ICS 03.060
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0320—2024

证券基金经营机构运维自动化能力成熟度规范

Maturity specification for operation and maintenance automation capability of securities fund management institutions

2024-11-20 发布　　2024-11-20 实施

中国证券监督管理委员会　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这些专利的责任。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC 180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：国信证券股份有限公司、广发证券股份有限公司、华泰证券股份有限公司、海通证券股份有限公司、中证信息技术服务有限责任公司、国泰君安证券股份有限公司、中国银河证券股份有限公司、博时基金管理有限公司、鹏华基金管理有限公司、上海艾芒信息科技有限公司、北京华佑科技有限公司、优维科技（深圳）有限公司、珠海金智维信息科技有限公司。

本文件主要起草人：杨阳、刘汉西、彭华盛、邱朋、刘博、路一、张帆、萧田国、吕斌、王逸、詹子曦、王厦、蔡志刚、王玉彬、祝芝、邓廷勋、黄炎韬、王金银、何鎏。

引　言

证券基金经营机构应用运维自动化程度和范围逐步扩大，制定具有全局视角和统一规范性的指导文件，为经营机构的运维自动化建设提供明确的思路和方法，指引经营机构开展运维自动化建设工作。通过管理和技术手段，有效控制和降低运维自动化所带来的潜在风险，增强对运维工具的自主掌控能力，进而推动和提升行业运维自动化的建设水平。

本文件结合了金融行业特点，基于实践经验，指导和规范经营机构通过定期全面评估运维自动化的能力成熟度，持续进行对标提升，提高运维自动化风险管控与防范能力，确保信息系统稳定、安全、可靠运行。

证券基金经营机构运维自动化能力成熟度规范

1 范围

本文件规定了证券基金经营机构的运维自动化能力框架和等级划分、能力成熟度评估方法与要求，以及安全与风险管理、工具与平台建设、组织管理以及过程管理等能力成熟度评估的具体要求。

本文件适用于证券基金经营机构信息技术运维服务自动化组织实施和服务过程的能力建设，以及能力成熟度评估。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

环境隔离 environment isolation

在互不影响的IT环境中部署相同功能的服务系统，用于不同使用目的。

注：环境是逻辑上或物理上独立的一整套系统，包含了处理用户请求的全部组件。

3.2

重要信息系统 important information system

为支持证券基金经营机构和证券基金专项业务服务机构关键业务功能的系统。

注1：重要信息系统包括集中交易系统、投资交易系统、金融产品销售系统、估值核算系统、投资监督系统、份额登记系统、第三方存管系统、融资融券业务系统、网上交易系统、电话委托系统、移动终端交易系统、法人清算系统、具备开户交易或者客户资料修改功能的门户网站、承载投资咨询业务的系统、存放承销保荐业务工作底稿相关数据的系统、专业即时通信软件以及与上述信息系统具备类似功能的信息系统。

注2：如果重要信息系统出现异常，将对证券期货市场和投资者产生重大影响。

3.3

稳态信息系统 steady-state information system

业务需求和负载在相对稳定与可预测的环境下运行的系统，倾向使用成熟的技术和架构，变更和升级频率相对较低，主要包括承载证券买卖、委托撤单、交易报盘、统一清算等证券基金公司核心业务的系统。

3.4

敏态信息系统 agile information system

应对快速变化的市场和业务需求而设计的系统，倾向使用弹性可扩展的云计算资源，具有快速迭代和频繁的软件发布周期，主要包括满足证券基金业务多样化和创新需求，承载智能选股决策分析等新生业务系统。

3.5

配置项 configuration item

为交付一项或多项服务所需要控制的元素。

注：配置项在复杂性、规模和类型方面变化可能很大，配置项可以是整个系统包括所有的硬件、软件和文档，也可以是单个模块或很小的硬件部件。

3.6

制品 artifact

构建过程输出物。

注：包括软件包、脚本、应用配置等。

3.7

部署流水线 deployment pipeline

软件从版本控制库到用户手中这一过程的自动化表现形式。

4 缩略语

下列缩略语适用于本文件。

CMDB：管理配置数据库（Configuration Management Database）

ETL：抽取转换加载（Extract-Transform-Load）

CPU：中央处理器（Central Processing Unit）

WebUI：网页用户界面（Web User Interface）

IT：信息技术（Information Technology）

IaaS：基础设施即服务（Infrastructure as a Service）

PaaS：平台即服务（Platform as a Service）

API：应用程序编程接口（Application Programming Interface）

SQL：结构化查询语言（Structured Query Language）

DBA：数据库管理员（Database Administrator）

AI：人工智能（Artificial Intelligence）

int：整数数据类型（计算机语言关键字，integer 的缩写）

QPS：每秒查询率（Query Per Second）

ITIL：IT 基础架构库（Information Technology Infrastructure Library）

SDK：软件开发工具包（Software Development Kit）

KPI：关键绩效指标（Key Performance Indicators）

ECC：应急指挥中心（Emergency Command Center）

RPO：恢复点目标（Recovery Point Objective）

RTO：恢复时间目标（Recovery Time Objective）

5 运维自动化能力框架

运维自动化能力包括安全与风险管理、工具与平台建设、组织管理三类技术管理能力，以及过程管理中的技术应用能力，具体包括21个能力域，46个能力项。运维自动化能力框架见表1。

表1　运维自动化能力框架

能力类	能力域	能力项
安全与风险管理	风险防范	管理流程与规范
	风险控制	风险控制策略
		研发管理
		运行管理
		应急管理
		外包风险管理
	安全审计	安全合规审计
工具与平台建设	功能设计	功能设计
	非功能设计	可维护性
		可用性
		开放性
	安全设计及可控性	安全设计
		安全可控性
组织管理	组织管理	组织架构设计
		组织目标管理
		人员能力管理
		文化管理

表 1　运维自动化能力框架（续）

能力类	能力域	能力项
过程管理	入库管理	资产入库
	上架管理	裸机交付
	基础资源交付	计算资源交付
		存储资源交付
		网络资源交付
	平台资源交付	中间件交付
		数据库交付
	云资源管理	多云与混合云管理
	环境管理	环境管理
	制品及物料管理	制品及物料管理
	数据管理	数据变更管理
	部署与发布管理	部署与发布模式
		部署流水线
	监控管理	监控数据采集
		监控数据处理
		监控数据应用
		服务巡检
	故障管理	故障发现
		故障定位
		故障处置
	连续性管理	备份恢复
		应急演练
		容灾切换
	调度与保障	流程自动化
		资源调度
		性能容量管理
	配置管理	资源模型管理
		配置项管理
		资源数据运营

6 运维自动化能力成熟度等级划分与评估

6.1 技术管理能力成熟度

技术管理能力成熟度体现了证券基金经营机构对于开展运维自动化所产生的系统性风险的管控能力，适用于安全与风险管理、工具与平台建设、组织管理三个能力类及下属的7个能力域，17个能力项。技术管理能力成熟度等级自低到高划分为G1至G3三级，等级划分与要求见表2。

表 2 技术管理能力成熟度等级划分与要求

等级代号	等级名称	等级要求
G1	基础级	a) 具备完整的制度规范体系且组织内部正式发文，风险防范措施覆盖全面并得到有效落实； b) 运维活动实现了自动化和工具化，运维自动化工具安全可靠； c) 具备基本、必要的安全风险控制组织，以及基本的运维自动化安全风险防范能力。
G2	全面级	a) 具备完整的制度规范体系和全面的风险防范措施，并通过运维自动化工具平台实现固化和落地，运维自动化的效率、质量和风险可量化； b) 运维工具平台互联互通，实现局部运维场景化； c) 具备完善、专业化的安全风险控制组织，支持运维自动化的规模化建设； d) 具备全面的安全风险防范能力，可全面和有效应对运维自动化所带来的安全风险。
G3	持续优化级	a) 运维自动化的效率、质量和风险防范全面实现数字化度量，具备持续分析、运营、智能化诊断与决策的能力； b) 运维自动化工具建设全面平台化场景化； c) 运维自动化组织支持中长期创新能力的实施和落地，通过技术创新、业务赋能，全面形成持续改进的文化，可随着业务、技术和组织的变化，不断优化、迭代和提升运维自动化的安全风险防范能力，实现运维自动化技术、安全风险防范与业务的深度融合。

6.2 技术应用能力成熟度

技术应用能力成熟度体现了证券基金经营机构通过广泛应用运维自动化技术，降低整体运维风险的能力，适用于过程管理能力类及下属的14个能力域，29个能力项。技术应用能力等级自低到高划分为Y1至Y5五级，等级划分与要求见表3。

表 3　技术应用能力成熟度等级划分与要求

等级代号	等级名称	等级要求
Y1	初始级 （脚本化运维）	a）基于脚本方式实现针对例行操作的初级自动化运维； b）实际工作过程中以非系统性的文档步骤来描述和定义日常运维操作； c）自动化运维能力的沉淀和积累主要基于运维个体； d）自动化运维脚本零散、不成体系，具备基本的安全防范意识及技术手段。
Y2	基础级 （工具化运维）	a）基于 IT 服务管理要求建立了相关运维工作流程，可将运维工作流程及自动化脚本固化在相关工具中，以完成常见的运维工作； b）自动化运维能力局限在相关流程和工具内部，工具间未实现横向打通且不成体系； c）自动化运维能力的沉淀和积累基于小型运维团队； d）具备较好的自动化运维安全意识并具备相关预防及解决方案。
Y3	先进级 （流程工具化运维）	a）基于运维场景实现了流程和操作的标准化、自动化，并在部分 IT 系统实现了技术落地； b）实现了常见操作的标准化并可以作业的方式调度运行； c）各运维工具的能力实现横向打通，工具化和脚本化能力进一步被系统/平台所封装，提供基于 WebUI 的操作能力； d）自动化运维能力在部分流程间实现了联动和打通； e）自动化运维能力的沉淀和积累基于 IT 系统，并实现了内部协同； f）可以从技术上规避常见自动化运维安全问题并具备较好的故障自愈能力。
Y4	领先级 （场景平台化运维）	a）运维场景面向组织级的全过程域，落地全局标准化和自动化； b）基于运维场景驱动运维服务目录的构建，可以提供自助式/租户式的服务能力； c）基于运维数据化能力，提供精细化运营能力； d）实现了部分智能运维如告警收敛，并可借助智能运维能力缩短故障时间，关键场景故障自愈及缩扩容，快速恢复业务，及时止损。
Y5	顶尖级 （智能化运维）	a）基于数据化全面实现组织级的智能化能力，实现运维能力闭环，实现运维核心场景无人化运维的能力； b）提供持续运营和改进的能力，主动服务业务，赋能业务； c）具备单场景智能运维模块串联协同及流程化编排的能力，实现了智能交付、智能变更及智能发布，大部分场景实现了故障自愈及缩扩容，可以提前预判运维操作带来的风险，并给出可操作的改进建议。

6.3 能力成熟度评估与要求

6.3.1 运维自动化能力成熟度评估方法

运维自动化能力成熟度可以综合运用下述方法对能力项、能力域、能力类进行定性评估，并给出相应成熟度等级：

——问卷调查：通过编制并组织填写问卷形式，对运维自动化状况等情况进行统计和调查；

——人员访谈：通过与被评估方进行交流、讨论方式，了解有关信息；

——文档查验：通过查验运维自动化相关文档材料，了解材料的完备情况；

——配置核查：登录相关信息系统工具平台，检查配置与前述文档材料的一致情况；

——工具测试：利用技术工具对信息系统、应用软件等进行实操测试，验证相关能力项的符合情况；

——旁站验证：通过对承载数据的信息系统、设备、网络等进行现场操作和演示，实地观察技术设施和环境状况，判断运维相关工作人员的安全意识、业务操作、管理程序等方面的安全情况。

6.3.2 运维自动化能力成熟度要求

重要信息系统的技术管理能力成熟度达到全面级（G2），非重要信息系统成熟度达到基础级（G1）。

对于稳态信息系统的技术应用能力成熟度达到基础级（Y2），敏态信息系统成熟度达到（Y3）。

7 安全与风险管理

7.1 风险防范

7.1.1 管理流程与规范

管理流程与规范成熟度从信息安全管理、风险控制管理、安全审计管理三个方面进行评估：

——信息安全管理：在自动化运维过程中，采取一系列措施和策略来满足生产运行的安全性和合规性；

——风险控制管理：在自动化运维过程中，采取一系列措施来识别、评估、监控和缓解可能对系统稳定性、安全性和业务连续性造成影响的风险；

——安全审计管理：对运维活动进行系统的记录、监控、分析和评估，以确保运维操作的合规性、透明度和安全性。

管理流程与规范成熟度等级要求见表 4。

表 4 管理流程与规范成熟度等级要求

等级	管理制度	风险控制管理	安全审计管理
G1	a) 具备完善的运维自动化管理制度； b) 运维自动化管理制度符合行业监管规范，满足生产运行需求。	a) 具备完善的风险控制制度与流程，通过定期和专项等方式开展风险控制工作； b) 风险控制应包括风险控制策略、研发管理、运行管理、应急管理、外包风险管理等方面。	a) 具备完善的安全审计制度与流程，按照制度与流程要求通过定期和专项等方式开展安全合规审计工作； b) 安全审计应覆盖运维自动化活动的全流程。

表 4　管理流程与规范成熟度等级要求（续）

等级	管理制度	风险控制管理	安全审计管理
G2	a）具备完善的运维自动化管理制度； b）运维自动化管理制度符合行业监管规范，满足生产运行需求； c）通过平台方式实现运维自动化管理制度流程相关活动的线上化管理； d）初步建立运维自动化指标体系。	a）具备完善的风险控制制度与流程，通过定期和专项等方式开展风险控制工作； b）风险控制应包括风险控制策略、研发管理、运行管理、应急管理、外包风险管理等方面； c）通过平台方式实现风险控制制度与流程相关活动的线上化管理。	a）具备完善的安全审计制度与流程，通过定期和专项等方式开展工作； b）安全审计应覆盖运维自动化活动的全流程； c）通过平台方式实现安全审计制度与流程相关活动的线上化管理。
G3	a）具备完善的运维自动化管理制度； b）运维自动化管理制度符合行业监管规范，满足生产运行需求； c）通过平台方式实现运维自动化管理制度流程相关活动的线上化管理； d）依据监管要求和实际生产情况进行定期回顾，并对相关流程规范及配套流程平台进行持续优化； e）依据运维自动化指标体系对能力成熟度进行数字化度量，不断完善指标体系，实现闭环管理。	a）具备完善的风险控制制度与流程，通过定期和专项等方式开展风险控制工作； b）风险控制应包括风险控制策略、研发管理、运行管理、应急管理、外包风险管理等方面； c）通过平台方式实现风险控制制度与流程相关活动的线上化管理； d）对风险控制流程的执行情况具备智能化分析和风险识别能力，可持续优化。	a）具备完善的安全审计制度与流程，按照制度与流程要求通过定期和专项等方式开展安全合规审计工作； b）安全审计应覆盖运维自动化活动的全流程； c）通过平台方式实现安全审计制度与流程相关活动的线上化管理； d）安全合规审计具备智能化分析能力，可持续优化。

7.2　风险控制

7.2.1　风险控制策略

风险控制策略成熟度从环境部署管理、角色权限管理、操作控制管理三个方面进行评估：

——环境部署管理：建立研发、测试、生产等环境隔离机制，以及有效的访问控制措施，以防止运维自动化工具在非预期的环境操作导致生产环境发生故障，并降低外部攻击者入侵的风险；

——角色权限管理：通过对运维自动化工具平台的开发人员、运维人员和平台用户在角色上进行分类和安全管理，授予不同角色适当的操作权限，以降低不同人员超越权限范围进行运维自动化活动所导致的风险；

——操作管控管理：运维自动化工具平台应在生产环境部署前通过充分的测试，以确保平台的可靠性，且在生产环境中进行运维自动化活动时，需区分操作时间窗口和操作地点进行操作管控。特别在开市期间，非常规的运维自动化活动需经过谨慎的决策和审批方可执行。

风险控制策略成熟度等级要求见表 5。

表 5　风险控制策略成熟度等级要求

等级	环境部署管理	角色权限管理	操作管控管理
G1	a）操作不同业务环境的运维自动化工具平台应分别部署，形成环境隔离； b）运维自动化工具平台的部署应与互联网隔离，从互联网访问运维自动化工具平台应严格受控，满足信息安全要求。	a）依据参与的运维自动化工作职责设置合理的角色定义，具有互斥要求的角色需要授予不同人员； b）依据实际业务需求和角色，按需分配运维自动化工具平台的权限，实现不同角色的权限隔离。	a）运维自动化工具平台应经过完备测试，确认无误之后再在生产环境投产； b）运维自动化工具平台的操作应根据业务需求对操作时间、操作地点等方面进行有效控制，确保操作准确有效。
G2	a）操作不同业务环境的运维自动化工具平台应分别部署，形成环境隔离； b）运维自动化工具平台的部署应与互联网隔离，从互联网访问运维自动化工具平台应严格受控，满足信息安全要求； c）针对生产应划分不同安全区域，具备适当的隔离和线上化管理能力，防止跨安全区域访问导致的风险。	a）依据参与的运维自动化工作职责设置合理的角色定义，具有互斥要求的角色应授予不同人员； b）依据实际业务需求和角色，按需分配运维自动化工具平台的权限，实现不同角色的权限隔离； c）通过运维自动化工具平台，实现角色和权限的线上化管理。	a）运维自动化工具平台应经过完备测试，确认无误之后再在生产环境投产； b）运维自动化工具平台的操作应根据业务需求对操作时间、操作地点等方面进行有效控制，确保操作准确有效； c）运维自动化工具平台具备判断、提示和阻断机制，防止操作时机不当带来的业务影响。
G3	a）操作不同业务环境的运维自动化工具平台应分别部署，形成环境隔离； b）运维自动化工具平台的部署应与互联网隔离，从互联网访问运维自动化工具平台应严格受控，满足信息安全要求； c）针对生产应划分不同安全区域，具备适当的隔离和线上化管理能力，防止跨安全区域访问导致的风险； d）通过数据分析和智能运维等技术，对运维自动化工具平台的环境访问情况和部署情况进行定期回顾，持续优化环境部署。	a）依据参与的运维自动化的工作职责设置合理的角色定义，具有互斥要求的角色应授予不同人员； b）依据实际业务需求和角色，按需分配运维自动化工具平台的权限，实现不同角色的权限隔离； c）通过运维自动化工具平台，实现角色和权限的线上化管理； d）通过数据分析和智能运维等技术，对角色适配情况和权限适配情况进行定期回顾，并根据业务进行动态调整。	a）运维自动化工具平台应经过完备测试，确认无误之后再在生产环境投产； b）运维自动化工具平台的操作应根据业务需求对操作时间、操作地点等方面进行有效控制，确保操作准确有效； c）运维自动化工具平台具备判断、提示和阻断机制，防止操作时机不当带来的业务影响； d）通过数据分析和智能运维等技术，对操作情况进行定期回顾，持续优化操作的风险预测、提示和阻断能力。

7.2.2　研发管理

研发管理成熟度从需求管理、开发管理、测试管理三个方面进行评估：

——需求管理：对运维自动化工具平台开发需求的申请、受理、评审、验收等环节的全流程管控工作机制；

——开发管理：制定运维自动化工具平台开发规范，实现开发过程中的代码编写、单元测试、代码评审、调试排错等环节的全流程管控工作机制；

——测试管理：制定运维自动化工具平台测试管理规范，测试人员根据需求规格说明对功能进行测试，并持续优化测试质量。

研发管理成熟度等级要求见表6。

表6　研发管理成熟度等级要求

等级	需求管理	开发管理	测试管理
G1	a）制定运维自动化工具平台需求管理规范，并纳入组织需求管理体系，统一管理，确保需求可得到及时的响应和处理； b）制定运维自动化工具平台需求评审规范，科学处理各类自动化需求，防范系统风险。	制定运维自动化工具平台开发管理规范，防范系统风险。	a）制定运维自动化工具平台测试管理规范（包含安全测试），对测试流程及结果进行管控，确保测试过程的完整性； b）建立独立的测试环境，避免风险传导。
G2	a）制定运维自动化工具平台需求管理规范，并纳入组织需求管理体系，统一管理，确保需求可得到及时的响应和处理； b）制定运维自动化工具平台需求评审规范，科学处理各类自动化需求，防范系统风险； c）实现需求的线上化全流程管理，确保需求申请、受理、评审、验收等各环节可视可控。	a）制定运维自动化工具平台开发管理规范，防范系统风险； b）通过工具自动实现对开发代码的安全审核，审核包括依赖包来源可信度、漏洞检测以及开源协议许可风险等，并对发现的问题进行追踪管理，保障开发工具的安全稳定运行。	a）制定运维自动化工具平台测试管理规范（包含安全测试），对测试流程及结果进行管控，确保测试过程的完整性； b）建立独立的测试环境，避免风险传导； c）实现测试过程的线上化管理，确保测试过程的正确性、完备性，有效防范测试风险； d）具备完备的运维自动化工具平台测试方案和自动化回归测试能力，以提高自动化测试效率和测试覆盖度。
G3	a）制定运维自动化工具平台需求管理规范，并纳入组织需求管理体系，统一管理，确保需求可得到及时的响应和处理； b）制定运维自动化工具平台需求评审规范，科学处理各类自动化需求，防范系统风险； c）实现需求的线上化全流程管理，确保需求申请、受理、评审、验收等各环节可视可控； d）对需求实现后的使用效果、频率等指标进行量化跟踪，定期对需求实施的效果进行评估反馈，持续优化需求管理细则；	a）制定运维自动化工具平台开发管理规范，防范系统风险； b）通过工具自动实现对开发代码的安全审核，审核包括依赖包来源可信度、漏洞检测以及开源协议许可风险等，并对发现的问题进行追踪管理，保障开发工具的安全稳定运行； c）实现运维自动化工具平台开发过程的线上化管理，满足合规及风险管理的要求；	a）制定运维自动化工具平台测试管理规范（包含安全测试），对测试流程及结果进行管控，确保测试过程的完整性； b）建立独立的测试环境，避免风险传导； c）实现测试过程的线上化管理，确保测试过程的正确性、完备性，有效防范测试风险； d）具备完备的运维自动化工具测试方案和自动化回归测试能力，以提高自动化测试效率和测试覆盖度；

表 6　研发管理成熟度等级要求（续）

等级	需求管理	开发管理	测试管理
	e）制定运维自动化工具平台需求管理规范，并纳入组织需求管理体系，统一管理，确保需求可得到及时的响应和处理； f）制定运维自动化工具平台需求评审规范，科学处理各类自动化需求，防范系统风险； g）实现需求的线上化全流程管理，确保需求提出、受理、评审、验收等各环节可视可控； h）对需求实现后的使用效果、频率等指标进行量化跟踪，定期对需求实施的效果进行评估反馈，持续优化需求管理细则。	d）制定运维自动化工具平台开发管理规范，防范系统风险； e）实现运维自动化工具平台开发过程的线上化管理，满足合规及风险管理的要求； f）通过工具自动实现对开发代码的安全审核，审核包括依赖包来源可信度、漏洞检测以及开源协议许可风险等，并对发现的问题进行追踪管理，保障开发工具的安全稳定运行； g）对运维自动化工具平台的研发效能和质量实施工程化管理，通过建立指标体系，进行数字化度量和分析，及时发现开发流程管理中存在的问题并持续优化，提高开发效率和质量。	e）制定运维自动化工具平台测试管理规范（包含安全测试），对测试流程及结果进行管控，确保测试过程的完整性； f）建立独立的测试环境，避免风险传导； g）实现测试过程的线上化管理，确保测试过程的正确性、完备性，有效防范测试风险； h）具备完备的自动化工具测试方案和自动化回归测试能力，以提高自动化测试效率和测试覆盖度； i）对运维自动化工具平台的测试能力实施工程化管理，通过建立指标体系，进行数字化度量和分析，对测试方案及过程的合理性进行评估，持续优化测试过程。

7.2.3　运行管理

运行管理成熟度从变更发布管理、监控管理、容量管理、高可用及备份管理四个方面进行评估：

——变更发布管理：落实变更发布工作机制，包括对运维自动化工具平台的变更审核、发布实施、发布验证、异常处理等过程进行管理，并持续优化变更发布管理能力；

——监控管理：落实监控相关的工作要求，包括对运维自动化工具平台运行的主机资源、服务可用性、功能、性能、自动化任务调度状态、作业运行状态等事项进行多维度的监控，对监控报警进行集中汇总并落实报警处理的行为；

——容量管理：落实容量管理的工作机制，包括对运维自动化工具平台的组件容量、服务容量、业务容量进行跟踪、分析和预测，提前发现容量瓶颈，实施容量管控，确保运维自动化工具平台的处理容量满足需求并稳定运行；

——高可用及备份管理：落实平台架构高可用与数据备份相关的工作要求，包括对运维自动化工具平台的部署架构、逻辑架构、数据备份、程序备份等进行管理，持续优化平台的高可用和备份能力。

