

CMC安全生产培训

CMC运维管理部

信息安全管理

上线质量管理

运维质量管理

什么是信息安全

- 保证信息的**保密性、完整性、可用性**。另外也可包括真实性、可核查性、不可否认性和可靠性等特性。
- 目标：**把信息安全风险降到最小。**

信息安全责任文化

- **“谁主管谁负责”** 的安全责任文化。
- 公司高层牵头，部门主管领导负责，专人管理，全员参与。
- 各级部门的负责人是本部门信息安全的**第一责任人**。各部门安全管理员，负责信息安全管理规定和要求，在本部门的推行和落实，检查和改进。

信息安全原则

遵循最小权限原则
仅赋予需要的最低权限

遵循职责分离机制
利益相关角色应不同人担任

遵循知其所需原则
只给访问主体应该知道的信息

遵循默认禁止原则
若无明确定义，则默认禁止


遵循最少功能原则
不需要的功能就取消


不同安全级别的系统 不能在一个安全域内

遵循深度防御原则
避免或限制单点失效

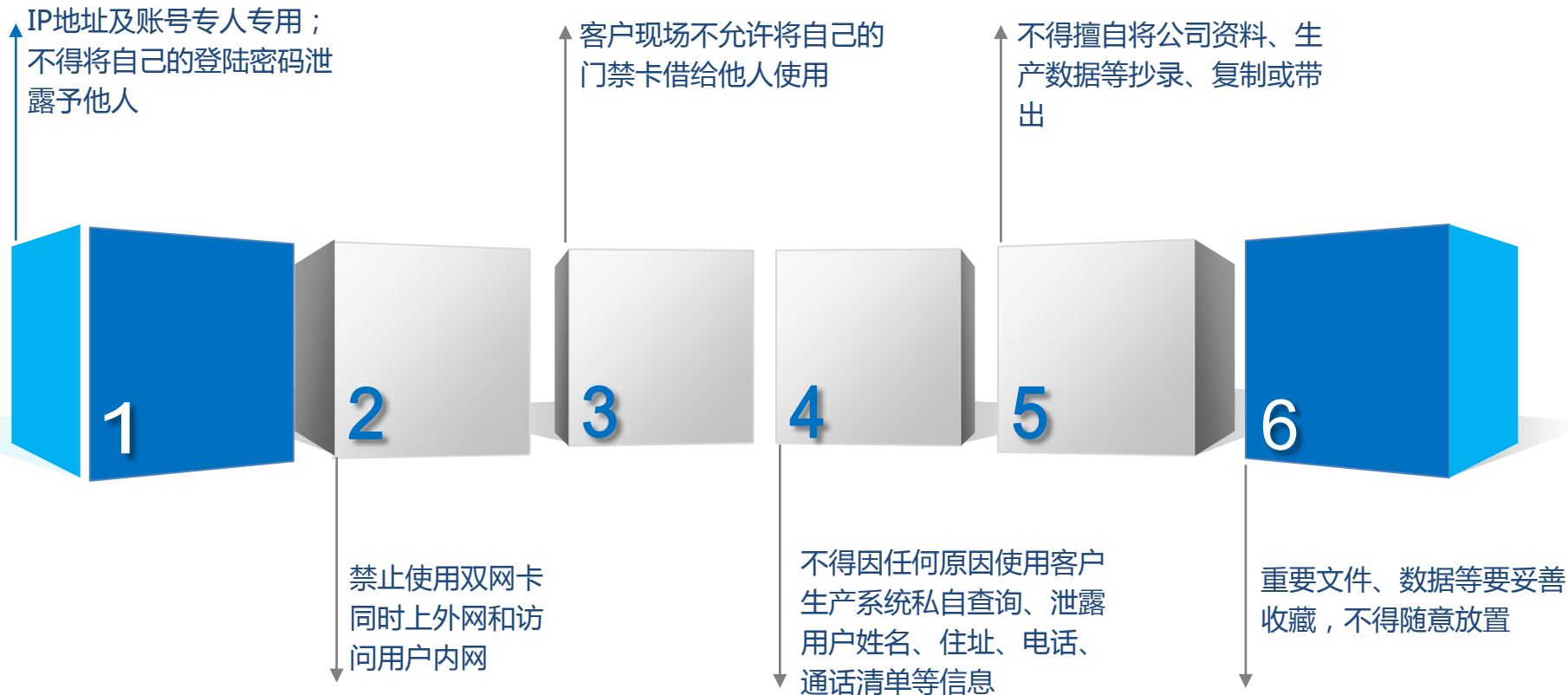
生产环境和开发、测试环境隔离 云环境下，网络逻辑隔离

信息安全组织

- 
- ◆ 设置安全管理接口人员、省级客户现场安全总负责人、驻场各项目安全负责人；对口合作伙伴安全相关主管

- 
- ◆ 现场的每名员工，需单独签署个人的保密承诺书

现场员工个人安全规范



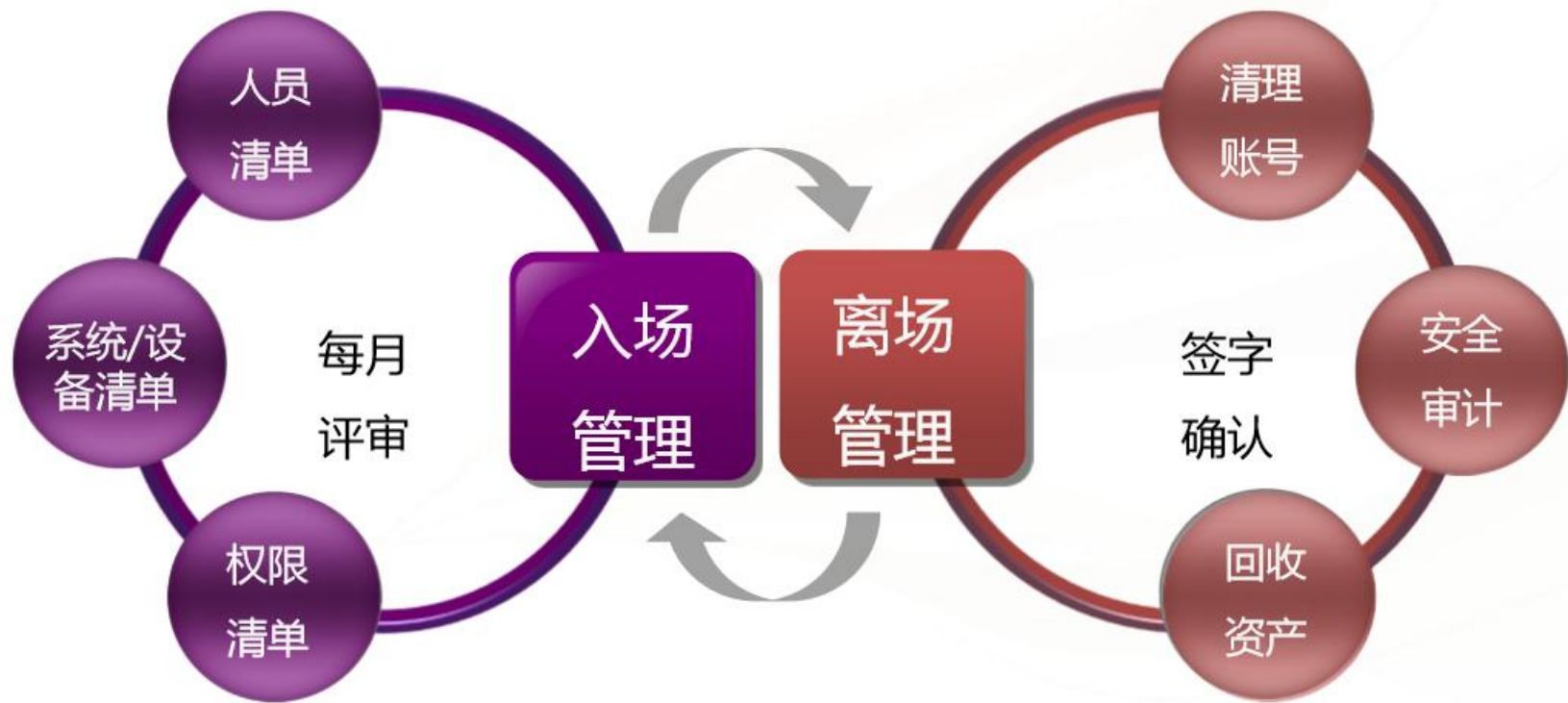
安全宣传和培训

- 新员工、外包或需要进行百一测评中的信息安全测试，并且达到90分才算合格。
- 每月进行组织内所有员工的信息安全管理培训。
- 张贴信息安全标识。

培训内容包括但不限于：

- ISO27001安全体系标准、公司安全管理相关的制度培训。
- 信息安全相关法律法规、个人信息安全培训。

