ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国　　行 业 标 准

XX/T XXXXX—XXXX

研发运营一体化（DevOps）能力成熟度模型 第 6 部分 安全风险管理

点击此处添加标准英文译名 The Capability Maturity Model of DevOps

Part 1 ： Security Risk Management

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－X

发 布

目　　次

前言 II

1 范围 1
2 规范性引用文件 1
3 术语 1
4 概述 1
5 控制研发运营一体化总体风险 2
6 研发运营一体化控制开发过程风险 3
7 研发运营一体化控制交付过程风险 4
8 控制研发运营一体化技术运营过程的安全风险 5

参考文献 1

前　言

研发运营一体化是指在IT软件及相关服务的研发及交付过程中，将应用的需求、开发、测试、部署和运营统一起来，基于整个组织的协作和应用架构的优化，实现敏捷开发、持续交付和应用运营的无缝集成。帮助企业提升IT效能，在保证稳定的同时，快速交付高质量的软件及服务，灵活应对快速变化的业务需求和市场环境。

本标准是“研发运营一体化（DevOps）能力成熟度模型”系列标准的第 6 部分 安全风险管理，该系列标准的结构和名称如下:

第1部分：总体架构

第2部分：敏捷开发管理

第3部分：持续交付

第4部分：技术运营

第5部分：应用设计

第6部分：安全风险管理

第7部分：组织结构

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、 DevOps时代社区、高效运维社区

本标准主要起草人：韩方、赵锐、公丽丽、李滨、毛茂德、王广清、郭雪、侯大鹏、陈雪秀、 王永霞、叶林、周麟

研发运营一体化（DevOps）能力成熟度模型 第6部分：安全风险管理

1 范围

本标规定了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。

本标准适用于具备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 32400-2015 信息技术 云计算 概览与词汇

[2] GB/T 32399-2016 信息技术 云计算 参考架构

[3] 银监发〔2016〕44号 银行业金融机构全面风险管理指引

3 术语

下列术语和定义适用于本文件。

3.1 研发运营一体化 DevOps

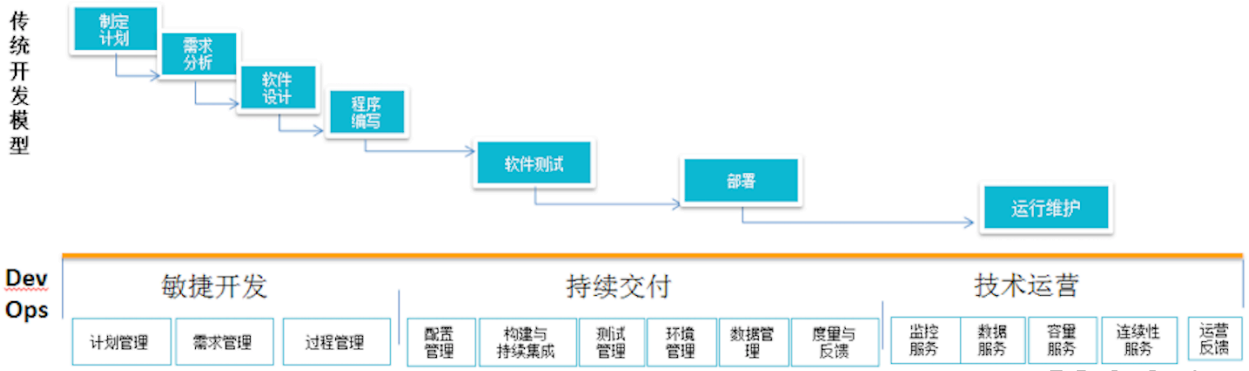
指在IT软件及相关服务的研发及交付过程中，将应用的需求、开发、测试、部署和运营统一起来，基于整个组织的协作和应用架构的优化，实现敏捷开发、持续交付和应用运营的无缝集成。

3.2 OWASP TOP 10 The Open Web Application Security Project TOP 10

中文全称开放Web应用程序安全项目，Top 10的首要目的是教导开发人员、设计人员、架构师、经理和企业组织，让他们认识到最严重Web应用程。

4 概述

本标规定了 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，相比于传统开发模型开发流程发生变化，如图一所示。



在 DevOps 开发模式下，安全将贯穿整个流程，每个参与人都是安全责任人，要保障 IT 软件或服务安全开发运行，需要对特定风险进行管理，包括控制安全责任人变更风险、控制人员协作风险、控制自动化工具风险、控制自动化平台风险、第三方合作风险等，同时对开发、交付、运营过程进行安全风险管理。

