

萨班斯——奥克斯利法案指南： 内部控制报告要求



关于 404 条款的 常见问题解答

精简版

protiviti®
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 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 **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

● 简介	P.1
● 404 条款的适用性	
1、404 条款对国外公司是否适用?	英文版常见问题: Q2 P.2
● 404 条款的内容及其与 302 和 906 条款的关系	
2、《萨班斯法案》404 条款与 302 和 906 条款有何关系?	英文版常见问题: Q20 P.2
● “财务报告内部控制”及“信息披露控制及程序”的含义	
3、何谓“财务报告内部控制”?	英文版常见问题: Q34 P.3
4、财务报告内部控制与信息披露控制及程序有何区别?	英文版常见问题: Q39 P.3
● 反虚假财务报告委员会成立的赞助组织委员会 (COSO) 内部控制 – 综合框架	
5、什么是 COSO?	英文版常见问题: Q41 P.4
6、什么是内部控制-综合框架?	英文版常见问题: Q42 P.4
7、COSO 框架在 404 条款评估报告中是如何应用于公司层面的?	英文版常见问题: Q43 P.5
8、COSO 框架在 404 条款评估报告中是如何应用于活动或流程层面的?	英文版常见问题: Q44 P.8
● 404 条款的实施	
9、就记录和评估对财务报告的内部控制而言, 公司应如何确定须审核的“重要领域”?	英文版常见问题: Q54 P.11
10、什么是“内控单位”? 为什么它们很重要?	英文版常见问题: Q56 P.11
● 确认申报要求及相关的流程	
11、管理层可否采用以风险为基础的方法来确定记录和验证内部控制的程度?	英文版常见问题: Q67 P.12
12、如何识别关键流程?	英文版常见问题: Q70 P.14

目录

● 确认、记录与评估控制

- 13、证交会有否就评估财务报告的内部控制向管理层提供任何指导意见? · 英文版常见问题: Q82 · · · P.14
- 14、证交会有否就记录对财务报告内部控制的评估向管理层提供任何指导意见?
· · · · · 英文版常见问题: Q83 · · · P.15
- 15、如何进行公司层面的评估? · · · · · 英文版常见问题: Q84 · · · P.15
- 16、如何考虑IT风险和控制? · · · · · 英文版常见问题: Q87 · · · P.16
- 17、如何进行流程或活动层面的评估? · · · · · 英文版常见问题: Q91 · · · P.18

● 运行成效的验证（控制测试）

- 18、建议使用什么样的方法“测试”财务报告内控的成效? · · · · · 英文版常见问题: Q119 · · · P.19
- 19、什么是“控制测试”? · · · · · 英文版常见问题: Q121 · · · P.20

● 报告

- 20、当管理层发现某控制缺陷可构成财务报告内部控制中的一个重大弱点时，即使该缺陷可在年底前被纠正，公司是否依然必须在公报中披露该缺陷？如果是，该规定何时生效？
· · · · · 英文版常见问题: Q167 · · · P.21

● 首次年度评估后的继续关注

- 21、首次年度评估完成后，管理层如何对从属于披露控制与程序的财务报告内部控制进行季度评估？
· · · · · 英文版常见问题: Q186 · · · P.21

● 管理层的角色

- 22、披露委员会的角色是什么? · · · · · 英文版常见问题: Q190 · · · P.22
- 23、披露委员会与项目指导委员会有什么关系？两者的职责范围有什么不同？两者应如何交流？两者的成员组成有什么不同？
· · · · · 英文版常见问题: Q193 · · · P.23

目录

● 内部审计的角色

24、内部审计在评估程序中的角色是什么? ·····英文版常见问题: Q204 ···P.24

● 独立会计师的角色

25、证交会对鉴证报告有提供任何指导吗? ·····英文版常见问题: Q208 ···P.24

26、在鉴证程序中, 管理层预期公司的独立会计师会开展什么样的工作? ···英文版常见问题: Q216 ···P.24

● 审计委员会的角色

27、审计委员会应怎样以及何时介入管理层的评估程序和独立会计师的鉴证程序?

·····英文版常见问题: Q226 ···P.25

● 国外编报公司及位置

28、国外编报公司需要符合302条款对执行人员声明的要求么? ·····英文版常见问题: Q246 ···P.25

29、根据截至目前为止从美国加速编报公司的经验, 对于刚刚开始为合规努力的国外编报公司来说有什么可以
作为借鉴?

·····英文版常见问题: Q247 ···P.25

30、美国以外的国家有关 404 条款的记录文件是否必须用英文编制? ···英文版常见问题: Q248 ···P.26

简介

美国证券交易委员会（以下简称“证交会”或“委员会”）# 于2002年8月29日颁布《2002年萨班斯法案》（以下简称“SOA”“法案”或“萨班斯法案”）其中第302和906条款规定了行政人员须进行核证的要求。这些核证要求成为公司提交的10-K及10-Q表格的核心，行政人员已在上述表格中就（其中包括）其财务报表的公允性及其信息披露控制及程序的成效发表多项公开声明。

302和906条款为投资者重拾对公开报告的真实性的信心奠定了基础。在此基础上，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，该报告还必须指出公司所聘请的独立执业会计师已鉴证了管理层对财务报告内部控制所做的评估，并对此出具了报告。此外，该内部控制报告须包含在公司的年度报告之中。证交会亦在404条款中规定公司管理层应就在最近一个季度中发生的有关公司财务报告内部控制的重大变化进行披露。

对许多公司来说，404条款无疑是一个挑战。因此，许多公司董事、提供声明的高级管理人员、高级经理以及审计人员在共同执行该条款的过程中会在许多方面有所疑问，而公司董事会及高层人员也可能需要独立顾问来帮助他们解决该等问题。

本书旨在回答您对《萨班斯法案》中有关公开报告的疑问，而毋需在一些已知的材料上浪费时间。此外，它还可协助404条款项目发起人、主管和小组成员在组织内的工作。本书所列问题都是我们在与客户、律师、审计师，以及其他有关人员的交流中发现的一些问题，我们已根据我们的经验对这些问题提供解答及意见，希望能够对公司记录、评估和改善财务报告内部控制有所帮助，并能改进行政人员的核证工作。我们亦已跟证交会工作人员进行讨论，了解证交会对一些关键问题的观点，以及证实我们对相关问题的诠释。

本书为中文版。该版本择录了英文版本的一些重要问题与解答。本书的原英文版本着重说明了证交会于2004年2月24日颁布的扩充规则对2003年6月发布的最终规则所作的修改产生的影响。书中包括国外编报公司和美国国内非加速编报公司所遇到的问题，并已根据公众公司会计监督委员会第二号审计准则的相关规定进行了相应更新，此外该书还包括其他一些经常反馈给我们的问题。同时新版本也反映了截止本书付印时，证交会和公众公司会计监察委员会就常见问题所作的回复。

甫瀚公司同时刊发了其它有关404条款的刊物，包括《内部审计指南：纽约证券交易所常见问题解答及建立有效的内部审计职能》及《萨班斯法案指南：信息技术风险及控制》（您可登陆 www.protiviti.com 获取该两本刊物的英文版。

本书并非拟作法律分析，也并非面面俱到。因此，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，同时也应该咨询公司独立审计师的建议。此外，公司应了解本书所涉及的某些问题会继续有所发展。您可以登陆 www.sec.gov 下载证交会发布的最终规则全文，以及证交会工作人员对常见问题所作的解答。您也可以登陆 www.pcaobus.org 下载公众公司会计监察委员会发布的第二号审计准则全文，以及其工作人员对常见问题所作的解答。

甫瀚

2004年8月

（注：甫瀚中国已于2006年1月根据有关公告对相关内容予以更新。。

404 条款的适用性

1. 404 条款对国外公司是否适用？

是的，国外发行商（包括加拿大发行商）都必须遵守该条款。然而，“国外私人发行商”（即按照 20-F 表格提交年度报告的非美国公司及按照 40-F 表格提交年度报告的加拿大公司）可以延迟执行该条款。非加速编报的国外发行商将于 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；而属于加速编报的国外私人发行商则须于 2006 年 7 月 15 日或之后结束的首个财政年度开始遵守该条款。404 条款最终规则重申外国私人发行商仅须在年度报告中（而非按季度标准）就其针对财务报告内部控制以及信息披露控制及程序的成效所作的结论进行评估和披露。该等发行商毋须遵守交易法中按季度报告的规定。

404 条款的内容及其与 302 和 906 条款的关系

2. 《萨班斯法案》404 条款与 302 和 906 条款有何关系？

302 条款和 906 条款包含两套核证要求，这些要求为恢复投资者对公开报告真实性的信心奠定了基础。404 条款正是基于这一基础。这三个条款和 409 条款（内容有关“信息的实时披露”）（以及《萨班斯法案》第四部份其它条款密不可分，共同组成该法案关于公开报告的内容。有关内容现总结如下：

302 条款、404 条款及 906 条款的比较			
	302 条款	404 条款	906 条款
生效日期	• 2002 年 8 月 29 日	截至下列日期或之后结束的财政年度： <ul style="list-style-type: none">• 2004 年 11 月 15 日（国内注册公司 - 加速编报公司）• 2006 年 7 月 15 日（国外私人发行商 - 加速编报公司）• 2007 年 7 月 15 日（非加速编报公司）	• 2002 年 7 月 30 日
签署人	• 首席执行官 • 首席财务官	• 公司管理层 • 独立会计师	• 首席执行官 • 首席财务官
内容	• 季度性行政人员的核证报告	• 年度内部控制报告 • 独立会计师出具的年度报告鉴证声明 • 季度变动回顾	• 季度性简明核证报告 • 刑事处罚
评估周期	• 季度评估	• 年度评估 • 季度变动回顾	• 季度评估

302 条款、404 条款和 906 条款（以及第四部份的其它条款）至少在以下两个重要方面存在联系：

- 首先，财务报告内部控制（由 404 条款规定）仅是信息披露控制及程序（由 302 条款规定）的一部份。证交会要求发行商维护并定期评估信息披露控制及程序的成效。该等披露控制及程序的设计旨在确保交易法规定须纳入报告的信息能够被及时地记录、处理、总结和呈报。

根据委员会的定义，“信息披露控制及程序”适用于公开报告中应包括的重大财务信息及非财务信息，以确保

投资者获得充分的信息。该定义比财务报告内部控制的范围更广。就财务报告内部控制会影响信息披露而言，公司的披露控制及程序明显包括上述内部控制，原因是信息披露控制适用于须包含于公开报告中的所有重大的财务及非财务信息，无论这些信息是否包含在财务报表之中。从这个意义上来说，“重大性”适用于投资者作出知情判断所需的所有信息。因而关于哪些是重大信息，哪些不是重大信息的描述对财务信息及非财务信息同等适用。

- 其次，《萨班斯法案》中有关公开报告的条款以及证交会颁布的准则的最主要的潜在信息是：不定期报告及披露活动的时代已经结束。财务报告的流程与为确保财务报告可靠而进行的有关内部控制应予以协调地执行，并应对其进行明确定义及施以有效的管理。呈列于财务报表以外的非财务信息的产生流程预计将趋于正规化，并与以流程为基础的方法更加一致。

