奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

冬奥实战化安全运行之资产运营服务

陈飞虎 冬奥项目组网络安全专家

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

基于系统安全平台的资产运营服务

基于系统安全平台的资产运营服务就是通过数据平台打通资配漏补四大部分的安全工作，通过以资产安全风险为中心的多源数据融合分析，产生资产、漏洞等相关运营工作任务，驱动安全服务人员与IT运维人员在运行平台的支撑下，共同完成控制资产风险保持安全阵型的常态化、实战化工作闭环。

资产运营的闭环管理

三位一体的全生命周期协同

	开发团队	服务团队	冬奥团队
规划阶段	架构设计 功能设计	归纳经验 传递需求	设定目标 提出需求
开发阶段	平台开发 平台测试	构建体系 测试运行	提供环境 实验测试
交付阶段	交付支持 需求定制	现场交付 适配需求	环境准备 交付配合
运行阶段	功能迭代	需求更新 常态运行	问题反馈

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

资产运营的开展过程

将运营目标按照自上而下的逻辑层层分解，明确实现目标的运营任务，制定各个任务的对应流程，最终形成支撑资产运营工作的服务体系和平台需求。设计过程环环相扣，涵盖项目前期调研至项目交付并进入常态化工作开展阶段的完整生命周期，以此确保项目目标能充分达成。

运营目标落实

明确资产运营需要实现的最终目标，后续的所有工作，都已完成该目标为核心

实现任务的完整流程，需要结合用户的现有流程和平台功能进行调整或重新设计

服务侧形成SOP标准文档，用于运行工作的实战化、持续化开展

确定宏观目标 → 实现目标对应任务 → 任务对应流程 → 任务流程目录

拆分实现目标需要开展的任务，任务一定要贴合业务，全面准确。任务可以进行分类，具体可以参考标准文档和用户已有方案

细化任务流程中的每个运行环节，形成任务流程目录

任务流程目录 → SOP设计
- 流程SOP：基于角色的详细流程图，每一个环节都需要进行说明和细化
- 规程SOP：基于操作的SOP文档，指导运行人员一步步的使用平台开展运行工作，以一线人员能够独立开展作为唯一标准

任务流程目录 → 平台需求
- 功能需求：平台功能的需求要由安服、产品经理讨论，然后由客户确认，最后通过JIRA提交平台需求
- 数据推导：各种数据源的导入碰撞分析定义，包括关联字段，字段映射关系，重要字段，可能的冲突

平台侧形成产品功能需求，进行需求输入

运营工作开展

前期咨询阶段

- 前期交流：初步调研 / 正式交流
- 管理调研：组织架构 / 管理制度
- 专项调研：现网调研 / 流程梳理 / 需求调研
- 文档输出：运行分析报告 / 系统安全方案

