2021-10-7

作者：夏晓捷

售后运维服务规范

上海南洋万邦软件技术有限公司

# 目录

[目录 2](#_Toc156467838)

[1 准备阶段 6](#_Toc156467839)

[1.1 阶段概述 6](#_Toc156467840)

[1.2 具体流程 7](#_Toc156467841)

[1.2.1 接触阶段 7](#_Toc156467842)

[1.2.2 评估阶段 7](#_Toc156467843)

[1.2.3 咨询阶段 7](#_Toc156467844)

[1.2.4 合同阶段 7](#_Toc156467845)

[2 方案设计阶段 8](#_Toc156467846)

[2.1 阶段概述 8](#_Toc156467847)

[2.2 具体流程 9](#_Toc156467848)

[3 运维服务实施阶段 9](#_Toc156467849)

[3.1 阶段概述 9](#_Toc156467850)

[3.2 流程体系 9](#_Toc156467851)

[3.3 组织架构图 10](#_Toc156467852)

[3.4 工具架构体系图 11](#_Toc156467853)

[3.5 事件 11](#_Toc156467854)

[3.5.1 事件定义 11](#_Toc156467855)

[3.5.2 事件处理&升级流程图 13](#_Toc156467856)

[3.5.3 事件等级SLA 13](#_Toc156467857)

[3.5.4 事件超时警告流程 14](#_Toc156467858)

[3.5.5 事件升级流程 16](#_Toc156467859)

[3.6 变更 17](#_Toc156467860)

[3.6.1 变更定义 17](#_Toc156467861)

[3.6.2 变更记录 17](#_Toc156467862)

[3.6.3 变更等级SLA 17](#_Toc156467863)

[3.6.4 变更执行及分类 18](#_Toc156467864)

[3.7 问题 21](#_Toc156467865)

[3.7.1 问题定义 21](#_Toc156467866)

[3.7.2 问题来源 21](#_Toc156467867)

[3.8 知识库录入 22](#_Toc156467868)

[3.9 原则 24](#_Toc156467869)

[3.9.1 常规原则 24](#_Toc156467870)

[3.9.2 分配&升级原则 25](#_Toc156467871)

[3.9.3 挂起原则 26](#_Toc156467872)

[3.9.4 关闭原则 27](#_Toc156467873)

[3.9.5 流程关联原则 27](#_Toc156467874)

[3.9.6 日志归档原则 28](#_Toc156467875)

[3.10 ITSM记录 29](#_Toc156467876)

[3.10.1 知识库录入 29](#_Toc156467877)

[3.10.2 项目记录 32](#_Toc156467878)

[3.10.3 巡检记录 32](#_Toc156467879)

[3.10.4 学习记录 33](#_Toc156467880)

[3.10.5 其他 34](#_Toc156467881)

[3.11 安全事件管理 34](#_Toc156467882)

[3.11.1 保障前期要求 35](#_Toc156467883)

[3.11.2 保障期间要求 37](#_Toc156467884)

[3.11.3 保障后期要求 39](#_Toc156467885)

[3.12 监控告警事件管理 39](#_Toc156467886)

[3.13 监控安全告警事件管理 41](#_Toc156467887)

[3.14 漏洞扫描 43](#_Toc156467888)

[3.15 安全加固 43](#_Toc156467889)

[3.16 补丁安装 43](#_Toc156467890)

[3.17 跨团队事件沟通矩阵 44](#_Toc156467891)

[4 发布管理程序 45](#_Toc156467892)

[4.1 目的 45](#_Toc156467893)

[4.2 过程定义 45](#_Toc156467894)

[4.3 范围 45](#_Toc156467895)

[4.4 过程负责人 45](#_Toc156467896)

[4.5 主要输入 45](#_Toc156467897)

[4.6 主要输出 46](#_Toc156467898)

[4.7 职责权限 46](#_Toc156467899)

[4.8 过程测量指标 47](#_Toc156467900)

[4.9 术语 47](#_Toc156467901)

[4.10 流程 48](#_Toc156467902)

[4.11 过程描述 48](#_Toc156467903)

[4.11.1 制定发布方案 48](#_Toc156467904)

[4.11.2 发布内容评审 49](#_Toc156467905)

[4.11.3 构建测试环境、测试和验收 49](#_Toc156467906)

[4.11.4 上线规划 49](#_Toc156467907)

[4.11.5 上线审批 49](#_Toc156467908)

[4.11.6 沟通和培训 49](#_Toc156467909)

[4.11.7 分发和部署 49](#_Toc156467910)

[4.11.8 更新配置库 50](#_Toc156467911)

[4.11.9 发布关闭 50](#_Toc156467912)

[4.11.10 发布报告 50](#_Toc156467913)

[4.12 相关文件 50](#_Toc156467914)

[4.13 相关记录 50](#_Toc156467915)

[5 附件 51](#_Toc156467916)

[附件1：《潜在项目跟踪表》模板 51](#_Toc156467917)

[附件2：《需求调研报告》模板 52](#_Toc156467918)

[附件3：《可行性分析报告》模板 55](#_Toc156467919)

[附件4：《会议纪要》模板 58](#_Toc156467920)

1. 准备阶段
   1. 阶段概述

|  |  |  |  |
| --- | --- | --- | --- |
| **分阶段** | **责任人** | **工作内容** | **输出** |
| 接触阶段 | 售前人员  销售人员 | 一般针对刚开始接触的潜在客户，该阶段售前人员与销售人员一起拜访潜在客户，进行初步沟通，沟通方法有：口头交流、PPT演示、系统功能演示等，通过沟通了解客户初步的需求和思路，为下一阶段做铺垫 | 《潜在项目跟踪表》  《需求调研报告》 |
| 评估阶段 | 售前人员  销售人员  技术工程师  项目经理 | 针对上一阶段所得的《需求调研报告》，从技术及经费两个维度考量分析，最终得出该项目需求是否有进一步投入及跟进的价值 | 《可行性分析报告》 |
| 咨询阶段 | 售前人员  销售人员  技术工程师  项目经理 | 该阶段目的是为客户提供针对性的解决方案，在初步接触的基础上，对客户的需求和思路进一步深入了解，根据情况整理出专业的解决方案类型的Word文档或演示用PPT等，目的是提出潜在的项目具体工作任务（包括范围、内容、合理的预算等），引导客户的思路，取得客户的初步信任 | 《专项解决方案》（Word或PPT）  《会议纪要》 |
| 跟踪阶段 | 售前人员  销售人员  项目经理  技术工程师 | 在本阶段售前人员的工作是积极配合客户逐步推进项目落地，包括根据意见修改上一阶段输出物《专项解决方案》 | 《专项解决方案》  《会议纪要》 |
| 合同阶段 | 售前人员  销售人员 | 在本阶段售前人员及销售人员需全力配合客户促成项目合同签订，在公司内部通过《成本核算单》审批流程 | 《合同》  《成本核算单》 |

注：

《潜在项目跟踪表》模板参考【附件1】

《需求调研报告》模板参考【附件2】

《可行性分析报告》模板参考【附件3】

《会议纪要》模板参考【附件4】

《合同》模板参考【附件5】

* 1. 具体流程
     1. 接触阶段

1. 接触阶段开始，由售前人员建立《潜在项目跟踪表》
2. 由售前人员与销售人员一起拜访潜在客户，进行初步沟通
3. 由售前人员每月更新《潜在项目跟踪表》
4. 由售前人员编制《需求调研报告》，进入下一阶段：评估阶段
   * 1. 评估阶段
5. 评估阶段开始，由售前人员协同技术工程师、项目经理，对上一阶段产物《需求调研报告》进行深入分析，从技术及经费两个维度考量分析（售前人员与技术工程师确认技术可行性，与项目经理确认项目周期、设备资源、人员资源分配的可行性，与项目经理及销售人员确认预算及成本的可行性）
6. 售前人员编制《可行性分析报告》，最终必须得出结论：该项目需求是否有进一步投入及跟进的价值，进入下一阶段：咨询阶段
   * 1. 咨询阶段
7. 咨询阶段开始，由售前人员根据之前阶段输出物《需求调研报告》《可行性分析报告》编制《专项解决方案》，并在公司内部通过会议的方式确认方案后发送给客户
8. 由售前人员协调各方：客户、销售人员、项目经理、技术工程师，对初步提出的《专项解决方案》进行修订，最终定稿《专项解决方案》，并在公司内部通过会议的方式确认方案后发送给客户 ，进入下一阶段：合同阶段
   * 1. 合同阶段
9. 由销售人员编制《合同》与《成本核算单》，协同售前人员共同确认上述两份文件
10. 公司内部通过《合同》《成本核算单》审批流程，由销售人员与客户签订正式《合同》，至此准备阶段全部结束
11. 方案设计阶段
    1. 阶段概述

|  |  |  |  |
| --- | --- | --- | --- |
| **分阶段** | **责任人** | **工作内容** | **输出** |
| 合同录入阶段 | 销售人员  项目经理 | 项目经理根据销售所提供的合同，将其录入至公司《项目管理系统》，对客户全称、公司内部项目号、项目名称、项目周期、项目关联部门、项目关联团队、项目工作范围、项目人天数、项目外包成本、项目人员成本、项目验收条件、内核成本预估进行录入 | 《项目管理系统-项目登记》 |
| 信息归集 | 项目经理  技术工程师 | 在正式进入运维服务阶段前，需对客户的整体环境进行排摸，并形成各类记录型文档 | 《系统CI信息登记表》  《服务器清单》  《网络拓扑图》  《机柜示意图》（非必须）  《端口连接表》（非必须） |
| 项目计划 | 项目经理  技术工程师 | 在本阶段，项目经理需协同技术工程师，就客户现状及最终目标进行沟通设计，收集材料，确定思路并由项目经理最终完成《工作说明书》《项目管理计划》的编制 | 《工作说明书》  《项目管理计划》（包括成本、进度、沟通、质量、风险）  《会议纪要》 |