有关披露控制及程序与财务报告内部控制的比较资料，请参考问题4。

核证人员签署其核证报告时，即代表他们掌握了或可以获得公司内任何投资者属重大的信息。实际上，他们应当就管理层的内部流程进行核证。因此，评估对财务报告的内部控制是核证过程中不可或缺的一部份。

“财务报告内部控制”及“信息披露控制及程序”的含义

3. 何谓“财务报告内部控制”？

证交会对“财务报告内部控制”的定义如下：

由发行商主要行政人员及主要财务人员或履行类似职能的其他人士设计或监督，并由发行商董事会、管理层及其他人员执行的一个流程，以确保财务报告的可靠性，并确保编制财务报表作外界用途时遵守公认会计准则。该流程须制定相关政策及程序以：

- 保存合理详细的记录，以准确及公平地反映发行商的交易及资产处置情况；
- 确保交易在必要时予以合理地记录，以便根据公认会计准则编制财务报表，并且仅在经发行商管理层及董事授权后，进行发行商的收支；及确保防止或及时察觉未经授权而又可能会对财务报表造成重大影响的收购、使用或出售发行人的资产。

上述定义与 COSO 框架的定义一致，此外该定义也包含萨班斯法案的内容，即最终责任将由公司的核证人员承担。该定义亦涉及对资产的维护，并参考了 COSO 在其综合框架首次公布后对其所作的补充。

证交会关于财务报告内部控制的定义并不包含公司运作的效果及效率以及公司对适用法律法规的遵守情况，惟直接有关财务报表编制的适用法律法规（比如证交会对财务报告的要求）的遵守例外。该定义符合《交易法》第 13 (b) (2) (B) 条中有关内部会计控制的内容。

4. 财务报告内部控制与信息披露控制及程序有何区别？

信息披露控制及程序包括财务报告内部控制中能确保交易按需要地被记录以便根据公认会计准则编制财务报表的要素。因此，总体上来说，财务报告内部控制是信息披露控制及程序的一部份。证交会在其 404 条款的最终条文中声明该两种控制及程序之间有重大的重叠部份。证交会根据国会的意图来区分信息披露控制及程序与财务报告内部控制：即要求高级管理人员确保所规定的重大财务及非财务信息均纳入公司的季度及年度报告。证交会拟使信息披露控制及程序概念相对财务报告内部控制概念可涵盖更多的非财务信息。同样，财务报告内部控制所涵盖（例如，合理保证在公司管理层和董事会的授权下才能进行收支业务）的项目并不一定直接涉及任何披露事项。

下面是财务报告内部控制与信息披露控制及程序的简单对比：

要求条款：		
公司管理层必须：	404 条款： 财务报告内部控制	302 条款： 信息披露控制及程序
总结公开信息的可靠性	财务报表	公众报告所包含的所有重大财务及非财务信息，包括财务报表
及时评估控制及程序	每年一次	每季度一次
进行审阅	年末	季度末或年末
记录评估以提交审计人员审核	每年一次	无
评估变动所产生之影响	每季度一次	每季度一次
在共同及相关流程中遵守 404 条款和 302 条款	与披露控制及程序披露有大量重叠	包含众多财务报告内部控制的要素
向公众报告	内部控制报告	有关人员的核证报告

反虚假财务报告委员会成立的赞助组织委员会（COSO）内部控制 - 综合框架

5. 什么是 COSO？

证监会规定管理层的评估标准必须源自一套合适的且已获认可的控制框架，且该框架的设立机构或集团必须已遵守各种必要的程序（包括广泛派发有关其框架的文件以征求公众意见）⁵ 根据最终条文的定义，“合适的框架”必须：不能持有偏见；能够对公司的内部控制进行合理及协调的质量上和数量上的测量；足够完整，以防止遗漏可能会改变公司内部控制成效结论的相关因素；以及与公司财务报告内部控制评估相关。证监会在最终条例中指出，COSO 内部控制 - 综合框架符合上述要求。委员会声称美国日后或会设立 COSO 框架以外的框架，使其在符合上述要求的同时不会影响投资者的利益。其它国家的其他框架或许也符合上述要求，例如控制标准委员会（COCO） 特恩布尔委员会（Turnbull） King 或者其它国家特有的权威框架。

COSO 是“反虚假财务报告委员会成立的赞助组织委员会”的简称，是一个自愿性的私人组织。该组织致力于通过商业道德、有效的内部控制以及企业管制，来提高财务报告的质量。COSO 成立于 1985 年，以协助独立私人机构美国全国反舞弊性财务报告委员会（也叫 Treadway 委员会）⁶ 该委员会研究可导致产生舞弊财务报告的各种因素，并为上市公司及其独立审计师、证监会及其它监管机构以及教育机构提供推荐意见。

赞助机构包括：美国注册公众会计师协会（AICPA） 内部审计师协会（IIA） 财务执行官组织（FEI） 管理会计师协会（IMA）以及美国会计协会（AAA） COSO 截止目前为止共已刊发两份文件，分别为于 1992 年刊发的“内部控制 - 综合框架”文件，以及于 90 年代中期刊发的关于衍生工具的文件。

6. 什么是内部控制 - 综合框架？

COSO 内部控制 - 综合框架将内部控制定义为“一套由董事会、管理层及其它相关人员实施的程序，以合理确保下列各项的目标得以实现：（a）财务报告的可靠性，（b）运作的成效和效率，以及（c）适用法律法规的合规性。”综合框架利用一个三维立体（如下图所示）为管理层提供评估内部控制的标准。

第一维是目标。内部控制的设计旨在确保下列各项的目标得以实现：运作的成效和效率（包括资产保护）& 财务报告的可靠性以及适用法律法规的合规性（图的顶部从左到右）（

COSO 规定第二维是公司级管理层面和活动作业层面（图的右面从前到后）\$ 内部控制必须从两个层面进行评估：公司层面，以及活动或流程层面。

第三维包括内部控制的五个组成部份（图的正面从下到上）：

- 1)=控制环境=J 控制环境确定了整个机构高层管理者的态度，影响员工的内控意识。该组成部份是内部控制所有其他组成部份的基础，提供了纪律要求和结构。
- 2) 风险评估=J 风险评估是识别及分析相关风险及其对公司目标实现的影响的工作，为管理层决定如何对风险进行管理设定了标准。
- 3) 控制活动=J 控制活动包括有助于确管理层的指令得到贯彻执行的政策及程序。
- 4) 信息与沟通=J 该组成部份包括若干程序和系统，以确保相关信息的确认、获取和交流必须在一定时间框架内进行，使员工能够各行其责。
- 5) 监督=J=包括定期评估内部控制质量的流程。

这五个组成部份为有效的财务报告内部控制提供了框架，同时，也为信息披露控制及程序提供了一个普遍通用的框架。五个组成部份为财务报告内部控制的评估提供了依据。

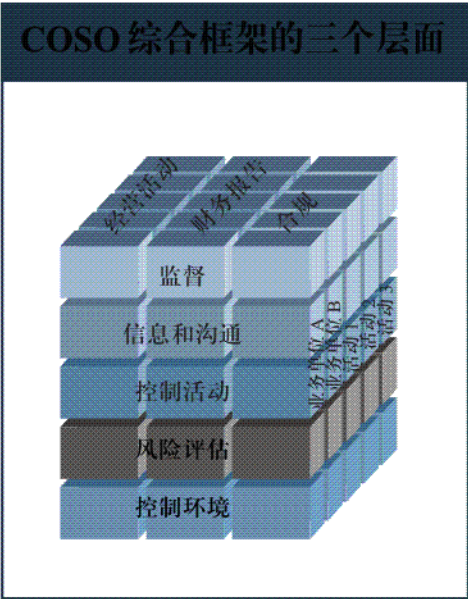
上述三个层面代表了整个综合框架。该框架按下述方式运作：对于任何既定目标，例如财务报告的可靠性，管理层必须同时在公司层面和活动（或流程）层面两个层面对内部控制的五个要素进行评估。

管理层必须选择一种控制框架，以作为对内部控制的成效进行认定及评估的基础。我们推荐使用 COSO 框架，它符合权威框架的要求，并且被人们广泛接受。证交会 404 条款也参考了 COSO 框架，并按照该框架来定义“财务报告内部控制”（自从 COSO 框架获颁布后，美国专业审计著作一直使用该框架。公众公司会计监察委员会发布第二号审计准则时，董事会重申 COSO 报告“为管理层对财务报告内部控制的评估工作提供了一个合适、可用的框架”\$ 符合《联邦存款保险公司改进法案》的银行已在使用 COSO 框架。

如管理层决定不使用 COSO 框架，则须选择另一种框架。无论管理层选择何种框架，有关框架均须符合证交会的规定。如公司选择 COSO 以外的框架，则管理层应将有关框架与 COSO 框架进行比较，以向可能会对有关框架提出质疑的外部审计人员和其它相关方证明有关框架已涵盖 COSO 框架的关键要素。

