



信息化实践过程中 **CIO**应关注的方法和技术

孙洪林 著



 原子能出版社

责任编辑：刘 朔 封面设计：赖仁金

ISBN 978-7-5022-4249-7



9 787502 242497 >

定价：35.00 元

信息化实践过程中

CIO 应关注的方法和技术

孙洪林 著

原子能出版社

图书在版编目 (CIP) 数据

信息化实践过程中 CIO 应关注的方法和技术 / 孙洪林著.
北京: 原子能出版社, 2008. 9
ISBN 978-7-5022-4249-7

I. 信… II. 孙… III. 企业管理—信息管理 IV. F270.7

中国版本图书馆 CIP 数据核字 (2008) 第 139293 号

信息化实践过程中 CIO 应关注的方法和技术

-
- | | |
|------|-----------------------------------|
| 出版发行 | 原子能出版社 (北京市海淀区阜成路 43 号 100037) |
| 责任编辑 | 刘 朔 |
| 责任印制 | 丁怀兰 刘芳燕 |
| 印 刷 | 北京市玖仁伟业印刷有限公司 |
| 经 销 | 全国新华书店 |
| 开 本 | 787 mm×1092 mm 1/32 |
| 印 张 | 7.0 |
| 字 数 | 189 千字 |
| 版 次 | 2008 年 9 月第 1 版 2008 年 9 月第 1 次印刷 |
| 书 号 | ISBN 978-7-5022-4249-7 |
| 定 价 | 35.00 元 |
-
- 版权所有 侵权必究 <http://www.aep.com.cn>

序 言

自 20 世纪 80 年代以来,信息技术的快速发展和广泛应用给经济和社会领域带来了革命性的变化,信息技术不仅快速推动着全球经济结构和增长方式的转变,同时也是社会变革和人类生活方式变化的巨大推动力。事实上,信息技术应用的广度与深度,即信息化水平已经成为衡量一个国家和地区现代化水平的重要标志。信息资源日益成为重要的战略性生产力要素,在经济发展和社会进步中发挥着重要作用。作为推动信息化进程主要负责人的 CIO(Chief Information Officer, 首席信息官)群体,在世界各国受到了普遍重视。

CIO 是一个政府机关或企事业单位中负责信息技术领域工作,并通过指导使用信息技术来实现本单位目标的高级管理人员;应具备技术和业务过程两方面的知识,常常是将组织的技术战略与业务战略紧密结合的最佳人选。CIO 负责信息技术、信息资源、信息服务、信息战略、知识管理与业务战略整合,通过组织和利用企业的 IT 资源,为企业创造效益。因此,CIO 的视野、能力、技术水平与本单位的信息化水平及目标实现有着极大的关系。

本书通过吸收、理解国内外众多成功 CIO 在信息化实践过程中对 IT 发展及应用的观点、技术和管理方法,归纳总结出自 2005 年以来 IT 环境、技术、技巧、方法及发展等方面的论述(包括 IT 环境和发展趋势,企业管理和人才培养,IT 技术和体系结构,信息安全、数据和存储等方面),帮助国内政府机关和企事业单位的 CIO 以国际化的视野,以及更前沿的 IT 技术、更有效的管理方法进行信息化实践,以迎接和面对未来的机遇和挑战。在当今这样一个全球化时代,学习和借鉴成功的信息化实践经验,研究总结国内外成功案例和失败教训,并在此基础上,推进本地区、本行业,以及本单位的信息化工作,无疑是一条行之有效的道路。

本书的编写得到了陈韵、闫光永、陈永华、孙宝春、陈慧明等人的大力帮助,在此向他们表示衷心的感谢!

在本书编写过程中,不足之处在所难免,敬请广大读者和各位同行提出批评指正。

作 者
二〇〇八年六月

目 录

第 1 章 IT 环境和发展趋势

1.1	实施萨班斯法案的重要性.....	2
1.2	遵守萨班斯法案的十大技巧.....	5
1.3	CEO 面临的十大挑战.....	8
1.4	影响反间谍软件改革所采取的合法行为.....	10
1.5	如何保护合法信息.....	12
1.6	警惕厂商出现的预兆迹象.....	14
1.7	开放源码的时代已经来临.....	18
1.8	美国的创新投资有法律保障.....	20
1.9	美国网上消费日益高涨.....	22
1.10	网上销售增加但服务水平需提高.....	24
1.11	电子商务在日常生活中发挥重要作用.....	26
1.12	IT 业发展的六大趋势.....	30
1.13	美国 IT 人员就业形势呈现好转.....	32
1.14	外包网络安全有一定的危险.....	34