运行管理成熟度等级要求见表 7。

表 7　运行管理成熟度等级要求

等级	变更发布管理	监控管理	容量管理	高可用及备份
G1	a）制定运维自动化工具平台变更管理规范，防范因系统变更造成的运行安全故障； b）制定运维自动化工具平台变更实施方案，并对系统变更操作行为进行记录、审查、确认和跟踪。	制定运维自动化工具平台的监控规范，及时发现平台运行过程中出现的异常并及时处理。	制定运维自动化工具平台容量评估规范，定期开展容量评估，及时发现平台运行的容量问题并进行容量调整。	a）实施运维自动化工具平台高可用建设，具备应急预案和切换机制； b）具备数据备份和恢复机制，定期进行数据备份、恢复验证工作，具备完善的数据维护措施，保障运行数据的安全、完整。
G2	a）制定运维自动化工具平台变更管理规范，防范因系统变更造成的运行安全故障； b）制定运维自动化工具平台变更实施方案，并对系统变更操作行为进行记录、审查、确认和跟踪； c）运维自动化工具平台的变更发布统一纳入线上化管理，确保变更风险可控； d）对运维自动化工具平台软件和配置信息实施版本化管理，异常情况下具备快速回退功能，以确保其可靠性，保障服务的连续性。	a）制定运维自动化工具平台的监控规范，及时发现平台运行过程中出现的异常并及时处理； b）运维自动化工具平台纳入统一的监控系统进行监控，对平台涉及的基础设施、操作系统、服务、客户终端等多个维度进行实时监控，并确保所有的告警信息都得到及时有效的处理，保障工具平台的正常运行。	a）制定运维自动化工具平台容量评估规范，定期开展容量评估，及时发现平台运行的容量问题并进行容量调整； b）容量分析可通过线上化工具实现统一管理、留痕，定期实施容量评估，容量事件及时得到有效的跟踪闭环。	a）实施运维自动化工具平台高可用建设，实现多数据中心部署，具备应急预案和快速切换机制； b）具备数据备份和恢复机制，采用线上备份工具，定期进行数据备份、恢复验证工作；备份执行的正确性通过线上工具实施监控，确保数据备份的完整性、有效性。
G3	a）制定运维自动化工具平台变更管理规范，防范因系统变更造成的运行安全故障； b）制定运维自动化工具平台变更实施方案，并对系统变更操作行为进行记录、审查、确认和跟踪；	a）制定运维自动化工具平台的监控规范，及时发现平台运行过程中出现的异常并及时处理；	a）制定运维自动化工具平台容量评估规范，定期开展容量评估，及时发现平台运行的容量问题并进行容量调整；	a）实施运维自动化工具平台高可用建设，实现多数据中心部署，具备应急预案和自动化切换机制，确保出现灾难事件时，服务不受影响；

表 7　运行管理成熟度等级要求（续）

等级	变更发布管理	监控管理	容量管理	高可用及备份
	c）运维自动化工具平台的变更发布统一纳入线上化管理，确保变更风险可控； d）对运维自动化工具平台软件和配置信息实施版本化管理，异常情况下具备快速回退功能，以确保其可靠性，保障服务的连续性； e）采用数字化智能分析，对变更前后的关键指标进行分析，能提前预测变更对系统功能、性能等维度的影响，及时发现存在的安全隐患，降低变更风险。	b）运维自动化工具平台纳入统一的监控系统进行监控，对平台涉及的基础设施、操作系统、服务、客户终端等多个维度进行实时监控，并确保所有的告警信息都得到及时有效的处理，保障工具平台的正常运行； c）对运维自动化工具平台的性能数据、告警数据等进行运营分析，结合算法，实现对潜在风险的洞察与预测，可快速定位已知故障； d）基于运行监控数据，结合自动化系统，实现告警自愈能力。	b）容量分析可通过线上化工具实现统一管理、留痕，定期实施容量评估，容量事件及时得到有效的跟踪闭环； c）对运维自动化工具平台的容量数据进行实时的、自动化和智能化分析，预测容量或性能瓶颈； d）根据运维自动化工具平台容量分析发现的问题，实现自动扩缩容，防范出现系统容量风险。	b）具备数据备份和恢复机制，采用线上备份工具，定期进行数据备份、恢复验证工作；备份执行的正确性通过线上工具实施监控，确保数据备份的完整性、有效性； c）运维自动化工具平台运行过程中的备份数据需在同城及异地备份中心实时同步，保持备份数据与原始数据的一致性，确保出现灾难时，服务不中断。

7.2.4　应急管理

应急管理成熟度从应急预案、应急演练、应急处置、应急复盘四个方面进行评估：

——应急预案：运维人员根据运维自动化活动可能触发故障的场景，制定具体的可操作的应对措施。应急预案的场景宜尽可能贴合实际、全面覆盖；

——应急演练：运维人员组织运维自动化应急人员根据应急预案，模拟预案场景的发生，并进行应急处置的活动；

——应急处置：在生产环境中，因运维自动化活动触发故障时，运维人员及相关方对故障积极响应与处置，尽可能快速恢复故障的活动；

——应急复盘：通过组织事后总结分析工作，剖析应急处置的过程，改进应急预案、应急演练环节，持续提高应急处置水平的活动。

应急管理成熟度等级要求见表 8。

表 8　应急管理成熟度等级要求

等级	应急预案	应急演练	应急处置	应急复盘
G1	具备完善的运维自动化应急预案，定期对应急预案进行评审与修订，保障预案内容的有效性。	a) 根据应急演练要求，定期按照运维自动化应急预案场景，组织应急小组成员模拟故障，进行故障诊断、故障恢复的真实演练； b) 准确、完整记录演练过程中关键的时点、步骤，及与应急预案中不一致的情形，进行优化完善。	具备明确的应急处置机制，包括但不限于故障发现、响应、通报、定位、恢复，定期对应急处置机制进行评审与修订。	具备完善的应急复盘机制，包括但不限于过程回顾、技术分析、经验总结、优化改进。
G2	a) 具备完善的运维自动化应急预案，定期对应急预案进行评审与修订，保障预案内容的有效性； b) 通过运维自动化工具平台进行应急预案的线上化管理。	a) 根据应急演练要求，定期按照运维自动化应急预案场景，组织应急小组成员模拟故障，进行故障诊断、故障恢复的真实演练； b) 通过线上化管理工具辅助运维自动化应急演练，量化演练指标，准确、完整记录演练过程中关键的时点、步骤，及时发现与应急预案中不一致的情形，进行优化完善。	a) 具备明确的应急处置机制，包括但不限于故障发现、响应、通报、定位、恢复，定期对应急处置机制进行评审与修订； b) 通过平台实现应急处置过程的协同和操作的线上化管理。	a) 具备完善的应急复盘机制，包括但不限于过程回顾、技术分析、经验总结、优化改进； b) 通过平台实现应急复盘的线上化管理。
G3	a) 具备完善的运维自动化应急预案，定期对应急预案进行评审与修订，保障预案内容的有效性； b) 通过运维自动化工具平台进行应急预案的线上化管理； c) 通过智能化手段，主动关联事件、变更等运维活动，触发应急预案的修订和持续优化。	a) 根据应急演练要求，定期按照运维自动化应急预案场景组织应急小组成员模拟故障，进行故障诊断、故障恢复的真实演练； b) 通过线上化管理工具辅助运维自动化应急演练，量化演练指标，准确、完整记录演练过程中关键的时点、步骤，及时发现与应急预案中不一致的情形，进行优化完善； c) 结合演练场景和演练数据分析，利用混沌工程能力，智能推荐应急演练场景，及时发现演练薄弱环节，持续提升应急演练的水平。	a) 具备明确的应急处置机制，包括但不限于故障发现、响应、通报、定位、恢复，定期对应急处置机制，进行评审与修订； b) 通过平台实现应急处置过程的协同和操作的线上化管理； c) 利用智能化手段，按应急预案实施自动化处置，实现故障自愈。	a) 具备完善的应急复盘机制，包括但不限于过程回顾、技术分析、经验总结、优化改进； b) 通过平台实现应急复盘的线上化管理。

7.2.5 外包风险管理

外包风险管理成熟度从入场前管理、驻场管理、离场管理三个方面进行评估：

——入场前管理：对于外包人员驻场前的风险管控措施，主要包括外包服务权责管理、外包服务及外包人员需求管理等；

——驻场管理：对于外包人员驻场工作期间的风险管控措施，主要包括外包服务安全管理、人员信息管理、外包服务绩效考核与评价、资源管理工作等；

——离场管理：对于外包人员离场过程的风险管控措施，主要包括服务终止原因及材料交接、设备归还和账号权限注销。

外包风险管理成熟度等级要求见表 9。

表 9 外包风险管理成熟度等级要求

等级	入场前管理	驻场管理	离场管理
G1	a) 外包服务厂商应完成行业信息技术服务机构备案手续，在相应的领域具有国家要求的服务资质，具有较高的知名度和良好的公司声誉； b) 外包人员应进行严格信息安全管控，在数据层面区分敏感数据与一般数据的使用权限； c) 具有明确的外包项目建议书，包括所需的硬件、软件、服务、成本与时间等要求； d) 外包服务协议应明确约定双方权利、义务、服务厂商考核和评价指标及安全保密协议。	a) 具备公司级外包人员安全管理制度，对外包人员进行宣导，并严格按照规定实施； b) 为外包人员申请资源时，应严格规定其使用权限，并做好记录和定时更新等管理工作； c) 建立配置备份和应急措施，以应对外包人员因操作失误导致数据丢失、程序丢失、文档丢失或系统异常故障等风险； d) 定期对外包厂商所提供的外包服务质量（工作进度控制、项目成果等）进行监督和考核，对服务质量进行评价，形成评价报告，并留档备查； e) 通过有效的技术手段，对外包人员在生产环境的操作行为进行审计，且符合实名制原则，防范数据泄露。外包人员终端接入网络应做访问控制。	a) 在外包服务合同到期时，应要求外包厂商提供完整的工作交接清单及有关交接材料； b) 具备外包人员资源回收和权限注销流程。
G2	a) 外包服务厂商应完成行业信息技术服务机构备案手续，在相应的领域具有国家要求的服务资质，具有较高的知名度和良好的公司声誉； b) 外包人员应进行严格信息安全管控，在数据层面区分敏感数据与一般数据的使用权限； c) 具有明确的外包项目建议书，包括所需的硬件、软件、服务、成本与时间等要求；	a) 具备公司级外包人员安全管理制度，对外包人员进行宣导，并严格按照规定实施； b) 为外包人员申请资源时，应严格规定其使用权限，并做好记录和定时更新等管理工作； c) 建立配置备份和应急措施，以应对外包人员因操作失误导致数据丢失、程序丢失、文档丢失或系统异常故障等风险； d) 定期对外包厂商所提供的外包服务质量（工作进度控制、项目成果等）进行监督和考核，对服务质量进行评价，形成评价报告，并留档备查；	a) 在外包服务合同到期时，应要求外包厂商提供完整的工作交接清单及有关交接材料； b) 具备外包人员资源回收和权限注销流程； c) 外包人员离场申请过程应通过线上流程系统进行管理；

表 9　外包风险管理成熟度等级要求（续）

等级	入场前管理	驻场管理	离场管理
	d）外包服务协议应明确约定双方权利、义务、服务厂商考核和评价指标及安全保密协议； e）通过平台实现入场前的线上化管理。	e）通过有效的技术手段，对外包人员在生产环境的操作行为进行审计，且符合实名制原则，防范数据泄露。外包人员终端接入网络需做访问控制； f）外包人员的安全权限（如系统资源访问权限等）分配通过模板自动化生成，并具备校验机制； g）外包商服务和外包人员管理应纳入线上化管理，定期对外包人员自动生成考勤、工作量报表，方便管理人员进行考核评价。	d）外包人员资源的回收通过运维自动化工具平台实现，在经过审批后，自动完成外包人员资源的回收。
G3	a）外包服务厂商应完成行业信息技术服务机构备案手续，在相应的领域具有国家要求的服务资质，具有较高的知名度和良好的公司声誉； b）外包人员应进行严格信息安全管控，在数据层面区分敏感数据与一般数据的使用权限，外包提供的服务范围参照重要信息系统的要求执行； c）具有明确的外包项目建议书，包括对所需的硬件、软件、服务、成本与时间等要求； d）外包服务协议应明确约定双方权利、义务、服务商考核和评价指标及安全保密协议； e）通过平台实现入场前的线上化管理。	a）具备公司级外包人员安全管理制度，对外包人员进行宣导，并严格按照规定实施； b）为外包人员申请资源时，应严格规定其使用权限，并做好记录和定时更新等管理工作； c）建立配置备份和应急措施，以应对外包人员因操作失误导致数据丢失、程序丢失、文档丢失或系统异常故障等风险； d）定期对外包厂商所提供的外包服务质量（工作进度控制、项目成果等）进行监督和考核，对服务质量进行评价，形成评价报告，并留档备查； e）通过有效的技术手段，对外包人员在生产环境的操作行为进行审计，且符合实名制原则，防范数据泄露，同时外包人员终端接入网络需做访问控制； f）外包人员的安全权限（如系统资源访问权限等）分配通过模板自动化生成，并具备校验机制； g）外包商服务和外包人员管理应纳入信息化管理，定期对外包人员自动生成考勤、工作量报表，方便管理人员进行考核评价； h）通过智能化手段和大数据分析技术，对外包人员的操作记录和权限使用情况等运营数据进行智能化的风险评估。	a）在外包服务合同到期时，应要求外包厂商提供完整的工作交接清单及有关交接材料； b）具备外包人员资源回收和权限注销流程； c）外包人员离场申请过程应通过线上流程系统进行管理； d）外包人员资源的回收通过运维自动化工具平台实现，在经过审批后，自动完成外包人员资源的回收； e）通过智能化手段隔离风险，确保敏感信息的安全。

7.3　安全审计

7.3.1　安全合规审计

安全合规审计成熟度从审计机制、审计范围、留痕管理、审计应对四个方面进行评估：

——审计机制：外部或内部审计人员在进行具体审计实施时的管理要求；

——审计范围：审计内容的使用范围和适用范围；
——留痕管理：运维自动化活动中所涉及的流程文档、交付文档、评审文档和平台层面所形成的事件记录的留痕管理；
——审计应对：在审计实施后对审计结果及审计发现的处理流程，包括审计结果的评审确认、问题发现的通报处理、缺陷不足的追踪改进。

安全合规审计成熟度等级要求见表 10。

表 10　安全合规审计成熟度等级要求

等级	审计机制	审计范围	留痕管理	审计应对
G1	具备完善的运维自动化审计制度，并开展审计活动。	a) 定期开展全面审计：依据本文件管理成熟度所有能力项进行运维成熟度的定期审计； b) 按需开展专项审计：当组织发生运维自动化相关的网络安全事件后，应在事件处理后立即组织执行专项审计及调查或自主进行运维自动化的专项分析，并对潜藏的问题进行改进。	a) 组织应在内部管理制度规范中，涵盖运维自动化的留痕管理要求，并开展留痕管理工作； b) 重要文档和日志留痕信息应满足保存时限的相关要求，以备审计需要； c) 审计材料应满足行业监管要求和保存期限。	a) 具备完善的运维自动化审计应对机制，针对审计结果进行审议及后续整改，跟踪审计的整改进展，形成审计闭环； b) 对于审计发现但未能按期解决的问题，应及时提供合理说明并经相关审批确认。
G2	a) 具备完善的运维自动化审计制度，并开展审计活动； b) 通过运维自动化审计平台实现运维自动化审计流程的线上化管理。	a) 定期开展全面审计：依据本文件管理成熟度所有能力项进行运维成熟度的定期审计； b) 按需开展专项审计：当组织发生运维自动化相关的网络安全事件后，应在事件处理后立即组织执行专项审计及调查或自主进行运维自动化的专项分析，并对潜藏的问题进行改进； c) 在运维自动化审计平台中应包含上述各审计项，组织应在平台中对自动化审计工作予以落实。	a) 组织应在内部管理制度规范中，涵盖运维自动化的留痕管理要求，并开展留痕管理工作； b) 重要文档和日志留痕信息应满足保存时限的相关要求，以备审计需要； c) 审计材料应满足行业监管要求和保存期限； d) 通过运维自动化审计平台实现留痕的线上化管理。	a) 具备完善的运维自动化审计应对机制，针对审计结果进行审议及后续整改，跟踪审计的整改进展，形成审计闭环； b) 对于审计发现但未能按期解决的问题，应及时提供合理说明并经相关审批确认； c) 通过运维自动化审计平台实现审计的整改、优化等活动的线上化管理。

表 10　安全合规审计成熟度等级要求（续）

等级	审计机制	审计范围	留痕管理	审计应对
G3	a) 具备完善的运维自动化审计制度，并开展审计活动； b) 通过自动化平台实现运维审计流程的线上化管理； c) 持续完善并改进运维自动化审计平台线上审计功能，具备智能化审计决策功能。	a) 定期开展全面审计：依据本文件管理成熟度所有能力项进行运维成熟度的定期审计； b) 按需开展专项审计：当组织发生运维自动化相关的网络安全事件后，应在事件处理后立即组织执行专项审计及调查或自主进行运维自动化的分析，并对潜藏的问题进行改进，同时在运维自动化审计平台中应包含上述各审计项，组织应在平台中对自动化审计工作予以落实； c) 应根据运维自动化的发展情况，依据运维自动化流程及平台的发展进程，同步更新审计范围，并持续优化。	a) 组织应在内部管理制度规范中，涵盖运维自动化的留痕管理要求，并开展留痕管理工作； b) 重要文档和日志留痕信息应满足保存时限的相关要求，以备审计需要； c) 审计材料应满足行业监管要求和保存期限； d) 通过运维自动化审计平台实现留痕的线上化管理； e) 通过智能化手段，持续优化留痕管理。	a) 具备完善的运维自动化审计应对机制，针对审计结果进行审议及后续整改，跟踪审计的整改进展，形成审计闭环； b) 对于审计发现但未能按期解决的问题，应及时提供合理说明并经相关审批确认； c) 通过运维自动化审计平台实现审计的整改、优化等活动的线上化管理； d) 通过智能化手段，定期对运维自动化审计的应对处理作出有效性评估，发现审计中的问题，持续优化审计应对能力。

8　工具与平台建设

8.1　功能设计

功能设计成熟度从监控管理、流程管理、操作自动化、运维分析四个方面进行评估：

——运维自动化工具平台宜具备多层次的监控能力，包括对硬件设备（计算、存储、网络等），系统软件（虚拟化、容器、操作系统等），应用可用性（架构高可用、应用服务可用性等），业务功能（安全、性能、体验、应用功能等）等维度的监控，并针对监控告警进行统一管理；

——运维自动化工具平台宜具备运维流程管理能力，证券基金经营机构可结合自身情况，从组织、规程、资源、工具等方面落地相应的流程管理措施；

——运维自动化工具平台宜具备操作自动化能力，将规律性、重复性的运维操作通过自动化方式实现；

——运维自动化工具平台宜具备运维数据分析能力，对监控性能指标、监控告警、系统日志、应用日志、流程管理、配置管理等数据进行深度分析。

功能设计成熟度等级要求见表 11。

表 11　功能设计成熟度等级要求

等级	监控管理	流程管理	操作自动化	运维分析
G1	a）具备对硬件设备、系统软件、应用可用性、业务功能、客户终端等层次的监控能力； b）监控告警可及时送达处理。	具备关键运维流程管理功能，全面实现流程管理留痕。	具备部分运维场景的自动化操作功能与操作留痕，实现基本的风险防范能力。	具备对部分生产运行数据进行采集、存储、加工、消费的基本能力。
G2	a）具备对硬件设备、系统软件、应用可用性、业务功能、客户终端等层次的监控能力； b）监控告警可及时送达处理； c）对各层次监控覆盖能力进行整合，实现指标、日志、调用追踪数据与监控告警数据的汇总，以及监控告警事件的统一管理。	a）具备运维流程管理功能，全面覆盖运维流程，实现流程管理留痕； b）运维流程管理工具实现与监控、自动化操作等工具平台的互联互通。	a）具备主要运维场景的自动化操作与操作留痕，实现全面的风险防范能力； b）具备脚本编写、脚本编排、任务调度等工具平台能力，支持根据不同的运维应用场景进行相应的自动化操作。	a）具备对生产运行数据进行全面采集、存储、加工、消费的能力； b）提供运维数据分析服务，具备对生产运行数据进行集中处理、分析挖掘、场景化应用的能力； c）运维数据分析服务可对外提供多层面的服务能力。
G3	a）具备对硬件设备、系统软件、应用可用性、业务功能、客户终端等层次的监控能力； b）监控告警可及时送达处理； c）对各层次监控覆盖能力进行整合，实现指标、日志、调用追踪数据与监控告警数据的汇总，以及监控告警事件的统一管理； d）利用智能算法，对监控数据进行全面深入的挖掘与分析，具备智能化的异常检测、故障定位、根因分析等能力。	a）具备运维流程管理功能，全面覆盖运维流程，实现流程管理留痕； b）运维流程管理工具实现与监控、自动化操作等工具平台的互联互通； c）可对运维流程实施数字化度量，支持从效能、风险等方面对相关流程进行专项分析，支持运维工作流程的持续优化与运营。	a）具备主要运维场景的自动化操作与操作留痕，实现具备全面的风险防范能力； b）具备脚本编写、脚本编排、任务调度等工具平台能力，支持根据不同的运维应用场景进行相应的自动化操作； c）结合智能算法，对生产运行数据、自动化操作数据进行分析，实现人机协同的自动化操作。	a）具备对生产运行数据进行全面采集、存储、加工、消费的能力； b）提供运维数据分析服务，具备对生产运行数据进行集中处理、分析挖掘、场景化应用的能力； c）运维数据分析服务可对外提供多层面的服务能力； d）结合智能算法，建立运维指标体系、规则引擎，具备可预测的数据感知能力和辅助决策能力。

8.2　非功能设计

8.2.1　可维护性

可维护性成熟度从状态监测、故障隔离、故障恢复三个方面进行评估：

——运维自动化工具平台宜具备对自身运行健康状态的可监测能力，包括性能、指标、日志、链路、容量、功能和体验等数据，同时具备运行状态的可观察性，可及时发现自身运行故障；

——运维自动化工具平台宜具备故障隔离能力，根据故障应对措施将异常模块隔离，提升运维自动化工具平台主要功能的连续性；

——运维自动化工具平台宜具备自身的故障恢复能力，根据故障恢复措施快速实现故障恢复，确保出现异常状况后功能连续性的恢复。

可维护性成熟度等级要求见表 12。

表 12　可维护性成熟度等级要求

等级	状态监测	故障隔离	故障恢复
G1	具备基础设备层、操作系统层、应用层等运行状态的监测能力，平台及任务的运行状态具备可观察性。	具备已知场景的故障隔离机制与方案，在故障发生后，可根据预案完成故障隔离操作。	具备已知场景的故障恢复机制与方案，在故障发生后，可根据预案完成故障恢复。
G2	a) 具备基础设备层、操作系统层、应用层、功能层、体验层等运行状态的监测能力，平台及任务的运行状态具备可观察性； b) 可输出资源、可用性状态、性能、指标、日志、链路、容量、功能和体验等运行数据，并实现数据的平台化管控。	具备已知场景的故障隔离机制与方案，在故障发生后，可采用工具辅助完成故障隔离，确保平台主要功能的可用性。	具备已知场景的故障恢复机制与方案，在故障发生后，可采用工具辅助完成故障恢复，确保平台业务连续性。
G3	a) 具备基础设备层、操作系统层、应用层、功能层、体验层等运行状态的监测能力，平台及任务的运行状态具备可观察性； b) 可输出资源、可用性状态、性能、指标、日志、链路、容量、功能和体验等运行数据，并实现数据的平台化管控； c) 具备平台运行状态的实时分析能力，通过智能化手段，可预测平台潜在运行风险； d) 可全面收集用户行为数据，供平台运营分析，持续优化用户体验。	a) 具备已知场景的故障隔离机制与方案，在故障发生后，可实施自动化故障隔离，确保平台主要功能的可用性； b) 对运行数据进行智能分析，建立故障隔离的专家知识图谱；具备未知和复杂场景下的故障快速隔离能力。	a) 具备已知场景的故障恢复机制与方案，在故障发生后，可实施自动化故障恢复，确保平台业务连续性； b) 对运行数据进行智能分析，建立故障定位、故障恢复的专家知识图谱；具备未知和复杂场景下，故障的快速诊断、定位以及快速恢复能力。

