正文 第一篇：IT 运维安全审计(堡垒机) 解决方案

网域 NSYS 运维安全审计（堡垒机） 解决方案

网域运维安全审计（堡垒机）提供运维用户操作以及违规事件等多种审计报表，过报表功能，即能够满足大部分客户的日常审计需求，也可满足如等级保护、"萨班斯法案"等合规性要求。同时，系统也支持通过自定义或二次开发方式进行灵活扩展。

集中统一管理、安全审计、统一账号管理,统一身份认证,统一授权管理,统一操作审计,流程管理，单点登录，并能图像形式的回放操作员记录、使管理员操作简单快捷。

运维用户通过一个统一的平台就能登录所有的目标 设备，包 Unix、Linux、Windows 服务器以及各类网络设备 。

集中管理用户、设备、系统账号；

集中管理用户、系统账号的密码；

所有用户集中登录、集中认证；

集中配置账号密码策略、访问控制策略；

集中管理所有用户操作记录；

访问控制

1. 根据用户角色设置分组访问控制策略；

2. 实现用户－系统－系统账号的对应关系；

权限控制

1.可设置以命令为基础的权限控制策略；

2. 可支持 IT 运维人员对多种远程维护方式，如字符终端方式(SSH、Telnet、Rlogin)、图形方式（RDP、X11、VNC、Radmin、PCAnywhere)、文件传输（FTP、SFTP）以及多种主流数据库工具按照用户/用户组、资源/资源组、运维时间段、运维会话时长等授权。

实时的操作告警及审计机制

监控告警机制

能对运维用户的所有操作进行实时的控制阻断、告警及监控，避免由于一些敏感的操作导致网络中断或企业信息泄露。

详尽的会话审计与回放机制

系统提供运维协议 Telnet、FTP、SSH、SFTP、RDP（Windows Terminal)、Xwindows、VNC、AS400、Http、Https 等完整会话记录，完全满足内容审计中信息百分百不丢失的要求。

1. 能记录所有操作并能随时根据审计的需要查询任何时候任何人员所做的任何操作。

2. 提供图像形式的回放，真实、直观、可视地重现当时操作过程。

3. 能记录加密维护协议 SSH 数据

符合法律法规

第二篇：IT 运维综合管控解决方案

IT 运维综合管控解决方案

针对安然、世通等财务欺诈事件，2021 年出台的《公众公司会计改革和投资者保护法案》（Sarbanes-Oxley Act）对组织治理、财务会计、监管审计制定了新的准则，并要求组织治理核心如董事会、高层管理、内外部审计在评估和报告组织内部控制的有效性和充分性中发挥关键作用。与此同时，国内相关职能部门亦在内部控制与风险管理方面制定了相应的指引和规范。 由于信息系统的脆弱性、技术的复杂性、操作的人为因素，在设计以预防、减少或消除潜在风险为目标的安全架构时，引入运维管理与操作监控机制以预防、发现错误或违规事件，对 IT 风险进行事前防范、事中控制、事后监督和纠正的组合管理是十分必要的。 IT 系统审计是控制内部风险的一个重要手段，但 IT 系统构成复杂，操作人员众多，如何有效地对其进行审计，是长期困扰各组织的信息科技和风险稽核部门的一个重大课题。

一、需求分析

系统的运维人员是系统的“特殊”使用团队，一般具有系统的高级权限，对运维人员的行为审计日渐成为安全管理的必备部分，尤其是目前很多企业为了降低网络与系统的维护成本，采用租用网络或者运维外包的方式，由企业外部人员管理网络，由外部维护人员产生的安全案例已经逐渐在上升的趋势。

