ManageEngine
ServiceDesk Plus

航空行业安全方法论，重塑 IT 服务管理

向航空安全学运维：打造高韧性 ITSM 的 5 条核心启示



Five aviation lessons your IT team can borrow from one of the world'smost reliable industries, to deliver excellent IT service experiences.

航空行业安全方法论

重塑 IT 服务管理

向航空安全学运维：打造高韧性 ITSM 的 5 条核心启示

目录

01 引言 1

02 概述 2

03 认识齐尔克科技 3

04 航空业与 ITSM：值得认真对待的相似之处 4

05 课程一——先标准化，再起飞 5

06 课程二——搭建你的中央监控：告诉你哪里出了问题 8

07 课程三——别等警示灯亮了才动手 11

08 课程四——在事故发生前先演练 15

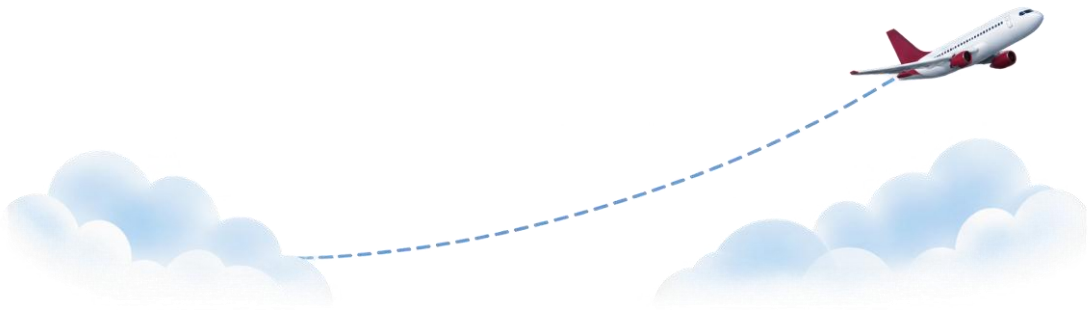
09 课程五——在下次起飞前先读黑匣子 19

10 结论 23

11 关于 ServiceDesk Plus 25

12 关于 ManageEngine 卓豪 26

13 关于作者 27



01 引言

每一次在计划外的服务中断都是有代价的：生产力下降、用户烦躁、客户关系紧张，IT 团队还需要耗费大量时间处理相应产生的用户问题。而这些问题本可以通过标准化流程规避的。对大多数服务台来说，从"被动救火"到"稳定运营"之间的差距，本质上就是流程差距。

本文找出了最容易拉开差距的五个环节，并逐一说明如何弥补——借鉴的是商业航空领域的运营原理。每一课都落在具体故事之上：为方便理解，我们从实际案例中抽象出来的一个虚构公司，**齐尔克科技**，这是一家拥有 1,200 名员工的金融服务公司，因为一次长达五小时的认证服务中断事故，痛定思痛，完成了一次彻底的 ITSM 重构。

五堂课、五种实践、一个平台

课程	ITIL 实践	带来的改变
先标准化，再起飞	变更赋能	变更相关事件更少
搭建你的中央监控	事件管理	响应更快、更有条理
别等警示灯亮起	问题管理	提前发现，减少重复
坠机演练	知识管理	团队在压力下也能执行到位
黑匣子分析	持续改进	在下次故障前就抓住规律

__说明__：每一课都对应一项 ManageEngine ServiceDesk Plus 的可用功能。

02 概述

商业航空是人类有史以来建造过的最安全的公共交通体系。2023 年全球事故率为每百万次起降 0.80 起——对于那些亲历过航空事故频发野蛮时代的工程师而言，这样的安全水平在当年简直无法想象。这份成果绝非偶然，而是层层体系化建设的结果：**严谨的事故溯源调查**、**严苛的标准化作业流程**，以及**整个行业坚持从每一次失败中持续学习**、**迭代优化。**

IT 服务台的运行逻辑与之相通。两个领域都依托高度复杂、彼此耦合的系统；团队常常需要在信息不全的条件下做出高风险决策，而服务对象都理所当然认为**业务应当持续稳定运行。**二者底层的复杂程度虽有差异，ITIL 实践也完全不同于航空领域的物理法则，但支撑时效敏感型核心业务所面临的管理挑战，远比大多数 IT 团队所感知的更为相近。

本文提炼的五大启示，正是源自航空业五项核心运营原则：**标准化作业、结构化告警处置、前瞻性监控、仿真化演练、数据驱动持续改进。**

上述每一条原则，都对应服务台建设的一项核心能力，并将通过**齐尔克科技 IT 团队**的故事逐一展开：在一场真实的故障压力中，习得这些宝贵经验。

本书所依托的 ITSM 平台为 ManageEngine 卓豪的 ServiceDesk Plus。ServiceDesk Plus 是由 AI 驱动的统一服务管理平台，涵盖事件、变更、问题、知识库、SLA 管理与数据分析等完整能力，全球已有超 100,000 家组织正在使用。文中案例所用到的平台功能包含变更模板、变更工作流、SLA 升级规则、问题模块、解决方案库以及报表分析模块。

03 认识齐尔克科技

齐尔克科技是一家拥有 1,200 名员工的金融服务公司，IT 团队 25 人。纸面上看一切正常：每月关闭数千张工单，一次解决率合理，服务台也很少违反 SLA——至少在没出什么大事的时候是这样。

然而，就在三月的一个普通周二上午，一份例行变更请求走完了齐尔克科技的变更咨询委员会（CAB）流程。这项变更是对公司认证服务的升级，之前做过很多次，CAB 20 分钟就批了。上午 10:47，变更上线。11:05，三个办公室的 1,200 名员工全部无法登录任何内部应用。客服系统瘫痪，财务无法处理发票，IT 团队一个小时之内就收到了 300 张工单。

