2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

DevSecOps标准解读

中国信通院云大所 牛晓玲

牛晓玲

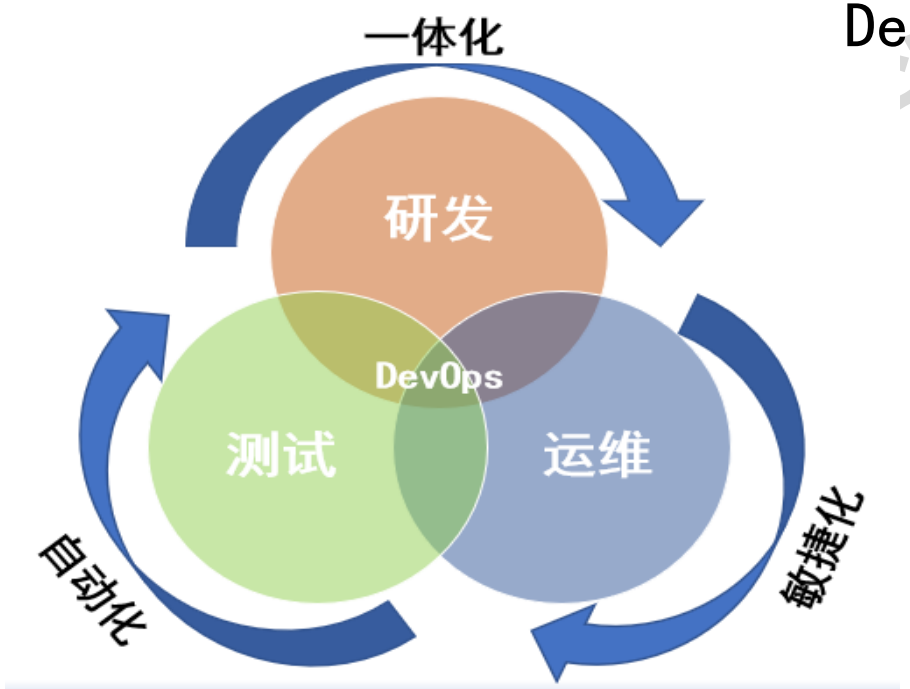
中国信息通信研究院
云计算与大数据研究所 云计算部 副主任

DevOps标准工作组组长，DevOps 国际标准编辑人。长期从事云计算领域开发运维研究的相关工作，包括云服务业务功能测试以及运维管理系统审查等相关工作。参与编写《云计算服务协议参考框架》、《对象存储》、《云数据库》、《研发运营一体化（DevOps）能力成熟度模型》系列标准、《云计算运维智能化通用评估方法》等多项标准20余项。参与多篇白皮书、调查报告等编制工作，包括《企业IT运维发展白皮书》、《中国DevOps现状调查报告（2019年）》等。参与评估DevOps能力成熟度评估超过40个项目，具有丰富的标准编制及评估测试经验。