运维人员具有“特殊”的权限，又往往是各种业务审计关注

不到的地方，网络行为审计可以审计运维人员经过网络进行的工作行为，但对设备的直接操作管理，比如 Console 方式就没有记录。

运维审计的方式不同于其他审计，尤其是运维人员为了安全的要求，开始大量采用加密方式，如 RDP、SSL 等，加密口令在连接建立的时候动态生成，通过链路镜像方式是无法审计的。所以运维审计是一种“制度+技术”的强行审计。一般是运维人员必须先登录身份认证的“堡垒机”(或通过路由设置方式把运维的管理连接全部转向运维审计服务器)，所有运维工作通过该堡垒机进行，这样就可以记录全部的运维行为。由于堡垒机是运维的必然通道，在处理 RDP 等加密协议时，可以由堡垒机作为加密通道的中间代理，从而获取通讯中生成的密钥，也就可以对加密管理协议信息进行审计。

二、运维安全审计面临的挑战

IT 运维人员一般应用命令行方式（Telnet、SSH)、和图形化方式（RDP、VNC)、客户端软件等方式对数据中心的服务器进行管理，这些方式虽然方便、灵活，但接入点多，存在重大安全隐患，并难于管理，特别是，面对成千上万台的设备，一个 IT 经理或者一个 CIO 如何能确保所有 IT 运维人员的操作都是安全的？ 倘若有违规操作，如果发现并有效阻止？若阻止不及，如何认定事故责任？

三、IT 运维综合管控解决方案

泰然神州 Zendeep 神电运维审计系统是用于数据中心 IT 运维的集中管理和审计系统，可以对基于 Telnet、SSH、RDP、VNC 等协议的访问操作进行过程的抓取，从而可以录象方式对所有运维人员的所有操作进行记录，并具备强大的搜索功能，可对特定时段、特定事件、特定用户等逻辑要素进行搜索与提取——从而达到真正意义上的审计与风险控制。

泰然神州 Zendeep 运维审计方案的功能架构模块（下图）

泰然神州 Zendeep 运维审计系统管理平台，不仅可以对 IT 运维人员应用带内管理工具（Telnet、SSH、RDP、VNC 等协议）的管理进行全面的集中管理与审计，可以制定有效的控制策略，进行访问授权、访问阻断，另外也可以根据不同的参数搜索调用历史操作画面，并进行画面回放、查看审计日志、从而进行有效的安全防护。

泰然神州运维审计系统由管理控制台、应用代理服务器、客户端安全插件和数据库四大部分构成。 管理控制台：

管理控制台负责实现系统的用户管理、代理访问策略管理、阻断策略管理、审计日志的查看与审计、对审计会话的画面回放和系统的基础配置等功能

管理控制台是一个基于 Web 的操作界面，可以对一个 ICS 对应的多台 ICA 的监控结果进行集中化的管理 应用代理服务器：

应用代理服务器用于实现代理应用的集中管理，对用户和客

户机进行合法性校验，受符合策略要求的代理应用连接请求

提供 TCP 阻断功能，对于网络中的非法网络连接可以根据阻

断策略自动实施阻断操作 数据库：

日志审计数据库，用于记录用户信息、策略信息和连接会话

的日志信息等内容

文件数据库，专门用于记录应用代理服务器所记录每个连接

会话的录像信息，录像信息与日志信息直接关联，直接通过

查询日志信息后播放对应的录像文件，真实再现当时的操作

画面 客户端安全插件：

终端客户机及和 IT 运维管控系统后台之间建立加密的连接通

道 终端安全登陆认证设备接口

四、方案应用部署

泰然神州 Zendeep 运维审计系统部署网络拓扑架构图：

五、方案特点

泰然神州 Zendeep 运维审计方案特点：

集中管理，提供后台设备、数据库及指定系统统一的操作维

护入口，实现单点登录。 身份管理，提供设置实名制登陆帐

号，详细记录后台数据库全部操作过程。

访问控制，提供管理员根据不同的用户配置不同的操作权限，

实现命令级别的严格控制，确保合法用户在其系统权限范围

内访问授权设备。

命令防火墙，实现当不同用户帐号与同一系统帐号关联时，

以命令为核心建立更加细粒度的权限控制。 操作审计，对用户实施的操作提供完整，详细记录服务。并可以安全地存放于管理平台中，管理平台能以方便、友好的界面方式提供对这些记录的操作查看，搜索，回放等审计功能。 支持协议：Telnet、SSH、RDP、VNC 等 强制主机审计，所有运维行为强制经过 IT 运维管控系统跳转 IT 运维管控系统所在服务器安全加固

