



# 萨班斯-奥克斯利法案指南： 信息技术风险及控制

常见问题解答

**protiviti**<sup>®</sup>  
Independent Risk Consulting

商业风险

技术风险

内部审计

# 全国Mini-MBA职业经理双证班



精品课程 权威双证 全国招生 请速充电

你可能准备跳槽或者求职, 却为缺少行业经验和专业证书而被用人单位百般挑惕!

你可能目前衣食无忧, 但随着年龄的增长和社会竞争压力的增大, 因为得不到专业的全新培训而失去竞争的机会和面临被淘汰的危机。

美华教育携手中国经济管理大学面向全国举办迷你 MBA 职业经理双证书班, 毕业颁发双证书。

## 招生专业及其颁发证书

认证项目	颁发双证	学费
全国《职业经理》MBA 高等教育双证书班	高级职业经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《人力资源总监》MBA 双证书班	高级人力资源总监职业经理资格证书+2 年制 MBA 高等教育研修证书	1280 元
全国《市场总监》MBA 高等教育双证书班	高级市场总监职业经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《酒店经理》MBA 高等教育双证班	高级酒店管理职业经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《营销经理》MBA 高等教育双证班	高级营销经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《企业培训师》MBA 高等教育双证班	企业培训师高级资格认证毕业证书+2 年制 MBA 高等教育研修证书	1280 元
全国《财务总监》MBA 高等教育双证班	高级财务总监职业经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《品质经理》MBA 高等教育双证班	高级品质管理职业经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《生产经理》MBA 高等教育双证班	高级生产管理职业经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《营销策划师》MBA 双证书班	高级营销策划师高级资格认证证书+2 年制 MBA 高等教育研修证书	1280 元
全国《物流经理》MBA 高等教育双证班	高级物流管理职业经理资格证书+2 年制 MBA 高等教育结业证书	1280 元
全国《项目经理》MBA 高等教育双证班	高级项目管理职业经理资格证书+2 年制 MBA 高等教育研修结业证书	1280 元
全国《企业总经理》MBA 高等教育双证班	全国企业总经理高级资格证书+2 年制 MBA 高等教育研修结业证书	1280 元



**【授课方式】** 全国招生、函授学习、权威双证

我校采用国际通用3结合的先进教育方式授课（远程函授+教学电子光盘自修+网络学院持续视频学习）



**【颁发证书】** 学员毕业后可以获取权威双证书与全套学员学籍档案

- 1、毕业后可以获取相应专业钢印《高级职业经理资格证书》;
- 2、毕业后可以获取2年制的《MBA研究生课程高等教育研修结业证书》;



## 【证书说明】

1. 证书加盖中国经济管理大学钢印和公章（学校官方网站电子注册查询、随证书带整套学籍档案）；
2. 毕业获取的证书与面授学员完全一致，无“函授”字样，与面授学员享有同等待遇，证书是学员求职、提干、晋级的有效证明；。



## 【学习期限】

3个月（允许有工作经验学员提前毕业，毕业获取证书后学校仍持续辅导2年）



## 【收费标准】

全部费用1280元（含教材光盘、认证辅导、注册证书、学籍注册等全部费用）

函授学习为你节省了大量的宝贵的学习时间以及昂贵的MBA导师的面授费用，是职业经理人首选的学习方式。



## 【招生对象】

- 1、对管理知识感兴趣，具有简单电脑操作能力（有2年以上相应工作经验者可以申请提前毕业）。
- 2、年龄在20—55岁之间的各界管理知识需求者均可报名学习。



## 【教程特点】

- 1、完全实战教材，注重企业实战管理方法与中国管理背景完美融合，关注学员实际执行能力的培养；
- 2、对学员采用1对1顾问式教学指导，确保学员顺利完成学业、胸有成竹的走向领导岗位；
- 3、互动学习（专家、顾问24小时接受在线咨询，第一时间回答学员的提问和咨询）



## 【考试说明】

1. 卷面考核：毕业试卷是一套完整的情景模拟试卷（与工作相关联的基础问卷）
2. 论文考核：毕业需要提交2000字的论文（学员不需要参加毕业论文答辩但论文中必修体现出5点独特的企业管理心得）
3. 综合心理测评等问卷。



## 【颁证单位】

中国经济管理大学经中华人民共和国香港特别行政区批准注册成立。目前中国经济管理大学课程涉及国际学位教育、国际职业教育等。学院教学方式灵活多样，注重人才的实际技能的培养，向学员传授先进的管理思想和实际工作技能，学院会永远遵循“科技兴国、严谨办学”的原则不断的向社会提供优秀的管理人才。



## 【承办单位】

美华管理人才学校是中国最早由教委批准成立的“工商管理MBA实战教育机构”之一，由资深MBA教育专家、教育协会常务理事徐传有教授担任学校理事长。迄今为止，已为社会培养各类“能力型”管理人才近10万余人，并为多家企业提供了整合策划和企业内训，连续13年被教委评选为《优秀成人教育学校》《甲级先进办学单位》。办学多年来，美华人独特的教学方法，先进的教学理念赢得了社会各界的高度赞誉和认可。



## 【咨询电话】

13684609885 0451--88723232 88342620

【咨询教师】王海涛 郑毅



## 【报名须知】

- 1、报名时请直接邮寄4张2寸免冠近照（要求蓝色背景）和一张身份证复印件
- 2、报名登记表格下载后详细填写并发送邮件至 [xchy007@163.com](mailto:xchy007@163.com) 或者传真至0451—88342620
- 3、交费后及时电话通知招生办确认，以便于收费当日学校为你办理教材邮寄等入学手续。



## 【报名地址】

哈尔滨市道外区南马路 120 号职工大学 109 室美华教育（ 邮政编码：150020）



## 【证书样本】(全国招生 函授学习 权威双证 请速充电)

(高级职业经理资格证书样本)

(两年制研究生课程高等教育结业证书样本)



## 【学费缴纳方式】

方式一	邮局邮寄	邮寄地址：哈尔滨市道外区南马路 120 号职工大学 109 室 邮政编码：150020
方式二	学校帐号	学校帐号：184080723702015 开户银行：哈尔滨银行龙江支行 企业户名：哈尔滨市道外区美华管理人才学校
方式三	交通银行 (太平洋卡)	帐号：40551220360141505 户名：王海涛 开户行：交通银行哈尔滨分行信用卡中心
方式四	邮政储蓄 (存折)	帐号：602610301201201234 户名：王海涛 开户行：哈尔滨道外储蓄中心
方式五	中国工商银行 (存折)	帐号：3500016701101298023 户名：王海涛 开户行：哈尔滨市道外区靖宇支行

可以选择任意一种方式缴纳学费，建议使用第五种方式（中国工商银行，比较方便快捷）收到学费的当天，学校就会用邮政特快的方式为你邮寄教材和考试问卷。

# 全国职业经理MBA双证班

## 精品课程 火热招生

函授学习 权威双证 全国招生 请速充电

**认证系列：**高级职业经理资格认证、人力资源总监、营销经理、财务总监、企业培训师、酒店经理、品质经理、生产经理、物流经理、项目经理、市场总监、营销策划师等学习认证系列。

**颁发双证：**通用高级经理资格证书 + MBA 高等教育研修结业证书 (含 2 年全套学籍档案)

**证书说明：**证书全国通用、国际互认、电子注册，是提干、求职、晋级、移民的有效依据

1280

元

**学习期限：**3 个月 (允许工作经验丰富学员提前毕业) **收费标准：**全部学费

**咨询电话：**13684609885    0451- 88723232    88342620    **邮箱：**xchy007@163.com

**学校网站：**[www.mhjj.net](http://www.mhjj.net)    **颁证单位：**中国经济管理大学    **承办单位：**美华管理人才学校

## 全国招生   函授教育   颁发双证   权威有效



# 目录

页码

简介.....	1
---------	---

## 遵守萨班斯法案时的整体IT风险及控制方法及应考虑的问题

1. 在考虑IT风险及控制时，是否存在一种可以采用的整体方法？ .....	2
2. 在进行财务报告内部控制的评估时考虑IT部份为何如此重要？ .....	4
3. 是否可以只是完全依赖人工控制，而毋须考虑对IT风险及控制进行评估的需要？ .....	4
4. 404条款合规小组应如何定义“IT风险及控制”？ .....	5
5. 管理层如何识别IT风险及对IT风险进行优先排序？ .....	6
6. COSO（反虚假财务报告委员会成立的赞助组织委员会）就IT控制提供了何种指引？ .....	6
7. ISACA（国际信息系统审计协会）的CobiT（信息及相关技术控制目标）框架就IT控制提供了何种指引？ .....	6
8. COSO和CobiT如何使404条规的合规项目事半功倍？ .....	7
9. 如果404项目只能严格遵守CobiT，其能否符合404条规合规项目？ .....	7
10. 管理层是否应考虑其他IT控制指引和标准，例如信息安全管理标准号ISO/IEC17799、ITIL（信息技术基础设施库）和CMM（能力成熟程度模型）？ .....	8
11. 整体来说，进行IT控制评估时，有什么重要方面必须考虑？ .....	8

## 与业务流程控制有关的IT控制考虑

12. 管理层如何依照问题1中所述的方法开始评估工作？ .....	9
13. 在进行整体404条款项目时，什么时候应对IT控制予以考虑？ .....	10
14. ERP（企业资源计划系统）如何影响IT评估？ .....	10
15. 共享服务中心如何影响内部控制的评估？ .....	10
16. IT活动的外包如何影响公司控制的评估方法？ .....	11

## 公司层面考虑

17. 什么是IT组织？ .....	13
18. 管理层如何考虑公司层面上有关IT风险及控制的问题？ .....	13
19. 是否存在仅仅包括IT操作或流程的独立“实体”？ .....	14
20. 就遵守萨班斯法案404条款及302条款而言，应考虑哪些IT治理问题？ .....	14
21. 若管理层对公司层面的IT相关项目有较强的控制，会有什么不同的结果？ .....	14

# 目录

## 页码

22. 管理层如何了解公司层面的控制是否提供了一个较强的控制环境？ .....	14
23. 若管理层对公司层面的控制较弱，会有什么不同的结果？ .....	14
24. 较弱的公司控制环境有什么例子？ .....	15

## 活动 / 流程层面考虑 — 基础设施控制问题

25. 何谓“IT 控制”？ .....	15
26. 哪类的控制属于“IT 控制”？ .....	15
27. 对安全管理进行评估时，404条款合规项目小组所关注的是什么？ .....	16
28. 对应用系统变更控制进行评估时，404条款合规项目小组所关注的是什么？ .....	17
29. 对数据管理和灾难恢复进行评估时，404条款合规项目小组所关注的是什么？ .....	18
30. 对数据中心的操作和问题管理进行评估时，404条款合规项目小组所关注的是 什么？ .....	19
31. 对资产管理进行评估时，404条款合规项目小组所关注的是什么？ .....	20

## 活动 / 流程层面的考虑 — 应用系统和数据负责人的角色

32. 谁是应用系统和数据负责人？ .....	22
33. 就IT组织而言，应用系统和数据负责人承担什么角色和责任？ .....	22
34. 应用系统和数据负责人应制定什么流程以协助遵守404和302条款？ .....	22
35. 要建立合适的安全管理和职责分离，需要制定什么流程？ .....	22
36. 就存取关键及 / 或敏感交易和数据的定期审核和审批而言，需要制定什么流程？ .....	23
37. 就业务影响分析和业务持续运作计划而言，需要制定什么流程？ .....	23
38. 在对生产应用系统作出变更之前，就建立、测试和审批有关应用系统变更而进 行的管理而言，从内部控制的角度看，应制定什么流程？ .....	24
39. 如果应用系统和数据负责人流程控制的设计和运作有效，对财务报告内部控制 的评估有什么影响？ .....	24
40. 如果应用系统和数据负责人流程控制的设计和运作没有成效，对财务报告内部 控制的评估有什么影响？ .....	24

## 活动 / 流程层面的考虑 — 应用系统层面的控制

41. 应用层面的控制考虑有哪些？ .....	25
42. 404条款合规项目小组如何决定每个主要业务流程的关键应用系统？ .....	25
43. 404条款合规项目小组如何在活动 / 流程层面上，将应用系统层面的控制考虑 纳入业务流程控制？ .....	26

# 目录

## 页码

44. 如果404条款合规项目小组发现业务流程层面有较强的应用系统控制，管理层应采取什么措施？ .....	26
45. 如果404条款合规项目小组发现应用系统层面有较弱的IT流程控制，管理层应采取什么措施？ .....	26
46. 就用户在财务报告流程中所采用的并不受限于ITGC环境的电子数据表和其他技术工具而言，管理层如何对这些工具的控制进行评估？ .....	26