7. COSO 框架在 404 条款评估报告中是如何应用于公司层面的？

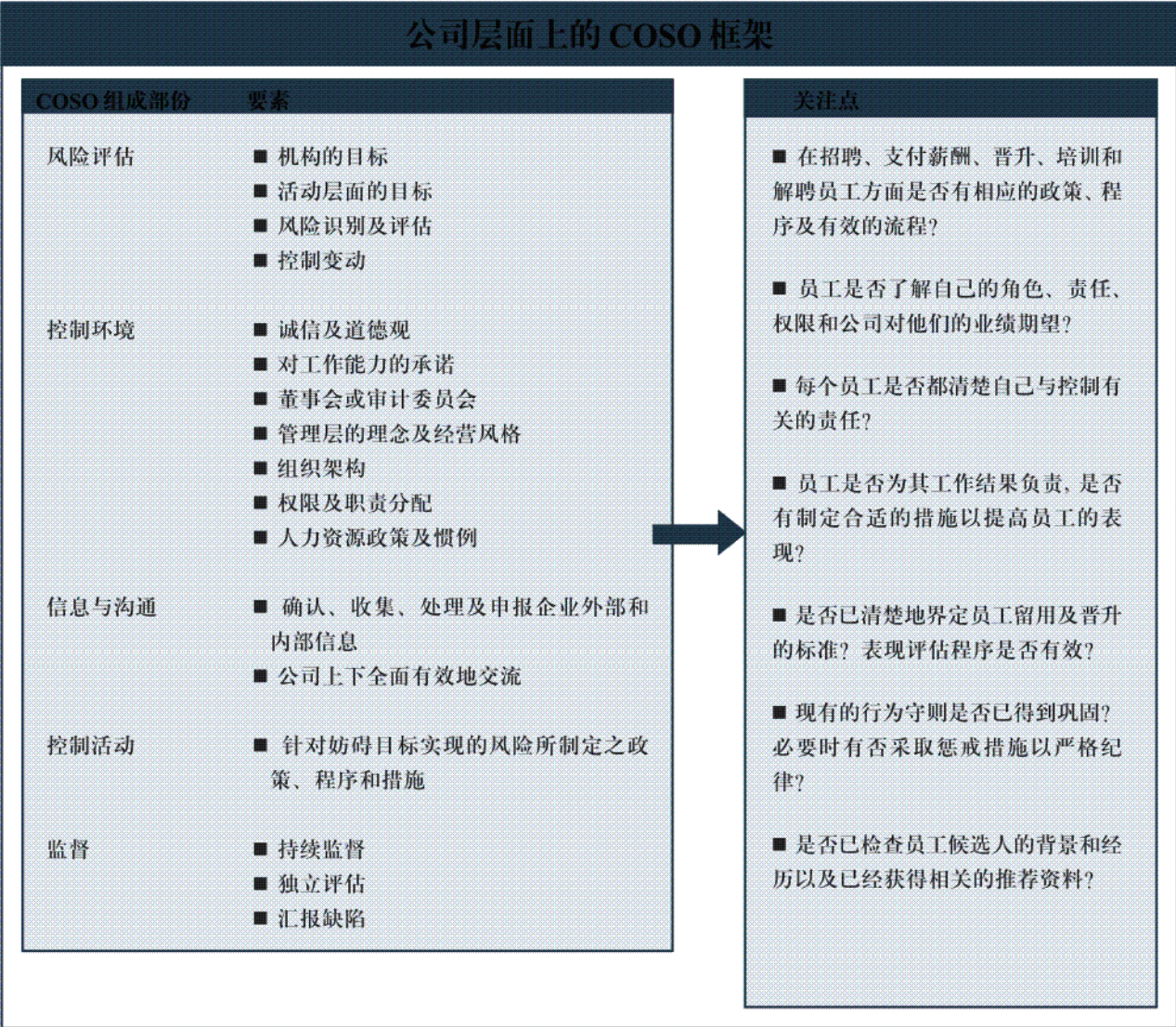
COSO 框架适用于两个层面 - 公司层面和活动（或流程）层面。对于公司层面，内部控制的五个组成部份的每个部份都被进一步细分为若干有利于评估进行的要素。“要素”界定每个组成部份的性质。正如下图所示，控制环境进一步采用七个要素进行界定。对于每一个要素，COSO 都提供适当的“关注点”# 代表与此要素有关的一些更为重要的事件，但并非所有关注点均适用于每间公司，或许其他的关注点更适合某些企业。就



资料来源: COSO 内部控制 - 综合框架

控制评估而言，COSO 建议每个企业都应该根据其实际情况和环境制定合适的关注点。例如，管理层较多参与公司实际经营的小型公司跟管理层架构较复杂的大型公司比较起来，就需要采取不同的评估方法。

公众公司会计监察委员会将公司级管理控制称为“公司层面控制”& 管理层可依赖该等控制，建立与财务报表相关的合适的“机构高层管理者的态度”* 该等控制通常会对流程层、交易层及应用层的控制的有效性产生深远的影响。对于公司级管理，管理层必须重视 COSO 为每个组成部份提供的要素。下表载列了五个组成部份的要素，同时列出了其中一个要素的关注点 - 人力资源政策及程序：



资料来源: =`lpl 内部控制-J=综合框架, 框架及评估工具

根据以上的例子引申下去，人力资源政策及程序的制定宗旨是聘用及挽留有能力实现公司目标，并能贯彻实行公司行政策略的员工。上述人力资源政策及程序的关注点仅作说明用途，并不是一个概括性的清单。正如前文所述，管理层应制定符合本公司需求的关注点，也就是说，管理层可对上述关注点进行增加、删除和修改。同时，管理层可对每个关注点增设一些特定的问题或事件。例如，上表中的第一个关注点是“在招聘、补偿、晋升、培训和解聘员工方面是否有相应的政策、程序及有效的流程？”对于此关注点，更细微的标准可能包括（但不限于）：

- 人事政策应获得有效实施，以（a）聘用或培训有能力且诚实的员工，以及（b）鼓励及奖励该等员工支持有效的内部控制系统。
- 现有聘用或提升有能力且可靠的员工的人事程序及流程符合有关政策，且被有效地实施。
- 现有鼓励及奖励员工支持有效的内部控制系统的人事程序及流程符合有关政策，且被有效地实施。
- 着力于聘用合适的员工并培训他们从事合适的工作。
- 管理层定期就所招聘员工应具备的特质进行交流。
- 人事政策应确保能够向工作上困难的员工提供咨询，以及解雇或处罚工作业绩未能达到标准的员工。

对于上述有关 COSO 框架应如何应用于公司层面的陈述，现总结如下：

- 对于五个组成部份中的每个部份，COSO 都制定了不同的要素。
- 对于每个要素，COSO 都制定了关注点。
- 对于每个关注点，都可以进一步制定更细微的标准来支持评估。

在公司层面实施评估需注意以下几点：

- COSO 的建议如下：
 - 记录对每个关注点而非更细微标准的回复。有关回复应基于管理层对有关政策、程序、人才、报告、方法及系确实存在，且正有效地实施的结论。
 - 回复不应仅仅是回答“是”或“不是”而应具体说明公司针对有关关注点所进行的工作。
- 管理层应就内部控制每一组成部份的每个要素的内部控制的成效作出总结。如上文所述，为各个关注点提供信息的答复能够支持管理层就各要素作出结论。为说明起见，管理层应就控制环境七个要素中的每个要素作出总结，包括人力资源政策及程序。
- 应就每个 COSO 组成部份作出全面总结。该全面总结应在对每个相关要素总结的基础上得出。因此，管理层便可对控制环境的有效性得出结论，惟结论的得出应基于对控制环境的各个要素所作的结论。
- 若有关某一要素的回复是“无效”或“有待提高”，这并不一定意味着公司层面的相关组成部份为无效。在其它区域也可能有相应的补偿控制措施。
- 若有关某一要素的回复是“无效”或“有待提高”，管理层应评估其内部控制是否需要改善，并采取措施减少差距。如管理层认为缺少一个或多个会导致重大控制风险的关键控制程序，则应尽快采取相应的解决办法。此外，管理层应将类似可构成重大缺陷的情况告知审计委员会以及独立会计师。

根据申报企业（也就是证交所说的“发行商”）划分其控制部门方法的不同，上述要素及关注点可能适用于其中一个部门但并不一定适用于其他部门。管理层必须考虑就各控制部门控制环境所作的所有评估，方能就公司整个控制环境得出全面的结论。

例如，某申报企业的综合报表涉及若干运作较独立的部门。假定该企业的每个运作部门均代表一个控制单位，那么就评估其控制环境而言：

- 申报企业可通过在全公司设定一系列道德规范来确定高层管理者的态度，并监督有关的遵守及

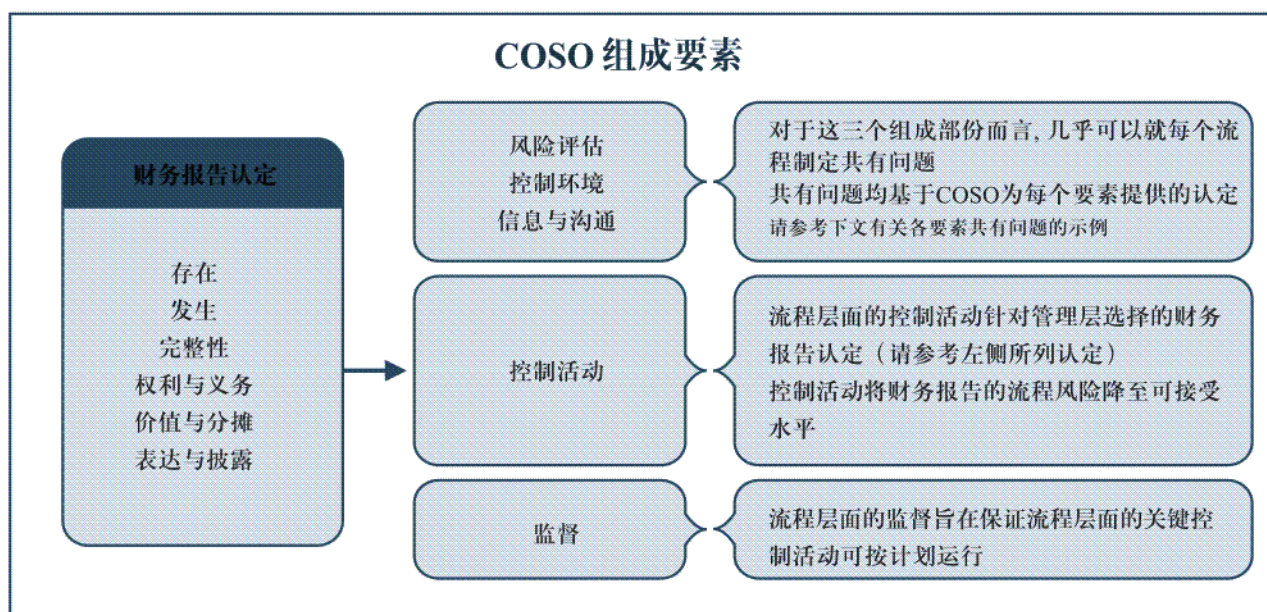
执行情况（比如“诚实及道德观”要素）！董事会及审计委员会应就公司层面的申报工作进行交流（控制环境的另一个单独要素）* 申报企业应制定组织架构（另一个单独要素）’提供全面的人力资源政策（要素的一部份）% 等等。

- 作为控制单位的各个运作部门应针对控制环境的其它要素，比如提高员工能力的承诺、公司管理层的经营风格、权限及职责的分配等。
- 公司管理层应考虑对所有该等部门的评估报告，从而对整个公司的控制环境作出评估。整体评估概括了各公司层面评估的影响。

总结：公司高层管理人员对综合报告企业的控制程度、企业营运及业务单位的性质和种类、有关营运及业务单位的固有风险，以及其他因素，均会影响项目小组评估公司层面控制的方法。

8. COSO 框架在 404 条款评估报告中是如何应用于活动或流程层面的？

正如COSO框架应用于公司层面，COSO框架也可应用于活动或流程层面。在评估财务报告流程层面控制的“设计成效”及记录相关评估时，COSO 的五个组成部份将如下图所示予以考虑：



从实际角度来看，审核财务报告的内部控制时，流程层面着重于控制活动和对该等活动的监督。在有关财务报告可靠性的认定获得共识并被记录后，控制活动将直接专注于该等认定，而监督则确保控制活动可按计划进行。

