辅助快速实现 SOX 法案遵循

解决方案

慧点科技开发有限公司

2005-03

摘要

慧点科技自 1998 年成立至今，始终致力于电子协同和知识管理领域的研究和开发，曾成功的实施了近百个大型企业的办公自动化系统。慧点科技是 IBM 高级合作伙伴，并且是 IBM WBCR 产品在中国大陆地区的唯一指定代理商。

本解决方案是建立在对中国在美上市公司的具体情况进行了较详细的了解和分析的基础上，并充分结合慧点科技在大型系统的成功实施经验而撰写的。本方案基于 IBM Workplace for Business Controls & Reporting，对系统的服务思路进行了总体的阐述，希望能够帮助中国在美上市公司满足 Sarbanes-Oxley 2002 法案（简称‘法案’）第 404、409 和 802 部分的内部控制、报告、披露和归档要求。

第一章 背景概述

1.1 Sarbanes-Oxley 2002 法案的由来

2001 年 12 月，美国最大的能源公司——安然公司，突然申请破产保护，此后，公司丑闻不断，规模也“屡创新高”，特别是 2002 年 6 月的世界通信会计丑闻事件，“彻底打击了（美国）投资者对（美国）资本市场的信心”（Congress report, 2002）。为了改变这一局面，美国国会和政府加速通过了《萨班斯法案》（以下简称 SOX 法案），该法案的另一个名称是“公众公司会计改革与投资者保护法案”。法案的第一句话就是“遵守证券法律以提高公司披露的准确性和可靠性，从而保护投资者及其他目的。”

美国总统布什在签署“SOX 法案”的新闻发布会上称“这是自罗斯福总统以来美国商业界影响最为深远的改革法案”。但由于该法案刚刚通过不久，其执行也不到两年，现在就来评价该法案的成败得失，为时尚早。但是，了解该法案的通过背景以及该法案制订过程中的一些问题，对我们正确认识、把握该法案，从而理性地看待我国资本市场的相关事件以及相应的对策问题，不无裨益。

1.2 Sarbanes-Oxley 法案第 404 节－－管理层对内部控制的评价

“SOX-404”（内部控制的管理评估） — 由布什总统于 2002 年 6 月 30 日写进法案，旨在通过加大控制力度来加重公有企业决策人的责任。

■ 内部控制方面的要求

SEC 应当相应的规定，要求按《1934 年证券交易法》第 13 节(a)或 15 节(d)编制的年度报告中包括内部控制报告，包括：

- 强调公司管理层建立和维护内部控制系统及相应控制程序充分有效的责任；
- 发行人管理层最近财政年度末对内部控制体系及控制程序有效性的评价；

■ 内部控制评价报告

对于本节中要求的管理层对内部控制的评价，担任公司年报审计的会计公司应当对其进行测试和评价，并出具评价报告。上述评价和报告应当遵循委员会发布或认可的准则。上述评价过程不应当作为一项单独的业务。

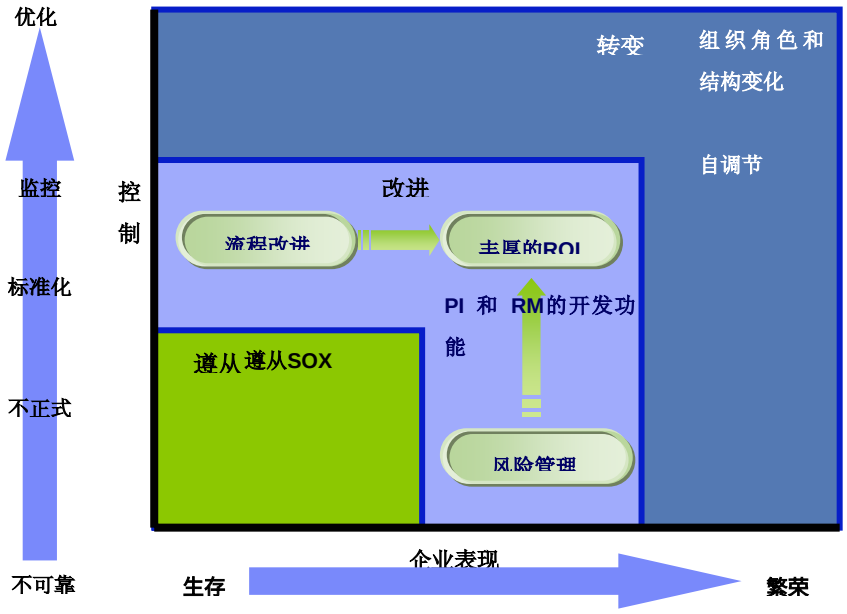

图 1 SOX 法案成长历程

1.3 Sarbanes-Oxley 法案对国内在美国上市企业的影响

总体而言，SOX 的目的在于促进企业责任感（302 条款），完善内部控制（404 条款），加强信息向公众的披露（409 条款），提高财务报告和审计的质量及透明度，并对违反证券法律和其它法规的行为加大惩罚力度及加重其刑事责任（906 条款）。