8.2.2　可用性

可用性成熟度从架构高可用、可扩展性、资源管控三个方面进行评估：

——运维自动化工具平台宜具备架构高可用，包括基础设施架构、数据库架构和平台应用架构高可用；

——运维自动化工具平台宜具备在同一逻辑单元增加容量或技术组件，实现整体或逻辑能力扩展的垂直扩展能力，同时具备增加多个逻辑单元，提升整体能力的水平扩展能力；

——运维自动化工具平台宜具备对自身资源消耗的管控能力，控制系统资源消耗，避免对业务系统产生影响。

可用性成熟度等级要求见表 13。

表 13　可用性成熟度等级要求

等级	架构高可用	可扩展性	资源管控
G1	基础设施架构、数据库架构和平台应用架构满足高可用要求，可实现应急预案的高可用切换。	a）平台应用及数据库模块具备垂直扩展能力，解决性能或容量不足等问题； b）支持对现有工具功能模块的扩展与升级。	可人工管控平台资源，限制自动化作业对业务系统资源的消耗。
G2	a）基础设施架构、数据库架构和平台应用架构满足高可用要求，可根据高可用策略实现自动化切换； b）支持多中心容灾，无单点风险，且 RPO、RTO 符合行业重要信息系统备份能力要求。	a）数据库模块具备垂直扩展能力，平台应用架构具备垂直、横向扩展能力，解决性能或容量不足等问题； b）可根据工作场景需求，快速构建场景化应用，满足灵活、可扩展的运维场景化需求； c）具备与平台以外的业务系统互联互通的能力，实现统一管控。	具备自动化的资源管理机制，可结合运行数据和预置策略，动态管控自动化作业的资源消耗。
G3	a）基础设施架构、数据库架构和平台应用架构满足高可用要求，可根据高可用策略实现自动化切换； b）支持多中心容灾，无单点风险，且 RPO、RTO 不低于行业重要信息系统备份能力要求； c）可根据容灾预案实施自动化的多中心容灾切换，无需人工干预。	a）数据库模块具备垂直扩展能力，平台应用架构上具备垂直、横向扩展能力，解决性能或容量不足等问题； b）可根据工作场景需求，快速构建场景化应用，满足灵活、可扩展的运维场景化需求； c）具备与平台以外的应用系统互联互通的能力，实现统一管控； d）平台在架构上可基于数据分析，预测潜在的运行风险，具备如动态扩容、缩容等自愈能力，且支持能力共享、复用。	具备智能资源管理机制，可实现复杂场景下的资源管控，及作业的智能调度和资源管理，在不影响业务系统的前提下最大化资源使用率。

8.2.3　开放性

开放性成熟度从开放 API、平台服务化、兼容开源/行业标准三个方面进行评估：

——运维自动化工具平台宜具备对外开放 API 的能力，提供统一的 API 管控，推动运维监控、流程、操作、分析等工具之间的互联互通；

——运维自动化工具平台宜具备可共享、可复用、可编排的服务化能力，以提升运维场景工具交付效率和应用效能；

——运维自动化工具平台宜兼容开源生态、行业标准以及使用范围广的“事实标准”，提升系统兼容性，降低平台使用门槛。

开放性成熟度等级要求见表 14。

表 14　开放性成熟度等级要求

等级	开放 API	平台服务化	兼容开源/行业标准
G1	提供标准的 API，供外部系统调用，API 管控具备基本的风险防范能力。	将监控、流程、操作、分析等常见运维自动化能力沉淀为标准化服务。	兼容开源生态指标、链路等监控标准，对符合规范系统能够无侵入快速对接。

表 14　开放性成熟度等级要求（续）

等级	开放 API	平台服务化	兼容开源/行业标准
G2	a）提供标准的 API，供外部系统调用，API 管控具备全面的风险防范能力； b）具备集中管理 API 的能力，提供服务接口申请、调试和使用等功能。	a）将监控、流程、操作、分析等常见运维自动化能力沉淀为标准化服务； b）提供统一的服务目录，支持用户按需、自助获得服务。	a）兼容开源生态指标、链路等监控标准，对符合规范系统能够无侵入快速对接； b）兼容应用范围较广的一些“事实标准”，对客户已有系统能够快速迁移，实现平台统一。
G3	a）提供标准的 API，供外部系统调用，API 管控具备全面的风险防范能力； b）具备集中管理 API 的能力，提供服务接口申请、调试和使用等功能； c）实现所有 API 接口调用的实时管控，具备接口编排能力，实现快速交付 API 接口； d）利用开放 API 的运营数据，实现 API 研发、调用、控制的智能化管理。	a）将监控、流程、操作、分析等常见运维自动化能力沉淀为标准化服务； b）提供统一的服务目录，支持用户按需、自助获得服务； c）具备对服务进行统一管控，支持对服务进行组件化编排，达到服务可共享、可复用、可编排； d）提供开放式的服务平台，全面支持自动化工具平台生态； e）利用服务开放的运营数据，实现平台研发、调用、控制的智能化管理。	a）兼容开源生态指标、链路等监控标准，对符合规范系统能够无侵入快速对接； b）兼容应用范围较广的一些“事实标准”，对客户已有系统能够快速迁移，实现平台统一； c）兼容行业通用标准，平台设计具备灵活的扩展性，能够适配兼容。

8.3　安全设计及可控性

8.3.1　安全设计

安全设计成熟度从认证与授权、通信安全、数据安全、行为审计、攻击防范五个方面进行评估：

——认证与授权：运维自动化工具平台通过有效的用户身份鉴别，进行细颗粒度的自主访问控制，可防范未授权访问、网络攻击访问、越权访问等常见安全风险；

——通信安全：运维自动化工具平台通过平台内外部的身份校验，确保数据传输的完整性和保密性；

——数据安全：运维自动化工具平台通过落地数据安全的相关措施，实现自身关键数据的安全存储和处理，实现数据的保密性；

——行为审计：运维自动化工具平台通过对用户行为记录的审计和分析，及时对违规操作进行处置；

——攻击防范：运维自动化工具平台通过输入验证、输出编码等技术，实现自身的安全防御。

攻击防范成熟度要求见表 15。

表 15　安全设计成熟度等级要求

等级	认证与授权	通信安全	数据安全	行为审计	攻击防范
G1	支持基本的用户身份鉴别和访问控制，可有效防范未授权访问。	a）支持完整性校验机制，实现对通信网络数据传输完整性的保护； b）各通信节点间应采用具有网络可信连接保护功能的技术，在节点连接网络时，对源和目标节点身份进行可信验证。	应采用校验机制，检验存储的关键数据的完整性，以确保其完整性未被破坏。	应记录系统的相关安全事件，具备较完整的审计信息，具备对审计信息进行查询、分析、报警等能力。	功能与架构安全应具备防御基本安全攻击的能力，确保平台的健壮性。
G2	a）具备全面的用户身份鉴别和访问控制，可全面防范未授权访问； b）具备对异常认证的安全处理机制； c）具备采用口令、密码技术、生物特征等两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护； d）具备完整的安全策略控制能力，可创建、分配访问操作权限。	a）支持完整性校验机制，实现对通信网络数据传输完整性的保护； b）各通信节点间应采用具备网络可信连接保护功能的技术，在节点连接网络时，对源和目标平台身份、执行程序进行可信验证，并形成相应的审计记录； c）支持加密机制，保证通信过程中数据的保密性。	a）应采用校验机制，检验存储的关键数据的完整性，以确保其完整性未被破坏； b）应采取冗余架构或分布式架构设计，支持数据多副本存储和快速恢复。	a）应记录系统的相关安全事件，具备较完整的审计信息线上化管理的能力，具备对审计信息进行查询、分析、报警等能力； b）应为安全管理中心提供接口，对安全审计进行统一管理。	a）功能与架构安全应具备全面防御安全攻击的能力，确保平台的健壮性； b）应具备与第三方安全平台联动的功能。
G3	a）具备全面的用户身份鉴别和自主访问控制能力，可全面防范未授权访问； b）具备对异常认证的安全处理机制； c）具备采用口令、密码技术、生物特征等两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护； d）具备完整的安全策略控制能力，可创建、分配访问操作权限，访问控制的颗粒度应达到主体为用户级，客体为文件和数据库表级； e）具备对平台认证与授权层面进行实时安全分析、风险预测等能力。	a）支持完整性校验机制，实现对通信网络数据传输完整性的保护； b）各通信节点间应采用具备网络可信连接保护功能的技术，在节点连接网络时，对源和目标平台身份、执行程序进行可信验证，并形成相应的审计记录； c）支持加密机制，保证通信过程中数据的保密性； d）具备对平台通信层面进行实时安全分析、风险预测等能力。	a）应采用校验机制，检验存储的关键数据的完整性，以确保其完整性未被破坏； b）应采取冗余架构或分布式架构设计，支持数据多副本存储和快速恢复； c）支持保密性保护机制，对存储和处理的关键数据进行保密性保护； d）具备对平台数据安全层面实时安全分析、风险预测等能力。	a）应记录系统的相关安全事件，具备完整的审计信息线上化管理的能力，具备对审计信息进行查询、分析、报警等能力； b）应为安全管理中心提供接口，对安全审计进行统一管理； c）具备安全审计数据的实时采集、处理和分析能力，具备对平台用户行为的分析、预测等能力。	a）功能与架构安全具备全面防御安全攻击的能力，确保平台的健壮性； b）应具备与第三方安全平台联动的功能； c）应具备智能的主、被动安全防御的能力，及时发现并阻断恶意入侵和用户异常操作。

8.3.2 安全可控性

安全可控性成熟度从运行可控和研发可控两个方面进行评估：

——运行可控：组织为降低在平台部署、实施、日常运行维护过程中对特定厂商或人员的依赖，宜建立的安全运作机制；

——研发可控：运维自动化工具平台需具备的开放定制性，以及组织为降低研发过程中对特定厂商和人员的依赖，宜掌握的研发技术。

安全可控性成熟度等级要求见表 16。

表 16 安全可控性成熟度等级要求

等级	运行可控	研发可控
G1	a) 工具平台具备基本的可维护性，架构可控，日志规范，文档完备； b) 运维组织具备基本的工具平台运维能力。	a) 工具平台具备开放性和可定制性； b) 供应商可对运维工具场景的定制开发提供技术支撑和交付能力； c) 运维组织具备基本的脚本、流程和组件的开发能力。
G2	a) 工具平台具备完善的可维护性，架构清晰，架构依赖可控、可扩展； b) 工具平台日志规范，文档完备，版本兼容性好，系统性能可控； c) 运维组织具备全面的工具平台运维能力； d) 工具平台的运行监控、健康巡检、架构依赖拓扑、日志集中管理、扩缩容操作、终端（含代理）版本发布、性能管理、应急预案管理等应全面实现线上化管理，部分实现脚本化和自动化。	a) 工具平台具备开放性和可定制性； b) 供应商可对运维工具场景的定制开发提供技术支撑和交付能力； c) 运维组织具备自主的脚本、流程和组件的开发能力，可基于平台对运维工具及场景实施自主研发； d) 运维组织的研发过程可控，可对运维工具及场景的开发进度、质量、成本、风险进行线上化管理，实现工具的持续交付。
G3	a) 工具平台具备完善的可维护性，架构清晰，架构依赖可控、可扩展； b) 工具平台日志规范，文档完备，版本兼容性好，系统性能可控； c) 运维组织具备全面的工具平台运维能力； d) 工具平台的运行监控、健康巡检、架构依赖拓扑、日志集中管理、扩缩容操作、终端（含代理）版本发布、性能管理、应急预案管理等应全面实现线上化管理，部分实现脚本化和自动化； e) 工具平台的运行数据可统一输出至大数据平台，具备实时分析、风险预测等能力，有效应对系统风险，提升平台稳定性和业务连续性； f) 工具平台可为平台运营人员提供运营数据，推动工具的持续迭代和落地推广。	a) 工具平台具备开放性和可定制性； b) 供应商可对运维工具场景的定制开发提供技术支撑和交付能力； c) 运维组织具备自主的脚本、流程和组件的开发能力，可基于平台对运维工具及场景实施自主研发； d) 运维组织的研发过程可控，可对运维工具及场景的开发进度、质量、成本、风险进行线上化管理，实现工具的持续交付； e) 运维组织的研发过程可量化，可进行主动的研发效能分析，持续提升研发效能。

9 组织管理

9.1 组织管理

9.1.1 组织架构设计

组织架构设计成熟度从职能设置、职能协同、架构优化三个方面进行评估：

——职能设置：组织内的角色与岗位设置，人员配备要求；

——职能协同：组织内各角色与岗位的职责划分及分工协作；

——架构优化：组织根据业务发展对组织架构自身的持续优化。

组织架构设计成熟度等级要求见表 17。

表 17 组织架构设计成熟度等级要求

等级	职能设置	职能协同	架构优化
G1	组织中具备基本的运维自动化角色，至少包括：产品设计、测试验证、自动化执行、平台管理以及审计等角色。	a) 组织内各角色、岗位职责清晰，有明确的风险防患和应急处置机制； b) 组织内形成较为清晰的自动化变更流程。	定期对组织架构中运维自动化相关角色职责、人员配备等情况进行回顾并对识别出的问题及风险进行改进。
G2	a) 组织中具备完善的运维自动化角色，至少包括产品设计、运维开发、测试验证、自动化执行、平台管理、平台运营和审计等角色； b) 组织人员配置满足必要的角色分离和互斥要求； c) 充分考虑了人员风险，对于关键岗位人员设置备岗，确保人员调整对运维自动化的负面影响可控。	a) 组织内各角色、岗位职责清晰，相互制约，有明确的风险防患和应急处置机制； b) 组织内形成较为清晰的组织流程，包括需求管理流程、变更发布流程、事件管理流程、问题管理流程； c) 各团队各司其职，按照规则和流程进行协作。	a) 定期对组织架构中自动化相关角色职责、人员配备等情况进行回顾并对识别出的问题及风险进行改进； b) 定期对组织间的协同情况，包括流程合理性、协同效率、执行情况等进行回顾并持续优化改进。
G3	a) 组织中具备完善的运维自动化角色，至少包括产品设计、运维开发、测试验证、自动化执行、平台管理、平台运营和审计等角色； b) 组织人员配置满足必要的角色分离和互斥要求； c) 充分考虑了人员风险，对于关键岗位人员设置备岗，确保人员调整对运维自动化的负面影响可控； d) 设置实体职能组织，全面负责运维自动化的规划、建设和运营工作； e) 组织中的运维人员以自动化相关的团队和人员为主。	a) 组织内各角色、岗位职责清晰，有明确的风险防患和应急处置机制； b) 组织内形成较为清晰的组织流程，包括需求管理流程、变更发布流程、事件管理流程、问题管理流程、服务管理流程； c) 各团队各司其职，按照规则和流程进行协作，将组织间的协作纳入量化评价体系； d) 组织内成员有很强的合作意识和全局意识，各部门之间协作高效，并定期积极组织沟通与分享会议。	a) 定期对组织架构中自动化相关岗位职责、人员配备等情况进行回顾并对识别出的问题及风险进行改进； b) 定期对组织间的协同情况，包括流程合理性、协同效率、执行情况等进行回顾并持续优化改进； c) 结合组织目标，定期对团队规模、职能进行主动规划。

9.1.2 组织目标管理

组织目标管理成熟度从目标制定、目标执行、目标考核三个方面进行评估：
——目标制定：运维自动化能力在组织目标中的设定方式和范围；
——目标执行：运维自动化能力在组织目标中分解以及各部门间的协作；
——目标考核：运维自动化能力的考核指标、考核频率以及考核结果应用。
组织目标管理成熟度等级要求见表 18。

表 18 组织目标管理成熟度等级要求

等级	目标制定	目标执行	目标考核
G1	组织具有短期、小范围的运维自动化能力建设目标、规划。	组织对运维自动化能力建设目标进行了较为清晰合理分解，并具备明确的执行角色。	a) 根据组织目标，结合职能与岗位设置，将运维自动化风险控制情况作为组织的考核指标； b) 管理者定期对部门及员工进行考核。
G2	a) 组织具有中长期的运维自动化能力建设目标、规划； b) 组织将运维自动化能力建设作为部门的重要目标之一； c) 组织具有统一的目标管理方法，通过上下级沟通确定运维自动化目标。	a) 组织对运维自动化能力建设目标进行了较为清晰合理的分解，并具备明确的执行角色； b) 通过有效的沟通、协作机制确保运维自动化能力建设目标的达成。	a) 根据组织目标，结合职能与岗位设置，将运维自动化风险控制情况、应急能力、覆盖率等作为组织的考核指标； b) 管理者定期对部门及员工进行考核。
G3	a) 组织具有中长期全局的自动化能力建设目标、规划，在运维自动化、研发运维一体化能力的基础上，大力发展业务流程处理自动化，实现企业内部管理和对外服务的降本增效，高效运作； b) 组织将运维自动化能力建设作为部门的重要目标之一； c) 组织具有统一的目标管理方法，通过上下级沟通确定运维自动化目标。	a) 组织对于全局的自动化能力建设目标进行了较为清晰合理的分解，并具备明确的执行角色； b) 通过有效的沟通、协作机制确保全局自动化能力建设目标的达成。	a) 根据组织目标，结合职能与岗位设置，将运维自动化风险控制情况、应急能力、覆盖率等作为组织的考核指标； b) 公司根据业务和管理目标，将业务流程自动化的风险控制情况、应急能力、业务流程处理自动化覆盖率等作为业务部门的考核指标； c) 管理者定期对部门及员工进行考核。

9.1.3 人员能力管理

人员能力管理成熟度从专业技能、专业培训、人才储备三个方面进行评估：
——专业技能：组织内部人员对于运维自动化专业技能的掌握程度；
——专业培训：组织内部进行运维自动化专业培训的目标、范围以及相关性；
——人才储备：组织内部运维自动化专业人员的储备以及稳定性。
人员能力管理成熟度等级要求见表 19。

表 19　人员能力管理成熟度等级要求

等级	专业技能	专业培训	人才储备
G1	组织内成员具备支持运维自动化活动的基本专业技能。	a）组织内成员的专业培训以运维自动化领域的管理、操作、配置等基本培训为主； b）培训对象主要为产品设计、测试验证、自动化执行、平台管理等角色。	具备合理的运维自动化安全运行相关角色的人员储备。
G2	组织内成员拥有全面、深入的运维自动化专业技能，实现对运维自动化领域的全覆盖。	a）组织内成员的专业培训以培养运维自动化领域专家为目标； b）培训对象扩展至部门使用运维自动化的所有角色。	具备足量的运维自动化相关的各角色的人员储备。
G3	a）组织内成员拥有全面、深入的运维自动化专业技能，实现对运维自动化领域的全覆盖； b）拥有自动化领域专家，对行业起到引领和带动作用，促进行业运维自动化的发展。	a）组织内成员的专业培训以培养运维自动化领域专家为目标； b）组织内成员能通过培训的方式对技术和业务部门宣导运维自动化技术； c）培训对象扩展至公司所有使用运维自动化工具平台的人员。	具有完备、充足的运维自动化人才梯队，且储备了专家人才。

9.1.4　文化管理

文化管理成熟度从协作文化、赋能文化、持续改进文化三个方面进行评估：

——协作文化：运维自动化扩展到 IT 组织、全公司范围进行协作的程度；

——赋能文化：通过组织内外部赋能以及跨组织赋能，利用运维自动化实现降本增效，高效运作的程度；

——持续改进文化：组织内对于运维自动化实施持续改进的程度。

文化管理成熟度等级要求见表 20。

表 20　文化管理成熟度等级要求

等级	协作文化	赋能文化	持续改进文化
G1	组织内部具备基本的协作流程，各角色按规章和流程协作。	在运维自动化能力的赋能方面，主要以运维工具平台厂商向组织赋能为主。	具备基本的运维自动化效果评价标准和考核指标。
G2	a）组织内部具备完善的协作流程，各角色按规章和流程协作； b）组织具备清晰全面的运维自动化协作流程，在组织范围内形成跨组织、跨领域的协作。	a）具备在运维自动化活动中鼓励员工创新的机制； b）初步具备运维工具和场景的自主研发能力，强调以组织内部跨团队赋能为主，外部厂商向组织赋能为辅，实现运维开发团队向应用运维团队赋能。	a）具备完善的运维自动化效能评估标准和考核体系； b）持续改进机制纳入运维自动化活动管理制度，并根据活动情况及时调整改进周期。

表 20　文化管理成熟度等级要求（续）

等级	协作文化	赋能文化	持续改进文化
G3	a）组织内部具备完善的协作流程，各角色按规章和流程协作； b）组织具备清晰全面的运维自动化协作流程，在组织范围内形成跨团队、跨领域的协作； c）组织外部具备清晰全面的自动化协作流程，在组织及公司范围内，形成跨技术部门、跨业务部门、跨领域的协作； d）协作文化成为组织文化组成部分，组织具备及时发现运维自动化协作过程中的障碍，持续优化协作效率的能力。	a）具备在运维自动化活动中鼓励员工创新的机制； b）具备较强的运维工具和场景的自主研发能力，在团队内部以组织内部跨团队赋能为主，外部厂商向组织赋能为辅，运维开发团队全面向应用运维团队赋能； c）赋能文化成为组织文化的组成部分，组织内部员工积极了解公司业务，实现向组织外部和业务部门的赋能，通过运维自动化技术，提升公司业务处理流程的质量和效率，实现公司内部管理和对外服务的降本增效，高效运作，实现运维自动化技术、安全风险防范与业务的深度融合。	a）具备完善的运维自动化效能评估标准和考核体系； b）持续改进机制纳入运维自动化活动管理制度中，并根据活动情况及时调整改进周期； c）持续改进成为组织文化的重要组成部分，团队和个人的日常工作和价值观以持续改进提升为目标。

10　过程管理

10.1　入库管理

10.1.1　资产入库

资产入库成熟度从策略与规程、管理流程与自动化、资产管理信息化三个方面进行评估：

——策略与规程：为确保资产入库规范、高效、稳定和安全运转而制定的一系列标准规范；

——管理流程与自动化：通过流程以及自动化方式实现资产入库的能力；

——资产管理信息化：将资产的信息进行规范化处理，实现资产信息共享与供外部消费。

资产入库成熟度等级要求见表 21。

表 21　资产入库成熟度等级要求

等级	策略与规程	管理流程与自动化	资产管理信息化
Y1	有简单的资产模型管理能力，包括制度要求及人员安排。	有简易的流程能力，主要是通过人工记录来完成。	有简单的电子表格记录资产信息。
Y2	具备可视化的资产管理能力，运维人员通过可视化界面的方式完成各类资产模型定义。	a）资产管理覆盖部分核心流程，资产具备固定唯一标识； b）对于采购或搬迁设备，具有入库或上架流程； c）上架信息与库存信息保持一致性，并具备快速维护的能力。	a）资产管理以系统维护为主； b）纳管资产相关信息，如资产编号、上架位置、分配属主资产、供应商、维保信息等； c）配套相应资产管理流程，具备资产信息导入导出及分析能力。

表 21　资产入库成熟度等级要求（续）

等级	策略与规程	管理流程与自动化	资产管理信息化
Y3	a）运维人员通过可视化界面的方式完成各类资产模型定义，且有明确模型管理职责分工； b）具备模型管理版本管理和审批行为或流程； c）具备完善的机制保证采购流程、入库流程及资产库存的相关数据一致性。	资产管理覆盖更多的流程，并同时具备全面自动化能力，如： a）资产分配自动化，资产分配可以基于资产管理平台自助完成； b）具备资产上架申请的能力，上架前置动作自动化，比如机柜分配、默认信息填充。	资产管理以平台化维护为主，流程与自动化能力结合，如： a）在资产管理流程中引入自动化管理能力； b）引入事后自动发现的能力模块，让资产管理流程更轻量化； c）建立资产资源池管理机制，分业务维度管理资源池。
Y4	a）运维人员通过可视化界面的方式完成各类资产模型定义，且有明确模型管理职责分工； b）具备模型管理版本管理和审批行为或流程； c）具备完善的机制保证采购流程、入库流程及资产库存的相关数据一致性； d）资产管理能力数据可开放给其他平台调用集成。	流程自动化能力开放化，端到端集成化，如： a）资产管理流程能力可以与后续其他运维流程对接，建立端到端管理流程； b）上架完成后，与 CMDB 平台对接，标识 CMDB 资源状态； c）数字化资产流程管理状态，按多个维度可视化，比如时间、资产类型、去向等。	资产管理能力开放化，数据化驱动，如： a）资产管理平台能力与周边能力集成连通； b）资产管理能力开放程序接口开放化，并提供严格的授权控制，其中包括资产管理、流程管理、自动化及资源池管理等； c）资产管理平台提供资产数据可视化能力，全面呈现可视化状态。
Y5	a）运维人员通过可视化界面的方式完成各类资产模型定义，且有明确模型管理职责分工； b）具备模型管理版本管理和审批行为或流程； c）具备完善的机制保证采购流程、入库流程及资产库存的相关数据一致性； d）资产管理能力可以开放给其他平台调用集成。	流程自动化能力开放化，端到端集成化，如： a）资产管理流程能力可以与后续其他运维流程对接，建立端到端管理流程； b）上架完成后，与 CMDB 平台对接，标识 CMDB 资源状态； c）数字化资产流程管理状态，按多个维度可视化，比如时间、资产类型、去向等； d）数字化度量流程和自动化过程，智能推荐资产管理流程优化点，不断提升流程与自动化能力。	资产管理能力开放化，数据化驱动，如： a）资产管理平台能力与周边能力集成连通； b）资产管理能力开放程序接口开放化，并提供严格的授权控制，其中包括资产管理、流程管理、自动化及资源池管理等； c）资产管理平台提供资产数据可视化能力，全面呈现可视化状态； d）基于资产的动态变化，自动构建资产变化模型，智能预测资产的未来需求规划。