- **控制活动**是业务流程正常运作不可或缺的一部份。控制活动包含在各流程之中，合理保证错误及不规则的事件可在接近来源的地方被预防及发现并保证达致有关认定。流程层面的控制活动是专门针对财务报告认定或风险的内部控制。控制活动应包含于流程，将“财务报告流程风险”降低到可接受的水平。财务报告认定及实现该等认定所涉及的风险（* 为评估流程层面控制活动设计的成效提供了一个依据。
- **监督**专注于评估控制活动的执行情况及流程的结果，以确保有关控制活动符合公司的目标及有关流程既定的执行标准。监督包括持续监督和独立评估。

所进行的控制活动应合理地保证管理层的财务报告目标或认定得以实现。管理层必须对控制活动的设计及运行的成效进行评估：

- 对设计成效的评估将确认控制活动是否能够保证减少已识别的风险，以及实现上述财务报告认定。
- 对运行成效的验证将说明控制活动是否能够如预想的那样发挥作用（例如，该等控制活动是否如设计的那样进行）§

在流程层面，监督将针对流程中主要控制活动的成效，以及控制环境、风险评估及信息 / 沟通等组成部分的成效。监督包括持续监督和独立评估。持续监督来自日常管理及监管活动、比较、调节，以及日常业务过程中就内部控制的成效持续提供反馈的其他正式及非正式机制。持续监控的示例包括：

- 监管人员和流程负责人进行每日监控
- 建立追踪来自外部的信息的正式流程，以改善内部流程，例如客户对帐单的投诉有助纠正发单系统中的缺陷
- 将实物资产与帐户资产进行比较，例如实物存货可导致帐面到实物的调整
- 积极追踪透过计划会议、雇员建议系统及定期培训收到的反馈意见
- 定期报告，例如，例外及“接近出错”报告，审计报告，界限违反报告，以及有关改善措施现状的报告
- 财务系统内建立的分析程序，以正确处理数据或“剔除”未能符合遴选标准的数据

高级管理层和业务单位管理人员、流程负责人，以及内部审计人员会定期检查内部控制（包括持续监督程序）的组成要素，以评估其成效。该等措施被称作“独立评估”§ 内部审计是一个普遍的例子。

监督需要用以发现、报告及追踪缺陷的原则及流程，以确保能够及时地解决所有重大缺陷及潜在的重大缺陷。

上述讨论着重于活动或流程层面最常见的两个 COSO 组成部份 - 控制活动及监督。就风险评估、控制环境及信息 / 沟通三个部份而言，可以创建应用于活动或流程层面的共有问题，以支持于相关层面对该等组成部分进行评估。为说明起见，下文载列适用于上述三个组成部份各部份的共有问题的示例，而该等示例亦或会适用于几乎所有流程。

风险评估

业务流程均面临来自外部或内部的风险。该等风险必须根据其对实现流程目标的影响来进行评估。流程负责人必须制定一套流程，或参与某个既定流程，以有效地确认及评估内外环境中会对流程目标的实现构成威胁的风险。

谨请注意以下问题：

- 流程负责人是否已制定了与报告机构或业务单位管理层所制定的整体目标相一致的流程目标？
- 流程目标是否清楚并足够详细地说明流程的设计宗旨？该目标与其它流程的目标是否一致（且不冲突）？管理层是否参与了流程目标的制定，尤其是那些对报告机构或业务单位的成功起关键作用的目标？
- 流程负责人是否拥有充足的资源以实现上述目标？

- 流程负责人是否拥有有效的程序，以（a）识别来自内部和外部会影响主要流程目标实现的重大风险；（b）评估风险的重要性和这些风险出现的可能性；及（c）评估可将这些风险降低到可接受水平的其他措施？
- 流程负责人是否会持续地预测、确认可能影响流程目标实现的常规及不断变化的环境和因素，并对其作出反应？
- 流程活动是否依赖已识别、处理及呈报的信息的完整性和可用性？如果是，那么流程负责人是否已对有关该信息的安全性、完整性和可用性的风险进行评估？

控制环境

流程负责人必须建立有效的控制环境，以为流程中的控制提供纪律要求、架构和强大的基础。控制环境包括流程负责人和负责执行该流程的其他人员，以及他们的工作环境。控制环境确定了流程有效运行的基调，影响所有参与该流程的员工对内部控制意识。控制环境是流程内部控制中所有其它组成部份的基础。

谨请注意以下问题：

- 流程负责人是否有一个有效和易懂的框架，可以（a）有效地促进监控及（b）使纵向和横向的信息交流畅通无阻以实现流程目标？
- 流程负责人阐述及说明角色、责任、权限和职责时所采取的方法是否符合机构或业务单位的既定政策？负责重要流程活动的个人是否对于恰当的政策、工作表现期望和既定职责均有准确的了解？
- 流程负责人有关聘用及挽留人才及培养人才的政策和惯例是否有清楚的界定？以支援流程目标的实现，同时符合机构或业务单位现有的人力资源政策？
- 就接受风险和促进经理与雇员之间的沟通而言，流程负责人是否保持积极的经营风格？而就财务报告而言，其又是否持有与高级管理层态度一致的支持态度（有恰当的行为为证）？
- 流程负责人是否已透过其举措或沟通向员工清楚地说明公司的诚信及道德观是流程执行过程中不可或缺的一部份，且绝对不容有失？

流程负责人是否已就内控负责人及其他雇员管理的包括以下领域的信息技术的政策与程序进行记录与沟通？

- 是否有对可支持流程的关键应用程序及数据文件的获取进行控制（包括尽量减小可支持流程的系统被电脑病毒入侵的可能性）？
- 是否有授权、记录、测试及有控制地实施可影响流程的新型应用程序及应用程序的任何变动？
- 是否有对所有支持流程的关键应用程序及数据文件进行适时备份和恢复的程序？

信息 L 沟通

要了解外部环境和机构业务流程的现况，必须首先获取相关的可靠信息。正确的实施措施和有效的沟通对确保内部控制的重要信息在整个流程中的有效传达和管理至关重要。

谨请注意以下问题：

- 流程负责人是否致力于创建必要的信息系统，以确保所有相关信息被适时获知、准确记录、处理和报告，从而能在财务报告中对其进行分析、评估及使用？

- 流程负责人是否有能力在高级管理层的帮助下从外部资源获取足够的信息，从而能够对环境改变给流程带来的影响、流程自身的执行以及有关执行的信息进行评估？例如，是否有关于客户需求、竞争、科技和监管环境，以及经济与产业整体趋势及状况的信息？
- 流程负责人能否获取机构有关环境及趋势变动的信息，而该等信息又会对流程的执行产生影响？
- 流程负责人是否决定将相关的、适时的信息详细地提供给控制负责人和其他流程工作人员，以确保他们履行自己的职责？
- 流程负责人是否有效地（a）与控制负责人及其他流程工作人员就流程目标进行沟通，（b）帮助流程中的沟通并与代表其它机构和业务单位的工作人员沟通，及（c）支持控制负责人和其他流程工作人员的相关工作程序，以将有关流程执行及控制的问题传达给上级？

404 条款的实施

9. 就记录和评估对财务报告的内部控制而言，公司应如何确定须审核的“重要领域”？

项目小组可根据管理层所选及所批准的标准将财务报告要素分级。这些要素包括单个报表项目或几组相关的报表项目（如应收帐款和销售额）以及财务报表中的附注披露信息。许多审计师认为已出版财务报表中的所有报表项目及文字说明以及所有附注披露均属重大。此外，在将财务报表中的报表项目及披露信息细分为具体的项目和要素时，许多审计师也要求采用定量重要性评估方法，即超出界定定量标准（有时称作“计划重要性水平”# 的所有项目与要素必须纳入界定范围。细分过程中，还必须考虑受面临不同风险和内控的不同交易所影响的会计项目和要素。

财务报告要素的分级基于单项重大错误（或多项重大错误的共同作用）可能会对财务报表产生重大影响的风险。此外，还应确认最可能出现财务错报或披露不及时的项目，比如收益确认、或然亏损、资本支出等等。相关信息应由管理层和审计委员会提供，并由管理层批准通过。根据证交会指南，许多审计师首先采取定量措施确认重要的财务报告要素，然后再采取定性措施确认也应纳入细分范围但低于定量标准的其它次要要素。定性考虑这样就成了辅助工具。

界定范围的结果应由独立执业会计师进行验证。实践已经证明，与审计师保持“界定对话”通常都会导致公司将先前未纳入细分范围的额外会计项目重新纳入进来。考虑到界定的判断性质及披露被细分为特定的会计项目的特点，如此这样的反复“给予和接受”也就可以理解了。

10. 什么是“内控单位”？为什么它们很重要？

“内控单位”是指在制定业务目标和管理日常营运方面相对独立的业务单位、部门、附属公司或共同经营区域。由于风险类型、业务性质以及管理层的偏好、价值判断、经营风格以及交易量不尽相同，所以不同单位的控制环境也各不相同。这种相对自主通常令单位管理层设立一系列的内部控制措施，他们在公司管理层面采取措施与否都可能会影响单位流程层面上内部控制的执行。

许多公司都拥有可共享的服务业务，其中涉及管理关键职能（例如 IT，工薪和应付帐款）的能力及系统。由于这些服务业务通常被视为独立的控制单位，所以管理层在决定有关控制措施时还应考虑这些共享服务业务的性质和覆盖范围以及在近期内拓展这些业务的计划。

此外，许多公司也将其某些重要的程序及职能外包，尤其在 IT 行业。证交会以及公众公司会计监察委员会均

财务报告要素的优先排序可以通过对下面两项的评估完成：

- 首先是线性报表项目或说明、报表项目结余，或有关财务状况、经营业绩和现金流量申报的披露的重要性水平。评价重要性水平时，须考虑上述各项对公平呈报及投资者充分理解财务报表的重要程度。
- 第二，错报和遗漏的风险。该评估过程应考虑以下因素：可能会发生的错误和遗漏的性质和种类（例如“会出现什么样的错误”）* 账目金额中存在的因素，通过监控和分析活动可靠地预测结果以及检测错误的能力，选定账户处理交易的数量和规模，计算的复杂程度，出现重大错误或遗漏或舞弊或损失的可能性。

评估具体的报表科目时，可以把受类似交易流程影响的报表科目合并起来。这些报表科目通常具有相似的风险特性，所以也通常可以采用相似的控制措施。

对财务报告要素进行优先排序时应考虑下列其它因素：

- 确定重要会计估计方法的主观性与可靠性
- 企业业务变更的程度，以及其对内部控制的预期影响
- 财务报表中存在潜在重大错误或遗漏之外的风险，例如，非法行为、利益冲突、管理层未经授权使用公司资产等
- 公司曾经出现过的或行业内普遍存在的问题报表项目，例如收益确认、储备计算等
- 管理层是否要求记录那些与一般不会出现重大错报且可以被合理预测的会计科目相关的流程。例如，对大多数公司来说，工资是可以合理预测的，但其在销售成本和一般管理费用中占有相当大的比重，因此，鉴于对有关工资的活动进行管理和控制的需要，管理层或会要求记录与工资相关的流程及内控。