什么是DevSecOps？

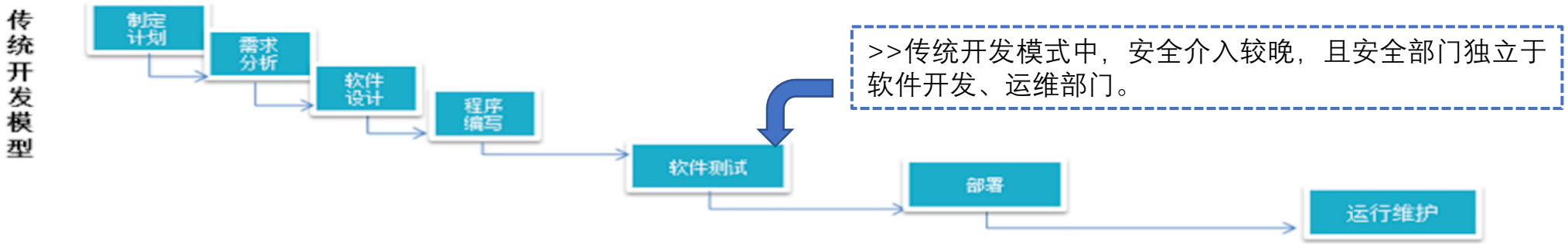
概念

- DevOps的定义：“开发（Dev）”和“运维（Ops）”的缩写，是一组**过程、方法**与**系统**的统称，强调业务人员及IT专业人员（开发、测试、运维等）在应用和服务生命周期中的协作和沟通；强调整个组织的**合作**以及**交付**和**基础设施变更**的自动化，从而实现持续集成、持续部署和持续交付等的无缝集成。
- DevSecOps的定义：是将信息安全的框架整合到DevOps的工作流程中，**研发、运营、测试、安全**多个部门紧密协作，在提升开发和运营敏捷性的同时，也保障了**数据和服务的可用性与安全性**。



DevSecOps概念示意图

DevSecOps的由来



2012 2017 2017-至今

2012年

Gartner的报告中首次提出了“DevOpsSec”这个概念

2017年

在RSA年度大会上“DevSecOps”成为了热门词汇，它是一种对DevOps的延展，DevSecOps提出安全是每个人的责任。

至今

DevOps的落地实践带动了DevSecOps的兴起，强调将信息安全的能力整合到DevOps的工作流程中，各部门重视安全，提升开发和运营敏捷性。

关于DevSecOps的几点理解？

❌ 部署应用程序的能力在规模和速度上都得到了改善，但安全方面的考虑却常常被忽略，更倾向于快速满足业务需求。
❌ 依靠应用程序来保持操作运行，开发过程中的安全性是上线的最后阶段执行，应用程序安全性必须加快以跟上软件开发的步伐。

Yes

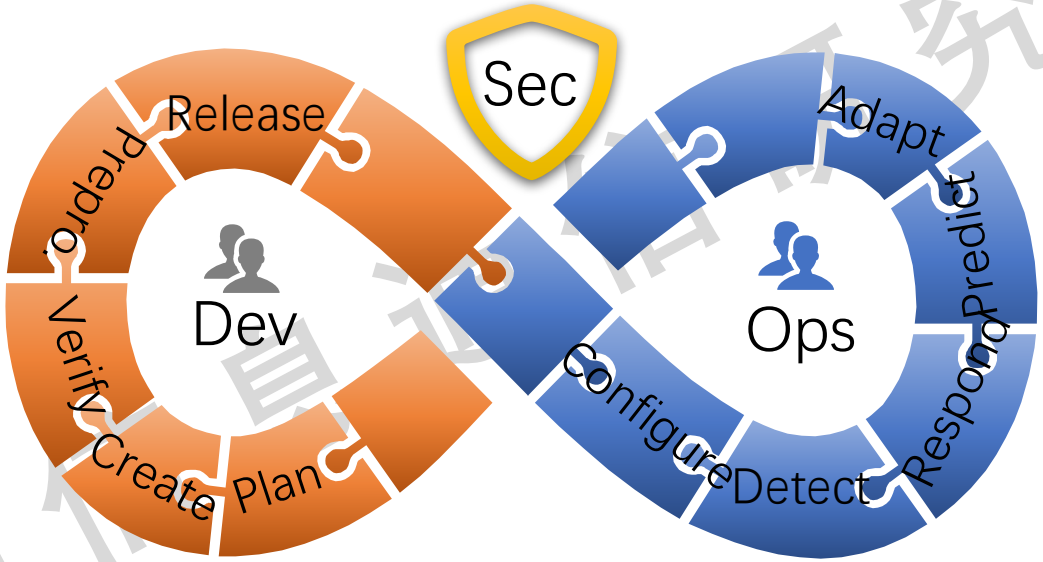
- 是一种安全的文化的渗透
- 是制度流程和工具的集合
- 是将安全性和合规性纳入软件全生命周期的方法
- 是由学习和实践驱动的战略

No

- 不是一种一刀切的全能方法
- 不是单一工具或方法
- 不单是在持续交付中增加安全性的手段
- 不是追求完美与合规的战略

DevSecOps生命周期

DevSecOps的主要特征是通过在**软件生命周期**的各个阶段进行自动化，监控和应用安全性来提高客户成果和使命价值，包括计划，开发，构建，测试，发布，交付，部署，操作和监控等阶段。



