S.O.X （英文）

2002 年，国会通过了《萨班斯-奥克斯利法案》（SOX），以应对包括 WorldCom 和 Enron 在内的几家公司发生欺诈事件和财务丑闻后的影响和不确定性。SOX 法案对财务披露和公司治理的监管进行了几项重大改革，旨在恢复公众对审计和财务报告的信心。SOX 法案，也称为“上市公司会计改革和投资者保护法案”或“公司和审计问责和责任法案”，以其主要设计者参议员 Paul Sarbanes 和众议员 Michael Oxley 的名字命名。

新的或扩展的合规性要求适用于所有美国上市公司董事会、管理层和会计师事务所。考虑 IPO 或准备合并或收购的私营公司也可能发现审查其 SOX 内部控制是谨慎的做法。除其他条款外，SOX 要求：

所有公司的财务报告都包括内部控制报告。

准确的财务数据和控制措施，以保护财务数据。

年终财务披露报告的出具。

通过保护举报人员工来披露公司欺诈行为。

Kim Pham 概述了 SOX 合规性、影响、挑战和关注点，以及利用技术解决方案实现 SOX 合规性。

Sarbanes-Oxley 法案增加了对领导者和管理层的问责要求，使他们对组织财务报表的准确性负责。高管不当行为在 Enron、WorldCom 和 Tyco 等丑闻中发挥了重要作用，并继续影响组织对财务披露和会计实践的态度。因此，SOX 为追究执行官对财务报告中的欺诈行为负责打开了大门。TL;DR SOX 合规性确保公司遵守严格的财务报告标准和内部控制，从而提高透明度和投资者信心。本文介绍了 SOX 法规遵从性的基本要素、实施以及它提供的好处，而不仅仅是遵守法规。

本文将分解不同的 SOX 合规性要求、SOX 挑战、符合 SOX 的好处以及 SOX 审计过程中的预期内容。

对 SOX 的遵守由证券交易委员会 （SEC） 强制执行 作为负责保护投资者和维护公平高效的市场的主要联邦机构，SEC 确保公司遵守 Sarbanes-Oxley 法案规定的严格要求。SEC 的监督有助于提高财务报告的透明度、问责制和完整性，从而增强投资者的信心和市场稳定性。 Public Company Accounting Oversight Board （PCAOB） 是由 SOX 成立的一个新机构，负责监督公共会计师事务所及其上市公司审计的质量。2002 年的 Sarbanes-Oxley 法案由 11 个标题组成，但有两个关于合规性要求的关键条款：第 302 节和第 404 节。

第 302 节：财务报告的公司责任

SOX 第 302 节规定，首席执行官 （CEO） 和首席财务官 （CFO） 直接负责财务报告的准确性。签署官必须审查和证明财务报表的准确性，建立和维护内部控制，并披露内部控制中的所有重大缺陷、欺诈和重大变化。

这项授权允许 CEO 和 CFO 对其组织财务报表中的不准确之处负责，最高可处罚并包括刑事处罚。不遵守 SOX Section 302 可能会导致严重的民事和刑事处罚，包括对故意证明虚假财务报告的执行官处以最高 500 万美元的罚款和最高 20 年的监禁。

第 404 节：内部控制的管理评估

第 404 条规定，所有年度报告必须包括一份内部控制报告，明确概述管理层维持适当内部控制结构的责任、对其有效性的评估以及这些控制中的任何缺陷。独立的外部审计师还必须证明公司关于内部控制措施已到位且有效的声明的准确性。第 404 条包括其他要求，例如由外部审计师审查公司的内部控制，并为某些公司提供豁免。审计委员会对 SOX 404 的审查提供了有关此 SOX 部分的更多详细信息。

为了限制利益冲突，外部 404 审计必须由独立审计师进行，他们以专业的怀疑和判断力来检查上市公司的内部控制状况。

SOX 404 合规性的优势

Sarbanes Oxley 法案的关键成果之一是结束了自我监管，并通过上市公司会计监督委员会 （PCAOB） 建立了对审计流程的独立监督。PCAOB 可以制定行业标准、调查欺诈指控并监管审计公司。事实上，PCAOB 会定期对审计师进行审计，以确保保持高质量并遵循行业最佳实践。