入场/离场管理



外包人员管理



外包人员入职时，安全要求同新员工一致：签署保密协议、信息安全培训、百一测评考试。

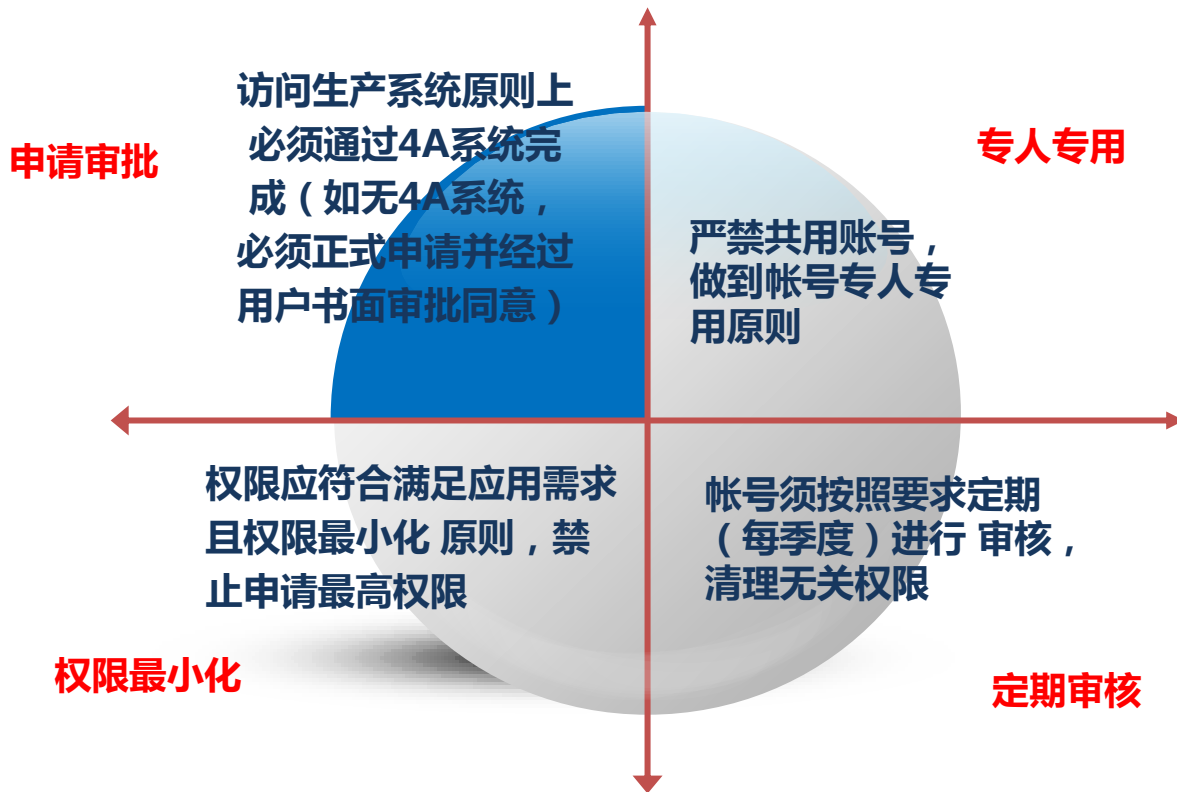


外包人员离职时，删除外包人员NT账号、访问应用系统/服务器的账号，并归还门禁卡、相关资料等。



发生外包人员造成的信息安全事件或安全隐患，由外包使用部门主管安全的VP承担第一责任，外包使用部门经理承担直接责任。

账号管理



备份和介质

备份

- 制定对软件、信息系统和数据的统一备份策略，并定期进行评审。
- 根据备份策略进行定期备份和恢复测试，确保备份策略的有效性。

介质

- 建立可移动介质的管理程序，当介质不再需要时，按照正式的程序进行完全可靠的销毁。
- 建立信息处置和存储程序，以防范该信息的泄漏或误用；应保护系统文档免受未授权的访问。