10.2　上架管理

10.2.1　裸机交付

裸机交付成熟度从策略与规程、安装部署、交付验证三个方面进行评估：

——策略与规程：为确保裸机交付规范、高效、稳定和安全运转而制定的标准规范；
——裸机安装部署：按资源池和业务应用的环境部署需求，实现主机环境安装和交付的过程；
——设备交付：裸机完成主机环境安装并交付后，对其交付结果进行验证，验证是否达到交付标准的过程。

裸机交付成熟度等级要求见表 22。

表 22　裸机交付成熟度等级要求

等级	策略与规程	安装部署	交付验证
Y1	有简易的交付标准要求。	以人工作业方式进行安装部署。	以人工方式进行交付验证。
Y2	建立通用的设备交付标准及规范，包括操作系统版本、主机命名规则、IP 地址规范等。	通过脚本或工具实现设备环境的初级自动化作业处理，如配置和安装，包括 IP 地址自动分配、OS 自动安装、环境自动初始化。	通过脚本及工具获取初始化后的设备信息，对比验证与预期是否一致。
Y3	a) 建立通用的设备交付标准及规范，包括操作系统版本、主机命名规则、IP 地址规范等； b) 有较为详尽的标准要求，内容要求涵盖网络、存储等区域规范标准等； c) 具备安装部署的工单管理能力。	a) 具备平台化安装部署能力； b) 基于带外控制与服务安装协议，实现自动化安装，交付标准环境； c) 实现工单流程与自动化能力对接，并在服务目录中提供相关服务。	通过平台自动化工具实现交付的一致性校验，包括主机名、IP、环境配置、网络及存储配置等。
Y4	a) 建立通用的设备交付标准及规范，包括操作系统版本、主机命名规则、IP 地址规范等； b) 有较为详尽的标准要求，内容要求涵盖网络、存储等区域规范标准等； c) 具备安装部署的工单管理能力； d) 建立规范与流程的执行效果检查与定期修订机制，实现管理闭环。	a) 具备平台化安装部署能力； b) 基于带外控制与服务安装协议，实现自动化安装，交付标准环境； c) 实现工单流程与自动化能力对接，并在服务目录中提供相关服务； d) 以上能力 OpenAPI 开放化，并提供严格的授权控制，供上层自动化运维平台调用，实现自动化场景流程的端到端调度。	a) 通过平台自动化工具实现交付的一致性校验，包括主机名、IP、环境配置、网络及存储配置等； b) 交付验证能力可以基于初始化配置模板自动化完成多维验证。
Y5	a) 建立通用的设备交付标准及规范，包括操作系统版本、主机命名规则、IP 地址规范等； b) 有较为详尽的标准要求，内容要求涵盖网络、存储等区域规范标准等； c) 具备安装部署的工单管理能力； d) 建立规范与流程的执行效果检查与定期修订机制，实现管理闭环。	a) 具备平台化安装部署能力； b) 基于带外控制与服务安装协议，实现自动化安装，交付标准环境； c) 实现工单流程与自动化能力对接，并在服务目录中提供相关服务；	a) 通过平台自动化工具实现交付的一致性校验，包括主机名、IP、环境配置、网络及存储配置等； b) 交付验证能力可以基于初始化配置模板自动化完成多维验证；

表 22　裸机交付成熟度等级要求（续）

等级	策略与规程	安装部署	交付验证
		d) 以上能力 OpenAPI 开放化，并提供严格的授权控制，供上层自动化运维平台调用，实现自动化场景流程的端到端调度； e) 数字化度量安装部署过程，智能推荐安装部署过程优化点，不断提升安装部署的质量与效率。	c）数字度量交付验证过程，持续提升交付验证的效率和覆盖度，不断提升交付质量。

10.3　基础资源交付

10.3.1　计算资源交付

计算资源交付成熟度从策略与规程、部署和配置、资源交付三个方面进行评估：

——策略与规程：为确保计算资源池的标准化交付，以及安全、稳定、有效运转，满足业务当前及未来需求而制定的一系列规则、方法及技术实现方式等；

——部署与配置：计算资源池（含操作系统）的安装、部署、配置、退服下线等使用及运行过程；

注：计算资源池通过部署和配置对外提供服务。

——资源交付：需求方提出资源申请，资源管理员将计算资源提供给业务使用的过程。

计算资源交付成熟度等级要求见表 23。

表 23　计算资源交付成熟度等级要求

等级	策略与规程	部署与配置	资源交付
Y1	具备基本的资源池建设标准、基础的服务器配置标准，用户资源申请依赖于简单的约定，资源交付依赖于管理员个体。	人工完成计算资源池规划、安装配置、验证和上线。	通过手工台账进行资源交付，管理员手工分配资源。
Y2	a) 具备标准化的操作系统目录及其配置规范（含安全基线、监控标准）； b) 具备标准化的计算资源规格，以线下流程管理为主来制定和发布计算资源交付验收标准。	脚本化、工具化完成计算资源池规划、安装配置、验证和上线。	通过脚本、工具完成虚拟化资源或物理服务器的分配，并利用脚本、工具完成操作系统的安装配置、验证和上线工作。
Y3	a) 具备标准化的操作系统目录及其配置规范（含安全基线、监控标准）； b) 具备标准化计算资源规格； c) 具备服务器配置标准，及资源池的建设标准和监控标准； d) 通过平台实现资源的申请、发放、扩容、回收等管理制度。	具备统一的部署与配置平台，自动化搭建计算资源池，并完成监控的配置，手工完成测试和验证。	具备统一的管理平台，基于流程自动化完成计算资源的申请、开通、配置和交付过程。

表 23　计算资源交付成熟度等级要求（续）

等级	策略与规程	部署与配置	资源交付
Y4	a）具备标准化的操作系统目录及其配置规范（含安全基线、监控标准）； b）具备标准化的计算资源规格； c）具备服务器配置标准，及资源池的建设标准和监控标准； d）通过平台实现资源的申请、发放、扩容、回收等； e）基于管理平台，实现基于租户配额的管理规范，并具备定期分析计算资源效能的机制； f）制定并发布适配业务场景的计算资源容量评估模型、流程和交付规范； g）建立规范与流程的执行效果检查与定期修订机制，形成闭环管理。	a）具备统一的部署与配置平台，通过平台自动化实现计算资源部署和配置的测试验证工作； b）根据不同应用需求，基于统一的平台实现存储、网络资源一体化全流程自动化部署与配置。	a）具备统一的管理平台，基于流程自动化完成计算资源的申请、开通、配置和交付过程； b）建立基于配额的资源管理模式，通过集中式的管理平台，用户自助化完成资源的申请和开通； c）具备与平台资源、应用一体交付的能力。
Y5	a）具备标准化的操作系统目录及其配置规范（含安全基线、监控标准）； b）具备标准化的计算资源规格； c）具备服务器配置标准，及资源池的建设标准和监控标准； d）通过平台实现资源的申请、发放、扩容、回收等； e）基于管理平台，实现基于租户配额的管理规范，并具备定期分析计算资源效能的机制； f）基于业务场景属性，自动发布与之相适配的计算资源容量评估模型、流程和交付规范； g）建立规范与流程的执行效果检查与定期修订机制，形成闭环管理。	a）具备统一的部署与配置平台，通过平台自动化实现计算资源部署和配置的测试验证工作； b）根据不同应用需求，基于统一的平台实现存储、网络资源一体化全流程自动化部署与配置； c）基于业务需求属性，自动构建计算资源池的部署规划，智能推荐资源部署流程。	a）具备统一的管理平台，基于流程自动化完成计算资源的申请、开通、配置和交付过程； b）建立基于配额的资源管理模式，通过集中式的管理平台，用户自助化完成资源的申请和开通； c）具备与平台资源、应用一体交付的能力； d）根据不同业务需求，智能推荐资源配置，自动化实现与存储、网络资源一体化交付。

10.3.2　存储资源交付

存储资源交付成熟度从策略与规程、部署和配置、资源交付三个方面进行评估：

——策略与规程：为确保存储资源池的标准化交付，以及安全、稳定、有效运转，满足业务当前及未来需求而制定的规则、方法及技术实现方式等；

——部署与配置：存储资源池的安装、部署、配置等过程，包括存储集群、多元化分级服务（如全闪存储池、混闪存储池、机械硬盘存储池等）的标准化设计、安装调试和配置优化等；

注：存储资源通过部署和配置对外提供服务。

——资源交付：需求方提出资源申请，资源管理员将存储资源提供给业务使用的过程。

存储资源交付成熟度等级要求见表 24。

表 24　存储资源交付成熟度等级要求

等级	策略与规程	部署与配置	资源交付
Y1	具备基本的存储资源池建设标准，用户资源申请依赖于简单的约定，通过人工操作交付资源。	人工完成存储资源池规划、安装配置、验证和上线。	通过手工台账进行资源交付，管理员人工分配存储资源。
Y2	a) 具备标准化的存储资源池配置规范（含基线配置和监控配置）； b) 具备标准化存储资源规格，以线下流程管理为主制定和发布存储资源交付验收标准。	脚本化、工具化完成存储资源池规划、安装配置、验证和上线。	通过脚本、工具完成存储资源的分配，并利用脚本、工具完成存储资源交付相关工作。
Y3	a) 具备标准化的存储资源池配置规范（含基线配置和监控配置）； b) 具备标准化存储资源规格； c) 通过平台实现存储资源的申请、发放、扩容、回收等管理制度。	具备统一的部署与配置平台，自动化搭建存储资源池，并完成监控的配置，手工完成测试和验证。	具备统一的管理平台，基于流程自动化完成存储资源的申请、开通，一体化向用户交付存储资源。
Y4	a) 具备标准化的存储资源池配置规范（含基线配置和监控配置）； b) 具备标准化存储资源规格； c) 通过平台实现存储资源的申请、发放、扩容、回收等管理制度； d) 基于管理平台，实现基于租户的配额管理规范，并具备定期分析存储资源效能的机制； e) 制定并发布适配业务场景的存储资源容量评估模型，管理流程和交付规范； f) 建立规范与流程的执行效果检查与定期修订机制，形成闭环。	a) 具备统一的部署与配置平台，通过平台自动化实现存储资源的部署和配置的测试验证工作； b) 根据不同应用需求，基于统一的平台实现云计算、网络资源一体化全流程自动化部署与配置。	a) 具备统一的管理平台，基于流程自动化完成存储资源的申请、开通、配置和交付过程； b) 建立基于配额的存储资源管理模式，通过集中式的管理平台，用户自助化完成存储资源的申请和开通； c) 具备平台资源、应用一体交付的能力。
Y5	a) 具备标准化的存储资源池配置规范（含基线配置和监控配置）； b) 具备标准化的存储资源规格； c) 通过平台实现存储资源的申请、发放、扩容、回收等管理制度； d) 基于管理平台，实现基于租户的配额管理规范，并具备定期分析存储资源效能的机制； e) 基于业务场景属性，自动发布与之相适配的存储资源容量评估模型，管理流程和交付规范； f) 建立规范与流程的执行效果检查与定期修订机制，形成闭环。	a) 具备统一的部署与配置平台，通过平台自动化实现存储资源部署和配置的测试验证工作； b) 根据不同应用需求，基于统一的平台实现云计算、网络资源一体化全流程自动化部署与配置； c) 基于业务需求属性，自动构建存储资源池的部署规划，智能推荐资源部署流程。	a) 具备统一的管理平台，基于流程自动化完成存储资源的申请、开通、配置和交付过程； b) 建立基于配额的存储资源管理模式，通过集中式的管理平台，用户自助化完成存储资源的申请和开通； c) 具备平台资源、应用一体交付的能力； d) 根据不同业务需求，智能推荐存储资源配置，自动化实现计算、网络资源一体化交付。

10.3.3 网络资源交付

网络资源交付成熟度从策略与规程、部署和配置、资源交付三个方面进行评估：

——策略与规程：为确保网络基础资源的标准化交付，以及安全、稳定、有效运转，满足业务当前及未来需求而制定的规则、方法及技术实现方式等；

——部署与配置：网络基础设施的安装、部署、配置等过程，包括二三层交换与路由、四层负载均衡、域名解析、安全防护的标准化设计、安装调试、配置及优化等；

注：网络资源通过部署和配置对外提供服务。

——资源交付：按照需求进行网络基础服务的查询、分配、配置、测试与交付的过程。

网络资源交付成熟度等级要求见表 25。

表 25 网络资源交付成熟度等级要求

等级	策略与规程	部署与配置	资源交付
Y1	具备简单的标准、规范、流程，资源的部署、配置、交付依赖于管理员个体，资源申请采用邮件等线下方式开展。	人工完成资源的配置、部署、调试和上线。	通过手工台账进行资源交付，手工分配网络资源，手工完成网络配置与测试。
Y2	a) 制定与发布网络配置规范、资源管理规范； b) 制定与发布资源使用规范，及资源的申请、变更、回收流程； c) 通过系统对流程和规范进行固化，利用线上流程完成资源的申请、变更、回收。	a) 制定网络设备配置基线； b) 利用工具自动完成与网络基础环境侧部署过程相关的网络配置。	a) 利用系统管理 IP 地址、线路、端口等网络资源； b) 利用工具完成与资源交付过程相关的网络配置。
Y3	a) 制定与发布网络配置规范、资源管理规范； b) 制定与发布资源建设标准，如标准架构、容灾方案等，规范网络资源建设过程； c) 制定与发布资源使用规范，及资源的申请、变更、回收流程； d) 通过系统对流程和规范进行固化，线上流程覆盖资源的部署与配置过程。	a) 利用平台自动实现交换机、路由器的配置管理； b) 具备基本的网络拓扑自动发现与识别能力； c) 设备、线路等部分网络资源初步实现池化部署与调度。	基于统一的管理平台，具备以下能力： a) IP 地址、线路、端口等网络资源的管理； b) 按需自动分配网络资源； c) 自动完成交换机、路由器配置； d) 基于业务需求自动完成安全策略配置。
Y4	a) 制定与计算、存储等基础资源的一体化交付标准； b) 资源的部署、配置、交付各环节均具备相应的规范与流程，并通过资源管理一体化平台对标准与流程的实施过程进行规范； c) 建立规范与流程的执行效果检查与定期修订机制，形成管理闭环。	a) 利用平台自动实现各类网络设备的配置管理； b) 具备网络全场景拓扑自动发现能力； c) 全面实现网络资源的池化部署与调度； d) 根据不同应用需求，基于统一平台按业务场景进行基础资源的自动化和一体化部署与配置。	a) 基于统一管理平台自动完成网络设备配置和管理，实现自动的基于业务的安全策略交付； b) 实现网络功能服务化，形成标准服务目录； c) 实现网络资源的自助式交付及自动化验证； d) 具备基于场景编排的资源交付能力，与计算、存储资源联动，实现基础资源的一体化交付。

表 25　网络资源交付成熟度等级要求（续）

等级	策略与规程	部署与配置	资源交付
Y5	a）制定与计算、存储等基础资源的一体化交付标准； b）资源的部署、配置、交付各环节均具备相应的规范与流程，并通过资源管理一体化平台对标准与流程的实施过程进行规范； c）建立规范与流程的执行效果检查与定期修订机制，形成管理闭环； d）基于应用需求场景，自动发布与之相适配的网络资源容量评估模型、管理流程和交付规范。	a）利用平台自动实现各类网络设备的配置管理； b）具备网络全场景拓扑自动发现能力； c）全面实现网络资源的池化部署与调度； d）根据不同应用需求，基于统一平台按业务场景进行基础资源的自动化和一体化部署与配置； e）根据不同应用需求，自动构建网络资源池的部署规划，智能推荐资源部署流程。	a）基于统一管理平台自动完成网络设备配置和管理，实现自动的基于业务的安全策略交付； b）实现网络功能服务化，形成标准服务目录； c）实现网络资源的自助式交付及自动化验证； d）具备基于场景编排的资源交付能力，与计算、存储资源联动，实现基础资源的一体化交付； e）根据不同应用需求，智能推荐网络资源配置，自动化实现与计算、网络资源联动的基础资源一体化交付。

10.4　平台资源交付

10.4.1　中间件交付

中间件交付成熟度从策略与规程、部署和配置、资源交付三个方面进行评估：

——策略与规程：为确保中间件的安全、稳定、有效运转而制定的规则、方法及流程；

——部署与配置：中间件的安装、部署、配置等使用及运行过程。整个过程包括对中间件部署方式（包括手工、脚本和自动化等）的要求，对其配置的生成和维护方式，以及回滚方案等方面的要求；

——资源交付：按照申请需求对中间件指标、功能、性能、架构等进行合理评估与规划，并部署交付，按时保质满足需求的过程。

中间件交付成熟度等级要求见表26。

表 26　中间件交付成熟度等级要求

等级	策略与规程	部署与配置	资源交付
Y1	具备基本的中间件管理流程及操作规范。	a）手工安装部署； b）手工配置维护。	通过手工台账进行中间件资源交付，管理员手工配置部署资源。
Y2	a）具备体系化的中间件管理流程及操作规范，包括人员、工具、流程机制、操作规范等； b）针对各种不同需求的应用，具备相应的中间件管理流程及操作手册。	a）对中间件进行规范化部署与配置； b）利用脚本实现中间件部署与配置的部分自动化； c）可按业务需求，为中间件自动生成不同配置参数。	通过脚本、工具完成中间件资源的部署，利用脚本、工具完成中间件的配置、验证和上线工作。

表 26　中间件交付成熟度等级要求（续）

等级	策略与规程	部署与配置	资源交付
Y3	a）具备体系化的中间件管理流程及操作规范，包括人员、工具、流程机制、操作规范等； b）针对各种不同需求的应用，具备相应的中间件管理流程及操作手册； c）具备完善的中间件备份、恢复及安全防控策略； d）中间件具备良好兼容性，包括对不同操作系统、开发语言及客户端类型等的兼容性。	a）分钟级中间件部署能力； b）中间件安装、部署过程中完全实现自动化； c）中间件在线进行配置升级、维护等自动化管理； d）具备完善的中间件备份、恢复、回滚能力。	具备统一的管理平台，基于流程自动化等手段，完成中间件资源的申请、开通、配置和交付等过程。
Y4	a）具备体系化的中间件管理流程及操作规范，包括人员、工具、流程机制、操作规范等； b）针对各种不同需求的应用，具备相应的中间件管理流程及操作手册； c）具备完善的中间件备份、恢复及安全防控策略； d）中间件具备良好兼容性，包括对不同操作系统、开发语言及客户端类型等的兼容性； e）具备集群容量规划管理能力、可视化能力，以保障运行性能可靠，容量可扩展。	a）分钟级中间件部署能力； b）中间件安装、部署过程中完全实现自动化； c）中间件服务在线进行配置升级、维护等自动化管理； d）具备完善的中间件备份、恢复、回滚能力； e）具备分钟级集群部署能力； f）实现分钟级的切换、回滚。	建立基于多租户的资源管理模式，通过统一的管理平台，用户自助化完成中间件资源的申请、开通、配置和交付等过程。
Y5	a）具备体系化的中间件管理流程及操作规范，包括人员、工具、流程机制、操作规范等； b）针对各种不同需求的应用，具备相应的中间件管理流程及操作手册； c）具备完善的中间件备份、恢复及安全防控策略； d）中间件具备良好兼容性，包括对不同操作系统、开发语言及客户端类型等的兼容性； e）具备集群容量智能规划管理能力、多维度可视化能力，以保障运行性能可靠，容量可扩展。	a）分钟级中间件部署能力； b）中间件安装、部署过程中完全实现自动化； c）中间件服务在线进行配置升级、维护等自动化管理； d）具备完善的中间件备份、恢复、回滚能力； e）具备分钟级集群部署能力； f）实现分钟级的切换、回滚； g）具备智能的容量评估及自动扩缩容的能力。	a）建立基于多租户的资源管理模式，通过统一的管理平台，用户自助化完成中间件资源的申请、开通、配置和交付等过程； b）具备与 PaaS、应用一体交付的能力； c）根据不同业务需求，智能推荐资源配置，实现中间件与基础资源以及配套监控的一体化智能交付。

10.4.2 数据库交付

数据库交付成熟度从策略与规程、部署和配置、资源交付三个方面进行评估：

——策略与规程：为确保数据库的安全、稳定、有效运转而制定的规则、方法及流程；

——部署与配置：数据库的创建、维护、配置等使用及运行过程，过程包括数据库的安装调试、数据库模型的设计、数据库的监控及故障管理、数据库的配置及优化、数据库的备份与恢复等维护工作；

——资源交付：按照申请需求对数据库指标、功能、性能、安全、架构等进行合理评估与规划，并部署交付，按时保质满足需求内容。

数据库交付成熟度等级要求见表27。

表 27 数据库交付成熟度等级要求

等级	策略与规程	部署与配置	资源交付
Y1	具备基本的数据库管理流程及操作规范。	a) 手工安装部署数据库； b) 手工配置维护数据库。	通过手工台账进行数据库资源交付，管理员手工配置部署资源。
Y2	a) 具备体系化的数据库管理流程及操作规范，包括人员、工具、流程机制、操作规范等； b) 针对各种不同类型的数据库，具备相应的数据库管理流程及操作手册。	a) 利用脚本实现数据库部署与配置的部分自动化； b) 可按业务需求特点对数据库选型，并能快速部署不同类型数据库系统； c) 对数据库、表进行规范化部署和配置； d) 可进行数据库常规维护，包括建库、建表、建索引、版本维护、补丁更新。	通过脚本、工具完成数据库资源的部署，利用脚本、工具完成数据库的配置、验证和上线工作。
Y3	a) 具备体系化的数据库安全防控策略； b) 具备可实施的数据库操作手册； c) 具备良好的数据库选型策略； d) 具备完善的数据库高可用、备份及恢复策略。	a) 具备规范化的数据库部署、操作； b) 在数据库安装、配置过程中引入了大量自动化技术，可以自动化安装和配置数据库； c) 数据库部署、配置、操作具备完善详尽的部署机制，包括存储引擎、字符集、表字段等具体设置方式； d) 可进行数据库深度维护，包括索引优化、容量配置优化、Bug 修复、在线打补丁等； e) 具备完善的数据库高可用、备份、恢复、回滚机制。	具备统一的管理平台，基于流程自动化等手段，完成数据库资源的申请、开通、配置和交付等过程。

表 27　数据库交付成熟度等级要求（续）

等级	策略与规程	部署与配置	资源交付
Y4	a）具备体系化的数据库安全防控策略； b）具备可实施的数据库操作手册； c）具备良好的数据库选型策略； d）具备完善的数据库高可用、备份及恢复策略； e）具备规范的数据库容量规划，运行性能可靠，容量可扩展； f）数据库部署、操作、配置等主要依靠自动化方式实现。	a）可实现分钟级数据库切换、回滚； b）可实现数据库分钟级部署、配置； c）数据库服务具备完备的接口规范。	a）建立基于多租户的资源管理模式，通过统一的管理平台，用户自助化完成数据库资源的申请和开通； b）通过统一管理平台的流程自动化等手段，完成数据库资源的配置和交付等过程。
Y5	a）具备体系化的数据库安全防控策略； b）具备可实施的数据库操作手册； c）具备良好的数据库选型策略； d）具备完善的数据库高可用和容灾体系； e）具备规范的数据库容量规划，运行性能可靠，容量可扩展； f）数据库部署、操作、配置充分考量人工智能能力和历史变更情况等因素。	a）可实现分钟级数据库切换、回滚和容灾； b）可实现数据库分钟级部署、配置； c）数据库服务具备完备的接口规范； d）实现数据库智能分库分表、自动重新负载均衡等。	a）建立基于多租户的资源管理模式，通过统一的管理平台，用户自助化完成数据库资源的申请和开通； b）通过统一管理平台的流程自动化等手段，完成数据库资源的配置和交付等过程； c）具备与 PaaS、应用一体交付的能力； d）根据不同业务需求，智能推荐资源配置，实现数据库与基础资源以及配套监控的一体化智能交付。