第 2 章 企业管理和人才培养

2.1	时代发展给信息技术提出更高要求.....	36
2.2	执行信息系统是企业的重要辅助工具.....	39
2.3	顾客忠诚才能带来盈利.....	42
2.4	怎样管理移动办公人员.....	44
2.5	托管客户关系管理系统.....	46
2.6	有关项目管理的十条谏言.....	49
2.7	如何解决软件项目费用过高问题.....	51
2.8	如何有效评估选择 IT 公司.....	54

2.9	通过 IT 部门为企业创造收益.....	57
2.10	通过 IT 技术简化管理.....	59
2.11	CIO 在外部采购时需把握五大要点	62
2.12	如何使技术顾问为企业带来最大效益	64
2.13	实施 CRM 系统的重要性	67
2.14	正确认识时间管理问题.....	71
2.15	领导应如何分配工作时间	74
2.16	如何解决工作堆积问题.....	77
2.17	如何迎接 IT 人才争夺.....	79
2.18	与员工沟通的重要性.....	82
2.19	退休 IT 专家发挥重要作用.....	84
2.20	IT 专业人士打造个人品牌的必要性.....	86
2.21	IT 专业人士如何打造个人品牌.....	89

第 3 章 IT 技术和体系结构

3.1	未来八大软件发展技术.....	93
3.2	无线网络在我们生活和工作中必不可少	96
3.3	结构技术的兴起.....	98
3.4	面向服务体系结构的远大目标.....	100
3.5	面向服务体系结构是高效的.....	103
3.6	商业智能很有发展价值.....	105
3.7	商业与 IT 项目联合的五步骤.....	108
3.8	RFID 将在未来五年内呈爆炸式增长	112
3.9	联合技术开发是一种优化的技术方法	113
3.10	美国科技执行官呼吁频谱改革.....	118
3.11	SaaS 取得了新的进展	120
3.12	解决 PPM 中观念混淆问题	123
3.13	PPM 报告的基本原则	126

3.14	实施业务流程管理的必要性.....	129
3.15	如何实施业务流程管理.....	132

第4章 信息安全、数据和存储

4.1	信息系统安全保障措施.....	138
4.2	对入侵防御系统的评估.....	142
4.3	设计安全方案的五个步骤.....	145
4.4	信任范围与信息安全.....	148
4.5	信息安全投资问题.....	151
4.6	IT 安全投资依然欠缺.....	155
4.7	IT 安全意识与行动须统一.....	157
4.8	身份证书管理的危机.....	160
4.9	用户名/密码认证方法将无法满足要求.....	163
4.10	黑客和骗子在网站上掩藏恶意 JAVA 脚本	166
4.11	VOIP 投放市场前还需解决安全问题.....	168
4.12	数据加密的安全之道.....	174
4.13	成功实施灾难恢复的四条原则.....	177
4.14	简化灾难恢复的方法.....	180
4.15	数据是否可以被永久删除.....	183
4.16	集成数据可以使你更深入地理解客户需求.....	187
4.17	优质数据管理的基本步骤.....	189
4.18	iSCSI 存储的新理念.....	193
4.19	存储软件的发展热潮.....	197
4.20	使存储管理成为现实.....	199
4.21	SAN 和 NAS 殊途同归.....	202
4.22	高性价比存储系统 Panasas.....	205
4.23	新型备份方法—磁盘到磁盘备份.....	208

第1章 IT 环境和发展趋势

1.1 实施萨班斯法案的重要性

由于企业最初实施萨班斯法案(Sarbanes-Oxley, 以下简称为 SOX 法案)时花费了大量的精力和财力, 因此一些企业刚刚从“SOX 法案后遗症”中恢复过来。然而, 企业在法案的实施过程中是否获得了有益的东西呢?