平台实施阶段

- 实施准备：部署方案 / 环境准备
- 实施交付：实施部署 / 交付测试
- 初始化盘点：资产盘点 / 漏洞盘点

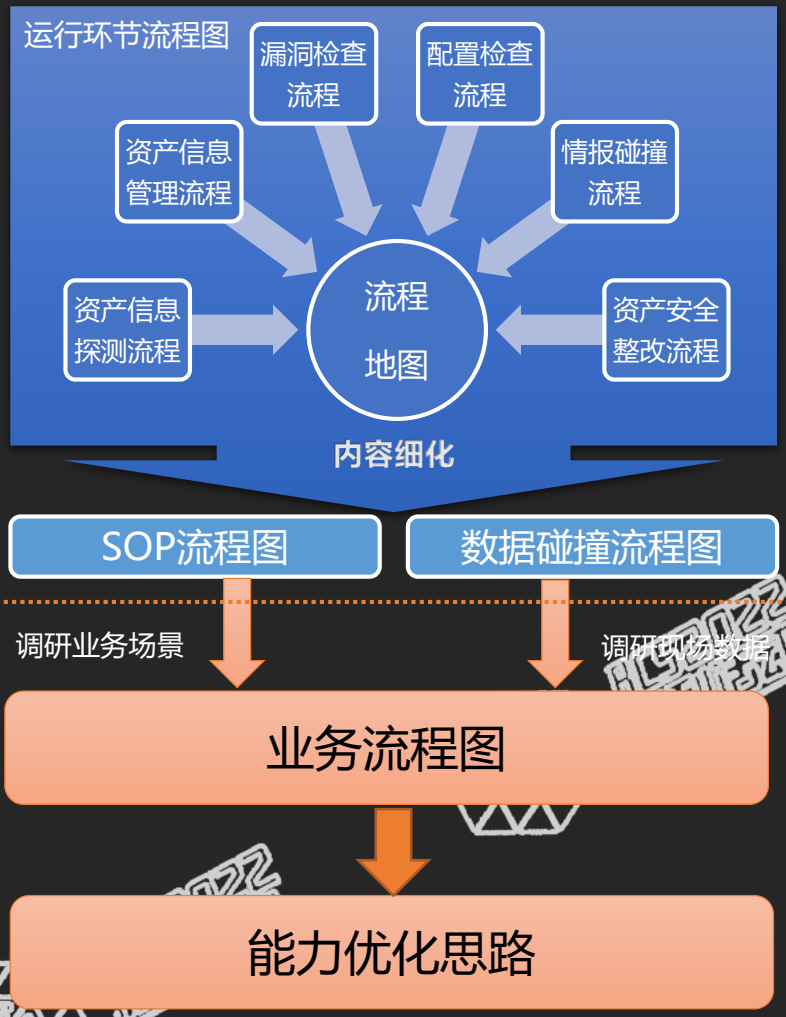
运行开发阶段

服务运行	平台运行	数据运行	产品运行
运行流程	功能磨合	数据治理	资产探测
服务标准	界面磨合	数据分析	漏洞发现
人员培养	工单磨合		配置发现
知识积累			

资产运营现状调研咨询

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

流程底稿



调研分析

调研业务场景

调研现场数据

业务流程图

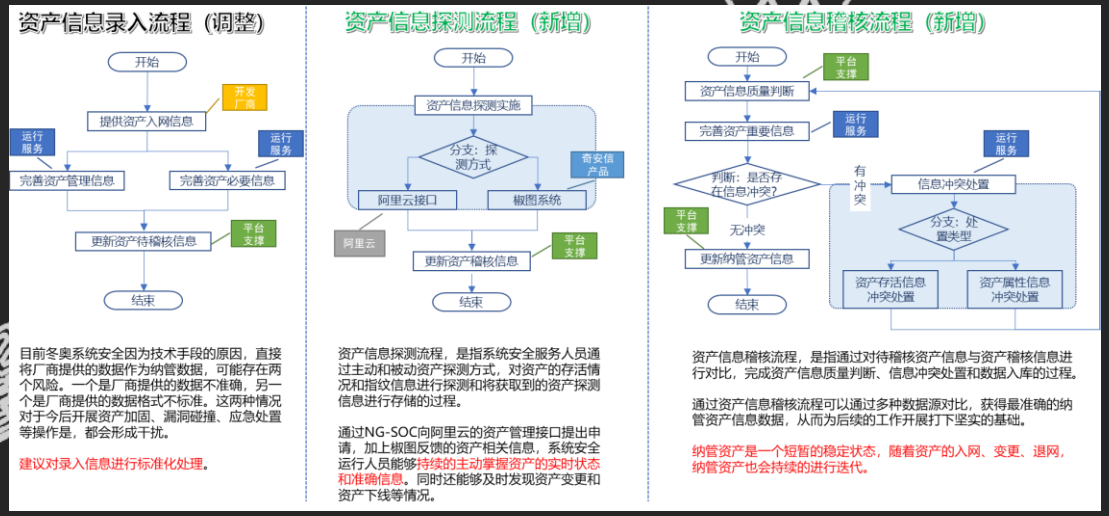
能力优化思路

业务流程优化

1.补充缺失流程
2.补充缺失环节
3.优化流程路径
4.明确角色分工
5.明确平台介入点

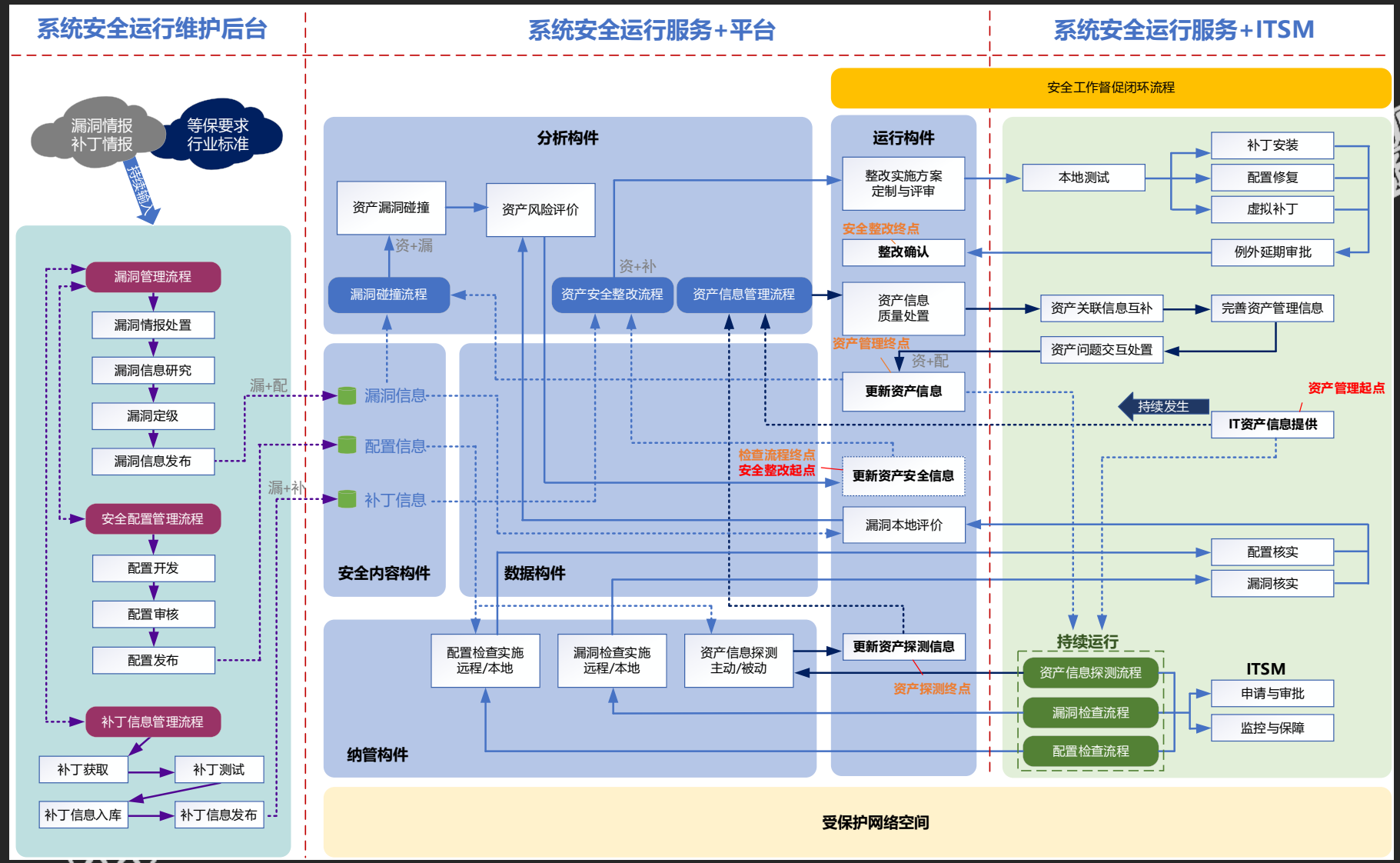
流程能力分析

1.明确数据来源
2.明确产品能力
3.明确角色职责
4.明确缺失知识
5.明确缺失文档



流程名	阿里云	奇安信（安全产品）	奇安信（运行平台）	奇安信（运行服务）	奇安信（NOX）	第三方	开发厂商
资产信息录入流程			更新资产待稽核信息（数据治理）	1.完善资产管理信息 2.完善资产必要信息			提供资产入网信息（表格）
资产信息探测流程（新增）	阿里云接口（NG-SOC）	椒图系统（资产信息）	更新资产稽核信息（对接稽核数据）				
资产信息稽核流程（新增）			1.资产信息质量判断（资产质量问题发现） 2.更新纳管资产信息	1.完善资产重要信息 2.信息冲突处置			
漏洞检查流程（阿里流程）	漏洞扫描报告						
配置检查流程（阿里流程）	配置检查报告						
漏洞碰撞流程					漏洞情报提供	漏洞情报提供	
资产安全整改流程	1.资产安全信息提供 2.整改确认		更新资产安全信息	1.整改方案编写评审 2.整改确认 3.残留风险确认			1.补丁安装 2.配置修复 3.补偿措施