计划阶段

定义研发安全指标，进行威胁建模，安全工具培训等

编码阶段

IDE安全插件方式实现

验证（测试）阶段

在软件开发阶段消除这些漏洞可以降低企业的信息安全风险，包括SAST/DAST/IAST,SCA

准生产环境

混沌工程、模糊测试和集成测试

发布阶段

软件签名，传输等过程中防篡改

优化 阶段

解决安全技术债、事件响应、纵深防御体系等不断适配、调整和优化

配置阶段

签名验证、完整性校验和纵深防御

检测阶段

RASP、UEBA、网络监控和渗透测试

响应阶段

安全编排，基于RASP / WAF的安全防护、混淆

预测阶段

相关的脆弱性分析 、IOC情报、STIX、TAXII

标准背景说明

- 牵头单位：工信部 中国信息通信研究院（国家智库，可信云等出品单位）
- 起草单位：中国信息通信研究院、云计算开源产业联盟 、DevOps时代社区、高效运维社区、BATJ、中国银行、招商银行、平安科技、中国移动、中国联通和华为等
- 目前进展：工信部和联合国 ITU-T 立项在研，2018年6月29日发布全量征求意见稿

研发运营一体化（DevOps）能力成熟度模型

能力类	一、研发运营一体化（DevOps）过程															
能力域	敏捷开发管理 (标准2)			持续交付 (标准3)							技术运营 (标准4)						
能力子域	价值交付管理	敏捷过程管理	敏捷组织模式	配置管理	构建与持续集成	测试管理	部署与发布管理	环境管理	数据管理	度量与反馈	监控管理	事件与变更管理	配置管理	容量与成本管理	高可用管理	连续性管理	用户体验管理
能力项	需求工件	价值流	敏捷角色	版本控制	构建实践	测试分层策略	部署与发布模式	环境管理	测试数据管理	度量指标	监控采集	事件管理	运营配置管理	容量管理	应用高可用管理	风险管理	业务认知管理
	需求活动	仪式活动	团队结构	变更管理	持续集成	代码质量管理	持续部署流水线		数据变更管理	度量驱动改进	数据管理	变更管理		成本管理	数据高可用管理	危机管理	体验管理
						自动化测试					数据应用					应急管理	

能力类	二、研发运营一体化（DevOps）应用设计 (标准5)
能力类	三、研发运营一体化（DevOps）安全及风险管理 (标准6)
能力类	四、研发运营一体化（DevOps）评估方法 (标准7)
能力类	五、研发运营一体化（DevOps）系统和工具 (标准8)