财务报告会计科目和披露事项的优先排序完成后，就要着手准备进行恰当的记录、评估和验证活动。上面的图示含有一份有关记录、评估和验证的标准示例。重要的财务报告要素须给予最多的关注。如果有效的分析及公司层面的监督可以确保报表项目及披露能够被公正和公平的呈现和陈述，那么较不重要的财务报告要素在公司层面上则需要较少的测试，而对于不重要的财务报告要素来说，记录要求则最低。

总之，要牢记以下四点：

- 上面的图示仅仅是一个例子而已，高级管理层和项目小组必须制定对财务报告要素进行优先排序的方法。
- 用“报表科目组”取代个别报表科目可以使优排序过程更为顺畅。例如，销售额、收益扣除额，销售成本、销售费用、应收账款和产成品都受到常规收益交易的影响。
- 将受个别交易流程影响的会计科目进行分类。
- 最后一点，但也是很重要的一点，要理解独立执业会计师的期望和要求，尤其是有关界定过程中重要性的定义和应用。界定结果必须得到独立会计师的同意。我们发现外部审计师有时会坚持将管理层依据风险评估决定界定于外的财务报告要素重新纳入界定范围。鉴于该流程需要作出判断的性质，这种与审计人员的重复对话将时有发生。

12. 如何识别关键流程？

关键的财务报告要素获确定之后，管理层必须确认影响这些要素的流程。对主要财务报告要素有重大影响的流程为关键流程。可以采用下面两种方法来确认这些关键流程：

- 一种方法是针对会对关键财务报告要素产生重大影响的交易和相关会计系统，总结其主要的交易流程。这可以通过将业务和相关会计系统分割成数量有限但相互联系的交易流程来实现。该等交易流程是机构直接与外界进行交易时所发生的类似经济事项。收益、采购、薪金、换算、财政和财务报告均属于这种交易流程。
- 另一种方法是将业务分割成其实际的流程。理想的情况是有关流程分类方案是现成的。业务被分解成不同的流程后，项目小组就要确认关键流程，以审核相关风险和内部控制。关键流程的确认须根据它对财务报告（或者业务）的重要性、出现内控缺陷或者流程发生问题的可能性来进行。这样，关键流程便与主要会计科目及披露事项联系起来，从而建立其与财务报告的相关性。

上述两种方法均可行。第一种方法可能更有效，原因是这种方法完全集中于支持管理层有关主要财务报告要素的认定所需要的信息，而第二种方法则超出了最低要求，并根据业务来记录相关流程，因此更具增值潜力。

需要铭记于心的是，即使所有的核心业务流程均已有所涵盖，也可能不能满足外部审计人员的要求，原因是他们对重要性的定义和应用可能会使他们认为仍然存在其他需要分析的财务报表会计科目或组成。这些额外的会计科目或组成可能来自具有不同风险及内部控制或者超出审计师计划的重要性水平的其他类型的单独业务，甚至管理层认为它们不必作为核心业务程序一部份。然而，它们可能对财务报告来说很重要。例如具有不同特点的收入（例如产品销售收入与服务收入，账面销售收入与销售型租赁或现金销售收入，零售销售收入与通过配送中心进行的直销等等）必须分别进行评估。

确认、记录与评估控制

13. 证交会有否就评估财务报告的内部控制向管理层提供任何指导意见？

有的。尽管最终条例并未规定财务报告内部控制评估过程中应采用的具体方法或步骤，但证交会提供了一些概括性的指导意见：

- 进行财务报告内部控制评估的方法应该针对不同公司的具体特点而定。例如，公司测试活动的性质主要取决于公司的实际情况和控制的重要性水平。
- 对公司财务报告的内部控制进行评估必须基于充分的程序，以评估内部控制的设计及测试内部控制的运行成效。需要进行测试的控制包括（但不限于）：
 - 与建立、授权、记录、处理和调节报表项目结余、交易分类及披露事项以及财务报表中包含的相关认定有关的控制
 - 与建立和处理非常规性和非系统性业务交易相关的控制
 - 与选择和应用适当的会计政策相关的控制
 - 与防止、确认和检测舞弊行为相关的控制
- 单独的查询工作一般不能为管理层进行评估提供充分的基础。

鉴于上述指导意见的概括性，管理层应制定一个全面的测试计划，并与独立审计师讨论该计划。

14. 证交会有否就记录对财务报告内部控制的评估向管理层提供任何指导意见？

是的，证交会有提出一些指导性意见。尽管最终条例并未规定评估财务报告内部控制应采用的具体方法或步骤，但证交会提供了一些概括性的指导意见：

- 在对财务报告内部控制的成效进行评估时，公司必须保存与设计过程和测试过程相关的证明文件。这些文件为管理层对公司财务报告内部控制有效性的评估提供合理的证明。建立和保存这些证明文件是有效内部控制的必要因素。
- S-K 和 S-B 法令第 308 条款以及 20-F 和 40-F 表格已加入提醒上市公司保留这些证明文件的指示。
- 证明文件，包括记录的文件，必需能为内部控制设计和测试程序的评估提供依据。证明文件应为下列各项提供合理的依据：
 - 就控制的设计是否能预防或检测到重大的错报和遗漏进行的评估
 - 测试已经过适当的规划和实施
 - 测试结果已被适当考虑

独立会计师须就管理层对公司财务报告内部控制成效所作的评估进行核实与申报，而该等独立会计师也会要求公司建立并保存这些证明文件，以支持管理层的评估。因此，在项目初期征求审计师有关记录标准的意见乃明智之举。

15. 如何进行公司层面的评估？

在评估流程中对公司层面的评估应该尽早进行。如果公司层面的控制存在重大问题，那么这些问题应尽快被发现并更正。如果公司层面的控制很强，并于各具体领域实施有效的分析和监督，那么这在项目的范围划定阶段就应该予以考虑。这样的控制可以降低对流程控制的依赖性，也可以降低测试要求。

如结论是公司层面的控制较弱，这对于完成评估而言可能会是一个非常棘手的问题。独立执业会计师可以对是否存在较强的公司层面的控制环境做出“合格/不合格”或者“通过/不通过”这样的决定。较弱的公司层面的控制将会造成对流程控制的依赖性以及测试要求的提高。

公司层面的评估可以被细分为四个步骤进行。这些步骤讨论如下：

定制公司层面的评估 - 项目小组根据企业所处的具体环境灵活应用 COSO 框架。可以使用管理层或者其它公司开发的工具完成相应的定制程序。一个典型有用的工具是一份与 COSO 组成要素和属性相关联的诊断调查问卷。

评估方法和定制化诊断一经完成，独立执业会计师就应对评估方法和计划进行审核。

COSO 的五个组成部份构成了在公司层面对财务报告内部控制进行评估的框架。COSO 的每个组成部份都有与其相对应的要素，而对于每个要素都有与其相对应的关注点。了解该等术语是充分理解以下讨论内容的前提。

评估公司层面的整体控制 - 项目小组从访谈核证人员（首席执行官和首席财务官）开始展开评估工作，以获得他们对公司层面的控制的观点，尤其是他们对控制环境的观点。讨论的主要内容集中在验证评估的方法和如何开展评估上。对于组织内的每一个“控制单位”，项目小组都应访谈各单位的经理以评估公司层面的控

制。对于每个关注点而言，项目小组应该从证据的本质和种类角度出发请求管理层提供相关的证据，用以支持所述控制的确存在。作为一个额外的步骤，项目小组可以请求管理团队中的特定成员使用定制化的评估工具进行自我评估。如果调查对象的数目比较庞大，项目小组应该考虑使用网络技术。作为一个替代性的步骤，项目小组应该考虑通过设立互助小组的方式与各单位经理一起工作。不管通过何种方式评估公司层面的整体控制，目标是记录那些现实存在的公司层面的控制。

收集支持性证据 - 对公司层面的控制进行的整体评估是主观性的而且需要相当多的人为判断。致使管理层和其它工作人员作出某选定要素为有效结论的评估需要相关的支持证据。评估公司层面的控制时，项目小组可以考虑可显示财务报告风险存在与否的风险指标进行判断。例如，是否有一位占绝对领导地位的首席执行官，高级行政人员是否生活奢靡？绩效期望值是否不切实际，投资或贷款是否都集中于高风险领域？管理层是否接受行业内不寻常的重大风险，等等。然而，对风险指标的评估比对政策、流程、人才、报告、方法论和系统的评估更为主观，而后面这些因素则极易受到独立验证的影响。项目小组应该制定并执行一项计划，以获取、记录及评估可以支持公司层面控制的证据。

评估对流程层面的控制的影响 - 当所有的评估完成以后，管理层对汇总后的结果进行评估，并对公司层面控制的每个 COSO 要素的成效作出结论。项目小组应该确定，管理层根据各要素的检测结果及有关证据作出总体结论。

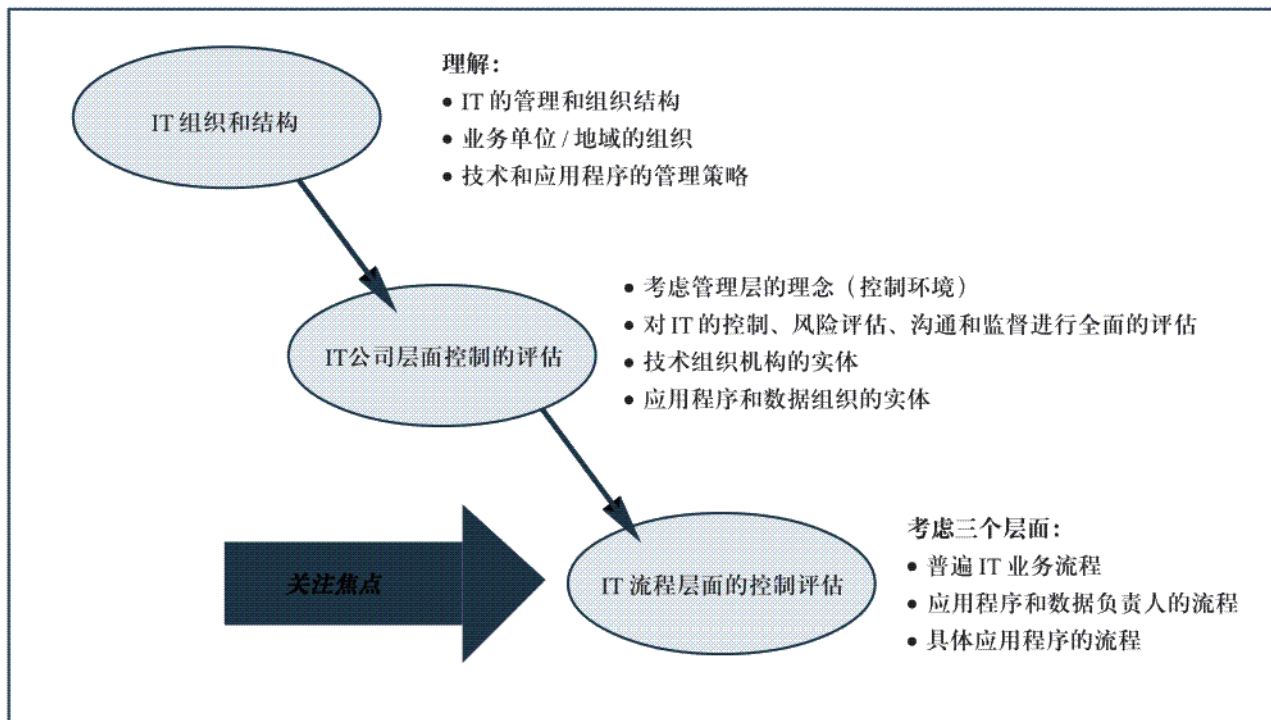
根据评估和验证结果，得出公司层面的控制为有效这一结论，可以减少对不易产生重大错报领域内的流程、风险和控制的记录。然而，对于公司层面控制负面的评估结果需要进行仔细的权衡，原因是这样的评估结果可能表明内部控制中存在一个或者多个重大缺陷或实质性缺陷。管理层应该将有关情况告知审计委员会和独立执业会计师。