注：

《系统CI信息登记表》模板参考【附件6】

《服务器清单》模板参考【附件7】

《机柜示意图》模板参考【附件8】

《端口连接表》模板参考【附件9】

《工作说明书》模板参考【附件10】

* 1. 具体流程

1. 合同录入阶段开始，项目经理根据销售所提供的合同，将其录入至公司《项目管理系统》，进入下一阶段：信息归集阶段
2. 信息归集阶段开始，由项目经理协同技术工程师对客户的整体环境进行排摸，并形成各类记录型文档，进入下一阶段：项目计划阶段
3. 项目计划阶段开始，由项目经理协同技术工程师，就客户现状及最终目标进行沟通设计，收集材料，确定思路并由项目经理最终完成《工作说明书》《项目成本管理计划》《项目进度管理计划》《项目沟通管理计划》的编制
4. 由项目经理将《工作说明书》发送给客户，并根据反馈进行修订，最终完成《工作说明书》的定稿
5. 由项目经理组织公司内部会议，内部完成《项目成本管理计划》《项目进度管理计划》《项目沟通管理计划》的审批，并报备给项目管理办公室，至此方案设计阶段全部结束
6. 运维服务实施阶段
   1. 阶段概述

|  |  |  |  |
| --- | --- | --- | --- |
| **分阶段** | **责任人** | **工作内容** | **输出** |
| 项目实施 | 项目经理  技术工程师 | 项目经理带领技术工程师按照《工作说明书》所约定内容实施运维服务 | 《故障处理报告》  《系统应急演练报告》 |

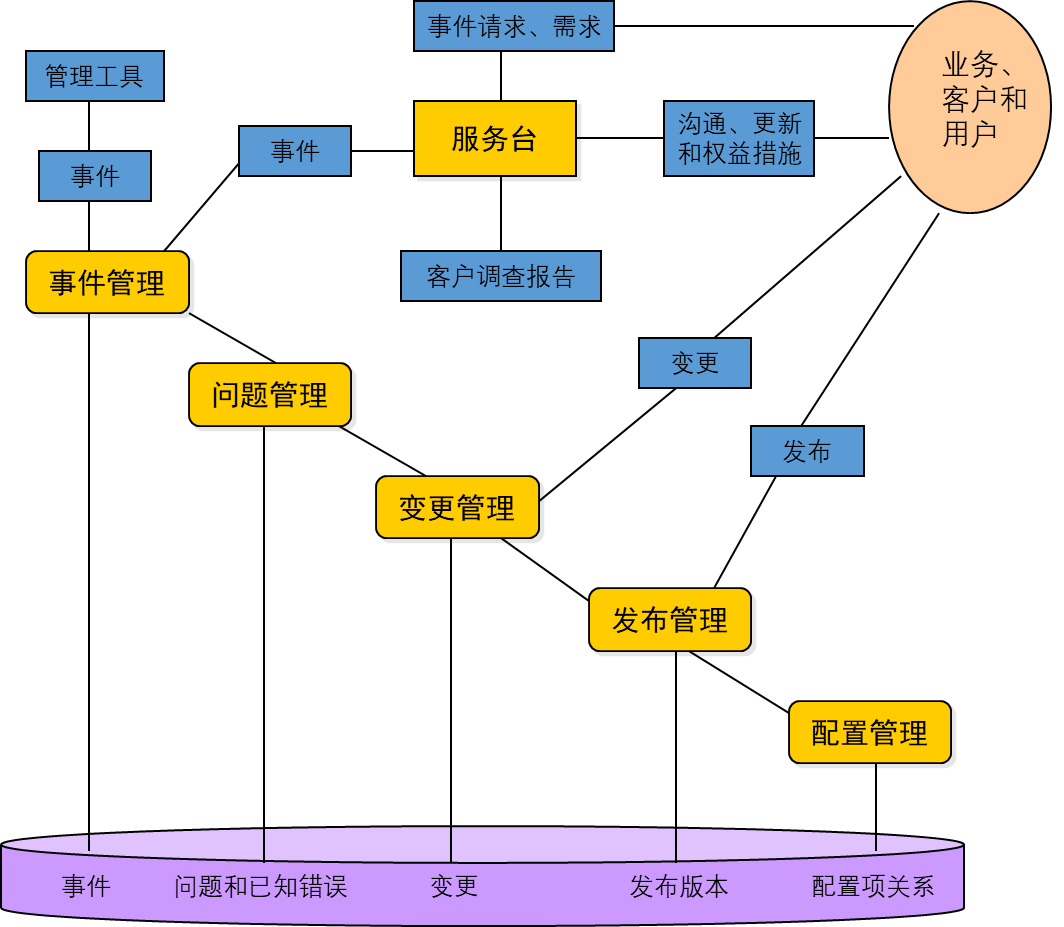
注：

《故障处理报告》模板参考【附件11】

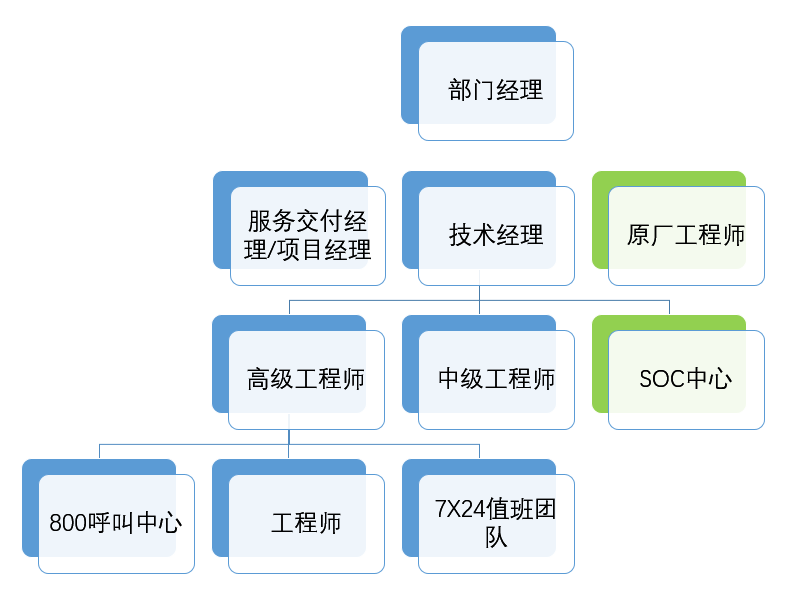
《系统应急演练报告》模板参考【附件12】

* 1. 流程体系

以事件管理，问题管理，变更管理，发布管理，配置管理为主要流程，辅以服务级别管理，能力管理，持续性管理等子流程，打造整体售后运维服务体系。



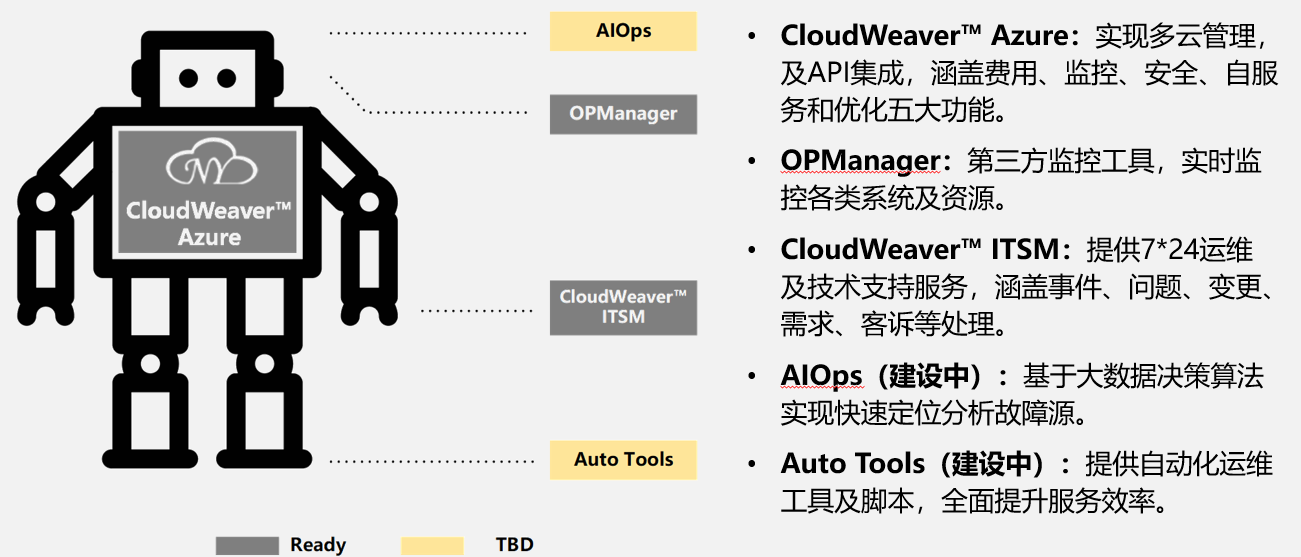
* 1. 组织架构图



* 1. 工具架构体系图

南洋运维服务工具以CloudWeaver为核心体系，做到多云管理，API集成，信息驱动，通过眼睛（OPmanager监控工具）实时监控各类系统，通过双手（ITSM服务交付系统）做到技术支持服务，事件，问题，变更，需求，客诉等处理。

计划将来以加强大脑（AIOPS大数据决策算法）能做到快速定位分析故障点，以及通过双脚（大量自开发自动化运维工具脚本）做到提升服务效率。



* 1. 事件
     1. 事件定义

事件是指在某一服务中不属于标准操作的导致或可能导致这个服务中断或服务质量下降的事件。事件管理流程是负责解决IT服务的突发事件的运维流程。它的目的是尽快恢复被中断或受到影响的IT服务，所以它的特点往往是以解决表面现象为目的，而不在于查找根本原因。