流程地图



蓝色：数据变化触发流程

流程的驱动依赖于数据涌现，比如ITSM提供的数据，通过资产、配置、漏洞检查产生的数据，以及其相互碰撞产生的数据。

绿色：运行操作触发流程

流程的驱动依赖触发机制，比如常态化运行时的周期工作开展，重要保障期间的紧急触发，触发的目的是为了产生数据。

紫色：后台维护流程

流程为后台团队通过收集、分析、研究、测试等操作形成的结果，直接输送给前台使用。

黑色箭头为资产管理大循环的流程步骤，包括资产信息录入流程、资产信息探测流程、资产稽核流程。

蓝色箭头为漏洞、配置与整改大循环的流程步骤，包括漏洞检查流程、配置检查流程、资产安全整改流程。

紫色箭头为维护后台流程，包括漏洞管理流程、配置管理流程、补丁管理流程。

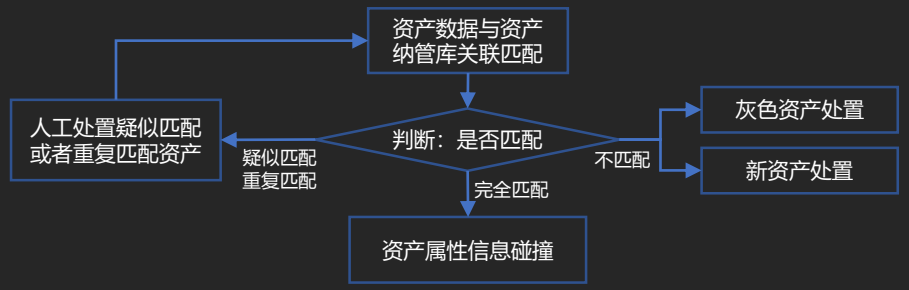
运行环节

白色方框为运行环节，是流程组成的重要部分。运行环节由运行服务人员结合平台及IT大运维进行实现。

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

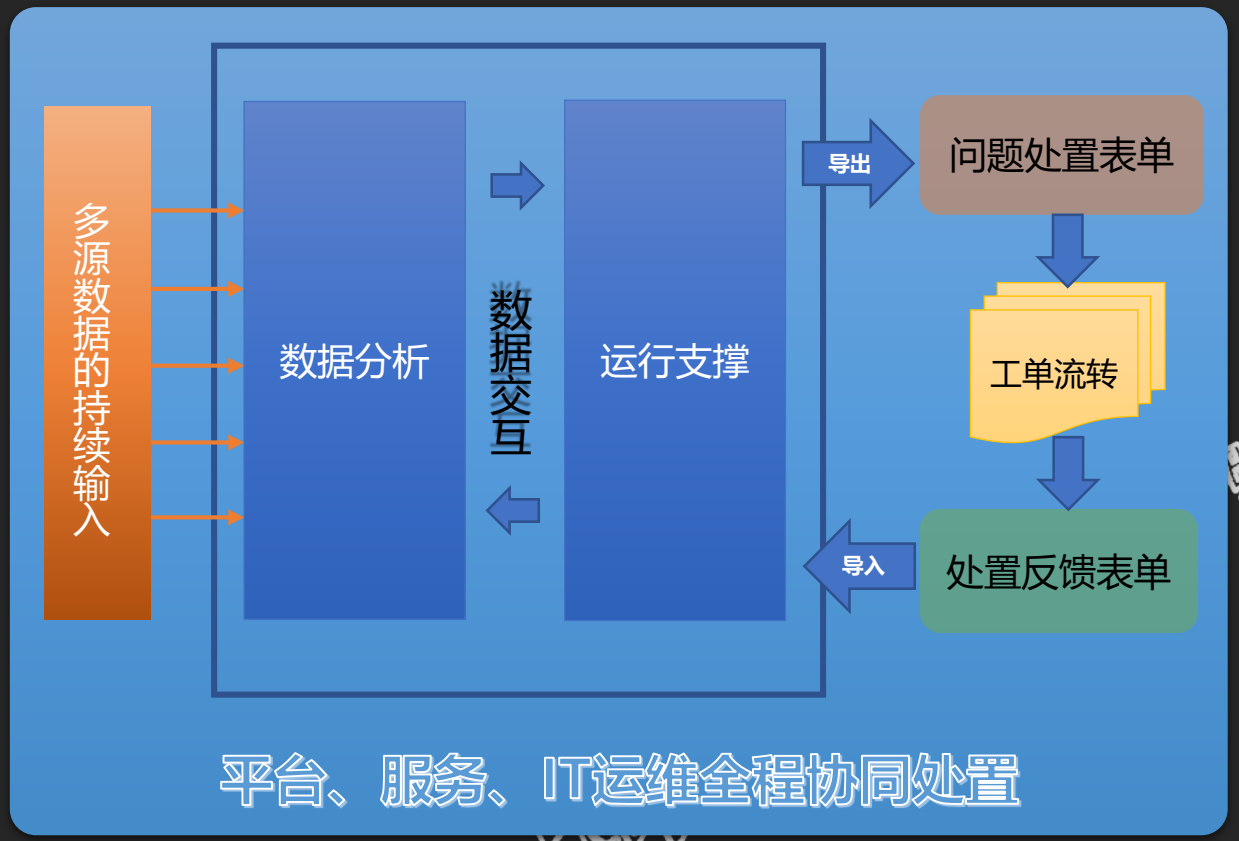
数据驱动事项运营