接下来五个小时，暴露了齐尔克科技 IT 运营的所有弱点。本电子书跟随这次事件，从变更部署讲起，一直讲到团队重构系统与流程为止。我们在这次案例中，一起学习。

04 航空业与 ITSM：值得认真对待的相似之处

航空业和企业 IT 的共通之处，比大多数 IT 团队以为的要多。仔细对比，我们发现有这样三个事实。

第一，两个领域都依赖复杂且相互依存的系统，单点故障可能以不可预测的方式在许多其他系统间蔓延。比如飞机的液压系统，一旦某一路液压失效，并不是仅仅 “某个零件坏了”，很多飞控、襟翼、刹车、起落架设备都会部分或全部不可用。认证服务中断也不只是让某个应用的用户登不进去，而是阻断了所有那些依赖它的服务。

第二，两个领域都要求团队在压力下、在信息不完整的情况下做出准确判断，同时还要应对已经做出的决策带来的后果。机组资源管理（CRM）规定了**驾驶舱团队**在紧急情况下如何沟通、如何分配工作、如何达成决策——这和你的**事件管理团队**的运作方式有直接的对应关系。

第三，两个行业在最关键的时刻都没有第二次机会。飞机不能靠边临时停车，支付系统也不能让用户明天再来一次。两种情况下的失败代价都是即时反应的。

关键区别在于：航空业很早就遭遇了惨痛的灾难性的事故，促使从业人员进行严谨的调查，建立行业级的学习机制——包括强制事故报告、标准化程序和独立的事故调查。每一次失败都转化为可度量、可复用的改进。



05 课程一——先标准化，再起飞

聚焦的 ITIL 实践：变更赋能

通过确保每项变更在实施前都经过评估、授权和评审，将变更的风险与影响降到最低——依靠的是标准化程序，无论变更由谁发起都一致适用。

在 ServiceDesk Plus 中：

变更赋能通过**变更模板**和**变更工作流**来支撑，两者结合可以强制必填字段、按阶段推进审批、执行 CAB 评估，并强制要求制定回退计划。

在驾驶舱：发号施令的检查单与起飞前的 SOP

1935 年，一架波音 B-17 原型机在俄亥俄州赖特机场的首次评估飞行中坠毁。事故原因不是机械故障。而是一个小疏漏，这名经验极其丰富的老手，在起飞前忘记拆除阵风锁。他飞过很多次类似的航线，却漏掉了一个必须执行的步骤——也就是后来所说的一个标准作业程序（SOP）。

军方的应对是建立强制性的航前检查单：把"靠个人记忆兜底"这个最后一层防线直接移除掉。这个决定后来成为现代航空安全文化的基石。

如今，每一次商业航班都在 SOP 之下运行，单是发动机启动之前就有数百项任务受其约束。在空客机型上，中央飞机监控系统（ECAM）会编排强制检查项，在每一项确认之前不允许机组继续。这些程序之所以存在，是因为这样才能构建出一个系统，有了系统，不论谁坐在驾驶位上都能稳定表现，这比依赖个人的专业判断更加可靠。



阵风锁（Gust Lock）：停机时锁住副翼、升降舵或方向舵这些操纵面，防止阵风（Gust）吹打舵面、损坏操纵钢索，连杆。必须在起飞前人工拆除。如果带着阵风锁起飞会导致操纵卡死、无法控舵，历史上有多起致命事故源于遗忘解除阵风锁。

变更模板的必填字段也是同理：只有在填写变更类型、相关配置项、影响范围以及上线和回退方案之后，流程才能继续推进，以此保证在执行变更之前，所有的关键信息都是准备就绪的。

在齐尔克科技：那次漏掉的变更

引发**齐尔克科技**故障的认证服务升级，是以标准变更提交的——这一类变更按定义是**低风险**、**预审批**的。

但齐尔克科技的标准变更流程，没有要求必须填写“测试环境执行结果”反馈，也没有强制要求填写“回退计划”。提交 20 分钟后 CAB 就批了，没人做过认真的评估，因为每个人都默认"别人已经做过完整评估了"。

提交请求的技术员用的还是他一贯使用的那张表，他并不知道自己漏了什么，因为表单本身没有提示必须要采集这些信息。

齐尔克做了什么

事故之后，齐尔克科技围绕标准化重建了变更赋能流程，把**模板和工作流**当成 IT 团队的**航前检查单**。齐尔克科技采取的具体动作如下：

- **在 ServiceDesk Plus 中按类别建立变更模板**，为网络变更、认证变更和数据库变更分别配置模板。每个模板都强制要求填写受影响服务、测试环境执行结果、回退计划、变更窗口，并且为各模板配置所需的审批人。
- **配置变更工作流**，按影响范围自动匹配不同类型的变更工作流。常规变更在没有获得 IT 管理层和受影响业务部门签署的情况下，无法通过 CAB 评估阶段。标准变更只要模板字段填写完整，即可自动审批通过。

- **为每个模板增加强制性的实施前验证字段**，询问该变更是否已在测试环境中测试过。该字段在模板中被设为必填，在确认前变更无法通过变更的“规划”阶段。

变更模板减少了团队内不同成员处理的流程差异，变更工作流在每个阶段强制落实责任。当每位工程师都基于同一张模板、同一组必填字段工作时，CAB 的注意力就能放在风险评估上，而不是追问那些没填的信息。

> **航空启示**
>
> 变更模板 = 航前检查单
>
> 变更工作流 = 标准作业程序（SOP）
>
> 回退计划 = 复飞程序
>
> 强制实施前的必填字段 = 无法绕过的 ECAM 程序——因为赌不起，不能临场发挥

标准化的意义，在于让流程能稳定可靠地捕捉到个人判断可能漏掉的东西，无论这条请求是谁处理的。

你的组织该怎么开始？

从风险最高的变更类型入手，逐渐扩展。

- 找出最可能导致服务中断的两三类变更——也就是万一出错就会直接造成停服务的那些。
- 检查这几类当前的变更模板。如果缺少受**影响服务**、**测试环境执行结果**、**回退计划**必填字段，就需要补上。
- 定义清楚具体什么样的变更算高影响的紧急变更、什么样的变更算低影响的常规变更，并把判断标准写成文档。
- 为影响最大的变更类型配置变更工作流，要求在变更的**规划**阶段结束前必须明确指定变更工作流。