## 文档记录

47. IT组织及应用系统和数据负责人应进行多少文档记录，以为应用系统的控制和运行提供证据？ .....	27
48. 404条款合规项目小组应如何记录公司层面的IT控制？ .....	27
49. 404条款合规项目小组应如何为活动 / 流程层面上的ITGC进行IT控制的文档记录？ .....	28
50. 404条款合规项目小组应如何为应用系统和数据负责人所操控的流程及具体应用系统领域，进行IT控制的文档记录？ .....	28
51. PCAOB最近颁布的披露草案着重强调了交易的“建立、记录、处理和报告”，有鉴于此，对交易流程进行文档记录的最佳方式是什么？ .....	28

## 测试

52. 如何进行IT控制的测试？ .....	28
------------------------	----

## 处理缺陷及报告

53. 管理层如何解决IT控制的缺陷和差距？ .....	29
54. 在鉴证程序中，外部审计师如何看待IT控制？ .....	29

关于甫瀚 .....	30
------------	----

词汇表 .....	33
-----------	----



## 简介

甫瀚于2003年7月刊发了广受欢迎的《萨班斯—奥克斯利法案指南：内部控制报告要求》第二版。该书旨在解答关于萨班斯—奥克斯利法案第404条款（以下简称“SOA”或“萨班斯法案”）的常见问题，并根据美国证券交易委员会颁布的最终规则进行了修订。404条款规定管理层须在年度报告中提交一份内部控制报告。该内部控制报告必须清楚地说明管理层有建立及维持充分的财务报告内部控制的责任，以及管理层须于年末就该等内部控制的成效作出评估。同时，该报告亦须指出公司所聘请的独立执业会计师已就管理层的财务报告内控评估进行鉴证，并已提交报告。

《萨班斯—奥克斯利法案指南：信息技术风险及控制》与甫瀚的404条款指南同步出版。在阅读本指南之前，读者应该已对404条款及内部控制评估和报告的基本要求有所认识。有关该要求的详情已载于甫瀚的《萨班斯—奥克斯利法案指南：内部控制报告要求》一书中。本公司的第十期通讯「技术风险及控制：你需要了解什么？」概括了本文中的观点，以供404条款项目发起人及其他有兴趣人士（包括最高级行政人员和董事）参阅。

本书为404条款的合规项目小组提供指南，指导组织应如何考虑公司层面及业务流程/操作层面上的信息技术风险及控制。本书中的问题及相关解答集中讨论信息技术组织与公司的应用系统及数据负责人之间应如何进行沟通，并就ITGC（基础设施控制）所产生的影响进行解释，以及讨论应如何考虑流程层面上的ITGC。本书亦探讨关于应用控制评估如何与业务流程控制评估互相协调，并讨论有关记录、测试及缺陷弥补等事项。

本书所列的问题都是我们在与客户及其他有关人员的交流中发现的一些问题。我们根据我们以往的经验对这些问题提供解答及意见，希望能够对公司记录、评估及改善财务报告内部控制有所帮助，并进一步完善管理层的评证工作。

本书并非拟就遵守萨班斯法案要求的合适方法作法律分析。公司应根据其具体情况就具体问题寻求律师和风险顾问的意见。公司的方针可能会受到PCAOB（上市公司会计监管委员会）即将颁布的鉴证准则影响。因此，本书所涉及的某些问题将会继续有所发展。

甫瀚

2006年6月



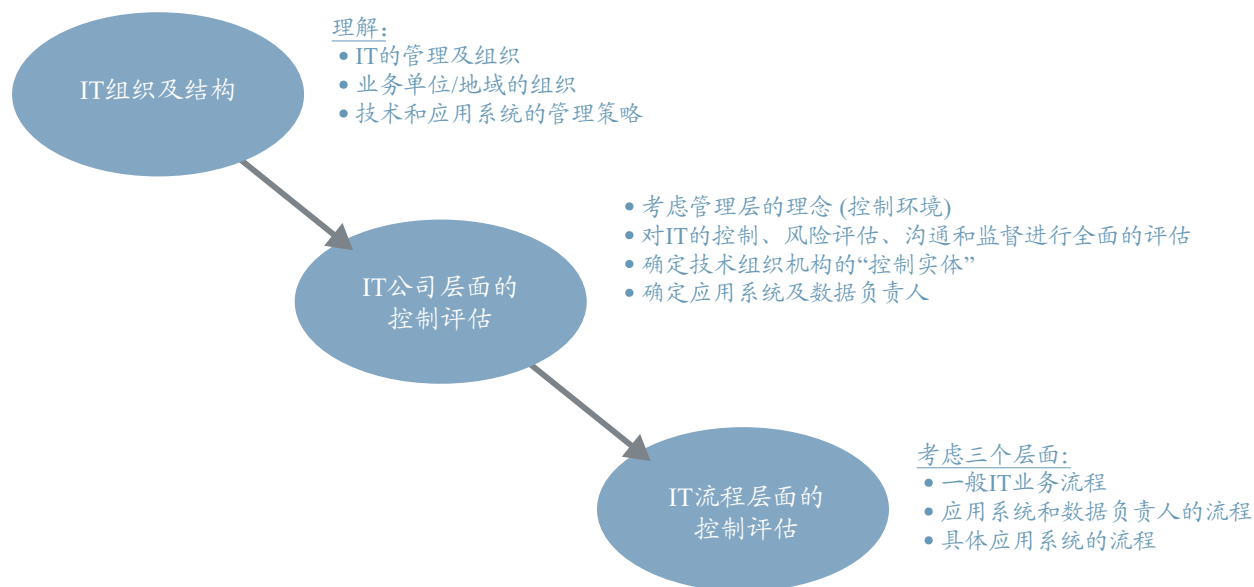
## 遵守萨班斯法案时的整体IT风险及控制方法及应考虑的问题

在进行财务报告内部控制的评估时，应谨慎考虑信息技术(IT)所产生的影响。其中包括一些IT独有的风险。我们就下列问题作出的回应，涵盖了一些整体的考虑因素，包括评估内部控制时，考虑信息技术的重要性、如何定义及识别“IT风险及控制”及利用有关框架协助IT风险及控制的评估。第404条款的合规小组在规划及组织项目时，应及早考虑这些因素。

### 1. 在考虑IT风险及控制时，是否存在一种可以采用的整体方法？

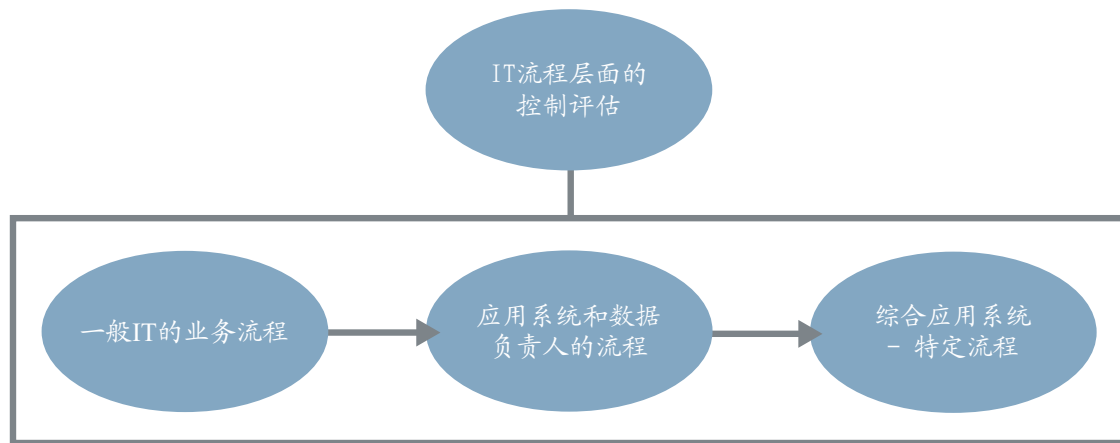
很明显，答案是“有”。有关我们建议方法的基本原理、主要词汇的定义，以及每一种要素，都会在本文的后面部份予以详细阐述。然而，我们首先提出该方法的大纲，以列示IT风险及控制评估的依据及“结局”。

下图简单描述了该整体方法：



IT评估方法应按上图所列顺序进行，原因是每一个步骤都会影响范围的界定，有时候还会影响下一步要进行的工作的性质。第一步是理解“IT组织和结构”，这一步为IT公司层面的控制评估奠定了基础。其后，公司层面控制的强弱又会影响对IT业务流程从三个层面进行控制评估的性质和程度。

对IT流程层面控制的评估是迄今为止404条款合规项目中最耗时费力的一项工作。对IT流程层面的评估要从三个不同层面予以考虑。



这三个流程应按所列顺序进行评估。下面是对每个层面简要的讨论：

### 一般IT的业务流程

IT基础设施控制的审核是针对公司的主要IT流程，或是支持财务报告的关键IT应用系统。敬请留意在若干情况下，404条款合规项目小组可能需要对同一个基础设施控制进行不止一次的审核。例如，如果多个流程同时影响每个重要财务报告领域，而该等流程又不是受限于相似的政策、流程活动和控制程序，那么该等流程则可能需要被分别予以审核。

几乎在所有情况下均应予以评估的一般IT流程包括：

- 安全管理
- 应用系统/系统变更管理
- 数据管理与灾难恢复
- 数据中心的操作及问题管理
- 资产管理

### 应用系统和数据负责人流程

这方面被评估的是那些直接被应用系统和数据负责人控制和管理的程序。我们认为，本项目阶段在所有情况下均应予以评估的流程包括：

- 建立和维持不兼容职责的分离（安全角色和管理）
- 确认/审核对关键交易和数据的存取
- 开发和维护业务影响分析/业务持续计划
- 制定和维护业务负责人变更控制

## 综合应用系统 - 特定流程

对业务流程层面的所有IT控制和人工控制进行综合评估是必须的。评估中有关IT的部份主要集中在对关键应用系统的控制。在对企业业务流程进行评估时亦应评估相关的IT风险和控制，从而对控制环境有全面了解。

负责人应对每个重要业务流程中关键财务应用系统的控制有充分的了解：

- 应用系统的程序化控制
- 关键交易和数据的信息获取控制
- 数据验证/错误检查程序
- 错误报告
- 复杂运算
- 报告的可靠性和准确性
- 关键接口

上述各方面会在以后部份有更详尽的讨论。

### 2. 在进行财务报告内部控制的评估时考虑IT部份为何如此重要？

业务流程对技术的依赖程度逐年增加，使得业务的执行更加及时、全面及准确。财务报告流程及其他流程，即财务报告所载之交易的获取、记录、累积、总结及呈报，均需依靠计算机、程序及其他技术性的工具和软件来完成。大部份企业（若非全部）都是如此。因此，应用系统和系统的控制成效会直接影响流程的完整性，包括输入流程的数据和流程完成时最终呈报的信息（即输出资料）。

应用系统和系统已有自己的控制程序。在这些程序化的控制中，有些可能是财务报告内部控制的关键。若这些程序化的控制有关键作用，在进行评估时必须予以考虑，特别是在流程结果没有经过验证或验证不足的情况下，管理层仍然依赖这些控制。

IT风险只在IT环境中存在。由于经常会有不同员工及供应商负责开发、维持及接触到技术环境中的硬件、软件及其他部份，这些人士行动若未经授权，会直接影响流程和数据的可靠性。因此，由技术衍生的相关风险必须在评估与财务报告相关的内控风险时予以考虑。这些风险是在技术的应用自身潜在的。例如，在未经授权下获取信息和数据、不准确的运算和程序，以及未经授权而更改或损害程序，均会使程序发生错误或导致程序不完整。负责人在审核内部控制的结构时必须注意和考虑这些风险。

简而言之，在当今高度计算机化的商业环境中，（根据萨班斯法案第404条款的规定）在进行财务报告内部控制的整体评估时，必须考虑有关IT的风险和控制。

### 3. 是否可以只是完全依赖人工控制，而毋须考虑对IT风险及控制进行评估的需要？

否，只要公司有任何的会计系统，这都是不可能的。除非其会计系统非常简单，主要是用作编辑，而且数据容易被系统用户验证。PCAOB 于2003年10月颁布了建议审计准则，当中涉及不少有关IT系统和IT环境的具体项目。于本书付印时，PCAOB 的颁布尚在建议阶段，但基于IT在现今商业和内部控制环境中的重要性，我们认为PCAOB对有关IT事宜的立场不会有任何实质的改变。例如，PCAOB提供了一连串的程序，让审计师可以遵循

这些程序对财务报告内部控制有所了解。其中的一项程序是“透过与财务报告有关的信息系统追踪交易数据”，了解特定控制的设计。PCAOB亦在别处指出，审计师必须“了解交易流程，包括如何建立、记录、进行和呈报交易。”这里的基本前提是信息系统在财务报告过程中占据重要位置；因此，在公司审计师开始审计程序之前，管理层必须对影响财务报告的应用系统、相关的风险及有助降低这些风险的控制有充分了解。