公司层面的审核完成后，管理层应该与独立执业会计师一起对总体结论、有关支持性证据以及对流程层面的控制评估造成的影响进行审核。管理层与独立执业会计师定期就检查结果进行交流可防止日后出现意想不到的情况。

16. 如何考虑 IT 风险和控制？

甫瀚同步出版的《萨班斯 - 奥克斯利法案指南：IT 风险及控制》一书中对该问题进行了更为详细的讨论。书中介绍了一种概括性的方法，可将有关 IT 风险和控制的考虑纳入 404 条款的合规项目中。该方法的描述如下：

IT 评估应按下图所列顺序进行，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。例如，理解“IT 组织和结构”的第一步是理解 IT 的组织架构（例如，集中型与分散型，共享服务，业务单位联盟，地域联盟等等）\$ 管理结构和报告事宜，以及单位的 IT 前景。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到对 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。下面是对每个层面简要的讨论：

- 普遍 IT 的业务流程 - 普遍 IT 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。普遍控制通常会对技术环境内众多的个体应用程序及信息有影响。一般来说，因为这些控制会影响相关程序和数据的安全性，所以最终会影响财务报表认定的实现。几乎在所有情况下均应予以评估的普遍 IT 流程包括：

- 安全管理
- 对应用程序的改变进行控制，以确保应用系统的变化（通过系统开发、升级和维护实现）在实施前已获授权、测试及批准
- 数据管理与备份 / 恢复
- 数据中心的营运及问题的管理
- 资产管理

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普遍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。

- 应用程序和数据负责人流程 - 这方面被评估的是那些直接被应用程序和数据负责人控制和管理的程序。一般来说，应用程序和数据负责人是业务流程的一部份，从控制设计和业务操作的角度来说，他们对整个企业的业务流程负责。流程总负责人可以将有关权责委派给他人，但是流程负责人必须与获委派人进行充分沟通，使之明白所委派的权责。应用程序和数据负责人必须负责理解、设计和维护相关应用程序范围的控制。这些人员必须了解计算机化控制，以便能从专业的角度设计控制点并与 IT 工作人

员就相关需要进行交流。应用程序和数据负责人员也需要了解计算机化的控制的局限，并能帮助设计检查性和监控性控制，以帮助弥补若干 IT 流程一般控制中存在的缺陷。

就完成 404 条款的合规项目而言，通常应予以评估的流程包括建立和维持不相容职责的分离（安全角色和管理）同时也包括确认 / 审核对关键交易和数据的存取。这些流程确保关键的 IT 组成部份及应用系统和数据的存在，从而保证唯有已获授权的人士和应用程序方可使用有关数据并执行某项指定职能，而这直接关系到对资产认定的授权和存取。应用程序和数据负责人在应用程序开发和维护过程中也扮演至关重要的角色，他们工作的成效也应作为程序的一个部份予以评估。

- **综合应用程序 - 特定流程 - 应用层面的控制**包括企业业务流程中的应用程序控制、信息获取控制（用于关键业务和数据的获取）数据验证和错误检查程序以及错误报告等各种控制。该等控制也包括对复杂运算、关键接口及流程中其他方面的控制，以确保报告的完整性和精确性。负责人员应对每个重要业务流程中关键财务应用程序的控制有充分的了解。对业务流程层面的所有 IT 控制和人工控制综合进行评估尤为重要。评估中有关 IT 的部份主要集中在对关键应用程序的控制。在对企业业务流程进行评估时亦应评估有关的 IT 风险和控制，从而全面了解控制环境。

《萨班斯 - 奥克斯利法案指南：IT 风险及控制》一书对上述三个方面均有更详尽的描述。在对内部控制进行评估时必须仔细考虑 IT 的影响。例如，如果管理层依赖程序化的控制（对于程序的结果只进行了有限验证或者没有任何用户验证）或者某项关键控制依赖由 IT 系统所产生的数据，那么在评估依赖 IT 系统或 IT 系统所产生的数据的流程层面控制时，总体 IT 控制的成效是须予考虑的一个重大因素。

在评估过程中，IT 人员和 404 条款合规项目小组会就与 IT 相关的风险以及 IT 控制的成效进行评估，同时亦会说明支持证据的性质和类型。在与合适的 IT 人员的协同工作下，合规项目小组必须有计划地获取、记录、评估和验证相关的支持性证据。

管理层的评估必须综合考虑普遍 IT 控制与应用程序和数据负责人控制的双重结果，并就该等控制作出结论。该等评估应对与业务流程相关的控制目标提供具体的内控证据（与具体财务报告认定相关的控制）。该等评估也可包括对普遍 IT 控制中用以弥补错误的探测性和修正性控制进行充分的评价。例如，用户输入输出控制可用来确保信息处理的完整性和准确性。但是，透过用户控制以弥补普遍 IT 控制缺陷的成效仍存在一些局限。

17. 如何进行流程或活动层面的评估？

问题 8 已经说明了 COSO 框架是如何在活动或流程层面实施的。总体来说，应采用下面的步骤：

记录目标流程- 这一步要根据管理层的记录标准，识别与主要财务报告要素相关的关键输入、运行和输出。该步骤须确认风险的来源并指明关键控制点。此外，在该步骤中流程负责人开始参与评估流程，包括获取他们的签署。

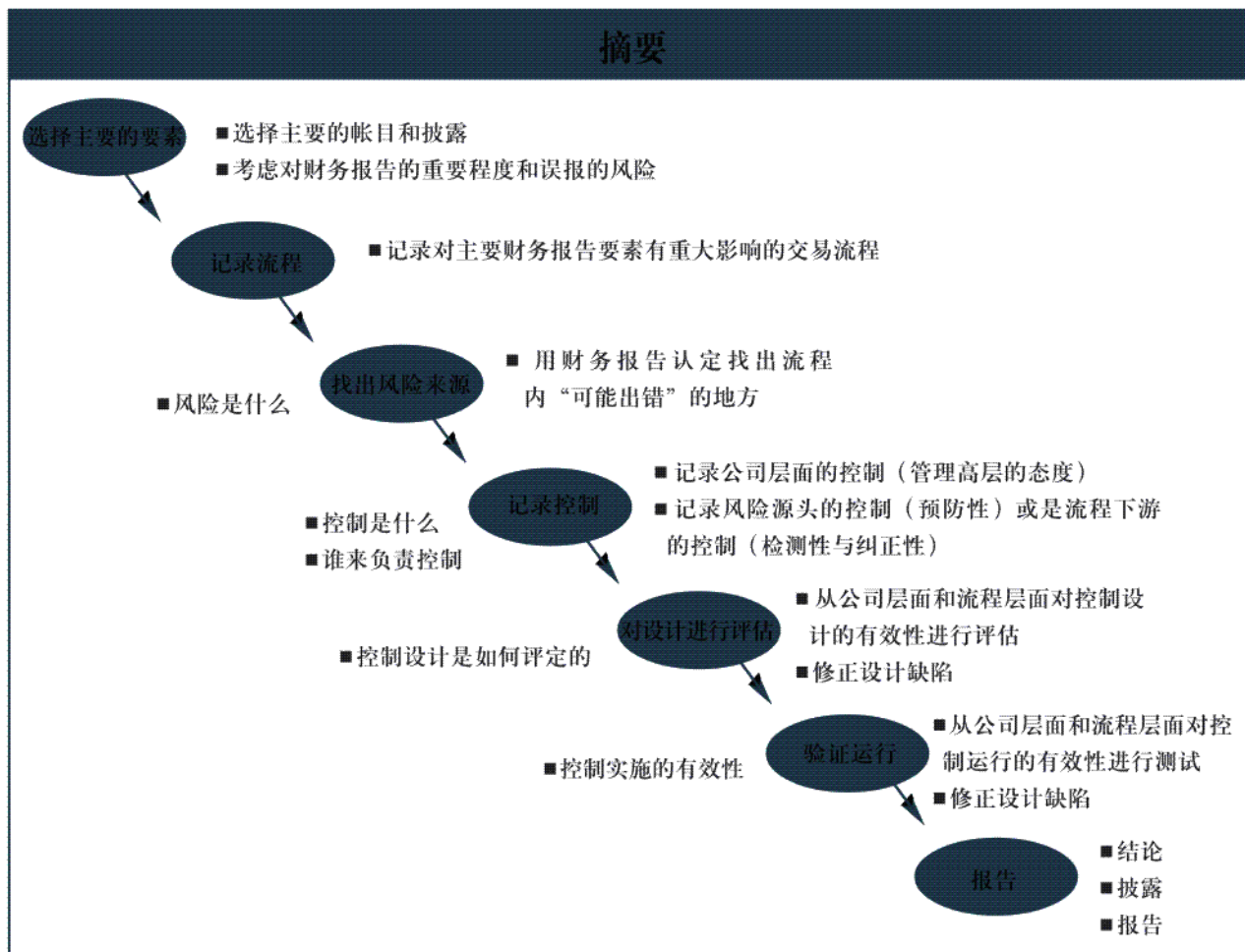
记录风险和控制- 流程的输入、运行和输出记录工作完成后，下一步就是与流程负责人共同确认有关流程中的财务报告风险，并确定风险源头或下游的关键控制点。财务报告风险源自财务报告认定。确认控制时，项目小组要逐一选择与风险相关的重要控制活动。在绘制流程图、确认风险和控制点时，应与流程负责人一并分析有关流程，并让他们签署已完成的记录文件。

评估设计成效- 在对风险和控制进行记录后，项目小组要评估有关控制是否按照其设计意图，确保已将风险降低到可接受的水平，即是否已经达到财务内控的目标。如存在重大的设计缺陷，则需要在检测运行成效前予以修正。

