ICS 35.020
I65

T/SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/SIA036-2023

应用现代化技术能力成熟度评估模型

Application modernization technology capacity maturity assessment model

2023-7-1 发布　　2023-7-1 实施

中　国　软　件　行　业　协　会　发　布

目 次

前 言

本文件按照GB/T1.1—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。

本文件由中国软件行业协会提出并归口。

本文件起草单位： 华为云计算技术有限公司、南京领行科技股份有限公司、金蝶软件（中国）有限公司、软通动力信息技术（集团）股份有限公司、深圳市明源云科技有限公司、用友网络科技股份有限公司、中软国际科技服务有限公司、北京国药新创科技发展有限公司、青岛海尔科技有限公司。

本文件主要起草人：徐博、冯景灿、李永杰、孟凡忠、黄毅刚、赵华、张西涛、时小伟、李帆、张利军、徐昊、王永海、窦力杰、郭世伟、蒋与杨、郑鹏、曹正凤、顾悦、曹奇、孙佳韡、高江、胡志方、张锋、甘威、王建敏、徐志方、王淼、余悦。

应用现代化技术能力成熟度评估模型

1 范围

本文件给出了应用现代化技术能力成熟度的模型构成、评估方法及等级要求。

本文件适用于数字化转型领域相关规划、设计、开发、管理人员开展应用现代化改造实践。

2 规范性引用文件

暂无规范性引用文件。

3 术语和定义

3.1

应用现代化 application modernization

基于云原生、人工智能等先进技术对传统应用升级改造或新建应用的方案和方法论。

3.2

可观测性 observability

是一种对系统运行时的指标进行实时跟踪和监控，并对系统内部的事件、日志和异常进行聚合和分析的质量属性。

3.3

服务化架构 service-based architecture

是一种适用于云原生应用的技术架构，其特征包括：进程级别的运行态隔离，以接口契约定义每个服务应用单元，各服务/微服务只能通过 API 进行业务流程和逻辑的交互、协同。

注：接口契约指的是 IDL、Swagger、RAML 等。

4 缩略语

下列缩略语适用于本文件。

ACL:访问控制表（Access Control List）

AI:人工智能（Artificial Intelligence）

API:应用编程接口（Application Programming Interface）

BI:商业智能（Business Intelligence）

CC:挑战黑洞（Challenge Collapsar）

CPU:中央处理器（Central Processing Unit）

CV:计算机视觉（Computer Vision）

DAG:有向无环图（Directed Acyclic Graph）

DDD:领域驱动设计（Domain-Driven Design）

DDoS:分布式拒绝服务（Distributed Denial of Service）

E2E:端到端（End to End）
FTP:文件传输协议（File Transfer Protocol）
HTTP:超文本传输协议（Hypertext Transfer Protocol）
HTTPS:超文本安全传输协议（Hypertext Transfer Protocol over Secure Socket Layer）
HYOK:拥有自己的密钥（Hold Your Own Key）
IDL:接口描述语言（Interface Description Language）
RAML:Restful API建模语言（Restful API Modeling Language）
IP:互联网协议（Internet Protocol）
LP:线性规划（Linear Programming）
MIP:混合整数规划（Mixed-Integer Programming）
NLP:自然语言处理（Natural Language Processing）
OIDC:开放用户身份识别连接（Open ID Connect）
OS:操作系统（Operating System）
OWASP:开放式Web应用程序安全项目（Open Web Application Security Project）
PKI:公钥基础设施（Public Key Infrastructure）
RTO:恢复时间目标（Recovery Time Objective）
RPO:数据恢复点目标（Recovery Point Objective）
SAML:安全断言标记语言 （Security Assertion Markup Language）
SIEM:安全信息与事件管理（Security Information and Event Management）
SOA:面向服务的架构（Service-Oriented Architecture）
SOAR:安全编排自动化与响应（Security Orchestration, Automation and Response）
TTM:需求到最终上线时间（Time To Marketing）
UDP:用户数据报协议（User Datagram Protocol）

5 概述

5.1 应用现代化技术能力成熟度模型构成

应用现代化技术能力成熟度评估模型包含5个能力域，每个能力域由若干能力项构成，每个能力项由若干能力指标构成，见表1所示。

能力域表征了现代化应用的特征和用户需求，能力项和能力指标表示支撑/满足这些特征/需求所需的技术要求，是产品、解决方案、服务等技术能力的抽象。

表 1 技术能力成熟度模型构成

序号	能力域	能力项	能力指标
1	应用敏捷	开发生产线	具体内容见第 6 章
		组装式开发	
		应用托管	
		可观测性	
		服务化架构	

2	稳定可靠	流量治理	具体内容见第 7 章
		业务弹性	
		多活容灾	
		混沌工程	
		性能压测	
3	安全可信	身份与权限安全	具体内容见第 8 章
		网络安全	
		应用安全	
		负载安全	
		数据安全	
		合规治理	
		安全运营	
4	业务智能	智能湖仓	具体内容见第 9 章
		数据治理生产线	
		AI 开发平台	
		智能决策	
5	成本优化	财务管理	具体内容见第 10 章