事件分类：【800】【紧急】【其他】【监控触发】

事件状态：待分配，解决中，待反馈，已关闭

故障等级：LV1严重、LV2高、LV3中、LV4低

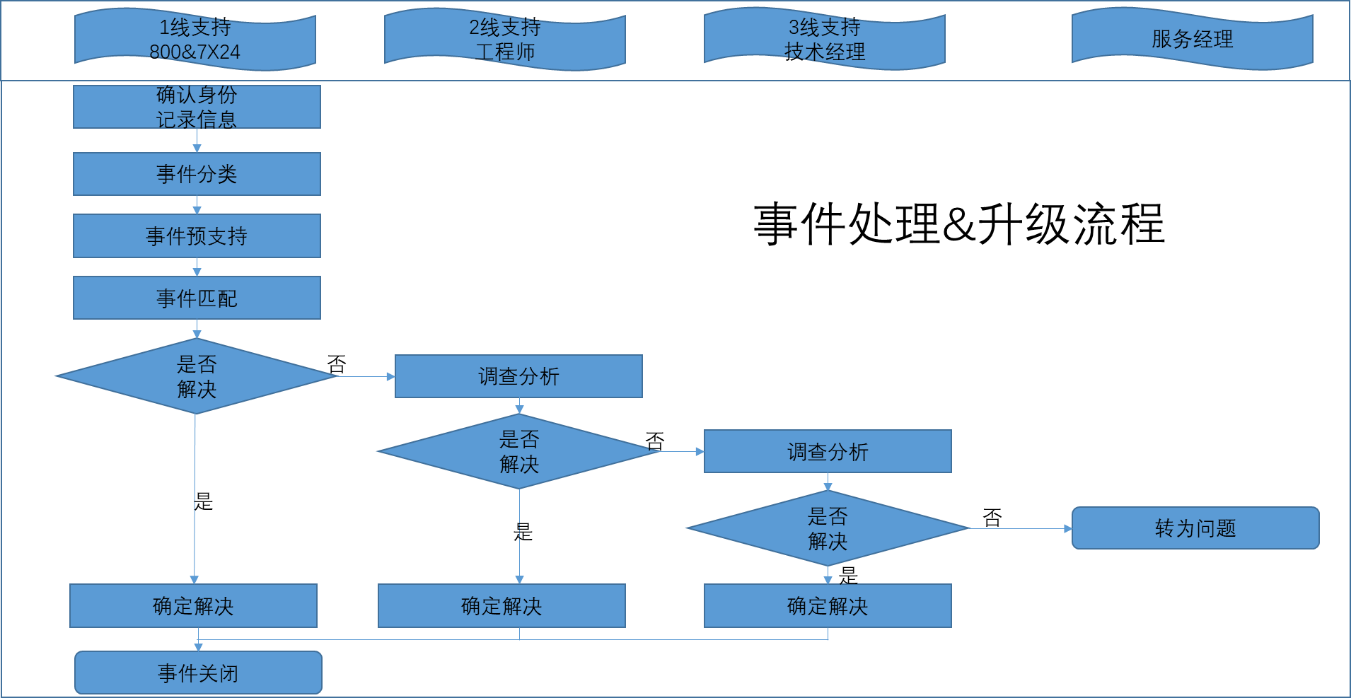
**LV1严重**：业务系统完全丧失了服务功能或丢失了所有的资源，工作无法再继续进行。界定原则：SLA协议中承诺的应用系统完全不可用，如：ERP系统崩溃、EMAIL服务器出现严重故障、SAP、A3、公共数据平台等系统不可用；或整个办公区网络主干中断，影响关键业务系统无法继续进行，如：公司主干线路中断、数据中心网络故障等。

**LV2高：**系统瘫痪或数据丢失，服务器端无法正常运行。某个业务系统丧失了重要的服务功能或丢失了重要的资源。例如：SAP数据库表不能正常访问、单台邮件服务器不可用或局部网络中断，导致主要的应用系统不能正常运行。

**LV3中：**系统局部功能模块影响部分客户使用，终端设备不稳定。业务系统丧失了较少的服务功能或丢失了较少的资源，个别用户某些业务功能不能使用。例如：一些exchange的功能特性或某一部分用户不能正常使用，但不影响整体系统的正常运行。

**LV4低：**用户操作错误，终端设备因运营商信号问题无法正常运行等。用户工作正常，没有因为该问题的存在而妨碍其工作，可正常查询和报告信息。例如：增加邮件黑白名单，添加审批人权限等。

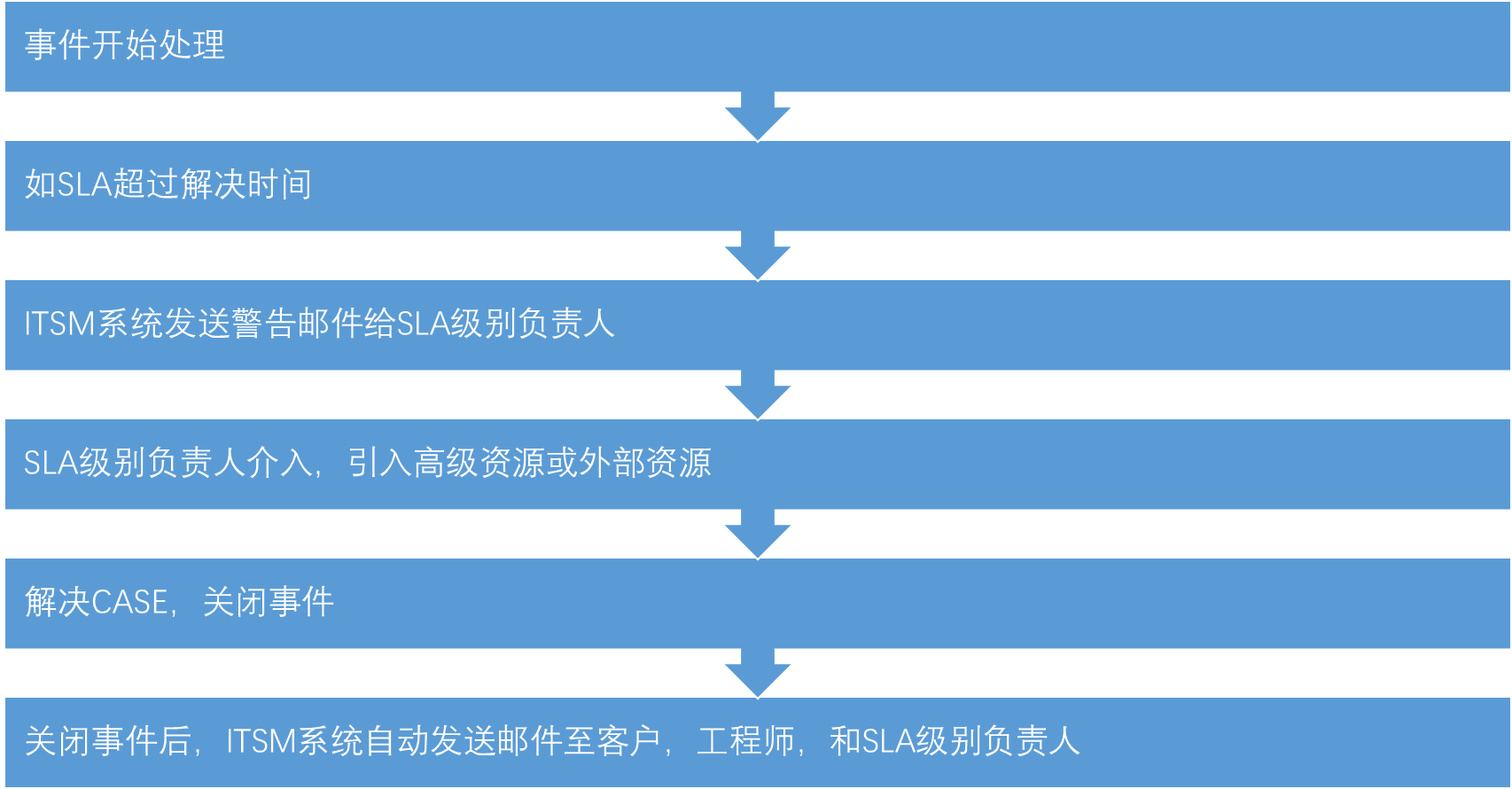
* + 1. 事件处理&升级流程图



* + 1. 事件等级SLA

|  |  |  |  |
| --- | --- | --- | --- |
| **事件等级** | **客户情况** | **上海南洋响应** | **客户响应** |
| **LV1**  **通过电话或网络提出** | 业务受灾难性影响：   * 客户核心（关键性任务）业务程序完全受损并无法适当继续工作 * 需要立即着手解决 | * 10分钟内进行首次电话响应 * 上海南洋资源在交通条件许可的情况下，最晚需在2小时内到达客户现场提供紧急救援服务 * 提供7\*24小时的服务 * 技术经理直接参与 * 通知上海南洋的高级管理人员/部门经理 * 由项目经理每1小时向最终用户报告案例进展 | * 通知客户所在地的高级管理人员 * 分配适当的资源，提供7\*24小时的配合 * 通过改变控制权迅速给予支持人员权限并响应 |
| **LV2**  **通过电话或网络提出** | 业务受严重影响：   * 客户业务严重受损或服务严重降级 * 需要在1小时内着手解决 | * 0.5小时内进行首次电话响应 * 上海南洋资源在交通条件许可的情况下，最晚需在4小时内到达客户现场提供技术支持服务 * 提供7\*24小时服务 * 高级工程师直接参与 * 通知上海南洋的运维服务经理/项目经理 * 由项目经理每2小时向最终用户报告案例进展 | * 分配适当的资源，提供7\*24小时的配合 * 通过改变控制权迅速给予支持人员权取并响应 * 通知客户管理层 |
| **LV3**  **通过电话或网络提出** | 业务受中度影响：   * 客户业务中度受损或服务中度降级，在受影响的情况下工作仍能合理继续 * 需要在营业时间的2个小时内着手解决 | * 4小时内进行首次电话响应 * 提供营业时间内的支持服务 * 由项目经理每8小时向最终用户报告案例进展 | * 分配适当的资源，提供营业时间内的配合 * 在营业时间的4个小时内通过改变控制权给予支持人员权限并响应 |
| **LV4**  **通过电话或网络提出** | 业务受最小程度的影响：   * 客户业务实质上正常进行，对服务仅造成微小障碍或无障碍 * 需要在营业时间的4个小时内着手解决 | * 第二个工作日首次电话响应 * 提供营业时间内的支持服务 * 由项目经理每16小时向最终用户报告案例进展 | * 故障所有者的准确联系信息 * 24小时内响应 |

* + 1. 事件超时警告流程



* + 1. 事件升级流程

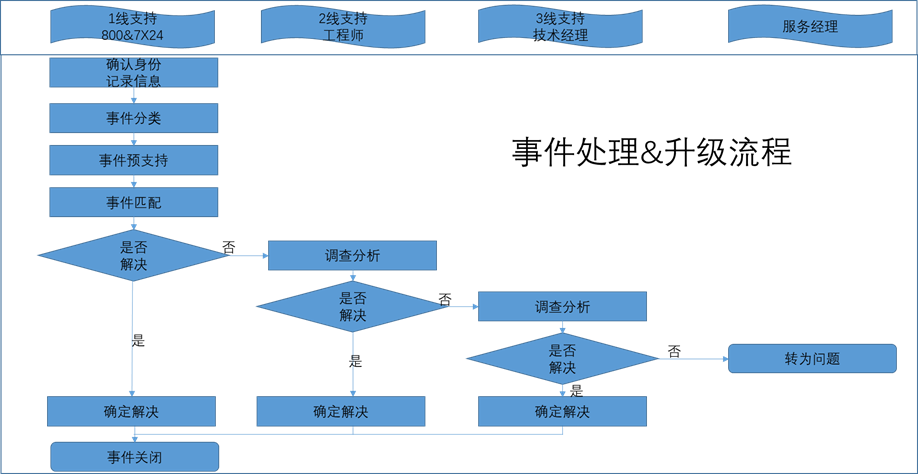
当事件未能或预计未能按照服务等级协议（SLA）的要求，得以修复时，将按照预定的时间表自动（或由服务台）发起事件升级。