验证运行成效- 就确认有效的内控设计而言，要求流程负责人和内部审计人员验证或测试控制的运行效率。如果存在重大缺陷，则应及时予以修正。

总结控制差距-根据对设计成效的评估和对运行成效的测试，确认和总结内部控制中尚待改进的地方。

下图简单描述了活动或流程层面的评估步骤。



运行成效的验证（控制测试）

18. 建议使用什么样的方法“测试”财务报告内控的成效？

管理层如要就财务报告内部控制的成效发表肯定的声明，那么评估设计的成效和验证运行的成效都是必需的。验证运行成效即为确定控制是否按照设计要求运行的过程。与测试有关的上市公司会计监管委员会（PCAOB）第二号审计准则第40段对管理层职责要求的规定如下：[管理层必须评估]“控制的运行成效，惟须以能够充分评估其运行有效性的程序为基础……这样的程序包括内部审计人员进行控制测试，其他相关人员在管理层指导下进行控制测试，使用某个服务机构的报告，检查控制运用的证据，或者采取自我评估的方法进行测试，其中某些程序可能是管理层进行持续监督活动中的一部份。”⁷

我们将“测试”视作验证运行成效的一个部份。验证控制的运行成效有几种方式，控制测试是其中之一。测试为评估者提供了最强的信心，因为它提供了运行成效的最直接的证据。然而，测试也是各种验证方法中最耗费时间的一种。

三种验证运行成效的方法分别是：

- **自我评估。**流程 and 控制的负责人对他们所负责的控制进行自我评估，并将结果传达给管理层。这种验证方法让认证官员随时可以对运行成效进行确认，包括在年末和季度末。自我评估通常涵盖了公司所有的主要控制，即对于减轻风险和最终实现一个或多个财务报表认定特别重要的那些控制。自我评估流程随时可以进行，这种灵活性是通过以技术为基础的方案实现的。
- **监督。**监督出现在两个层面上，一个是公司层面，另一个是流程层面。管理层在公司层面上推行的监督和分析为在流程层面上的控制运行提供直接的证据。流程负责人通过其直接对流程运行情况进行监控活动和定制标准来进行监督。对监督的评估是基于它能否有效地确定控制运行的成效及识别有关控制流程未能检测到的重大错误或遗漏。
- **控制测试。**控制测试应在公司层面和流程层面上同时进行。在流程层面上的测试包括对整体流程控制的测试以及对信息流程控制的测试。对于关键控制的定期测试也包括对自我评估和监督过程质量的评估。

上述三种验证方法相互关联。例如，以流程为基础的自我评估可以成为协助管理层支持其控制成效结论的一个有效工具，然而，自我评估不能排除监督和测试控制的需要。如果自我评估的结果是全面的和肯定的并有很强的公司层面的监督控制和分析，那么测试信心要求水平可能会降低并且样本量可能会减少。这种自我评估取决于很多因素，包括控制的关键程度、发生变化的风险，以及流程内交易的数量、复杂程度和进行速度。

19. 什么是“控制测试”？

控制测试是一种验证控制运行的方式。评估者利用控制测试确定所选内部控制在某个时期内或某个时点的运行是否有效。测试包括访谈流程和控制的负责人，检查相关的控制记录文件，观察正在进行中的控制，以及利用所选交易分析或者重新执行某项控制。上述测试程序通常会综合使用以获取有关某个控制运行成效的充分证据。一般认为如果综合使用上述测试程序来验证内部控制的运行情况，那么管理层提供的证据会更可靠。

财务报告内部控制旨在（a）预防财务系统出现错误，或（b）及时检测和纠正已发生的错误。因此，控制测试针对（a）预防性控制在预防错误及例外情况方面的成效，以及（b）正予以测试的“检测和纠正”类控制所披露的错误和例外情况的性质、数量和处理情况。这些测试也涉及控制是如何被应用的，控制在应用过程中的一致性以及控制由谁来应用。

对控制的测试紧随对控制设计的评估之后。为支持其有关财务报告内部控制的认定，管理层首先要对控制设计的成效进行评估。然后，管理层再对运行的成效进行评估，内容包括评估记录在案的控制是否将已识别的风险降低至一个适当的水平并确保财务报表内管理层的认定得以实现。验证运行成效（包括控制测试）需要评估控制是否在按照设计的要求运行。

因此，“控制测试”确定公司内部控制是否按照它们所设计的方式运行。

报告

20. 当管理层发现某控制缺陷可构成财务报告内部控制中的一个重大弱点时，即使该缺陷可在年底前被纠正，公司是否依然必须在公报中披露该缺陷？如果是，该规定何时生效？

S-K 法规第 308 (c) 项条款要求公司披露发生在最近期会计季度期间，且对公司财务报告内部控制产生重大影响（或者很可能会产生重大影响）的任何变化（可以认为包括为纠正实质性漏洞而作的变化）² S-K 法规的 308 (c) 项条款目前是有效的，并且遵照了 10-Q 表格的报告要求。就披露任何有关变化而言，公司可以认为对任何会引起变化的重大弱点（或潜在的重大弱点）进行描述实属谨慎之举。

美国证券交易委员会工作人员指出他们期望注册机构定期改进内部控制，并欢迎注册机构披露对控制做出的所有重大变化，不管有关变化是否是在萨班斯-奥克斯利法案 404 条款的规则遵循日之前发生。然而，如果注册机构选择不就其编制第一份有关财务报告内部控制的管理层报告时所作的变化进行披露，证交会的工作人员亦不会反对。此外，与我们上述观点相一致的是，美国证券交易委员会工作人员亦重申如果注册机构已经发现了一个重大弱点，那么有关注册机构就应该仔细考虑是否应对该弱点以及针对该弱点所作的变化进行披露。

注册机构第一份有关财务报告内部控制的管理层报告发布以后，根据 S-K 或 S-B 法规 308 项条款的规定，美国证券交易委员会工作人员指出注册机构须在每份季报和年报中确认和披露财务报告内部控制中发生的任何重要变化。应予以披露的有关变化（包括一项改进措施）并不局限于针对已经发现的重大缺陷或者实质性漏洞而作出的变化。如果有关变化对注册机构的财务报告内部控制产生重大影响（例如一个新的信息系统的启用）那么注册机构也应对这种变化进行相应的披露。

首次年度评估后的继续关注

21. 首次年度评估完成后，管理层如何对从属于披露控制与程序的财务报告内部控制进行季度评估？

美国证券交易委员会 404 最终条款规定，毋须对财务报告内部控制进行季度评估。然而，自 2002 年 8 月起开始生效的规则则要求公司须按季度评估披露控制与程序，以及按季度对有关披露控制与程序成效的结论进行披露，而该等规则自被采纳以来并无发生实质性的改变。在 404 最终条款规则中，美国证券交易委员会规定“这些评估和披露要求将继续适用于披露控制与程序，包括从属于披露控制与程序的财务报告内部控制要素”⁴

管理层应该如何按季度审核这些财务报告内部控制要素？首次年度评估期间确认的关键控制为后来开展季度评估提供了基础。网络技术可协助监督流程负责人在季度末向部门经理汇报的自我评估。部门经理进而向高级管理层（核证人员）或披露委员会汇报。任何异常情况都将呈报给获指派负责解决有关异常情况的官员。

现总结如下：

- 首次年度评估须记录流程负责人执行的所有关键控制；
- 管理层必须确认从属于披露控制与程序的财务报告内部控制要素；
- 管理层必须在首次年度评估之后每年按季度评估财务报的内部控制的变化，包括作为披露控制与程序

一部份的控制的变化;

- 技术为流程负责人随时对控制运行成效进行持续自我评估提供了基础。根据在首次年度评估期间确认的关键控制，专门定制一些问题以在自我评估流程中使用;
- 根据流程负责人每个季度的反馈意见，管理层（即核证人员）将决定是否需要就有关变化，如流程、系统、运行及其他因素中发生的变化，以及有关变化对内部控制有效性的影响进行披露。

由于首次年度评估是以流程为基础进行的，所以流程负责人对上级的汇报将真正地成为一种“责任链”# 这种责任链与许多公司创立的要求流程负责人直接汇报以对有关结果分别进行核证的“核证链”形成了鲜明的对比。实际上，这些直接汇报反过来又要求对方同等程度的汇报，等等。通常被称作“备份核证”的核证链法虽然能够让流程负责人介入其中，但是不一定能够确保管理层可获得更好的信息以及及时采取行动及进行披露。首次年度评估的结果与持续进行的季度评估相关联，从而产生了上述责任链，因此这种责任链是一种以流程为基础的更有效的方法。通过这种方法，404 条款的合规工作使有关披露程序及控制的评估更为有效。

管理层的角色

22. 披露委员会的角色是什么？

美国证券交易委员会建议编报公司建立一个披露委员会以考虑信息的重要性、决定披露要求、确定相关的披露事宜，以及协调创建一个适当的架构，以确保优质的重要信息能够及时地披露予管理层以便其进行相关行动和披露。美国证券交易委员会期望披露委员会将向高级管理层，尤其是向核证人员进行汇报。

美国证券交易委员会表示披露委员会成员可以包括主要会计人员（或财务总监）% 首席法律顾问（及 / 或另外一位负责美国证券交易委员会披露事宜的公司内部的高级律师）：首席风险管理官员以及首席投资者关系官员（或者承担同等企业沟通责任的官员）/ 委员会还应该包括首席信息官员，来自公司运营部门的相关代表以及其他公司认为合适的行政人员。为了有效行使其职责，披露委员会应该包括一位美国证券交易委员会报告与申报要求方面的专家。

以下是对于披露委员会角色的进一步阐述：

- 委员会对何谓“重大的”交易或事件作出定义，并确保核证人员知晓可能会影响公司披露的重要信息。委员会还考虑就满足美国证券交易委员会要求而言，哪些是重要的而哪些是不重要的信息，以进行适当的披露从而使谨慎的投资者做出知情决定；
- 一个有效的披露委员会能够确认申报的信息是否完整（比如，考虑管理层决定终止一个业务部门所产生的影响）# 就职于委员会的个人必须具有业务及其风险的相关知识，而且要熟悉同行业其他公司的披露惯例。他们应该了解公开报告的编制流程以及为此流程而要准备的关键“资料”此外，他们应该在公司内有充分的权威以在需要时采取适当的行动；
 - 委员会还负责确定公司文化中是否存在任何可能会妨碍报告准确完整性的因素。例如，如果首席财务官和会计部门官员的薪酬中有很大一部份与利润挂钩，那么委员会应该检查有关方法以确保合格报告已予以充分的权衡；
 - 除直接向核证人员汇报（并对其负责）外，披露委员会主席应该与审计委员会定期会晤。审计委员会应该获取有关披露委员会各项工作内容的报告，包括公司申报和其他披露内容的质量，以及

披露委员会与核证人员或诸如法律顾问或外部独立审计师之间的任何分歧。至少，审计委员会应与核证人员以及披露委员会一起评估下列流程（i）确认重要的财务报告问题；（ii）及时向有关责任方呈报这些问题；（iii）确保这些问题在公司的对外披露中根据公认会计准则进行了正当的披露。审计委员会应在解决重大分歧中发挥作用；