就识别有关的财务报告认定而言，PCAOB认为要确定一项认定是否有关，取决于很多因素。PCAOB例举的其中一个因素是“系统的性质和复杂性，包括公司在处理用作支持认定的控制信息时所使用的信息技术”。PCAOB亦指出，在进行期末财务报告流程的评估时，审计师必须考虑“期末财务报告中每一个元素所涉及信息技术的范围”。最后，PCAOB亦要求审计师就重要流程进行穿行测试。关于这一点，“审计师需透过公司的信息系统，由源头开始追踪所有种类的交易和事件……务求这些信息均能于财务报告中反映出来。”PCAOB进一步规定穿行测试“应包含建立、记录、处理和呈报个别交易的完整流程。”

鉴于PCAOB多次提及应用系统和相关的IT控制，因此毫无疑问，PCAOB视IT和有关IT的控制为进行财务报告内部控制评估的重要方面。显而易见，审计师势必关注信息技术。在现今大部份(若非全部)的业务上，有关IT的控制不能被忽视，也不能只给予草率考虑。

有些人或许会争辩，认为若IT控制强差人意，便没必要对其进行记录和评估。但我们认为，即使IT控制的情况未如理想，仍然应该对它们进行评估。若404条款合规小组了解IT控制的弱点所在，那么对于那些可能存在的不合规问题，他们能够更有效地识别其性质和范围。这种风险评估有助项目小组对适当的补偿控制进行评估，并在必要时对额外的控制进行评估，从而在从最可能发生错误的源头来发现和纠正有关的具体错误。

#### 4. 404条款合规小组应如何定义“IT风险及控制”？

404条款合规项目小组应考虑的风险及控制包括(i)因技术(例如应用系统中的程序化控制)而存在的风险及控制，或(ii)影响相关程序或数据完整性的风险及控制。此外，就404条款合规工作而应予以考虑的IT风险及控制，只限于那些与实现财务报告可靠性该内部控制目标有关的风险及控制。

为方便讨论，在本书中，“IT风险及控制”主要涉及两个大的领域-基础设施控制(ITGC)和应用系统控制(ITAC)。

**ITGC**通常会影响到技术环境内众多单一的应用系统及信息。一般来说，由于这些控制会影响相关程序和数据的可靠性，所以最终会影响财务报表认定的实现。换句话说，控制能防范或预防某些会影响相关程序和数据可靠性的事件发生。(本书稍后会进一步讨论有关影响。)





ITAC方面，有以下两个重要领域：

- a) 由相关的应用系统和数据负责人设计，并实施业务中的控制及流程
- b) 应用系统中的程序化控制，负责执行控制有关的特定活动，例如在输入过程中，对主要栏目中的被输入的数据进行错误检查或验证

其中一个应用系统控制的例子是不兼容职责的分离。数据负责人需负责设计及合理地判断哪些责任和职责应被分离。程序编制小组在负责设计和开发应用系统，使交易能够按照系统负责人的设计旨意，在程序化和其他形式的控制下完成，为达到财务报告认定提供一定的保障。

## 5. 管理层如何识别IT风险及对IT风险进行优先排序？

IT风险的识别和优先排序的框架和方法与跟那些影响财务报告要素的关键流程的风险的识别是相同的。一般来说，风险的识别是基于其与具体财务报表认定的相关性而进行的，而有关风险的识别是对内部控制环境作出概括性结论的基础。风险的优先排序是根据他们对财务报表的影响的大小和发生的可能性而进行。

使用相同的整体框架和方法是处理IT风险的一个优秀策略。不论影响财务报告内部控制的风险性质如何，财务报表的认定始终不变。这些认定通常包括授权、完整性和准确性、以及资产存取的共有目标。针对IT而制定的控制目标，包括程序和数据的可靠性（以实现财务报告的完整性和准确性、一致性、和及时性这些目标），以及（有助实现授权目标和资产存取目标的）数据程序和具体交易的正确存取有关。认识这些技术领域如何直接或间接影响（或有可能影响）财务报告认定的实现，将有助于集中对基础设施控制和应用过程控制领域中的风险和控制进行评估。

## 6. COSO（反虚假财务报告委员会成立的赞助组织委员会）就IT控制提供了何种指引？

COSO内部控制的综合框架有关IT控制的论述依据与其他人工控制的论述依据一样。论述依据包括内部控制的五个组成部份，这五个组成部份必须存在于组织的公司层面和活动层面，以实现管理层的目标。在404条款的合规工作中，管理层的目标是可靠的财务报告。这五个组成部份包括控制环境、风险评估、控制活动、信息与沟通及监督。当进行公司层面和活动层面的IT控制成效评估时，这五个组成部份是其考虑的准则。

（内部控制的综合框架中的IT控制会在“控制活动”和“信息与沟通”部份作具体讨论。）

## 7. ISACA（国际信息系统审计协会）的CobiT（信息及相关技术控制目标）框架就IT控制提供了何种指引？

现有若干框架是专为与IT有关的控制而设计的。由IT治理中心及ISACA所制定的CobiT框架，是众所周知的框架之一。CobiT是一个提供治理（公司层面）及详细（活动层面）目标的IT治理框架。该框架亦就IT环境向有关人士提供一个全面的概览和概括性的了解。因此，它可作为一种参考，也可被视作IT风险及控制工作的一部份。

CobiT框架是由占“基础设施控制”范围其中一大部份的 IT流程组成，提供控制目标、风险和范例控制。在404条款合规项目中应用该框架（或其他框架）时，应特别专注于财务报告内部控制目标的实现。换句话说，404条款的合规方法的主要关注点在于如何达到使财务报告过程具有自身存在的、内在的可靠性。

CobiT的建立旨在用于实现更广泛的COSO整体内控目标。如404条款合规项目小组决定采用CobiT框架，他们应具体考虑公司的IT组织结构，以便CobiT的目标能够与公司的IT组织及结构相一致。此外，CobiT的目标与财务报告认定之间必须建立联系。公司应将CobiT与财务报告的认定相结合，建立相对应的关系。在此基础上，财务报告过程中的风险和CobiT目标的实现就会甚有显而易见的联系了。

2003年10月，ISACA和IT治理中心出版了一白皮书“萨班斯-奥克斯利法案的IT控制目标—IT在披露及财务报告的内控设计、实施和持续性中的重要性。”在白皮书中，ISACA和IT治理中心试图将CobiT框架及目标应用在萨班斯法案的财务报告目标上。此白皮书概括地讨论了IT控制，并列出与萨班斯法案合规有关的控制目标。此文件所描述之控制目标对审计著作有重大贡献，原因是它们把更广泛的CobiT框架整体控制目标，集中在与404条款合规有关的目标上。但此白皮书指出，“一刀切式的方法并不是可行的方法。每一个组织均应该按其具体情况度身订造合适的方法。”我们相信这确实是一个适当的做法，每间公司均须按其特定的组织结构、流程和风险度身订造其合规的方法。”

## 8. COSO和CobiT如何使404条款的合规项目事半功倍？

鉴于404条款的规定，COSO提供了一个有助实现有效的财务报告内部控制的整体框架。CobiT框架围绕IT控制环境的若干方面提供概括性的指引，以实现涵盖更广泛的内部控制。在执行404条款合规项目时，必须对COSO予以考虑，因为证交会在404条款的最终规定中特别提到这框架。CobiT亦提供了有用的指引和背景资料，在执行404条款合规项目时可予以考虑。

## 9. 如果404项目只能严格遵守CobiT，其能否符合404条款合规项目？

我们在问题7中已经讨论过，CobiT是一个全面的控制框架，其所考虑的不仅仅是有关财务报告内部控制目标的实现。如果使用CobiT，那么有关技术控制的记录文件将远远多于与404条款合规项目有关的记录。若要进行完整的CobiT记录，则需要开展筛选对应及联系工作，以确定管理层必须依赖的财务报告控制。在制定决定运行成效的测试计划时，这些工作也是不可缺少的。合规小组亦需关注问题41-46所提及的，与具体应用系统有关的应用系统层面控制，以达到全面合规的404项目要求。

我们在问题7中已讨论过，若要采用IT治理中心新出版刊物中所推举的方法，就必须根据（a）具体的组织，（b）对财务报告信息及披露的可靠性有重大影响的具体应用系统，以及（c）用以支持与IT相关的应用系统及数据负责人流程，而度身订造。

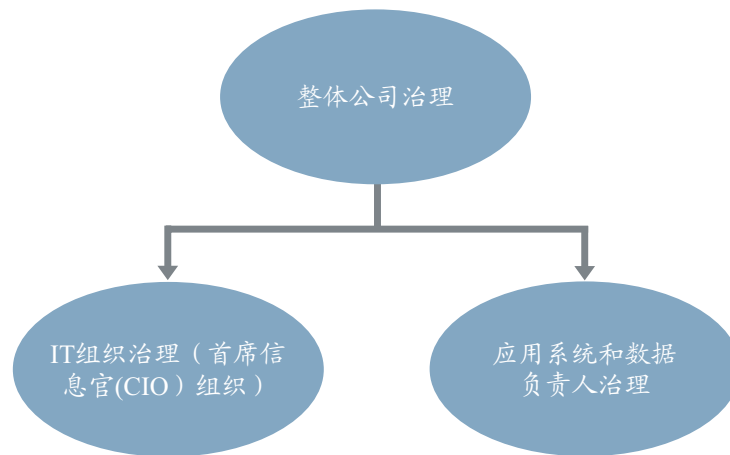
**10. 管理层是否应考虑其他IT控制指引和标准，例如信息安全管理标准号ISO/IEC 17799、ITIL（信息技术基础设施库）和 CMM（能力成熟程度模型）？**

除CobiT外，还有许多其他框架和材料，可以就IT领域的风险及控制提供指引。每一框架均提供具体指引，致力协助机构“改善”他们的IT操作和流程。此外，每一框架亦提供一些极好的范例，说明应怎样组织流程，以及展示IT组织的设计及操作流程的最佳作业。如果公司的IT组织已经采用一种或多种框架对操作进行记录，那么以该等框架为基础展开与404条款合规有关的工作，也是合情合理的。然而，对风险及控制的评估，还是要依据问题4所阐述的财务报告内控目标或认定而进行。

**11. 整体来说，进行IT控制评估时，有什么重要方面必须考虑？**

正如整体控制领域一样，IT领域也以公司治理和IT治理作为起步点。首先是整体公司治理，这是由首席执行官、董事会和行政人员的言行决定的“管理高层的态度”。

IT治理方面，有两个方面必须关注，原因是它们均会影响IT控制评估在财务报告内部控制中产生的作用。请参考下图：



IT组织包含IT运作和对IT有影响的流程的整体治理。IT一般由CIO组织构成，对一般或总体控制的成效产生影响。（IT组织和ITGC所产生的影响将于问题17-31再作讨论。）

应用系统和数据负责人是与业务流程负责人有联系的业务小组。应用系统和数据流程控制的成效，会对活动或流程层面控制的成效产生重大影响。（应用系统和数据流程控制所产生的影响将于问题32-40再作讨论。）

## 与业务流程控制有关的IT控制考虑

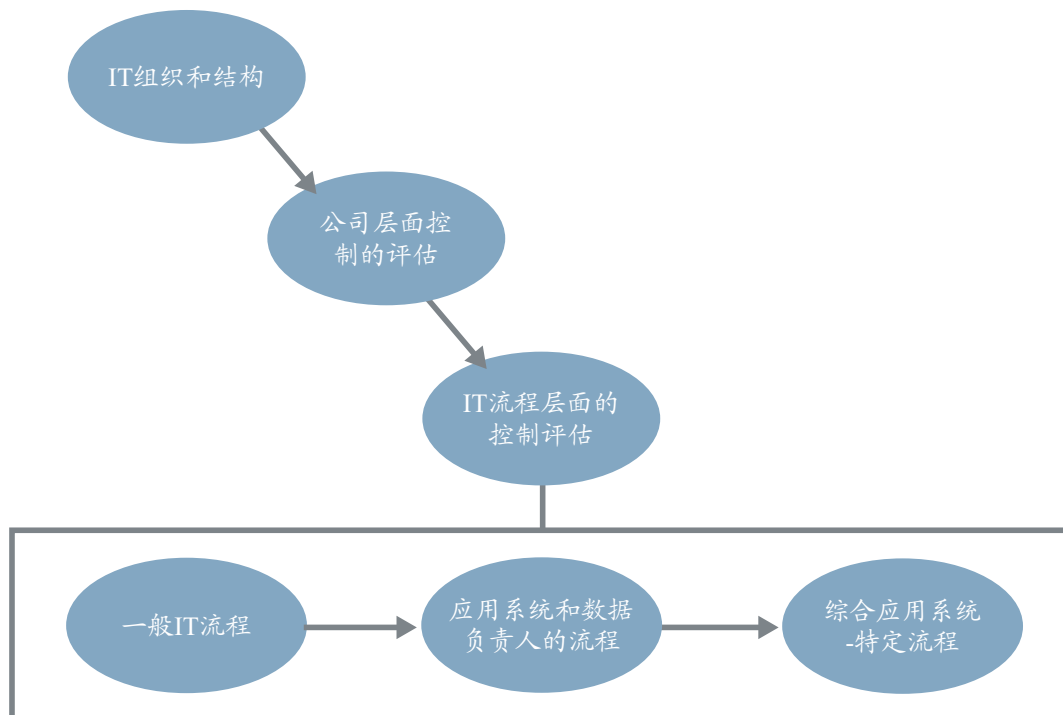
现今的技术已经与业务流程不可分割，因此，在进行流程或活动层面的控制评估时，必须考虑具体的技术控制，即在设计用于支持流程的应用系统时被纳入在内的控制。在许多情况下，活动/流程层面在很大程度上依赖这些控制以降低风险，以及实现与财务报告内部控制有关的相关目标。