另当，用户或支持队伍认为有必要时，可以要求发起事件升级。

事件升级时间表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 事件等级 | 执行人 | 工程师/技术经理/高级工程师 | 项目经理/服务交付经理/高级工程师 | 备注 |
| LV1事件 |  | 8小时 | 12小时 | 开启电话会议在线实时沟通  开启原厂CASE |
| LV2事件 |  | 24小时 | 36小时 | 提交至技术经理  开启原厂CASE |
| LV3事件 |  | 72小时 | 88小时 | 提交至高级工程师  提交至技术经理 |
| LV4事件 |  | 144小时 | 160小时 | 提交至高级工程师  提交至技术经理 |
|  | 升级至 | 项目经理/服务交付经理 | 部门经理/技术经理 |  |

事件升级流程图



* 1. 变更
     1. 变更定义

变更是指在服务过程中对系统或服务所作出的各种改变，包括增补、移除和其他修改。说的再具体一点，变更的对象是两个，一个是IT基础架构，一个是IT服务（包括与流程和文档），与这两个对象相关的改变都要归入变更的范围。

* + 1. 变更记录

指经授权的变更（包括计划中的和已实施的），对哪些配置项产生影响以及怎样产生影响的详细信息的记录。比如优先权的分配情况、影响评估与授权的具体时间等。

* + 1. 变更等级SLA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **变更类别** | **响应变更** | **变更实施时间** | **变更响应率** | **变更成功率** | **测量周期** | **备注** |
| 重大变更 | 3个工作日内响应 | 按计划 | >95% | >90% | 季度 |  |
| 重要变更 | 3个工作日内响应 | 按计划 | >95% | >90% | 季度 |  |
| 一般变更 | 5个工作日内响应 | 按计划 | >90% | >90% | 季度 |  |
| 紧急变更 | 2小时内响应 | 4小时 | >98% | >90% | 季度 |  |

* + 1. 变更执行及分类

**变更确认受理**

由事件管理流程、问题管理流程、第三方提出变更请求，变更负责人确定是否需要受理变更。

**变更记录和分类**

初步为变更分配类型、风险等级等，必须提出可能会影响哪些业务系统和业务部门，以供决策参考；

变更按不同的权限及重要程度分为**重大变更、重要变更，一般变更，**在非计划时，**存在紧急变更**，通过预先设置的分类定义，执行相关的SLA标准。

**一般变更（预授权变更）**：要求很低，且造成重大服务问题的风险也极低的变更。变更经理可以无须将它们提交给CAB，就批准这些变更。

**重要变更（标准变更）**：需要做大量的工作，且对服务有切实影响的变更。这些变更在CAB会议上讨论以决定所需的工作和潜在的影响。在会议之前，相关的文档会在CAB成员，可能包括专家以及业务部门之间进行同步。

**重大变更**：需要做很大量的工作，且会影响到组织的重要部分的变更。变更经理需要有IT管理或IT筹备指导委员会的优先级授权，在此之后，变更必须提交给CAB。

**紧急变更：**在计划外，如有发生意外情况，需执行紧急变更，紧急变更需要项目经理或服务经理紧急提出变更申请，由部门经理或以上级别的领导口头同意，事后并补记相关变更的流程和记录步骤，以确保每次变更都有记录和配置更新记录。

**保证变更信息项的完整性和正确性；**

对预授权变更，直接转执行变更任务；

对非紧急不在预授权范围内的变更，直接提交变更经理，进行变更审批；

对紧急变更，确认后立刻提交给变更经理按紧急变更快速处理；

备注：预授权变更可以经由服务经理与客户代表商讨，确认日常可直接由变更执行人员处理的变更。

变更负责人必须确定该变更请求的类别和优先级以便按照不同的流程执行后续变更动作。

**变更方案**

由变更执行人员根据变更的不同等级制定相应变更相关的实施计划（如何执行）、测试计划（如何确认变更成功）、回退计划（如何确保变更失败后可还原变更前状态）。

备注：属于以往多发变更、已有相关熟练操作经验可裁剪,只在RFC中‘服务计划’简略即可。

**变更实施**

变更执行人员需提前将变更计划和具体任务发送所有实施人员。分派具体任务给每个实施人员。

**执行回退**

变更失败，必须恢复到变更之前的状态，根据之前拟定的回退计划进行，恢复生产环境；

**验证**

确认回退是否成功，进行相关数据测试等，如不成功则检查可能出现故障的环节并排除后再次执行回退直至成功；当回退成功，或回退效果不理想不得已情况下放弃，也可选择再次变更或终止此次变更。

**核实变更实施完成并监控**

汇总数据填写由该变更所引起业务中断的关键系统名称和中断时长，如果此变更涉及关键系统较多，并在中断关键业务、中断时长中填写所有的关键系统名称及关键系统中断总时长；变更执行人员负责监控该次变更的总体效果；

**变更关闭**

变更实施人员关闭变更请求。

**变更报告**

变更管理负责人每月对变更数量进行统计，对变更过程存在的问题进行分析，形成变更服务报告。变更的度量指标包括：

* 各种类型变更的数量；
* 变更期间的服务中断时间；
* 计划时间内完成的重大变更百分率；
* 未达到预期结果的变更数量。

紧急变更流程为紧急变更提供了快速处理机制，但为了良好的控制，事后应尽可能通过业务管理系统平台完成变更所要求各环节加以补全。

注：变更记录建立，处理和关闭，必须要上传，并确认标题中记录变更类型，重大变更，重要变更必须要上传3个变更文件后，才可关闭。

【变更方案】：变更类型，变更背景、原有环境、原数据备份、实施步骤、时间计划、风险及回退、测试步骤

【变更实施申请表】：重大变更需要按模板填写，发送给客户，请其确认后方可执行，若不便让客户在申请表上签字，至少也需要通过邮件的方式发于客户，请其通过邮件的方式答复确认，如无客户确认，则不允许进行变更操作，以避免风险。

【变更完成报告】：变更执行人员负责监控该次变更的总体效果

* 1. 问题
     1. 问题定义

问题管理指负责解决客户服务过程中遇到的所有问题的流程。问题管理包括问题处理和问题控制，目标在于将由于IT基础架构的错误而导致的问题和事件对业务产生的负面影响降到最低，以及防止与这些错误有关的事件再次发生。为了实现这个目标，问题管理调查分析事件的根本原因然后采取相关行动改进和纠正错误。

* + 1. 问题来源

**问题的主要来源有三个：**

1. 从事件生成：当故障发生时，通过事件采取临时措施、替代方案的方式暂时解决事件，却没有了解事件的深入根源。此时可从事件管理流程生成问题并与之相关联。（由疑难事件转为问题）

LV1事件和LV2事件关闭后，由负责该事件的服务交付经理，开启一个问题记录，并进行问题记录分配。

LV3事件和LV4事件如在SLA时间内无法解决，则由服务经理与技术经理确认，将该事件转为问题记录，继续跟进处理。

1. 客户提出：在服务过程中存在的问题。（大量频繁发生的事件生成的问题。）（重大影响事件转为的问题）

3) 趋势分析后提出：通过对历史数据、统计报表等进行分析后得出的需要进行根本原因分析的结论，也可创建问题。（特定趋势事件转为的问题）

问题分类：硬件设备、软件系统、服务器、数据库、客户端等等

问题分级：严重、高、中、低（如有问题）（对应L1，L2，L3，L4）

问题状态：未解决、已解决

* 1. 知识库录入

当问题被解决时，经过项目经理确认无误后，由该问题OWNER负责将该**问题现象，处理方法，预防措施**等信息录入至知识库中，由项目经理审批确认通过后，可发布至知识库中供其他同事和客户参考阅读。

同时，如工程师或项目经理在其他途径获得有价值知识时，可以录入知识库中。

**技术经理：** 负责流程的设计、回顾和改进，审核人的任命；确认知识的分类，负责程序文件的更新维护；收集汇总流程信息，提出改进建议，制定改进计划。

**知识提交人（工程师）：**负责按要求提交知识素材并分类；负责错误知识素材反馈的确认修改和用户反馈。

**知识审核人（项目经理）：**负责新提交的知识内容正确性的审核；负责按照知识管理标准规范要求进行知识的过滤和抽取；负责错误知识抽取反馈的确认修改；负责对已有知识的定期复审，评定知识是否需合并或废止。负责知识的审核、发布和通知；定期回顾整理知识库中的知识；负责知识的汇总及分类整理；负责知识格式规范性的审核；对提交岗、审核岗的内容错误及格式不规范问题进行反馈；负责发布知识中格式不规范问题反馈的确认修改；负责知识录入和知识变更；负责定期组织知识复审。

**知识分类：**

知识库目前分为硬件、软件和其它三类：

1、硬件：

2、软件：

3、其它

**知识分类标准：**

由技术经理进行知识分类，知识的分类以能显著区分各类不同种类知识为标准，目前暂定为3种。

如产生已知知识的事件和问题，则无需记录至知识库中。

**知识库录入来源：**

问题转换成知识

互联网中有价值的案例参考

自身在以前项目经验中的知识分享

**知识库录入标准：**

知识库由各工程师撰写和提交，可根据事件处理过程中提炼有价值的知识信息提交至知识库。

1、知识库标题要求：知识库的标题格式要求用知识库分类子类加若干个汉字的简要描述合并组成。

2、归类说明：有类别归为响应类别，都找不到则归为其他。

3、知识库内容分3部分描述：

一，问题现象描述要求清晰、详细的描述症状发生的具体现象，有图片或错误日志等附件的，要求上传相应的附件，并注明“附件”；

二，处理方法对症状进行原因分析和解决方案的具体描述，解决方案中有附件标明“见附件”。内容中不要包含“问”“答”等字眼或客户信息、人员信息、日期时间等信息；

三，预防措施对该问题如何进行预防及避免下次发生做相关讲解，以避免其他客户再次发生同类问题。

4、如果内容中包含来自互联网的信息，请先将文章格式清除，之后套用知识库格式；如果来稿内容中有图片，请先将图片中的厂家、网站等水印清除，图文排版要规范。

5，知识库审核标准，该知识具有普遍意义，或具有代表意义，或者能显著提高工程师技术支持效率的知识认定。

* 1. 原则
     1. 常规原则
* 服务台（一线工程师）作为事件总负责人，监督事件的处理，负责事件的提起与关闭；
* ITSM作为统一服务平台，是事件开启，处理，关闭的统一系统；
* 从事件记录时起至事件关闭时结束，事件全生命周期监控事件的影响及处理情况；
* 所有事件都应该被记录在业务系统中，记录的信息应足够详细，包括事件处理交互过程，详细的解决方案和相应的信息；
* 所有IT支持人员按照服务级别协议规定时限对事件进行处理，当事件冲突时，对优先级为重大紧急的事件所采取的服务恢复行动，在比对其它行动的时候，将拥有优先处理级别，如果优先级别相同，则优先处理相对简单事件；
* 事件处理过程中，应持续保持与客户的沟通，通知客户事件处理进展；
* 每月产生事件管理报表，对重复发生的事件和变通方法解决的事件，应该举行定期的事件管理会议对这些事件进行评估；
* 应该定期对流程进行回顾，回顾内容包括流程关键衡量指标、流程执行效率和流程支持工具的有效性，以改进事件管理流程。
  + 1. 分配&升级原则