实际上, 根据目前的分析报告, 只有 37%的人认为 SOX 法案的实施对他们公司的发展没有任何帮助; 同时, 如果 IT 执行者认为遵守 SOX 法案无法达到企业的预期目标, 那么他们往往就会失去促进他们企业更快发展的一个大好时机; 然而, 如果他们的竞争对手认为可以从法案的实施中获得潜在的平衡优势, 那么这些 IT 执行者就可以获得主要的竞争优势。

一、法案实施的生命周期

大部分企业的法案生命周期主要有以下三个阶段: 首先, 当最初执行法案时, 通常会以“强制性”方法创建或调整内部手工控制来充分满足规章需求; 第二阶段是内部控制的自动操作, 使用自动操作可以使基础设施更加有效地运作, 同时, 比使用非自动操作控制的设备更安全; 最后一个阶段就是全面实施。这时可以提高企业的效益。

由此, IT 管理者可以营造一个更丰富、更有效和更有竞争力的 IT 操作环境, 而不只是单纯为了遵守法案形式。

因此, 一个企业如何通过遵守法案来更有效地促进企业发展呢? 第一步就是要遵守法案规则。

这种行为方式并没有过时, 而且还会不断颁布新的法案。此外, 还需具备一个在任何时候都不会被淘汰的制度。因此, 企业必须要遵守法案, 越早把这项任务作为其项目实施的一部分, 企业的发展就会越快。

如果分散法案的实施过程, 管理实际的内部控制就会如同管理数据一样。同时, 还可以让程序员创建程序来确保更有效地进行控制。

当然，这项工作会被许多内部和外部的 IT 审计员进行审计；然而，成功地执行法案是每个企业的责任。

实施分散控制策略应该是集中性和一致性的统一。如果每一个单位都试图以自己的方式去遵守一个特定的法规，那么将会导致社会混乱，审计工作也将变得更加困难。

所以，要确保一个稳固、集中的法案策略并且要监视其实施流程；同时，每个人都要进行实际的控制管理，然后让评估小组来进行评估。

下一步，每个人都要对执行法案提出自己的建议，并把其视为个人责任。

法案并不是由那些周期性地审查实施过程的内部审计员来执行。这是企业员工每天必须执行的一项工作，他们的工作职责就是接触所有规定的内部控制。

二、促进企业发展

理论上听起来很好，然而你是如何促进企业发展，并把它作为一个长久的奋斗目标呢？如何促进企业发展的细节问题，对每一个企业来说都很详细、具体。为达到企业发展目标而实施的一些典型、强制性的方法简述如下：

1. 减少风险。一些企业发现 SOX 法案的实施使得内部安全控制变得更加稳固。比如，控制整个企业使用权限，对于保护应用程序和数据来说可以更加稳固、持久。

减少 IT 风险同样是为了减少整体的企业风险。相对低的企业财务风险，可以使企业更加有利地吸引投资者和询问者。然而，降低主管和执行者的个人责任保险成本，会提高财务收益；最终将会减少精力、成本，以及即将进行的最终审计工作。

2. 提高效率。从整体上说，法案是为了揭露和调整不稳定、低效率的内部控制所颁布的。因此，不能只从资源和金钱上的开销来考虑法案的实施，应该考虑这些法案是如何实施的，也许他们的实施成本会比较高，却可以有效减少 IT 成本。

3. 优化企业流程。实施法案的最有利之处在于可以深入分析、优化内部控制和企业流程。

为了确保企业正确和成功地实施法案，需要深入了解法案规则，以及进程情况。有时会出现低效率或多余的法案实施或是无效的内部控制进程。

首先，解决这些问题可以使企业操作更加流程化。同时，IT基础设施的安全性也会更有保障；其次，还有一点很重要，就是法案的实施可以确保企业履行责任。

当分析内部进程时，应该包括商业进程中每一阶段，以及每一步的实施所应有的责任。正如在我们的日常工作环境中所经常看到的，责任明确可以提高企业效益，而遵守法案也需要明确责任。

4. 更好地制定策略。SOX 法案的实施需要制定安全控制策略，其主要目的是确保那些没有使用权限的人禁止使用、修改，对财务或企业信息进行保护。同时，管理控制的实施可以使有权限的人快速、方便地使用那些受保护的信息。

及时访问重要的商业信息，就可以更好地进行计划、预算和全面地制定策略。更准确地说，更好和更有效地制定策略可以提高企业整体的竞争地位，同时，这也是负责法案实施的员工经常忽视的地方，他们经常把注意力集中在满足法律形式上，而忽视了法案的实施可以为企业带来的潜在利益。