06 课程二——搭建你的中央监控：告诉你哪里出了问题

聚焦的 ITIL 实践：事件管理

根据事件的严重程度，对每一事件都采用结构化的、统一的响应方式，尽快恢复正常服务运营，同时将不利业务的影响降到最低。

在 ServiceDesk Plus 中：

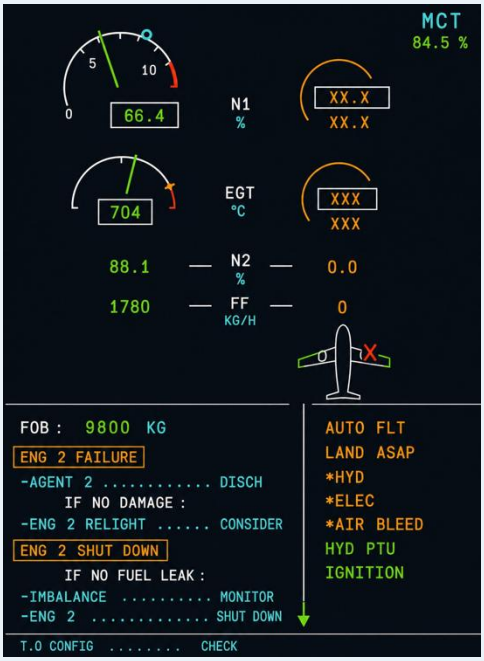
事件管理通过**事件模板**、**优先级与紧急程度字段**、**SLA 升级规则**和**通知规则**来支撑。

在驾驶舱：ECAM 与分级告警机制

2010 年 11 月 4 日，澳洲航空 QF32 航班从新加坡樟宜机场起飞，机上共有五名飞行员。起飞后不久，一起非包容性发动机故障造成灾难性损坏，同时触发了液压、燃油、飞行操纵和起落架等多个系统故障。几秒钟之内，飞机的 ECAM 就显示了 60 多条警告信息。

不幸中的万幸，后来机上 469 人全部生还，飞机安全着陆，这很大程度上要归功于 ECAM 的设计方式。它不是把所有告警同时抛出来，而是按严重程度排序、依次呈现，并为每一条告警提供对应的处理动作。机组在 90 分钟内系统性地逐条处理完毕，随后安全返回新加坡，未再发生其他险情。

波音的对应系统是发动机指示与机组告警系统（EICAS）。两者建立在同一个原则之上：在高压情境下，**机组成员不应当自己去判断优先级**——这个判断由系统替他们做出。



空客 ECAM 的监视系统：按严重程度分级提示故障时直接给出对应的处理动作，自带电子检查清单。其中红色表示危险；橙色表示故障；蓝色表示对应的处理动作；绿色为正常状态；白色为备忘与提示信息

ServiceDesk Plus 的工作逻辑与之相同：借助事件优先级、SLA 升级机制，保障团队优先处理对业务影响最大的问题，每一步操作都有明确规定，即便处于高压场景下也同样适用。

在齐尔克科技：50 分钟才召集起应急指挥室

齐尔克科技的认证服务故障在上午 11:05 蔓延开来时，三个监控工具同时告警。一个发了邮件，一个给基础设施团队发了短信，第三个在 ITSM 平台里记录了一条严重事件——但这条告警并没有配置对应的升级策略。第一响应人确认这张工单，手动指派给应用团队；应用团队又把问题手动升级给基础设施团队，基础设施团队再打电话给厂商。整整 50 分钟过去，才有人确定这是重大事件。

但此时，工单已经积压超过 300 张。没有分级的事件分类，没有重大事件预案，没有定义好的升级路径。整个团队都在临场发挥——就像当时的 QF32 的机组，如果在 ECAM 同时抛出 60 条未分级的告警、既无先后顺序也无对应处置程序，全靠机组乘员临场发挥，后果就不堪设想了。

齐尔克做了什么

意识到"没有流程"让他们白白损失了近一小时的黄金响应时间，齐尔克科技对事件管理流程做了全面重构，把分级分类体系、正式的升级路径和专门的"事件经理"角色直接配置进 ServiceDesk Plus。齐尔克科技梳理这些动作的优先级如下：

- **定义三个事件优先级层级，并写明判断标准**，确保分类标准一致：P1 用于业务关键事件——多项服务中断且生产业务受影响；P2 用于服务降级——部分功能仍可用且有临时解决方案；P3 用于孤立的轻微问题，无实质性业务影响。
- **编制 P1 事件预案**，覆盖事件发生后五分钟内该通知谁、何时升级到 IT 管理层、如何与受影响的业务部门沟通、什么情况下需要引入外部厂商，以及如何在 ServiceDesk Plus 中持续维护事件时间线。
- **在 ServiceDesk Plus 中配置 SLA 升级规则**，让它们在响应时限和解决时限违反**之前**触发，而不是之后——这样技术员和值班经理就能在**还有时间采取行动时**提前得到通知。P1 事件直接向值班经理发送短信告警和电话语音告警，而不只是发邮件告警通知。
- **为每一张 P1 事件指派事件指挥人**，明确指定一个人，拥有协调响应、管理对外沟通和做出升级决策的清晰权限。

> **航空启示**
>
> 按优先级对事件分级 = ECAM 的警告/提示/咨询三级体系
>
> 事件预案 = ECAM 处置程序顺序
>
> 事件经理 = 机长
>
> P1 自动升级 = 空管宣布紧急状态并执行对应策略

那次让齐尔克科技花了五小时才解决的认证服务事故，如果使用这套新的事件管理机制。在 10 分钟内就 IT 团队就能组件起紧急事件处理团队。IT 团队还是同一个，变的是提前梳理了"如何响应"的框架，并且在发生时，系统能够自动提示对应的处理动作，不再靠个人的临场发挥。

你的组织该怎么开始?