制定分配&升级原则的目的是确保事件在规定的解决时限内能够及时通知相关技术人员和领导，引起更多的重视，提供合适的资源，从而快速找到解决事件的方案。

* LV1的事件：
* 由事件接收者确认，如确认了事件等级为LV1，则立即分配到到技术经理，并通知相应的管理层（包含服务交付经理，部门经理，公司销售，公司高层等）（通过ITSM平台/邮件/电话），由服务经理启动LV1事件处理流程。
* 如8小时之内无法有效恢复使用，ITSM系统将发出警告提醒SLA负责人/服务经理，由服务交付经理汇报至部门经理，由部门经理开启原厂CASE。
* 如12小时内仍然无法有效解决，ITSM系统将发出警告提醒SLA负责人/服务经理，由部门经理召开一个在线电话会议，由服务交付经理，技术经理，客户IT，客户管理层，原厂工程师实时在线沟通，实时保持事件处理交流。
* LV2的事件：
  + 由事件接收者确认，如确认了事件等级为LV2，则立即分配到到高级工程师团队，并通知相应的服务交付经理（通过ITSM平台/邮件/电话），由服务交付经理启动LV2事件处理流程。
  + 如24小时之内无法有效恢复使用，ITSM系统将发出警告提醒SLA负责人/服务经理，由高级工程师汇报至技术经理，由技术经理参与一起处理。
  + 如36小时内仍然无法有效解决，ITSM系统将发出警告提醒SLA负责人/服务经理，由技术经理汇报至部门经理，由部门经理开启原厂CASE。
* LV3的事件：
  + 由事件接收者确认，如确认了事件等级为LV3，则立即分配到到工程师团队，由工程师启动LV3事件处理流程。
  + 如72小时之内无法有效恢复使用，ITSM系统将发出警告提醒SLA负责人/服务经理，由工程师汇报至技术经理，由技术经理分配至高级工程师参与一起处理。
  + 如88小时内仍然无法有效解决，ITSM系统将发出警告提醒SLA负责人/服务经理，由高级工程师汇报至技术经理，由技术经理参与处理。
* LV4的事件：
  + 由事件接收者确认，如确认了事件等级为LV4，则立即分配到到工程师团队，由工程师启动LV4事件处理流程。
  + 如144小时之内无法有效恢复使用，ITSM系统将发出警告提醒SLA负责人/服务经理，由工程师汇报至技术经理，由技术经理分配至高级工程师参与一起处理。
  + 如160小时内仍然无法有效解决，ITSM系统将发出警告提醒SLA负责人/服务经理，由高级工程师汇报至技术经理，由技术经理参与处理。
    1. 挂起原则

如事件在处理过程中，由于用户需要确认观察状态，或用户待反馈，用户正忙于其他事情等原因，导致需要暂停工作时间计算的情况下，工程师需写明理由，再将事件状态从【解决中】改为【挂起】，在【挂起】下，不会计算工作持续时间，是不计算SLA的。如客户再次发送反馈或用户给予回复时，工程师需将CASE从【挂起】状态转回【解决中】，并继续在工作日志中，添加操作记录，开始继续处理事件。

事件可多次挂起，但每次挂起后恢复处理时，都需要解除挂起。

挂起的理由必须充分有效。如有邮件往来，需将往来邮件贴入挂起理由。

* + 1. 关闭原则

由IT用户申报的事件单，关闭必须由服务台完成。

* 已关闭的事件单不允许重开，如果事件重复发生，则创建一个新的事件单。
* 事件处理人员在解决完成事件时，根据实际解决情况填写事件的结束代码，由IT用户认可获得关闭的事件单的结束代码为"成功关闭"；
* 监控平台产生的事件发送到服务台，由服务台分派处理人员解决并关单。
  + 1. 流程关联原则

事件管理与问题管理、变更管理、发布管理、配置管理存在以下关联原则：



* 和问题管理的关联

LV1事件和LV2事件关闭后，由负责该事件的服务交付经理，开启一个问题记录，并进行问题记录分配。

LV3事件和LV4事件如在SLA时间内无法解决，则由服务经理与技术经理确认，将该事件转为问题记录，继续跟进处理。

* 和变更管理的关联

事件处理过程中，如果需要对系统进行变更，必须按照变更管理的定义，提交变更请求单（变更单必须和事件单建立关联），变更完成后，继续事件单的处理。

LV1和LV2事件的处理过程中，如果需要对系统进行变更，必须按照变更管理的定义，提出紧急变更请求，变更完成后，补录紧急变更单，并和紧急事件单建立关联。

* 和配置管理的关联

事件处理过程中，可以通过配置管理查询相关的配置项信息以及该配置项历史上发生的事件或变更，来帮助故障的定位。

事件处理过程中，如果可以将故障定位到某个配置项，则必须将事件单与该配置项关联。

* 和发布管理的关联

发布工作结束后，可能触发新事件的产生。

发布管理应向事件管理提供发布相关信息，包括：年度发布计划，发布信息等。

* + 1. 日志归档原则

根据SOC的日志归档流程定义，运维服务过程中，在取得客户的确认后，应将重要服务器的系统日志，应用程序日志，审核日志，安全日志等日志信息做归档处理，并最少保留90天。

将归档日志保留至\\192.168.20.237\log-backup\[server-ip]\

* 1. ITSM记录
     1. 知识库录入

当问题被解决时，经过项目经理确认无误后，由该问题OWNER负责将该**问题现象，处理方法，预防措施**等信息录入至知识库中，由项目经理审批确认通过后，可发布至知识库中供其他同事和客户参考阅读。

同时，如工程师或项目经理在其他途径获得有价值知识时，可以录入知识库中。

**技术经理：**负责流程的设计、回顾和改进，审核人的任命；确认知识的分类，负责程序文件的更新维护；收集汇总流程信息，提出改进建议，制定改进计划。

**知识提交人（工程师）：**负责按要求提交知识素材并分类；负责错误知识素材反馈的确认修改和用户反馈。

**知识审核人（项目经理）：**负责新提交的知识内容正确性的审核；负责按照知识管理标准规范要求进行知识的过滤和抽取；负责错误知识抽取反馈的确认修改；负责对已有知识的定期复审，评定知识是否需合并或废止。负责知识的审核、发布和通知；定期回顾整理知识库中的知识；负责知识的汇总及分类整理；负责知识格式规范性的审核；对提交岗、审核岗的内容错误及格式不规范问题进行反馈；负责发布知识中格式不规范问题反馈的确认修改；负责知识录入和知识变更；负责定期组织知识复审。

**知识分类：**

|  |  |  |
| --- | --- | --- |
| 一级目录 | 二级目录 | 说明 |
| 安全类 | Windows |  |
| MangoDB |  |
| MySQL |  |
| Zabbix |  |
| 开源产品类 | Hadoop |  |
| Redhat |  |
| CentOS |  |
| Zabbix |  |
| Zookeeper |  |
| 微软产品类 | Windows更新 |  |
| Exchange |  |
| O365 |  |
| SCCM |  |
| SCOM |  |
| SharePoint |  |
| Sky for Business |  |
| SQL |  |
| 云产品类 | Azure |  |
| 项目专属：阿特斯 |  |  |
| 项目专属：党校 |  |  |
| 项目专属：政务云 |  |  |

**知识分类标准：**

由技术经理进行知识分类，知识的分类以能显著区分各类不同种类知识为标准，目前暂定为3种。

如产生已知知识的事件和问题，则无需记录至知识库中。

**知识库录入来源：**

问题转换成知识

互联网中有价值的案例参考

自身在以前项目经验中的知识分享

**知识库录入标准：**

知识库由各工程师撰写和提交，可根据事件处理过程中提炼有价值的知识信息提交至知识库。

1、知识库标题要求：知识库的标题格式要求用知识库分类子类加若干个汉字的简要描述合并组成。

2、归类说明：有类别归为响应类别，都找不到则归为其他。

3、知识库内容分3部分描述：

（1）问题现象描述要求清晰、详细的描述症状发生的具体现象，有图片或错误日志等附件的，要求上传相应的附件，并注明“附件”；

（2）处理方法对症状进行原因分析和解决方案的具体描述，解决方案中有附件标明“见附件”。内容中不要包含“问”“答”等字眼或客户信息、人员信息、日期时间等信息；

（3）预防措施对该问题如何进行预防及避免下次发生做相关讲解，以避免其他客户再次发生同类问题。

4、如果内容中包含来自互联网的信息，请先将文章格式清除，之后套用知识库格式；如果来稿内容中有图片，请先将图片中的厂家、网站等水印清除，图文排版要规范。

5、知识库审核标准，该知识具有普遍意义，或具有代表意义，或者能显著提高工程师技术支持效率的知识认定。

* + 1. 项目记录

当在实施一个持续性的，长期的售后服务项目时，亦需要每日记录工作量，此时就应该选择此项。比如政务云相关，系统调优项目，请统一记录为【项目】类别

**解决时间和响应时间**：项目是没有响应时间和解决时间限制的，项目整体进度由项目经理线下把控，我们ITSM系统仅仅记录工作量，暂时还不包括项目管理功能，目前还无法在ITSM中体现项目进度。

**记录格式：**举例如下

20181229-曹佳兴-今日wowdc501替换已完成，现场工作如下：

1.旧域控服务器DHCP\CA备份至共享路径，删除服务器上各角色并降级更名退域关机。

2.新硬件服务器使用相同FQDN加域，安装原有角色，并提升为域控制器完成DNS复制。

3.DHCP\CA通过备份文件还原，重新添加DFS命名空间。

4.CA验证过程中发现客户端无法向Wowdc502申请计算机证书。

报错信息：由于吊销服务器已脱机。吊销功能无法检查吊销。Error Constructing or Publishing Certificate 请求ID为2262