尽管公司最初为合规性的成本和资源负担而苦苦挣扎，但随着时间的推移，他们看到对 SOX 合规性的投资在几个重要方面得到了回报。

1. 改进公司治理：SOX 合规性通过加强对审计委员会的监管来改善公司治理。在 SOX 之前，51% 的上市公司拥有完全独立于管理层的审计委员会。SOX 要求所有上市公司都有一个审计委员会，其成员独立于管理层，并且至少包含一名财务专家。因此，今天的审计委员会更有能力提供准确和真实的财务报告。独立审计委员会的任务与其他委员会不同，为财务报告流程增加了另一层治理。

2. 加强问责制：SOX 合规性使高管更加负责并保护投资者。高管必须亲自认证财务报告，并对欺诈活动进行严厉处罚。审计师也肩负着维护诚信和独立性的重大责任，因为助长 Sarbanes-Oxley 法案的欺诈丑闻还导致了当时最大的会计师事务所之一 Arthur Andersen 的倒闭。

3. 提高审计师的独立性和质量：SOX 合规性通过禁止审计公司向他们审计的公司提供簿记、精算或管理职能来增强审计师的独立性。外部审计师必须在外观和事实上保持独立性。这可以提高审计质量和审计的严谨性。

4. 财务重述减少：在 SOX 之后，财务记录重述的数量继续逐年下降，从 2006 年的 1,784 次减少到 2012 年的 738 次。

5. 改善风险管理和网络安全态势：当今组织作为 SOX 合规性的一部分实施的许多最佳实践，尤其是 IT 一般控制，与 NIST CSF 等网络安全框架的指导重叠。这种重叠的一个例子是呼吁进行强大、受限的访问控制和访问管理，以保护敏感系统和信息免受未经授权的访问 — 大多数 SOX 404 审计都要求对财务上重要的信息系统进行此操作，NIST CSF 强烈建议将其作为其“保护”支柱的一部分。

总而言之，除了简单地保持合规性之外，在您的组织中维护和迭代 SOX 合规性的一些主要好处是：1） 改进的公司治理，2） 增加问责制，3） 提高审计师的独立性和质量，4） 减少财务重述，以及 5） 改进风险管理和网络安全态势。

SOX 的演变：业务变化、网络和 ESG 要求中的技术采用和成本重点

SOX 审计流程

SOX 审计可以分为任意数量的步骤，从执行风险评估到审计委员会报告中应包含的内容。我们将 SOX 审计流程的大纲缩小到以下八个步骤：

使用风险评估方法定义审计范围

确定重要性和风险 – 账户、报表、位置、流程、系统和主要交易

识别 SOX 控制 – IT 一般控制 （ITGCs）、应用程序控制、实体级控制 （ELC） 等。

执行欺诈风险评估

管理过程和控制文档

测试关键控件

评估缺陷

提供管理层的控制报告

1） 使用风险评估方法定义 SOX 审计范围

对于执行风险评估，PCAOB 会计准则第 5 号规定，“自上而下的方法始于财务报表层面，审计师了解财务报告内部控制的整体风险。然后，审计师专注于实体层面的控制，并深入到重要账户、披露及其相关主张。归根结底，PCAOB 建议审计从最高级别开始，变得更加精细。审计范围的重点应该是那些影响财务披露流程的资产、人员、系统和流程——这意味着并非组织中的一切都在范围内。

SOX 审计范围应包括并考虑组织财务报告内部控制的所有风险，以风险优先的方法实现 SOX 合规性。

SOX 合规性审计中的此步骤不应产生合规性程序列表。尽管如此，它仍应帮助审计师识别潜在风险和来源、它可能对业务产生的影响，以及内部控制是否将提供合理保证，以避免、防止或检测到重大错误。

2） 确定 SOX 中的重要性 – 账户、报表、地点、流程和主要交易

第 1 步 – 确定什么被视为损益表和资产负债表的重要内容。方法：如果财务报表项目可以影响用户的经济决策，则它们被视为“重大”。审计师通常可以通过计算一定比例的关键财务报表账户来确定什么是重要的。例如，总资产的 5%，营业收入的 3-5%，或者对多个关键 P&L 和 BS 账户进行一些分析。