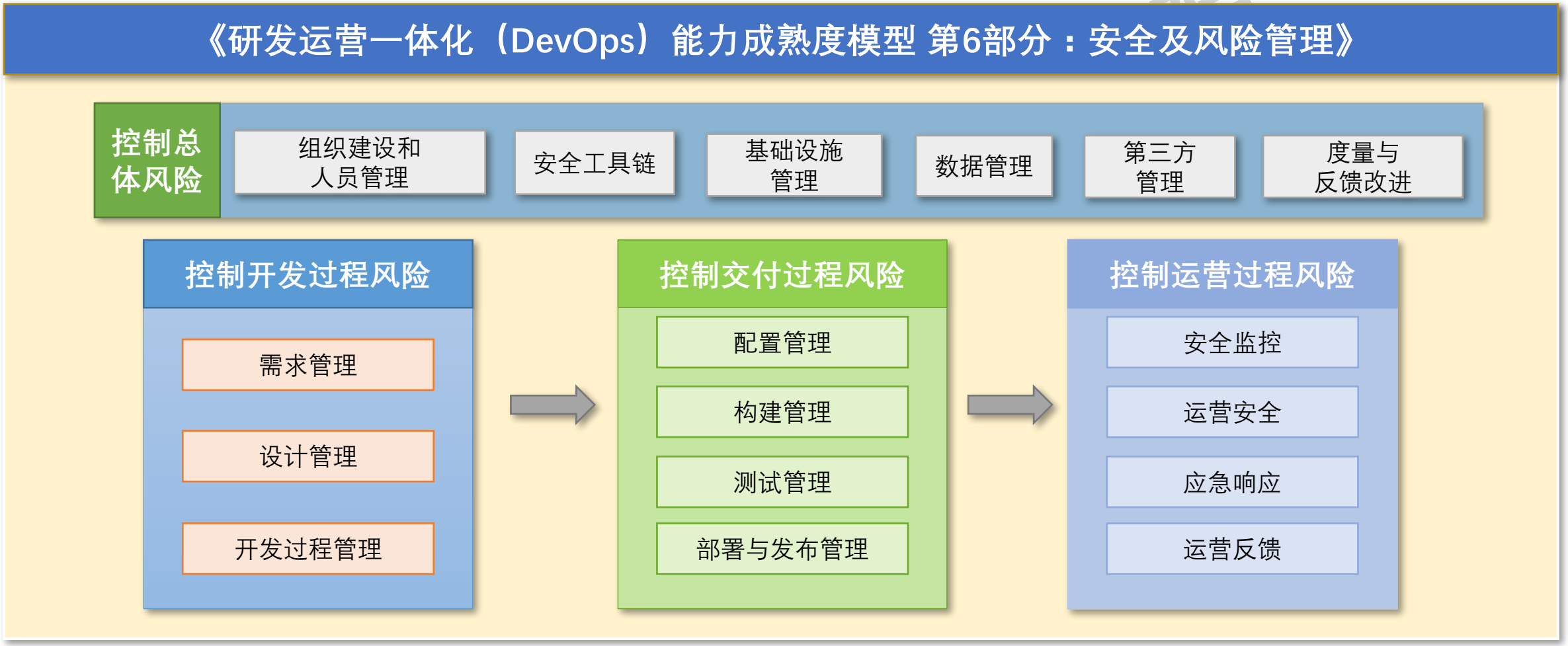
安全风险管理标准

整体级别说明

级别	名称	级别特点
1级	初始级	初始状态
2级	基础级	安全风险管理具备简单的规范及工具化实现方式
3级	全面级	安全风险管理自动化、规范化
4级	优秀级	安全风险管理平台化、服务化、可视化，实现度量驱动改进
5级	卓越级	安全风险管理高度智能化、数据化、社会化

安全及风险管理标准框架

《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》标准是一种全新的安全理念与模式，强调安全是每个人的责任，指将安全内嵌到应用的全生命周期，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，框架划分依据DevOps全生命周期分为：控制总体风险、控制开发过程风险、控制交付过程风险和控制运营过程风险四大部分。