5.2 应用现代化技术能力成熟度评估方法

通过计算公式可以得出被评估系统每个能力项、每个能力域满足能力指标要求的情况，然后基于评判原则给出待评估对象系统的成熟度等级。具体评估方法见第 11 章。

5.3 应用现代化技术能力成熟度级别划分

根据目前云计算领域技术、服务的现状及发展趋势，应用现代化技术能力自低向高依次划分为 3 个级别：初始级（L1）、发展级（L2）、优秀级（L3）。

6 应用敏捷能力指标

6.1 开发生产线

6.1.1 初始级要求

开发生产线达到初始级，应满足以下要求：

1) 应用软件开发过程采用单层级的需求进行管理；
2) 应用软件按固定节奏发布，部署频率为季度或者年；

3) 通过手工方式提供和管理应用的部署运行环境，应用生产过程的自动化低，每个环节都需要人工审批；
4) 需求 TTM 时长粒度为年；
5) 应用生产全过程无法度量，无法定位研发过程的效率瓶颈，缺乏可持续自主改进的基础输入；对应用生产过程的质量无法进行跟踪管理；
6) 应用上线前才进行必需的安全检查，或者全过程都没有必需的安全检查，或者安全检查采用单独团队手工执行的方式。

6.1.2 发展级要求

开发生产线达到发展级，应满足以下要求：

1) 初步需求管理采用多层次模型进行分解，能够实现战略级规划到具体迭代开发任务的端到端追溯、协同，需求收集分解采用手工方式；
   注：多层次模型例如 Epic-Feature-Story-Task。
2) 应用软件按固定节奏发布，部署频率为月；
3) 半自动化方式提供和管理应用的部署运行环境，能定义测试、生产等环境，在关键环节进行人工审核，如：上线前；
4) 需求 TTM 时长粒度为季度或者月；
5) 应用生产全过程的数据主要以人工收集，人工汇总，事后分析透视为主，无法实时反馈应用生产的状态；
6) 通过半自动化（人工+自动）对应用生产过程实施必需的安全检查和防护，安全检查覆盖的范围相对较窄，如：仅使用代码静态检查。

6.1.3 优秀级要求

开发生产线达到优秀级，应满足以下要求：

1) 规模化使用敏捷开发的需求多层次模型，需求管理全过程数字化、可视化，实现从战略需求到开发需求任务的无缝协同；
2) 应用软件以按需、随时、增量等不同方式部署发布；
3) 应用部署运行环境的提供和配置完全自动化，CI/CD 流水线自动化；
4) 需求 TTM 时长粒度为天；
5) 应用生产全过程数据收集自动化，信息可视化（如当前需求接纳率，需求 TTM，软件质量缺陷，代码安全超过阈值等），并能依据这些数据持续优化；
6) 应用生产过程中采用漏洞扫描，开源风险分析，多语言代码检查等全流程的安全措施；
7) 开发生产线为用户自建应用提供开放构建能力，对接外部或者第三方生态。

6.2 组装式开发

6.2.1 初始级要求

组装式达到初始级，应满足以下要求：

1) 应用开发基于 SOA 架构和内部 API 组件开发，各模块间耦合性强；
2) 应用交付基于服务化架构通过内部标准协议进行内部开放。

6.2.2 发展级要求

组装式达到发展级，应满足以下要求：

1) 应用开发基于微服务架构，用户界面无组装能力，按项目定制开发；
2) 前端开发人员需要理解微服务 API，根据业务场景设计用户界面，完成前端代码开发、联调和上线工作。

6.2.3 优秀级要求

组装式达到优秀级，应满足以下要求：

1) 应用开发基于组装式架构，可 E2E 组装用户界面和服务端组件（业务逻辑和数据实体）；
2) 应用通过零码/低码平台拖拉拽组件完成开发和交付；
3) 应用通过零码/低代码平台可视化开发，平台侧自动实现应用的部署、托管和运维，业务人员无须关注系统架构和基础设施、技术选型；
4) 提供组装式开发的开发能力，即基于原厂功能可以做扩展。