5 研发运营一体化控制总体风险

在 DevOps 开发模式下，开发、测试、运营人员责任发生变化，同时引入自动化工具，需要综合考虑人员、自动化工具、内部共享代码、外部第三方合作的安全风险管理。

级别	人员管理	自动化工具管理	共享代码管理	第三方合作管理
1	无统一的人员管理	不涉及自动化工具管理	无共享代码管理	无第三方合作管理
2	明确每个人的权利和权限； 降低对于职责分离的依赖度； 明确不同团队协作流程和规范。	监测自动化工具运行状态，提前制定应急预案，保证自动化工具可用性	需要对第三方库文件或代码进行安全风险评估，安全策略应用到共享代码或共享服务过程中；	控制第三方软件接入风险；
3	明确每个人的权利和权限； 设立信息安全管理的职能部门 明确不同团队协作流程和规范。 加强各管理人员之间、不同团队之间的沟通交流，定期或不定期召开会议，共同协作处理关键问题； 开发人员、测试人员和运营测试人员分离。	同上	同上	同上
4	明确每个人的权利和	监测自动化工具运行	同上	控制第三方人员操作

	权限； 设立信息安全管理的职能部门，配备安全主管； 明确不同团队协作流程和规范。 加强各管理人员之间、不同团队之间的沟通交流，定期或不定期召开会议，共同协作处理关键问题。 开发人员、测试人员和运营测试人员分离。	状态，提前制定应急预案，保证自动化工具可用性； 对自动化平台进行分级认证、分级授权。		风险；控制第三方软件接入风险。
5	明确每个人的权利和权限； 设立信息安全管理的职能部门，配备安全主管； 安全责任人的认命、安全管理制度的制定，必要时应征求国家指定部门或机构的意见； 明确不同团队协作流程和规范； 加强各管理人员之间、不同团队之间的沟通交流，定期或不定期召开会议，共同协作处理关键问题； 开发人员和、测试人员和运营人员分离。	同上	需要对第三方库文件或代码进行安全风险评估，安全策略应用到共享代码或共享服务过程中； 共享库或代码管理应该进行安全策略控制和评估。	控制第三方人员操作风险；控制第三方软件接入风险；控制第三方合作数据安全风险，保证数据主体权利，控制处理过程合规。

6 研发运营一体化控制开发过程风险

为降低后续交付、运营中的安全风险，保障研发运营一体化的整体安全，必须提前实施安全风险管理工作。在制定计划的每个步骤时纳入安全风险管理，确定整体的安全风险需求，并在过程中实施安全风险管理。通过自动化、智能化的方式实现，这是研发运营一体化的基础。

级别	计划管理	需求管理	过程管理
1	计划管理中无安全内容	无安全需求	无安全的过程管理

2	将安全纳入测试计划	有安全需求	过程中每位成员均参与安全过程
3	将安全纳入质量、测试计划	在需求收集、需求分析、需求与用例、需求验收四部分均实现安全，根据根据业务逻辑和已知风险，确定安全需求，包括基础平台、开源工具、编码安全。	过程中每位成员均参与安全过程,产品每次迭代中按照安全线性过程进行管控
4	将安全纳入开发、质量、测试计划	在需求收集、需求分析、需求与用例、需求验收四部分均实现安全，根据根据业务逻辑和已知风险，确定安全需求，包括基础平台、开源工具、编码安全、接口服务安全。	过程中每位成员均参与安全过程,产品每次迭代中按照安全线性过程进行管控,并将这些安全过程进行可视化
5	将安全纳入整体计划，在需求、设计、开发、测试所有阶段	在需求收集、需求分析、需求与用例、需求验收四部分均实现安全，根据根据业务逻辑和已知风险，确定安全需求，包括基础平台、开源工具、编码安全、接口服务安全、业务安全、整体架构安全。	过程中每位成员均参与安全过程,产品每次迭代中按照完整的安全生命周期过程进行管控,并将这些安全过程进行可视化

7 研发运营一体化控制交付过程风险

在系统整个生命周期中，安全交付是实现安全运营的前提条件。在智能化、自动化地实现配置管理、环境管理、测试管理、数据管理的过程中，纳入安全风险管理，通过反馈和度量不断发现、评估、处置安全风险问题，让系统、产品、服务在最佳状态下交付。