我们就这部份的问题所作的回复，旨在协助404条款合规小组将IT内控的考虑纳入财务报告内部控制的评估之中。最终，这个纳入程序亦必然在流程层面发生。本部份的问题解答将包括从对IT风险及控制的评估入手，在那个项目的时间段来考虑IT控制，ERP（企业资源计划系统）对IT控制的评估的影响，共享服务中心对内控评估的影响，以及IT活动的外包对评估的影响。

### 12. 管理层如何依照问题1中所述的方法开始评估工作？

问题1所述的方法为管理层提供了综合框架，以便展开IT风险及控制的评估。该方法是以管理层对财务报告要素和与这些要素有直接关联的重要业务流程所作的综合识别和优先排序为基础。有关的识别和优先排序流程是404条款合规项目中不可或缺的一部份，并且是考虑IT风险及控制的一个合理起点。基于这点，问题1所述的建议方法，是展开IT风险及控制考虑的可行方法。项目小组应考虑的前提是，不论在ITGC或应用系统层面上，IT风险及控制均对财务报告内部控制的评估极其重要。

为说明有关IT控制评估的逻辑进程，对于与重要财务报告要素相关联的关键业务流程，项目小组应首先就有关的主要应用系统进行记录。其后，项目小组便可以进行有关技术组成部份和ITGC（见问题5）的识别流程，从而确保主要应用系统的进行和其数据的可靠性。这些组成部份和ITGC一经识别，相关的记录和评估工作便会与相应的业务流程（及有关的应用系统）产生联带或对应关系。





### 13. 在进行整体404条款项目时，什么时候应对IT控制予以考虑？

IT风险及控制的评估应与整体404条款合规项目同步展开。尽早完成评估是十分重要的，原因是404条款合规项目小组在计划业务流程的控制评估及界定其范围时，必须了解在公司层面的及在活动/流程层面的IT控制的强弱。



这些公司和IT基础设施控制的强弱的程度，将决定应用系统和业务流程控制，应进行什么程度的记录和评估，以便对业务流程层面的财务报告内部控制的成效作出合适的结论。例如，若计算机安全管理的ITGC领域存在缺陷，便需要加强业务流程层面的额外检测性（或监控或监督）控制的记录和评估。但是，若在ITGC层面上有严格的预防性计算机化控制以限制资产的存取，业务流程层面便不需要额外的检测性或监督性控制。

### 14. ERP（企业资源计划系统）如何影响IT评估？

公司所使用的ERP系统可为404条款合规工作中的IT风险及控制考虑带来众多益处。若只有一种全球性实施方法，很多影响财务应用系统的ITGC和应用过程控制是统一部署的。但是，我们还应该清楚了解组织如何实施其ERP方案。很多组织都拥有不止一个ERP“实例”（安装实体）。通常来说，ERP应用系统的安装和操作会因业务单位或地理位置不同而有所差别。若公司存在众多个安装实体，便需就每一个安装实体进行记录和评估，并将此视为404条款合规工作的一部份。

ERP应用系统的另一项优点是，它们已被广泛应用，从而带来潜在的高效率。许多应用系统专家对主要ERP的控制特性和功能均有所了解。根据公司的应用系统性质，这些专家可以了解组织内所部署的特定配置，并迅速确定公司是否已经采用了最佳的控制机制。如果没有的话，他们便会向管理层提出合适的建议。相反地，若公司采用为其度量定制的应用系统或经过多方面按其公司需求修改过的ERP系统，则必须对每一个应用系统或系统的程序化（计算机化）控制的设计有所了解，并对其进行记录和评估。

### 15. 共享服务中心如何影响内部控制的评估？

共享服务中心的特点跟问题14所讨论的ERP应用系统的特点有些相似。就共享服务而言，企业内的若干流程和程序相类似，同时亦对企业的风险及控制产生相关影响。就问题25至31所讨论的一般IT流程来说，在共享服务环境中，对这些流程的管理越多，在IT流程评估上所耗费的整体时间和努力便会越少。例如，如果企业设有共享服务中心，透过统一的流程来处理所有应用系统的变更，便只需进行一次应用系统变更流程的评估。因此其发现结果及评估可适用于共享流程下的所有应用系统。相比之下，若每个应用系统或每组应用系统的转变控制流程有所不同，便需就每一个重要应用系统或每一组重要应用系统的流程分别进行评估。

## 16. IT活动的外包如何影响公司控制的评估方法？

即使已将交易处理外包,管理层仍须对那些对公司会计系统及其控制有重大影响的流程中的控制进行评估。不论交易处理是在公司内或公司外进行, IT及其他控制问题始终存在。根据萨班斯法案第404条款的规定, 管理层必须就那些对公司财务报告内部控制起关键作用的流程活动和应用系统的控制进行评估。此评估必须针对公司的运作流程和应用系统, 以及公司将工作外包给外界服务商的流程和应用系统。PCAOB亦已对这点加以强调。

组织在考虑与外包流程和系统有关的内部控制时, 首要的步骤是审阅外包协议书。理想的协议书应明确制订双方在流程主要方面的责任, 以及在应用系统的操作和维护上的责任(例如, 安全管理、变更管理、数据管理和拥有者权利等)。公司亦应制订服务层面的协议书, 针对一些控制方面的问题作清楚陈述。此合约是外包关系中唯一真正的控制文件, 因为它列明“各自的责任”。

业务流程的内部控制评估应考虑实现财务报表认定目标所需的控制, 很可能需要服务组织(外包商)拥有合适的控制。在执行404条款合规项目时, 必须跟其他由公司所直接管理和控制的流程或应用系统的控制一样, 对这些控制进行评估和测试。PCAOB已清楚说明, 服务组织的委托并不会减少管理层在维护有效的财务报告内部控制上的责任。组织可透过以下途径完成评估和测试: 由外包商提供审计准则第70号报告(假设以下提到的问题已获得解决), 或由公司指派人士(例如, 内部审计、外面的顾问等)进行独立测试。

在决定采用何种方法进行上述评估时, 可参考以下数点:

- 审计准则第70号报告内容的审阅应根据用户组织的控制进行。因此, 用户组织应建立流程图以对输入控制、服务组织所处理的程序, 以及输出和输出控制进行记录。此外, 用户亦可设计应用系统中的重要主档案的维护流程及用户组织的安管理程序, 因为一般来说, 授权和职责分离的主要控制属于用户组织的内部活动, 且为组织所控制。

服务组织只是执行用户组织的指示, 于大部份的外包安排中, 用户只是购买服务组织的专业知识和能力, 而不会将流程风险转嫁予服务组织。

- 以往, 审计准则第70号报告的编制和范围界定, 是为方便服务组织的独立审计师与用户公司的外部审计师之间的沟通, 后者更可同时参考此报告及用户组织的财务报表审计。404条款已经改变了这些要求。根据规定, 管理层有责任就有关公司的财务报告内部控制作出认定。因此, 管理层有可能需要从服务组织的审计师手上取得审计准则第70号报告。另一选择是, 管理层可以对服务组织的控制进行独立测试, 但这可能不是一个可行的选择。

如果管理层计划使用审计准则第70号报告, 需注意以下几点:

- 首先, 审计准则第70号报告中清楚地指出, 此报告用作审计师与审计师之间的沟通用途。因此, 从规管角度而言, 审计准则委员会可能会不赞成将此报告用作管理层的依赖依据。尽管这并不一定会构成任何问题, 但管理层仍需就依赖此报告所衍生的法律问题咨询法律顾问。如果外包服务协议已作适当修改, 使其清楚

反映审计准则第70号报告的要求，协议书的字面内容和呈报关系便能合乎有关要求。

- 第二，需要对审计准则第70号报告的审阅范围进行仔细的评估。之前为满足审计师就财务报表发表意见之目的而设定的范围，或许需要予以大幅扩展，以符合管理层的额外要求。例如，审计准则第70号报告必须涉及相关的财务报告认定，并集中关注设计和操作成效，而这亦是萨班斯法案明确规定的管理层责任。除由公司管理的流程及应用系统控制之外，管理层亦必须就审阅范围的足够性作出决定，并负责判断测试范围的充分性，以及对测试结果进行评估。在服务供应商的控制方面，管理层要负责作出上述决定的程度受很多因素影响，包括输入、输出、职责分离及用户组织的其他控制，以及服务供应商的流程及应用系统对财务报表可靠性的关键程度。
- 证交会已延长404条款的过渡期，我们期望公司和其服务供应商能利用该机会重新商讨其服务协议。例如，管理层可在外包协议书中具体列明其测试要求，而服务供应商的审计师便能按照这些要求编制报告。事实上，很多外包服务供应商会就该等要求与其所有客户及独立会计师进行协调，以避免不可行且耗费时间地于不同情况下使用不同方法的做法。
- 根据404条款的规定，管理层须于年终时在年度报告中提交某个时点的内部控制报告<sup>1</sup>。审计准则第70号报告可涵盖某个时点或某个时期，并就预测未来业绩提出警告。如果审计准则第70号报告的日期与管理层于年终提交控制报告的日期相距甚远，那么404条款的这项规定会如何影响管理层就财务报告内控进行的认定？至少，管理层应了解在服务供应商的审计师报告所涵盖的时期之后，服务组织的控制是否曾出现任何变动。这些变动可能包括：（1）由服务组织告知管理层的变动，（2）服务组织的人事变动，且有关人士是管理层所接触的人士，（3）由服务组织提供的报告中的变更或其他数据的变更，或（4）在服务组织的程序中发现的错误。此外，服务组织可让其审计师定期刊发审计准则第70号报告（例如季度报告），以供有兴趣的用户组织参阅。

尽管有很多问题需要考虑，但在重要的应用系统上，服务供应商很明显需要开展若干工作。审计准则第70号报告是一个很好的起点，但是如上文所述，审计准则第70号报告的呈报程序仍需作出修改，以合乎404条款的规定。外包安排的财务报告影响是关键，管理层最终需负责决定须采取何种行动。鉴于管理层对内部控制进行报告的责任，以及独立审计师对管理层的认定进行鉴证及报告的责任，现在有必要加强关注审计准则第70号报告的准确性，以便管理层开展认定工作。

本文就下列标题项下的问题所给出的指引，有关公司应予以仔细考虑：活动/流程层面考虑 – 应用系统和数据负责人流程的角色，活动/流程层面考虑 – 应用系统层面控制。这些领域不能有效地外包 – 他们仍属于公司管理层的直接责任。

---

<sup>1</sup> 诚如在我们刊发的《萨班斯-奥克斯利法案指南：内部控制报告要求》一文中所述，根据404条款的规定，有关需要在财政年度结束时提交一份某个时点的评估报告。公司若在其财政年度末符合某些条件（例如，于最近第二个财政季度的最后一个营业日，市场资本至少达到\$75,000,000元），将被视作“加速编报公司”，且必须于2006年7月15日或之后结束的首个财政年度开始遵守404条款。其他公司，例如“小企业发行商”，必须于2007年7月15日或之后结束的首个财政年度开始遵守404条款。



---

## 公司层面考虑

在404条款合规项目中，404条款合规项目小组需考虑IT控制环境的整体优势及弱势。整体公司层面控制包括：

- 控制环境，包括包含IT操作及应用系统管理的授权及责任、统一的政策及程序，以及全公司性的政策，例如适用于所有营业地点及业务单位的行为准则及防止欺诈
- 管理层和流程负责人所使用的风险评估程序
- 围绕着统一流程和控制的组织和结构的方面的考虑，包括共享服务的环境
- 用来监督和分析操作/运作结果的步骤
- 有关预防、制止及发现欺诈的控制
- 监督控制表现的流程，包括内部审计活动和自我评估的方案
- 期终财务报告流程的控制

这些类别的控制，其范围通常涵盖全公司，并且在IT方面及业务流程方面同样重要。以下部份将对与IT相关的若干公司层面控制问题进行更详细的讨论。对这些问题所作的回复，可将IT组织与公司的应用系统及数据负责人区分开来，并探讨如何考虑公司层面有关IT风险及控制的问题，以及就公司层面控制的强弱所产生的不同影响提供指引。

### 17. 什么是IT组织？

如问题11中所述，“IT组织”包括IT运作，以及就会对IT产生影响的流程进行的整体治理。IT组织通常包含CIO的组织，为整个公司IT风险的有效控制确定了基调。IT组织对界定影响财务报告应用系统的领域进行管理。这些领域包括整体的安全管理政策、应用系统的变更控制环境、数据管理和灾难恢复流程，以及数据中心的操作和问题管理领域。在对公司层面的管理高层态度进行评估时，这些流程应予以考虑。IT组织在这些流程的监管上担任重要角色。