- 委员会应该审阅所有公开披露的信息，包括 1934 法案申报文件，注册声明以及管理层就披露控制及财务报告内部控制所作的季度和年度评估。审阅的信息还应包括：
 - 所有为投资者提供财务信息或指导的新闻资料；
 - 向股东广泛派发的函件；
 - 向投资者会议、分析师、评级机构以及贷款人所作的说明；
 - 公司在投资者关系网上公布的披露；
- 委员会应该审阅与需要披露的问题有关的内部信息，包括内部审计报告、递交给董事会和董事会委员会的报告，以及递交给高级管理层的报告。

以上是有关披露委员会工作内容的若干示例。美国全国投资者关系协会最近对近 400 家上市公司进行的一项调查显示，85% 的公司已按照美国证券交易委员会的定义建立了披露委员会。就 404 条款项目而言，相较于项目的管理与指导，披露委员会对项目的结果和其披露的影响更感兴趣。

谨此提醒：如果公司设立了披露委员会，那么管理层应该确保委员会严格遵守其章程。已建立一个有明确章程的披露委员会，但又不能根据其章程开展工作，这将使管理层遭受指责。

23. 披露委员会与项目指导委员会有什么关系？两者的职责范围有什么不同？两者应如何交流？两者的成员组成有什么不同？

披露委员会比指导委员会有更广义的范围。指导委员会关注的是公司对 404 条款的成功遵守，而披露委员会重点则放在公司公开报告的公正性、准确性、完整性以及及时性等方面。披露委员会是公司披露控制与程序的一个重要组成部份。披露委员会应该确保公司披露控制与程序的设计与执行的有效性。

关于交流方面，与指导委员会不同的是，披露委员会不像指导委员会那样关注 404 条款合规情况的整体规划。然而，披露委员会却关注 404 条款合规执行过程的结果，包括对披露事项的影响等。因此，披露委员会和指导委员会可以相互交流以解决共同的问题，例如，确认内部控制的设计或运行是否存在“重大缺陷”或“重要缺点””他们也可以合作审阅控制缺陷，以建议公司在公开报告中对有关缺陷进行披露。

就会员资格而言，披露委员会与指导委员会的会员组成存在重叠现象。基于两个委员会各自的成员构成情况，我们做出以下概括：

- 两个委员会都可以包括经营部门的领导或代表以及相关部门的领导，比如，首席法律顾问、信息技术以及内部审计人员等；
- 主要会计人员（或财务总监）可服务于披露委员会，但也可以作为 404 条款项目领导向指导委员会作报告；
- 证交会建议在披露委员会中包括首席风险管理官员和首席投资者关系官员（或承担同等企业沟通责任的官员）”而指导委员会通常不需要该等人员。

核证人员可任职指导委员会，然而，披露委员会要向他们作报告。实际上，404 条款项目领导人可能是其中一名核证人员，而该核证人员甚至可能是指导委员会的主席。

内部审计的角色

24. 内部审计在评估程序中的角色是什么？

在记录内部控制，测试内部控制以及向管理部门提供有关设计与运行成效结论方面的意见时，内部审计能够起到非常重要的作用。内部审计能够为管理部门提供一个额外的参考资源，以便遵守萨班斯·奥克斯利 404 条款。COSO 框架指出，由内部审计开展的独立评估也是一种监督形式。

独立会计师的角色

25. 证交会对鉴证报告有提供任何指导吗？

根据新的规定，公司需要提交独立审计师的鉴证报告作为年度报告的一部份。有关鉴证必须根据由公众公司会计监察委员会颁布或采纳的鉴证业务标准进行。404 条款进一步规定鉴证工作不能成为会计师事务所的单独工作项目。

26. 在鉴证程序中，管理层预期公司的独立会计师会开展什么样的工作？

独立会计师会希望了解管理层有关财务报告内部控制的认定以及管理层如何支持这些认定。管理层可预期独立会计师会进行（其中包括）以下的工作：

- 采访管理层以及参与评估的主要负责人；
- 审阅支持评估的记录；
- 检测公司层面及流程层面的记录，以确保有关记录能够公平地反映实际运作中的控制；
- 评估管理层对有关设计成效的结论；
- 对运作成效进行独立审核并有选择性地审计测试；
- 评估证明文件能否共同支持管理层对有关内部控制的认定；
- 评估有关审阅结果对披露事项之影响，并提供意见。

管理层还可预期独立会计师会考虑对财务报表进行的审计工作的结果。如果审计师的测试发现财务报表中出现差错或遗漏，那么审计师将评估出现差错的根本原因，以确定有关差错是否由内部控制的缺陷所引起。

审计委员会的角色

27. 审计委员会应怎样以及何时介入管理层的评估程序和独立会计师的鉴证程序？

审计委员会目前正在提出这个问题。在证交会就 404 条款举行的公开研讨会上，证交会的职员表示审计委员会在要求作出变化以纠正内部控制缺陷方面应起到重要的管治作用。审计委员会希望了解在有关管理层内部控制报告与独立会计师鉴证报告方面他们必须做出努力的程度。这个问题应咨询法律顾问的意见。我们了解法律顾问建议审计委员会使用其出具年度鉴定审计意见时使用的调查方法，也就是说，询问发现了什么问题以及如何加以解决。

由于财务报告内部控制是披露控制与程序中的一个部份，我们期望审计委员会在财务报告内部控制的季度评估中的作用与其目前在披露控制与程序中要求的评估中的作用类似。至少审计委员会应该与首席执行官、首席财务官及披露委员会主席（如有）一起评估程序以(i)确认重要的财务报告问题，(ii)及时地向有关负责人呈报这些问题，以及(iii)确保这些问题在公司的对外披露中根据公认会计原则进行了正当的披露。

外国编报公司及位置

28. 国外编报公司要符合 302 条款对执行人员声明的要求么？

提交 20-F 和 40-F 表格的国外私人发行商不需要遵守季度报告的要求。

29. 根据截至目前为止从美国加速编报公司所获得的经验，对于刚刚开始为合规努力的国外编报公司来说有什么可以作为借鉴？

与计划、组织和管理项目相关的主要经验教训如下：

- 对于大多数加速编报公司来说，404 条款合规工作是一个需要“项目管理组织”参与的主要项目；
- 高级管理层的支持至关重要，没有他们的支持，404 条款合规工作很难成功；
- 让业务单位经理和流程负责人（包括内部人员及外聘人员）介入并使他们对项目负责；
- 对项目负责。避免出现组织中的非高层人员管理该项目的情况，以及项目小组太过注重不相关的细节而使关键的范围界定决策长时间得不到解决等问题；
- 不要浪费时间。404 条款的合规工作是一项巨大的工程。根据国际财务执行官杂志的一份研究报告显示：对于年收入在 10 亿至 50 亿美元的公司来说，公司内部人员在该合规项目上投入的时间平均为 14,000 个小时。因此，应尽早开展该项目；
- 在组织上下、内外全方位开展沟通；
- 在项目执行过程中于适当时间让外部审计师进场工作。和他们一起工作并讨论问题，了解他们对项目的期望和时间要求，定期检查项目的执行情况并制定计划以给外部审计师预留充分的时间。确认管理层必须表示他们并未使用外部审计师在审计程序期间使用的程序；

与执行项目有关的一些主要经验教训如下：

- 尽早解决有关范围界定的关键问题－该项目涉及哪些财务报告元素，哪些经营场所和业务单位，以及

哪些流程和系统？

- 在项目执行过程中，尽早评估公司层面的控制及整体信息技术控制，以及计划在评估中揭露舞弊行为；
- 重点放在最重要的财务报告元素、认定以及风险上。将最重要的元素、流程、主要的认定以及风险与控制联系起来。将信息技术风险和控制与 404 条款评估结合起来；
- 保存公司目前的控制记录文件，使用流程图来提供最有效的“穿行测试”\$ 确保流程负责人已为审计师的“穿行测试”做好准备；
- 关注细节。阅读上市公司会计监管委员会制定的准则并记录公司遵守准则的途径。运用 COSO 框架（或其他合适的框架）& 把首次年度评估作为一个学习的经历。做好会在项目执行过程中遇到障碍的心理准备，因为第一年对每个人来说都将是具有挑战性的一年；
- 明确测试计划以及预先制定“项目规则”\$ 选择要进行测试的控制，确定判定控制失败的条件，阐明控制测试记录文件的格式并决定在碰到失败的状况时采取什么样的举措。根据控制的发生频率确定测试的范围，测试的程度至少要与审计师测试的程度一样，样本量要合适，以达到较高系数的保证，使用有能力的客观的评估员，以及不忘重新测试接近年末时出现的新情况；
- 考虑及时弥补措施的性质与范围。尽快开始评估程序及解决重要的设计缺陷。认真地弥补执行缺陷，确保重新测试弥补控制。

30. 美国以外的国家有关 404 条款的记录文件是否必须用英文编制？

美国证券交易委员会和其他相关组织并未规定所有内部控制记录文件必须用英文编制。对于大多数公司来说，这种要求会是一个不必要的负担。审计公司一般会将有关工作交给其具备必要语言技能的办事处来完成。当地管理层是否具备有效地评估各种程序及控制并就其有效性作出结论的能力是在决定翻译是否必要时需考虑的一个因素。此外，公司评估方法的严谨性和一致性以及支持评估的工具及培训也需要考虑在内。

如果认为有必要进行翻译，那么或许只需根据重要程度对记录文件的某些部份进行翻译。比如，依据重要程度，可以用英文编制一份全面的备忘录以及概要计划的节选，以将重要的事宜呈报给注册公司管理层。此外，需要合并的事宜通常需要翻译成申报企业所用语言。

在决定记录文件中的哪些内容（如有）必须用英语编制时，必须对国外公司的规模与风险进行个案考虑。关键是要确保翻译不会影响评估的质量或者控制的执行。不加选择地强调翻译可能会增加风险。比如，在像日本这样的国家，日文翻译成英文的质量很差，因此翻译会使流程复杂化，更难保证风险的正确识别以及适当控制的应用。用英文编制记录文件还可能限制参与工作的人数，因为在许多国家，很少有本国人会说英语，更不用说熟练地用商业英文进行交流。该问题同样存在于其他一些国家，由于评估内部控制的复杂性，而极难使用英语编制记录文件。因此，对跨国公司来说，除非英语是商业环境（如新加坡）中常用的语言，否则使用当地的语言编制记录文件更为明智。

鉴于诸多此类的问题，我们强烈建议申报企业尽早与公司的外部审计师进行商讨。有关翻译的问题也强调了公司的内部审计部门应具备适当的语言技能，或者能够聘请业内的专业公司，以提供熟练掌握当地语言的合资格内部审计师或风险咨询专家，共同完成有关项目。

笔记

甫瀚是一家提供独立内部审计和风险咨询服务的专业公司。本公司帮助客户确定、评估以及管理他们在其行业内所遇到的有关经营及技术的风险，并协助客户执行有关程序及控制，以确保他们能够进行持续监督。此外，本公司还提供全面的内部审计服务，利用深入的技能与技术专长来实现企业风险管理以及持续转变的内部审计职能。