第 2 步 – 确定具有重大帐户余额的所有库位。方法：分析您开展业务的所有地点的财务状况。如果这些位置的任何财务报表帐户余额超过了确定为重大的余额（在步骤 1 中），则它们很可能会被视为重要余额，并且在来年的 SOX 范围内。第 3 步 – 识别填充重大账户余额的交易　方法：与您的控制员和特定流程所有者会面，以确定导致财务报表账户增加或减少的交易（即借方和贷方）。这些交易是如何发生的以及如何记录的应该记录在叙述、流程图或两者中。

步骤 4 – 识别重要科目的财务报告风险。方法：设法了解哪些因素会阻止交易被正确记录，或风险事件。然后，记录风险事件可能对账户余额如何被错误记录或财务报表断言的细分产生的影响。

3） 识别 SOX 控制 – 关键和非关键控制、ITGC 和其他实体级控制 （ELC）

在重要性分析期间，审计师将识别并记录可能防止或检测交易被错误记录的 SOX 控制措施。他们将寻求确定财务报告流程中的制衡机制，以确保交易记录正确，账户余额得到准确计算。预防性或检测性 SOX 控制的一些示例包括：

分离冲突和不兼容的职责（例如，过帐和批准发票的能力），

对期间内记录的单笔或多笔交易的审核，以及

Account Reconciliations（账户对账）。

其次，重大账户通常需要采取多种控制措施来防止发生重大错报。您必须分析所有控制措施，以确定哪些控制措施最能提供保证，同时牢记现有的人员、流程和技术。

每当发现新风险时，审计团队都会被警告不要应用暴力破解方法和创建新的 SOX 控制。无意中，每个新控制措施通常被归类为 “关键”，而没有执行真正的风险评估，从而导致控制措施数量不断增加。通过了解关键控制和非关键控制之间的差异，内部审计团队可以有效地应对不断上升的控制数量和“范围蔓延”。

为简单起见，区分非关键vs. key控制的最快方法是参考要解决的风险级别。控制措施是缓解低风险还是高风险？通过了解影响 SOX 合规性流程的风险，审计团队可以更好地确定优先级并将工作重点放在关键控制上。

最后，为了最终确定和规划有效的内部控制系统，您的审计团队必须确定手动和自动控制。对于确定的自动控制措施，您应该评估底层系统是否在 IT General Controls （ITGC） 测试的范围内，这将影响控制措施的整体测试策略。如果您对底层系统感到满意，则可以大大减少需要执行的控制测试量。运营强大的 ITGC 和网络安全相关控制措施是 SOX 合规性的另一个好处。

4） 进行欺诈风险评估

有效的内部控制系统包括对可能的欺诈活动的评估。预防和早期检测对于减少组织中的欺诈事件至关重要。内部控制在减少欺诈机会以及发生欺诈将产生的重大影响方面发挥着关键作用，包括手动推翻内部控制。

以下是组织可以实施的反欺诈内部控制和实践示例，以显著降低欺诈造成的损失。

职责分离：内部审计师协会 （IIA） 将职责分离的基本理念描述为“任何员工或员工群体都不应在正常职责过程中犯下和隐瞒错误或欺

诈行为。也就是说，一个人的工作应该独立于另一个人的工作，或者起到检查另一个人的工作的作用。例子：

资产托管

对影响这些资产的相关交易进行授权/批准

记录和报告相关交易

费用报销：根据 ACFE 2014 年的报告，很大一部分资产挪用计划涉及员工要求报销虚构或夸大的业务费用的情况。为防止此类骗局，管理层应确保将有关员工报销的相关政策和程序传达给员工，并在必要时进行更新。此外，此类报销的审批流程应包括与直接主管一起，其他关键利益相关者，例如受影响的业务团队成员、工资单或内部审计。