六、泰然神州 Zendeep 运维审计系统方案效益分析

通过实施泰然神州 Zendeep 运维审计系统方案，安全审计工作可以得到有效简化，可以进行全面的集中管理与审计，真正做到运维全程操作可见、可控、可查。

1、本系统可对所有用户进行集中管理，包括本地管理用户及远程管理的用户。可以通过本系统行使如下功能：用户的创建、修改、删除和查询、用户的启用和挂起控制、用户的权限管理功能。

2、可以对历史操作画面回放，掌握第一手客观公正的操作记录。

3、对所有通过基于 Telnet、SSH、RDP、VNC 等协议的访问操作，进行全生命周期录像，可实现对历史操作过程的真实再现。

4、根据用户设置的规则、关键字、用户名称、目标地址、源地址负载名称、部门名称、描述信息和时间进行审计信息的

查询检索，对查询的结果进行回放，再现历史操作画面。

5、本系统对通过应用代理服务器访问的负载的操作信息进行记录，包括访问负载 IP 地址、客户端地址、运维用户名称、操作开始和结束时间等等，管理人员可以通过时间、客户端类别（TELNET、SSH、RDP、VNC）、负载 IP 地址、客户端 IP 地址和运维用户对审计信息进行查询。

6、可以制定有效的控制策略——将风险远远阻在门外，访问授权控制策略：可以根据企业内控与管理的要求配置应用代理访问控制策略，经过授权的客户端可以通过代理访问负载，未经过授权的客户端则不可以访问负载。

7、阻断访问控制策略：通过访问控制策略阻断控制，可以强制用户必须通过应用代理访问负载。

第三篇：IT 运维监管控一体化解决方案

IT 运维监管控一体化解决方案

IT 运维管理闭环体系

2021-11-17

本文论述了 IT 运维监管控一体化趋势，建设要求、原则，方案整体设计和具体实现。

IT 运维监管控一体化解决方案

目 录

IT 运维监管控一体化解决方案

1. IT 运维服务管理概述

随着企业信息化程度的提高、IT 环境规模的扩大和 IT 环境复杂度的增加、行业内服务竞争的加剧，如何保证 IT 系统安全稳定运行，为业务提供可持继性的支撑，最优化 IT 环境的性能，有效控制 IT 成本和计划 IT 投资，这些都对 IT 系统运行

维护支持以及 IT 服务水平提出了新的要求和挑战。

面对的挑战：

越来越高的服务成本　　以流程管理为驱动的转型阶段

从以“技术为中心”向“业务驱动”的转型　　服务协议成为最佳成果的代名词

合作伙伴关系将替代“客户－供应商”的简单关系

服务成为应用的代名词

信息技术在业务中起着越来越重要的作用，越来越多的业务流程依赖 IT 技术。从技术和业务的双重视角对其进行有效管理，保障业务处理平台高效、安全、正常运行，为业务服务提供有力支撑成了运维人员和 IT 部门的常态工作。

如何在企业内部建立起一套有效的运维交互平台，理顺不同部门以及上下级之间的协作关系，规范工作流程，提高工作效率，实现故障处理、资源调度优化、系统割接、业务保障等运维工作的闭环流程监控和管理，是目前各 IT 运维部门关心的问题。

5 / 28

IT 运维监管控一体化解决方案

但是，由于业务快速变化、用户环境日益复杂、IT 应用日益繁多等因素导致了 IT 服务与实际业务需求脱钩，IT 服务与业务部门的实际要求出现鸿沟，由此催生了面向“IT 服务”的管理挑战与需求－－－IT 服务管理。IT 服务管理立足于服务，