处理方法：CMD运行命令Certutil -CRL后重启CA服务。

5.客户端DHCP\DFS验证完成，至此wowdc501替换工作完成。

6.如沟通，按需周一至现场进行standby支持。

* + 1. 巡检记录

根据和客户预约的巡检计划，按时执行各类系统和设备定期检查工作，根据定义好的巡检模板，完成巡检报告制作工作。类别为【巡检】

**解决时间**：和项目类似，巡检是没有解决时间限制的。巡检服务安排由项目经理线下预约，并分配至工程师。

**记录格式**：客户名称-【类别】XXXXX

**示例**：

XX公司-【巡检】2018年第一季度服务器巡检

XX公司-【点检】2018年1月上海机房点检

注：巡检记录关闭，必须上传巡检报告后进行关闭

**巡检流程：**

* 预约巡检，创建ITSM巡检记录
* 上门巡检，编辑巡检报告
* 发送巡检报告，将巡检报告上传至ITSM中，并关闭记录。
  + 1. 学习记录

如平日里在公司进行了学习，或进行了动手实验，需要每日进行记录，类别为【学习】。并将客户记录为上海南洋自己

**解决时间**：和项目类似，没有解决时间限制

**记录格式：举例如下**

今日完成：

*在公司测试环境中搭建Exchange 2016，完成2台CAS和2台MBX安装*

遇到问题：

*在创建DAG时出现报错：XXXXXXXX*

后续计划：

*继续进行测试，尝试解决DAG报错*

* + 1. 其他

如有其他无法匹配的服务记录，如购买需求，服务需求，技术咨询，服务咨询，产品咨询等，记录类别为【其他】。

**解决时间**：和项目类似，没有解决时间限制。

**记录格式**：客户名称-【类别】XXXXX

**示例**：

XX公司-【其他】安全漏洞扫描咨询

XX公司-【其他】机房服务器硬件保修续保需求

* 1. 安全事件管理

坚持统一领导、分工负责、密切协同、快速响应、及时处置的工作原则，充分发挥各部门力量，共同做好突发事件的应急工作。

“不发生重大网络安全事件”原则，即安全首要原则；

“谁主管，谁负责”、“谁运营，谁负责”；

“互联网暴露面最小化”原则；

发生重大安全事件时“先关停再处置”原则。

* + 1. 保障前期要求

组织机构



针对重大活动期间的网络安全保障任务，由客户方网络安全领导小组（简称“领导小组”）统一领导中心的网络安全保障管理工作。并设立“安全保障工作小组”（简称“保障工作小组”）,协调云服务商团队，安全服务厂商团队，应用服务商团队，统一做好网络安全保障任务。

**职责划分**

领导小组负责贯彻落实法律法规和各网络安全主管部门有关国家重大活动期间的安全保障工作要求，进行任务分解和监督检查，建立跨部门联动处置机制，对处置网络安全事件进行统一指挥，在重大活动保障期间统一领导网络安全保障管理工作。

保障工作小组负责作为本次网络安全保障期间突发事件的应急联动，作为先期处置的智能团队和统一联络平台，根据既定的处理原则，履行应急联动处置突发事件，开展保障期间网络安全突发事件的预防、监测、报告和应急处置工作，并归口管理职责范围内的重大活动网络安全保障工作报告。同时根据领导小组的相关要求，制订各部门职责范围内的重大活动网络安全保障方案。保障期间如发生重大活动网络安全问题统一归口、上报至保障领导小组。

云服务商负责云平台层面的物理环境、网络、数据、安全防护服务等方面的安全保障工作。负责保障工作期间发现异常情况第一时间响应处理，并及时上报保障工作小组。

安全服务厂商负责重大活动网络安全保障工作期间各单位安全服务产品软、硬件支撑保障工作。负责数据中心整体安全监控，以及安全事件的应急处置和安全威胁的分析。

应用服务商负责各自涉及业务系统的应用安全保障工作，并提交参天制药保障期间的7\*24小时紧急联系人名单。

**管理要求**

保障工作小组的各保障部门应该制定各部门的保障方案，保障方案必须包括以下内容：保障小组名单、保障要求、保障前期和保障期间的工作内容、保障值守安排、详细的应急响应方案及流程图、常见问题的解决方案手册等内容。

保障工作小组的各保障部门应制定保障期间的值班表，明确值班要求和保障联络接口人。

**技术要求**

保障工作小组的各保障部门应该在保障前期安排针对应急响应方案的演练。

保障工作小组的各保障部门应上报在保障期间的保障信息系统对象名称与安全威胁监测预警措施。

保障工作小组的各保障部门必须对所辖信息系统进行风险评估及渗透测试等安全自查工作，并上报测试报告。对发现漏洞隐患后应及时整改，确保保障期间信息系统安全。

1. 制定工作计划

重点网络安全保障前期准备工作计划，模板如下

|  |  |  |
| --- | --- | --- |
| 时间 | 工作内容 | 责任单位 |
|  | 重点网络安全保障工作小组成立 | 客户方/领导小组 |
|  | 下发重点网络安全保障工作计划 | 客户方/保障工作小组 |
|  | 重点业务系统漏扫检查，各部门编制重保方案和保障人员名单。 | 保障工作小组/各部门 |
|  | 重保前任务确认 | 保障工作小组/各部门 |
|  | 确认重保前所有准备工作就绪 | 各小组 |

* + 1. 保障期间要求

1. 管理要求
2. 未经风险评估及渗透测试的系统或新增应用功能在保障期间不得上线运行。
3. 保障前期发现存在中、高危漏洞的系统在未修复确认以前不得上线运行。
4. 保障期间停止所有信息系统的安全扫描及渗透测试操作，关闭所有系统开发的测试环境，暂停系统开发及新功能上线。
5. 按照“互联网暴露面最小化原则”，保障期间对于可以关闭的互联网系统尽可能关闭。
6. 防护要求
7. 保障期间安全防护策略遵照最严配置原则设置，网站应进行应用防火墙（WAF）和网页防篡改防护。
8. 保障期间重要系统和相关网站应进行7\*24小时安全监测。
9. 保障措施
10. 保障工作小组的各保障部门必须对所辖信息系统安排工程师及厂商进行7\*24小时现场保障，并实行7\*24小时系统监控。
11. 保障工作小组的各保障部门，需要在保障期间安排值班人员现场监控系统的运行状况，对出现的异常事件做出及时处理，不能解决的故障应快速做出技术支持请求，尽量控制故障范围和时间。
12. 事件处置
13. 遵照“先关停再处置”原则，一旦发现网站I和II级网络安全事件（事件分级详见附件一），应用服务商需在规定时间内关停相关网站或应用，并按要求立即上报保障工作小组7\*24统一热线，由保障工作小组上报至保障领导小组。
14. 各部门发生安全事件处置后，需要提交安全事件报告给保障工作小组，由保障工作小组审核确认后上报至保障领导小组。
15. 通报机制

保障期间执行“每日安全保障日报”工作汇报。

1. 保障工作小组建立保障工作微信群，由值班人员每日三次上报安全保障情况。
2. 保障工作小组的各保障部门在保障期间需要每日提交安全保障日报，汇报安全保障情况；
3. 保障工作小组的各保障部门一旦发现安全事件，必须第一时间通报至保障领导小组，提交对应事件的网络安全事件通报。

按照安全事件等级，上报机制如下：

I级事件：15分钟内，将处理结果上报至领导小组。

II级事件：30分钟内，将处理结果上报至领导小组。

III级事件：当天18:00以日报的方式上报至领导小组及保障工作小组。

IV级事件：当天18:00以日报的方式上报至领导小组及保障工作小组。

* + 1. 保障后期要求

1. 保障工作小组的各保障部门在保障结束后，需要分别编写保障总结报告，并提交给保障领导小组。
2. 保障领导小组针对保障工作小组在保障期间发现的安全问题，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。
   1. 监控告警事件管理

**告警事件（EVENT）定义：**

告警事件（EVENT）是指在监控系统中发现监控对象产生的警告事件，可能是系统日志等，应用程序日志告警等。当告警事件出现时，会由监控系统发出警告通知邮件，发送至相应1线团队和相关负责人，由1线团队通过ITSM系统手动开启事件，并进行事件分类和事件预处理，再进行事件分配，事件处理，最后将事件关闭。

**处理定义：**

当由系统中发出的Critical级别的

**监控告警事件（EVENT）处理流程如下：**

* 1. 监控安全告警事件管理

**安全告警事件（Security EVENT）定义：**

安全告警事件（Security EVENT）是指在监控系统中发现监控对象产生的安全警告事件，可能是安全日志，审核日志等。当安全告警事件出现时，会由监控系统发出通知邮件，发送至相应1线团队和相关负责人，由1线团队通过ITSM系统手动开启事件，并进行事件分类和事件预处理，再进行事件分配，（如有已经对接到ITSM平台的系统，将会自动发送邮件至指定邮箱，由系统自动开启CASE并分配指派）经工程师处理后，最后将事件关闭。