10.5　云资源管理

10.5.1　多云与混合云管理

多云与混合云管理成熟度从策略与规程、资源池管理、配额及用量管理、资源交付、成本与计费五个方面进行评估：

——策略与规程：为确保多云与混合云的安全、稳定、有效运转而制定的规则、方法及流程；

——资源池管理：对 IT 资源池的管理过程，包括整体资源池的管理和多租户管理；

——配合及用量管理：对资源配额的分配及使用过程的监控与管理；

——资源交付：向用户交付资源的管理过程，包括单个资源实体交付和基于应用架构的整体资源交付；

——成本与计费：通过业务、租户等多维度，对资源使用实施的成本管理。

多云与混合云管理成熟度等级要求见表28。

表 28　多云与混合云管理成熟度等级要求

等级	策略与规程	资源池管理	配额及用量管理	资源交付	成本与计费
Y1	手工录入信息到 CMDB。	具备人工的资源池管理手段。	无资源池的配额和容量管理，按需提供资源。	资源交付以手工操作为主，登录不同的云管理控制台分配需求方所需要的资源。	以手工的方式统计资源的使用成本。
Y2	通过资源申请流程与 CMDB 接口对接，数据同步到 CMDB 中，并通过流程做好数据同步的校验。	建立了统一的资源池管理规范，按照一定的时间周期（年、季、月）检查资源池使用情况。	建立了资源池配额管理规范，按照一定的时间周期（年、季、月）检查资源配额使用情况。	构建了统一的自动化资源交付工具，IaaS 资源（如主机、存储）具备自动化交付能力。	以 Excel 表格的方式统计资源的使用成本。
Y3	a) 多云管理平台和 CMDB 平台自动对接，直接数据同步； b) 对 CMDB 的数据同步结果做好检查校验，确保数据一致性； c) 建立容量、成本、配额相关管理制度，进一步规范成本管理要求。	a) 建立了统一的资源池管理规范，按照一定的时间周期（年、季、月）检查资源池使用情况； b) 建立了规范的资源池管理流程，实行线上化管理。	a) 多云管理平台覆盖多种资源类型，包括 IaaS、PaaS 资源等； b) 主动推送资源配额及用量情况给相关责任人，确保该信息的透明化。	a) 构建统一的自动化资源交付工具，IaaS 资源（如主机、存储）具备自动化交付能力； b) 覆盖多种的 PaaS 层资源交付能力； c) 具备标准的资源交付流程。 注：不具备蓝图资源交付的能力。	a) 成本和计费具备平台化、可视化管理能力； b) 成本和计费关联到各资源类型，可按照时间周期来统计成本与计费情况。
Y4	a) 进一步解耦多云管理平台和 CMDB 资源同步接口，以消息通知的方式让 CMDB 启动资源自动发现或者同步； b) 对 CMDB 的数据同步结果做好检查校验，确保数据一致性；	a) 可结合业务、应用的趋势和容量，自动对资源池容量做好规划预测； b) 可反向结合资源使用情况（成本和用量）精细化控制多租户资源池。	a) 资源的配额和使用量可以细化管理到多租户级别（组织、业务、时间周期），并且可以根据业务容量的规划，实时调整资源配额； b) 主动推送多租户资源配额及用量情况给相关责任人，使之关注资源的有效利用；	a) 构建统一的自动化资源交付工具，具备基本资源的（如主机、存储）自动化交付能力； b) 覆盖多种的 PaaS 层资源交付能力； c) 具备标准的资源交付流程； d) 基于需求可实现多类型资源的统一交付；	a) 成本和计费具备平台化、可视化管理能力； b) 成本和计费和多租户关联，精细化到组织、业务、时间维度； c) 主动推送多租户资源的成本情况到干系人，使之关注资源成本情况；

表 28　多云与混合云管理成熟度等级要求（续）

等级	策略与规程	资源池管理	配额及用量管理	资源交付	成本与计费
	c）建立容量、成本、配额相关管理制度，进一步规范多云资源管理要求。		c）资源配额和用量与资源池规划的一致性，反向驱动资源池的规划。	e）基于应用服务、网络、主机架构的服务依赖关系交付资源。	d）结合业务、应用使用情况（成本与容量），评估资源容量使用的合理性，推动资源容量的持续优化。
Y5	a）进一步解耦多云管理平台和 CMDB 资源同步接口，以消息通知的方式让 CMDB 启动资源自动发现或者同步； b）对 CMDB 的数据同步结果做好检查校验，确保数据一致性； c）建立容量、成本、配额相关管理制度，进一步规范多云资源管理要求。	a）可结合业务、应用的趋势和容量，自动对资源池容量做好规划预测； b）可反向结合资源使用情况（成本和用量）精细化控制多租户资源池； c）基于资源池的使用历史数据，借助人工智能能力，实现更科学的资源预测管理。	a）资源的配额和使用量可以细化管理到多租户级别（组织、业务、时间周期），并且可以根据业务容量的规划，实时调整资源配额； b）主动推送多租户资源配额及用量情况给相关责任人，使之关注资源的有效利用； c）基于资源配额的使用历史数据，借助人工智能能力，实现更科学的资源池规划。	a）构建统一的自动化资源交付工具，具备基本资源的（如主机、存储）自动化交付能力； b）覆盖多种的 PaaS 层资源交付能力； c）具备标准的资源交付流程； d）基于需求可实现多类型资源的统一交付； e）基于应用服务、网络、主机架构的服务依赖关系的交付资源； f）IaaS 层云资源交付为 PaaS 容器资源调度服务弹性提供支持。	a）成本和计费具备平台化、可视化管理能力； b）成本和计费和多租户关联，精细化到组织、业务、时间维度； c）主动推送多租户资源的成本情况到干系人，使之关注资源成本情况； d）基于业务、应用使用的历史数据（成本与容量），借助人工智能能力，评估资源容量使用的合理性，推动资源容量的持续优化。

10.6 环境管理

10.6.1 环境管理

环境管理成熟度从环境类型、环境构建、环境依赖三个方面进行评估：

——环境类型：研发、测试和生产环境种类的齐备性，用于满足不同阶段业务需求的能力；

——环境构建：环境的生成方式和交付能力，从交付过程和交付效率中体现；

——环境依赖：环境所依赖内容的识别和管理方法，以及环境变更的有效跟踪反馈，用于确保环境的一致性和受控。

环境管理成熟度等级要求见表29。

表 29 环境管理成熟度等级要求

等级	环境类型	环境构建	环境依赖
Y1	环境类型只有生产和非生产环境，具备物理隔离能力。	a) 人工创建环境； b) 环境准备需要数周完成。	a) 具备离线系统依赖管理； b) 环境的管理为操作系统的交付方式。
Y2	环境类型具备研发、测试及生产环境的划分，包括预发布等，同时具备物理隔离能力。	a) 通过脚本创建环境； b) 环境准备时间需要数天完成。	a) 通过配置管理工具实现操作系统级别的依赖管理，包括操作系统版本、组件版本、程序包版本； b) 环境的管理为操作系统的交付方式。
Y3	环境类型具备研发、测试及生产环境的划分，包括预发布、功能及性能测试环境等，同时具备物理隔离能力及 ACL 控制能力。	a) 环境构建通过自动化来完成； b) 环境准备时间以天为单位； c) 具备构建过程安全特征检测能力； d) 环境的构建可以通过容器化等快速交付； e) 具备自定义流程管控能力，底层镜像安全更新通知。	a) 具备快照、镜像复制操作系统的交付能力； b) 具备容器交付能力； c) 通过配置管理工具进行应用版本依赖管理，实现环境一致性。
Y4	a) 环境类型具备研发、测试及生产环境的划分，包括预发布、功能测试、性能测试及标准研发环境等，同时具备物理隔离能力及 ACL 控制能力； b) 在创建研发测试环境时，自动创建相关灾备环境。	a) 环境构建通过自动化来完成； b) 环境准备时间为小时级； c) 具备构建过程安全特征检测能力； d) 环境的构建可以通过容器化等快速交付； e) 具备自定义流程管控能力，底层镜像安全更新通知；	以应用为中心，具备服务级依赖的配置管理能力，包括依赖的关联服务，数据库服务、缓存服务、关联应用服务。

表 29　环境管理成熟度等级要求（续）

等级	环境类型	环境构建	环境依赖
		f）环境的构建通过自服务的资源交付平台来完成。	
Y5	a）环境类型具备研发、测试及生产环境的划分，包括预发布、功能测试、性能测试及标准研发环境等，同时具备物理隔离能力及ACL控制能力； b）建立全面的测试与灰度环境包括开发环境，技术测试及业务测试环境以及灰度发布环境； c）根据业务与应用的需要，弹性分配各类环境，并具备完善的灾备策略。	a）环境构建通过自动化来完成； b）环境准备时间为分钟级； c）具备构建过程安全特征检测能力； d）环境的构建可以通过容器化等快速交付； e）具备自定义流程管控能力，底层镜像安全更新通知； f）环境的构建通过自服务的资源交付平台来完成； g）环境根据业务及应用架构弹性构建。	a）环境和依赖配置管理实现代码化描述； b）环境和依赖配置可以做到实例级的动态配置管理能力，根据业务和应用架构弹性变化。

10.7　制品及物料管理

10.7.1　制品及物料管理

制品及物料管理成熟度从制品管理、物料管理、单一可信数据源三个方面进行评估：

——制品管理：用于管理源代码编译后的构建产物，包括支持各种包等常见制品库类型，要求在存储结构、版本号、权限控制等方面对其进行管理；

——物料管理：用于管理保证包括制品发布等运维活动正常进行所需的相应物料，如应用环境及参数配置，数据库变更脚本和不可变基础设施等；

——单一可信数据源：一种数据模型和关联模式，保证每个数据元素只存储一份，确保数据的一致性。

制品及物料管理成熟度等级要求见表30。

表 30　制品及物料管理成熟度等级要求

等级	制品管理	物料管理	单一可信数据源
Y1	构建产物分散在研发本地自行管理，由管理员手工维护。	物料分散在研发本地自行管理，由管理员手工维护。	具备基本的单一可信数据源管理，采用分散的源代码版本控制系统。

表 30　制品及物料管理成熟度等级要求（续）

等级	制品管理	物料管理	单一可信数据源
Y2	a）使用统一的制品库管理构建产物； b）制品具备清晰的存储结构及唯一的版本号，版本信息有对应源码库版本（如：git commit），以及编译时环境信息（如：语言版本、容器镜像等），做到制品可追溯； c）用脚本自动化备份，保障可用性。	a）使用统一的版本控制系统，并将全部物料纳入版本控制系统管理； b）通过脚本自动化备份保障可用性。	开发测试部署环节所用到的源代码来源于统一版本控制系统。
Y3	a）使用统一的制品库管理构建产物； b）制品具备清晰的存储结构及唯一的版本号，版本信息有对应源码库版本（如：git commit），以及编译时环境信息（如：语言版本、容器镜像等），做到制品可追溯； c）将依赖组件及所有交付制品纳入制品库管理，比如：测试报告； d）制品库读写具备清晰的权限管控制度； e）通过统一的制品库地址进行构建产物分发； f）已建立体系化的制品库管理策略，包括：备份与恢复机制、策略管理，制品库完整性与一致性保障机制。	a）使用统一的版本控制系统，并将全部物料纳入版本控制系统管理； b）具备健全的版本控制系统管理机制，包括代码库命名规范； c）已建立体系化的版本控制系统管理策略，包括备份与恢复机制、策略管理，版本控制系统完整性与一致性保障机制； d）具备专人专岗管理基础的权限模型，并具备专人专岗管理。	版本控制系统和制品库作为单一可信数据源，覆盖生产部署环节。
Y4	a）将制品管理系统作为统一纳管平台； b）制品具备清晰的存储结构及唯一的版本号，版本信息有对应源码库版本（如：git commit），以及编译时环境信息（如：语言版本、容器镜像等），做到制品可追溯； c）将依赖组件及所有交付制品纳入制品库管理，比如：测试报告； d）制品库读写具备清晰的权限管控制度； e）通过统一的制品库地址进行构建产物分发； f）已建立体系化的制品库管理策略，包括：备份与恢复机制、策略管理，制品库完整性与一致性保障机制； g）制品库支持制品晋级的分级管理并充分适用于持续交付和技术运营等场景。	a）使用统一的版本控制系统，并将全部物料纳入版本控制系统管理； b）具备健全的版本控制系统管理机制，包括代码库命名规范； c）已建立体系化的版本控制系统管理策略，包括备份与恢复机制、策略管理，版本控制系统完整性与一致性保障机制； d）具备专人专岗管理完善的权限模型； e）版本控制系统相关操作以自动化的方式实现，并充分适用于持续交付和技术运营等场景； f）具备针对版本控制系统的度量与监控机制。	单一可信数据源进一步覆盖生产环境及研发本地环境。

表 30　制品及物料管理成熟度等级要求（续）

等级	制品管理	物料管理	单一可信数据源
Y5	a）将制品管理系统作为统一纳管平台； b）制品具备清晰的存储结构及唯一的版本号，版本信息有对应源码库版本（如：git commit），以及编译时环境信息（如：语言版本、容器镜像等），做到制品可追溯； c）将依赖组件及所有交付制品纳入制品库管理，比如：测试报告； d）制品库读写具备清晰的权限管控制度； e）通过统一的制品库地址进行构建产物分发； f）已建立体系化的制品库管理策略，包括：备份与恢复机制、策略管理，制品库完整性与一致性保障机制； g）制品库支持制品晋级的分级管理并充分适用于持续交付和技术运营等场景； h）实现持续优化的制品管理机制，借助人工智能能力，实现无效制品空间的释放和清理等能力。	a）使用统一的版本控制系统，并将全部物料纳入版本控制系统管理； b）具备健全的版本控制系统管理机制，包括：代码库命名规范； c）已建立体系化的版本控制系统管理策略，包括备份与恢复机制、策略管理，版本控制系统完整性与一致性保障机制； d）具备专人专岗管理完善的权限模型； e）版本控制系统相关操作以自动化的方式实现，并充分适用于持续交付和技术运营等场景； f）具备针对版本控制系统的度量与监控机制； g）将软件生命周期的所有配置项纳入版本控制系统管理； h）可完整回溯软件交付过程满足审计要求； i）借助人工智能能力，实现无效代码空间的释放和清理等能力。	a）单一可信数据源贯穿整个研发价值流交付过程； b）在组织内部开放共享，建立知识积累和经验复用体系。

10.8　数据管理

10.8.1　数据变更管理

数据变更管理成熟度从变更过程、兼容回滚、数据监控三个方面进行评估：

——变更过程：对数据库相关信息的更新方法和实现过程；

——兼容回滚：数据变更过程所具备的向下兼容性以及变更回滚能力；

——数据监控：对数据变更过程的日志、状态、数据指标的收集分析和辅助决策的能力。

数据变更管理成熟度等级要求见表31。

表 31　数据变更管理成熟度等级要求

等级	变更过程	兼容回滚	数据监控
Y1	数据变更以脚本的形式手工完成。	a）建立初步的数据库版本管理，数据库和应用存在不兼容风险； b）备份数据不及时，需要较多的人工操作及回溯。	变更过程缺乏监控。

表 31　数据变更管理成熟度等级要求（续）

等级	变更过程	兼容回滚	数据监控
Y2	持续优化数据管理方法，提升数据管理效率，借助人工智能能力等机制，实现高危 SQL 自动识别等功能。	a）数据变更具备向下兼容性，支持保留数据的回滚操作和零停机部署； b）具备秒级、分钟级回滚恢复能力； c）自动生成可执行的回滚脚本。	具备持续监控和优化数据变更机制。
Y3	a）数据变更以脚本的形式手工完成； b）数据变更通过文档方式实现标准化。	a）建立数据库和应用的版本对应关系，并持续跟踪版本变更； b）具备全量备份和增量备份能力。	a）数据变更结果通过访问数据库进行验证； b）收集和分析数据变更日志，可实现变更问题定位。
Y4	a）通过 Web UI 实现数据库变更的操作，操作记录可回溯； b）使用自动化脚本完成数据变更； c）具备自动化 SQL 审核能力； d）数据变更作为软件发布的一个独立环节，单独实施和交付； e）将数据变更纳入持续部署流水线（而不是由 DBA 操作），经人工确认后自动完成。	a）每次数据变更同时提供明确的回滚机制，可实现一些脚本自动化，包括提供升级和回滚两个自动化脚本； b）具备冗余的（如热备份、冷备份、同城/异地灾备）、完备的全量备份和增量备份数据能力，并定期进行有效性验证； c）针对 Update、Delete 操作，自动生成可执行的回滚脚本。	a）针对不同环境和危险程度对数据变更建立分级监控机制； b）数据操作日志、变更记录保留至少 6 个月，并定期审核。
Y5	a）应用程序部署和数据库变更解耦，可单独执行； b）数据变更随应用的部署自动化完成，无需专业人员单独执行。	a）数据变更具备向下兼容性，支持保留数据的回滚操作和零停机部署能力； b）具备秒级、分钟级回滚恢复能力； c）自动生成可执行的回滚脚本。	a）对数据变更进行监控，自动发现和修复异常变更； b）具备自动化审计能力。

10.9　部署与发布管理

10.9.1　部署与发布模式

部署与发布模式成熟度从部署方式、部署过程、部署策略、部署质量、发布管理五个方面进行评估：

——部署方式：软件包部署到线上生产环境或者交付用户的过程所采用的工具和方法；

——部署过程：软件上线部署环节的实践方法以及完成部署的活动；

——部署策略：部署过程的执行频率、部署内容以及部署手段，以保证安全快速地生产部署；

——部署质量：部署活动的成功率和确保部署质量提升的机制和能力；

——发布管理：确保部署后的发布活动成功率以及确保发布质量提升的机制和能力。

部署与发布模式成熟度等级要求见表32。

表 32　部署与发布模式成熟度等级要求

等级	部署方式	部署过程	部署策略	部署质量	发布管理
Y1	以人工方式完成所有环境的部署。	具有部署规划和常见步骤相关流程。	a）具备部署策略，如部署频率以月为单位； b）部署包的功能互相不独立。	a）部署整体一次性成功概率低； b）部署无法回滚，生产问题只能在线上修复，修复时间不可控。	人工方式完成所有环境的发布。
Y2	部分部署过程通过脚本实现自动化部署。	a）具有完善的安全部署规划； b）部署过程的服务有较长的中断时间； c）具备基本的安全检测机制，如非必要端口检测。	a）具备定期部署策略，如部署频率以周为单位； b）应用和数据库部署实现分离； c）应用作为部署的最小单位。	a）一次性部署失败率中等； b）实现应用部署的回滚操作，问题可及时修复。	发布过程部分自动化，如通过自动化脚本实现发布。
Y3	制品可实现全自动化部署。	a）部署过程通过流程文档方式实现标准化； b）使用相同的过程和工具完成所有环境部署； c）部署过程中具备安全审查、检测能力，包括动态检测、静态检测、代码审查等。	a）采用定期部署策略，具备按天进行部署的能力； b）应用和环境整体作为部署的最小单位； c）应用和配置进行分离； d）基础包及应用部署环境统一规范、安全可靠，如基础包来自可信源。	a）一次性部署失败率低； b）部署活动集成自动化非功能测试，并以测试结果为部署前置条件； c）每次部署活动提供变更范围报告和测试报告。	发布实现全自动化。

表 32　部署与发布模式成熟度等级要求（续）

等级	部署方式	部署过程	部署策略	部署质量	发布管理
Y4	a）部署发布服务化，实现团队自助一键式多环境自动化部署； b）支持数据库自动化部署； c）实现应用部署和基础资源部署的打通及联动； d）实现面向业务模块的部署。	部署过程可灵活响应业务需求变化，通过合理组合实现灵活编排。	a）实现环境的自动化部署； b）采用按需部署策略，具备一天部署多次的能力； c）通过低风险的部署发布策略保证部署流程风险可控，如：蓝绿部署，金丝雀发布。	建立监控体系跟踪和分析部署过程，出现问题自动化降级回滚。	发布实现服务化，实现团队自助一键式多环境自动化发布。
Y5	a）部署发布服务化，实现团队自助一键式多环境自动化部署； b）支持数据库自动化部署； c）实现应用部署和基础资源部署的打通及联动； d）实现面向业务模块的部署； e）实现基于 AI 能力的、持续优化的部署发布模式和工具系统平台。	a）部署过程可灵活响应业务需求变化，通过合理组合实现灵活编排； b）实现智能化部署，变更可自动化触发生产环境部署过程，部署失败率极低。	a）实现环境的自动化部署； b）采用按需部署策略，具备一天部署多次的能力； c）通过低风险的部署发布策略保证部署流程风险可控，如：蓝绿部署，金丝雀发布； d）团队基于人工智能能力，自主进行安全可靠地部署和发布，失败率极低。	a）建立监控体系跟踪和分析部署过程，出现问题自动化降级回滚； b）持续优化的部署监控体系和测试体系，部署失败率维持在极低水平，借助 AI 能力，自动识别部署风险。	a）发布实现服务化，实现团队自助一键式多环境自动化发布； b）基于人工智能能力，实现持续优化的部署发布模式和工具系统平台。

10.9.2 部署流水线

部署流水线成熟度从协作模式、流水线过程、过程可视化三个方面进行评估：

——协作模式：软件从需求到上线交付各个环节中，各责任主体之间的信息传递和交互方式；

——流水线过程：软件交付过程中，各环节的流水线能力与操作过程；

——过程可视化：软件交付过程中，信息的可见程度，以及所展现数据对于业务价值的展现能力。

部署流水线成熟度等级要求见表33。

表 33 部署流水线成熟度等级要求

等级	协作模式	流水线过程	过程可视化
Y1	测试和部署仅发生在开发完成后，并且以口头线下沟通为主。	软件交付过程中的大部分工作通过手工方式完成。	a) 交付过程中的信息不开放； b) 交付状态无法追溯。
Y2	a) 存在复杂的部门间协作和等待； b) 整个软件交付过程严格遵循预先计划； c) 借助协同工具进行沟通。	软件交付过程中部分环节建立了自动化能力，提升部分环节的处理效率。	a) 交付过程在团队内部可见； b) 交付状态部分可追溯。
Y3	a) 通过定义完整的软件交付过程和清晰的交付规范，保证团队之间交付的有序； b) 团队间交付基于统一的协作平台进行，按照约定由系统间调用自动完成，仅在必要环节进行手工确认。	a) 软件交付过程中各个环节均建立自动化能力，提升各环节的处理效率； b) 打通软件交付过程中的各个环节，建立平台级、全流程的自动化能力，并根据自动化测试结果保障软件交付质量。	a) 信息在团队间共享； b) 交付状态可追溯； c) 交付过程在组织内部可见； d) 团队共享度量指标； e) 按照角色、权限分级展示可视化。
Y4	团队间依赖解耦，可实现独立安全的自主部署到非生产环境。	建立可视化部署流水线，覆盖整个软件交付过程。	a) 部署流水线全员可见； b) 对过程信息进行有效聚合分析展示趋势。
Y5	持续优化的交付团队，灵活响应业务变化，改善发布效率。	a) 部署流水线持续改进； b) 每次变更都会触发完整的自动化部署流水线。根据历史数据，结合 AI 能力，实现流水模块及模板配置的智能推荐。	借助人工智能技术，对部署流水线过程信息进行数据价值挖掘，推动业务改进。

10.10 监控管理

10.10.1 监控数据采集

监控数据采集成熟度从策略与规程、监控数据采集、监控数据传输三个方面进行评估：

——策略与规程：为确保监控数据采集过程的安全、稳定、有效运转而制定的一系列规则、方法及技术手段等；

——监控数据采集：包括监控数据采集的手段、支持的协议、兼容性、颗粒度、采集端的基础逻辑和扩展逻辑等；

——监控数据传输：包括监控数据传输的质量保障、传输的可用性、传输过程中支持的功能特性等。

监控数据采集成熟度等级要求见表34。

表 34　监控数据采集成熟度等级要求

等级	策略与规程	监控数据采集	监控数据传输
Y1	对不同系统、设备具备数据采集的措施，未形成策略与规范。	a) 具备操作系统级的监控指标采集能力，如CPU、内存、磁盘等； b) 采集过程，需要较多的人工配置。	通过标准协议传输数据，仅能传输单一格式内容。出现问题需要事后进行人工处理。
Y2	a) 具备初步的数据采集策略与规范； b) 对不同系统、设备具备对应的数据采集策略与规范。	a) 具备操作系统级的监控指标采集能力，及系统日志、应用日志、接口日志的采集能力，可支持多种采集方式，如嵌入SDK、API、私有协议等； b) 采集以自动化的形式进行。	a) 通过标准协议传输数据，可传输不同格式的数据，如int、char、binary等格式； b) 出现问题需要事后进行人工处理。
Y3	a) 具备较完善的数据采集策略与规范； b) 具备完善的安全管理策略； c) 对采集程序、采集设备的管理规范统一。	a) 具备操作系统级监控指标的采集能力，及系统日志、应用日志、接口日志的采集能力，可支持多种采集方式，如嵌入SDK、API、私有协议等； b) 量化管理采集服务，如企业应用覆盖率； c) 提供开放式、自定义的数据内容采集上报能力，采集频率可自定义配置调节，可自定义监控内容； d) 数据采集上报到多个服务端，可支持可扩展，高可用的采集架构，采集方式安全、可靠，不影响业务。	a) 通过标准协议传输数据，可传输不同格式的数据，如int、char、binary等格式； b) 单份数据多份订阅及分发传输； c) 具有高可靠数据传输通道和高可用容灾方案，支持多种传输方案，如同时具备推与拉数据，具备数据传输的完整性和安全性。