资产数据碰撞分析过程

- 资产数据导入平台后首先和平台的资产纳管库进行关联匹配，从而判断出哪些资产是纳管库中已经存在的资产，哪些是新增或者灰色资产；
- 针对纳管库中已经存在的资产，则会用最新的资产属性信息和纳管库中的资产属性信息进行碰撞分析，从而产生相互补充、相互验证、相互冲突等问题；
- 平台根据算法自动处理数据碰撞产生的问题，对于平台无法自动处理的问题，则生成交互处置任务，由系统安全资产运行人员连同IT运维人员进行处置；

资产交互处置过程



资产问题交互处置

- **资产运营人员判断：**优先解决可通过简单判断就可以识别解决的问题；
- **资产下发交互处置：**将问题资产拆分为三类分别填入资产确认单、资产维护单、资产说明单进行下发，每一条由资产责任人确认属性信息正确并签字确认，然后邮件反馈至资产管理员；

处置记录&修改数据源错误

- **维护资产全表：**针对三类资产均分别形成一张最全、最可信的资产全表；
- **资产处置记录：**记录从资产现状分析、问题分类、资产分发处置的每一个环节的处置记录与资产详细数据；
- **修改错误数据源：**将通过交互处置修正的正确数据反馈到NGSOC、手工登记表，对源数据进行更改及维护；