6.3 应用托管

6.3.1 初始级要求

应用托管达到初始级，应满足以下要求：

1) 各个业务使用独立的发布工具管理应用，通过各自脚本实现部分自动化，没有统一的应用发布平台；
2) 应用通过人工方式部署在云资源上，如：裸金属机或云主机；
3) 人工维护应用与应用依赖资源的配置关系。

6.3.2 发展级要求

应用托管达到发展级，应满足以下要求：

1) 通过统一的发布平台发布应用，业务团队各自管理和运维基础设施；
2) 应用通过发布系统部署到资源，如：云主机或容器；
3) 提供应用与其使用的基础设施资源的拓扑，如：中间件，数据库，节点等。

6.3.3 优秀级要求

应用托管达到优秀级，应满足以下要求：

1) 有统一的发布平台，提供基于模板的自动化应用交付能力；组织内不同团队的最佳实践沉淀为模板，通过发布平台复用团队经验；
2) 用户能够自定义应用与资源的模型，并对模型进行编排调度，将应用及依赖的资源一键式部署上云；
3) 能够进行灰度发布，实现业务在线发布；
4) 提供变更管理，实现变更可追溯，开发人员按照变更管控要求对生产环境进行操作。

6.4 可观测性

6.4.1 初始级要求

可观测性达到初始级，应满足以下要求：

1) 通过手工查看日志文件或通过 OS 命令查看指标数据，对问题进行分析，缺少日

志/监控平台。

6.4.2 发展级要求

可观测性达到发展级，应满足以下要求：

1) 自建日志、监控和性能平台；
2) 指标、日志、性能等运维数据孤立，缺少联动分析；
3) 观测数据收集后缺少权限管理，能够被公司内部所有研发团队查看。

6.4.3 优秀级要求

可观测性达到优秀级，应满足以下要求：

1) 使用全托管式可观测分析平台；
2) 指标、日志和性能数据可联动分析，并以应用或资源的维度统一呈现；
3) 观测数据按照运维或管理人员角色划分权限，控制观测数据的操作范围和权限；
4) 提供用户侧到云服务侧的全链路性能追踪能力；
5) 兼容云原生可观测性南北向数据规范，如：OpenTelementry、Prometheus、OpenTracing 等。

6.5 服务化架构

6.5.1 初始级要求

服务化架构达到初始级，应满足以下要求：

1) 采用单体或 SOA 架构；
2) 应用依赖的基础设施，如；缓存、消息和数据库、容器平台、对象存储等，均为自建和维护，缺少安全、可观察性等方面建设。

6.5.2 发展级要求

服务化架构达到发展级，应满足以下要求：

1) 采用微服务架构，包含注册中心，配置中心等基础组件，各服务可独立交付、部署和扩容；
2) 采用云上托管中间件、数据库，应用无需关注部署、维护和自身稳定性。

6.5.3 优秀级要求

服务化架构达到优秀级，应满足以下要求：

1) 采用微服务架构，各服务可独立交付、部署和扩容；
2) 使用 DDD 方法论指导微服务架构设计；
3) 采用云上托管中间件和数据库，应用无需关注部署、维护和自身稳定性；
4) 使用无服务器托管形式，开发者仅需维护业务逻辑，节点运维由云服务提供商管理。如：使用函数服务、事件驱动服务、无服务器容器等。

7 稳定可靠能力指标

7.1 流量治理

7.1.1 初始级要求

流量治理达到初始级，应满足以下要求：

1) 各个业务团队使用不同的开源流量治理工具实现，能力层次不齐，如：Sentinel、Hystrix 等。

7.1.2 发展级要求

流量治理达到发展级，应满足以下要求：

1) 使用服务治理框架，支持部分开发语言与框架；
2) 服务治理框架需要业务团队持续升级，版本碎片化严重；
3) 提供服务的限流、降级和故障隔离等基础治理能力。

7.1.3 优秀级要求

流量治理达到优秀级，应满足以下要求：

1) 具备统一服务治理框架，支持多语言异构应用统一治理；
2) 支持非侵入模式，业务开发不感知，治理能力与业务解耦；
3) 提供服务的限流、降级、故障隔离以及全链路灰度发布能力。

7.2 业务弹性

7.2.1 初始级要求

业务弹性达到初始级，应满足以下要求：

1) 缺少自动弹性能力，手动对业务负载进行弹性扩缩容。

7.2.2 发展级要求

业务弹性达到发展级，应满足以下要求：

1) 支持定时、周期、CPU/内存利用率等触发扩缩容；
2) 提供分钟级内数百容器实例批量创建的弹性扩展能力；
3) 提供业务在单个云服务提供商的云之间弹性调度能力。