此外，该法规还包括以下方面：

■ 加大了对企业欺诈行为的惩罚，加强了对企业检举人的保护；

■ 要求包括公司财务报告在内的所有美国证券交易委员会（SEC）定期备案材料，必须经公司首席执行官和首席财务官签名确认；

■ 要求年度报告中必须出具一份内部控制报告，与 CEO 和 CFO 对年度和季度报告的签名确认书一起备案。

SOX302 节“公司对财务报告的责任”中，明确要求公司 CEO 和 CFO 等签字官员在报告中指明，在他们对内部控制评价之后，内部控制是否发生了重大变化，或是其它可能对内部控制产生重要影响的因素，包括对内部控制的重大缺陷或重要缺点的更正措施。

由于这些新法规的出台，CEO 和 CFO 将受到比以往任何时候更为严格的监督。即使是最具有职业操守、最小心谨慎的首席经理人，也需要采取额外的措施以记录恰当的合规行为，确保所有相关各方都能获得充分和独立的法律支持，并推行鼓励职业操守行为的企业文化。

SOX 要求，大多数的美国注册上市公司在 2004 年 12 月 31 日前必须符合 SOX404 的要求，而对于小公司和外国公司的最后期限是 2005 年 12 月 31 日。

可见，在美国上市的企业已经没有太多的选择，要么合规，要么只有退出市场（已有一些中小公司表示，会因为 SOX 实行后管理成本的提高而退出市场）。随着时间的推移，限期的逼近，原来一些采取“等等看”态度的企业也已经开始采取积极的态度来应对 SOX。

1.4 Sarbanes-Oxley 法案对遵从企业的要求

- 成立独立的合格的董事会审计委员会
- 由内部人士及时汇报公司的证券交易（2 天内）
- 全面记录内部控制/披露程序
- 具备遵从这些控制所需的审计能力
- 记录主要控制的设计方法
- 评估控制的设计和效力
- 识别随之而来的控制问题并监控相应的修复措施
- 记录流程和控制的变化；发现任何相关问题
- 记录控制设计效力测试的结果
- 披露任何主要缺陷
- 获取外部审计公司审核以证明相关报告

第二章 IT 工具在 SOX 遵从中的作用

2.1 总体作用

提供有效的辅助工具，使在美上市公司在萨奥法案遵从过程中更好地完成 404、409、802 部分的执行，达到法案对内部控制、报告、披露和归档等方面的要求，并以此为契机在长期战略上改进内部控制。

2.2 具体作用

为遵守 SOX 法案企业加大了 IT 投入。为了实现内控的实时性和有效性，IT 工具提供了有效的保障。要想跨越 SOX 法案这道坎，必须精心完善信息系统。

IT 工具在法案遵循过程中主要作用为两方面：透明性和问责制。

所谓透明性就是指 IT 工具提供了完善的文档管理系统，它可以在最短的时间内让有权限的用户看到制定的文档，其中包括企业的管理层、会计师事务所、审计委员会、投资人等，增加企业的透明度。

所谓问责制就是指 IT 工具制定了完善的权限管理系统，不同角色的人员只看到与自己本身相关的内容。在系统中所有人员的操作动作都被记录，每个人的职责被明确划分，每个人的工作被清晰记录。

那么 IT 工具做为法案遵从过程中有效的辅助工具，它具有以下优点：

- 紧密结合 404 法案要求，引导公司 404 项目组工作，涵盖文档记录、评估、改进、测试等阶段的工作
- 管理 404 项目文档，实现信息共享、更新和检索；文档存贮备份
- 对 404 项目进行有效的项目管理
- 满足公司基于 404 项目对各种报告的需求
- 建立有效的安全机制
- 系统扩展和升级
- 完善的权限管理

- 准确的审计跟踪
- 流程化的遵从活动

第三章 解决方案

3.1 慧点解决方案概述

慧点科技在对中国多家在美上市公司 SOX 遵从需求的理解基础上以及在对 IBM WBCR 产品充分了解的基础上，慧点科技推荐采用 IBM SOX 解决方案。

IBM 的新产品 IWBCR(IBM Workplace for Business Controls and Reporting)即为帮助企业满足 Sarbanes-Oxley 2002 法案而开发。该产品使企业能够以更一致、更系统的方式收集并监视控制信息，由此构成企业评估财务报告流程的基础。通过使用 IWBCR 产品，企业将能够更好地评估其内部控制表现，并有助于对财务报告活动建立透明的流程。它也使公共企业能够与审计员、审计委员会、分析家及投资人等财务报告链中的其他参与者共享信息。