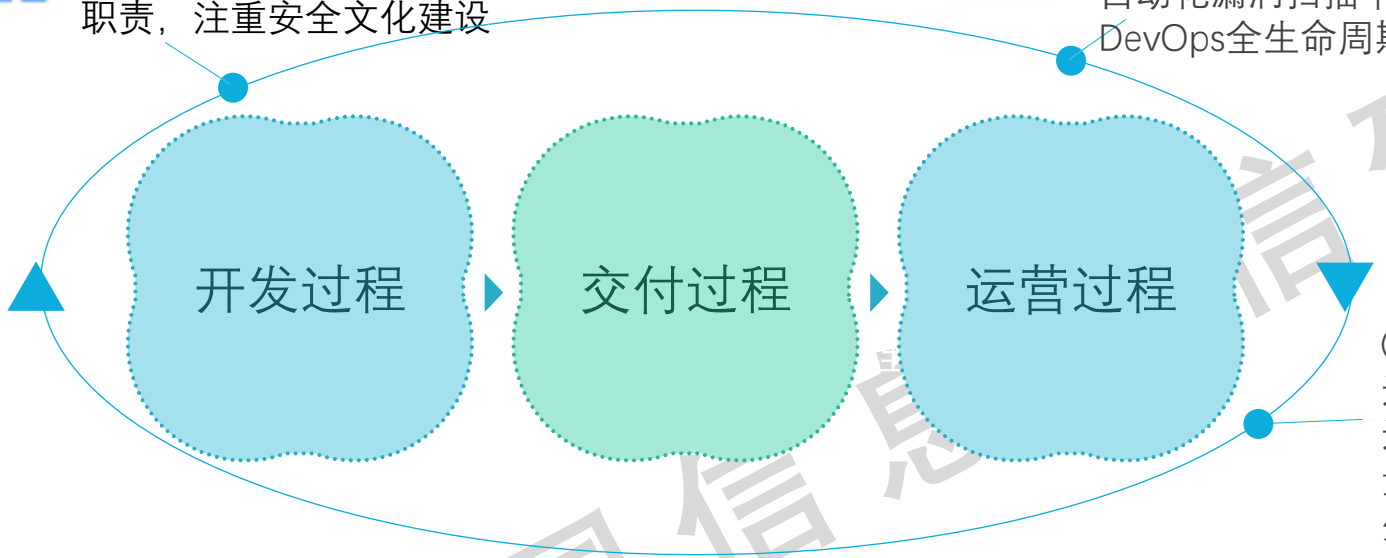
人人为安全负责 · 安全左移 · 全流程的安全内建 · 安全闭环

控制总体风险

控制总体风险：在DevOps模式下，安全内建于开发、交付、运营过程中，总体风险包括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。

①**组织建设与人员管理**：在DevSecOps全过程中，建立对应的组织负责不同的安全职责，注重安全文化建设

②**安全工具链**：要求安全左移，将漏洞扫描、应用安全测试、开源合规、威胁建模、自动化漏洞扫描平台等安全工具嵌入DevOps全生命周期



⑥**度量与反馈改进**：通过对研发、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

③**基础设施管理**：要求基础设施在DevOps全生命周期中，提供安全、可靠、稳定、可持续的基础环境以及支撑服务的平台

⑤**数据管理**：在DevOps过程中对涉及的各类数据进行安全管理，利用制度、流程及工具化等手段保障数据的安全性

合作/接入的安全风险控制

④**第三方管理**

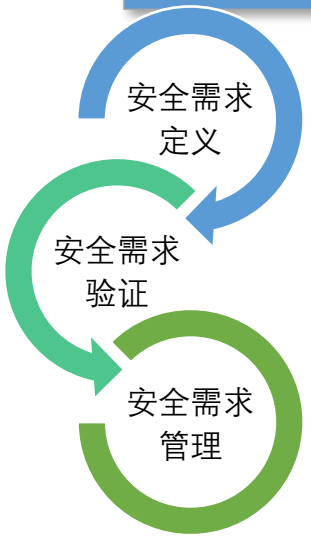
- 第三方机构
- 第三方人员
- 第三方软件
- 第三方服务

控制开发过程风险

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。在应用的需求阶段就进行安全风险控制，同时关注架构与设计的安全风险，并在开发过程中实施安全风险管理。

需求管理

将安全工作左移，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。



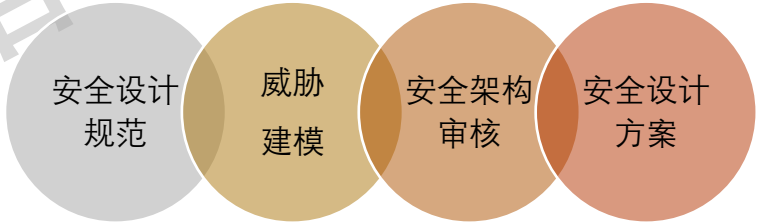
安全需求包括：应用的安全功能和功能的安全性两方面。

对**安全需求测试用例**的编写、验证与管理，提出相关要求。

安全需求基线>>持续更新的安全需求标准库与管理平台>>自动化、智能化的需求管理平台

设计管理

关注开发过程中架构与设计的安全风险。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，制定措施消减威胁、规避风险，确保产品的安全性。



开发过程管理

关注编码过程的安全管理，以安全编码方式实现功能。

01 安全编码

02 源代码安全检测

03 开源组件安全风险与合规检测

控制交付过程风险

控制交付过程风险：安全交付是将安全内建到交付过程中，是实现安全运营的前提条件。通过将配置管理、构建管理、测试管理及部署与发布管理等交付过程纳入安全风险管理，使得系统、产品、服务可以在安全完整的最佳状态下交付。