因此，当企业在实施进程中获得更多经验时，他们就可以更加流畅和更加有效地进行企业操作，法案的长期实施所带来的利益也将会变得更加显著。

1.2 遵守萨班斯法案的十大技巧

自从美国联邦证券交易委员会执行了萨班斯法案（Sarbanes-Oxley，以下简称为 SOX 法案）第 404 节到现在已经一年多了。然而，遵守这条法案就意味着在企业忙碌的进度表中又增加了许多新的实施项目；此外，还需要对这些项目进行审查、文件分类，以及程序控制。为了保证企业的 IT 基础设施能够满足企业需要，这是你每天需要做的额外工作。

遵守 SOX 法案对于上市企业和上市会计师事务所来说都是非常必要的。这些企业需要遵守这些法案来执行文件分类、评估，以及报告财务控制情况。上市会计师事务所需要这些法案去执行他们自己的评估和控制；另外，他们必须审查和评估企业的第 404 节法案文件分类，以及报告。这就意味着一个 IT 部门必须满足企业多层需要，并且至少要分别参与两次审查。

即使你不是上市企业的 CIO，你仍然需要遵守第 404 节法案。SOX 法案是一个范围很广的规则，它对政府、企业和会计师事务所都适用。证券交易委员会设立了上市公司会计监督理事会来管理上市会计师事务所。新的上市公司会计监督理事会标准将应用到所有上市会计师事务所，这些标准有 SOX 法案和常规的审计惯例等。这就意味着，一个私有企业的 IT 部门也必须进行年审；必须根据第 404 节法案的审计结果制定标准来满足 IT 需求。

“综合审计”综合了内部控制对标准审计程序的所有审计。综合审计的一个关键程序是对 IT 常规控制的审查。

IT 常规控制的审查涉及文件分类、评估和 IT 控制等环节。对于上市企业来说，在遵守第 404 节法案时将涉及这些环节；而对于私有企业来说，将在年终审计时涉及这些环节。

在每一个过程中，企业都需要去处理多层请求来完善 IT 文件分类、提供明确的文件格式类型、更改你的操作程序，以及承担重复测试。

如何避免出现多层窗口和多种格式的文件，成功地与企业进行链接，并且得到它们的认可，同时保持在 SOX 法案中的地位呢？以下十种方法可以确保你顺利实施：

1. 接受教育。要求企业财务部门安排一个与上市企业会计师的联席会议，对 IT 的常规控制提出建议；另外，IT 部门专门研究 SOX 的公司信息，比如，接受上市会计师事务所和 ISACA（国际信息系统审计协会）提供的有关 SOX 法案的教育。

2. 确定正确进程。确定企业团队明白 SOX 法案是如何适应 IT 环境的；确定 IT 团队是从项目实施开始，然后再进行更新，包括基于 IT 系统和基础设备的企业过程审查。

3. 确定对现有文件的评估。IT 部门在他们的 SOX 法案中对现有的程序、政策和文件进行分类评估，这非常重要。比如，一些药物厂商和制造商已经遵守了联邦条款，其中一些制造商还通过了 ISO9000 的认证。

4. 确定设计一个适合你企业需要的计划。制定遵守 IT SOX 404 的计划应该符合你的企业需求。

5. 确定要雇用那些精通 IT 管理和 SOX 404 法案的顾问。许多 CPA 公司在会计、审计和 SOX 方面都很专业，但是却从来没有管理过 IT 部门。此外，许多企业都需要最前线的专家来制定对公司有利的决策。同时，需要把会计实践转换成 IT 部门可执行的术语和可实施的行为。

6. 确定执行团队。明确执行团队已经了解 IT 需要做的事情，以及如何实施计划；同时，CIO 或类似的执行者应该成为 SOX 指导委员会的成员。

7. 更改标准程序。确保所有企业都按照标准程序来进行评估、文件分类，以及执行控制，但是要记住每个企业的执行过程都是不一样的。要对一些单位的 IT 控制开发一个鉴别和描述程序，并且对标准控制的原理要有一套自己的理论方法。

8. 不要试图一次去承担太多工作。遵守 SOX 404 对于一些 IT 组织来说是一个艰巨的任务。对任务进行优先次序的划分, 先执行重要任务, 然后执行其他任务。一些任务的执行可能要拖延一年时间。