7.2.3 优秀级要求

业务弹性达到优秀级，应满足以下要求：

1) 支持定时、周期、事件触发、自定义监控指标等触发扩缩容；
2) 提供分钟级内数千容器实例批量创建的弹性扩展能力；
3) 提供业务在多云服务提供商的云之间，以及云计算数据中心和本地数据中心之间的弹性调度能力。

7.3 多活容灾

7.3.1 初始级要求

多活容灾达到初始级，应满足以下要求：

1) 提供基于基础设施层的计算、存储、网络资源的灾备；
2) 支持 RTO/RPO 小时级的基础设施灾难恢复。

7.3.2 发展级要求

业务弹性达到发展级，应满足以下要求：

1) 提供基于基础设施、数据层、流量层的同城多活能力；
2) 提供分钟级的 RTO/RPO 的故障切换能力；
3) 提供数据同步、一致性保障、应用部署等能力，保障故障过程中业务不中断。

7.3.3 优秀级要求

业务弹性达到优秀级，应满足以下要求：

1) 提供管理、流量、应用、数据、基础设施等全层次的异地多活能力；
2) 提供秒级的 RTO/RPO 的业务之间切换的能力；
3) 基于单元化架构构建业务，支持业务的灵活扩展、故障爆炸半径缩小到单元内。

7.4 混沌工程

7.4.1 初始级要求

混沌工程达到初始级，应满足以下要求：

1) 支持基于测试环境开展故障注入，验证系统可靠性能力或者需求；
2) 通过故障注入工具开展基本的资源类故障，如突发高 CPU、高内存等；通过人工观测监控数据和分析系统可靠性能力。

7.4.2 发展级要求

混沌工程达到发展级，应满足以下要求：

1) 建立被测系统故障模式库，制定测试方案并在测试环境例行开展可靠性测试；
2) 通过故障注入工具开展复杂场景故障注入测试，如机房级故障、主机故障、应用进程故障、数据库/中间件故障、网络故障等；自动采集监控数据，通过人工开展可靠性量化评估；
3) 基于测试环境或者预发环境开展故障演练，制定演练计划、演练方案、组织阵型、应急响应策略，建立基础的故障演练流程。

7.4.3 优秀级要求

混沌工程达到优秀级，应满足以下要求：

1) 系统性建立和持续更新故障模式库，研发环境全面例行开展可靠性测试，支持故障模式全覆盖和自动化评估；
2) 故障注入工具具备完备的故障场景仿真能力，支持故障注入、稳态指标监控、可靠性量化评估、结果分析、实验防护、环境修复等全自动化；
3) 基于故障演练平台系统性建立故障演练体系和流程，包括演练计划、演练方案、组织阵型、演练通知、演练实施、演练报告和复盘、演练场景库等能力；
4) 生产环境按照月度或者周常态化开展故障演练、红蓝对抗、突击演练等实践，持续提升系统故障响应和恢复能力。

7.5 性能压测

7.5.1 初始级要求

性能压测达到初始级，应满足以下要求：

1) 压测过程中手动调节压测流量、根据指标熔断压测；
2) 支持配置请求内容的字段、检查点、超时间等，实现自定义内容的编写。

7.5.2 发展级要求

性能压测达到发展级，在满足初始级要求的基础上，应满足以下要求：

1) 支持在线编辑压测脚本，参数文件；
2) 支持在线调试压力脚本，兼容开源脚本工具如 Jmeter 等，覆盖多种常见协议，如：HTTP/HTTPS/FTP/UDP/WebSocket 等，实现自定义测试内容；
3) 支持从指定的环境、多执行器发起压力，如：私有资源组；
4) 支持被测系统的监控与告警。

7.5.3 优秀级要求

性能压测达到优秀级，在满足发展级要求的基础上，应满足以下要求：

1) 支持压测过程中自动调节压测流量；
2) 支持指定云厂商提供的网络或多地域网络发起压力；
3) 支持被测服务链路追踪；
4) 支持部分场景压测熔断，如：支持按照响应时间、成功率指标的压测熔断；
5) 支持压测数据隔离。

8 安全可信能力指标

8.1 身份与权限安全

8.1 初始级要求

身份与权限安全达到初始级，应满足以下要求：

1) 根据企业组织架构和角色设置不同访问权限,实现基于角色的访问控制；
2) 支持基础级联邦身份认证,如基于 SAML、OIDC 标准协议，实现单一身份源登录。

8.1.2 发展级要求

身份与权限安全达到发展级，应满足以下要求：

1) 根据部门、项目等次级组织单位细分访问权限；
2) 支持多种联邦身份认证，在多个内部身份源基础上，实现无缝单点登录业务系统、运维及管理平台；
3) 支持用户组划分，对用户进行批量的权限管理，例如：将不同用户放到同一用户组中，统一配置权限策略，无需为每个用户单独配置。