是保障交付过程正确性的前提，主要包括对源代码及相关脚本、依赖组件、发布制品、应用配置、环境配置等的安全管理。

在应用发布前，通过安全测试发现并排除应用的安全缺陷，提高安全质量。

- 安全流程与规范
- 安全质量门限
- 安全控制方式嵌入DevOps流水线
- 低风险发布机制

配置管理

- A 代码评审
- B 代码保护机制
- C 防篡改机制
- D 软件资产安全风险库

构建管理

安全的构建管理可提升应用的发布制品安全性，可靠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。

测试管理

01 黑盒安全测试
02 静态代码安全扫描
03 开源组件安全扫描
04 容器安全扫描
05 ……

部署与发布管理

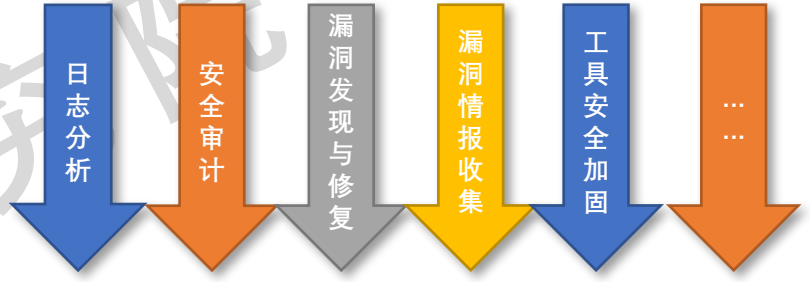
安全的部署与发布关注安全的流程与规范、过程中的安全控制与低风险的发布机制。

控制运营过程风险

控制运营过程风险：关注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过程中安全风险的闭环管理，包括：安全监控、运营安全、应急响应和运营反馈。

