



团 体 标 准

T/CIE 186—2023

业务研发安全运营一体化能力成熟度模型

BizDevSecOps capability maturity model

2023-08-03 发布

2023-08-03 实施

中国电子学会 发布
中国标准出版社 出版

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 总体架构及级别划分	6
5 持续规划	8
6 持续设计	10
7 持续测试	13
8 持续集成	15
9 持续部署	18
10 持续安全	20
参考文献	23

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。

本文件由中国电子学会提出并归口。

本文件起草单位：北京易科绅国际信息科技有限公司、思特沃克软件技术(北京)有限公司、中国电子学会、埃森哲(中国)有限公司、华为云计算技术有限公司、中兴通讯股份有限公司、联想(北京)有限公司、中国国际金融股份有限公司、凯捷咨询(中国)有限公司、广州嘉为科技有限公司、华中科技大学、腾讯云计算(北京)有限责任公司、京东科技信息技术有限公司、恒生电子股份有限公司、优维科技(深圳)有限公司、北京光环国际教育科技股份有限公司、励德爱思唯尔信息技术(北京)有限公司上海分公司、福建理工大学。

本文件主要起草人：肖然、谢保龙、张霖、张海云、周纪海、曹学勤、陈崇发、黎明、杨璐、杜巍、闫林、徐毅、王娟、张玲、陈磊、郭瑞、杨浩、郑伟娜、李增和、蒋帆、李文乔、李之琳、邵双全、丁宁、杨信、刘劲辉、李聃、汪珺、万学凡、杜伟、王志民。

引言

数字化时代是软件改变世界的时代。如今任何一个行业中的任何一项业务都离不开软件平台的支撑。在确保业务价值的前提下,安全可靠地提升软件开发效能已经成为全球企业数字化时代的核心竞争力。BizDevSecOps 作为业务研发安全运营一体化的英文缩写,已经成为一个专有名词并在国际上得到广泛认可和接纳。

业务研发安全运营一体化是指在软件产品和服务的规划、设计、研发和交付过程中,通过优化整个组织在需求、开发、测试、部署、安全和运营等关键阶段的协作机制和实践,实现基于业务价值交付的全生命周期治理。

本文件在总结国际金融机构、科技组织及大量行业的实践和评估模型并充分研究和验证的基础上,结合国内企业特点进行了本土化适配,是汇聚国内外优秀实践总结的结果。

本文件可以从多个维度评估组织的业务研发安全运营一体化成熟度,主要包括工具支撑、价值流动、成效度量以及角色定位等。通过深入理解和应用这些成熟度标准,组织能够逐步提升研发效能,实现更快速、更高质量的软件交付,以及更紧密的业务研发与安全运营的协同业务。

研发安全运营一体化是一种重视“业务(Biz)”“软件开发(Dev)”“信息安全和数据隐私(Sec)”和“业务运营以及 IT 运维(Ops)”之间沟通合作的文化和方法实践,鼓励跨职能协作和持续学习改进。通过持续规划、持续设计、持续测试、持续集成、持续部署、持续安全等一系列的组织级能力的打造,透过“滚动规划”“持续交付”和“安全内建”等系列实践活动,构建面向未来、基于业务价值实现的软件开发体系。最终使数字化产品和服务能够更加快捷、频繁、高价值地迭代和可靠发展。

业务研发安全运营一体化可以帮助企业在数字化转型中提升软件开发效能、促进业务与技术融合。同时,在保证质量的前提下,实现高质量的软件产品和服务的快速交付,以及业务需求和市场环境变化的灵活应对。

业务研发安全运营一体化的理念基于国际数字化能力基金会(iFDC)发布的数字化转型与创新管理知识体系 VeriSM。VeriSM 的核心价值主张包括:

- 价值驱动(Value Driven):面向客户的端到端价值流;
- 持续演进(Evolving):持续优化流程、实践和架构;
- 及时响应(Responsive):快速适应业务和市场变化;
- 协调整合(Integrated):跨领域跨纬度的持续协调整合。

业务研发安全运营一体化能力成熟度模型

1 范围

本文件规定了业务研发安全运营一体化(BizDevSecOps)能力成熟度模型中的总体架构、级别划分,以及持续规划、持续设计、持续测试、持续集成、持续部署和持续安全。

本文件适用于各类组织开展 BizDevSecOps 能力成熟度模型建立及优化活动的评估、实施和改进。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

业务研发安全运营一体化 BizDevSecOps

用于促进业务、开发(应用程序/软件工程)、技术运营和质量保证(QA)部门之间的沟通、协作与整合的一组过程、方法与系统的统称。

3.1.2

持续集成 continuous integration

开发人员每天一次或者多次将代码集成到主干/集成分支上,每次集成都会通过自动化的流水线进行验证并发现集成的问题。

3.1.3

持续部署 continuous deployment

在软件版本控制过程中,通过自动化流程,快速、频繁地实现软件的构建和测试,并发布到生产环境中。

3.1.4

持续交付 continuous delivery

一种软件开发实践,目标是创建可以随时发布到生产环境的软件,在保证软件质量的同时,提高发布的频率和效率。

3.1.5

成效度量 effectiveness measurement

用于量化某个具体活动实际达成效用的方式或方法。

注:可以从定性或者定量的维度来对成效进行描述。

3.1.6

成效度量指标 effectiveness measurement indicator

用于量化某个具体活动实际达成效果的可量化指标。

注:该指标可以是定性的指标[例如:用户的 NPS(Net promoter score,净推荐值)],也可以是定量的指标(例如:千次点击转化率等)。