表 34　监控数据采集成熟度等级要求（续）

等级	策略与规程	监控数据采集	监控数据传输
Y4	a）具备完善的数据采集策略与规范； b）具备完善的安全管理策略； c）对采集程序、设备的管理规范统一； d）具备采集服务的管理方法，如采集范围限制、采集限频等方法； e）策略与规范可灵活满足不同的数据采集场景； f）可有效应对大规模的数据采集场景。	a）具备操作系统级监控指标的采集能力，及系统日志、应用日志、接口日志的采集能力，可支持多种采集方式，如嵌入 SDK、API、私有协议等； b）提供开放式、自定义的数据内容采集上报能力，采集频率可自定义配置调节，可自定义监控内容； c）数据采集上报到多个服务端，可支持可扩展，高可用的采集架构，采集方式安全、可靠，不影响业务； d）具备采集管控、发送延迟、数据校验、统计等管理能力，可通过插件化扩展采集逻辑； e）具备统一的数据采集方式且跨平台兼容，自动化脱敏，以及大规模、自动化采集数据的能力与集中式的采集配置，包括但不限于采集内容、开关等。	a）通过标准协议传输数据，可传输不同格式的数据，如 int、char、binary 等格式； b）单份数据多份订阅及分发传输； c）具有高可靠数据传输通道和高可用容灾方案，支持多种传输方案，如同时具备推与拉数据，具备数据传输的完整性和安全性； d）数据采集架构具备平行扩展数据汇聚和高效传输等能力； e）具备大量数据的并发传输能力，保证数据传输质量，全程加密数据传输。
Y5	a）具备完善的数据采集策略与规范； b）具备完善的安全管理策略； c）对采集程序、设备的管理规范统一； d）策略与规范可灵活满足不同的数据采集场景； e）具备采集服务的管理方法，如采集范围限制、采集限频等方法； f）可有效应对大规模的数据采集。	a）具备操作系统级监控指标的采集能力，及系统日志、应用日志、接口日志的采集能力，可支持多种采集方式，如嵌入 SDK、API、私有协议等； b）支持提供开放式、自定义的数据内容采集上报方式，采集频率可自定义配置调节，可自定义监控内容； c）数据采集上报到多个服务端，支持可扩展，高可用的采集架构，采集方式安全、可靠，不影响业务； d）具备采集管控、发送延迟、数据校验、统计等管理能力，可通过插件化扩展采集逻辑； e）具备统一的数据采集方式且跨平台兼容，自动化脱敏，以及大规模、自动化采集数据的能力与集中式的采集配置，包括但不限于采集内容、开关等； f）数据采集规则通过智能技术动态调整，支持与技术运营活动联动，支持关联运维事件，采集对象包含全流程物联网和互联网等。	a）通过标准协议传输数据，可传输不同格式的数据，如 int、char、binary 等格式； b）单份数据多份订阅及分发传输； c）具有高可靠数据传输通道和高可用容灾方案，支持多种传输方案，如同时具备推与拉数据，具备数据传输的完整性和安全性； d）数据采集架构具备平行扩展、数据汇聚和高效传输等能力； e）具备大量数据的并发传输能力，保证数据传输质量，全程加密数据传输； f）支持物联网、互联网多渠道、多元化数据传输与汇集。

10.10.2 监控数据处理

监控数据处理成熟度从策略与规程、监控数据接收、监控数据加工、监控数据存储四个方面进行评估：

——策略与规程：为确保监控数据管理过程的安全、稳定、有效运转而制定的一系列规则、方法及流程；

——监控数据接收：从数据源端（主动或被动）收集传输过来的监控数据，可支持各种传输协议，并且具备良好的数据格式兼容性，拥有良好的吞吐性能和可扩展性；

——监控数据加工：对监控数据进行清洗、转换、统计、分析等处理，支持逻辑运算、统计方法、机器学习等计算能力，可基于业务场景，灵活实现数据的扩展与智能关联分析；

——监控数据存储：对监控数据的存储，可从存储的方案、架构、存储成本、数据高可用等方面进行综合评估。

监控数据处理成熟度等级要求见表35。

表 35 监控数据处理成熟度等级要求

等级	策略与规程	监控数据接收	监控数据加工	监控数据存储
Y1	对数据具备简单的分类策略和处理措施。	可收集主要目标系统或设备的数据。	对数据具备一定的统计和追溯能力。	具备基本的数据存储能力。
Y2	a) 具备基本的数据管理策略与规范； b) 具备基本的数据分类与分级。	具备收集所有目标系统、设备及异构数据源数据的能力。	a) 具备数据预处理、异常数据识别与校对的能力； b) 具备异构数据源数据简单处理能力，如打标签，做分类，格式化。	a) 支持同构及异构数据的存储； b) 支持多种数据类型存储，如文本、数值型和位图等，支持时序数据的存储。
Y3	a) 具备完善的数据管理策略与规范； b) 数据管理系统架构设计合理、有效、可扩展强； c) 数据接收、加工和存储具备完善的安全机制。	a) 具备收集所有目标系统、设备及异构数据源数据的能力； b) 具备数据筛选过滤、原始数据的规则化处理和数据校验的能力； c) 数据接收架构具备可维护性和高扩展性。	a) 具备数据预处理、异常数据识别与校对的能力； b) 具备异构数据源数据简单处理能力，如打标签，做分类，格式化； c) 具备监控数据全面分类分级、常用逻辑运算及ETL能力； d) 数据加工具备可扩展的架构能力； e) 具备数据校正、数据持久化能力，保证数据加工的完整性。	a) 支持同构及异构数据的存储，支持分类分级数据存储，支持冷热数据分离存储； b) 支持多种数据类型存储，支持时序数据的存储及统计； c) 数据存储架构具备高可扩展性、高可用性和高安全性。

表 35　监控数据处理成熟度等级要求（续）

等级	策略与规程	监控数据接收	监控数据加工	监控数据存储
Y4	a）数据管理策略与规范具备持续更新迭代能力； b）具备海量数据高效、低风险且高质量管理的能力。	a）具备收集所有目标系统、设备及异构数据源数据的能力； b）具备数据筛选过滤、原始数据的规则化处理和数据校验的能力； c）数据接收架构具备可维护性、高扩展性和过载保护能力； d）对外提供统一的数据上报服务，动态管理数据接收容量与吞吐性能。	a）具备数据预处理、异常数据识别与校对、数据校正和数据持久化的能力； b）具备对同构/异构数据源的处理及关联分析的能力； c）具备监控数据全面分类分级、常用逻辑运算及 ETL 能力； d）具备处理结构化与半结构化数据、数据处理过程的监控和告警能力； e）数据加工具备可扩展、实时计算与离线分析的能力，实时计算的数据处理延时小于 1 分钟。	a）支持同构及异构数据的存储，支持分类分级数据存储，支持冷热数据分离存储，具备结构化与半结构化数据的存储与快速检索能力； b）支持多种数据类型存储，支持时序数据的存储及统计； c）数据存储架构具备高可扩展性、高可用性和高安全性； d）具备数据高频查询的吞吐能力； e）具备持续优化数据存储成本的方案，可根据业务场景动态设置存储周期。
Y5	a）数据管理策略与规范具备持续更新迭代能力； b）借助智能化技术等手段，具备海量数据高效、低风险且高质量管理的能力，且可以动态调整相关策略与规程。	a）具备收集所有目标系统、设备及异构数据源数据的能力； b）具备数据筛选过滤、原始数据的规则化处理和数据校验的能力； c）数据接收架构具备可维护性、高扩展性和过载保护能力； d）对外提供统一的数据上报服务，动态管理数据接收容量与吞吐性能； e）具备数据秒级上报和海量数据的收集能力，支持高性能并发 QPS 请求量的数据接收与筛选。	a）具备数据预处理、异常数据识别与校对、数据校正和数据持久化的能力； b）具备对同构/异构数据源的处理及关联分析的能力； c）具备监控数据全面分类分级、常用逻辑运算及 ETL 能力； d）具备处理结构化与半结构化数据、数据处理过程的监控和告警能力；	a）支持同构及异构数据的存储，支持分类分级数据存储，支持冷热数据分离存储，具备结构化与半结构化数据的存储与快速检索能力； b）支持多种数据类型存储，支持时序数据的存储及统计； c）数据存储架构具备高可扩展性、高可用性和高安全性； d）具备数据高频查询的吞吐能力；

表 35　监控数据处理成熟度等级要求（续）

等级	策略与规程	监控数据接收	监控数据加工	监控数据存储
			e）数据加工具备可配置、可视化和可编排、可扩展、实时计算与离线分析的能力，实时计算的数据处理延时小于 1 分钟； f）具备灵活的数据建模能力，可关联多种数据，具备智能化数据处理能力，如智能数据分析、事件预测等。	e）具备持续优化数据存储成本的方案，可根据业务场景动态设置存储周期； f）具备海量数据的存储能力，存储模型具备支持智能化技术所需的数据集规模。

10.10.3　监控数据应用

监控数据应用成熟度从策略与规程、告警与管控、数据服务、可视化管理四个方面进行评估：

——策略与规程：为确保监控数据应用过程的安全、稳定、有效运转而制定的规则、方法及流程；

——告警与管控：对监控数据的异常识别能力，并对异常指标、日志、链路进行告警通知，以及异常逻辑判断等相关管控能力；

——数据服务：对监控数据可开放数据服务能力，为其它关联系统提供数据接口服务，供其调用和消费；

——可视化管理：多维度展现监控数据，具备灵活定制能力，并可以通过智能化与运维场景结合。

监控数据应用成熟度等级要求见表 36。

表 36　监控数据应用成熟度等级要求

等级	策略与规程	告警与管控	数据服务	可视化管理
Y1	具备简单的监控措施。	实现简单告警。	不提供数据服务。	数据图表单一化。
Y2	a）具备监控数据应用策略与规范； b）支持监控数据的分场景应用。	a）具备按照阈值规则进行异常告警的能力，具备日志、链路等文本类异常识别的告警能力； b）具备多通道发送告警信息的能力； c）具备基于告警日历（A 股日历、港股通日历等）的告警管控能力。	提供基础的数据接口服务。	具备多种在线数据图表展示的能力。

表 36　监控数据应用成熟度等级要求（续）

等级	策略与规程	告警与管控	数据服务	可视化管理
Y3	a）具备完善的监控数据应用策略与规范； b）数据应用系统架构设计合理、有效、可扩展强。	a）具备按照阈值规则进行异常告警的能力，具备日志、链路等文本类异常识别的告警能力； b）具备多通道发送告警信息和自动告警升级的能力； c）具备基于告警日历（A 股日历、港股通日历等）的告警管控能力； d）具备基于历史数据比对（根据历史数据环比、同比、历史峰值均值等比对配置告警）的告警配置能力； e）支持告警分级及简单收敛、常见告警统计分析，如告警触达率等； f）具备告警明细的记录存储和告警统计数据导出的能力； g）针对标准告警信息，关联提供标准运维操作的提示性建议。	a）提供面向应用场景的数据服务化能力； b）具备常规数据处理、按条件导出数据接口及数据迁移的能力； c）支持对外提供自定义数据查询接口。	a）具备自定义图表、场景化的在线数据查询和数据维度展开与下钻能力； b）支持提供指标强化展示的特性，如业务监控指标的重点展示； c）具备基于业务拓扑架构或调用关系的可视化能力，并可标示出监控异常点。
Y4	a）具备完善的监控数据应用策略与规范； b）数据应用系统架构设计合理、有效、可扩展强； c）监控数据应用策略与规范持续更新迭代。	a）具备监控阈值动态调整能力； b）具备多通道发送告警信息和自动告警升级的能力； c）具备基于告警日历（A 股日历、港股通日历等）的告警管控能力； d）具备基于历史数据比对（根据历史数据环比、同比、历史峰值均值等比对配置告警）的告警配置能力； e）支持告警分级及简单收敛、常见告警统计分析，如告警触达率等； f）具备告警明细的记录存储和告警统计数据导出的能力； g）具备标准化的告警关联自动化预案，实现常见技术运营场景下的故障自愈； h）具备规则化的告警关联分析、关联收敛和告警风暴管控能力。	a）提供面向应用场景的数据服务化能力； b）具备常规数据处理、按条件导出数据接口及数据迁移的能力； c）支持对外提供自定义数据查询接口、数据接口管控和常用数据安全管控； d）具备大规模数据计算的能力；支持在线自定义数据统计分析的功能，如在线 SQL 等。	a）具备数据维度展开与下钻、按条件进行数据统计与展现的能力； b）具备基于业务拓扑架构或调用关系的可视化能力，并可标示出监控异常点； c）多用户权限管理，如权限分级、支持按需申请； d）具备自定义业务视图及被关联方调用的能力； e）具备覆盖全业务的统一可视化。

表 36　监控数据应用成熟度等级要求（续）

等级	策略与规程	告警与管控	数据服务	可视化管理
Y5	a）具备完善的监控数据应用策略与规范； b）数据应用系统架构设计合理、有效、可扩展强； c）监控数据应用策略与规范持续更新迭代。	a）具备监控阈值动态调整能力； b）具备多通道发送告警信息和自动告警升级的能力； c）具备基于告警日历（A 股日历、港股通日历等）的告警管控能力； d）具备基于历史数据比对（根据历史数据环比、同比、历史峰值均值等比对配置告警）的告警配置能力； e）支持告警分级及简单收敛、常见告警统计分析，如告警触达率等； f）具备告警明细的记录存储和告警统计数据导出的能力； g）具备标准化的告警关联自动化预案，实现常见技术运营场景下的故障自愈； h）通过智能化技术等手段，支持更有效的文本规则匹配，告警风暴管控，智能根因分析，进行快速问题定位与修复。	a）提供面向应用场景的数据服务化能力； b）具备常规数据处理、按条件导出数据接口及数据迁移的能力； c）支持对外提供自定义数据查询接口、数据接口管控和常用数据安全管控； d）具备大规模数据计算的能力；支持在线自定义数据统计分析的功能，如在线 SQL 等； e）支持监控链条秒级的端到端分析与输出结果，支持智能数据推荐。	a）具备数据维度展开与下钻、按条件进行数据统计与展现的能力； b）多用户权限管理，如权限分级、支持按需申请； c）具备自定义业务视图及被关联方调用的能力； d）具备覆盖全业务的统一可视化及智能基线可视化； e）具备特定节点智能关联展示相关节点的可视化，如数据库异常的监控点，可关联展示其他架构层的异常指标。

10.10.4　服务巡检

服务巡检成熟度从策略与规程、巡检任务、巡检流程、巡检可视化四个方面进行评估：

——策略与规程：为确保巡检工作的有效运转，满足业务当前及未来需求而制定的规则、方法及技术实现方式等；

——巡检任务：完成巡检的方案计划，一般包括时间计划、人员安排、工具配置和预算计划等；

——巡检流程：为了完成巡检目标，对若干巡检对象，应用若干巡检任务的一个完整的过程；

——巡检可视化：对于巡检的任务状态、巡检过程以及巡检结果的可视化能力。

服务巡检成熟度等级要求见表37。

表 37　服务巡检成熟度等级要求

等级	策略与规程	巡检任务	巡检流程	巡检可视化
Y1	a) 建立了基本规程，管理工作有章可循； b) 巡检操作主要依靠人工，部分巡检工作通过脚本完成，脚本编写无管理要求。	a) 对重要系统设计了明确的周期性巡检任务，但未能覆盖到所有系统服务； b) 任务的调度主要依靠人工； c) 未考虑非常态巡检任务。	a) 通过纸质或电子表格来定义巡检流程； b) 通过纸质或电子表格来记录巡检结果； c) 对巡检结果的纸质文件或电子表格进行归档管理。	a) 对纸质表格缺乏统计和可视化分析； b) 对电子表格提供简单的图表分析； c) 缺乏对历史巡检结果的连续分析和趋势分析。
Y2	a) 巡检工作已实现标准化、文档化，建立了基础设施、网络通信、应用系统及安全保障的相关巡检制度； b) 推行巡检脚本和工具的使用，并建立完善的管理规范； c) 建立了巡检工作培训和审查规范。	a) 针对不同的巡检对象，采用相应的运维工具软件来定义和配置相关的巡检任务； b) 巡检基本覆盖了所有业务系统，但无法覆盖所有配置对象； c) 具备任务自动调度执行机制； d) 未考虑非常态巡检任务。	a) 定义了巡检流程模板，但各个巡检流程在不同的运维工具软件上进行流程执行和结果记录； b) 巡检流程结果依靠各个工具自身进行归档管理。	a) 巡检报告的格式、样式未统一； b) 巡检报告以电子表格为主； c) 巡检可视化集中在巡检结果可视化领域，可提供简单的统计、分析； d) 巡检报告文件可以由工具软件进行编辑整理自动生成。
Y3	a) 巡检工作流程化、体系化，基于巡检脚本和工具，制定各类巡检工作的巡检流程； b) 针对不同的巡检对象定义完备的巡检内容和指标，规定巡检频率、覆盖率等定量工作目标； c) 巡检工作的质量是可量度的，并制定相应考核办法。	a) 针对不同的巡检对象，采用相应的运维工具软件来定义和配置相关的巡检任务； b) 巡检基本覆盖了所有业务系统和所有配置对象； c) 具备任务自动调度执行机制； d) 具备非常态巡检机制，已针对同一个巡检对象定义一些非常态巡检任务； e) 非常态巡检由人工发起。	a) 定义了完整的巡检流程模板，通过一套工具来完成流程执行和结果记录； b) 对巡检流程结果进行统一归档管理； c) 报告文件可以由（版本管理）工具软件自动进行归档管理，包括审阅、查阅管理。	a) 巡检报告的格式、样式已经统一； b) 巡检报告以电子档案为主，除现场巡检外，基本无纸质文档，巡检工具可以将巡检任务、巡检过程和巡检结果进行可视化展示； c) 报告文件可以由工具软件进行编辑整理自动生成。

表 37　服务巡检成熟度等级要求（续）

等级	策略与规程	巡检任务	巡检流程	巡检可视化
Y4	a）规划建设巡检工作平台，集成自动化巡检技术能力，全面覆盖巡检规划、执行、分析和改进工作； b）可取得巡检有效性的统计数据，并通过对数据的分析，拥有识别薄弱环节以及加以改进的手段。	a）针对不同的业务应用，设计不同的巡检任务； b）巡检覆盖了所有业务系统和所有配置对象，并针对量化指标设立了健康度模型； c）设立了交易日历，可以根据交易情况设计不同的自动调度任务，并提供接口，可以供第三方系统发起巡检； d）具备非常态巡检机制，已针对同一个巡检对象定义各种非常态巡检任务； e）非常态巡检由人工发起，或临时调整自动巡检任务来适配。	a）具备自动化平台，对所有的巡检流程进行系统化的管理，包括对巡检流程的定义、启停、执行日志审计； b）定义有完整的巡检流程模板，可复用在不同业务场景； c）对巡检流程结果进行统一归档管理； d）报告文件可以由平台工具软件自动进行归档管理，包括审阅、查阅管理。	a）具备自动化平台，由系统自动生成巡检报告，提供巡检报告的管理，包括在线审阅、查阅管理、导出文件管理等功能； b）可以将巡检任务、巡检过程和巡检结果进行可视化展示； c）可使用历史数据提供复杂的统计、分析。
Y5	a）利用人工智能技术，分析巡检结果数据，持续改进巡检工作； b）利用成熟的自动化技术，自动调度执行巡检任务，实现无人值守。	a）针对不同的业务应用，设计不同的巡检任务； b）巡检覆盖了所有业务系统和所有配置对象，并通过智能算法根据业务系统历史指标趋势以及相互偏离/趋同关系，自动对健康度进行智能评估； c）设立了交易日历，可以根据交易情况设计不同的自动调度任务；并提供接口，可以供第三方系统发起巡检； d）具备非常态巡检机制，已针对同一个巡检对象定义各种非常态巡检任务； e）非常态巡检除了可以由人工发起，或临时调整自动巡检任务来适配； f）通过机器学习算法，联动 ITIL 系统、监控系统等生成智能巡检任务。	a）具备自动化平台，对所有的巡检流程进行系统化的管理，包括对巡检流程的定义、启停、执行日志审计； b）定义完整的巡检流程模板，可以适用于各样不同的业务场景； c）对巡检流程结果进行统一归档管理； d）可结合 CMDB 的设备变化，动态适应配置项的变化，智能调整巡检流程； e）通过机器学习算法，对巡检流程的执行调度进行优化，提高并发能力，缩短巡检时间。	a）具备自动化平台，由系统自动生成巡检报告，提供巡检报告的管理，包括在线审阅、查阅管理、导出文件管理等功能； b）可以将巡检任务、巡检过程和巡检结果进行可视化展示； c）可使用历史数据提供复杂的统计、分析； d）通过智能算法，提供预测性分析，并对预测性分析的正确性提供评价体系，可持续优化预测性分析。

10.11 故障管理

10.11.1 故障发现

故障发现成熟度从策略与规程、故障监控、故障分析三个方面进行评估：

——策略与规程：为确保故障发现过程及时准确、协同有序而制定的一系列规则、方法和技术实现方式等，包括ECC、一线与二线运维人员及服务台管理等；

——故障监控：发现潜在风险或故障异常的重要手段，推动故障监控的覆盖面、准确率、告警触达能力的提升，是缩短故障发现时长的关键举措；

——故障分析：强调主动运行分析，重点是围绕运行环境的日志、应用性能、网络报文、监控性能、监控报警等数据，基于海量数据计算、统计算法、可视化等技术，分析发现故障。

故障发现成熟度等级要求见表38。

表38 故障发现成熟度等级要求

等级	策略与规程	故障监控	故障分析
Y1	具备简单故障发现管理涉及的监控、服务台、值班等管理机制。	具备基础设施、硬件资源、平台软件、应用服务的可用性监控。	通过手工方式进行性能和容量等运行分析，发现潜在的运行风险。
Y2	具备ECC应急管理机制，通过线上化的方式进行值班管理、一二线管理、服务台管理、故障发现协同和信息传递等。	a) 具备基础设施、硬件资源、平台软件、应用服务的可用性监控，并支持与故障协同涉及的事件管理流程、自动化应急工具关联； b) 具备将不同监控工具的告警推送到统一监控告警系统的能力。	a) 通过流程规范的方式进行性能和容量等运行分析，发现潜在的运行风险； b) 具备日志、应用性能、监控性能等数据采集、存储、计算的能力，为运行分析提供数据支撑。
Y3	具备ECC应急管理机制，通过线上化的方式进行值班管理、一二线管理、服务台管理、故障发现协同和信息传递等。	具备基础设施、硬件资源、平台软件、应用服务、应用功能的可用性监控。	具备将不同监控工具的告警推送到统一监控告警系统的能力。
Y4	a) 具备ECC应急管理机制，通过线上化的方式进行值班管理、一二线管理、服务台管理、故障发现协同和信息传递等； b) 具备一二线管理、值班任务、监控等数字化度量能力，为持续提升故障发现能力提供数据支撑。	a) 具备基础设施、硬件资源、平台软件、应用服务、应用功能的可用性监控； b) 具备将不同监控工具的告警推送到统一监控告警系统的能力； c) 具备企业级故障管理平台，支持监控告警、工单流程、自动化工具和应急预案等功能； d) 具备故障发现的数字化度量能力，支持持续提升监控发现故障的覆盖面、及时性，降低监控发现故障的误报率。	a) 通过流程规范的方式进行性能和容量等运行分析，发现潜在的运行风险； b) 通过运行分析平台进行性能和容量等运行分析，发现潜在的运行风险，实现运行分析平台与故障管理平台的互联互通； c) 具备企业级的运维数据平台，支持包括海量日志在内的多种监控数据的采集、存储、计算、管理和消费，支持数字化度量故障发现。

表 38　故障发现成熟度等级要求（续）

等级	策略与规程	故障监控	故障分析
Y5	a）具备ECC应急管理机制，通过线上化的方式进行值班管理、一二线管理、服务台管理、故障发现协同和信息传递等； b）具备一二线管理、值班任务、监控等数字化度量能力，为持续提升故障发现能力提供数据支撑； c）基于智能化技术，具备智能化的应急指挥协同能力。	a）具备基础设施、硬件资源、平台软件、应用服务、应用功能的可用性监控； b）具备将不同监控工具的告警推送到统一监控告警系统的能力； c）具备企业级故障管理平台，支持监控告警、工单流程、自动化工具和应急预案等功能； d）具备故障发现的数字化度量能力，支持持续提升监控发现故障的覆盖面、及时性，降低监控发现故障的误报率； e）基于智能化技术，具备智能化调整监控报警基线、多维度故障发现等能力。	a）通过流程规范的方式进行性能和容量等运行分析，发现潜在的运行风险； b）通过运行分析平台进行性能和容量等运行分析，发现潜在的运行风险，实现运行分析平台与故障管理平台的互联互通； c）具备企业级的运维数据平台，支持包括海量日志在内的多种监控数据的采集、存储、计算、管理和消费，支持数字化度量故障发现；基于智能化技术，进行智能化的故障分析，具备故障预测的发现能力。

10.11.2　故障定位

故障定位成熟度从策略与规程、故障响应、故障诊断三个方面进行评估：

——策略与规程：为确保故障定位过程及时准确、协同有序而制定的一系列规则、方法和技术实现方式等；

——故障响应：在故障事件发生后，告警信息根据监控规则触达相关系统或运维人员，由运维人员或相关程序介入应急处理，对故障进行判断和定位的过程；

——故障诊断：在故障响应后，技术人员及时采取多种方式和手段，对故障进行判断和定位的过程。

故障定位成熟度等级要求见表39。

表 39　故障定位成熟度等级要求

等级	策略与规程	故障响应	故障诊断
Y1	a）具备基本的故障分类、故障定位流程和策略； b）具备基本的故障响应与诊断相关组织。	具备基本的告警系统，被动地手工应急处理故障。	通过手工方式进行故障诊断。