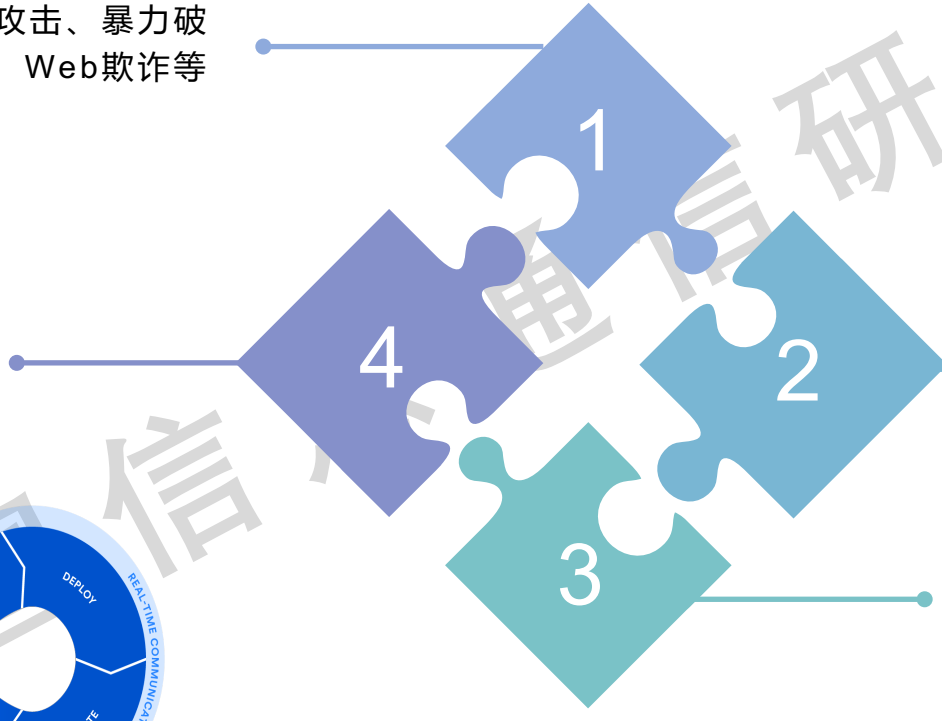
安全监控

对运营过程中的安全进行监控，覆盖业务场景与基础运营环境，如：病毒攻击、DDos攻击、暴力破解、注入攻击、接口滥用、Web欺诈等



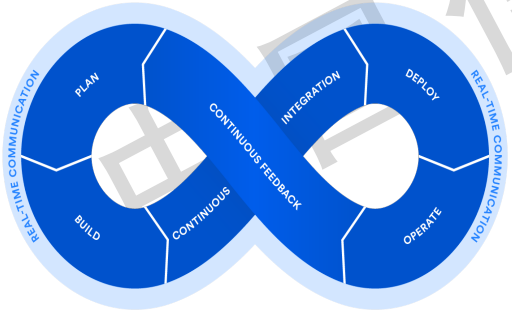
运营安全

应用在运营过程中实施安全控制，识别、评估漏洞与缺陷，并降低或消除风险。也包括对运营过程中配置管理、变更管理等的安全管理。



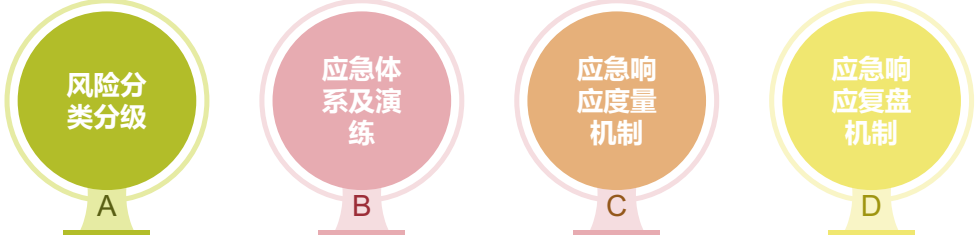
运营反馈

关注运营过程中安全的**动态性、持续性和整体性**，通过对安全漏洞、缺陷、事件等的分析与反馈，实现从运营到开发过程的DevSecOps**闭环管理**。



应急响应

针对运营过程中的安全事件、风险进行响应、跟踪和处置，及时降低风险和影响，保障业务连续性。



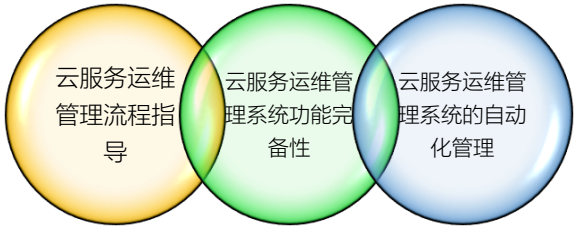
中国信通院关于开发运维相关工作

云计算运维工作组

开发运维类行业标准制定 → 交流研讨、输出软科研成果 → 标准推广 → 标准符合性验证和评测

云运维标准

《可信云服务专项评估 第1部分 面向云服务提供商的运维管理指南》



《研发运营一体化（DevOps）能力成熟度模型》系列标准

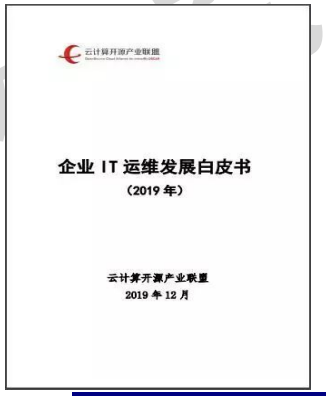
-= 研发运营一体化（DevOps）能力成熟度模型 =-

能力类	一、研发运营一体化（DevOps）过程															
能力域	敏捷开发管理			持续交付						技术运营						
能力子域	价值交付管理	敏捷过程管理	敏捷组织模式	配置管理	构建与持续集成	测试管理	部署与发布管理	环境管理	数据管理	度量与反馈	监控管理	事件与变更管理	配置管理	容量与成本管理	高可用管理	连续性管理	用户体验管理
能力项	需求工件	价值流	敏捷角色	版本控制	构建实践	测试分层策略	部署与发布模式	环境管理	测试数据管理	度量指标	数据采集	事件管理	运营配置管理	容量管理	应用高可用管理	风险管理	业务认知管理
	需求活动	仪式活动	团队结构	变更管理	持续集成	代码质量管理	持续部署流水线		数据变更管理	度量驱动改进	数据管理	变更管理		成本管理	数据高可用管理	危机管理	体验管理
						自动化测试					数据应用					应急管理	
能力类	二、研发运营一体化（DevOps）应用设计																
能力类	三、研发运营一体化（DevOps）安全及风险管理																
能力类	四、研发运营一体化（DevOps）评估方法																
能力类	五、研发运营一体化（DevOps）系统和工具																