举报热线：尽管有联邦法规，但实施强有力的举报人计划的最终责任在于管理层。从历史上看，内部员工举报是检测欺诈的最佳方法。因此，管理层不能忽视组织内部的举报机制。

银行账户的定期对账：银行对账突出了每个资产负债表的现金和银行对账单之间的差异，同时也确认了组织现金分类账中记录的数据的准确性。执行银行对账的核心职责不仅是识别意外差异，还需要防止未来发生，例如会计延迟、限制自动借记给供应商等。根据组织的规模，应每天、每周或每月进行银行对账，以监控和检测欺诈活动。

正是管理层对欺诈检测和预防的积极方法，加上强大的内部控制，最终将减少欺诈的机会，并在组织内灌输道德文化。

5） 管理流程和 SOX 控制文档

控制叙述和文档确定了关键控制操作的详细信息，例如控制描述、频率、测试程序、相关风险、总体和证据。风险和控制映射通常具有多对多关系，这使得手动记录变得困难。一些示例包括跨多个流程或业务部门出现的风险、影响多个控制措施或流程的审计问题，以及映射到多个控制措施的 COSO 原则。正如审计经理可以证明的那样，如果团队中的一名成员未能及时进行编辑或忘记对所有测试表进行更新，则下游的连锁反应可能会使经理花费数小时的清理工作。解决方案是利用底层关系数据库作为中央存储库和审计计划的基础。基于专门构建的数据库结构构建的 SOX 软件可以允许审计员快速将信息拉入或推送到数据库或从数据库中推送信息，并使这些结果立即在整个 SOX 计划中级联。控件文档很简单，不需要在多个独立的电子表格文件中进行编辑。此外，对于年复一年使用的年度审计结果，电子表格无法处理大量数据。数据库解决方案的速度、准确性和可扩展性将超过“熟悉电子表格”的好处。

6） 测试关键控件

SOX 控制测试的总体目标有三个方面 – 1） 确保概述的过程或测试程序是测试控制的有效方法，2） 在整个期间由指定的过程所有者执行控制，以及 3） 控制已成功防止或检测任何重大错误陈述。简而言之，控制测试验证了控制措施的设计和运行有效性。

实际的 SOX 控制测试过程可能包括各种或组合的测试过程，包括持续评估、观察、与流程所有者的询问、交易演练、文档跟踪检查和/或流程的重新执行。

7） 评估 SOX 中的缺陷

对 SOX 计划的持续投资自然会带来您的行动、政策和程序的改进。随着控制环境的改善，企业也可能会看到自动化水平的明显提高，审计师所需的手动测试量也相应减少。最终，这将导致您的团队花更少的时间管理更少的整体问题。缺陷应该减少到可接受和可预测的水平，并且应该几乎没有意外。

在 SOX 控制测试过程和分析期间，审计员可能会识别测试样本中的豁免、缺陷或差距。如果发生这种情况，则会创建一个 “issue”。除了补救和纠正问题外，审计团队还会评估是控制中的设计失败还是需要调整培训、职责或流程的操作失败。最后，管理层和审计团队评估这是否是一个重大缺陷（如上所述，通常是一定比例的差异，并且具有高风险水平），并将在年终财务报告中报告，或者它是否只是一个重大缺陷。

8） 交付管理层的控制报告

SOX 控制测试的最终产品是向审计委员会提交管理层关于财务报告控制情况的报告。虽然在此过程中收集了大量文件和数据，但报告应包括：

管理层的意见和对这些结论的支持摘要。

审查所使用的框架、收集的证据和结果摘要。

每项测试的结果 – 实体级、IT、关键控制。

识别控制故障、差距和相应的根本原因。

由公司的独立外部审计师进行评估。

SOX ITGC 和安全控制

随着技术形势的快速发展，公司对信息技术和系统管理财务信息的依赖会显著影响公司编制和交付其证券交易委员会 （SEC） 报告的方式。由于大多数公司已将具有财务重要性的职能和运营转移到信息系统，包括会计职能、财务职能，甚至零售/电子商务职能，因此成功的网络攻击对组织的影响可能很严重。即使不影响企业的 SOX 合规活动，安全事件也可能导致数据泄露和数据丢失，从而给公司带来另一组挑战。