建立以客户为中心，以流程为导向，从业务角度出发的全新的 IT 管理模式，通过整合 IT 服务与业务，提高了组织对外提供服务的能力，是真正实现这种服务管理的有效途径，能帮助用户最终实现 IT 与业务的融合。

2. IT 运维管理一体化管理解决之道

受习惯、时间、财力等诸多因素的影响，在迈入 IT 服务管理过渡阶段过程中，大多数客户的 IT 服务部门管理的变革没能跟上技术的发展，未对 IT 服务管理进行整体规划，没有导入适合现阶段的管理机制，依然沿用“被动响应、救火队”服务支持管理模式，依然缺乏适用的自动化管理流程，导致 IT 服务管理能力低下。

IT 运维一体化平台依靠对复杂异构的 IT 资源环境(网络设备、安全设备、服务器、存储、机房环境、操作系统、数据库、中间件、业务系统、IT 资产、日常工作、外包管理.....）的一体化监（面向业务服务的监视)、管（面向运维流程的管理)、控（面向日常运维的控制)，最终达到保障 IT 基础架构稳定可靠运行、降低系统和业务应用宕机风险、提高运维支持和服务管理效率、优化运维流程、建立绩效体系、控制运维成本、改进决策过程的目标。

3. IT 运维一体化建设目标

IT 运维一体化平台的总体目标是建立一个稳定、高效、灵活的 IT 运行和维护管理体系，涵盖 IT 运维工作中的监、管、

控三方面，为业务应用正常运行提供有力的支撑，提高信息系统运行效率，提高服务质量，降低运营的成本。

实时管理：及时发现故障与异常，并迅速定位，尽快解决；通过运行分析，调整运行策略；通过业务系统性能的测量和管理，优化系统性能，提高系统运行效率。　　闭环管理：通过科学规范化的流程管理保证故障、异常、隐患由相应的人员采用必要的方式闭环处理；促进巡检、变更的工作标准化、规范化；通过流程运行的考核数据，促进运维质量和运维效率的提高。

精益管理：通过丰富完善的报表和图档资料，为运行维护工作提供直观准确基础数据；避免维护工作中的疏漏而带来的人力、资金浪费；分析信息基础设施的运行负荷，制定合理的资源调配方案。

战略管理：优化现有的 IT 基础设施的运行性能；提升系统性能；预测并计划信息基础设施的需求；考核并不断提升服务水平。

4. 系统设计原则

4.1. 系统的先进性

先进性是每一个 IT 系统建设不断追求的目标。随着 IT 技术的迅速发展，更新的、更先进的技术和思想总是在不断出现，

因此，系统设计必须兼顾先进性。

系统规划的先进性是将系统看成一个有机的整体工程，不但在规划时要考虑到它的目前现状，还要考虑它的发展和未来。不论硬件或软件，在应用目前相对成熟的技术基础之上，系统必须能够不断完善、扩充，功能越来越丰富，尽可能小的代价来适应系统需求的不断增长和技术的不断发展，使现有系统能够与 IT 运维需求同步增长。

4.2. 系统的实用性

IT 运维一体化平台建设能否成功，实用性非常重要。系统设计必须以实用为出发点，而不是一味追求新技术、新理念和照搬国外模式。IT 运维平台是为 IT 环境支撑提供运维管理的基础。要达到实用性的要求，必须设计时充分考虑到国内情况、本行业特点和本企业实际状况，充分明确：提高自身的 IT 运维管理水平和提供更好的业务服务能力才是 IT 运维管理平台建设的根本目标。

4.3. 系统的有效性

IT 运维管理系统是 IT 部门每天工作的基础和平台，是 IT 部门的根本。如果不具备有效性，华而不实，很难设想 IT 部门如何开展工作，如何实现有效的 IT 运维管理，更无法谈论提供高质和高效的 IT 服务。