此产品可用于帮助企业满足 SOX 第 404 部分的要求，并帮助企业通过定制来快速实施战略。

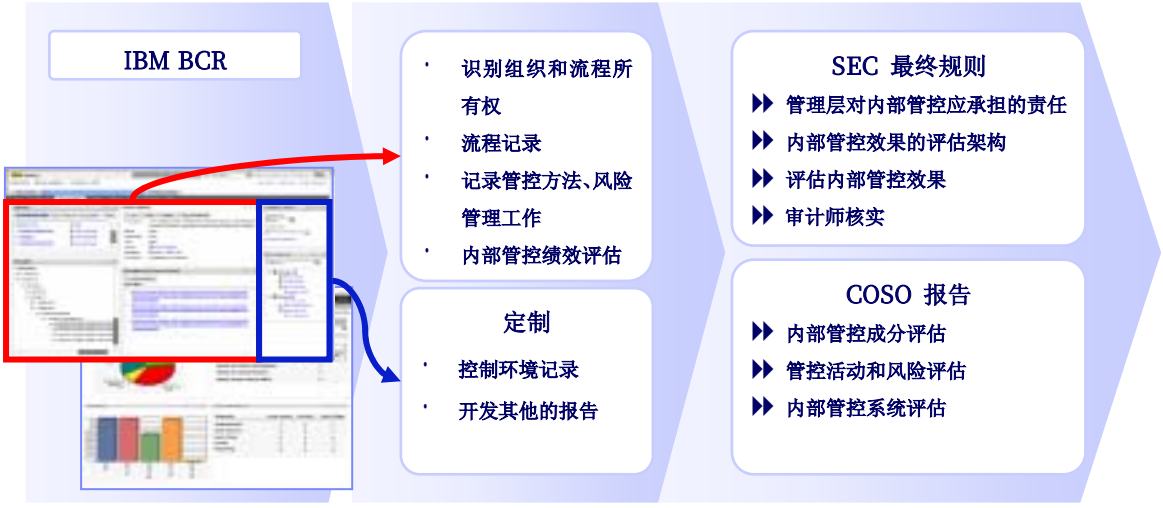

图 2 SOX 解决方案

3.2 IBM WBCR 对 SOX 法案遵从的响应

法案条款	法案要求	WBCR 响应
302	财务报告的季度证明	将财务报告作为控制实现控制管理
	内控效力的按季度披露	提供控制文档，测试和状态报告

404	内控效力和变更的年度证明	提供控制文档，测试和状态报告
409	重要事件的实时归档	提供内置的工作流电子表单
802	记录保持	提供实时归档和提取功能

表 1 IBM WBCR 对 SOX 法案的响应

3.3 IBM WBCR 对在美上市公司萨奥法案需求的响应

■ **紧密结合 404 法案要求，引导公司 404 项目组工作，涵盖文档记录、评估、改进、测试等阶段的工作**

- IBM WBCR 在业务工作流程上完全遵循 404 法案要求，涵盖了文档记录、评估、改进、测试等业务；
- 只要按照 WBCR 内定流程操作即可完成 404 法案要求的各阶段工作，快速实现 404 法案遵从。

■ **管理 404 项目文档，实现信息共享、更新和检索**

- DB2 数据仓库的海量存储
- 多角色跨部门跨流程的信息封装与共享的权限体系
- 在线协同
- 文档变更痕迹跟踪
- 文档变更的自动邮件通知
- 多层次文档检索

■ **对 404 项目进行有效的项目管理**

- 责任到人，分工明确
- 所有人与代理人多种控制方式
- 待办事件的自动提前提醒
- 存取自如的版本控制

- 从宏观到微观的多维监控体系

■ **满足公司基于 404 项目对各种报告的需求**

提供多达 30 余种的监控视图和报告

- 关键控制矩阵报告
- 无效关键控制报告
- 未测试控制报告
- 文档状态报告
- 所有者与委托人报告
- 执行视图
- 全部控制效力视图
- 控制状态报告
- 缓解控制报告
- 新增控制报告
- 删除控制报告
- 评估状态报告
- 评估状态详细信息报告
- 90 内到期关键控制报告
- 组织结构报告
- 链接矩阵报告
- 观察和建议报告
- 控制评估报告
- COSO 热图报告
- COSO 热图详细信息报告
- COSO 控制组件报告

