，能够覆盖部分业务场景，包括但不限于：病毒攻击、DDoS 攻击、暴力破解、注入攻击、接口滥用等。	1） 运营过程具备基础的安全管理规范，包括但不限于：变更管理安全审核机制、配置管理权限控制、自动化运维工具安全准入机制与操作权限管理等； 2） 定期进行常规安全检查与改进，检查内容包括但不限于：应用运行状态、系统漏洞和数据备份等； 3） 定期进行线上应用安全检测与处置，如：定期 Web 漏洞扫描、主机漏洞扫描、渗透测试等； 4） 具备对不符合安全质量门限的应用上线检查与发现机制，如：应用上线安全检查清单等； 5） 通过对告警信息、日志等进行自动化分析，发现线上应用存在的安全风险并进行通知、处置、跟踪； 6） 收集漏洞和情报信息，对线上应用的运行环境、系统服务、使用框架及三方组件等进行预警及处置。	1） 制定和发布应急响应流程与规范，有基本的事件记录，针对不同级别的事件有对应的响应要求与处理流程； 2） 设立专门的安全应急响应角色，跟进安全应急响应与处置； 3） 对安全事件建立复盘机制并形成知识库。	1） 有持续反馈的流程、规范与组织，包括但不限于：安全问题收集、分类分级、反馈、跟踪等机制； 2） 持续反馈的安全问题能够自动化反馈到问题跟踪管理系统，并且实现闭环管理； 3） 有周期性的安全报告总结机制，如：安全漏洞的处理报告等。
3	1） 同上，且需达到以下要求：	1） 运营过程具备全面的安全管理制度体系，包括但不限于安	1） 同上，且需要达到以下要求：	1） 有完善的持续反馈的流程、规范、组织与平台，包括但不

	2） 具有完善的安全监控指标并可视化展示，包括但不限于：分类型和级别的安全事件数、安全攻击类型、攻击来源、攻击次数等； 3） 具有安全监控平台，能够可视化展示应用运行状态，包括：收集、分析运行数据，发现潜在安全缺陷，并进行分级告警； 4） 具有集中、统一的管理平台实现监控关联分析。	全策略、安全管理制度、安全操作规程等； 2） 对于自动化运维工具进行安全加固并具备自动化监控机制，及时发现工具的操作安全风险； 3） 具备自动化安全审计机制，对权限管理制度和操作流程等进行合规审查及风险控制； 4） 具备自动化运营日志分析系统，对于运营过程中日志进行自动化分析，发现安全风险并告警； 5） 针对应用及组件信息建立专门的漏洞和情报监测渠道，对线上应用的运行环境、系统服务、使用框架及三方组件等进行预警、处置与闭环，并有标准的流程与规范； 6） 具备从外部接收相关漏洞通告和情报的渠道，并有完整的运营机制。	2） 有专门的安全事件管理平台，能够对安全事件进行跟踪、统计、分析、可视化展示等； 3） 具备安全应急响应职能团队，跟进安全应急响应与处置，设立不同的应急角色； 4） 具备完善的应急体系，包括但不限于：定期开展应急演练计划、安全应急预案、启动条件、应急组织、应急策略、应急资源、恢复机制等； 5） 建立安全应急响应度量机制，对响应团队响应效能等作出要求，驱动团队改进优化。	限于：安全问题收集、分类分级、反馈、跟踪、处理、汇总分析等机制； 2） 持续反馈平台具有一定的自动化能力，如：情报收集、发现处置、事件升级、持续监测、预警通知等； 3） 持续反馈安全问题汇总分析结果，如：安全漏洞的处理报告、自动化系统的汇总分析结果等。

4	1） 同上，且需达到以下要求： 2） 监控服务的安全指标覆盖全部业务场景和基础运营环境，如：容器化环境等； 3） 安全监控平台能够针对业务场景有专项监控，如：超时场景的监控、Web 欺诈、垃圾注册等； 4） 安全监控平台具备全面自动化能力，及一定的智能化能力，能实现应用软件资产的安全画像，如：秘钥、配置、证书、组件等； 5） 应用系统自身能够主动识别潜在的威胁并进行自动化控制，如：采用 RASP 技术等。	1） 同上，且需达到以下要求： 2） 具备运营过程的自动化安全验证联动机制，如：端口变更自动触发自动化安全漏洞扫描等； 3） 具备安全分析平台，可对应用运行时监控的各项数据进行自动化关联分析、统计、展示等； 4） 具备持续的安全漏洞外部反馈机制，如：漏洞赏金运营机制等； 5） 对于多种渠道的漏洞与情报预警监测进行自动化的管理，包括受影响资产排查、通知相关责任人进行修复、修复后的验证、展示、统计等功能； 6） 具备线上应用漏洞发现与自动化修复机制，如：通过安全基线核查发现漏洞、自动化推送补丁进行修复等。	1） 同上，且需要达到以下要求： 2） 定期开展实战化安全演练，验证保障预案的有效性，提升响应效率； 3） 应急响应具备一定的智能化，可实现智能化安全风险与事件预测，自动化告警，自动化止损等。	1） 同上，且需达到以下要求： 2） 持续反馈平台具备自动化能力，包括但不限于：情报收集、发现处置、统计分析、事件升级、持续监测、预警通知、可视化等； 3） 对运营过程中收集的安全情报进行自动化分析并反馈，实现整个研发运营过程安全的持续优化； 4） 对国家、行业、组织的安全态势感知时效性高，具有智能化的安全态势感知平台，如：自动匹配收集规则等。
5	1） 同上，且需达到以下要求： 2） 实现安全监控服务全面智能化，如：对业务场景有自学习能力，能够识别未知	1） 同上，且需达到以下要求： 2） 具备智能化运营安全风险管控平台，智能化感知变更管理、配置管理、运维工具失控等带来的潜	1） 同上，且需要达到以下要求： 2） 应急响应实现全面的智能化，如：无人干预止损等。	1） 同上，且需达到以下要求： 2） 自动化和智能化的情报验证、问题修复验证、安全趋势预测与关联分析；

	威胁及攻击。	在安全风险，进行智能化处置。		3） 具备安全问题的智能化分析及反馈能力，实现整个研发运营过程安全的自动优化。