8.1.3 优秀级要求

身份与权限安全达到优秀级，应满足以下要求：

1) 支持精细的权限管理，支持对象粒度细致的访问控制（精确到 API）,最大程度实现权限分离；
2) 支持多种标准联邦认证协议,支持联合身份认证方式与风险策略相结合的安全认证。例如：IAM 与 AD 之间的联邦、不同 IAM 之间的联邦、或者与 LDAP 的联邦；
3) 支持用户组划分，对用户进行批量的权限管理，支持同一用户划分到不同用户

组中；

4) 支持区域内资源隔离，实现跨系统和跨区域的单点登录；
5) 支持对用户登录后的操作行为进行完整审计，如：新增账号、将账号切换到更高权限的群组中等，以识别敏感操作；
6) 提供灵活的委托管理机制，如：委托其他帐号或者云服务管理资源；
7) 提供访问策略管理，如：支持根据不同用户组、不同云资源类型及属性、不同操作类型进行细粒度控制等，用于管理用户组、用户的访问权限。

8.2 网络安全

8.2.1 初始级要求

网络安全达到初始级，应满足以下要求：

1) 支持 G 级别带宽的 DDos 防御能力；
2) 支持南北向 ACL 访问控制、访问记录，支持网络安全区域隔离划分。

8.2.2 发展级要求

网络安全达到发展级，应满足以下要求：

1) 支持 10G~1000G 带宽的 DDos 防御能力；
2) 支持南北向、东西向 ACL 访问控制，访问记录，支持网络安全区域隔离划分；
3) 支持南北向基于网络流量特征的访问控制、威胁预警。

8.3.3 优秀级要求

网络安全达到优秀级，应满足以下要求：

1) 支持 1T 及以上带宽的 DDos 防御能力，同时时延不超过 ms 级别；
2) 支持南北向、东西向 ACL 访问控制，访问记录，支持网络安全区域隔离划分；
3) 支持南北向、东西向基于网络流量特征的访问控制、威胁预警；
4) 提供传输通道的安全保障能力，如：支持 TLS2.0 及以上版本的协议；
5) 支持对服务端的身份认证，在安全等级要求较高场景下，支持双向身份验证，如：基于 PKI 数字证书的身份验证；
6) 支持南北向、东西向网络请求流量的限流降级保护，确保源站正常服务。

8.3 应用安全

8.3.1 初始级要求

应用安全达到初始级，应满足以下要求：

1) 安全防护规则覆盖 OWASP TOP 10 中常见安全威胁。

8.3.2 发展级要求

应用安全达到发展级，在满足初始级要求基础上，应满足以下要求：

1) 支持自定义安全规则配置，如：智能访问控制、CC 安全防护、黑白名单等，保障应用运行安全。

8.3.3 优秀级要求

应用安全达到优秀级，在满足发展级要求基础上，应满足以下要求：

1) 提供应用开发阶段端到端的安全合规检测，包括：安全设计、隐私合规分析、代码检查、二进制成分分析、移动应用安全等；
2) 支持内容的安全检测，如：识别文本、图片、视频的不规范内容。

8.4 负载安全

8.4.1 初始级要求

负载安全达到初始级，应满足以下要求：

1) 自动检测主机中的口令复杂度策略，关键软件中含有风险的配置信息；
2) 针对所发现的风险提供修复建议。

8.4.2 发展级要求

负载安全达到发展级，在满足初始级要求基础上，应满足以下要求：

1) 支持漏洞管理，如检测 Linux 漏洞、Windows 漏洞、Web-CMS 漏洞、应用漏洞。

8.4.3 优秀级要求

负载安全达到优秀级，在满足发展级要求基础上，应满足以下要求：

1) 支持对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。

8.5 数据安全

8.5.1 初始级要求

数据安全达到初始级，应满足以下要求：

1) 支持数据库的数据资产安全管理；
2) 提供数据加密能力。

8.5.2 发展级要求

数据安全达到发展级，应满足以下要求：

1) 支持对象存储、数据库的数据资产安全管理；
2) 提供专属的数据加密能力，如：HYOK 加密。

8.5.3 优秀级要求

数据安全达到优秀级，应满足以下要求：

1) 支持对象存储、数据库、大数据系统的数据资产安全管理；
2) 通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。