### 18. 管理层如何考虑公司层面上有关IT风险及控制的问题？

在决定公司层面有关IT的问题时，管理层应首先考虑如何管理其IT组织（见问题17）。IT是由公司高层哪个部门所管理的及如何管理？IT是被视为业务单位中不可或缺的一部份，还是单独的一部份，抑或是两者的混合？

在现今的环境下，业务单位之间通常会存在一些共享的技术基础建设。如果公司拥有一个中央技术基础设施，由业务单位层面管理应用系统亦非异常。该结构显然会影响对公司层面控制的理解、记录及评估。例如，业务单位极可能拥有一个属于组织一部份的技术基础建设实体（例如CIO），而不同的应用系统可视为业务单位实体结构的一部份，可能是业务单位内的独立实体，或两者的混合。鉴于有关方面的所有权和责任的易变因素，在进行公司层面评估时，对每一个组织结构的评估方式应略有不同，包括处理和记录这些评估的方法。



## 19. 是否存在仅仅包括IT操作或流程的独立“实体”？

如问题18中所述，许多组织可能会设有仅与IT工作有关的单独的部门（从COSO的角度来说）。此外，一个企业中也可能设有多个与IT有关的部门。由于即使在同行业内，各企业对IT的处理手法及管理方式也不尽相同，因此有多少仅与IT相关的部门在各企业中不等，且因组织规模大小而有所不同。404条款合规项目的其中一个首要步骤是了解IT组织和结构，以及决定如何对其进行管理和组织。该步骤对于为404条款合规项目提供一个有效的IT评估方案十分关键。

## 20. 就遵守萨班斯法案404条款及302条款而言，应考虑哪些IT治理问题？

如问题11所述，IT结构中包含两个方面的整体治理。一个与技术领域的管理有关，通常指CIO组织，另一个与应用系统和数据负责人有关。IT治理在每一方面的重要性体现在，组织会指导流程负责人如何了解、评估及管理风险和控制，以及如何解决控制问题。在公司层面上，重点应放在问题27-31和35-38所讨论的关键流程领域的治理上。治理对于建立“管理高层的态度”的COSO“控制环境”组成部份起关键作用。若IT的治理不足，那么亦不大可能出现较强的整体公司层面控制。

## 21. 若管理层对公司层面的IT相关项目有较强的控制，会有什么不同的结果？

较强的公司层面控制为流程/活动层面的控制打下一个好的基础。较强的公司层面控制证明，管理层已将有效降低风险及实施有关控制作为组织的重要任务予以执行。管理层一般都拥有一个程序，以评估和了解风险的所在；也会经常进行沟通，了解他们必须拥有相关信息以支持整个控制流程；并会监督流程的关键部份，从而使他们能够在出现问题时及时获悉。管理层在这些方面的能力能大大提高了IT基础控制活动/流程层面和应用系统层面具有较强控制的可能性。

## 22. 管理层如何了解公司层面的控制是否提供了一个较强的控制环境？

一个较强的公司层面IT环境，是一个IT组织的高级管理层（例如CIO）及应用系统和数据负责人，对整体控制环境具有全面了解、沟通和监督的环境。换句话说，这样的环境具有一定的透明度，使管理层能够了解正在发生的一切情况，以及是否存在任何问题。企业通常会召开管理层会议，按照会议议程讨论内部控制及有关问题。企业并具有正规的内部控制的政策和纲要，明确内控的目标和管理层的期望。这个层面的指导可以针对整体的目标，也可深入到更详细的层面。此外，该层面亦应有若干流程以对环境进行监督，以及确保有效的承上交流及部门间交流，以提高透明度。另外，需要对有关流程的关键步骤进行书面记录（作为证据需要）。

## 23. 若管理层对公司层面的控制较弱，会有什么不同的结果？

如果公司层面的控制较弱，在业务流程/活动层面维持较强的一般控制的可能性会大大减低。这并不表示一般控制流程/活动层面不可能存在较强的控制，但却说明高级管理层并未充分沟通这些控制的必要性，而且缺乏对环境的持续监督。公司层面若缺乏有效的领导，可导致缺乏规律及不一致的控制环境。在这种环境下，管理层及流程负责人可能忽略了对有助于有效地实现财务报表内控目标与IT相关联的控制的足够关注。

## 24. 较弱的公司控制环境有什么例子？

一个较弱的公司层面控制环境缺乏对有效内部控制结构的沟通和承诺。公司也不具备或缺乏健全的用以指导发展和维护较强的流程层面控制的整体政策和指引。强调公司需要一个较强控制的沟通也并不明显。IT组织的目标和宗旨（管理层所确定的基调）通常注重“低成本”及维持预算，而不是服务质量或风险管理。

---

## 活动/流程层面考虑 – 基础设施控制问题

这部份的问题将说明“IT基础设施控制”的性质，以及其对财务报告内部控制评估的重要性。亦会就404条款合规项目小组在进行这些控制的评估时所关注的事项提供指导。虽然这些控制由始至终都很重要，但它们所产生的影响却经常被误解。我们的观点是，404条款合规小组应从流程的角度去了解这些控制。在本部份中，我们会将IT控制细分为若干基本流程，阐述这些基本流程与财务报告的相关性，并就流程的优势及弱势对应用系统和数据流程控制评估所产生的影响进行讨论。这些控制包括安全管理、应用系统的变更控制管理、数据管理和灾难恢复、数据中心操作、问题管理，以及资产管理与有关的流程。

## 25. 何谓“IT控制”？

ITGC控制通常会影响到基础设施技术环境内不止一个的应用系统及数据。一般来说，因为这些控制会影响相关程序和数据的可靠性，所以最终会影响财务报表认定的实现。“控制层面”是指对多个应用系统有影响的流程，因此，对这些IT运作流程的控制被称为IT基础控制。

控制避免一些对相关流程处理和数据的可靠性有影响的事情发生。例如，如果某项关键的人工控制依赖由IT系统所产生的数据，那么在评估这些依赖IT系统或IT系统所产生的数据的流程层面控制时，IT控制的成效是须予考虑的一个重大因素。

## 26. 哪类的控制属于“IT控制”？

IT基础设施控制是总体或整体的流程层面控制。COSO将ITGC定义为“有助于确保计算机信息系统能持续及正确操作的政策及程序。这些政策及程序包括数据中心的操作控制、系统软件的获取和维护、存取的安全，以及应用系统的开发和维护。基础设施控制能够为程序化应用系统的控制提供支援。用来描述基础设施控制的其他称谓有一般计算机控制和信息技术控制。”



在本书中，我们会采用上述COSO的基本定义，将其理解为COSO对IT组织中一连串的流程和活动进行了描述。在现今的IT组织中，这些流程一般包括安全管理、应用系统变更控制、数据管理和灾难恢复、数据中心的操作、问题管理，以及资产管理。这些IT流程的控制跟一般在所有业务流程上的控制类别相同。以人工为基础和以系统为基础的控制

活动同时存在，并会执行预防性和检测性的控制，包括监督和管理控制。于所有流程中，最重要的是管理层必须为每一个IT流程订立相关的具体控制目标，以协助实现财务报告的整体内部控制目标。专按IT流程来说，控制目标应与流程和数据的可靠性（即实现完整性和准确性、一致性及时性等财务报告目标），以及对数据程序和具体交易的正确访问有关（这与授权和资产存取这两个目标有直接关系）。

我们对问题27至31作出的回复，主要针对一些404条款合规项目中应予以考虑的更为一般的控制目标和控制活动。然而，我们的回复并非面面俱到，不应被视作于任何情况下均应考虑的事项清单。然而，这些回复提供了良好的依据，在考虑目标和控制时可作为参考。

就问题27-31所涉及各领域而言，我们为以下问题提供指引：

- a) 控制领域与财务报告内部控制目标的相关性
- b) 较强控制的影响
- c) 较弱控制的影响

## 27. 对安全管理进行评估时，404条款合规项目小组所关注的是什么？

### 背景

在安全管理领域中，首要的流程目标是创建和维护IT环境的整体计算机安全措施。安全管理的焦点是全面性的，其中包括关于应用系统、数据库、平台和网络的流程；还有其他的流程，涉及识别风险、制订策略以便将风险减低至可接受的程度，以及管理层明确接受剩余的风险或风险容忍度。安全管理需要一套有效的流程，以便执行及监控IT环境各个层面中的政策和流程的执行。此外，还有一些子流程，负责处理个别信息资产的存取，以及控制非授权存取的风险。

在很多公司，安全管理是一个复杂且分散的流程，涉及众多的“技术层”（例如应用系统、数据库、平台和网络），分别由不同的IT部门负责处理。应用系统上的安全管理会被派发到不同的IT和用户群组。进行内部控制评估时的一个严峻挑战是要了解公司是如何部署安全管理的。因此，404条款合规项目小组须了解关于IT组织的足够细节，从而能够了解公司的关键数据及应用系统的授权获取及应用是在哪个“技术层”被怎样管理的。安全管理流程亦包括如何管理那些拥有全面权限可自由访问系统中储存的各种交易及数据的特殊用户。公司应了解这些特殊用户的特殊权限存在的必要性（而且在许多情况下这些权限不能全部被限制）；但是公司应具备严格的控制来尽量限制和监控这些特殊权限的使用。

以下简要地列出对公司财务报告认定的影响，以及安全管理的控制强弱如何影响萨班斯法案404条款合规项目的范围：

### 对财务财务报告认定的影响

- a) 按业务需要限制对关键系统（交易、应用系统、数据库、平台和网络）的操作，以确保数据（资产）的访问权限。
- b) 执行、审批和检视交易的权利只限于有正当业务需求的人士，以确保授权是按照管理准则适当受到限制。



### 较强控制的影响

- a) 对关键信息资产的存取采取了适当限制；其他与资产控制目标的存取有关控制活动（例如比较低层面的检测性和监督性活动）都因此而不必要了。
- b) IT基础控制层面（如问题25所述）能确保授权控制目标的实现。在进行应用系统和数据负责人流程层面（问题35及36所述）及具体应用系统的流程层面（问题41所述）的授权控制评估时，应考虑这些控制的效应，从而对目标作出全面的评估。

### 较弱控制的影响

- a) 若有关信息资产（交易、数据和系统资源）访问权限的IT基础控制较弱，便需要评估和了解可能的补偿控制。为对适当的控制进行评估，就每一个独立的资产（交易、数据和系统资源）而言，应从“可能会出现什么错误”的角度对其进行评估。对每一个资产进行评估时，应对适当的额外预防性、检测性和其他控制进行记录和评估。主要的问题是：“既然我不确定资产的存取是否正确，那么我如何才能知道是否已经发生了未经授权的修改、增加或删减？”
- b) 如果有关安全管理的IT基础控制中存在整体缺陷，便不能保证所有交易都已根据管理层所制订的一般和特别准则获得授权。由此衍生出的问题是，要确定非授权交易是否存在。如果存在，应如何发现这些交易以便作出适当修正。同样地，该问题应根据审核中的具体交易加以考虑。

## 28. 对应用系统变更控制进行评估时，404条款合规项目小组所关注的是什么？

### 背景

应用系统变更控制是财务报告内部控制其中一个尤其重要的因素。应用系统变更的可靠性会直接影响交易流程的准确性、一致性和完整性，以及交易的及时累积、总结和呈报。

公司变更其应用系统时所面临的风险是，新的变更可能导致曾用于处理和呈报交易的应用系统，失去其原有的可靠性。这将造成财务报告不准确、不完整或不正确等潜在的重大风险。鉴于可能出现这些与财务报告有关的风险（以及其他显着的策略及业务操作风险问题），公司必须有一个设计周详且运作有效的应用系统变更管理流程。

该变更流程应包括适当的程序，以建立、监督、测试及审批有关变更，并将经适当审批的变更转移至生产环境。该流程必须设置适当的保安措施，以防止负责该流程的人员在未被发现的情况下，对程序或有关数据作不适当变更。考虑到变更可能产生的所有影响，例如系统接口、数据和例行错误侦测程序、应用系统的安全管理变更、管理报告等，因此变更流程必须包括周全的措施及步骤。

### 对财务报告认定的影响

- a) 应用系统的变更直接影响应用系统的完整性、准确性和一致性，这里的应用系统是指进行交易、将会计信息总结、分类和披露时所用到的程序。
- b) 因为增加或修改职责及/或因为对敏感交易及数据的存取授权加以修改而作出对应用系统的变更时，可能影响不兼容职责的适当分离。
- c) 在变更的操作过程中可能会使未获授权人士亦能够存取信息资产，而这将导致应用系统或数据在无从被一般控制活动发现的情况下，被有意或无意地更改。