级别	配置管理	环境管理	测试管理	数据管理	度量与反馈
1	配置管理中不涉及安全 制定交付清单,根据清单进行清点。	无安全环境管理	无安全测试	无数据安全	无安全的度量与反馈
2	对源代码进行安全管理	区分生产、非生产环境，并对基础环境进行加固	使用符合OWASPTOP10等最佳实践的安全测试或静态代码扫描工具进行安全测试和合规扫描。	非生产环境中没有未清洗的敏感数据	在持续交付各个阶段定义安全度量指标，报告并跟踪在测试或其他过程中发现的安问题
3	对源代码、配置库进行安全管理	区分生产、非生产环境，两个环境中的安全基线一致	使用符合OWASPTOP10等最佳实践的安全测试或静态代码扫描工具进行安全测试和合规扫描，	非生产环境中没有未清洗的敏感数据，上线系统中没有开发、测试数据	在持续交付各个阶段定义安全度量指标，报告并跟踪在测试或其他过程中发现的安

			具备业务发布上线自动化安全评估和扫描能力，并补充有手工安全测试		问题，将这些内容通过可视化的方式进行管理
4	对源代码、配置库、变更过程进行自动化的安全管理	区分生产、非生产环境，非生产环境中没有未清洗的敏感数据，两个环境中的安全防护方式一致	使用符合OWASPTOP10 等最佳实践的安全测试或静态代码扫描工具进行安全测试和合规扫描，具备业务发布上线自动化安全评估和扫描能力，并补充有手工安全测试，将测试结果可视化	非生产环境中没有未清洗的敏感数据，上线系统中没有开发、测试数据，非生产环境中的数据按数据安全生命周期进行管理	同上
5	同上	区分生产、非生产环境，非生产环境中没有未清洗的敏感数据，两个环境中的安全管控一致	使用符合OWASPTOP10 等最佳实践的安全测试或静态代码扫描工具进行安全测试和合规扫描，具备业务发布上线自动化安全评估和扫描能力，并补充有手工安全测试，将测试结果可视化并与前后过程进行自动关联	自动生成非生产环境中的使用数据，上线系统中没有开发、测试数据，非生产环境中的数据按数据安全生命周期进行管理	同上

8 研发运营一体化控制技术运营过程的安全风险

在技术运营过程中对监控服务、数据服务和运营反馈三部分的安全风险管理不可或缺，监控服务中应该考虑到对于安全风险的监控能力，以及自动化和智能安全能力监控融入到整体监控服务中，数据服务尤其是涉及到用户数据和敏感数据相关的安全要求显得尤为重要，以及在整个数据生命周期的安全要求，运营反馈是指有针对性的对安全问题的融合。

级别	监控服务	数据服务	运营反馈
1	监控服务中无集成安全监控	数据服务没有考虑安全要求；	无安全问题反馈机制
2	具有基本的安全监控，	数据服务符合当地法	反馈的安全问题

	能够覆盖部分业务场景；	律法规要求；数据服务具有明确的安全要求并能够形成指导规范，覆盖部分数据生命周期，以及部分业务场景；数据具有明确的分级管理办法和相关密级管理规定；具有数据安全事件预警能力；	能够同业务问题统一跟踪状态；
3	具有完善的安全监控指标；具有自动化安全监控体系；	数据安全要求覆盖整个数据生命周期，包括数据采集，传输，存储，使用，分享和销毁等场景安全要求，数据服务安全要求覆盖全部业务场景；数据使用具有完善的审批和审计机制；	能够制定详细的安全问题等级和跟进流程并执行；自动化整合到问题跟踪管理流程中。
4	监控服务的安全指标覆盖全部业务场景和基础运营环境；并能够形成安全自动化监控服务体系；	数据服务能够自动化服务化统一安全技术框架，包括但不限于加解密、秘钥管理和脱敏等统一数据安全服务框架；	安全问题的反馈和处理机制和流程能够持续的优化；
5	安全监控服务智能化	数据流向可视化管理；智能预测数据安全风险和事件；	具有反馈安全问题智能分级分类机制；

参 考 文 献

1. John, Willis, Patrick, Debois, Jez, Humble, Gene, Kim. The DevOps Handbook[M]. 美国:IT Revolution Press, 2016-10.
2. Neil, MacDonald, Ian, Head. DevSecOps: How to Seamlessly Integrate Security Into DevOps[EB/OL]. https://www.gartner.com/doc/3463417/devsecops-seamlessly-integrate-security-devops, 2016-9.
3. Mark, Horvath, Neil, MacDonald, Ayal, Tirosh. Integrating Security Into the DevSecOps Toolchain[EB/OL]. https://www.gartner.com/doc/3463417/devsecops-seamlessly-integrate-security-devops, 2017-11.