个人移动设备

- 个人电脑需安装防病毒软件，并定期更新防病毒库。
- 电脑开机密码要满足复杂性要求，勿使用姓名、电话、生日做为密码。
- 离开座位时，电脑要锁屏。

- 对工作成果要及时存储。
- 重要文档和工作目录要加密。
- 开会后，会议室白板上的信息及时清除。
- 佩戴工牌。

数据安全

数据
安全

生产数据禁止被导入到测试环境或开发环境

生产数据禁止被导出到用户终端

导出重要据时要进行加密保护

重要的数据在传输、存储等过程中都要加密

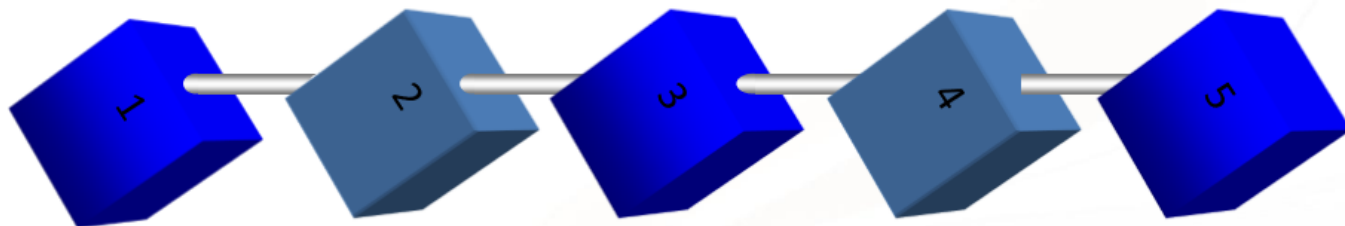
未经授权禁止查看用户个人资料信息

软件开发过程

- 开发过程中：使用静态代码安全扫描工具（SonarQube或VCG等）。
- 上线前：系统级漏洞扫描、应用级漏洞扫描工具，解决中级别及以上漏洞（集团提供支持：绿盟硬件、Acunetix软件）。
- 定期漏洞扫描：大版本上线后，进行漏洞扫描。

技术文档管理

- 生产过程中所产生技术文档包括各种WORD、PPT等材料都是属于公司的财产。在技术文档外发到第三方时（包括局方），必须要有审批流程。



运维过程符合
“**操作安全**”
的要求。主机、
数据库和网络
设备执行复杂
密码策略

主机**关闭**无用
的服务和端口，
数据库**关闭**不
必要的功能
(存储过程或
服务等)

禁止使用**不安全**
的网络协议 (如
telnet, rsh , ftp,
rlogin, rcp等) ,
使用**安全的网络**
协议 (如ssh,
tls, sftp等)