先把判断标准写下来，每一步都依赖它。

- 写出具体标准，明确什么样的事件算 P1、什么样的算 P2。这套区分需要足够清晰，让团队内容技术员都能一致地给事件定级。
- 起草一页的 P1 事件预案：明确联系人顺序、通知时限与上报路径，可快速查阅，聚焦故障发生第一时间的联络协同。不必面面俱到，有用就行。
- 为 P1 事件指定事件经理，并至少指定一名备用联系人，以防事件经理主联系人不在。
- 检查当前的 SLA 升级规则，确认至少有一档规则是在 SLA 时限到期**之前**触发，而不只是 SLA 时限违约之后。



07 课程三——别等警示灯亮了才动手

聚焦的 ITIL 实践：问题管理

通过识别根本原因、管理临时解决方案和已知错误，降低事件发生的可能性与影响，让团队从被动救火转向主动的服务健康保障。

在 ServiceDesk Plus 中：

问题管理通过**问题模块**来支撑：创建问题记录、关联相关事件，并跟踪根因分析直至彻底解决。对事件数据的聚类分析，可以找出任何单张工单都看不出来的规律——这让团队有可能从"解决故障"转向"消除产生故障的条件"。

在驾驶舱：GPWS 与主动预警的价值

20 世纪 70 年代近地警告系统（GPWS）问世之前，**受控撞地（CFIT）**是航空领域最主要的致死事故类型之一。这类事故的特殊之处在于：飞机本身各项设备运转完好、完全具备飞行能力，却意外撞向地面或水面。事故发生时，飞行器硬件并无故障，但机组得不到可靠告警提示，无法知晓按照当下的下降轨迹，飞机即将会撞地；等到机组凭借主观感知察觉危险时，往往已经错失挽回的机会。

GPWS 的工作逻辑不止是单纯监测飞行高度，它还会同步采集下降速率、起落架与襟翼状态，以及飞机与地形的距离。当多项参数共同指向危险飞行轨迹时，系统便会向机组发出告警。它不会等到撞地风险已经确凿形成才触发提醒，而是在飞行态势刚出现恶化苗头的时候就发出预警。

现代航空公司借助机载航电遥测技术，将这套前置预警思路进一步拓展：持续采集数百项发动机与整机系统参数，并和正常运行基线做比对。行业头部航司能够实现 99% 以上的签派可靠率，核心就在于预测性维护能力 —— 可以在地面定检阶段，就识别出性能正在劣化的零部件，赶在飞行途中发生故障之前完成处置。



空客导航显示的地形模式（TERR）：红色是高于飞机当前高度的地形，黄色接近，绿色低于航迹——把看不见的地形变成可以判断的颜色。

EGPWS 的价值在提前量。它不只测高度，还把下降率、起落架与襟翼状态、地形距离放在一起算，当这组参数共同指向危险轨迹时就发出告警。

与之类似，OpManager Nexus 中的阈值告警会在问题影响用户之前，将基础设施的异常状态报告工单。

在齐尔克科技：那个早就存在的预警

认证服务故障之后，齐尔克科技的团队做了事故复盘并调取了系统日志。复盘得出的结论，事后回看并不出人意料，却值得警醒：早在事故爆发前 48 小时，系统就已经出现数据库性能异常；事故前 24 小时内，查询延迟更是先后两次急剧冲高。但这两处风险迹象既没有触发有效告警，也没有被运维团队关注和研判。

其实早期预警信号一直留存于日志之中。齐尔克科技的 IT 团队并不缺少相关的风险线索，而是缺少一套能够在隐患累积演变为停机事故前，主动挖掘风险的机制。原有监控体系本质属于被动响应模式：告警阈值设置在故障已经实际发生的节点，而不是能够干预的风险萌芽窗口阶段。

齐尔克做了什么

齐尔克科技以此为契机重新搭建监控体系，确立核心建设原则：**监控的目标，不只是感知已经发生的故障，更要识别有趋势发生的隐患。**基于该原则，团队落地了一系列改造举措：

- **将 ManageEngine OpManager Nexus 接入支撑关键服务的服务器、网络设备和应用层**——认证、邮件和核心业务应用。为每项服务定义性能基线，并针对 CPU 利用率、内存压力、查询响应时间和接口错误率配置阈值告警。任何指标偏离基线时，OpManager Nexus 会自动在 ServiceDesk Plus 中开出一张事件工单，自动关联**受影响的设备**、**当前指标值**和**告警严重程度**。这张工单在任何用户报障之前就已经存在了，真正的防患于未然。
- **使用 ServiceDesk Plus 的分析模块**，每周对近期关闭和仍未关闭的事件做一次聚类分析，按受影响的配置项（CI）、上报的服务分类和症状类别进行分组。不同部门的用户在三天内分别报上来的五起认证失败，在工单层面看都很平常——每张都被单独解决然后关闭了。但当作一个聚类来看，它们指向的是 OpManager Nexus 已经标记了 36 小时的 **SQL 查询延迟升高**的服务。在这批聚类的**第六张工单**进来之前，系统就把底层问题暴露了出来。
- **建立持续管控规则**：在滚动 14 天窗口内，任何同一配置项、服务或症状特征、且数量达到三张以上的事件，一律立即升级为问题记录，不论每张工单本身是否已经解决。关闭工单不等于关闭问题——只有确认了根本原因并完成修复，问题记录才能关闭。
- **把每周事件复盘写进服务台经理的周一例行工作**：30 分钟，按类别、技术员和服务三个维度复盘上一周的数据。聚类分析在会议开始前就完成，在讨论开始前就已经摆在桌面上的，而不是讨论中才发现的。

OpManager Nexus 在一张故障工单创建之前，就在指标层面捕捉到了基础设施的趋势；聚类分析，则在一个问题反复出现之前，通过捕捉到了跨工单的规律。两者给了齐尔克科技的 IT 团队两个不同层级的早期预警：**一个在基础设施层，一个在事件记录层。**