**安全告警事件（Security EVENT）处理定义**

当由系统中发出的Critical级别的

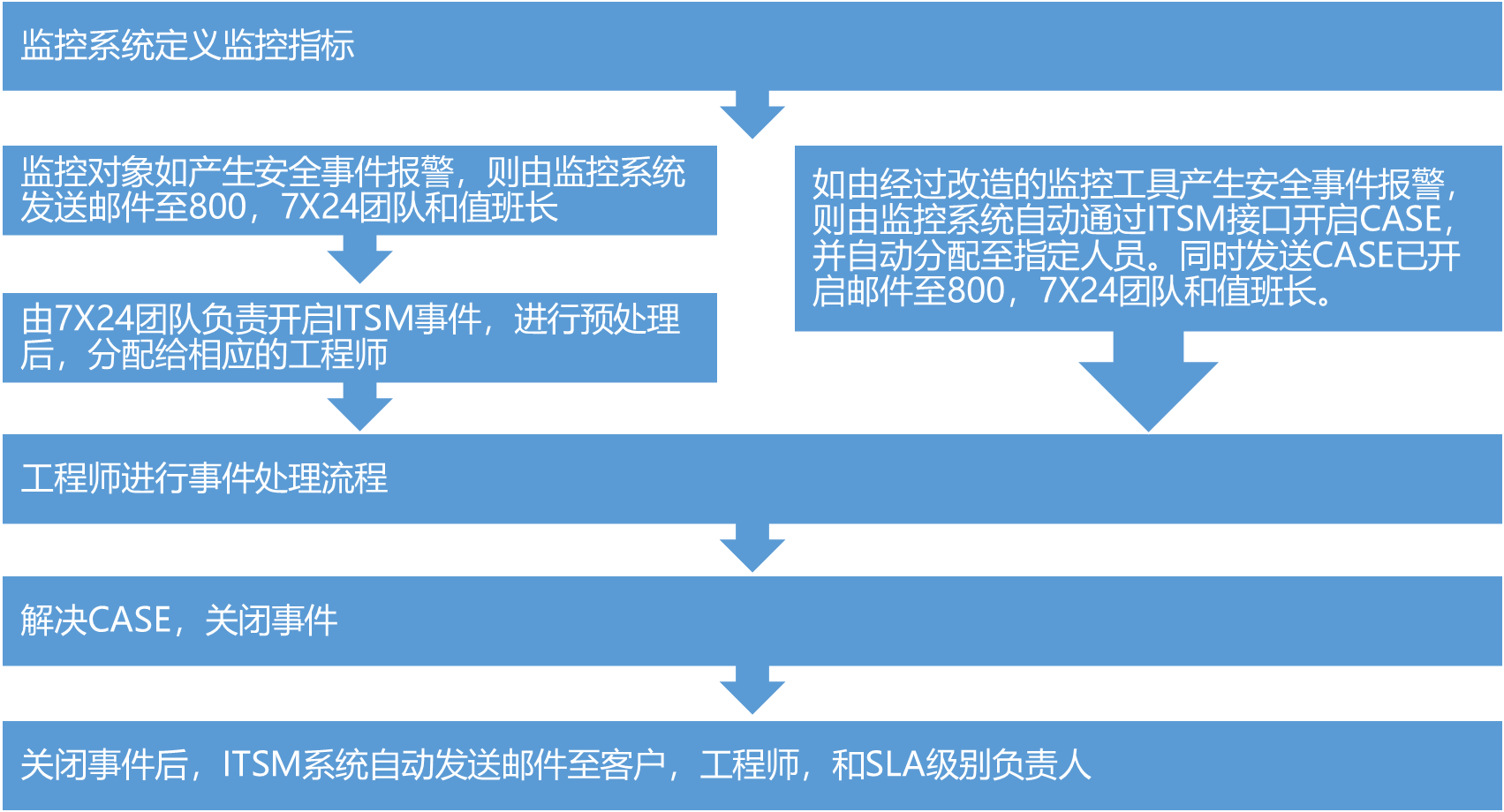
当由系统发出审核失败的

**安全告警事件（Security EVENT）保留时间**

安全告警事件（Security EVENT）需要保证可保留90天以内的安全告警事件（Security EVENT）日志，以便日后做事后审计。

安全告警邮件自动发送至800邮箱，并另行归档至mosupport@nysoftland.com.cn，该邮箱中的数据需保留90天以上，以备审计。

**安全告警事件（Security EVENT）处理流程如下：**



* 1. 漏洞扫描
* 客户提出需求
* 工程师制作漏扫方案

1. 说明漏扫原因
2. 服务器范围
3. 修复方法及详细步骤
4. 风险及回退步骤
5. 测试步骤
   1. 安全加固

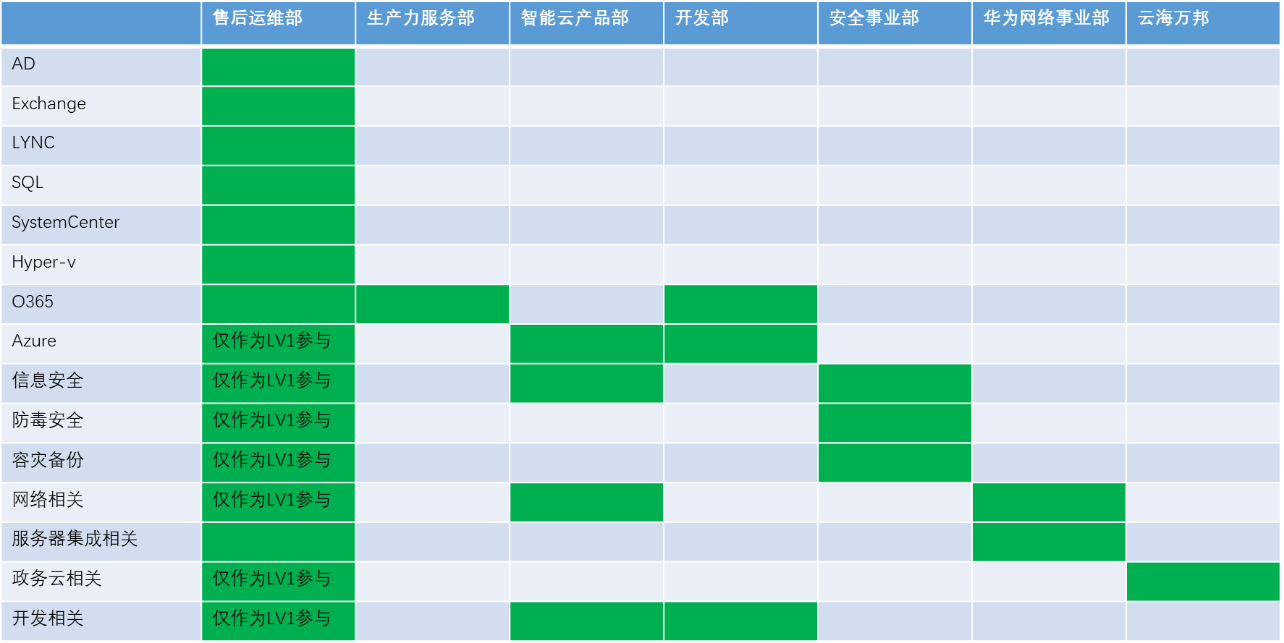
* 客户提出需求
* 工程师制作安全加固方案
* 确定安全加固流程
* 制作安全加固步骤：
* 准备工作

1.收集系统信息

2.做好备份工作

3.加固系统

* 复查配置
* 应急恢复
* 确认安全加固内容
  1. 补丁安装
* 向客户阐明目标和用途
* 说明范围
* 安全补丁的风险与影响评估
* 在系统环境中实施补丁
* 制作补丁回退计划，并向客户确认
  1. 跨团队事件沟通矩阵



由于南洋实行首问负责制，所以跨团队转记录及其流转时间，都会被记录在SLA解决时间中，所以希望首问工程师和服务经理，能及时跟进各类跨团队CASE，督促2线及时解决，或及时PENDING等待状态的CASE。

1. 发布管理程序
   1. 目的

确保与管理系统的发布是可追溯的和安全的，确保只有正确的、经过批准和测试的版本才能被安装；

在发布的规划和试运行期间与用户进行沟通并考虑他们的期望；

确认所有最终发布软件正本的拷贝是安全可靠的，确保软件的原始拷贝被安全地存放在固定位置以及配置管理数据库(CMDB)得到及时的更新；

确保所有的软件变更都得到发布，而且发布过程是安全和可追踪的。

* 1. 过程定义

发布管理是采用一种项目规划的方法来实施IT环境中的变更，负责处理变更项目所有技术和非技术方面的问题。

在现实的IT模式中，一般变更都会在复杂、关联的环境中产生变化，因此，配置项的发布和实施需要进行慎重的规划。一项发布是一组新的或变更后的配置项，经过测试后被导入实际运营环境的过程。

* 1. 范围

发布管理涉及的范围包括：

1 公司的信息系统版本升级发布。Ⅱ变更的信息发布

* 1. 过程负责人

发布管理负责人

* 1. 主要输入

|  |  |
| --- | --- |
| **输入** | **来源** |
| 变更方案 | 变更管理 |
| 发布计划 | 产品集成部 、运维服务部 |

* 1. 主要输出

|  |  |
| --- | --- |
| **输出** | **去向** |
| 发布方案 | 本次发布的影响范围及涉及的业务系统。 |
| 测试验收报告 | 发布管理过程负责人及相关责任人 |
| 上线计划 | 发布管理过程负责人、相关责任人及涉及的业务单位 |

* 1. 职责权限

发布管理负责人主要具有以下职责：

1. 定义并维护发布管理流程文件及所需要的记录模板；
2. 管理发布管理流程的实施；
3. 确保发布管理流程目标的实现；
4. 识别发布管理过程中存在的问题并提出改进措施；
5. 定期向服务管理负责人汇报实施过程中存在的问题；
6. 负责发布方案的审批。

发布负责人主要职责：

1. 负责发布方案的落实；
2. 负责发布计划的安排，以及在发布过程与用户的沟通协调工作；
3. 负责整个发布过程的跟踪，直到关闭；
4. 确保发布前的测试是可靠、稳定的；
5. 协助发布管理负责人不断完善发布管理流程。