- 用户管理报告

■ **建立有效的安全机制**

- 多角色多级别的权限控制体系
- 灵活易用的权限分配体系
- IBM Portal＋LDAP＋IBM Tivoli 的认证机制
- DB2 高安全高可靠性能

■ **系统扩展和升级**

- 易于应用集成的 Portal 门户
- 可扩展的 J2EE 架构
- 通用基础设施，易于辅助遵从多种法案

3.4 IBM WBCR 对 COSO 框架的支持

COSO	WBCR	备注
活动	流程	
	子流程	子流程与目标相对应
目标	目标	
风险	风险	
控制	控制	
	控制过程	在 COSO 中没有明确定义控制过程，控制过程是用来支持控制的测试的。

表 2 IBM WBCR 对 COSO 框架的支持

3.5 IBM WBCR 主要功能

IBM® Lotus® Workplace for Business Controls and Reporting 是端到端的解决方案，提供知识和信息管理以及门户和协作基础设施，帮您满足内部企业控制与报告的要求。 它可帮您：

- 允许高层管理人员察看公司内部企业控制的成效。
- 记录流程、识别风险和控制方法、并促进对控制效力的评估。
- 收集公司各级部门关于法案遵守问题的报告。
- 允许高级执行官员听取公司总结以及制度遵守情况的概述（高级官员通常与内部审计和控制小组一起制定规则和程序）。
- 推动外部审计公司审计贵公司控制程序的运行情况。

为了实现上述目标，该产品在一个集成的信息库中提供文件管理、协作、审计跟踪和归档等功能。

建立统一的遵从活动内容库为组织控制活动、分发信息、收集所需信息以帮助评估风险和监视内部控制系统奠定了基础。知识收集和报告功能可帮您快速发现内外部风险，以便及时做出明智决策。

该产品提供：

- **支持决策和披露活动**

  允许基于角色访问关键的财务指标，从而快速评估您的流程。

- **提供构成随需应变运行环境的信息**

  您可快速应答瞬息万变的需求，从而创建表现不凡的工作队伍。同时，这个解决方案还能帮您有效管理内容的协作创建、存储 、访问和分发等工作。强韧的文件管理功能能够为审计跟踪、访问控制和安全性等提供帮助。

- **帮助提高生产力**

  通过在适当时候提供适当信息（如关于标准运行程序的信息），您可提高整个公司的生产力。在线感知和在线交谈等功能可帮助改善交流并通过实时协作快速解决问题。

- **扩展 IT 环境的价值**

  Lotus Workplace for Business Controls and Reporting 构建在开放的 Java™ 2 企业版标准平台（J2EE™）基础上，使您能够实施模块化解决方

案，帮助扩展现有 IT 基础设施的价值。它同时还构建在业界领先的 Portal 和 Content Manager 软件基础上，可提供基础设施灵活性，同时提供全球最大的软件供应商之一，IBM 公司的全部优势和长期支持。

- **内部控制报告：详述**

该解决方案设计用于帮您定制公司的控制评估流程以满足特定需求，随后发送请求，要求向运行部门报告这些控制点。提供报告的每个部门都描述自己如何遵守（或不遵守）制度，并提交文件来支持这些声明。通过各部门提供的所有报告，您可洞悉整个公司对制度的遵守情况。通过相关的所有支持材料，审计人员或其他相关人员可以向高层管理人员揭示哪些地方有待改进，哪些地方已基本实现了控制目标。

以电子方式监督企业控制和报告流程优于传统的审计评估方法，是审计评估工作的一大步飞跃，可大大减少无效的信息报告，这也是新法律要求企业达到的主要目标之一。

Lotus Workplace for Business Controls and Reporting 使用基于角色的工作空间，可为控制并共享控制文件提供统一的信息库，如组织图、策略和标准运行程序等。

与内部控制活动相关的所有内容，以及描述政策、程序或制度遵守流程的文件，都可存储在 LWBCR 工具中，供内部员工、审计员、董事会及外部法律顾问等按需访问。您也可按事件生成报告，以便更轻松地评估控制活动的效力。

Lotus Workplace for Business Controls and Reporting 的强大功能可通过 IBM DB2® Records Manager 得到扩展，IBM DB2® Records Manager 基于由策略驱动的全面的维系规则（基于时间或事件），对内容和记录进行结构化保存和处理操作。此外，它还能传递依法中止的活动信息。

确保长期参加适当的培训和学习，是明确了解控制角色与职责的关键因素。IBM Lotus Learning Management System（LMS）可帮您确保员工能就最新的标准运行程序得到适当培训，并确保他们了解自己的角色（由此，