> ***航空启示***
>
> **OpManager Nexus 阈值告警 → ServiceDesk Plus 工单** = 航电遥测：持续的参数监控在机组察觉异常之前就发出告警
>
> **跨事件工单的聚类分析** = 飞行运行质量保证（FOQA）：没有哪一次单独的飞行触发过告警，但分析大量飞行数据后发现了一个液压密封件的不良趋势，让飞机在发生故障前就执行停机检查
>
> **由事件聚类触发的问题记录** = 国家运输安全委员会：调查不会因为提交了一份事故报告就结束——只有当诱因也被消除，调查才结束
>
> **每周事件复盘** = 签派可靠性跟踪：在趋势变成故障之前执行结构化复盘

从被动式 ITSM 迈向主动式 ITSM，绝非仅仅是运维团队思维心态的转变，更是**整套技术**与**流程架构**的**重塑**。齐尔克科技搭建完成的这套体系，让风险警觉成为运维工作的常态。

你的组织该怎么开始？

先看看过去 30 天的事件。

- 拉过去 30 天的事件报表，按受影响的配置项和服务类别分组。找出任何出现在三张及以上不同工单里的配置项或服务——哪怕每张都已被解决。这个聚类就是你需要分析的问题记录。
- 为最关键的三项服务定义性能基线：正常的 CPU、内存、响应时间和错误率是什么水平？没有基线，任何监控工具都无法告诉你趋势什么时候开始走偏。
- 如果你已经在用 OpManager Nexus 或同类的基础设施可观测性工具，确认阈值告警被配置为**创建 ServiceDesk Plus 工单**，而不只是发邮件。邮件会被淹没，但是在队列里的工单就会被分派、跟进。
- 安排固定的事件复盘会。在会议开始前先跑好聚类分组报表，让所有资料在讨论开始前准备就绪。



08 课程四——在事故发生前先演练

聚焦的 ITIL 实践：知识管理

确保正确的信息在正确的时间传达给正确的人——尤其是在压力之下。

在 ServiceDesk Plus 中：

知识库文档统一存储于解决方案模块。该模块支持设置仅技术员可见，可将操作步骤、升级路径以及重大事件处置的 SOP 限定仅供 IT 团队内部访问。IT 团队开展桌面推演时，可直接调用这些文档开展模拟演练，充分熟悉平台的操作逻辑与业务工作流。

每轮演练结束后，可在解决方案中补齐演练时暴露出的流程缺口，所有变更都会记录到知识库文章的版本历史中，清晰留存修改内容与修改时间。这就保障了 IT 团队在真实故障处置时所使用的，都是经过实战演练、确认有效的最新版知识库文档。

在驾驶舱：模拟机与机组资源管理

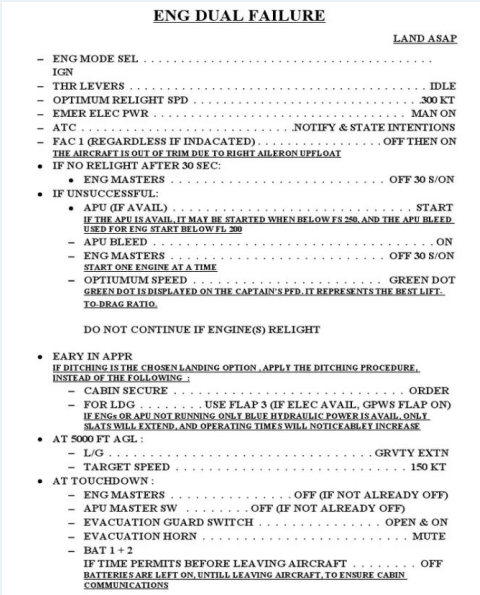
商业飞行员在取得载客运行资质前，需要投入大量时间在飞行模拟机中开展训练。训练内容不只是常规的标准飞行，更要反复演练各类故障险情：起飞阶段发动机起火、高空液压系统失效、鸟击撞击、仪表飞行环境下电气故障等。这类险情在飞行员的整个职业生涯都未必会亲身遭遇一次，但一旦发生，机组必须立刻做出正确的反应。

机组资源管理（CRM）培训，将这种应急准备提升到新的高度。培训重点聚焦：高压环境下机组如何开展沟通协作、紧急状态下如何分配工作负荷、飞行员职级如何对决策产生影响，以及如何规避高压场景下人为失误的各类认知陷阱。机组资源管理这门学科，正是源于

每一次的事故调查报告 —— 尤其是那些硬件本身完好可正常飞行的情况，却因为机组在压力之下沟通、协同机制失效，最终酿成悲剧的事故。

模拟机训练与机组资源管理，建立在一套成文的规范之上：标准作业程序 SOP、应急检查单以及处置讲评指引，明确规定机组的反应动作。模拟机的核心价值，就是验证这些流程规范在真实险情下是否切实可行，在正式操作之前，提前暴露潜在漏洞。

2009 年的 “哈德逊河奇迹” 就是最好的佐证：切斯利・萨伦伯格机长执飞全美航空 1549 航班，遭遇双发发动机故障之后，成功将客机迫降于哈德逊河。萨伦伯格机长演练了各类发动机失效的场景长达 40 年。遭遇鸟击险情的瞬间，他对副驾驶下达的第一句指令就是**冷静、明确，完全聚焦故障处理的任务**。整套操作最终保障机上 155 名人员全部生还，这份奇迹，正是持续演练与体系化训练造就的结果。