冬奥项目资产处置按照以上逻辑开展工作，**完成每一条资产处置及信息确认**，确保资产属性信息的**准确性**与重要属性信息的**完善程度**。在此基础上形成闭环的资产管理流程，动态维护资产上线、变更、下线全生命周期过程，做到资产数据变化的实时动态维护，以保证以资产为基础的漏洞管理、风险识别工作的更好开展，最大程度上保障资产的安全姿态；

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

资产管理常态化工作开展情况

资产的问题处置是一个由数据驱动的持续常态化的过程。伴随多源资产数据的不断更新，通过大数据分析平台碰撞产生资产事项，驱动资产管理处置流程，由一线运营经理及资产责任人交互处置资产事项，完成资产数据的闭环管理。

第一次常态化资产梳理结果

类别		云上资产	数据中心资产	云下场馆资产	外围资产	资产总数
无问题资产		224	1264	193	121	1802
有问题资产	冲突资产	427	51	24	0	502
	待补全资产	319	147	148	0	614
总数		970	1462	365	121	2918

问题资产处置

运营经理团队自行判断处置资产问题，核实并处置问题资产500余条

由资产责任人交互处置资产问题，核实并处置问题资产320条

常态化资产梳理结果

类别		云上资产	数据中心资产	云下场馆资产	外围资产	资产总数
无问题资产		835	1084	340	121	2380
有问题资产	冲突资产	0	0	0	0	0
	待补全资产	296	0	0	0	296
总数		1131	1084	340	121	2676

处置说明：

- 云上资产：主要处理资产属性信息冲突问题、关联字段问题、资产重要属性信息补全问题、新资产上线
- 数据中心资产：主要处理资产重要信息补全问题，其中删除无效资产信息，导致资产数减少
- 云下场馆资产：主要处理资产重要信息补全问题，其中删除无效资产信息，导致资产数减少

- 问题资产：存在属性冲突或属性信息待补全的资产
- 冲突资产：资产属性信息在多个数据来源中不一致，发生冲突
- 待补全资产：资产的属性信息值为空值的资产，隶属于国外IT公司资产，重要信息已经完备，少量信息未补全

漏洞运行状态的变化及流程驱动

在常态化漏洞安全运营过程中，漏洞存在各种运行状态（实体本身客观存在的状态，初始状态由数据驱动产生），通过漏洞运营、新数据的导入、时间的变化，漏洞的运行状态会产生或者发生变化。通过将不同的运行状态和漏洞运营环节建立关系，可以驱动漏洞处置工作的持续开展，最终实现从漏洞处置的全流程闭环。

漏洞运营的状态变化

数据输入的状态变化

状态驱动条件 \ 当前漏洞运行状态		无状态	【待复测】	【已修复】
新数据输入	【无需处置】过滤	【无需处置】		
	与上次漏洞归一		【待处置】	【待核实】
	剩余新漏洞	【待核实】		
	上次漏洞未出现		【已修复】	

时间指标的状态变化

状态驱动条件 \ 当前漏洞运行状态		【误报】	【无需处置】	【延期处置】	【例外处置】
时间指标	指标到期	【待核实】	【待核实】	【待核实】	【待核实】

资产运营服务文档体系

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

分层展现，由浅入深

- 运行服务方案 → 流程设计与流程SOP → 操作规程 三级结构，由浅入深，由粗到细展示工作开展的关键环节和工作要求。

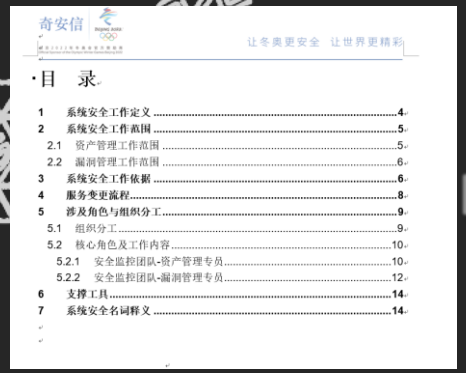
流程简化，操作精炼

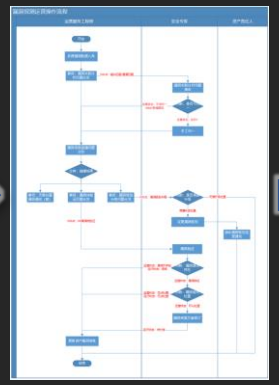
- 穿行和优化设计，避免冗余操作，最简化完成业务的操作动作，避免成为产品说明书和功能说明。