企业可以将人事调动对发案遵从工作的影响降至最低）。IBM LMS 是可扩展的灵活的教学管理解决方案，支持企业全面的培训活动、资源和课件。

IBM 业务伙伴同时创建了定制的和现成的内容，作为 IBM Ready For Program 项目的一部分支持 Sarbanes-Oxley 培训活动。

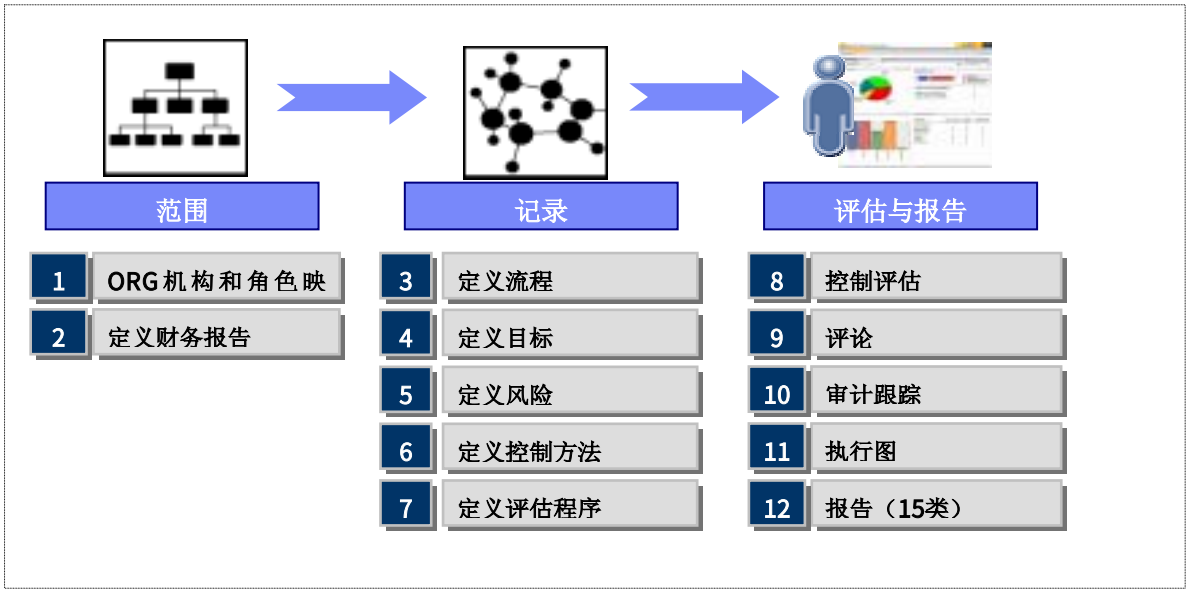

图 3 WBCR 主要功能

3.6 IBM WBCR 的主要特性

- 报告
  - 提供企业高层仪表版式视图，按角色提供广泛的“细分”说明
  - 30 个标准模板，包括 COSO 热图和链接图
  - 保留审计痕迹和归档
- 导航
  - 基于浏览器的轻松灵活的使用、导航界面
  - 能够根据组织要求调节界面外观
- 安全性
  - 电子签名

- 基于角色 – 根据授权指派相关人士负责控制工作

■ 可定制性及可扩展性

- 轻松添加新的制度遵从版本（Basel II、IAS 以及 CFO 法案等）
- 与现有基础设施集成
- 支持本机 Excel 电子数据表输入

■ 支持 Windows 和 AIX 平台

■ 提供 SOX 法案要求的归档功能

- 在年末归档数据；
- 提供复位标志以供审核

■ 审计痕迹保留/跟踪功能

- 跟踪变化以及变化的实施人信息

■ 与 Lotus Workplace Instant Messaging 集成(应用中的“Live names“功能)