表 39　故障定位成熟度等级要求（续）

等级	策略与规程	故障响应	故障诊断
Y2	a）具备较为完备的故障分类、故障定位流程和策略； b）设立完整的故障响应与诊断相关组织，定义一二线团队的基本职责并和业务团队打通。	a）具备基于流程的告警系统，自助化地应急处理故障； b）具备值班接口人角色，进行 7*16 小时监控，主动响应故障事件； c）具备事件管理平台，支持基于规则的告警信息的简单收敛。	a）基础层通过信息系统进行故障诊断，仅需少量人工分析即可定位问题； b）业务层具备反映业务层面运行状况的监控，支持查看业务请求的调度情况，支持故障快速定位； c）链路层基于纵向依赖关系，基于手工和部分能力； d）实现网络等环节的故障定位和诊断。
Y3	a）具备完备的故障分类、故障定位流程和策略； b）具备 ECC 应急指挥中心，中心具备值班接口人、二线运维专家等岗位和人员，进行 7*16 小时监控，主动响应故障事件，事件处理组织扩展至外部供应商和第三方服务商等。	a）具备基于流程、平台化的告警系统，在决策支持下，自动化地应急处理故障； b）具备完整的重大故障处理预案，覆盖信息安全、舆情等场景；具备事件管理平台，支持告警信息关联收敛。	a）基础层通过信息系统进行故障诊断，支持监控系统和配置管理系统的联动，如实时更新运行状态信息； b）业务层具备反映业务层面运行状况的监控，支持查看业务请求的调度情况，支持故障快速定位； c）链路层基于纵向和横向依赖关系，使用自动化工具和历史案例等辅助手段对交易和架构的调用链进行故障的跟踪、定位和诊断； d）支持全链路、多维度集中展示故障信息，具有较高全面性、及时性和准确性。
Y4	a）具备完备的故障分类、故障定位流程和策略，借助历史故障情况，给出流程和策略的优化建议； b）具备 ECC 应急指挥中心，中心具备值班接口人、二线运维专家等岗位和人员，进行 7*24 小时监控，主动响应故障事件，事件处理组织扩展至外部供应商和第三方服务商等，借助历史故障情况给出组织的动态调整的建议。	a）具备基于流程、平台化的告警系统，在决策支持下，自动化地应急处理故障； b）具备完整的重大故障处理预案，覆盖信息安全、舆情等场景； c）具备事件管理平台，支持告警信息关联收敛； d）监控告警系统与故障处置系统打通，具备告警的自动分析和升级能力。	a）基础层通过信息系统进行故障诊断，支持监控系统和配置管理系统的联动，如实时更新运行状态信息，部分场景引入智能化技术手段，支持如智能故障预警、智能动态止损和智能调度等场景； b）业务层具备反映业务层面运行状况的监控，支持查看业务请求的调度情况，支持故障快速定位，部分场景引入智能化技术手段，支持如智能预测业务增长及下降等场景； c）链路层基于纵向和横向依赖关系，使用自动化工具、历史案例、第三方软件和脚本等辅助手段对交易和架构的调用链进行故障的跟踪、定位和诊断； d）支持全链路、多维度集中展示故障信息，具有较高全面性、及时性和准确性。

表 39　故障定位成熟度等级要求（续）

等级	策略与规程	故障响应	故障诊断
Y5	a）具备完备的故障分类、故障定位流程和策略，借助智能化技术等手段，给出流程和策略的优化建议； b）具备 ECC 应急指挥中心，中心具备值班接口人、二线运维专家等岗位和人员，进行 7*24 小时监控，主动响应故障事件，事件处理组织扩展至外部供应商和第三方服务商等，借助智能化技术等手段，给出组织的动态调整建议。	a）具备基于流程、平台化的告警系统，在决策支持下，自动化地应急处理故障； b）具备完整的重大故障处理预案，覆盖信息安全、舆情等场景； c）具备事件管理平台，支持告警信息关联收敛； d）监控告警系统与故障处置系统打通，具备告警的自动分析和升级能力；具备智能化能力，自动展示受故障影响的关键指标，对故障级别判定和相关资源调配等给出决策性建议。	a）基础层通过信息系统进行故障诊断，支持监控系统和配置管理系统的联动，全面引入智能化技术手段，支持所有关键场景故障诊断的智能化； b）业务层具备反映业务层面运行状况的监控，全面引入智能化技术手段，支持所有关键业务场景预测的智能化； c）链路层基于纵向和横向依赖关系，全面引入智能化技术手段，对交易和架构的调用链进行智能化的故障跟踪、定位和诊断，具备极高的全面性、及时性和准确性。

10.11.3　故障处置

故障处置成熟度从策略与规程、故障恢复、故障总结三个方面进行评估：

——策略与规程：为确保故障处置过程及时准确、协同有序而制定的一系列规则、方法和技术实现方式等；

——故障恢复：在故障定位诊断后，根据故障处置流程策略执行应急处置，以尽快恢复系统正常运行；

——故障总结：在事件处置恢复后，通过复盘学习与改进，从不同维度对故障进行全面分析总结，确保事后改善工作落地，持续提升故障管理经验和能力。

故障处置成熟度等级要求见表40。

表 40　故障处置成熟度等级要求

等级	策略与规程	故障恢复	故障总结
Y1	具备基本的应急响应预案。	业务发生故障后可以快速处理和恢复，恢复的方法主要是重启系统或应用程序，较大程度依赖专家经验及人工操作。	a）对于事件具备基本的记录； b）具备事后的分析和通报。

表 40　故障处置成熟度等级要求（续）

等级	策略与规程	故障恢复	故障总结
Y2	a）建立事件处理规范，根据不同事件级别具备相应的应急响应和故障处理时效； b）具备详尽的应急响应预案，准确说明启用条件，操作人和操作步骤等； c）事后可较准确的判断故障影响面。	a）当业务发生故障，根据应急预案文档，对发生故障的业务系统进行重启、回切或切换等操作； b）所有处理的事件过程均具备记录和反馈； c）设定专职团队进行事件处理，并设定事件跟进角色，对事件处理过程进行追踪和协调。	a）建立基本的事后学习改善机制，如事后复盘、案例学习等手段避免事件重复发生。根据事件处理规范的要求，可以对故障进行定级； b）事件定位可客观找到原因和责任归属； c）建立事后度量和质量文化，开展基本的度量考核工作、事件记录，关注事故数、止损时效和解决率等，并建立起奖惩制度。
Y3	a）建立事件处理规范，根据不同事件级别具备相应的应急响应和故障处理时效； b）具备详尽的应急响应预案，准确说明启用条件、操作人和操作步骤等； c）具备集中管理且及时更新的应急响应预案，具备完善的知识库，方便检索及应用； d）具备标准化的管理流程，如 IT 服务台统一接收和分发事件、最优服务资源分配、跨团队沟通协作等； e）提前对影响业务系统、平台软件、基础设施等层面的运维对象进行分析，对影响这些对象的关键 KPI 指标进行提前定义，帮助一线运维人员、二线运维专家、故障协调的决策层快速判断故障影响面。	a）业务、系统、网络类事件实现流程化自愈，可通过架构的容错能力实现部分无人化自愈的功能； b）所有处理的事件过程均具备记录和反馈； c）设定专职团队进行事件处理，并设定事件跟进角色，对事件处理过程进行追踪和协调； d）通过一站式脚本或工具高效执行预案； e）对重大事故、突发事件实施快速决策、合理止损和快速处理，保证重大、突发事件的处理效率与质量。	a）事后复盘具备正确的改善点，复杂事件能区分出主次责任和根本原因，并对复杂事件中的多个故障分别进行定级； b）执行优化改进，将改善措施进行落地和验证，验收演习必须在规定时效内完成，并进一步完善预案内容； c）通过工具平台执行度量分析、改善追踪、知识库沉淀等； d）度量关联绩效考核，驱动团队重视问题和改进优化。

表 40　故障处置成熟度等级要求（续）

等级	策略与规程	故障恢复	故障总结
Y4	a）建立事件处理规范，根据不同事件级别具备相应的应急响应和故障处理时效； b）具备详尽的应急响应预案，准确说明启用条件、操作人和操作步骤等； c）具备集中管理且及时更新的应急响应预案，具备完善的知识库，方便检索及应用； d）具备标准化的管理流程，如 IT 服务台统一接收和分发事件、最优服务资源分配、跨团队沟通协作等； e）具备对应用架构、业务功能等有综合能力的专家，在应急的情况下可以快速准确的判断故障影响面； f）引入智能技术，智能分析运行数据，智能推荐适合采用的应急预案，可结合应急预案的操作步骤进行自动化的止损操作。	a）业务、系统、网络类事件实现部分智能化自愈，可通过架构的容错能力实现部分无人化自愈的功能，如 50%以上的事件实现智能化自愈； b）所有处理的事件过程均具备记录和反馈； c）设定专职团队进行事件处理，并设定事件跟进角色，对事件处理过程进行追踪和协调； d）通过一站式脚本或工具高效执行预案； e）对重大事故、突发事件实施快速决策、合理止损和快速处理，保证重大、突发事件的处理效率与质量； f）事件处理具备平台化支撑，如预案平台的一键执行、执行结果的可视化反馈、可视化展示执行后各项数据的变化等；且绝大部分的预案可授权一线直接处理。	a）事后复盘具备正确的改善点，复杂事件能区分出主次责任和根本原因，并对复杂事件中的多个故障分别进行定级； b）执行优化改进，将改善措施进行落地和验证，验收演习必须在规定时效内完成，并进一步完善预案内容； c）通过工具平台执行度量分析、改善追踪、知识库沉淀等； d）度量关联绩效考核，驱动团队重视问题和改进优化； e）事后复盘总结可以自动化形成知识、规则库并智能化应用到后续故障无人化自愈机制中； f）具备智能化分析能力，通过持续的信息输入，提前给出潜在风险的预判。
Y5	a）建立事件处理规范，根据不同事件级别具备相应的应急响应和故障处理时效； b）具备详尽的应急响应预案，准确说明启用条件、操作人和操作步骤等；具备集中管理且及时更新的应急响应预案，具备完善的知识库，方便检索及应用； c）具备标准化的管理流程，如 IT 服务台统一接收和分发事件、最优服务资源分配、跨团队沟通协作等； d）引入智能技术，利用已有关键 KPI 指标，智能判断故障影响面； e）引入智能技术，智能分析运行数据，智能推荐适合采用的应急预案，可结合应急预案的操作步骤进行自动化的止损操作。	a）业务、系统、网络类事件实现智能化自愈，可通过架构的容错能力做到无人化自愈，如 90%以上的事件实现智能化自愈； b）所有处理的事件过程均具备记录和反馈；设定专职团队进行事件处理，并设定事件跟进角色，对事件处理过程进行追踪和协调； c）对重大事故、突发事件实施快速决策、合理止损和快速处理，保证重大、突发事件的处理效率与质量； d）事件处理具备平台化支撑，如预案平台的一键执行、执行结果的可视化反馈、可视化展示执行后各项数据的变化等；且绝大部分的预案可授权一线直接处理； e）借助平台和智能化手段实现秒级操作时效。	a）事后复盘具备正确的改善点，复杂事件能区分出主次责任和根本原因，并对复杂事件中的多个故障分别进行定级； b）执行优化改进，将改善措施进行落地和验证，验收演习必须在规定时效内完成，并进一步完善预案内容； c）通过工具平台执行度量分析、改善追踪、知识库沉淀等； d）度量关联绩效考核，驱动团队重视问题和改进优化； e）事后复盘总结可以自动化形成知识、规则库并智能化应用到后续故障无人化自愈机制中； f）具备智能化分析能力，通过持续的信息输入，提前给出潜在风险的预判。

10.12 连续性管理

10.12.1 备份恢复

备份恢复成熟度从数据备份、数据校验、数据恢复三个方面进行评估：

——数据备份：为防止因操作失误、系统故障等因素导致信息系统数据丢失，将数据通过一定的方法从主计算机系统的存储设备中复制到其它存储设备的过程；

——数据校验：为保障信息系统数据备份的完整性、有效性，定期对备份数据的完整性和有效性进行验证的方法；

——数据恢复：为获得历史某时段的数据，从备用系统或离线存储介质中将数据恢复，通常数据恢复是为了应急补救。

备份恢复成熟度等级要求见表41。

表 41 备份恢复成熟度等级要求

等级	数据备份	数据校验	数据恢复
Y1	具备备份设备，通过手工或脚本方式实现数据备份。	通过手工或脚本方式对备份介质数据进行有效性、完整性校验。	通过手工或脚本等方式完成备份数据的恢复。
Y2	a) 提供数据备份软件工具，实现数据在线备份管理； b) 具备线上化流程或工具登记数据备份过程的能力，能对备份过程进行记录。	a) 提供数据校验软件工具，实现对备份数据有效性、完整性的在线校验管理； b) 具备线上化流程或工具登记数据校验过程管理的能力，能对校验过程进行记录。	a) 提供备份恢复软件工具，实现对备份数据的在线恢复管理； b) 具备线上流程或工具支持数据恢复过程的管理的能力，能对校验恢复过程进行记录。
Y3	a) 构建数据中心级的集中备份系统，支持公司重要系统数据备份的统一管理； b) 数据备份过程的线上化流程管理工具、集中备份系统等可互联互通，实现流程驱动的自动化备份。	a) 数据中心级的集中备份系统支持统一、在线的数据有效性、完整性的数据校验； b) 数据校验过程的线上化流程工具、集中备份系统等可互联互通，实现流程驱动的备份数据有效性、完整性校验。	a) 数据中心级的集中备份系统支持统一、在线的数据恢复； b) 数据恢复过程的线上化流程工具、集中备份系统等可互联互通，实现在线的数据恢复。

表 41　备份恢复成熟度等级要求（续）

等级	数据备份	数据校验	数据恢复
Y4	a）构建数据中心级的集中备份系统，支持公司重要系统数据备份的统一管理； b）实现数据备份的平台化能力，并与“流程、自动化、监控”等能力进行全在线整合，将数据备份能力融入企业数据管理、系统迁移、数据归档、故障后自动备份等场景； c）集中备份管理数字化，可度量，支持数据备份能力的持续优化。	a）数据中心级的集中备份系统支持统一、在线的数据有效性、完整性的数据校验； b）实现数据校验的平台化能力与“流程、自动化、监控”等能力进行全在线整合，将数据在线校验能力融入企业数据管理、演练等场景； c）数据校验管理数字化，可度量，支持数据校验能力的持续优化。	a）数据中心级的集中备份系统支持统一、在线的数据恢复； b）实现数据恢复的平台化能力与“流程、自动化、监控”等能力进行全在线整合，将数据在线恢复能力融入企业数据管理、周末测试、故障处理、数据调阅等场景； c）数据恢复管理数字化，可度量，支持数据恢复能力的持续优化。
Y5	a）构建数据中心级的集中备份系统，支持公司重要系统数据备份的统一管理； b）实现数据备份的平台化能力，并与“流程、自动化、监控”等能力进行全在线整合，将数据备份能力融入企业数据管理、系统迁移、数据归档、故障后自动备份等场景； c）集中备份管理数字化，可度量，支持数据备份能力的持续优化； d）应用人工智能等技术，实现无人值守的数据备份管理。如：支持机器人协助进行备份的优先级、策略范围、备份介质等管理等。	a）数据中心级的集中备份系统支持统一、在线的数据有效性、完整性的数据校验； b）实现数据校验的平台化能力与“流程、自动化、监控”等能力进行全在线整合，将数据在线校验能力融入企业数据管理、演练等场景； c）数据校验管理数字化，可度量，支持数据校验能力的持续优化； d）应用人工智能等技术，实现无人值守的数据校验管理，如：根据历史数据基线自动校验数据的有效性与完整性，决策数据异常处置等。	a）数据中心级的集中备份系统支持统一、在线的数据恢复； b）实现数据恢复的平台化能力与“流程、自动化、监控”等能力进行全在线整合，将数据在线恢复能力融入企业数据管理、周末测试、故障处理、数据调阅等场景； c）数据恢复管理数字化，可度量，支持数据恢复能力的持续优化； d）应用人工智能等技术，实现无人值守的数据恢复管理。如：支持机器人协助进行数据发现、介质调取等数据恢复管理。

10.12.2　应急演练

应急演练成熟度从方案管理、过程执行、恢复验证、评估改进四个方面进行评估：

——方案管理：应急演练计划，以及描述应急演练剧本或方案的管理方法，演练的方案包括演练计划、应急预案、线上故障注入等场景的管理；

——过程执行：应急演练过程中按应急预案的描述执行演练的方法，包括已知预案的演练，以及对复盘系统故障注入的破坏性过程执行；

——恢复验证：应急处置、应急演练、生产测试后，将演练使用的环境进行恢复验证的方法，确保演练后数据完整性和服务可用性是主要验证目标；

——评估改进：应急演练后，对演练过程和效果、演练目标达成情况进行评估的方法。

应急演练成熟度等级要求见表42。

表 42　应急演练成熟度等级要求

等级	方案管理	过程执行	恢复验证	评估改进
Y1	制定演练计划，以及配套的应急预案，模拟已知故障下，验证架构高可用、协同机制、技术应急方法等完备性。	具备相关机制，根据演练计划与操作方案定期组织应急演练工作，验证应急协同、架构高可用，及系统稳定性措施。	具备相关机制，落实演练后环境恢复、系统健康验证、演练结果通报等工作。	具备相关机制，落实演练后的复盘，对演练问题有闭环的跟踪。
Y2	a）支持演练计划的申请、审批等线上化管理； b）支持演练预案的新建、修订、发布等线上化管理。	a）支持演练审批流程、演练过程时序任务线上化管理； b）对于已知应急演练方案，提供自动化工具，如切换、重启等工具。	a）支持演练恢复验证过程时序任务线上化管理； b）提供生产环境恢复的线上化、自动化工具系统，如：服务可用性、业务关键指标感知等工具。	演练过程数据化，提供在线的复盘总结模块，并支持对演练过程问题的闭环提示与跟踪。
Y3	a）实现演练计划、演练预案、线上化审批流程，以及应急演练涉及的时序任务等能力的整合； b）线上化的演练方案与方案涉及的协同、操作动作的自动化进行了关联。	a）实现演练审批流程、演练操作时序任务、操作执行过程自动化等能力的整合，支持演练过程流水线的配置编排； b）整合实时的监控、日志、性能等数据，可在线感知演练执行结果，调动演练协同。	a）实现系统恢复操作时序任务在线化，环境恢复动作与检查自动化，链路关系检查； b）整合实时的监控、日志、性能等数据，支持在线感知恢复状况。	实现演练复盘总结，问题揭示，并支持将问题跟踪与企业内的问题或风险管理系统整合。

表 42　应急演练成熟度等级要求（续）

等级	方案管理	过程执行	恢复验证	评估改进
Y4	a）提供一体化演练平台，提供全在线的演练计划、应急预案、应急协同、操作自动化等管理，对计划的执行、预案的可靠性进行量化管理； b）提供破坏性故障注入的相关应急策略库的管理。	a）一体化演练平台提供演练审批流程、演练操作时序任务、操作执行等过程的在线控制，支持演练过程流水线的配置编排，可度量，可视化，可监控； b）实现破坏性的故障注入的演练系统，发现复杂系统的架构风险，最小化爆炸半径，具备异常情况下快速终止演练的能力。	一体化演练平台提供恢复操作时序任务在线化，环境恢复动作与检查自动化，链路关系检查等，自动化执行环境恢复，在线感知运行环境状态，检测业务关键指标可用性，可根据动态基线判断恢复的正确性。	一体化演练平台支持复盘过程、环境性能、监控、日志等数据的自动化采集，形成应急演练的全方位画像，并基于数据，驱动运维、研发、测试团队的持续提升。
Y5	a）提供一体化演练平台，提供全在线的演练计划、应急预案、应急协同、操作自动化等管理，对计划的执行、预案的可靠性进行量化管理； b）提供破坏性故障注入的相关应急策略库的管理； c）应用人工智能等技术，引入应急演练的计划管理助手的机器人角色，支持从运维知识图谱感知已知预案与未知场景下应急策略的有效性。	a）一体化演练平台提供演练审批流程、演练操作时序任务、操作执行等过程的在线控制，支持演练过程流水线的配置编排，可度量，可视化，可监控； b）实现破坏性的故障注入的演练系统，发现复杂系统的架构风险，最小化爆炸半径，具备异常情况下快速终止演练的能力； c）应用人工智能等技术，引入机器人角色，实现人机协同的应急演练管理，提供全数字化的运行感知能力，支持机器人自动化演练，自动决策故障注入，实现更高效的应急演练管理。	a）一体化演练平台提供恢复操作时序任务在线化，环境恢复动作与检查自动化，链路关系检查等，自动化执行环境恢复，在线感知运行环境状态，检测业务关键指标可用性，可根据动态基线判断恢复的正确性； b）应用人工智能等技术，支持自动化流水线的恢复操作，建立动态的运行基线，提供全数字化的环境恢复后的运行感知。	a）一体化演练平台支持复盘过程、环境性能、监控、日志等数据的自动化采集，形成应急演练的全方位画像，并基于数据，驱动运维、研发、测试团队的持续提升； b）应用人工智能等技术，实现在线复盘，在线洞察问题，在线决策与跟踪演练风险问题。

10.12.3 容灾切换

容灾切换成熟度从策略与规程、切换执行、指挥协同三个方面进行评估：

——策略与规程：为确保发生信息系统灾难事件时，可按照既定要求快速、准确完成容灾切换动作，确保业务连续性目标达成所制定的规则与方法；

——切换执行：为快速、准确完成容灾切换所需配套的必要技术手段；

——指挥协同：为快速、准确完成容灾切换所需的联动指挥而配备的固定场所、技术手段及管理协同资源。

容灾切换成熟度等级要求见表43。

表 43 容灾切换成熟度等级要求

等级	策略与规程	切换执行	指挥协同
Y1	a) 具备核心业务系统基本的容灾建设要求与例行切换演练制度； b) 核心业务切换方案能满足业务连续性要求。	a) 可通过手工或脚本方式完成容灾切换，切换时效满足监管要求； b) 容灾切换技术能力覆盖核心业务系统。	无固定指挥协同场所和工具，通过事件触发临时召集人员、决策方案、现场指挥实施完成协同工作。
Y2	a) 具备完整的业务分级体系及对应分级的容灾切换要求，并通过公司或部门发文等方式进行固化； b) 各级业务切换方案满足对应的业务连续性要求。	a) 可通过工具提升容灾切换的效能，降低切换人员投入，避免切换误操作； b) 容灾切换技术能力覆盖核心业务系统。	a) 具备正式的容灾切换指挥场所和协同调度手段（如实时通信手段、签到或协调工具等）； b) 依托容灾切换场所和协同调度工具完成容灾切换的演练及正式执行。
Y3	a) 具备完整的业务分级体系及对应分级的容灾切换要求，并通过公司或部门发文等方式进行固化； b) 各级业务切换方案满足对应的业务连续性要求； c) 按照要求定期组织容灾切换工作； d) 具备平台化承载容灾切换任务分派、执行、记录、审计的能力。	a) 具备容灾切换操作平台，有效串联切换前检查、切换执行、切换后业务测试、持续监控等环节； b) 容灾切换能力覆盖所有重要信息系统。	a) 具备指挥中心作为容灾切换的专业实施场所； b) 指挥中心具备常态的指挥协同组织和人员值班响应机制； c) 指挥中心通过平台化的手段辅助人工完成召集、签到、决策、执行、观测等动作。
Y4	a) 按照要求定期组织容灾切换工作； b) 具备平台化承载容灾切换任务	a) 可根据不同的业务场景，预置对应的平台化容灾切换方案，依据实际情况完	a) 具备指挥中心作为容灾切换的专业实施场所； b) 指挥中心具备常态的指挥协同组织

表 43　容灾切换成熟度等级要求（续）

等级	策略与规程	切换执行	指挥协同
	分派、执行、记录、审计的能力； c）通过平台承载容灾切换一体化管理工作，并能持续完善容灾切换流程，确保容灾能力持续提升。	成解决方案级多系统联动切换或选择特定系统一键式切换动作； b）容灾切换能力覆盖所有重要信息系统。	和人员值班响应机制； c）指挥中心通过平台化的手段辅助人工完成召集、签到、决策、执行、观测等动作； d）指挥中心具备场景化、一体化和智能化的人员召集、调度及切换过程控制平台，有效减少流程流转环节人工参与及延迟时间。
Y5	a）按照要求定期组织容灾切换工作； b）具备平台化承载容灾切换任务分派、执行、记录、审计的能力； c）通过平台承载容灾切换一体化管理工作，并能持续完善容灾切换流程，确保容灾能力持续提升。	a）可根据业务运行指标，智能识别故障场景，自动化执行容灾切换动作，实现业务和数据无损式快速容灾切换； b）一键式或智能容灾切换技术能力覆盖所有重要信息系统。	a）建设有指挥中心作为容灾切换的专业实施场所； b）指挥中心具备常态的指挥协同组织和人员值班响应机制； c）指挥中心通过平台化的手段辅助人工完成召集、签到、决策、执行、观测等动作； d）指挥中心具备场景化、一体化和智能化的人员召集、调度及切换过程控制平台，有效减少流程流转环节人工参与及延迟时间。

10.13　调度与保障

10.13.1　流程自动化

流程自动化成熟度从流程场景设计、流程支持技术、流程安全管控三个方面进行评估：

——流程场景设计：作为流程自动化的前提，通过对流程的规则、业务执行规模、流程可行性、流程收益等要素进行评定，对现有事件、日志等进行挖掘，以发现、监控和改进实际流程；