## 较强控制的影响

- a) 应用系统能够如用户所期望的那样运作。系统功能和控制能够按预定的计划稳定及准确的运行。变更控制直接影响与流程的完整性、准确性和一致性相关的控制认定的实施。

提示 - 这些控制确保应用系统按照设计和计划发挥作用。每一应用系统的控制考虑必须经过评估，从而确定应用系统的设计是否包含所有必需的控制，以达致可靠的财务报告。

- b) 可以确保变更控制流程并未损害数据的可靠性。

## 较弱控制的影响

- a) 不能确保对程序所作的修改不会对预期的程序化控制有负面影响。因此，可能需要进一步对补偿控制进行评估和记录。这些补偿控制一般来说应是由人工操作的及具有检测性的控制，并可能需要进一步地详细的实施。此外，亦可能需要进一步了解对一些关键程序所作的变更（性质及次数），从而确定应用系统发生不适当变更时，应需要哪些特定种类的控制，以发现其所引起的具体错误。
- b) 如果在应用系统变更流程中并未对应用系统和生产数据的存取进行适当限制，便可能需要考虑和记录补偿控制，以发现那些因疏忽或故意对数据或程序所作的变更。

## 29. 对数据管理和灾难恢复进行评估时，404条款合规项目小组所关注的是什么？

### 背景

数据管理对技术组织的工作成效和效率起关键作用。为便于讨论，我们将“数据管理”归纳为与数据备份、恢复和修复有关的流程。在很多情况下，需要进行数据的恢复，大部份原因是由于硬件或软件损坏而导致数据受损或遗失。公司必须有能力和重新启动系统，以确保持续操作及不损害交易或数据的可靠性和完整性。交易和数据的损失显然会影响流程的准确性和完整性。

数据管理亦包括应用系统的关键性，以及备份流程的合适时间和次数的考虑。备份流程的次数和可靠性能够反映出一间公司对成本/风险/得益的判断结果，即在不会对业务造成负面影响的情况下，该公司可以承受多大的数据损失或多少交易的损失。

灾难恢复的流程和程序是与数据管理相关联的。业务的持续运作和IT的灾难恢复，主要涉及公司是否能够持续遵照证交会的规则和条例，准确且适时地提交其财务报告和其他报告。诚如问题37所述，灾难恢复需要合公司的业务影响分析和业务持续计划。

有些人认为，萨班斯法案第404条款要求公司制定一个全面的业务持续运作和灾难恢复计划，目的是符合财报告模型中既有的“持续经营”这个假定。“持续经营”这个假定存在已久，且我们认为并未在萨班斯法案下被修改。如果公司在萨班斯法案通过前已有“持续经营”这个概念，现在也不会欠缺，除非公司的运作和前景有所转变，反之亦然。然而，话虽如此，我们仍深信谨慎经营的公司应根据全面的业务影响分析，制定合适的业务持续运作和灾难恢复计划。如问题37所述，这是管理业务风险的一个重要组成部份。

### 对财务报告认定的影响

- a) 公司能否完整及准确地报告交易和财务报告数据的能力，会受到数据管理和灾难恢复流程的影响。
- b) 如果透过数据管理流程而赋予对生产或备份数据不适当的存取权利，资产的获取可能会受到影响。
- c) 如果业务持续运作和灾难恢复计划不够全面和得到及时更新，那么公司履行其义务的能力，即完整且准确的报告及时提交证交会的能力将会受到影响。

### 较强控制的影响

- a) 数据管理流程确保数据的完整性和准确性；因而使修复和恢复之后的处理更可信赖。
- b) 恰当地限制存取，以确保数据不会在数据管理过程中而被变更或删除。
- c) 充分降低因缺乏处理能力及遗失重要数据而未能按证交会要求提交报告的风险。

### 较弱控制的影响

- a) 不能确保在数据管理过程中未对数据产生不良影响。有必要就那些为发现潜在错误或遗漏而设计的舒缓控制进行记录和评估。这些步骤和控制可能包括在数据被修复或尝试修复之后通知用户的程序。舒缓控制应包括具体的检测性控制，以确定修复或恢复时是否出现不适当的数据变更。
- b) 就公司遵守证交会要求提交报告的能力而言，公司的业务影响及/或灾难恢复计划或许并不充分。在这种情况下，公司应考虑如何施行短期及长期的解决方案。根据萨班斯法案第302和404条款规定的信息披露要求，这种情况可能成为一个具争议性问题。因此，必须仔细考虑要采取的步骤，并作出适当的行动。

## 30. 对数据中心的操作和问题管理进行评估时，404条款合规项目小组所关注的是什么？

### 背景

数据中心的操作和问题管理也会像问题29所讨论的数据管理流程一样影响应用系统和数据。这些流程会影响数据的可靠性及程序的完整性和准确性。当有问题发生时，数据中心的操作和问题管理会影响应用系统的正常操作。在诸如接口的处理不完整或程序被中断等类似情况下，交易或数据的处理不完整或不准确的风险概率就会增高。计算机操作和问题管理方面的步骤，旨在提供处理这些问题的方法。这些流程通常涉及数据和应用系统负责人之间就解决相关事宜和问题而进行的交流与沟通。此外，这些部门的负责人员通常在数据的存取和应用系统的操作方面拥有广泛的权力，以及时解决出现的有关问题。这就增加了交易及数据在非常情况下，未经正常授权下被存取的风险。

### 对财务报告认定的影响

- a) 报告的完整性、准确性和一致性会直接受计算机操作和问题管理流程影响。
- b) 如果没有适当地限制和监督计算机的操作和问题的管理，信息资产的存取会受直接影响。

### 较强控制的影响

- a) 确保这些流程不会影响程序的完整性、准确性和一致性。
- b) 适当地限制和监督关键交易程序和数据的存取，以确保任何重大的错误或遗漏能够被发现。

### 较弱控制的影响

- a) 因数据操作或问题管理方面的薄弱环节而产生的潜在错误或遗漏，需要对其有关的补偿控制程序进行记录和评估。若在计算机操作方面存在整体弱点，便需要更多详细的检测性和监督性控制。这些额外的步骤应使用户对潜在问题有所警惕（例如有些应用系统的问题需要负责计算机操作的人员来处理），以便特别执行额外的人工的检测性和监督性控制。
- b) 若计算机操作和问题管理方面的安全存在弱点，便需要在应用系统和数据负责人层面，以及IT组织层面，增加额外的人工检测控制。在应用系统和数据负责人，这些控制则包括设计更详细的步骤，以发现应用系统和数据的变更。IT组织中的额外程序包括对这些领域的个别项目进行监督和监管，以及监督并报告利用广泛的访问权限进行的活动。



### 31. 对资产管理进行评估时，404条款合规项目小组所关注的是什么？

#### 背景

资产管理领域是现今IT组织中重要的一环。原因是除了硬件和软件的价格不菲，该领域在以往的管理一直欠佳。从萨班斯法案404条款合规项目的角度来看，资产管理的重要方面与IT资产的获取、操作和报废的正确会计处理有关。此外，该领域亦存在一些涉及软件版权的适当使用及监督的潜在问题。不正确使用软件可导致未记录的负债，以及围绕正确使用软件和遵守软件使用法例而产生的潜在信息披露问题。就公开报告的角度而言，另一个值得关注的领域是对资产存在的定期验证、记录余额的定期评估，以及根据使用年期进行的资产变现。

有关IT资产管理的主要报告问题，与有关所有固定资产的报告问题并无差异。本书选择前者进行讨论，原因是该等IT资产的会计处理所经常涉及的流程，不同于其他固定资产的监管及程序。IT资产包括硬件和软件，以及用户的桌上计算机和 workstation。该等资产都是现今技术环境中的重要投资。

### 对财务报告认定的影响

- a) 资产应在财务报表中予以正确呈列。这意味着，该等资产已根据普遍公认会计准则，适当地予以资本化或计作开支，且已对所有资本租赁作出适当的会计处理。此外，任何及所有要求的披露均已在财务报表中呈报。
- b) 资产余额可透过观察或其他一些途径进行周期性披露，以验证它们的存在。此外，需对资产的账面值进行周期性评估，并审核相关资产类别的预计可使用年期是否合理。
- c) 资产的存取以适当方式予以保护，从而合理保证任何报告日期下资产的存在。

### 较强控制的影响

- a) 确保已对IT资产进行适当的呈报和会计处理；有关余额已予以定期评估和验证。
- b) 确保所规定的任何披露（租赁义务，以及与潜在的法律及规管事宜有关的承担及或有事项）均恰当无误，并已就必需的支持作出适当记录。

### 较弱控制的影响

- a) 资产余额及有关费用或未予以适当呈列。因此，或会需要补偿控制和额外控制。补偿控制将集中用于验证余额及资产的存在，可能包括多种临时应急的用于消除差距的资产余额评估控制。
- b) 对固定资产的披露或会缺乏足够的支持及识别。如要确保能够适当地识别和支持信息披露，则可能需要额外的控制和程序。从长远的角度而言，一个明确的披露流程极可能是保证财务报告认定得以实现的途径。然而就短期情况而言，有关控制或会涉及大量的人工操作，且属于临时性质。

---

## 活动/流程层面的考虑 – 应用系统和数据负责人的角色

在下列问题的回复中，我们就应用系统和数据负责人，以及他们在IT组织及协助404和302条款合规工作中的角色及责任进行了阐述。本部份亦就应用系统和数据负责人须在有关领域实施的流程提供了指引。有关领域应对内部控制的有效运行起到关键作用。本部份亦就应用系统及数据负责人的流程控制对财务报告内部控制评估的影响进行了阐述。就主要的财务报告应用系统而言，404条款合规小组需要确定应用系统和数据负责人。在某些情况下，该等人士可能是流程负责人。该等人士所负责的主要活动和流程包括：安全角色和管理、管理关键交易和数据的存取、开展和维护业务影响分析和业务持续计划，以及建立和维护业务负责人的交接控制。



### 32. 谁是应用系统和数据负责人？

一般来说，应用系统和数据负责人是业务流程的一部份。从控制的设计和操作方面来说，通常他们也负责整体业务流程。整体流程负责人可将此责任委托给其他人，但流程负责人必须清楚说明被委托之人所应负的责任。应用系统和数据负责人有责任去了解、设计和维护应用系统中所执行的控制。该等人士必须对计算机化控制有所了解，方能有效设计有关控制，并向IT人员传达该等控制的必要性。应用系统和数据负责人亦必须了解计算机化控制的局限性，并能够协助设计检测性和监督性控制，以弥补若干IT流程中IT基础控制的不足。

### 33. 就IT组织而言，应用系统和数据负责人承担什么角色和责任？

应用系统和数据负责人必须能够在IT组织内就预想的应用系统角色，包括有关的内部控制，进行有效的交流。这种交流就好像为楼宇设计蓝图，楼宇建设过程中，须了解其结构是否符合期望的规格。若楼宇结构并不符合规格，应用系统和数据负责人便须清楚指示所需要作出的整体调整，以填补缺漏，尤其是内部控制方面。应用系统和数据负责人担当的角色是，在应用系统发时变更及修订时，与IT组织进行持续协作。由于应用系统不断变更和修改，因此，制定和维护应用系统中不可或缺的控制是该等负责人应担当的角色。整体来说，应用系统和数据负责人确保整体流程保持适当协调，以保证财务报告的内部控制有充分的目标。

### 34. 应用系统和数据负责人应制定什么流程以协助遵守404和302条款？

与其他流程负责人一样，应用系统和数据负责人应定期对他们所负责的控制进行自我评估。应用系统和数据负责人应从整套业务流程控制的角度，包括人工和自动化的控制，了解他们所负责的应用系统。由于应用系统的发展和变更，应用系统和数据负责人应在302条款季度性行政人员的核证流程和404条款年度评估流程中起到积极的作用。在这两个流程中，核证人员均依赖重要财务应用系统的完整性和可靠性。因此，应用系统和数据负责人的反馈意见，不论是直接的或透过单位管理层及/或披露委员会传达的，对核证人员评估变更的影响来说均是宝贵的意见。

### 35. 要建立合适的安全管理和职责分离，需要制定什么流程？

应用系统和数据负责人必须清楚了解他们所负责的交易和数据，以确保这些交易和数据的有关活动，在内部控制中有适当的职责分离。例如，将交易的授权、管理和记录职责适当分离，是内部控制的基本原则。应用系统和数据负责人不应容许技术环境破坏这一原则。因此，他们应对所需的不兼容职责的分离进行记录，使IT组织能从应用系统的安全角度，了解和制定这些规定。换句话说，应用系统和数据负责人有责任将应用系统的安全要求备案。