- 用户可以随时知道另外用户的在线状态
- 可以与在线的人员进行即时交流

■ 是基于 web 的集成解决方案，面向控制管理与评估。

■ 邮件通知功能

- 业务信息变更将自动通知相关人
- 自动提醒评估人员执行评估

■ 支持多语言功能

- 包括韩国语、英语、中文、法语、日语、西班牙语和意大利语。

3.7 IBM WBCR 的优势

■ 透明性

- 提供企业级的信息汇聚
- 提供遵从状态的管理快照，以随时了解企业遵从状态

- 帮助了解相关的具体详情

■ 一致性和自动化

- 用户可以快速各自的相关任务，并可以随时延续之前的工作
- 流程可以与相应的财务报表相链接
- 可以定义控制，并可通过测试案例检查控制从而进行验证

■ 责任制

- 按流程定义主要角色和风险（CFO、业务部门负责人、流程负责人以及控制负责人等）
- 分配所有权，驱动实施责任制

■ 跨平台

- 支持 Windox 和 AIX 平台
- 支持 Win2000、win2003 和 AIX400 操作系统

■ 扩展性

- Portal 门户
- J2EE 架构

3.8 IBM WBCR 的工作流程

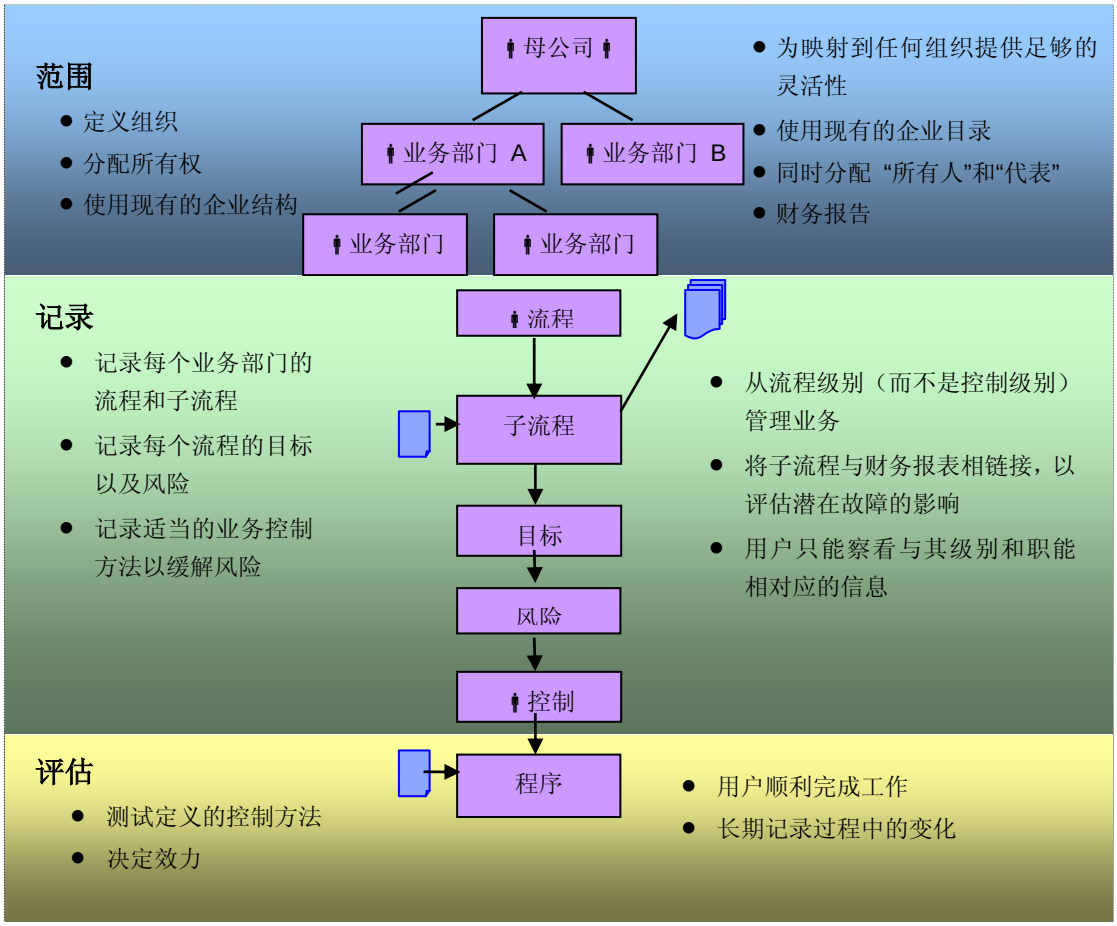

图 4 WBCR 的工作流程

3.9 WBCR 产品架构

- 平台
  - 可扩展的、支持安全接入的、基于标准的开放平台
  - 基于 WebSphere Portal 和 DB2 Content Manager（各自领域的领导者）
- 应用
  - 支持灵活的无限组织分级
  - 基于角色的访问、用户验证和应用安全性