ENG DUAL FAILURE

LAND ASAP

- ENG MODE SEL . . . . . IGN
- THR LEVERS . . . . . IDLE
- OPTIMUM RELIGHT SPD . . . . . 300 KT
- EMER ELEC PWR . . . . . MAN ON
- ATC . . . . . NOTIFY & STATE INTENTIONS
- FAC 1 (REGARDLESS IF INDACATED) . . . . . OFF THEN ON
  THE AIRCRAFT IS OUT OF TRIM DUE TO RIGHT AILERON UPFLOAT
- IF NO RELIGHT AFTER 30 SEC:
  - ENG MASTERS . . . . . OFF 30 S/ON
- IF UNSUCCESSFUL:
  - APU (IF AVAIL) . . . . . START
    IF THE APU IS AVAIL, IT MAY BE STARTED WHEN BELOW FS 250, AND THE APU BLEED USED FOR ENG START BELOW FL 200
  - APU BLEED . . . . . ON
  - ENG MASTERS . . . . . OFF 30 S/ON
    START ONE ENGINE AT A TIME
  - OPTIUMUM SPEED . . . . . GREEN DOT
    GREEN DOT IS DISPLAYED ON THE CAPTAIN'S PFD. IT REPRESENTS THE BEST LIFT. TO-DRAG RATIO.

  DO NOT CONTINUE IF ENGINE(S) RELIGHT

- EARY IN APPR
  IF DITCHING IS THE CHOSEN LANDING OPTION , APPLY THE DITCHING PROCEDURE, INSTEAD OF THE FOLLOWING :
  - CABIN SECURE . . . . . ORDER
  - FOR LDG . . . . . USE FLAP 3 (IF ELEC AVAIL, GPWS FLAP ON)
    IF ENGs OR APU NOT RUNNING ONLY BLUE HYDRAULIC POWER IS AVAIL, ONLY SLATS WILL EXTEND, AND OPERATING TIMES WILL NOTICEABLEY INCREASE
- AT 5000 FT AGL :
  - L/G . . . . . GRVTY EXTN
  - TARGET SPEED . . . . . 150 KT
- AT TOUCHDOWN :
  - ENG MASTERS . . . . . OFF (IF NOT ALREADY OFF)
  - APU MASTER SW . . . . . OFF (IF NOT ALREADY OFF)
  - EVACUATION GUARD SWITCH . . . . . OPEN & ON
  - EVACUATION HORN . . . . . MUTE
  - BAT 1 + 2
    IF TIME PERMITS BEFORE LEAVING AIRCRAFT . . . . . OFF
    BATTERIES ARE LEFT ON, UNTILL LEAVING AIRCRAFT, TO ENSURE CABIN COMMUNICATIONS

双发失效应急检查单：即两个发动机都没推力了，在飞机继续滑翔的过程中，检查清单的步骤依次为：优先尝试重启发动机，重启不成功就找地方迫降，同时做好乘客撤离准备。

在真实的事故之前，飞行员都会一遍又一遍地演练。同样在 ServiceDesk Plus 中的重大事件应急预案，只有在团队真正演练使用过之后，才能在压力下正常执行。

在齐尔克科技：那份从没演练过的预案

认证服务故障过去三个月后，齐尔克科技已经完成知识管理相关建设：一份经过 IT 管理层评审、内容完备的 P1 重大事件响应预案，已录入 ServiceDesk Plus 解决方案模块，对全体团队成员开放访问权限。

然而在这之后一个周四下午，网络故障突然爆发。尽管知识库中早有预案，团队也清楚预案的存在，但实际处置依旧暴露出了短板：团队耗费 40 分钟才完成重大事件处理团队的组建。因为预案中指定的事件经理正值休假，却没有配置替补人员；两名资深工程师在互相没有沟通的情况下，并行处理同一故障；面向业务干系人的情况通报也延迟了一小时。重大事件的应急预案有了，由于没有演练过，仍然有缺口。

齐尔克做了什么

齐尔克科技建立了季度桌面推演机制，依托 ServiceDesk Plus 内现成的处置预案，开展贴近真实故障场景的结构化模拟演练。具体落地举措如下：

- **区分公开知识库与内部知识库**：将 P1 重大事件处置预案、升级流转路径、值班联系人、厂商 SLA 以及业务干系人沟通模板统一收纳至解决方案模块，并设置为**仅技术员可见**。通过知识库的权限控制，终端用户访问一套公开知识库；事件处理团队则访问一套内部管控、内容可信、持续更新的知识库文档。
- **基于真实历史故障设计演练场景**：参考企业过往实际事件来搭建桌面推演案例，调度完整的应急响应团队参与，明确划分各角色职责。演练复盘环节除评估技术处置动作之外，同步审视团队沟通、协作模式与决策过程，借鉴机组资源管理理念开展复盘评审。
- **在真实产品环境完成推演操作**：要求所有参与者直接在正式的 ServiceDesk Plus 操作界面执行一次预案，和真实故障发生时的操作步骤完全一致。以此暴露出高压情境下容易出现的执行偏差，并且在下次演练前完成整改闭环。
- **版本化管理处置文档，实现可追溯更新**：将每一轮演练识别出的流程缺口，创建为 ServiceDesk Plus 跟进任务，实现闭环，完成整改后同步更新对应的知识库文档。版本历史完整记录修改内容与修改时间，保障运维人员使用的始终是经过演练验证、具备修订追溯记录的最新预案。

> **航空启示**
>
> 桌面推演 = 定期模拟机复训
>
> 仅技术员可见的解决方案文章 = 机组操作手册
>
> 在 ServiceDesk Plus 中演练 = 拿着真实 SOP 演练
>
> 版本受控的解决方案文章 = 飞行手册的修订

六个月后下一次网络故障发生时，团队在 22 分钟内解决了问题。事件经理从一开始就明确，应急指挥室在 10 分钟内就绪，对业务干系人的更新在半小时内发出。他们用的还是类似的预案。区别在于——这一次团队已经真正演练过了。

你的组织该怎么开始？

把演练当成常态，而不是出事了才想起来的事。

- 选一个你团队最可能遇到、也最难处理的场景，作为第一次桌面推演的主题。
- 确认预案里的每个角色都有明确的人，而且至少有一个替补人员。
- 演练时要求所有人使用真实平台和真实预案，不要走"我们过一遍流程就行"。
- 演练后立刻把发现的差距变成任务，并更新对应的知识文章。演练不做改进，等于没演练。