——流程支持技术：利用自动化技术对系统场景、业务场景进行支持的能力，包括组件功能支持，流程调度支持，其他功能支持等；

——流程安全管控：依靠自动化能力，结合各种手段，对流程安全运行提供保障的过程。

流程自动化成熟度等级要求见表44。

表 44　流程自动化成熟度等级要求

等级	流程场景设计	流程支持技术	流程安全管控
Y1	依赖脚本串联，手工运行，口头约定执行顺序等实现方式，完成场景设计。	流程脚本可提供基本的执行能力，如可对进程级或文件级的操作对象进行操作，对数据库进行操作，对内存句柄级进行操作等。	依靠文档约定和人工对流程进行管控。
Y2	通过图形化编辑工具，形成模块化的脚本库支持，由组织的专业团队，进行可视化的流程编排设计。	a）流程脚本可提供基本的执行能力，如可对进程级或文件级的操作对象进行操作，对数据库进行操作，对内存句柄级进行操作等； b）流程作业平台具备丰富的执行操作设置，包括操作故障处理机制，包括重试、忽略、终止等多种操作。	通过人工在现场，采用多种自动化工具和监控工具组合完成流程管控。
Y3	a）通过图形化编辑工具，形成模块化的脚本库支持，进行可视化的流程编排设计； b）提供流程设计平台，支持团队进行线上协同设计。	a）流程脚本具备基本的执行能力，如可对进程级或文件级的操作对象进行操作，对数据库进行操作，对内存句柄级进行操作等； b）流程作业平台具备丰富的执行操作设置，包括操作故障处理机制，包括重试、忽略、终止等多种操作； c）流程作业平台具备应用级安全管理：强密码策略，严格的权限控制，包括访问控制、资源控制等； d）流程作业平台支持具备支持操作日志审计等功能。	a）通过工具以及预先的规则定义，完成无人值守的流程管控； b）支持多种告警渠道，如邮件、短信、外呼等方式，流程执行日志除文本外还可以提供截屏、录像等多种记录方式，提供存档和查验； c）具备流程执行时间范围控制能力，以及流程作业执行超时、未触发执行、执行异常终止等告警能力，同时无人值守流程具备异常时电话告警通知能力。
Y4	a）提供流程设计平台，通过图形化编辑工具，形成模块化的脚本库支持，进行可视化的流程编排设计； b）打通流程设计平台与日志监控等平台的壁垒，通过离线分析日志，提取过程模型，自动发现关联场景，并通过案例预测等方式，对流程设计功能进行扩充。	a）流程脚本具备基本的执行能力，如可对进程级或文件级的操作对象进行操作，对数据库进行操作，对内存句柄级进行操作等； b）流程作业平台具备丰富的执行操作设置，包括操作故障处理机制，包括重试、忽略、终止等多种操作； c）提供应用级安全管理：强密码策略，严格的权限控制，包括访问控制、资源控制等； d）流程作业平台支持具备支持操作日志审计等功能； e）流程自动化平台支持热备或服务器集群等高可用安全架构。	a）通过开放易扩展的平台级工具，完成无人值守的流程管控； b）具备灵活的展示、故障通知、处置能力； c）具备流程执行时间范围控制能力，以及流程作业执行超时、未触发执行、执行异常终止等告警能力，同时无人值守流程具备异常时电话告警通知能力。

表 44　流程自动化成熟度等级要求（续）

等级	流程场景设计	流程支持技术	流程安全管控
Y5	a）提供流程设计平台，通过图形化编辑工具，形成模块化的脚本库支持，进行可视化的流程编排设计； b）打通流程设计平台与日志监控等平台的壁垒，通过离线分析日志，提取过程模型，自动发现关联场景，并通过案例预测等方式，对流程设计功能进行扩充； c）引入在线分析技术，通过对流程运行情况进行建模分析，对现有的流程模型与来自该流程的事件日志作比较，完成一致性检验和过程改进。	a）流程脚本具备基本的执行能力，如可对进程级或文件级的操作对象进行操作，对数据库进行操作，对内存句柄级进行操作等； b）流程作业平台具备丰富的执行操作设置，包括操作故障处理机制，包括重试、忽略、终止等多种操作； c）提供应用级安全管理：强密码策略，严格的权限控制，包括访问控制、资源控制等； d）流程作业平台支持具备支持操作日志审计等功能； e）流程自动化平台支持热备或服务器集群等高可用安全架构； f）流程作业平台引入人工智能技术，例如文字识别技术，自然语言处理技术，自然语音识别技术等，提升流程作业平台的模型化、算法化、数据化能力。	a）通过开放易扩展并具备人工智能能力的平台级工具，完成无人值守的流程管控； b）在故障预测、弹窗理解等方面，可基于历史数据进行智能学习和适配，进一步提升流程适应能力； c）具备流程执行时间范围控制能力，以及流程作业执行超时、未触发执行、执行异常终止等告警能力，同时无人值守流程具备异常时电话告警通知能力。

10.13.2　资源调度

资源调度成熟度从资源分配、资源回收、资源监测三个方面进行评估：

——资源分配：根据用户需求，对计算、存储、网络、服务等资源进行具体分配的过程，资源分配关注资源的可用性、可靠性、交付时效性，以及在线服务的吞吐率、响应时间等指标；

——资源回收：对暂时不需要使用的资源进行回收的过程，资源回收主要包括资源消费用户需求驱动、主动性的资源使用状况分析驱动两种方式；

——资源监测：对资源运行的负载、性能、质量、安全等维度进行在线观测的方法，并针对观测结果决策应对措施。

资源调度成熟度等级要求见表45。

表 45　资源调度成熟度等级要求

等级	资源分配	资源回收	资源监测
Y1	根据用户需求，通过手工或脚本方式为用户分配需要的资源。	根据用户需求或主动分析资源负载状况，通过手工或脚本方式回收资源。	资源消费的运行对象具备对资源负载、可用性进行巡检或监控的能力。

表 45　资源调度成熟度等级要求（续）

等级	资源分配	资源回收	资源监测
Y2	a）提供在线的资源申请、审批、分配的管理系统； b）提供资源分配的工具，实现计算、存储、网络等 IaaS 层资源自动化调度工具。	a）提供在线的资源回收申请、审批、回收的管理系统； b）提供资源回收的工具，实现计算、存储、网络等 IaaS 层资源自动化调度工具。	资源消费的运行对象具备对资源负载、容量、可用性进行线上监控管理，以及提供配套的日志管理工具。
Y3	构建公司统一的 IaaS 资源管理平台，提供服务目录，支持所见即所得的 IT 资源分配管理，支持在线与动态弹性的资源分配管理。	IaaS 资源管理平台支持在线与动态弹性的资源回收管理能力。	IaaS 资源管理平台支持对分配资源对象的实际运行状况进行监控，支持日志管理，并整合应对资源不足或低效资源的自动化工具。
Y4	a）构建公司统一的 IaaS 资源管理平台，提供服务目录，支持所见即所得的资源分配管理，支持离线与动态弹性的资源分配； b）构建公司统一的 PaaS 层的资源管理平台，支持中间件、数据库、容器等资源分配管理，支持提供在线与动态弹性的资源分配； c）对资源的在线交付时效性，以及在线服务资源的吞吐率、响应时间等指标进行数字化管理，持续提升资源分配的效能。	a）IaaS 资源管理平台支持在线与动态弹性的资源回收管理能力； b）PaaS 资源管理平台支持在线与动态资源回收能力； c）对在线的资源消耗进行实时监测，洞察资源负载低的运行对象，提供资源回收的决策支持。	a）IaaS 资源管理平台支持对分配资源对象的实际运行状况进行监控，支持日志管理，并整合应对资源不足或低效资源的自动化工具； b）PaaS 资源管理平台支持对分配资源对象的实际运行状况监控，支持日志管理、链路调度管理，并整合应对资源不足或低效资源的自动化工具； c）对在线的资源运行状况进行全数字化管理，支持在线的数据洞察、决策、执行能力。
Y5	a）构建公司统一的 IaaS 资源管理平台，提供服务目录，支持所见即所得的资源分配管理，支持在线与动态弹性的资源分配； b）构建公司统一的 PaaS 层的资源管理平台，支持中间件、数据库、容器等资源分配管理，支持提供在线与动态弹性的资源分配；	a）IaaS 资源管理平台支持在线与动态弹性的资源回收管理能力； b）PaaS 资源管理平台支持在线与动态资源回收能力； c）对在线的资源消耗进行实时监测，洞察资源负载低的运行对象，提供资源回收的决策支持；	a）IaaS 资源管理平台支持对分配资源对象的实际运行状况进行监控，支持日志管理，并整合应对资源不足或低效资源的自动化工具； b）PaaS 资源管理平台支持对分配资源对象的实际运行状况监控，支持日志管理、链路调度管理，并整合应对资源不足或低效资源的自动化工具；

表 45　资源调度成熟度等级要求（续）

等级	资源分配	资源回收	资源监测
	c）对资源的在线交付时效性，以及在线服务资源的吞吐率、响应时间等指标进行数字化管理，持续提升资源分配的效能； d）应用人工智能等技术，对资源分配的可用性、可靠性进行管理，提供最佳的分配决策，支持在线、自动化的资源分配交付能力。	d）应用人工智能等技术，对资源运行状况的负载与容量进行管理，提供最佳的资源回收决策，支持在线、自动化的资源回收能力。	c）对在线的资源运行状况进行全数字化管理，支持在线的数据洞察、决策、执行能力； d）应用人工智能等技术，实现智能的监控、动态链路、日志的管理，支持动态弹性的在线、自动化的资源调度管理。

10.13.3　性能容量管理

性能容量管理成熟度从容量规划与评估、性能压测、扩缩容管理三个方面进行评估：

——容量规划与评估：根据业务需求、行情变化，结合系统运行状况，合理的规划系统容量，制定相关的容量调整方案（如扩容方案/缩容方案）；

——性能压测：根据容量调整方案，组织相关测试，验证容量调整方案与预期业务容量的匹配情况，为生产实施提供实践验证；

——扩缩容管理：根据前期的容量评估和压测，在生产环境实施扩缩容工作并确保实施完毕后的业务稳定运行，达成既定扩缩容效果。

性能容量管理成熟度等级要求见表46。

表 46　性能容量管理成熟度等级要求

等级	容量规划与评估	性能压测	扩缩容管理
Y1	a）根据业务发展需要，组织相关的容量规划与评估活动； b）容量规划与评估形成文档化的方案，指导性能容量管理工作。	a）形成文档化的性能压测方案； b）通过手工或脚本手段开展性能容量的压测活动。	通过手工操作进行扩容或缩容工作。
Y2	具备容量规划与评估的流程，并作为流程制度通过发文等形式进行固化执行。	依据压测场景，具备工具化的性能压测手段，多种工具未整合。	通过脚本自动化操作进行扩容或缩容工作。

表 46　性能容量管理成熟度等级要求（续）

等级	容量规划与评估	性能压测	扩缩容管理
Y3	通过平台承载容量的分析与评估工作，并记录和跟踪相关分析过程和结果。	a）具备较为完整统一的性能压测平台，可完成大部分的场景统一压测； b）性能压测数据化存储，并作为后续的优化依据沉淀。	a）具备扩缩容的流程化决策审批平台，并实现基于流程触发的扩缩容动作； b）具备支持扩缩容的自动化服务平台，并形成扩缩容动作的平台化执行能力，可检测扩缩容执行过程的结果。
Y4	具备个别场景下的容量智能分析和评估能力。	a）性能压测平台与容量分析系统、扩缩容自动化平台形成对接，实现容量管理的全流程串联； b）按照业务线形成自助化的压测能力。	部分无状态化业务模块具备基于智能运维的动态扩缩容能力，实现快速扩缩容动作。
Y5	按照业务流程具备端到端的智能化容量分析能力，并在容量预测、瓶颈点分析等场景进行应用。	a）基于智能运维手段的性能压测，可自动分析压测数据，形成压测报告； b）具备策略化的智能压测能力，根据业务容量的实际情况，智能分析和调整请求比例，形成贴近实际生产场景的压测方案。	智能动态扩缩容能力覆盖端到端的业务线，实现基于业务量的感知和分钟级自动扩缩容能力。

10.14　配置管理

10.14.1　资源模型管理

资源模型管理成熟度从策略与规程、资源模型定义、资源模型交付三个方面进行评估：

——策略与规程：为资源模型的定义和交付实施规范化的管理，确保后续数据维护质量所制定的规则与方法；

——资源模型：IT 资源统一标准化的模型定义，是其属性和关系的组合；

——资源模型交付：资源模型在多环境之间的交付手段和方法，以确保模型一致性。

资源模型管理成熟度等级要求见表47。

表 47　资源模型管理成熟度等级要求

等级	策略与规程	资源模型定义	资源模型交付
Y1	有简易的管理标准和规范要求。	有简易的定义方式，如通过人工方式进行模型定义和维护。	a）电子表格管理和定义模型； b）尚未对资源交付环境进行分类分级。

表 47　资源模型管理成熟度等级要求（续）

等级	策略与规程	资源模型定义	资源模型交付
Y2	初步定义模型管理的标准和规范，支持标准设备模型定义。	a）运维人员通过可视化界面完成资源模型的定义； b）资源模型存储在数据库或电子文档中； c）实现 IaaS 层和部分 PaaS 层模型管理，包括其关联关系。	a）模型交付可以通过可视化完成； b）资源交付模型的环境具备版本及权限控制，及定期备份的能力。
Y3	a）建立模型版本化控制策略； b）具备多环境管理模型的能力； c）模型管理具备多租户能力，可以实现分类分级授权管理。	a）运维人员通过可视化界面完成元数据定义； b）资源模型具备平台化管理能力； c）实现全面 PaaS 层模型和部分应用层模型管理，包括其关联关系； d）实现以应用、服务为中心的资源管理模型。	a）具备平台化模型版本化管理； b）模型作为资源进行集中管理，可以分发到多环境使用； c）在开发和测试环境之间，模型可以快速导出和导入实现模型同步。
Y4	a）建立模型版本化控制策略； b）具备多环境管理模型的能力； c）模型管理具备多租户能力，可以实现分类分级授权管理； d）建立模型发布和部署机制，模型变更质量得到控制； e）具备模型备份策略和管理要求。	a）运维人员通过可视化界面完成元数据定义； b）资源模型具备平台化管理能力； c）满足关系任意建模需要； d）实现全面应用服务、业务层模型管理，包括其关联关系； e）实现以应用、服务为中心的资源管理模型； f）模型定义可以是批量管理行为，也可以通过借助外在工具（如电子表格）格式化定义导入后生成。	a）具备平台化模型版本化管理； b）模型作为资源来集中管理，可以分发到多环境使用； c）提供模型回滚、指定版本发布的能力； d）模型采用定时备份的策略； e）提供模型多环境快速同步的功能。

表 47　资源模型管理成熟度等级要求（续）

等级	策略与规程	资源模型定义	资源模型交付
Y5	a）建立模型版本化控制策略； b）具备多环境管理模型的能力； c）模型管理具备多租户能力，可以实现分类分级授权管理； d）建立模型发布和部署机制，模型变更质量得到控制； e）具备模型备份策略和管理要求。	a）运维人员通过可视化界面完成元数据定义； b）资源模型具备平台化管理能力； c）满足关系任意建模需要； d）实现全面应用服务、业务层模型管理，包括其关联关系； e）实现以应用、服务为中心的资源管理模型； f）模型定义可以是批量管理行为，也可以通过借助外在工具（如电子表格）格式化定义导入后生成； g）可以借助人工智能手段，根据实际使用场景，自动推荐资源模型定义。	a）具备平台化模型版本化管理； b）模型作为资源来集中管理，可以分发到多环境使用； c）提供模型回滚、指定版本发布的能力； d）模型采用定时备份的策略； e）提供模型多环境快速同步的功能。

10.14.2　配置项管理

配置项管理成熟度从发现与采集、服务流程变更、场景化变更三个方面进行评估：

——发现与采集：通过工具对IT资源对象实施自动发现与采集，降低人工维护的代价；

——服务流程变更：依赖IT服务流程，对CMDB数据进行线上化维护；

——场景化变更：通过场景化的运维工具，对CMDB数据进行线上化维护。

配置项管理成熟度等级要求见表48。

表 48　配置项管理成熟度等级要求

等级	发现与采集	服务流程变更	场景化变更
Y1	以人工触发脚本方式实现数据采集。	存在个别单一 IT 服务管理流程与 CMDB 联动。	存在个别单一场景与 CMDB 数据消费联动。
Y2	a）自动化采集脚本采用定时任务机制执行； b）自动化采集脚本是以孤立的工具存在； c）IaaS 层与部分 PaaS 层资源实现自动采集与发现能力。	a）部分 IT 服务管理流程以读的方式和 CMDB 数据对接、消费 CMDB； b）流程服务灰度导入，体系化不足； c）IaaS 层和部分 Paas 层资源可以通过流程变更。	a）围绕读的场景建设，如 CMDB 数据可视化、监控类、运营分析类、安全类； b）IaaS 层和部分 PaaS 层资源可以通过场景变更。

表 48　配置项管理成熟度等级要求（续）

等级	发现与采集	服务流程变更	场景化变更
Y3	a）具备 CMDB 平台化管理能力，采用定时任务的机制执行； b）采集发现能力应与模型关联，并版本化管理； c）PaaS 层资源和应用层资源实现自动采集能力，主要是实例级别。	a）面向资源生命周期过程的 CMDB 信息维护； b）IT 服务变更服务流程以写的方式与 CMDB 对接，加强 CMDB 信息实时维护，确保准确性； c）PaaS 层资源和应用层资源可以通过流程变更，主要是实例级别。	a）围绕写的场景建设，如自动化运维场景、DevOps 应用交付、一键化资源交付等； b）数据的变更管理应具备审核校验能力； c）PaaS 层资源和应用层资源可以通过场景变更，主要是实例级别。
Y4	a）执行能力被 CMDB 平台接管，采用定时任务的机制执行； b）采集发现能力应与模型关联，并版本化管理； c）PaaS 层资源和应用层资源可以通过自动采集与发现获取，主要是关系与拓扑级别； d）采集与发现策略全面完整，指定目标执行、时间、执行频率等； e）数字化采集任务执行状态，并生成采集报告。	a）面向全部资源生命周期过程的 CMDB 信息维护等； b）IT 服务变更服务流程以写的方式与 CMDB 对接，加强 CMDB 信息实时维护，确保准确性； c）PaaS 层资源和应用层资源可以通过流程变更，更多是关系与拓扑级别； d）CMDB 作为基础元数据平台，实现所有 IT 数据集中管理； e）基于 CMDB 数据底层，提供平台数据互联互通的能力。	a）CMDB 提供基础数据支撑能力，支持复杂运维场景的 CMDB 数据消费能力等； b）PaaS 层资源和应用层资源可以通过场景变更，更多是关系和拓扑数据； c）数据的变更管理应具备审核校验能力。
Y5	a）执行能力被 CMDB 平台接管，采用定时任务的机制执行； b）采集发现能力应与模型关联，并版本化管理； c）PaaS 层资源和应用层资源可以通过自动采集与发现获取，主要是关系与拓扑级别； d）采集与发现策略全面完整：指定目标执行、时间、执行频率等； e）数字化采集任务执行状态，并生成采集报告。	a）面向全部资源生命周期过程的 CMDB 信息维护等； b）IT 服务变更服务流程以写的方式与 CMDB 对接，加强 CMDB 信息实时维护，确保准确性； c）PaaS 层资源和应用层资源可以通过流程变更，更多是关系与拓扑级别； d）CMDB 作为基础元数据平台，实现所有 IT 数据集中管理； e）基于 CMDB 数据底层，提供平台数据互联互通的能力； f）CMDB 数据支持智能化运维流程，如故障自愈。	a）CMDB 提供基础数据支撑能力，支持复杂运维场景的 CMDB 数据消费能力等； b）PaaS 层资源和应用层资源可以通过场景变更，更多是关系和拓扑数据； c）数据的变更管理应具备审核校验能力； d）CMDB 数据作为核心数据标签，支持智能化运维场景，如异常监测、故障根因、事件关联分析与容量预测等。

10.14.3 资源数据运营

资源数据运营成熟度从运营场景定义、运营场景实施、数据运营与校验三个方面进行评估：

——运营场景定义：资源数据根据场景分类定义场景框架，场景框架包含运维平台建设的不同维度，支撑运维平台建设在自动化、数据化和智能化等方面的要求；

——运营场景实施：根据资源数据运营场景的分类定义和阶段性导入要求，确定相应的实施方案；

——数据运营和校验：资源数据的生成、消费和运营，作为CMDB运营的标准化过程，宜建立指标体系来度量和校验CMDB的数据建设情况。

资源数据运营成熟度等级要求见表49。

表49 资源数据运营成熟度等级要求

等级	运营场景定义	运营场景实施	数据运营与校验
Y1	具有单一的CMDB数据场景运营意识，注重CMDB资源配置库的数据维护。	具有单一，无相关系统关联的场景。	具备简单的数据运营体系及数据校验能力。
Y2	a) 建立多种场景的数据运营能力，例如从可视化类、流程类、安全类、自动化、数据化类以及智能化等多个方面定义，并对其重要性分级； b) 定义场景运营流程与CMDB数据的交互逻辑。	a) CMDB以人工为主、自动化为辅的混合维护模式； b) CMDB具备支持简易的数据运营场景实施，例如在可视化、IT交付流程等场景中以低频率、小范围进行数据运营。	a) 具备基本的CMDB数据运营策略，分平台、数据、场景建设与管理规范； b) 具备基本的CMDB数据运营标准，分多指标展示CMDB数据状态，如全面性、实时性； c) 可视化展示CMDB中可视化展示CMDB的IaaS层和PaaS层数据状态。
Y3	a) 建立多种场景的数据运营的能力，并对其范围等属性进行分级； b) 定义自动化场景与CMDB运营的交互逻辑。	a) CMDB数据维护以自动化为主，人工为辅的混合运维模式； b) CMDB作为可靠的权威数据源，避免数据割裂； c) 业务运营场景全面实现流程化，建立起与CMDB的数据运营联动能力，如在事件、问题、变更与发布等场景中体现高效运营数据的服务价值； d) 以部分自动化为主要运营场景。	a) 具备统一的CMDB平台，并且CMDB是自动化运维唯一权威数据源； b) 具备全面的CMDB数据运营策略，支持分平台、分场景的管理策略； c) 具备全面的CMDB数据运营标准，多维度展示CMDB数据状态，如全面性、实时性； d) 可视化展示CMDB的应用层资源数据状态； e) 可视化展示服务流程及其他场景的CMDB消费接口情况。

表 49　资源数据运营成熟度等级要求（续）

等级	运营场景定义	运营场景实施	数据运营与校验
Y4	a）建立多种场景的数据运营的能力，并对其范围等属性进行分级； b）场景定义增加业务价值维度。	a）CMDB 数据维护以自动化/流程化的数据管理模式； b）CMDB 作为可靠的权威数据源，避免数据割裂； c）以全面自动化和数据化为主要运营场景； d）具备精细化 IT 运营分析场景消费 CMDB 数据，如成本管理、容量管理等。	a）具备统一的 CMDB 平台，并且 CMDB 是自动化运维唯一权威数据源； b）具备全面的 CMDB 数据运营策略，支持分平台、分场景的管理策略； c）具备全面的 CMDB 数据运营标准，多维度展示 CMDB 数据状态，如全面性、实时性； d）可视化展示 CMDB 的应用层资源数据状态； e）可视化展示服务流程及其他场景的 CMDB 消费接口情况； f）提供更实时的数据校验机制和能力，检查数据的准确性。
Y5	a）运营场景实现业务驱动、价值驱动，并结合事务驱动； b）运营场景的数据价值实现模板化、可视化、并可以预定义。	a）CMDB 数据维护以自动化/流程化/智能化的数据管理模式； b）CMDB 作为可靠的权威数据源，避免数据割裂； c）以全面智能化为主要的运营场景，如故障根因分析、多指标检测； d）CMDB 资源图谱作为知识图谱的一部分，供故障根因分析、多指标检测等场景调度使用。	a）具备统一的 CMDB 平台，并且 CMDB 是自动化运维唯一权威数据源； b）具备全面的 CMDB 数据运营策略，支持分平台、分场景的管理策略； c）具备全面的 CMDB 数据运营标准，多维度展示 CMDB 数据状态，如全面性、实时性； d）可视化展示 CMDB 的应用层资源数据状态； e）可视化展示服务流程及其他场景的 CMDB 消费接口情况； f）提供更实时的数据校验机制和能力，检查数据的准确性； g）CMDB 资源图谱成为智能运维知识图谱的一部分； h）可视化展示资源图谱的应用状态。

参 考 文 献

[1] GB/T 32399—2016 信息技术 云计算 参考架构
[2] GB/T 32400—2015 信息技术 计算 概览与词汇
[3] GB/T 33136—2016 信息技术服务数据中心服务能力成熟度模型
[4] JR/T 0099—2012 证券期货业信息系统运维管理规范
[5] JR/T 0112—2014 证券期货业信息系统审计规范