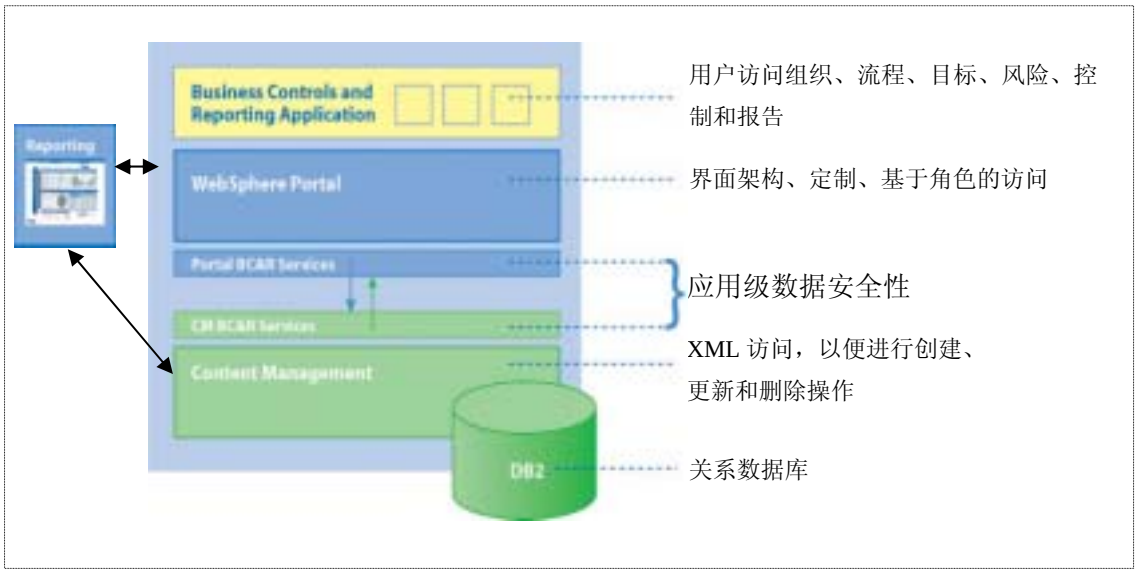

图 5 WBCR 产品架构

3.10 WBCR 业务架构

- 存储层：保存各种文档和数据，以及记录流程和控制的变化
- 应用层：记录并统计测试结果、生成报表、管理文档
- 业务流程层：定义业务流程、子流程、目标、风险、控制和过程
- 表示层：浏览文档、数据和报表，识别问题、披露缺陷
- 安全层：提供三级访问控制，确保业务和数据安全

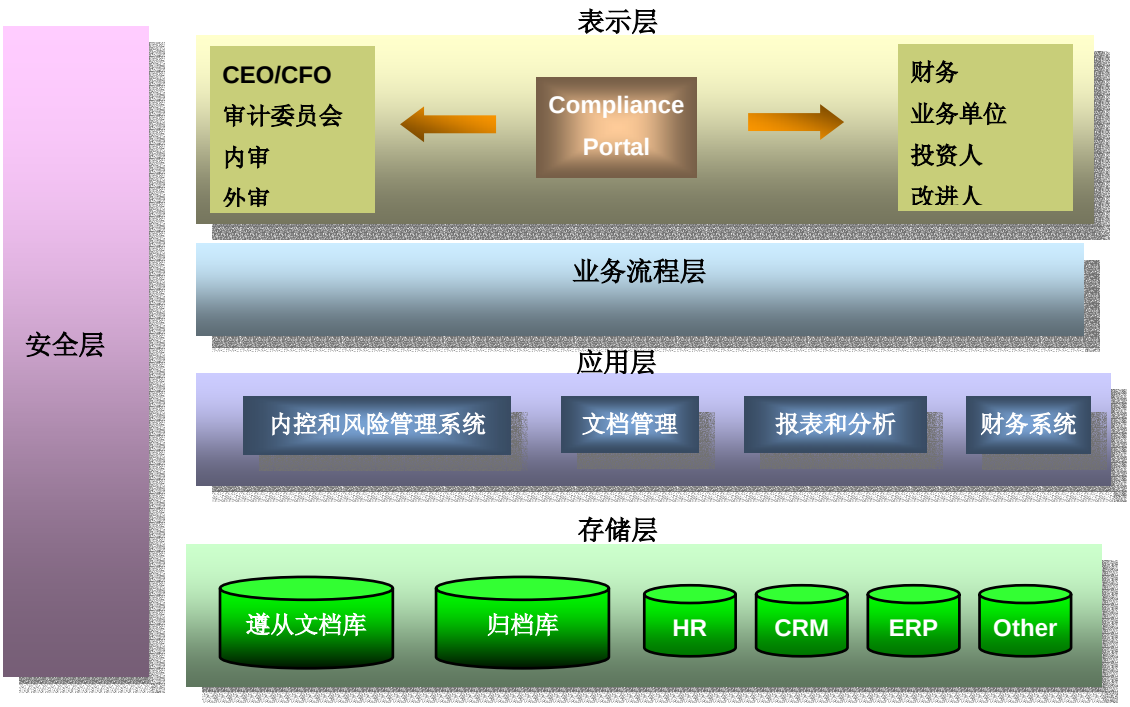

图 6 WBCR 业务架构

3.11 IBM Lotus 软件专业服务

IBM® Lotus® 软件专业服务在帮助企业利用现有的IBM Lotus软件投资驱动商业价值方面经验丰富，擅长为评估企业需求提供技术服务、培训和专业知识。并在评估组织需求以及帮助组织安装、集成和定制 IBM Lotus Workplace for Business Controls and Reporting 方面发挥领导作用。IBM Lotus 软件专业服务可指导客户部署工作，并与 WebSphere® Portal 和 DB2® Content Manager 领域的专家一起为解决方案提供关键的安装和配置服务。技术专家将与客户的管理和支持人员一起工作，向其传授技能并提供企业在部署 IBM Lotus Workplace for Business Controls and Reporting 时必须用到的专业技术知识（如架构规划、配置与测试等），从而帮助加速安装工作。