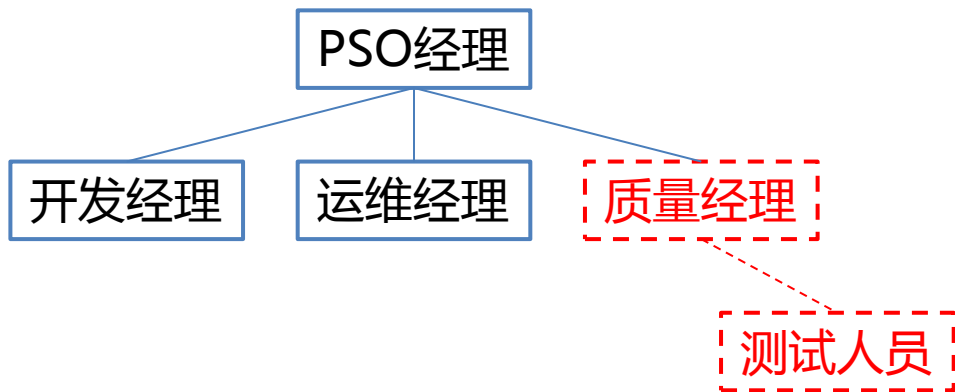
维护人员间禁
止**共享账号** ,
root用户不能
直接连接访问
系统

所有的设备和
系统都要在**资**
产清单中被记
录，所有运维
过程都要有**文**
档记录

信息安全管理

上线质量管理

运维质量管理



- PSO设立专职质量经理
- 质量经理负责测试团队，对需求的测试质量负责
- 质量经理负责测试环境、预发布环境、测试用例库的建设和完善

- 对所有需求的测试质量负责
- 对所有需求的测试进行统一管理
- 参与需求分析评审
- 组织需求上线评审
- 指导测试人员编写测试用例。
- 对内部测试结果进行审核