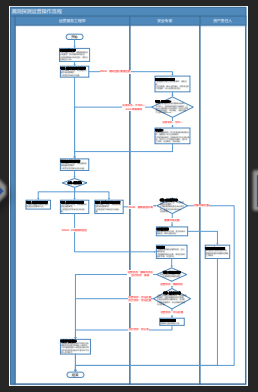
基于角色，循序渐进

- 操作文档基于角色编写，目标是引导角色能够快速的根据流程开展运营工作；
- 操作文档避免集中出现新的知识点，形成阅读障碍，注意知识点的分布；
- 操作文档采用横排版式，充分利用屏幕可视空间，将流程路标、注释等内容置于右侧。

文档类目	文档层级			
	01 综述类	02 制度策略类	03 流程操作类	04 表单工具类
资产运行Asset Operation（AO）		QAX-SSOS-02-系统安全-资产管理流	QAX-SSOS-03-系统安全-资产管理操作手册	QAX-SSOS-04-AO-《外围资产表》
				QAX-SSOS-04-AO-《云上资产表》
				QAX-SSOS-04-AO-《云下资产表》
				QAX-SSOS-04-AO-《资产问题处理脚本操作流程》
				QAX-SSOS-04-AO-《资产信息确认单》
				QAX-SSOS-04-AO-《资产信息确认通知》
				QAX-SSOS-04-AO-《资产信息收集计划》
				QAX-SSOS-04-AO-《资产信息收集台账》
				QAX-SSOS-04-AO-《资产信息问题跟踪表》
				QAX-SSOS-04-AO-资产管理脚本
漏洞运行Vulnerability Operation（VO		QAX-SSOS-02-系统安全-漏洞管理流	QAX-SSOS-03-系统安全-漏洞管理操作手册	QAX-SSOS-04-VO-《漏洞通报》通知邮件
				QAX-SSOS-04-VO-NESSUS漏洞报告
				QAX-SSOS-04-VO-安骑士漏洞报告（app）
				QAX-SSOS-04-VO-安骑士漏洞报告（corperoteIT漏洞
				QAX-SSOS-04-VO-安骑士漏洞报告（emg）
				QAX-SSOS-04-VO-监理漏洞汇报
				QAX-SSOS-04-VO-漏洞处置通知
				QAX-SSOS-04-VO-周四漏洞汇报表
				QAX-SSOS-04-VO-资产漏洞信息表
项目管理project management（PM）	QAX-SSOS-01-系统安全运行总纲			QAX-SSOS-04-PM-《项目通讯录》