09 课程五——在下次起飞前先读黑匣子

聚焦的 ITIL 实践：持续改进

依靠数据和证据而不是直觉，持续识别并改进服务、组件和实践，让组织 IT 服务不断适配动态变化的业务诉求。

在 ServiceDesk Plus 中：

持续改进能力由报表模块、调查模块以及可自定义的首页仪表板共同支撑。报表模块支持自定义报表，涵盖请求矩阵报表、SLA 合规率、工程师绩效等统计维度；调查模块可在工单办结后自动推送用户满意度调研；定制化仪表板搭载工单、问题、变更相关的表格与图表组件，实现多类数据集中可视化呈现。

在驾驶舱：飞行数据记录仪与系统性学习

一架商用客机均配备两台飞行记录设备：飞行数据记录仪（FDR）与驾驶舱语音记录仪（CVR），二者就是大众熟知的 “黑匣子”。设备按照抗坠毁标准制造，能够存储上千项飞行运行参数与数小时驾驶舱录音，帮助事故调查人员精准还原事件全貌，定位根因。

但黑匣子对于航空安全最大的价值，**并不局限于事故发生后的溯源调查，更体现在每一次正常航班落地后的数据分析工作。**

航司普遍将飞行记录仪数据纳入飞行运行质量保证（FOQA）项目，借助自动化工具自动识别各类异常行为，例如重着陆、不稳定进近、飞行速度偏移、设备温度超限等。**绝大多数风险苗头，在演变为安全事故之前就被识别并完成整改。**

美国国家运输安全委员会（NTSB）会针对每一起重大航空事故输出完整调查报告，不只定位表层直接诱因，更深挖背后的系统性问题，并面向全行业发布安全改进建议。**防撞告警系统**、**风切变探测技术**、**燃油耗尽处置流程**，诸多航空安全成果，都源自 NTSB 的事故调查结论。



飞行数据记录仪：俗成“黑匣子”，橙色外壳便于搜寻，抗坠毁设计让它在高温、冲击和水下仍能保住数据。

黑匣子会记录每一项飞行参数，方便调查人员找出故障背后的规律；与之类似，ServiceDesk Plus 的报表和仪表板能将已结工单转化为具备分析价值的依据，而不只是归档存放的记录。

在齐尔克科技：那些本该被连起来的点

认证服务故障六个月后，齐尔克科技的服务台面貌焕然一新：未再发生重大故障，SLA 持续稳定达标。依托变更模板，三项高风险变更在上线生产环境前被准确拦截，这类风险在旧流程中会被直接忽视掉。

到了十月，服务台经理输出了第一份体系化的月度分析报表。报表虽然任何紧急告警，却揭示出一个关键的隐患。

远程访问类工单的平均解决时间（MTTR），在过去一个季度攀升 40%。单独看任意一周的数据，都还达不到需要介入处置的程度，但把三个月的变化趋势串联起来，问题便一目了然。**工单调查模块**采集的用户满意度数据则进一步佐证该现象：**远程访问**成为服务台评分最低的服务分类。问题并非长期的工单搁置未处理，而是同一批用户反复提交相同的故障工单。

将工单数据与问题记录、变更历史做交叉分析后发现：大量看似互不关联的工单，都在复用同一套临时解决方案 —— 涉及的用户不同、上报症状不一样、发生时间也有差异。这套临时解决方案虽然帮助团队守住 SLA 指标，提高了首次呼叫解决率，各项表面指标全部显

示正常。但拨开数据表象，暴露出典型的**西瓜效应**：指标页面一片绿灯，内部隐患早已滋生，反复发作的潜在问题持续侵蚀着 IT 运营韧性。

整套治理流程本身可以正常运转，原有机制没有设计自我复盘、挖掘隐性规律的能力。齐尔克科技已经搭建起属于自己的 IT “黑匣子”，这份十月的报表，是企业第一次真正打开它。借助可视化仪表板与分析报表，管理者能够提前识别能力短板、定位问题根因，在故障爆发之前，把持续改进机制固化到日常运维当中。齐尔克科技的 IT 团队又要开始着手处理远程访问的问题处理了。

齐尔克做了什么

齐尔克科技依托 ServiceDesk Plus 的全量数据，搭建起了一套体系化数据分析实践。团队将历史事件、变更、问题记录视作事故调查员手中的飞行数据记录仪：这些数据不是仅仅用来归档留存的档案。更是可供研判核验的证据。

- **月度 ITSM 健康报告，跟踪指标长期趋势。**借助 ServiceDesk Plus 请求矩阵报表模块，面向 IT 管理层输出月度 ITSM 健康报告。报告按事件类别统计 MTTR，按工程师、服务维度统计 SLA 合规率，并核算首次呼叫解决率。十月生成的这份报告，是齐尔克科技首次将各项指标作为连续趋势进行观察，而非只看孤立时间点的数据快照，正是这份报告让持续恶化的远程访问隐患得以暴露。
- **工单闭环自动推送满意度调研，补充定性视角。**在工单办结时自动触发满意度调查。除 MTTR 这类量化指标之外，满意度评分给管理层带来业务侧的定性洞察，从侧面证实了远程访问场景下用户反复遭遇故障：工单虽然标记关闭，但底层根源问题并未消除。
- **基于数据分析创建问题记录，推动根因彻底修复。**针对远程访问隐患创建正式问题记录，这也是企业第一条不靠事件数量自动升级、完全通过数据分析识别出来的问题记录。结合工单数据、满意度评分以及工单处理备注，团队定位到一处已知错误：十余条看似互不相关的工单，都在重复使用同一套临时解决方案临时处理。该问题记录持续保持打开状态，直至根因确认、完成永久性修复才予以关闭。
- **固化持续改进规则，区分工单闭环与问题闭环。**建立持续改进评审规则：月度报告中发现的异常趋势，例如 MTTR 攀升、满意度下降、临时解决方案高频复用等，即便单张工单未达到升级阈值，也要纳入潜在问题记录进行评审。**工单完成关闭，不等于根源问题已经解决。**