3.11.1 安装服务

这项服务旨在加速 IBM Lotus Workplace for Business Controls and Reporting 在客户位置的部署。Lotus 顾问小组将负责该产品所有组件的最初安装和配置工作。此外，Lotus 顾问还将与客户的管理和支持人员一起工作，向他们传授技能和知识，同时针对系统的快速启动和运行提供指导。

- 制定安装计划
- 设置用户帐号
- 安装 DB2 Server
- 安装 DB2 Client
- 安装 LDAP Server
- 安装并配置 WPS
- 设置 Portal
- 安装水晶报表服务

- 安装 WBCR2.5
- 知识传输

3.11.2 移植服务

这项服务旨在帮助加速传统数据到 IBM Lotus Workplace for Business Controls and Reporting 产品的移植。技能娴熟的 Lotus 顾问将对现有环境进行全面的最初评估。评估结果将帮助客户了解移植到 IBM Lotus Workplace for Business Controls and Reporting 产品的必要条件。

该解决方案聚焦了解客户的现有系统，并定义将财务报告数据从该系统移植到 IBM 产品需要完成的工作。目标是保持现有数据的完整性并能够在全新的 IBM 产品中提供此类数据。

这项服务的主要内容：

- 规划、开发并管理全面的移植方案，以便将现有的内控体系移植到 Lotus Workplace for business controls and Reporting 中
- 在移植前对您现有的环境进行最初评估
- 定义移植财务报告数据所需的步骤
- 帮助保持现有数据的完整性
- 在数据从现有的内控工具移植到 IBM 产品后，帮助确保数据的可用性

第四章 典型案例

4.1 美国亨廷顿国家银行

■ 客户：

亨廷顿国家银行是总价值 300 亿美元的地区银行股份公司，在美国设立有 300 多家办事处。

■ 商业需求：

- 管理财务报告的内部控制流程，以满足新法律的要求（SOX 404）
- 需要能够帮助简化银行内部控制和报告流程的解决方案

■ 解决方案

IBM Lotus Workplace for Business Controls and Reporting 软件基于开放标准，因此可轻松部署到银行现有的基础设施中。解决方案构建在亨廷顿国家银行技术战略的主要组件上 - IBM Lotus 软件套件 – 扩展了现有投资并反映了银行对长期需求（而不是一次性到位的解决方案）的关注。

IBM Lotus 软件服务部正在提供安装测试和生产环境、以及用户培训服务。IBM 业务伙伴 KPMG 为亨廷顿银行的执行官提供咨询服务，将自己的领域专长融入到该解决方案中。

■ 客户评价

“我们希望部署提供强韧功能的解决方案，并且该解决方案得到合法供应商的支持与增强，以便不断发展。选择 IBM 解决方案能使所有人安心。该产品功能丰富、价格合理，是真正的智能解决方案。"

--David Sewalk,亨廷顿国家银行商业解决方案开发部高级副总裁

4.2 美国 Ceres 集团公司

■ 客户

Ceres 集团公司通过其保险子公司，为个人、家庭、协会、中小企业以及

55 岁以上（含 55 岁）的美国人提供医疗和寿险服务。

■ 商业需求

为了遵从 Sarbanes-Oxley 法案的要求，Ceres 集团请求 IBM 提供软件解决方案，帮助他们监视并跟踪组织中的财务运行。

■ 解决方案：IBM Lotus Workplace for Business Controls and Reporting

IBM 提议的软件 /服务包，允许 Ceres 在不到两周时间内启动并运行业务控制和报告解决方案。

在 IBM 业务伙伴 KPMG 的帮助下，IBM Lotus 软件服务部 (ISSL) 开始实施并定制使用 IBM Lotus Workplace for Business Controls and Reporting 的解决方案。ISSL 在客户站点现场工作一周，以评估组织需求并帮助安装、集成和定制应用。

■ 客户评价

IBM 全面的软件和服务解决方案帮助 Ceres 集团发现了内外部部署风险，并及时做出了明智决策，以遵从联邦政府强制实施的 Sarbanes-Oxley 法案。

4.3 华能国际电力股份有限公司

■ 客户

华能国际电力股份有限公司在中国全国范围内开发、建设和经营管理大型火力发电厂，是中国最大的独立发电公司之一。

■ 商业需求

为了遵从 Sarbanes-Oxley 法案的要求，华能国际希望使用软件辅助快速实现 SOX 法案遵从。

■ 解决方案：IBM Lotus Workplace for Business Controls and Reporting

慧点科技提供的 WBCR 软件安装、配置和培训服务，允许华能国际在 2 个月内启动并运行业务控制和报告解决方案。