用户评审/确认过程

- 用户评审需求分析输出并确认
- 用户评审测试报告并确认
- 用户批准上线申请
- 上线后，用户确认上线验证结果



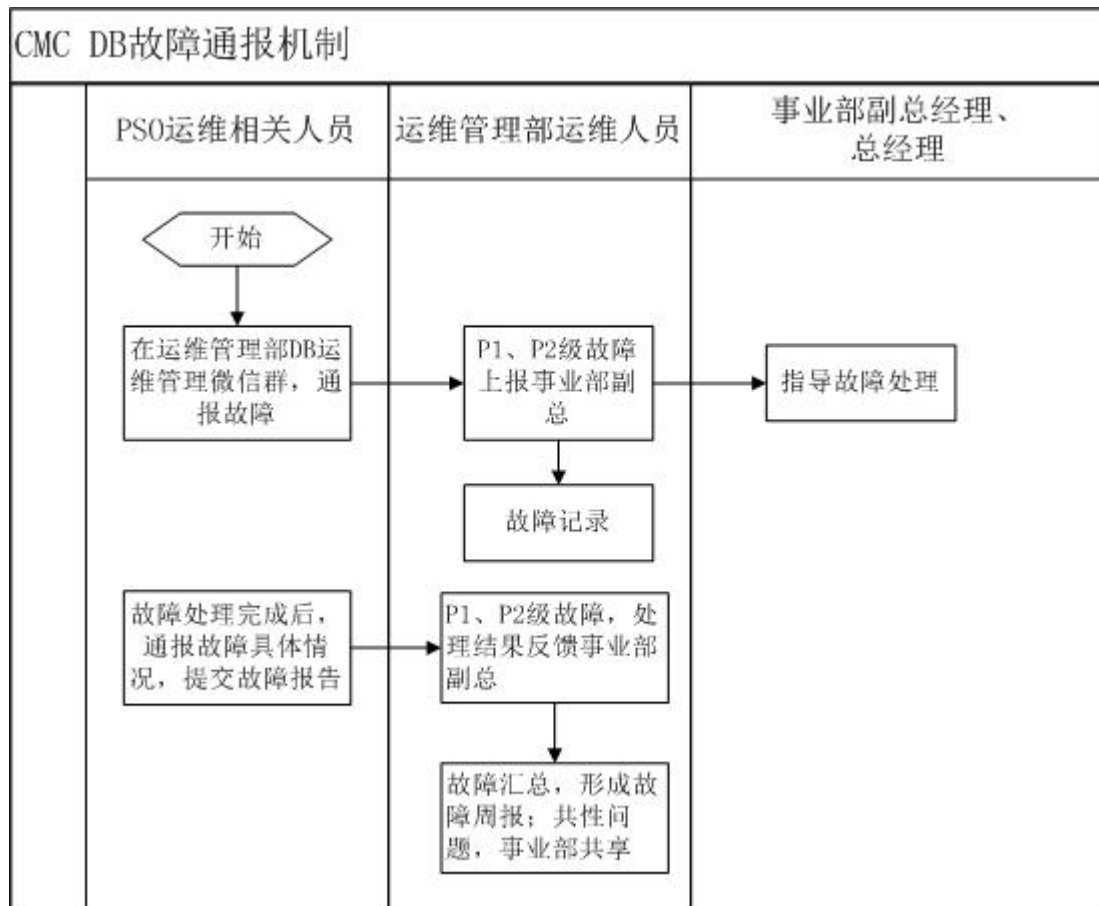


信息安全管理

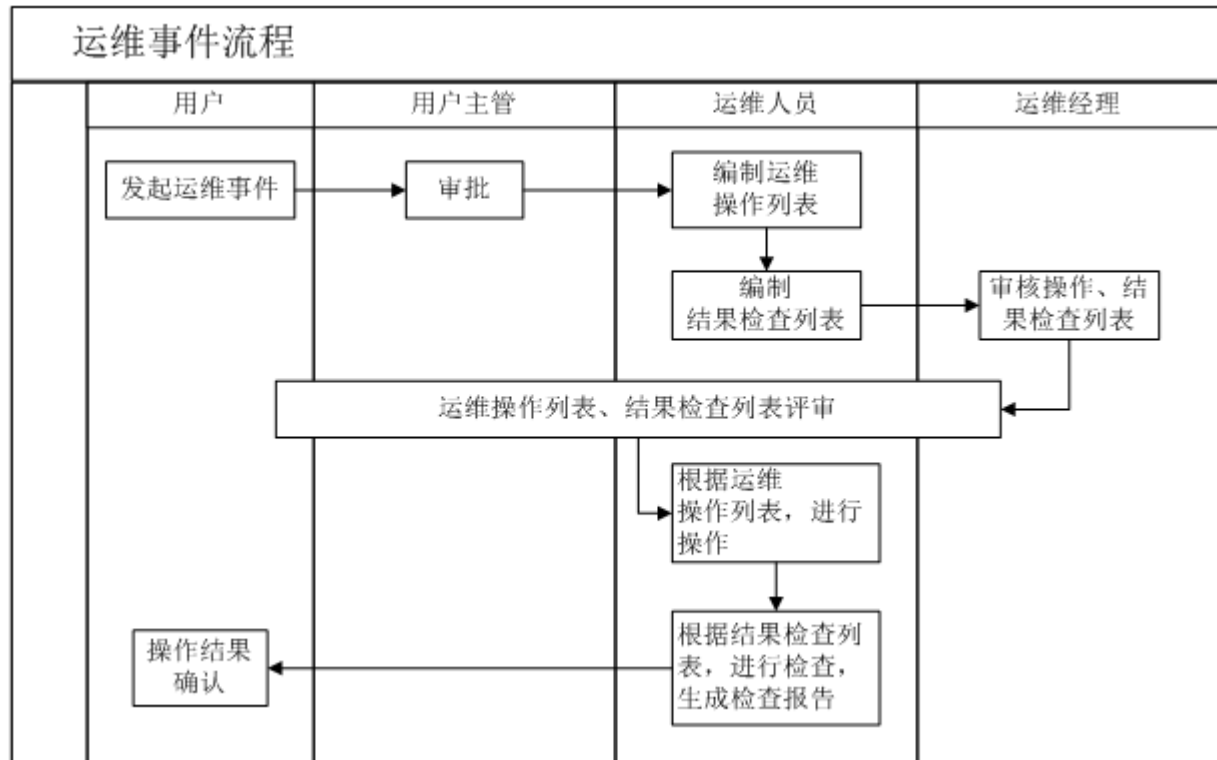
上线质量管理

运维质量管理

故障处理-通报流程



发生故障后，需要把故障信息，及时在微信群中通报。



- 事件必须是用户发起
- 必须经用户主管审批
- 运维事件操作必须经过审批、评审
- 结果必须反馈



- 应用配置事件必须是用户发起
- 必须经用户主管审批
- 应用配置操作必须形成操作列表
- 运维事件操作必须经过运维经理审批
- 用户、运维人员、运维经理共同对操作步骤进行评审
- 由运维人员根据操作列表进行操作
- 结果反馈给用户相关人员

资源变更管理

- 建立资源变更管理流程，由用户发起流程，并由相关主管审核
- 建立资源变更管理操作常规列表，运维经理审核后提交用户确认。
- 变更当天，操作人员根据列表进行操作
- 建立资源变更业务验证列表，变更完成后，测试人员根据业务验证列表进行业务验证操作，形成业务验证报告。
- 业务验证报告提交给用户相关人员进行确认。
- 第二天安排业务保障