此外，应用系统和数据负责人亦有责任在各应用系统延续发展和变更时，对“交易和职责分离清单”进行持续更新和维护。

### 36. 就存取关键及/或敏感交易和数据的定期审核和审批而言，需要制定什么流程？

作为其责任之一部份，应用系统和数据负责人亦应负责监督就关键交易的存取过程、存取频率及存取人而进行的定期审核。该等审核是要确保只有那些有合理业务需要的人士，方能够获得授权以执行及/或检视关键的交易和数据。审核应根据交易和数据的关键性和敏感性定期进行。审核流程应予以记录，以显示应用系统和数据负责人已审批该审核阶段的正当存取。如果需要实施措施或变更，便需要制定有关流程，以确保对这些异常的活动予以及时的适当处理。如果在该领域中发现有安全管理流程失灵迹象（见问题27），便应采取根源分析，及时解决相关事宜。

### 37. 就业务影响分析和业务持续运作计划而言，需要制定什么流程？

应用系统和数据负责人与业务流程负责人应是同一人，或至少应向其直接汇报。流程负责人负责确保适当的业务影响分析，以及制定和维护根据影响分析而制定的业务持续计划。IT组织的责任则是建立一个灾难恢复计划，用以制定业务持续运作计划。

对公司的整体商业风险进行管理的一个重要方面，是其有效处理业务持续和灾难恢复的能力。鉴于2001年的911事件，这很明显是一项需予以管理的重要商业风险。2003年在美国东岸发生的电力供应中断事件，充分暴露了组织过度依赖所属国家关键基础设施（即电讯、公用事业、供水系统、银行系统、交通等）的不堪一击的弱点。

证交会已刊发一项政策声明，指出负责交易市场及电子通讯网络运作的自我监管组织，应在其业务持续运作中遵守若干基本原则。例如，证交会的原则包括：

- 最迟须于紧接大规模中断发生后下一个营运日恢复交易
- 备份应于异地存放
- 确保重要共享信息系统（例如综合市场数据流）能完全被恢复
- 透过测试确定备份安排的有效性

证交会要求这些由自我监管组织运作的交易市场及电子通讯网络尽快落实相关计划，以遵守这些原则，并已将完成期限定于2004年末。此行动表明，即使监管者本身亦已对该等风险时期作出响应，表示支持业务持续计划的标准。

根据萨班斯法案第302、404和906条款的规定，公司须设计及维护若干程序和控制，以确保能够及时识别与有关行动和披露相关的所有重要信息均及时地呈报，并透过周期和当前报告，将财务信息和披露事项公平地呈报予公众。财务报告中有一项假定，即上市公司有能力于期限截止日期前提交报告，并拥有进行公平呈报和披露所必需的所有重要信息，包括利用当前和可靠的信息更新会计估计。为履行该等要求所产生的责任，公司需有完整备案的业务影响分析，当中包括管理层的同意和签署，并针对公司更广泛的商业风险及监管和合规风险，包括与公开呈报有关的风险。充分的业务影响分析一经完成，公司便能够评估是否需要对其业务持续运作和灾难恢复计划作出任何变更。这些计划必须予以持续更新及定期测试，以维持其充分性，从而确保公司能够履行萨班斯法案项下的义务。

**38. 在对生产应用系统作出变更之前，就建立、测试和审批有关应用系统变更而进行的管理而言，从内部控制的角度看，应制定什么流程？**

应用系统和数据负责人需要与IT组织中的变更控制流程开展有效协作。该等负责人应该：

- a) 有能力建立应用系统的变更。
- b) 透过经同意的记录文档将有关变更传达予IT组织。
- c) 对所有建议变更对内部控制环境所产生的影响进行评估和记录。
- d) 在变更实施于生产环境中之前对其进行测试。这些测试包括验证关键自动化控制的运作（以确保变更并未对控制环境造成预期以外的影响）。对应用系统所作的任何紧急变更均需进行测试，也就是说，在作出紧急变更前，应通知应用系统和数据负责人，以便其对有关变更进行适当的评估。

以上每项流程均需作充分记录，以证明流程如预期般操作，并表明应用系统和数据负责人及IT组织之间的协作富有成效。

**39. 如果应用系统和数据负责人流程控制的设计和运作有效，对财务报告内部控制的评估有什么影响？**

如果关键应用系统和数据负责人的所有相关流程控制均能有效地运作，从自动交易和数据的角度看，便可确保适当地维持职责分离。如此一来，应用系统和数据负责人便可确保不兼容职责的分离及关键应用系统系统的安全管理均已到位，从而保证数据的存取只限于已获授权的人士及应用系统，然后进行与授权和资产认定的存取有直接关联的具体职责。因此，没有必要为确保流程层面上不兼容职责的适当分离，而对其他补偿流程和程序进行独立评估，惟并非以系统为基础的人工职责除外。

如果变更控制的运作有效，便能保证程序的准确性和一致性，而额外或补偿的检测性控制程序也能相应减少。应用系统系统的变更（透过系统开发、提升和维护的）于实施前应予以授权、测试和审批，而这直接关系到授权、完整性和准确性、分类，以及资产认定的存取。

在施行有效的业务影响分析和持续计划程序的情况下，那些会导致公司未能根据证交会规定及时提交报告的业务中断便会减少。

若干基本的例子便可说明有效的应用系统和数据负责人控制对财务报告内部控制目标所产生的影响。但我们必须在此提出警告。如上文所述，IT组织中的IT基础控制与应用系统和数据负责人方面的程序和控制成效有直接关系。如要获得一个较强的整体环境，IT基础控制及应用系统和数据负责人控制均必须有效地设计和操作。

**40. 如果应用系统和数据负责人流程控制的设计和运作没有成效，对财务报告内部控制的评估有什么影响？**

我们在问题39的回复指出，如果应用系统和数据负责人的控制较强，404条款合规小组则毋须就职责分离及程序的准确性和完整性制定额外或补偿控制。然而，若应用系统和数据负责人的控制不够充分，则必须对额外或补偿控制进行记录、评估和测试。

若没有充分的业务影响分析和持续计划，业务中断的风险便会加大，进而影响公司根据证交会规定及时提交报告。如果有关风险较大，则必须对披露事项的影响进行评估。



---

## 活动/流程层面的考虑 – 应用系统层面的控制

应用系统层面控制包括业务流程中的控制，例如应用系统的程序化控制、信息获取控制（关键业务和数据）、数据验证和错误检查程序、错误报告及其他控制。我们对这些问题的回复就活动/流程层面上的具体应用过程控制作出阐述，包括为每个主要业务流程选择关键的应用系统，将应用系统层面的控制纳入业务流程的控制评估。我们也就活动/流程层面上较强和较弱的具体应用系统的影响提供指引。

### 41. 应用层面的控制考虑有哪些？

具体的应用系统控制的考虑主要与应用系统内被程序化的控制有关（所谓的“程序化控制”或“自动化”）。可依赖该等控制减低业务流程层面的风险。

COSO将应用系统控制定义为“应用软件中的程序化程序，以及相关的人工程序，旨在协助确保信息流程的完整性和准确性。有关范例包括：数据输入的计算机化编辑检查、数字顺序检查，以及就错误报告中所列项目而须进行的人工程序。”

为回应本问题，我们会集中关注程序化程序和控制。这些程序化控制确保交易能够透过有关财务报告的应用系统而予以完整、准确、及时和适当地进行及呈报。这些控制考虑源于关键的业务流程作业位置，而这些作业位置的应用系统会：

- a) 作出运算
- b) 执行数据验证和编辑检查
- c) 透过电子途径与其他系统接合
- d) 将那些管理层认为完整和准确并可依赖的关键财务信息进行分类、总结和呈报
- e) 限制交易和数据的存取

这些应用系统层面的控制考虑源于应用过程控制的正确设计，以及该等控制乃按管理层预期的方式及时间进行操作这一事实。这些控制也基于一个假设，即无论是程序化控制，抑或围绕程序化控制的应用系统，均不会有任何变更，因而，这些控制便不再按管理层预期的方式或时间执行。

在应用系统层面上，不兼容职责的分离是亦是一个关键问题。在应用系统中，有关的职责分离乃根据严格的业务规则，透过对交易和数据的存取作出限制得以实现。这些规则避免用户执行或存取从内部控制角度而言属不兼容的交易或数据。举例来说，如果可以由同一人委任销售商并在其后支付该销售商的发票，这两项职责便是不相容的，应予以分离。

### 42. 404条款合规项目小组如何决定每个主要业务流程的关键应用系统？

业务流程中务必要对其有所了解的一部份，是识别那些与影响财务报告要素的关键流程互相作用的应用系统。为对流程有所了解，项目小组应对主要输入、流程活动和流程输出进行记录，且记录中应包括流程中不可或缺的应用系统系统的描述或图标。换句话说，项目小组选择的应用系统应是（a）成功执行流程不可或缺的，及/或（b）相关财务报告认定未能实现的风险增加时予以施实的流程。



应考虑因素包括:

- a) 所处理的交易量 (交易量越多, 应用系统越关键)
- b) 交易的币值 (币值越大, 应用系统越关键)
- c) 运算的复杂性 – 这里所指的复杂性是指用户适当运算的能力 (运算越复杂, 应用系统越关键)
- d) 数据和交易的敏感度 (敏感度越大, 应用系统越关键)

此外, 进行应用系统的优先排序时, 识别所有被使用的应用系统是很重要的, 这些应用系统包括工作表格、电子数据表、用户数据库程序 (例如Access), 以及以通过互联网联接到的程序和运算器。这类程序需要进行适当记录, 而变更控制、安全、备份和恢复等程序则需分别进行评估, 尤其是在应用系统会对整体财务报告流程产生影响的情况下。

#### **43. 404条款合规项目小组如何在活动/流程层面上, 将应用系统层面的控制考虑纳入业务流程控制?**

具体应用系统的控制是业务流程中的关键部份, 有关该等控制的记录和评估应与业务流程控制同时进行。项目小组须考虑流程风险和主要控制点, 并判断哪些控制是程序化应用过程控制, 以及哪些控制须依赖由计算机产生的信息而方能有效运作。接下来, 小组需考虑应采取哪些必要步骤, 以充分了解和记录应用系统中的主要控制(即透过专家了解应用系统的设计和操作)。

在很多情况下, 对控制和流程活动的识别和了解须依赖由计算机产生的可靠信息。为合理证明这些控制和活动的可靠性, 404条款合规项目小组应对产生信息的应用过程控制进行评估。如问题25至31所述, 该等评估通常会与IT基础控制有效运作的影响发生关联。

#### **44. 如果404条款合规项目小组发现业务流程层面有较强的应用系统控制, 管理层应采取什么措施?**

如果应用系统层面的控制较强, 一般也会存在较强的预防性和程序化检测性控制。在这些情况下, 便无需执行多余的人工检测性控制。若存在较强的应用过程控制, 监督性控制便可专注于更高层面, 且其容忍范围与比较弱的应用系统层面的控制相比要大。

#### **45. 如果404条款合规项目小组发现应用系统层面有较弱的IT流程控制, 管理层应采取什么措施?**

如果应用系统层面的控制较弱, 便须对补偿检测性控制和监督性控制进行记录和评估。这些检测性和监督性控制应具有具体及周详的本质, 无需依赖计算机程序也能有效地操作。根据有关应用系统的控制弱点的性质和严重性, 可能需要对其作出改进, 从而改善应用系统层面的控制。此外, 若缺少必需的应用系统层面控制, 也许就不能够判断内部控制将在将若干风险减低至可接受水平方面的有效性。

#### **46. 就用户在财务报告流程中所采用的并不受限于ITGC环境的电子数据表和其他技术工具而言, 管理层如何对这些工具的控制进行评估?**

关键的工作表格、电子数据表和其他由用户开发和实施的技术工具, 均需如其他控制或IT组成部份一样, 对其进行记录和评估。唯一的不同是, 这些工具通常是由IT控制环境

以外的用户设计和采用。举例来说，IT部门要实施一个应用系统时，在应用系统得以实施前须对其进行严密且广泛的测试。此外，IT部门亦设立一系列的操作流程，例如变更控制、安全、备份和恢复，以确保应用系统的正当维护和操作。对于由用户开发和维护的应用系统，有必要对这些应用系统的IT相关流程进行单独评估，特别是在这些应用系统会对整体财务报告流程产生重大影响的情况下。有关的单独评估应针对与这些应用系统有关的变更控制、安全、备份和恢复等等事宜。就应用系统的功能而言，评估必须考虑的方面包括：关键运算的准确性、数据验证和错误检查、完整性和准确性问题、主要接口，以及报告流程的可靠性。此外，亦需根据审计追踪和其他有关流程的证据，对流程的一致性、准确性和持续性进行评估和总结。其中，有关流程是指那些由用户开发的应用系统、电子数据表和工具所执行的流程。

---

## 文档记录

文档记录在财务报告的内部控制评估中占重要地位。在本部份的问题回应中，我们就各个层面的文档记录提供指引，包括公司层面和活动/流程领域层面。IT风险和控制的文档记录必须与404条款合规小组所定的整体标准和方法一致。

### 47. IT组织及应用系统和数据负责人应进行多少文档记录，以为应用系统的控制和运行提供证据？

该问题须从两个方面予以考虑。首先要考虑的是需要作什么记录，以为程序的运行和控制提供证据。其次是须进行哪些技术性记录，以确保应用系统的维护能够使程序和控制的可靠性得到保证。