4.4. 系统的可行性

IT 运维的理念和设计规划再好，如果不具备可行性，也只是

空中楼阁。因此，必须考虑系统建设的可行性。可行性的考虑包括：目前技术上是否可以实现、自身人力、物力和财力上的支撑。

4.5. 系统的可靠性

IT 运维系统的重要性不言而喻。如果 IT 运维系统运行故障而停止工作，那么企业的 IT 环境犹如没有控制盘的汽车，处在无序、惯性行驶的状态。此时，IT 环境对于 IT 运维人员而言，完全陌生，处于隔离、未知、失控的状态。

对于 IT 运维管理系统，监控的失败或瘫痪相当于人失聪、失明，流程管理的失败相当于大脑丧失了思考能力，自动化运维操作的失败相当于截肢瘫痪。因此，任何模块的失败，后果都是严重的。IT 运维系统本身的健壮性、自身完善性、稳定性是至关重要的。

IT 运维平台是企业 IT 环境中实现正常运维工作的基础和管理平台。因此，IT 系统建设一定要考虑系统的可靠性。

4.6. 系统的开放性

IT 技术发展日新月异，IT 系统的开放性和标准性越来越成为一种趋势。只有采用开放的系统，使用开放的技术，才能保证整个系统有持久的生命周期，才能长期保护企业在 IT 运维的有效投入。例如：接口之间采用 Corba,xml,jdbc,ftp,jdbc

等开放技术。

4.7. 系统的扩展性

随着 IT 业务系统的增加和 IT 环境规模的扩大，随着时间的推移和情况的变化，无不需要考虑系统功能的变化和调整。因此，IT 运维一体化平台系统需要具有很强的扩展能力和适应能力。

4.8. 系统的安全性

基于 IT 运维管理系统的角色，IT 运维系统的安全变得至为关键。很难想象，IT 运维管理系统由于病毒或者安全入侵，导致 IT 运维平台瘫痪带来的后果。

5. IT 运维一体化平台建设原则

5.1. 统一规划

IT 运维一体化建设中必须坚持统一的规划、明确的发展方向和思路，在全局、宏观上做到统筹安排，合理规划。实施对整体架构和数据模型的统一管控。

5.2. 转变观念

任何生产活动都是人来主导的，IT 运维管理体系的建设不单是一个软硬件系统的建设，还是一个运维团队和人文的建设。IT 运维一体化平台的建设，是 IT 运维理念和管理上的一次划阶段的变革，它需要整个 IT 运维部门的文化、体制和思想也

要作相应的转变和调整才能成功。根据以往情况，企业的 IT 部门往往都是技术至上的工程师文化，而这种源于研发企业的文化和现今 IT 管理部门作为业务支撑部门的定位严重不符。因此，完善 IT 服务管理的过程，也必然是部门文化和 IT 运维理念和体制转变的过程。在建设 IT 服务管理体系的过程中应遵循以下 2 个原则：

高起点，借鉴业界先进的管理模型和方法。

重执行，任何管理规范和流程的制定都要以可执行，可考核为前提。

5.3. 分步实施

IT 管理体系的建立和完善不可能一蹴而就，需要有长期的计划步骤实施，必须循序渐进，遵循分阶段和迭代实施的原则。

横向扩展：从个别的业务系统扩展到所有的业务系统，规模上逐步从小到大。　　纵向加深：功能上逐步完善、丰富和细化，模块和子模块数量从少到多，从有到优。　　制定计划，“有重点、分阶段”展开。

5.4. 可插拔模块化

IT 运维一体化平台涵盖了 IT 运维工作的各个方面，从全局到局部，从宏观到细节。系统架构设计必须以模块化为基础。

必须平衡考虑系统内部模块的松散性和耦合性。作为同一平台内部的模块，由于相互协作，模块和子系统之间必然存在着耦合性。另一方面，为了控制单点故障带来的对系统整

体的影响，必须有效控制单点故障后所影响的范围并在此基础上才有可能提供快速恢复的能力。

模块化为可插拔性提供了可能，使得系统设计上可扩展性原则得以实现。　　可插拔化：为模块的升级、优化和采用新技术，提供了实现的前提。不同组件、不同层面的模块的替换，对系统的其他模块是透明的。局部的调整和升级并不对系统的整体架构产生必要的调整。

5.5. 有所为，有所不为

在一个阶段，不求大、不求全。求大求全，则难以有所为，必然陷于被动。必须明确，有所不为而后可以有为。

5.6. 不唯美，而唯实

过分追求完美，会导致华而不实，会导致系统本身和建设上的虚、浮、躁。只有尊重实际情况，才能脚踏实地，步步为营，有效推进 IT 运维管理工作的建设并不断提高。

6. IT 运维一体化解决方案

6.1. 理解 IT 运维一体化

针对 IT 运维，我们划分为三个方面，监视、管理和控制。“监、管、控”三者紧密关联，逻辑上是一条龙过程，并形成闭合环路。

监控的结果作为依据来分析、决策和指导 IT 运维工作的进行；

IT 运维工作本身需要流程管理来进行规范和控制；自动化运维操作将运维工作中大量、重复的劳动来批量控制，自动完成，节省人力，并提高效率。运维工作的质量和结果需要监控来进一步实现观察和确认，以判断是否符合工作预期，必要时，再次调整和提高。

可以说，监视是我们的眼睛，帮助我们透视和认清网络、主机、应用等整个 IT 环境，是我们的情报来源；流程管理是我们的大脑，帮助我们思考、制定决策和完成流程控制和管

理，是我们的情报分析和决策中心；控制是我们的双手，完成自动化批量处理，是我们的实施力量和手段。由此，我们说，“监、管、控”，这是有序的一条龙过程。

双手完成运维处理和控制动作之后，我们需要眼睛再次监视，来查看控制结果。继而，需要大脑来审验：是否符合预期？是否需要进一步调整和控制？如是，进而开始新的“监管控”流转过程。由此，我们还可以说，“监、管、控”，这又是一个闭合的环路过程。

IT“监管控”一体化运维，就是真正实现上面的一条龙过程和达到闭合环路的目的。在 IT“监管控”一体化运维模式下，当监控管理模块发现故障并产生告警后，如满足相应的过滤和触发条件，通过接口会自动触发运维流程管理模块生成相

应的工单，运维流程管理模块依据工单信息和相应运维人员预先设置好的关联条件，自动寻找、识别和匹配自动化运维模块中的操作脚本，实现自动和快速的故障操作处理。由此实现从发现故障到解决故障的 IT 运维全自动化，并自动完成运维操作日志记录，以备事后回顾和审计。

IT 运维自动化不是 IT 运维工作简单的维护过程的改变，而是 IT 运维管理工作的根本变革，是 IT 运维管理的发展趋势。

在 IT“监管控”一体化的运维平台中，原来的网管监控、运维流程管理和自动化运维操作平台转化为对应的“监、管、控”三个模块。

IT 运维一体化平台应在设计之始即充分遵循 ITIL 理论，并结合国内现状、行业特点与实践经验，建立以服务流程为驱动的管理平台，实现人员、流程、技术三方面的完美结合。唯此，才能够在帮助用户深耕基础架构、夯实基础之后，与用户一起建立遵循先进流程管理思想的 ITIL 理论、实现以服务流程驱动为导向的实用的“人管流程”。 IT 运维一体化平台为用户带来“IT 管理理念+系统工具+过程方法”的全新的 IT 服务管理组合，为用户提供包括管理流程与规范、业务及实施方法在内的全方位 IT 运维服务管理一体化解决方案。

IT 服务管理的最终目标是实现业务与技术的融合，IT 运维一体化平台紧扣业务部门与 IT 部门融合要求，提供业务与技术沟通和连接的平台，将业务部门与 IT 部门紧密结合在一起，

能够帮助用户持续提高业务部门和客户的满意度，为客户的IT 服务管理做出贡献，提高用户的核心竞争能力。

实施 IT 运维管理一体化可以帮助企业将 IT 系统原来的混乱状态变到主动的管理状态，包括将技术导向变为流程/服务导向，将被动处理变为预防为主，将孤立、分散系统变为集成化的系统等等。

总之，IT 运维管理一体化通过将人才、流程和工具技术进行有机结合，实现高质量、高可靠性的 IT 服务服务管理。

6.2. 监视模块建设

IT 监控内容：网络设备、链路、主机操作系统、数据库、存储、中间件、应用软件、业务服务、机房环境（温度、湿度）、机房门禁等。

通过 IT 网管监控，可以帮助运维部门和人员实现全天候自动检测，可以及时、快速发现故障，通过事件关联分析，并结合问题管理，实现快速定位故障根源、快速预防和恢复，从而提升 IT 运维响应能力，变被动式管理为主动式运维，使 IT 运维工作从事后“救火式”管理转变到事前预防型管理。

6.3. 流程管理模块建设

IT 运维管理涉及的对象包括设备、技术和人员。其中，人是 IT 运维生产力决定的因素。如何有效实现设备、技术和人员

的统一管理，如何实现人的组织和行为的科学化和规范化，需要 IT 运维流程管理。

IT 运维工作本身具有工作量大、全面、繁琐和复杂的特点，通过有效的 IT 运维流程管理平台，既可以梳理工作流程，又可以理顺部门之间和人员之间的职责关系，达到标准、规范、统一和科学的运维，保证 IT 运维工作无论是整体和全局，还是细节和局部，都能有效推进，避免 IT 运维工作的无序和混乱。

IT 运维监管控一体化解决方案

IT 运维流程管理通过建模，提高流程的可控性。同时，IT 运维流程管理提高 IT 运维管理和执行工作的透明度。传统手工运维流程的不可控性和不透明性给流程定制、管理和优化带来相当大的困难，而 IT 运维管流程管理可以帮助 IT 运维部门一目了然地看到整个流程的全局和各运维工作节点的状况。

通过标准化的 IT 运维流程管理，可以不断提高 IT 运维工作质量，提升企业内外的 IT 服务满意度。

电子运维流程管理系统定位于通过电子化手段来确保运维工作的流程化、工单化、自动化和信息化，实现对流程的实时监控与闭环管理。

6.4. 自动化操作模块建设

在 IT 运维工作中，存在着大量和重复的劳动，如补丁安装、合规检查、配置收集、日常巡检等。计算机的一个重要特点，就是可以帮助人类完成大量的、重复的劳动。自动化运维，就是人类在 IT 运维工作中具体操作层面的计算机化。

通过自动化运维：

实现批量处理，高效、快速工作；　　节省人力，降低人力成本；

将有限的 IT 运维人员解放出来，避免大部分时间和精力是处理简单的、大量的、重复的问题和工作，而是更多时间和精力关注如何提高和保障 IT 运维；　　技术知识和操作脚本共享，运维操作精确化、同质化、优质化、规范化、统一化，避免运维工作中操作质量依赖于个体人员的知识、技术水平、工作责任心和态度等不可控因素；

实现转变：以前运维工作更多依赖于“运维英雄”和埋头苦干型员工，现在更多依赖于运维集体的力量；

交由计算机操作，可以避免人工误操作导致的逻辑错误；

实现运维操作简约化、透明化、规范化、标准化，有利于事前审核和事后检查。

6.5. CMDB 建设

6.5.1. CMDB 战略核心地位

作为 ITIL/ITSM(IT 服务管理)的核心，CMDB 正从管理软件附属品的地位逐渐走入主流的战略核心地位。

企业的 IT 环境越来越复杂，数量庞大、品种繁多。信息散布在企业的不同地方、不同系统中，而且信息的格式、内容也是千差万别，难以统计、查询、利用这些信息，由此给使用、更新、维护、优化等管理工作造成了很大的麻烦，如何快速提供准确的配置信息是一个重大的挑战。

CMDB 储存与管理企业 IT 架构中设备的各种配置信息，它与所有服务支持和服务交付流程都紧密相联，一方面支持这些流程的流畅运转、发挥配置信息的价值，同时依赖于相关流程保证数据的准确性。CMDB 常常被认为是构建其它 ITIL 流程的基础而优先考虑，ITIL 项目的成败与是否成功建立 CMDB 有非常大的关系。

CMDB 是描绘 IT 基础设施如何构建的一个蓝图，它记录了各种各样的配置项（即硬件、软件、事故、协议、服务级别、文档、部门、人员等资源）是如何相互关联的、以及各个系统是如何发挥作用的。

CMDB 与传统的资产库有着根本的差别。资产库是一个存储企业所有资产的数据库，而 CMDB 不仅仅存储所有 IT 元素，更重要的是可以展示它们之间的相互关联，从而帮助企业了解 IT 资产的运行状态是什么样子，它对企业业务有什么影响等。

IT 运维监管控一体化解决方案

IT 环境视图清晰地展现了各种 IT 设备、其属性以及相互关系；业务视图可以让每个人员明确，业务运作模式是什么样，不同业务关联到哪些设备，每个设备的故障影响到哪些业务等。

6.5.2. CMDB 建设方法

CMDB 是一个特殊的数据库，它必须拥有 4 个至关重要的功能：

联邦性：是指 CMDB 能直接获取多种数据源并与数据源联系在一起；　　协调性：能够避免重复，并对来自不同数据源的配置项进行自动匹配；　　同步性：即确保整个系统中的信息是同步更新的；　　可视化：即可提供配置项(CIs)的端对端及层次化视图。

CMDB 有两种，一种是物理的数据库，要求客户把全部配置项都拷贝到物理数据库里面去；另一种是虚拟的数据库，如 MO 的 CMDB，不要求客户把全部配置项都拷贝到物理数据库里，只维持关联关系就可以。

物理型 CMDB 数据库：存在两个问题：其一，不同数据库中的数据要全部无冗余地拷入 CMDB，存在一定困难；其二，不同数据库中的数据也是不断地更新，要想同时把变更之后的数据传递给物理型 CMDB，会带来网络流量方面的问题，也很难做维护。

虚拟型 CMDB：通过指针索引的方式去获得其他数据库里的配置项信息，不存在以上两个问题。 但是，虚拟性 CMDB 需要

人工梳理和比对大量的关联关系，并不断更新。

CMDB 通常采用三种实施方法：自上而下、自中而上、自下而上。每种方法对现有配置数据的实施要求在范围和程度上都不一样。

自下而上的方法：也就是从底层开始，首先查找企业内的所有 CI（配置项），着手建立一个大的数据库，然后查找 CI 之间的关联关系和对业务的影响。这种方法往往要花几年时间才能完成。

自上而下的方法：就是从小的局部系统开始实施，比如信贷核心系统，从这个业务开始着手，然后把底下与此业务相关的所有 IT 元素全都关联过来。这样的好处是可以在比较短的时间内即一个月做出一个完整的 CMDB，而不需要花若干年。

自中而上的方法：就是采用折中方法建立 CMDB，它是通过在企业建设过程中，将逐步形成的分散的、独立的、自身需要的信息资源库在 CI 层面上进行逻辑联邦和同步，建立起虚拟的 CMDB。

自中而上的方法，可以帮助用户在短时间内建立起企业内需要的 CMDB。CI 信息全面，同时见效快，既避免大规模的 CMDB 建设的时间长、见效慢的缺点，也避免了单点突出建设 CMDB 的 CI 范围狭窄、完整度不足的缺点。