8.6 合规治理

8.6.1 初始级要求

合规治理达到初始级，应满足以下要求：

1) 支持安全合规治理法规标准条款代码化，周期性、自动化扫描租户云上资产的合规情况。

8.6.2 发展级要求

合规治理达到发展级，应满足以下要求：

1) 支持安全合规法规标准条款转化成检查项，可根据检查项完成租户自身业务的合规评估。

8.6.3 优秀级要求

合规治理达到优秀级，应满足以下要求：

1) 提供 ISO27701、ISO27001 等安全合规治理模板，合规策略和自评估检查项；
2) 自动化、持续性扫描租户云上资产的合规状态，快速梳理业务情况并且提供证据链管理功能。

8.7 安全运营

8.7.1 初始级要求

安全运营达到初始级，应满足以下要求：

1) 支持基础资产安全管理，如：对主机、IP 类型的资产导入、导出等；
2) 支持安全风险扫描,如：发现互联网暴露高危端口的资产、未覆盖安全服务产品的资产。
3) 支持收集、查看部分安全服务产品的告警，如：主机、应用、网络，可提供简单的告警处理操作；
4) 支持整体云上资产安全健康现状评估，快速感知安全状态，快速了解未处理风险对用户资产的整体威胁状况。

8.7.2 发展级要求

安全运营达到发展级，应满足以下要求：

1) 支持云上资产自动盘点；支持其它资产的导入，如：云外资产、多云资产；资产具有明确的归属，如：应用、部门；
2) 支持安全风险扫描,如：发现互联网暴露高危端口的资产、未覆盖安全服务产品的资产；支持安全基线扫描，如：发现最佳实践基线检查弱配置；支持漏洞扫描，如：发现 OS 漏洞、应用漏洞；
3) 支持基于 SIEM 分析威胁，可自定义配置威胁告警处理规则；提供基本的安全事件跟踪审计；
4) 支持提供整体而全面的安全评估结果，定期或按需生成任一安全运营报告和安全运营大屏，且必须有云上态势的呈现能力。

8.7.3 优秀级要求

安全运营达到优秀级，应满足以下要求：

1) 支持对多类型的资产安全管理，如：主机、IP、网站/域名、数据库/数据平台等；云上资产自动盘点；支持其它资产的导入，如：云外资产、多云资产；资产具有明确的归属，如：应用、部门；资产与告警、事件、漏洞、基线之间可关联；资产与资产之间可关联；
2) 支持安全风险扫描,如：发现互联网暴露高危端口的资产、发现未覆盖安全服务产品的资产；支持多类型安全基线扫描，如：发现最佳实践基线检查弱配置、

发现 PCI-DSS/ISO 等法规标准基线检查弱配置、发现自定义基线检查弱配置；支持漏洞扫描，如：发现 OS 漏洞、应用漏洞；支持云防护策略的设置与维护；

3) 支持基于 SIEM 分析威胁，开放式采集数据；可构建复杂威胁告警分析模型；基于 SOAR 响应威胁，开放式联动安全服务产品或其他任意工具；支持外部威胁情报信息接入，并运用到威胁分析及响应流程中；支持完整的攻击链还原分析；
4) 支持提供整体而全面的安全评估结果，定期或按需生成任一安全运营报告，并支持发送、可自定义安全运营报告；支持安全运营大屏呈现云上多种态势，如：综合态势、资产态势、风险态势、威胁态势、值班响应等；
5) 统一运营、作战协同：支持云上云下统一管理。

9 业务智能能力指标

9.1 智能湖仓

9.1.1 初始级要求

智能湖仓达到初始级，应满足以下要求：

1) 依赖开源 Hadoop 大数据分析/数仓技术，自建数据分析平台；
2) 分析组件按业务需要和技能熟悉度自主搭配集成，数据分析引擎性能与开源社区持平；
3) 数据湖存储仅支持本地 HDFS，不支持对象存储。

9.1.2 发展级要求

智能湖仓达到发展级，在满足初始级要求的基础上，应满足以下要求：

1) 大数据分析/数仓分析平台分析引擎性能较开源社区技术有差异化提升，包括功能增强、性能增强；
2) 数据湖支持存算分离弹性架构，数据存储支持对象存储，计算和存储可灵活弹性扩展；
3) 湖和仓之间数据能够共享，实现快速数据流动；
4) 湖仓平台增强企业级管理能力，包括：监控、告警、日志、审计、用户管理、作业管理等。