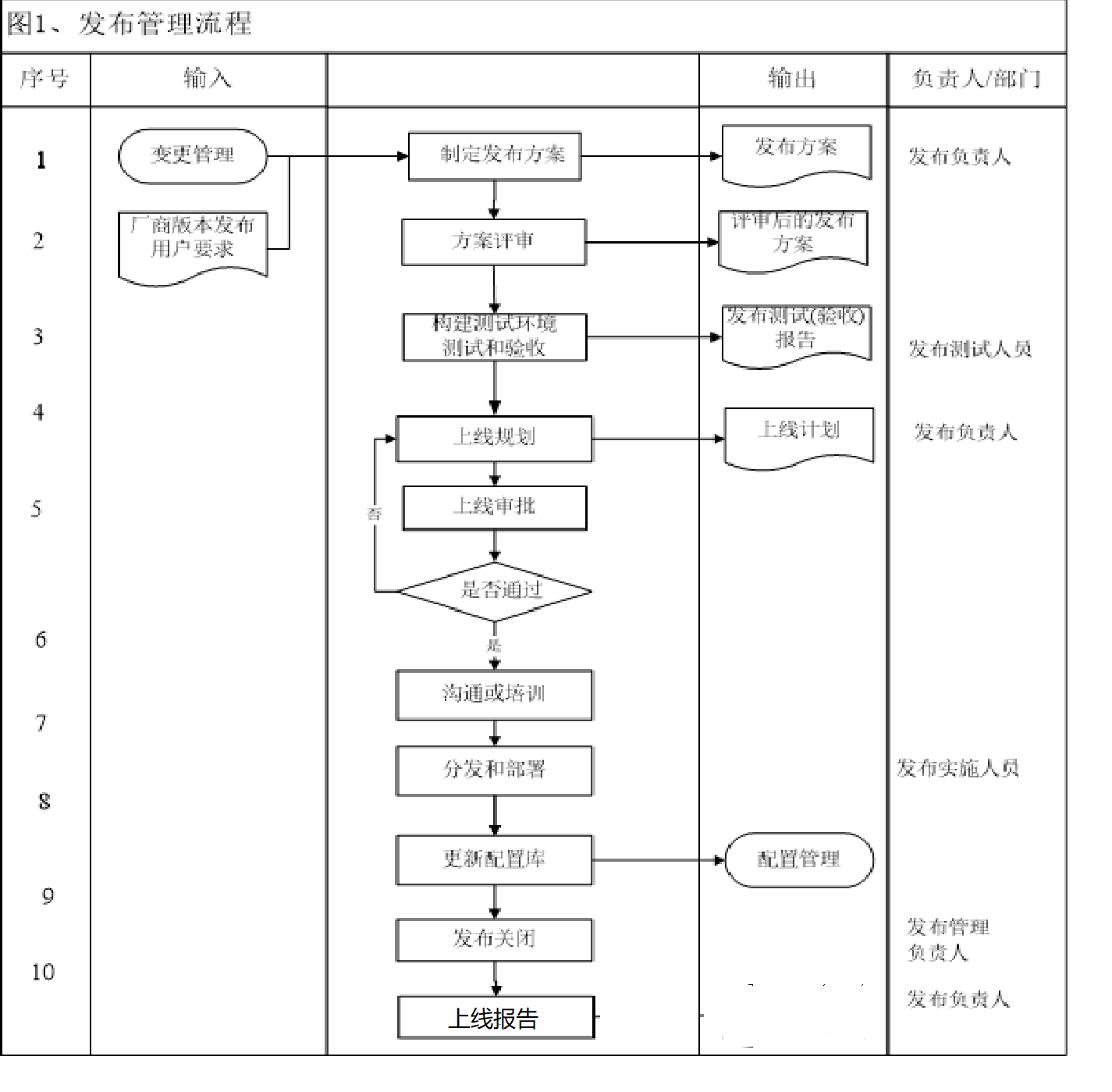
发布测试人员主要职责：

1. 根据发布方案和计划进行版本的测试；
2. 提交测试报告。
   1. 过程测量指标

* 成功发布数
* 发布导致的事件或问题数量
  1. 术语

|  |  |
| --- | --- |
| **术语** | **定义** |
| 发布 | 发布管理是采用一种项目规划的方法来实施IT环境中的变更，负责处理变更项目所有技术和非技术方面的问题。 |
| 变更 | 变更是指在维护过程中对系统或服务所作出的各种改变，包括增补、移除和其他修改。 |
| 发布方案 | 实施发布所制定的详细方案。 |
| 上线计划 | 有关发布部署和用户沟通培训等的时间安排。 |

* 1. 流程



* 1. 过程描述
     1. 制定发布方案

发布负责人根据变更计划制定《发布方案》，发布方案一般包括：

1. 描述发布的目的和背景；
2. 描述发布影响范围；
3. 确定参与发布的部门及人员；
4. 对客户和服务支持人员的交流、准备、备案和培训；
5. 确定测试、培训、客服支持、现场部署等工作计划，包含上线规划；
6. 安排部署完成的后续工作计划；
7. 确定在发布失败情况下的退回方案；
8. 可预见问题以及相应的解决方法；
9. 确定与软、硬件有关的配置基线。
   * 1. 发布内容评审

由发布负责人牵头，有关部门负责人参与评审发布内容，评审通过后实施。

* + 1. 构建测试环境、测试和验收

根据方案，在实施之前如果需要内部测试，需要测试人员根据发布方案搭建测试环境。内部测试，包括软件功能测试以及安装流程等方面的测试。测试完成后则完成系统程序的验收。测试和验收结果将在《发布测试报告》中体现。测试结果得到认可后安排上线。

* + 1. 上线规划

通常情况下发布内容包括：已经确定了上线计划，个别重大发布可对原有发布计划的拓展，其中要说明安装和测试预期结果，并制作详细的上线时间安排、工作安排和详细的上线步骤、回退计划等。

* + 1. 上线审批

通常情况下发布内容审批时已对《上线计划》也同时确认。

* + 1. 沟通和培训

系统版本升级部署前，需要对服务支持人员进行沟通、知识更新培训，保障发布后的客服支持工作；需要对企业用户相关人员进行沟通和培训，发布上线通知，使得用户明确软件上线后对其工作有何影响，必要时对用户进行培训。

* + 1. 分发和部署

经过环境构建、测试和试运行后，可进行软件的上线部署工作。系统升级时填写《变更记录》。

* + 1. 更新配置库

发布实施完成后，发布人员更新配置库的配置项信息。

参照《配置管理程序》。

* + 1. 发布关闭

发布实施人员整理发布资料，对资料归档给配置管理员，最后由发布管理负责人关闭。

* + 1. 发布报告

发布完成后，对用户提出的因为升级导致的错误或问题，由信息部填写《升级反馈表》，收集如下的信息：

* 发布引起的事件或问题数量；
* 发布的数量。

对发布数据进行分析，找出存在的问题，并提出纠正或预防措施，编写出《发布报告》，成为服务报告的一部分。

* 1. 相关文件

《变更管理程序》

《配置管理程序》

* 1. 相关记录

《变更记录》

《发布方案》

《上线计划》

《发布测试报告》

《上线报告》

1. 附件

附件1：《潜在项目跟踪表》模板

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 客户 | 销售 | 事宜 | 预估合同金额 | 目前状态 | 备注 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

附件2：《需求调研报告》模板

XXXX有限公司

运维服务需求（20XX年）

上海南洋万邦软件技术有限公司

目录

[第一章：总则 3](#_Toc64905235)

[1.1工作范围 3](#_Toc64905236)

[1.2.规范和标准 3](#_Toc64905237)

[第二章：运维服务需求 3](#_Toc64905238)

[2.1服务范围需求 3](#_Toc64905239)

[2.2服务内容需求 3](#_Toc64905240)

[2.3系统检修需求 4](#_Toc64905241)

[2.4业务应用分析要求 4](#_Toc64905242)

[第三章：进度需求 4](#_Toc64905243)

[3.1服务期限： 4](#_Toc64905244)

[3.2计划时间安排 4](#_Toc64905245)

[第四章：服务质量要求 5](#_Toc64905246)

[第五章：人员要求 5](#_Toc64905247)

**第一章：总则**

1.1工作范围

2.规范和标准

**第二章：运维服务需求**

2.1服务范围需求

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 系统名称 | 应用范围 | 备注 |
|  |  |  |  |
|  |  |  |  |

2.2服务内容需求

|  |  |  |
| --- | --- | --- |
| 序号 | 项目 | 备注 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

2.3系统检修需求

2.4业务应用分析要求

**第三章：进度需求**

3.1服务期限：

3.2计划时间安排

满足运维进度要求

|  |  |  |
| --- | --- | --- |
| 内容 | 完成时间/日期 | 备注 |
| 运维人员进场 |  |  |
| 运维服务 |  |  |
| 验收 |  |  |

**第四章：服务质量要求**

**第五章：人员要求**

附件3：《可行性分析报告》模板

**XXX可行性研究报告**

完成人:

上海南洋万邦软件技术有限公司

目录

[1.引言 1](#_Toc64905353)

[1.1编写目的 1](#_Toc64905354)

[1.2背景 1](#_Toc64905355)

[1.2术语定义 1](#_Toc64905356)

[1.3相关文档 1](#_Toc64905357)

[2.组织机构与业务范围 2](#_Toc64905358)

[2.1组织概况 2](#_Toc64905359)

[2.1各部门业务范围及职能说明 2](#_Toc64905360)

[3可行性综合评述 2](#_Toc64905361)

[3.1经济可行性 2](#_Toc64905362)

[3.2技术可行性 3](#_Toc64905363)

[3.3管理可行性（略) 3](#_Toc64905364)

[4．方案选择 3](#_Toc64905365)

[4.1 首选方案 3](#_Toc64905366)

[4.2可选方案: 3](#_Toc64905367)

[5.项目发展概况 3](#_Toc64905368)

[6.项目进度计划 3](#_Toc64905369)

[7.已进行的项目及其成果 3](#_Toc64905370)

[8.存在问题及建议 3](#_Toc64905371)

[9.可行性研究结论与建议 3](#_Toc64905372)

**1.引言**

**1.1编写目的**

说明可行性分析的必要性。

**1.2背景**

简述项目的来源、现状,研发组织，要求，目标等。

**1.2术语定义**

将该可行性分析中的术语、缩写词进行定义。

**1.3相关文档**

当该文档变更时，可能对其他文档产生影响，受影响的文档叫相关文档，需将它们列出。

**2．组织机构与业务范围**

2.1组织概况

2.1各部门业务范围及职能说明

**3可行性综合评述**

3.1经济可行性

对需要的资金与其他资源进行估计，并分析可能的效益

3.2技术可行性

3.3管理可行性（略)

**4．方案选择**

4.1 首选方案

4.2可选方案:

**5.项目发展概况**

**6.项目进度计划**

**7.已进行的项目及其成果**

**8.存在问题及建议**

**9. 可行性研究结论与建议**

附件4：《会议纪要》模板

|  |  |  |  |
| --- | --- | --- | --- |
| **会议记录表** | | | |
| **Meeting Minutes Form** | | | |
| **会议名称**  **Meeting** |  | | |
| **会议内容**  **Topics** |  | | |
| **会议地点**  **Location** |  | | |
| **主持人**  **Host** |  | | |
| **出席人**  **Participants** |  | | |
| **会议纪要**  **Meeting Minutes** | | | |
|  | | | |
| **本周会议总结：** | | | |
| **待处理事项(Follow-up Lists)：** | | | |
| **编号 NO** | **事项 Task Description** | **预计完成时间  Plan Date** | **责任方 Owner** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |