ManageEngine
Log360

IT 在实现 SOX 合规性方面的作用

介绍

2002 年，美国国会通过了《萨班斯-奥克斯利法案》（SOX），以保护股东和公众的利益。该法案防止企业会计制度和政策中的错误和不当行为强制采取充分的安全措施、透明的程序，以及准确的公司信息披露。

SOX 法案是为了应对知名公司的会计丑闻而起草的，
安然和安达信等公司导致投资者损失数十亿美元。该法案旨在将企业及审计机构从事欺诈性会计操作的可能性降至最低。

所有在美国注册的公司（无论美国公司还是其他国家公司）美国证券交易委员会（SEC）以及这些公司为这些公司提供金融服务的机构必须遵守法案。这意味着所有美国上市公司、在美国有业务的非美国公司、寻求上市的公司以及为所有这些企业提供金融服务的公司均须遵守 SOX规定。

遵守 SOX 法规需要财务和 IT 部门的大力支持。本文主要关注企业的 IT 部门如何实现 SOX 合规性。

与 IT 部门相关的 SOX 部分

部分	内容
第302节：公司的财务报告的责任	公司的首席执行官和财务官对财务报告的准确性和会计系统的内部控制负有最终责任。
第404节：内部控制的管理评估	所有年度财务报告均须包括内部控制报告，该报告： a. 阐明管理层对内部控制结构负责。 b. 包括对内部控制结构有效性的评估。 c. 要求注册的外部审计师证明该评估的准确性。
第409节：实时信息披露	公司必须迅速、及时地向利益相关者和公众披露任何可能影响其财务状况或运营的信息。
第802节：确保记录保留	与公司财务交易有关的所有物理和电子通信及其他记录均须保留至少五年，并提供给外部审计师。

IT 如何协助实现 SOX 合规性

鉴于大多数财务记录都是以电子方式存储的，您组织的 IT 流程和系统在实现 SOX 合规性方面发挥着关键作用。由于错误或疏忽而导致财务数据丢失或损坏不是不遵守规定的有效借口。根据第 302 条，高级管理人员必须能够声明所有敏感数据均已安全存储和处理。完全准确的财务报告如果公司的 IT 系统暴露出弱点，那么仍然会受到质疑。这就是为什么组织的安全政策、备份系统和审计报告必须严密无懈可击。

为了遵守 SOX 第 302、404、409 和 802 条，IT 团队应：

- 根据内部控制结构向高级管理人员提供深入的审计报告。
- 保持 IT 系统最新并不断监控任何安全漏洞。
- 识别并保护处理敏感财务数据的所有设备、应用程序和 IT 流程。
- 测试所有系统和应用程序是否存在弱点。
- 建立预警机制，及时发现安全事件。
- 有效地调查和应对事件，以最大限度地减少损害并创建详细的取证报告。
- 建立系统将已确认的事件传达给所有利益相关者。
- 整合所有财务记录、通信和相关日志并安全存储。
- 建立自动备份程序并定期测试。
- 通过提供关于网络钓鱼和其他问题的意识计划来防止员工犯错
  社会工程攻击。
- 定义明确的访问策略并确保用户仅获得执行其工作所需的权利。

使用 Log360 实现 SOX 合规性

Log360 通过帮助您审计和保护敏感信息，帮助您的组织实现 SOX 合规性
财务记录。借助 Log360，您可以审计与机密财务数据相关的活动，并确保
防止数据受到未经授权的访问和攻击；调查潜在的安全事件；并安全地
尽可能长时间地保留审计日志。

第 302 条：企业对财务报告的责任

Log360 提供超过 1,200 份直观、预定义的报告，详细列出您的
网络。这包括 Windows、Unix 和 IBM 系统、应用程序、网络设备中的活动，
文件服务器以及 Active Directory、Office 365 和 Exchange Server 环境。您可以
甚至使用自定义日志解析器为内部财务应用程序构建自定义报告。

您可以使用这些报告让高级管理人员了解重要信息的安全性和完整性
财务数据。可根据需要导出或安排所需报告，并进行多种自定义
选项可用。此外，基于角色的访问控制允许您限制查看这些
向授权用户报告。

亮点

全面的网络审计 | 自定义日志解析器 | PDF 和 CSV 报告导出 |
报告调度 | 报告定制 | 基于角色的访问控制

第 404 条：内部控制的管理层评估

为了对会计系统建立有效的内部控制，您需要考虑几个方面
网络安全。Log360 可帮助您覆盖以下领域：

- **审计对机密财务记录的访问和更改。**保持数据完整性并证明
  通过提供详细的审计线索，数据得到妥善处理。您还可以生成报告来证明
  您的数据会定期备份，一旦发生任何损坏即可恢复。
- **监控特权用户活动。**确保特权账户不被盗用，并且
  以负责任的方式使用。
- **检测整个网络中的攻击。**获取以下即时通知：
  - 多个设备之间存在关联的可疑活动模式。
  - 防火墙、IDS/IPS 和其他网络设备检测到的攻击。
  - 与您的网络交互的恶意实体。
  - 在您的 Active Directory、Office 365、Exchange Server 中检测到异常，
    和文件服务器环境。
  - 其他可疑事件，如政策变化、日志被清除等。
- **提供网络状态的透明度。**报告漏洞、病毒、系统崩溃和
  网络中发现的其他问题。SOX 要求对所有可能影响网络的问题保持透明。
  您的财务记录的安全，这些报告可以帮助您提供安全。

亮点

预定义 SOX 合规性报告 | DDL/DML 报告 | Windows 和 Linux 文件完整性监控 | 特权用户监控 | 事件关联 | 威胁情报 | 漏洞报告

第 409 条：实时信息披露

SOX 要求“迅速、及时”地公开披露任何可能影响公司的财务状况。这些事件包括财务系统或数据的安全漏洞。为了确认安全事件已经发生或正在发生，你必须能够进行及时进行彻底的法医调查。Log360 的搜索引擎有助于快速调查并允许您以最小的努力找到事件的根本原因。

其内置的票务功能和帮助台集成还允许您简化事件管理。通过自动分配事件单、跟踪其状态并维护通过过去事件的内部知识库，您可以监督顺利的事件解决过程。

亮点

高级搜索引擎 | 内置票务控制台 | 外部帮助台集成

第 802 条：确保记录保留

所有财务交易和通信记录必须保留至少五年组织需要花费数年时间才能遵守 SOX 规则。日志是这些记录的重要组成部分。使用 Log360，您可以选择保留日志的时间，并且可以导入存档日志随时进行进一步调查。日志以安全、防篡改的方式传输和存储，确保在审计时不会受到质疑。

亮点

灵活期限日志保留 | 防篡改存档 | 安全的网络通信 | 历史日志导入

结论

IT 在支持组织实现 SOX 合规性方面发挥着重要作用。凭借其全面的日志管理和安全功能，Log360 可帮助 IT 管理员构建强大的内部控制系统来保护公司的敏感财务数据。

我们的产品

AD360| ADAudit Plus| EventLog Analyzer |Datasecurity Plus

Exchange Reporter Plus| M365 Manager Plus

ManageEngine
Log360

Log360 是一款集成 DLP 和 CASB 功能的统一 SIEM 解决方案，可检测、确定优先级、调查和应对安全威胁。该解决方案的 TDIR 模块 Vigil IQ 结合了威胁情报、基于 ML 的异常检测和基于规则的攻击检测技术来检测复杂的攻击，并提供事件管理控制台来有效补救检测到的威胁。

Log360 凭借其直观、先进的安全分析和监控功能，提供跨本地、云和混合网络的整体安全可见性。

有关 Log360 的更多信息，请访问manageengine.cn/log-management/。

$ 获取报价　　⬇ 下载