正在研制中的标准

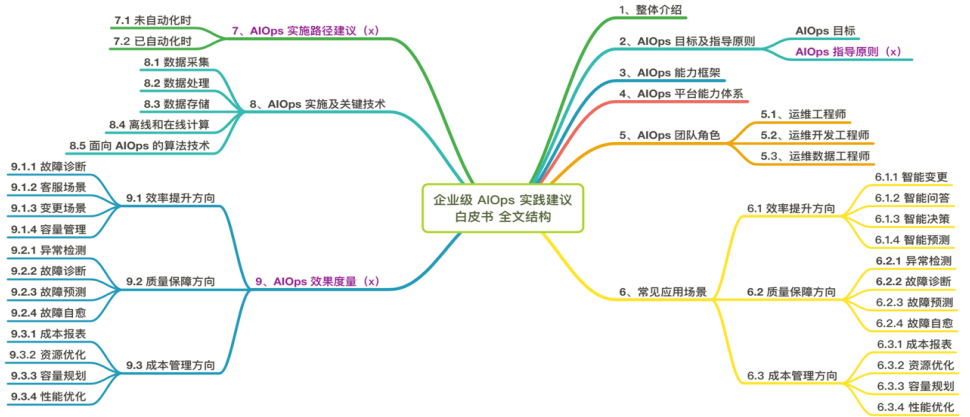
运维研究成果

《企业IT运维发展白皮书（2019年）》



《中国DevOps现状调查报告（2019年）》

《企业级 AIOps 实施建议白皮书》



《研发运营一体化能力成熟度模型》评测与推广

重磅！ 2020年DevOps 标准持续交付和技术运营评估报名正式...

MONDAY, MARCH 9, 2020

DevOps从概念的提出到落地实践，发展异常迅猛，它促进开发、运维、测试等不同部门之间的沟通、协作与整合，为各个实施的组织带来可观收益的同时，也一直在塑造着整个软件世界，DevOps已经成为软件开发和IT运营的主流趋势...

持续交付

中国工商银行 INDUSTRIAL AND COMMERCIAL BANK OF CHINA
中国银行 BANK OF CHINA
招商银行 CHINA MERCHANTS BANK
中信银行 CHINA CITIC BANK
郑州银行 BANK OF ZHENGZHOU
去哪儿 Qunar.Com 聪明你的旅行
华泰证券 HUATAI SECURITIES
Tencent 腾讯
中国移动 China Mobile 浙江公司 广东公司 北京公司
中国电信 CHINA TELECOM 江苏公司
Ultrapower 神州泰岳

技术运营

华泰证券 HUATAI SECURITIES
中国移动 China Mobile 北京公司

企业级DevOps赋能（共促）计划


企业级 DevOps 赋能（共促）计划
Enterprise DevOps Promoting Program , EDOPP
合作单位
Partnership
中国工商银行软件开发中心
Industrial and Commercial Bank of China Software Development Centre
为促进国内外企业技术交流，快速实现组织级 DevOps，高效打造业界领先的 DevOps 平台，使得 DevOps 彰显业务价值，云计算开源产业联盟与开放运维联盟联合发起此计划。
In order to promote the technical communication among enterprises domestically and internationally, realizing organization-level DevOps quickly, building industry-leading DevOps platform efficiently, demonstrating the value of DevOps in business , The OpenSource Cloud Alliance for Industry (OSCAR) and the Open OPS Alliance (OOPSA) initiate the Enterprise DevOps Promoting Program (EDOPP) .
编号：EDOPP-001
Partnership No.
颁发日期：2019-04-12
Date of Issue
截止日期：2021-04-12
End of Issue
云计算开源产业联盟 OpenSource Cloud Alliance for IndustRy,OSCAR
开放运维联盟 OOPSA Open OPS Alliance
云计算开源产业联盟由中国信息通信研究院发起，联合多家云计算开源技术公司成立，开发运维联盟是中国第一个运维行业协会，汇聚超多企业运维专家。
The OpenSource Cloud Alliance for Industry was initiated by the China Academy of Information and Communications Technology with numerous cloud computing open source technology companies. OOPSA is the first IT operations association in China, assembles operations experts from numerous enterprises.

联系我们

刘老师

- 电话：15650786171
- 邮箱：liukailing@caict.ac.cn


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音