9. 在执行过程中尽早获得反馈信息。与你的 SOX 项目管理办公室 (PMO) 和会计师事务所一起来分享你的程序设计, 以保证你的设计思路是正确的。在执行程序前, 要事先审查被提议的变更程序, 来确定你的程序变更能够满足企业的需要。

10. 保持灵活性。规则在不断变化, 并且还将不断改进。因此, 为了保证企业 IT 团队更好发展, 必须要集中发展如何维护企业资产、维持数据完整性, 以及为 IT 部门提供他们所需要的基础设施。

遵守 SOX 404 法案与建立一个持续性的网络体系同等复杂。但是, 对于那些需要遵守 SOX 法案的企业来说, 不必太担心其实施的难度。

1.3 CEO面临的十大挑战

全世界的首席执行官(Chief Executive Officer, 以下简称为 CEO)都将期待 IT 业有更快发展, 以及带来更多收益, 然而通过调查发现, 对于全世界 37% 的 CEO 来说, 保持持续并稳固的发展将成为他们最大的挑战。

美国的 CEO 对 IT 技术与商业的结合, 以及不断上涨的员工薪水、福利非常关心, 但根据 Conference Board 公司的一项对全世界 CEO 的调查, 对于亚洲和欧洲的 CEO 来说, 这个问题的重要性不是排在第一位。

Conference Board 公司的调查报告表明, 来自 40 个国家的 658 位 CEO 面临十大挑战。每年 CEO 都会面临这种挑战, 这种挑战为美国和其他主要发达国家建立了消费者信心指数和经济前导指数。在其他国家, CEO 还会面临很多其他挑战, 比如公司的规模、产业和取得成功的等级, 这些挑战都会引起 CEO 的关注。

在美国, 排在前四位的挑战依次是:

第一位, 保持持续不变和稳定的增长速度, 占 40%。

第二位, 管理高层对决策的统一执行, 占 38%。

第三位, 顾客忠诚度, 占 37%。

第四位, 利润增长, 占 27%。

这些挑战对 IT 来说意味着什么? 根据 Conference Board 公司的一名评论员兼研究室主任 Linda Barrington 说, 如果 CEO 可以在自己的岗位上充分发挥职能, 那么 CIO 和其他高层 IT 经理就需要清楚地知道 CEO 的顾虑和需要。

这些挑战占据了 CEO 的日常工作, 所以必须争取时间来真正了解这些挑战, 然后再安静地思考一下: 我怎样才能使它成为我职责的一部分? 管理高层对决策进行统一执行, CIO 应和 CEO 说些什么, 怎样支持 CEO 设法对管理高层的决策进行统一执行? 这是一个需要深思熟虑的问题。

通过对行业的划分，金融业、其他服务行业和制造业的 CEO 也同样把商业和 IT 技术的结合划分为十大挑战。同时，所有的 CEO 都指出为了跟上技术的发展步伐，他们花费了大量的时间和精力。

CEO 发现和去年相比，与技术同步发展是一个很大的挑战。这个挑战也许是他们自己的产品没有跟上发展，也许是他们还没有领悟到自身的发展方向。

亚洲的 CEO 最为关心的是利润增长，占 42%；紧接下来的是保持持续和稳固的增长，占 41%；加速、机动性和适应性的变化，占 41%；顾客忠诚度，占 35%；市场占有率和公司信誉，各占 33%。

欧洲国家的 CEO 最为关心的是加速、机动性和适应性的变化，占 39%；然后是利润增长，占 38%；保持持续和稳固的增长，占 37%。

这次调查也表明挑战与竞争压力不断增长。与去年相比，许多 CEO 重视以更快速度占领市场，并通过技术发展并购其他企业。

在过去的几年中，各个管理层更清楚地认识到利润主要来自于合并、收获、联盟，以及道德规范；同时，还来自于现金管理、短期业务压力、资金成本、债务负担，以及跨国规章问题等。

在这次调查中，还发现了其他一些关键问题：

1. 在欧洲和美国的十大挑战排行中，产品创新在 CEO 中居于第 6 位；但在亚洲的 CEO 中只排在第 25 位；

2. 高级管理层持续和稳定的发展、策略的一致性执行是所有规模企业的 CEO 最为关心的问题；

3. 企业销售量高于 5 亿美元的 CEO 处于更高级的挑战，他们需要推进改革和创新，充分发挥管理层的职权并加速机动性和适应性的变化。