运行服务方案　流程设计　流程SOP　操作规程

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

资产运营管理成果

资产管理成果

- 多源资产持续运营，动态掌握纳管资产数据变化
- 规范资产管理的流程体系，建立标准管理处置流程
- 摸清家底，梳理建立最全面、最准确的资产数据库

漏洞管理成果

- 自动化能力，取代人力维护，提高效率保证质量
- 资产漏洞库维护，漏洞生命周期可记录，可追溯
- 视角转换，漏洞视角转向资产视角、信息系统视角

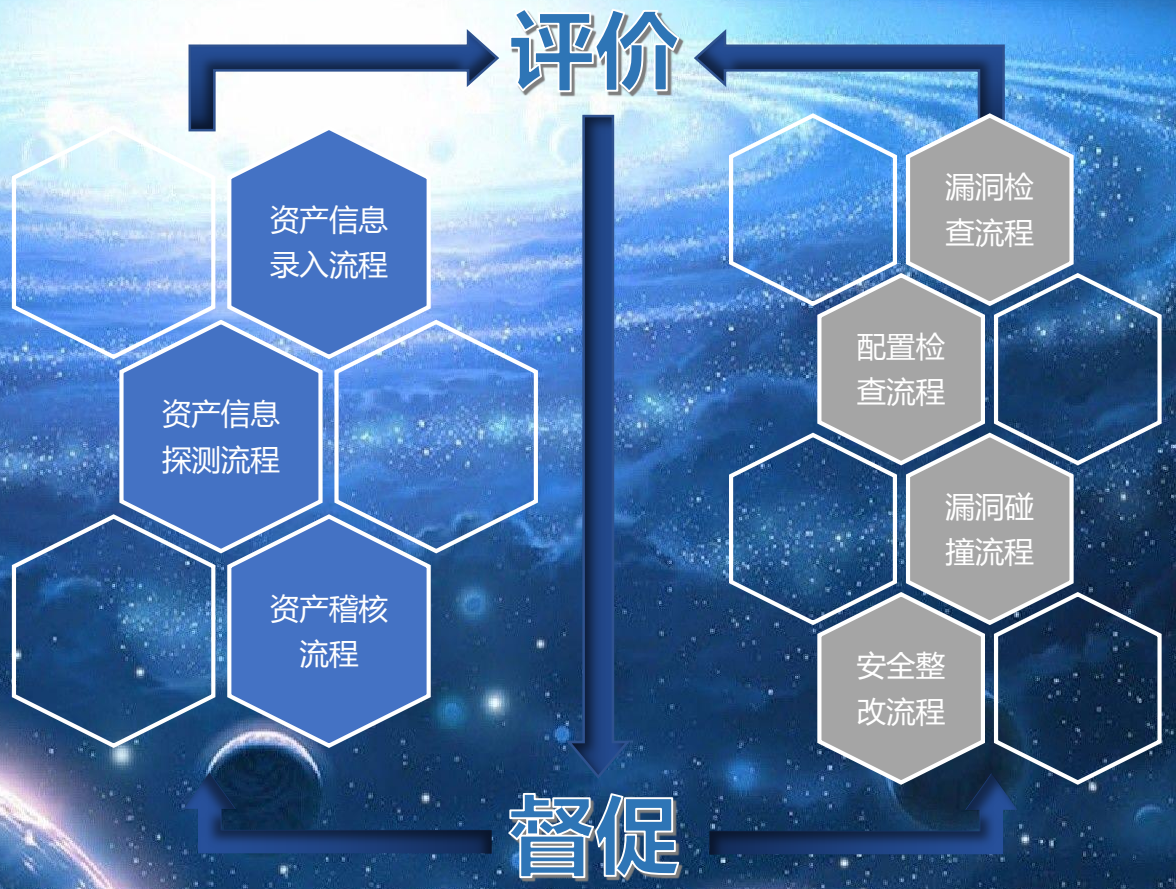
- 建立完善资产漏洞信息库、情报信息库,资产风险持续跟踪
- 反哺各个数据源，使企业信息系统相关数据保持一致
- 为其它平台提供详细准确的资产安全数据
- 帮助企业发现灰色资产和沉默资产

资产运营服务的持续开展

资产安全的持续运行，是一个从黑暗到光明，从无序到有序的过程

空间维度

纳管范围
纳管级别
风险级别



时间维度

资产纳管时间
安全整改时间

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

资产运营服务体系

- 以系统安全现状调研分析为起点，设定可度量的运营目标、可分析的多源数据和情报、可运行的实战化业务流程；
- 通过运营服务进行持续流程优化、持续人员优化、持续数据优化，同时通过策略部署和数据处置赋能系统安全平台，最终实现流程、人员、数据和平台运营成熟度目标；
- 运营过程中，持续输出资产安全数据保鲜、资产与漏洞问题智能分析处置、团队成长与精力释放、知识沉淀等运营价值。

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

THANKS