2018年9月16日晚操作计划

操作项目	模块	工作任务	开始时间	结束时间	操作人员
准备	免考核申请	免考核申请，免考时间			杨卓
	屏蔽相关主机告警	屏蔽告警 CRM云化APP, AEE, WEB	18:00前	22:00	吴海林
	经分接口	经分接口延后	22:30	23:00	武创
	统计报表	停统计	22:30	23:00	赵福栋
	携号转网	携号转网	22:00	23:00	胡永亮
		计费修改批价配置，屏蔽BDS消息	22:40	23:00	伏树林
		停周期费计算	22:30	23:00	杜永平
业务保障		提醒	23:00	23:05	伏树林
			23:00	23:05	徐道超
			22:30	23:00	徐道超
			23:00	23:05	陈斌
			23:00	23:05	王爽
			23:05	23:10	廖巍
			23:05	6:30	杨卓
			23:10	6:00	杨卓

模块	巡检内容	检查方法和口径	异常判断标准
APP应用，主机和性能监控	APP应用检查	登陆地址  http://1 “APP应用监控”，“WEB应用监控”。 应用监控下需关注APP应用监控、WEB应用监控。	“探测返回时间”在50ms以内为正常。持续多次刷新超过1000ms为异常。
	主机检查	“WEB主机监控”，“APP主机监控” 主机监控里需关注CPU使用率、内存使用率、套接字监控、磁盘使用率	字体显示红色为异常。
	性能监控	登陆地址  http://...jsp 该页面会按耗时排序列出sql，也可以输入服务名查询耗时情况	

事件管理-监控有效性

- 每月进行系统监控情况分析
- 形成告警量前10名事件
- 分析事件形成原因
- 把相关事件形成问题跟踪单
- 跟踪解决相关问题
- 调整相关告警配置

二、CRM告警分析 2018.8月（二）

五月份监控告警总体情况：

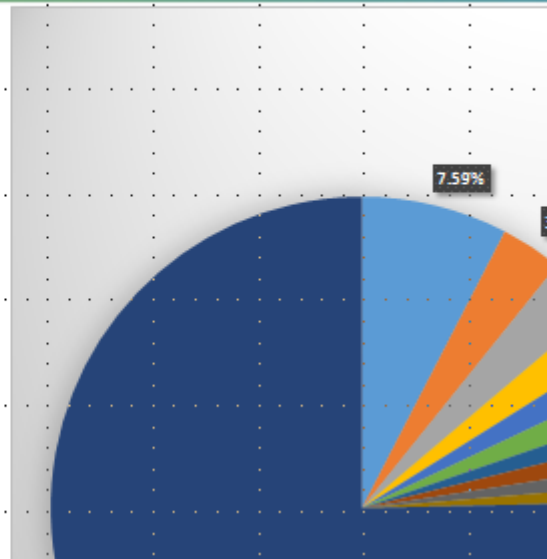
告警总量：9310

告警种类：382种

其中Top10告警共占比：24.64%

八月份新增告警：12个（info_id:1732-1743）

八月份下线告警：0个



应用配置文件管理

- 整理系统中配置文件列表
- 对列表中的配置文件，定期进行备份，建议每月一次。
- 包括但不限于以下三类配置文件
 - 应用配置文件
 - 中间件配置文件
 - 数据库配置文件

序号	svn地址	备份路径
1	http://	/svn/j2ee_ghai./app/config/trace.xml
2	http://	/svn/j3ee_ghai./app/config/msg.xml
3	http://	/svn/j4ee_ghai./app/config/memcache.xml
4	http://	/svn/j5ee_ghai./app/config/localcache.xml
5	http://	/svn/j6ee_ghai./app/config/database.xml
6	http://	/svn/j7ee_ghai./app/config/service/dev-response.xml
7	http://	/svn/j8ee_ghai./app/config/service/serviceconfig.xml
8	http://	/svn/j9ee_ghai./app/config/service/ngfa.xml
9	http://	/svn/j10ee_gha./app/config/service/ngpf.xml
10	http://	/svn/j11ee_gha./app/config/service/common.xml
11	http://	/svn/j12ee_gha./app/config/service/centerservice.xml
12	http://	/svn/j13ee_gha./app/config/dsf.xml
13	http://	/svn/j14ee_gha./app/config/IKEExpression.cfg.xml
14	http://	/svn/j15ee_gha./app/config/search.xml