9.1.3 优秀级要求

智能湖仓达到优秀级，在满足发展级要求的基础上，应满足以下要求：

1) 提供统一的数据湖构建能力，打通湖与仓、湖与 AI 平台、仓与 AI 平台，实现统一的元数据和安全，减少数据搬迁；
2) 湖仓平台提供细粒度的监控，支持作业智能诊断和调优推荐能力；
3) 支持湖仓平台软硬调优能力，具备一些硬件加速的算子。

9.2 数据治理生产线

9.2.1 初始级要求

数据治理达到初始级，应满足以下要求：

1) 支持通过开源数据集成工具构建数据接入能力，以批量接入为主；
2) 提供简单的数据 SQL 开发界面，实现数据的关联查询分析。

9.2.2 发展级要求

数据治理达到发展级，在满足初始级的基础上，应满足以下要求：

1) 提供统一的数据开发平台，提供可视化作业编辑和基于 DAG 的编排能力，提供脚本代码多个版本的统一管理；
2) 支持血缘分析和质量监控，业务流程能够有效打通；
3) 提供基本的数据安全管理能力，包括认证、授权、存储加密、传输加密、基本的脱敏等。

9.2.3 优秀级要求

数据治理达到优秀级，在满足发展级要求的基础上，应满足以下要求：

1) 提供自动化数据管理能力，包括：自动提供数据质量评估结果（如：数据重复度等）、自动识别敏感数据、自动实现数据分级分类、自动进行数据关联分析和搜索推荐（如：基于数据资产图谱）；
2) 支持维度建模、关系建模等数据标准规范，以提升数据开发的质量以及后期数据指标和对象的可维护性；
3) 统一管理数据资产（如：提供企业全局资产目录等方式），支持不同业务单元进行快速查找、申请和分析数据；
4) 提供数据安全管理能力，支持敏感数据分级分类自动管理，采、存、算、管、用全流程支持敏感数据保护，支持数据水印跟踪，面向不同场景的数据合规性诊断、数据安全态势感知和风险管理；
5) 提供智能化数据管理能力，包括：智能分类分级、智能脱敏、智能清洗等。

9.3 AI 开发平台

9.3.1 初始级要求

AI 开发平台达到初始级，应满足以下要求：

1) 基于开源框架和 Notebook 类工具自建 AI 训练平台，AI 平台管理无规范化；
   示例 1：框架指 TensorFlow、PyTorch、Spark 等。
   示例 2：Notebook 工具指 Jupyter、Zepplin 等。
2) 预置算法以开源算法为主；
3) 开发过程中的多人协同主要靠人工交流。

9.3.2 发展级要求

AI 开发平台达到发展级，在满足初始级的基础上，应满足以下要求：

1) 提供模型开发全生命周期的工具链，支持模型、算法等资产管理和共享；
2) 提供模型全生命周期的管理能力，包括：提供统一的模型仓库，支持模型发布管理，支持多厂家算法的统一管理；
3) 提供面向多角色的统一开发环境，支持多版本、多人协作的交互式 AI 算法开发，提供云上、云下一致的开发体验；
4) 提供基础通用 AI 能力，如：计算机视觉、自然语言处理、语音语义识别等，支

持通过工作流集成通用 AI 能力以进行场景化模型二次开发；

5) 提供异构算力资源统一管理能力，支持多种标准接口访问，提供机器学习、深度学习、强化学习等能力，提供基本的数据准备能力、数据标注能力和特征管理能力。

9.3.3 优秀级要求

AI 开发平台达到优秀级，在满足发展级的基础上，应满足以下要求：

1) 支持分布式、高性能、大规模训练能力，支持模型并行、数据并行、混合并行等加速能力；
2) 支持智能数据标注，提供多场景训练数据；
3) 支持预训练模型，如：NLP 大模型、CV 大模型、多模态大模型等，缩短场景化二次训练的周期；
4) 支持多种 AI 硬件和框架；

   示例 1：硬件指的是昇腾、昆仑芯、曙光 DCU、寒武纪等。

   示例 2：AI 框架指的是 MindSpore，PanddlePanddle 等。
5) 支持边缘推理，端、边、云 AI 场景联动，模型下推和数据回流。

9.4 智能决策

9.4.1 初始级要求

智能决策达到初始级，应满足以下要求：

1) 支持基于具体的业务场景或部门需求定制开发业务决策系统及业务指标统计的大屏应用；
2) 具备基础的数据处理和分析，如采用 Excel 表格功能分析数据；
3) 支持规则可自定义配置的决策引擎。