- **配置实时可视化仪表板，消除手工导出数据的痛点。**为服务台经理与团队负责人配置实时仪表板，通过表格、图表组件整合工单、问题、变更全维度数据。工单优先级分布、工程师工作负载、未闭环问题、SLA 执行状态等以往需要手工导出整理的信息，全部实现集中可视化。
- **开展季度跨业务服务评审，对齐业务认知。**面向各业务部门建立季度服务评审机制，依托 ServiceDesk Plus 报表展示 IT 服务表现，识别差距并跟进改进项。远程访问已经成为第四季度评审重点议题，理解该问题长期隐匿的原因，同步后续完整的整改方案。

> **航空启示**
>
> 月度 ITSM 健康报告 = NTSB 调查结论
>
> MTTR 趋势分析 = FOQA 异常检测
>
> 季度服务评审 = 安全委员会讲评
>
> 通过分析创建问题记录 = NTSB 安全建议

十月暴露的远程访问隐患最终并未演变为重大故障，并非风险本身不足为惧，而是依靠主动数据分析，在隐患爆发之前就完成识别。相关数据其实已经在 ServiceDesk Plus 中沉淀了数月，真正的转折点，仅仅是团队养成了主动审视数据的习惯。

10 结论

齐尔克科技的故事并未止步于那场认证服务故障。这场历时五小时的重大事件，成为企业搭建真正具备韧性的 IT 运营体系的催化剂。它倒逼这支习惯临场应急、靠个人处置问题的 IT 团队，重新审视系统的连锁失效风险，直面数百位受影响用户带来的业务压力。整个转型过程既没有更换团队成员，也没有替换底层技术，所有改变全部来源于流程与架构层面的重塑。

航空业能够成为全球安全性最高的大众交通运输行业，依靠的从来不是运气或是个人天赋，而是一整套结构性安全防护机制：摆脱对个人经验、记忆的依赖，推行标准化作业；搭建高压场景下可自动排序关键信息的告警体系；通过监控手段捕捉隐患趋势，在彻底故障发生之前介入处理；借助模拟演练将危机响应打磨成本能；建立数据驱动的文化，把每一次事件都视作可供复盘核验的证据。这些并非一次性就能做完的优化措施，而是深度嵌入日常运营模式，也正因如此才能够持续发挥长期价值。

你的 IT 服务台同样可以复刻这套方法论。本书介绍的五大启示并非理想化愿景，而是可落地、可衡量，并且在齐尔克科技得到实践验证的实操方法。

当工具配置就绪，整套运行模式也经过严苛场景的检验之后，这五条经验便可供所有 IT 团队借鉴落地。

航空原则	对应的 ITIL 实践	ServiceDesk Plus 对应能力
强制性航前检查单	变更赋能	变更模板、变更工作流
ECAM 分级告警	事件管理	事件模板、SLA 升级、通知规则
GPWS 主动预警系统	问题管理	问题记录、关联事件、聚类分析、根因分析
定期模拟机复训 + 版本受控的机组操作手册	知识管理	解决方案模块：仅技术员可见的知识文章，含版本历史、任务、回复模板
黑匣子分析 / FOQA / NTSB	持续改进	自定义报表、计划报表、仪表板

11 关于 ServiceDesk Plus

ServiceDesk Plus 是 ManageEngine 卓豪推出的 AI 驱动统一服务管理平台。基于业界推荐的 ITSM 最佳实践构建，ServiceDesk Plus 内置了丰富的 IT 与第三方系统集成，帮助服务台团队更好地让 IT 服务与组织的业务目标对齐。

覆盖预测型、生成型、对话型和智能体的 AI 能力，确保服务交付团队把合适的技术用在合适的场景上，把时间留给真正需要人类判断的工作。凭借原生的企业服务管理能力和通过低代码脚本带来的不受限制的可扩展性，ServiceDesk Plus 帮助组织设计、交付并支撑自己的业务与 IT 服务。基于你的需求提供标准版，专业版和企业版三个版本，支持本地部署以及 Saas 部署。支持 43+ 种语言。

进一步了解 ServiceDesk Plus 及其功能

ServiceDesk Plus 被全球领先企业信赖的五个理由：

- IT 与企业服务管理的高价值 AI 能力，无需额外付费。
- 强大工作流，实现企业服务及 IT 服务端到端编排。
- 覆盖服务器、网络、交换机、工作站及外设，支持自动扫码的统一台账系统。
- 平台能力赋能 ServiceDesk Plus，实现办公服务交付的数字化与优化。
- ServiceDesk Plus 可与 ManageEngine 以及第三方业务应用原生集成。

了解 ServiceDesk Plus 服务管理落地方案，欢迎联系我们

邮箱：sales@manageengine.cn | 专线：400-660-8683

12 关于 ManageEngine 卓豪

ManageEngine 卓豪是 Zoho Corp 旗下事业部，为全球企业与托管服务提供商提供完整的本地部署与云原生 IT 及安全运维管理解决方案。

依靠 ManageEngine 卓豪的 IT 管理工具，无论是初创团队还是成熟企业，都可保障网络、服务器、应用、终端等 IT 基础设施稳定高效运行。业务覆盖 190 个国家和地区，获得超过 280000 家企业组织的信赖。

13 关于作者

Saket Pasumarthy 是 ManageEngine 卓豪 ServiceDesk Plus 产品营销专家，同时也是一名 ITSM 爱好者，持续关注 IT 领域前沿动态。通过撰写指南、技术文章与博客内容，助力全球 IT 服务管理团队攻克服务管理难题，并在 ServiceDesk Plus 大师课系列中承担用户培训授课工作。闲暇之余，热爱足球，也喜欢飞行模拟器体验