■ 整理系统中脚本文件列表

■ 脚本列表包括但不限于以下内容

- 脚本名称，脚本功能说明
- 脚本运行主机或者数据库
- 脚本运行方式
- 脚本运行频率
- 脚本有效期

A	B	C
编号	主机IP	脚本
1	1	0 1 * * * /home/deploy/control/sec/crontab-task.sh
2	1	1 * * * * /home/deploy/yanghong/getkeylog.sh
3	1	10 0,1 * * * /home/deploy/control/search/crontab-task.sh
4	1	5,10,15,20,25,30,35,40,45,50,55,59 * * * * /home/deploy/control/app/c.sh >>/hom
5	1	0 * 2-4 * * /gboss/mddms/interface/bi/shell/BI_to_BOSS/stat_report/sp_stat_inco
6	1	0 0 3 * * /gboss/mddms/interface/bi/shell/cron_new/new/M3-00.sh 1>/dev/null 2>/
7	1	0 0 4 * * /gboss/mddms/interface/bi/shell/cron_new/new/M4-00.sh 1>/dev/null 2>/
8	1	0 0 5 * * /gboss/mddms/interface/bi/shell/cron_new/new/M5-00.sh 1>/dev/null 2>/
9	1	0 0 6 * * /gboss/mddms/interface/bi/shell/cron_new/new/M6-00.sh 1>/dev/null 2>/
10	1	0 1 * * * /gboss/mddms/interface/bi/shell/cron_new/new/1-01.sh 1>/dev/null 2>/d
11	1	0 1 * * * /gboss/mddms/interface/bi/shell/dav all/other/zhanal ec.sh 1>/dev/nu

■ 对列表中的配置文件，定期进行备份，建议每月一次。

■ 每月对脚本列表进行检查，及时处理其中的无效脚本

业务连续性演练

■整理系统高可性列表，列表中应该包括系统中所有子系统、模块的高可用性情况，列表应该包括下述

内容：

- 子系统所在平台
- 子系统的是否支持高可用
- 子系统高可用方式

■对不支持高可用性子系统，应该和用户沟通高可用性改造事宜，并计划落实

■业务高可用性演练至少每季度一次

■高可性性演练应该包括如下内容

- 有演练方案
- 方案中包括操作列表
- 有演练报告

分类	切换点	切换场景	切换方式	验证场景	操作主机IP	执行脚本
数据库	CRM中心库	1、依次停止RAC的1,2结点，停1,2节点前需要把3,4节点启起来；	自动切换	验证CRM APP服务(含AEE)上RAC1,2的连接是否依次切换到RAC3,4上，并能正常办理业务；	135.191.124.36	20
	CRM地市库	1、依次停止RAC的3,4结点，停3,4节点前需要把1,2节点启起来；			135.191.124.38 135.191.124.41 135.191.124.43	
会话缓存	会话缓存	1.保持CacheNode01缓存，停止CacheNode02缓存；	自动切换	验证已登录工号是否正常； 验证重新登录是否正常；		切换目录：cd /home/deploy/console/sma 修改配置：仅放开脚本里操作的IP（其它注释）；
		2.保持CacheNode02缓存，停止CacheNode01				切换目录：cd /home/deploy/console/sma 修改配置：仅放开脚本里操作的IP（其它注释）；
		3.保持CacheNode01缓存，停启CacheNode01主备缓存；				停止进程：./stop-master.sh; 启主进程：./start-master.sh; 停备进程：./stop-slave.sh;
	缓存全停	4.缓存全停				切换目录：cd /home/deploy/console/sma 修改配置：放开脚本里操作的IP; 停启程：./stop-sma-all.py
		1.保持CacheNode01,02缓存，停止				切换目录：cd /home/deploy/console/sma



THANK YOU