9.4.2 发展级要求

智能决策达到发展级，在满足初始级要求基础上，应满足以下要求：

1) 具备通用的决策平台，支持自主分析的 BI 工具和可视化决策大屏；
2) 支持规则引擎结合预测模型进行商业决策，规则引擎覆盖已知业务模式，预测模型满足部分场景预测，实现智能优化业务决策；
3) 具备自研或者集成商业求解器，提供常规数学规划建模求解能力；
4) 求解器支持十万级参数，在有限时间内（小时级）找到可行的决策方案。

9.4.3 优秀级要求

智能决策达到优秀级，在满足发展级要求基础上，应满足以下要求：

1) 支持 NLP 等 AI 能力，通过自然语言交互式分析查询到用户所需数据，实现自动分析、智能推荐；
2) 支持数据片段和数据点的智能根因分析，关联指标及图表推荐，多维下钻；
3) 求解器覆盖大部分现实中的数学规划问题，包含 LP 和 MIP 等问题的建模求解；
4) 求解器支持百万级以上参数。

10 成本优化能力指标

10.1 财务管理

10.1.1 初始级要求

财务管理达到初始级，应满足以下要求：

1）通过账单了解云资源消费和支出。

10.1.2 发展级要求

财务管理达到发展级，应满足以下要求：

1) 部分组织有成本意识和成本管理；
2) 通过账单了解云资源消费和支出，并监控账户和资源包；
3) 提供少量维度的成本分析报告，通过成本可视化难以看清各个部门、项目成本，无法对超支的部门、项目问责；
4) 对部分资源利用率进行监控和优化。

10.1.3 优秀级要求

财务管理达到优秀级，应满足以下要求：

1) 在组织内部贯彻成本意识，创建成本透明度和成本问责制；
2) 提供工具制定预算支出规划，并对已上云业务和新增业务对资源的需求成本进行预测，预测成本与估算成本之和与实际支出差异不高于 20%；
3) 通过工具监控预算、账户和资源包，当出现预算超支、异常高成本、账户和资源包额度不足等情况，通过短信、邮件等方式提供预警；
4) 通过多种形式的账单查看云资源消费支出情况，对支出信息和账单进行多维度、分层管理以提升对账效率，如：支出情况的汇总、分布、明细等，设置账单汇总的次序和层级；

   示例：自定义账号、产品、计费模式等嵌套式的账单。
5) 通过图形化方式多维度、多周期粒度查看云上资源成本分布和趋势，以及各个部门和项目的支出；
6) 根据历史费用和资源使用等情况给出费用优化建议和资源优化建议。

   示例 1：费用优化建议如指的是节省计划购买建议、资源包购买建议、包年包月购买建议等；

   示例 2：资源优化建议如指的是虚拟机资源优化建议、容器资源优化建议等。

11 成熟度评估方法

11.1 单个能力项得分的计算方法

初始级、发展级、优秀级的满分分别是1分、2分、3分。满足对应等级的全部能力指标要求得满分，否则得0分。

表 2 单个能力项得分示例

序号	能力项	满足程度	能力项得分
1	开发生产线	满足所有优秀级要求	3
2	组装式开发	满足所有发展级要求	2

表 2 单个能力项得分示例（续）

序号	能力项	满足程度	能力项得分
3	业务智能	满足所有初始级要求	1

11.2 单个能力域得分的计算方法

单个能力域得分的计算方法见公式（1），其中，m为该能力域的能力项个数总和。以“应用敏捷”能力域为例，单个能力域得分参见表3。

$$能力域得分 = \sum_{i=1\sim m} 能力项得分(i) \quad (1)$$

表 3 单个能力域得分示例

能力域	能力项	满足的级别	能力项得分	能力域得分
应用敏捷	开发生产线	优秀级	3	12
	组装式开发	发展级	2	
	应用托管	优秀级	3	
	可观测性	发展级	2	
	服务化架构	发展级	2	

11.3 成熟度评估方法

被评估系统的单个能力域成熟度得分，按照公式（2）进行计算，其中分母为对应级别的能力域满分。

单个能力域的成熟度得分达到80分及以上，视为成熟度符合对应级别要求。计算公式及评估方法的示例见表4。

$$成熟度得分 = 能力域得分/\sum_{j=1\sim n} 能力项满分(j)x100 \quad (2)$$

表 4 成熟度得分及等级评估方法示例

能力域	能力域得分	初始级满分	发展级满分	优秀级满分	成熟度得分	成熟度级别
应用敏捷	14	5	10	15	（14/15）x100=93	优秀级
业务智能	7	4	8	12	（7/8）x100=87	发展级
成本优化	1	1	2	3	（1/1）x100=100	初始级