这两个考虑有明显的关系。应用系统的记录文文件应具体说明应用系统的主要组成部份被应用在哪些环节及如何操作。主要组成部份应包括问题41-46所讨论到的关键应用过程控制。记录文档的形式可以有多种：程序流程和描述、展示程序操作步骤的流程图，以及其他展示数据关系和数据库设计的技术文档。技术文档的记录，应使不熟悉该程序（但具技术知识）的程序员能够明白该程序如何操作，以及其关键接口、数据处理和安全特点，并可以合理地加以维护。

在大多数情况下，仅仅包含基本程序编码和技术数据库规格的记录文档还不足以满足404项目的文件记录要求。

如果应用系统的记录文档不充足，对系统实施不适当的变更的风险便会增加，若是这样，便需考虑问题28至38中就较弱变更管理所提供的指引。

### 48. 404条款合规项目小组应如何记录公司层面的IT控制？

IT领域控制的文档记录方法，应与其他业务领域控制的文档记录方法类似。在公司层面上，文档记录的焦点应集中于政策、程序、公司沟通、管理层会议记录，以及调查问卷和具体说明公司控制如何运行的其他项目。



#### 49. 404条款合规项目小组应如何为活动/流程层面上的ITGC进行IT控制的文档记录?

就应用在活动/流程层面上的IT基础控制而言，我们相信流程图和风险及控制矩阵是为其进行文档记录的最适当工具。这种文件记录与其他业务流程的文档记录相似。

#### 50. 404条款合规项目小组应如何为应用系统和数据负责人所操控的流程及具体应用系统领域，进行IT控制的文档记录?

就应用系统和数据负责人所操控的流程而言，我们相信流程图和风险及控制矩阵是为其进行文档记录的最适当工具。在业务流程层面，对应用系统层面控制进行记录的最佳方式，是与其他业务流程风险及控制的记录相结合。该方法了解内部控制对IT依赖程度的最佳方法。此外，该方法亦有助我们发现业务流程控制与应用过程控制的重迭，以便应用过程控制的专家能够于需要时对该等控制进行审核和测试，主要的应用系统应有额外的文档记录。这些应用系统包括：系统图标或数据流程、显示影响业务流程的应用系统的矩阵，以及主要应用过程控制考虑的矩阵。对主要控制的考虑着重于复杂运算、主要数据的验证和核实检查，以及重要及/或复杂接口等。

#### 51. PCAOB最近颁布的披露草案着重强调了交易的“建立、记录、处理和报告”，有鉴于此，对交易流程进行文档记录的最佳方式是什么?

我们相信对交易流程进行文档记录的最佳方式是透过应用系统和数据流程图表。这些图表描绘了公司不同应用系统中的重要数据流程，由数据的起点至它们最终影响财务报表和披露。我们认为，开始制作这些图表时，有必要采用一种概览的方式，其后再就最为重要的交易和应用系统提供详细记录。在详细图表中，重点突出数据输入、处理和输出将是一种有效的做法，原因是该记录文档可以表明审计师已遵守PCAOB的要求，即透过仔细查核获取对“重要业务流程”的理解。

---

## 测试

与其他控制一样，IT控制必须经过测试，以确定它们按设计的要求运行。《萨班斯—奥克斯利法案指南：内部控制报告要求》第二版提供了测试的指引。我们对以下问题的回应是该指引的伸延，主要针对有关IT的控制。

#### 52. 如何进行IT控制的测试?

IT控制的测试方式应与其他流程领域的控制测试相似，其中包含咨询、检查、观察及重新应用和/或重新执行。在任何情况下，均应对测试进行充分的文档记录。综合使用这些测试通常足以就运行成效提出结论。

在IT公司层面，大部份的测试均与咨询、检查和观察有关，原因是就大多数该类控制而言，重新执行和重新应用均无法实现。至于IT基础控制领域中的流程及应用系统和数据负责人控制，则有必要进行全部四种测试，包括重新执行和/或重新应用。这些流程的流程层面控制设计，一般应提供证据，证明流程的若干部份已经完成（例如签名或其他表格的签署等）。



---

## 处理缺陷及报告

如果内部控制存在重大缺陷，便必须予以修正。甫瀚刊发的《萨班斯—奥克斯利法案指南：内部控制报告要求》第二版就内部控制的缺陷提供指引。我们对以下问题的讨论是该指引的伸延，主要针对有关IT的控制。

### 53. 管理层如何解决IT控制的缺陷和差距？

管理层有两种解决IT控制缺陷的可行方法。第一个方法，也是最显著的方法，是对设计或运行无效的流程或控制进行差距分析，并制定行动计划弥补差距。另一个可行方法（至少适合短期施行），是要确保对缺陷风险及相关补偿控制（如有）的进行透彻的分析，从而判断对财务报告认定的风险范围，以及有关风险是否已被充分降低。该方法于短期来说或许十分重要，原因是对差距的分析及弥补可能需花费较长一段时间方能改善IT控制。在很多情况下，对人工发现控制的需求可能会大幅增加，以识别和纠正那些可导致业务流程层面上的错误或遗漏的具体项目。

### 54. 在鉴证程序中，外部审计师如何看待IT控制？

很明显，这是每间外部审计公司都需要与其审计客户商讨的一个问题。然而，有一点可以肯定，独立会计师在就内部控制报告中公司管理层的认定的基础进行评估时，会考虑与IT有关的风险和控制。IT基础控制属于总体控制，会影响所有或大部份交易的可靠性，以及所有或大部份衍生财务报表的内部财务报告的可靠性。IT基础控制中若存在弱点，很可能对重要交易和会计科目产生影响。若IT基础控制存有差距，外部审计师很可能会坚持首先处理这些差距的问题，方对内部控制的成效达成整体意见。举例来说，我们了解在有些情况下，外部审计公司已通知其审计客户，表示客户公司必须就应用系统安全制定较强的控制，特别是有关安全管理人员及用户访问权限的管理，审计公司方能就管理层对控制环境作出的正面认定进行鉴证。有鉴于此，404条款合规小组应尽快评估流程中的IT控制环境，包括IT基础控制，从而判断当中是否存在一些必须处理的差距。

应用系统和数据负责人流程层面的IT控制及具体应用系统的IT控制，对有关应用系统的整体内部控制结构有相似的影响，而该类应用系统对财务报表中有重大影响。公司应把流程层面上的应用系统和数据控制考虑纳入其404条款的合规方法，便是基于这个原因。404条款合规小组应确保该过程的实现。



---

## 关于甫瀚

甫瀚是一家提供独立内部审计及商业和技术风险咨询服务的公司，在业内处于领先地位。本公司帮助客户识别、评估及管理其在所属行业及其系统及流程中面临的各种营运及技术风险。甫瀚协助各公司开展萨班斯法案的合规工作，帮助他们财务报告内部控制及有关的披露控制及程序进行记录，设计及推荐该类程序和控制和改进策略，以及组织并管理有关萨班斯法案的合规项目。

作为Robert Half 国际公司（Robert Half International Inc., 简称RHI）的全资子公司，甫瀚于北美、欧洲及亚洲等地拥有五十多间办事处。

### 信息技术内部审计的分包及有关信息技术的萨班斯法案合规服务

甫瀚为信息技术内部审计的分包和外包提供全面的解决方案。我们的信息技术审计师拥有广泛专长，就信息技术审计服务的各个方面提供协助，从定义审计范围和执行风险评估，到年度规划和职责范围界定，以及执行各类与技术相关的内部审计。我们亦就萨班斯法案合规工作的技术风险及控制提供咨询服务。我们的专业人士能够帮助客户记录关键的业务流程、确认风险和降低风险的控制、分析表现差距，以及建议和执行行动计划以改善控制。

我们协助公司了解和评估有关以下项目的技术风险：

- 技术审计规划和风险评估
- 应用系统控制审核和内部审计
- 安全评估和内部审计
- IT流程控制审核和内部审计
  - 变更控制和管理
  - 安全管理
  - 数据中心的操作和问题管理
  - 数据管理和灾难恢复
  - IT资产管理

### 我们的技术风险咨询服务

#### 安全和隐私的处理方案

甫瀚从业务的角度处理企业的安全和隐私问题。我们首先会了解贵公司的核心业务流程、贵公司的行业、相关法规，以及用以支持贵公司当前和未来业务策略的技术，继而透过我们的专业知识和一个有组织的方案，包括经过验证的方法和工具，施行可持续的解决方案。我们的方案特点包括：

- 评估弱点及风险
- 制定政策
- 设计体系架构
- 施行解决方案
- 培养意识
- 监督合规工作

## 业务持续运作方案

甫瀚协助贵公司管理主要业务流程及技术资产的持续性和可用性。我们会按照贵公司的业务需要，根据经验证的流程建立一个解决方案。由危机管理到业务持续运作和信息技术灾难恢复，我们的专业人员均会帮助贵公司克服其自身缺陷，使业务蓬勃发展。我们的方案特点包括：

- 评估弱点及风险
- 设计及制定有关流程以维护可用性
- 执行有关程序并与业务的运作结合
- 对业务持续运作和恢复程序进行测试及验证
- 建立员工对灾难恢复能力的自信

## 变更管理方案

技术变更管理是指，由最初提出变更要求直至实施有关变更这整段期间，对技术环境中的变更进行管理和控制。甫瀚透过一致且可实施的程序，帮助组织管理信息系统中发生的建设性变更。我们的整体方案专注于协调性、效率和控制改善，从而将客户信息系统在可用性、可靠性、可扩展性、表现及安全性方面的风险减至最少。我们的方案包括：

- 评估当前状况，作为日后发展的基准
- 设计可实现贵公司业务目标的方案
- 采用有关工具，以实现有效的变更管理
- 将变更管理纳入技术操作管理
- 定义表现矩阵及执行有关机制，以报告和分析变更的根源

## 信息技术资产管理方案

甫瀚协助客户实现其信息技术资产价值的最大化。通过有效管理贵公司的成本、特许权协议、业绩表现及复杂的信息技术基础建设，贵公司得以从能够为公司带来价值的位置管理其资产。我们会与主要的软件公司合作发掘符合贵公司业务状况和目标的方案。我们的方案包括：

- 建立成本最优化的策略性计划
- 进行评估和根本原因分析
- 设计和执行处理方案
- 评估运作和表现

## 项目管理方案

甫瀚的项目风险管理服务为贵公司提供指示，以识别及减低有关管理、执行和控制的风险，并追溯这些风险的根本原因。我们为贵公司提供一系列的服务和工具，协助贵公司执行有关策略、流程和控制，从而改善贵公司的项目执行环境。我们可帮助贵公司有效地管理对业务的成功起关键作用的项目。此外，我们会将情况如实呈报，以便贵公司作出实时处理，以防延误。我们的方案包括：

- 评估风险管理及控制环境
- 设计及执行项目管理
- 管理整个企业范围内的项目
- 建立及执行办公室模板
- 进行执行前及执行后的审核

## 应用系统成效方案

甫瀚透过有效的方案管理，帮助贵公司取得成功。凭借我们的技术及在业务流程方面的专长，我们能够了解贵公司的业务目标，并识别有关风险。我们帮助贵公司降低现有应用系统的风险，以及帮助贵公司在执行新的应用系统时，设计相关的控制。

我们的方案包括：

- 评估公司具体控制的优先次序
- 评估与设计有关的控制及识别有关差距
- 观察及测试控制的运作成效
- 执行有关控制，帮助贵公司实现目标
- 设计有关方法和工具以监督持续成效

---

## 词汇表

Access Control – 权限控制

Authorization – 权限

Automated Control – 自动控制

Business Continuity – 业务持续运作

CMM (Capability Maturity Continuum) – 能力成熟程度模型

Compensating Control – 补偿控制

Cobit (Control Objectives for Information and Related Technologies)

– 信息及相关技术控制目标

COSO (The Committee of Sponsoring Organization of the Treadway Commission)

– 反虚假财务报告委员会成立的赞助组织委员会

Detective Control – 检测性控制

Disaster Recovery – 灾难恢复

ERP (Enterprise Resource Planning) – 企业资源计划系统

ISACA (Information Systems Audit and Control Association) – 国际信息系统审计协会

ITAC (IT Application Control) – IT应用系统控制

ITGC (IT General Control) – IT基础设施控制

ITIL (Information Technology Infrastructure Library) – 信息技术基础设施库

Manual Control – 人工控制

Mitigating Control – 舒缓控制

Preventive Control – 预防性控制

Public Company Accounting Oversight Board (PACOB) – 上市公司会计监管委员会

Security Administration – 安全管理

Walkthrough Testing – 穿行测试



甫瀚致力于提供独立的内部审计、业务及技术风险咨询服务，在业内处于领先地位。本公司帮助客户识别、评估及管理其在所属行业及其系统及流程中所面临的各种营运及技术风险。此外，本公司亦提供全面的内部审计服务，利用深入的技能及技术专长来实现业务风险管理及内部审计职能的持续转变。