作为 SOX 的一部分经过测试的一些基础 ITGC 可以帮助避免安全漏洞和篡改财务重要信息。通过围绕数据保护、变更管理和敏感数据

建立有效的安全控制，IT 部门可以更好地检测、预防和修复任何潜在的安全事件。即使是大量利用云服务且没有自己的数据中心的公司也应定期查看其第三方供应商的合规性报告，以验证供应商的数据安全标准是否符合您的组织。供应商的不合规行为仍可能给该供应商的客户带来相当大的风险。

常见的 SOX 合规性挑战

电子表格和最终用户问题

低调的电子表格已经发展到不仅仅是一个簿记工具。随着时间的推移，简单的电子表格已经演变成 SOX 工作流程的主打产品，部分原因是它能够跨不同文档链接数据并自动执行基本任务。同时，现代审计项目现在需要有关控制的更多属性和详细信息。无论是记录证据的完整性和准确性，还是验证关键报告的完整性，测试程序都已经超越了简单的属性勾选和捆绑。现代电子表格可以处理这种强大的测试过程，但缺乏速度、效率和一致性。

除了上述内容之外，在 SOX 计划中使用电子表格还存在一些风险，包括但不限于：

用户错误或已删除的数据

分析不一致的数据集 — 即总体不正确

进程所有者被蒙在鼓里

负责日常控制活动的流程所有者在涉及自己的控制时，往往被蒙在鼓里。内部审计团队依靠电子表格和共享文件夹来管理他们的控制措施，因此文档通常保留在内部审计团队的桌面上，远离流程所有者。

当控制文档存在于内部审计中时，流程所有者每个季度只能查看一次他们的控制，从而创建自己的日常活动，这些活动由他们自己的任务版本驱动，而不一定在他们自己的控制范围内。

不断上升的成本和资源

虽然 SOX 对财务报告产生了积极影响，但人们仍然担心 SOX 法规遵从性成本不断增加和资源负担沉重。根据 Protiviti 的年度 Sarbanes Oxley 调查，许多公司的 SOX 成本逐年上升。原因包括引入 COSO 等新框架以及不断发展的 Section 404 合规性外部审计师要求。如今，公司每年平均在 SOX 计划上花费 100 万到 200 万美元和高达 10,000 小时。

使用专用技术简化 SOX 合规性

降低 SOX 合规性的成本和耗时性并最大限度地利用 SOX 资源的一个关键在于利用专门构建的技术来实现流程自动化。有远见的 SOX 团队正在利用 SOX 自动化工具来减少在 SOX 上花费的管理时间和精力。SOX 合规性软件使团队能够腾出时间来执行更多的增值审计

，提高内部控制的质量，提高对 SOX 环境的实时可见性，促进外部审计师的协作，并最终避免财务重述。

有关 SOX 合规性的常见问题

什么是 Sarbanes-Oxley 法案 （SOX），为什么要颁布它？

Sarbanes-Oxley 法案，通常称为 SOX，是 2002 年颁布的美国联邦法律，旨在通过提高公司披露的准确性和可靠性来保护投资者。该法案的通过是为了应对重大企业和会计丑闻，包括涉及安然和世通的丑闻，以恢复公众对金融市场的信心。

SOX 合规性的关键要求是什么？

SOX 合规性要求公司实施和维护对财务报告的强大内部控制。关键要求包括 CEO 和 CFO 对财务报表的认证（第 302 节）、建立内部控制框架（第 404 节）以及外部审计师的独立性（第 301 节）。公司还必须定期进行 SOX 审计，以确保符合这些标准。

公司如何确保成功遵守 SOX？

为确保成功遵守 SOX，公司应建立专门的 SOX 合规团队，实施全面的内部控制，并定期对员工进行培训。利用 Audit Board 等审计管理软件可以通过自动化工作流程、提供实时数据分析和生成详细的合规报告来简化合规流程。定期审计和持续监控对于保持合规性和及时解决任何问题也至关重要。

副

Vice Vicente 的职业生涯始于安永，过去 10 年一直在 IT 合规、风险管理和网络安全领域工作。Vice 已为 120 多家客户提供服务、审计或咨询，实施安全性和合规性计划和技术，围绕 SOX 404、SOC 1、SOC 2、PCI DSS 和 HIPAA 执行项目，并指导公司做好安全性和合规性准备。在 LinkedIn 上与 Vice 联系。