第 64 讲-公司治理，风险与合规性（1）

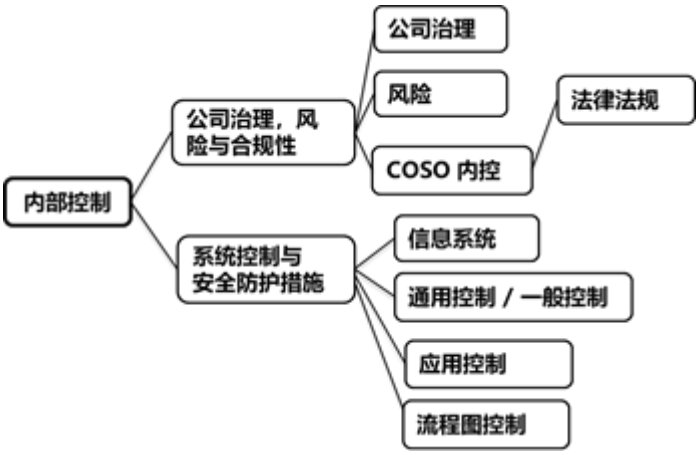
第五章/E 内部控制

本章考点框架

第 E.1 节 - 公司治理、风险与合规性

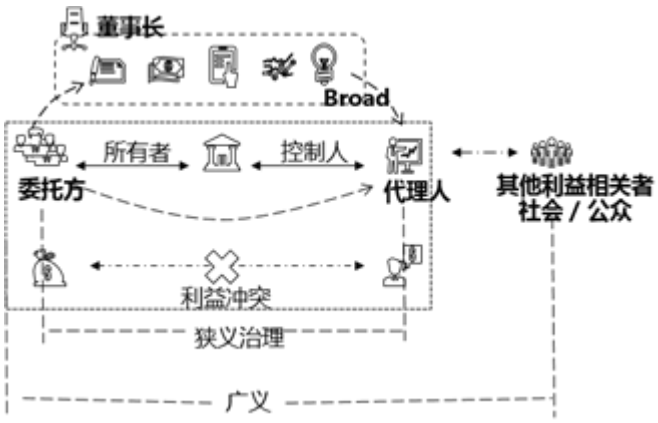
第 E.2 节 - 系统控制和安全防护措施

内部控制



第 E.1 节 公司治理，风险与合规性

公司治理



公司治理，从广义角度理解，是研究企业权力安排的一门科学。从狭义角度上理解，是居于企业所有权层次，研究如何授权给职业经理人并针对职业经理人履行职务行为行使监管职能的科学。

基于经济学专业立场，企业有两个权：所有权和经营权，二者是分离的。企业管理（Corporate Management）是建构在企业“经营权层次”上的一门科学，讲究的就是企业所有权人向经营权人授权，经营权人在获得授权

的情形下，以实现经营目标而采取一切经营手段的行为。与此相对应的，公司治理（Corporate Governance）则是建构在企业“所有权层次”上的一门科学，讲究的是科学的向职业经理人授权，科学的向职业经理人进行监管。

公司治理模式主要有三种：英美模式、日德模式和家族模式。

- 英美模式 - 公司内部的权力分配是通过公司的基本章程来限定公司不同机构的权利并规范它们之间的关系的。各国现代企业的治理结构虽然都基本遵循决策、执行、监督三权分立的框架，但在具体设置和权利分配上却存在着差别。
- 德日模式 - 德日治理模式被称为是银行控制主导型。
- 家族模式 - 由于国情和企业所处的成长与发展环境的差异，使得韩国和东南亚通常为家族型。
- 公司治理又名公司管治、企业管治，是一套程序、惯例、政策、法律及机构，影响着如何带领、管理及控制公司。
- 公司治理方法也包括公司内部利益相关人及公司治理的众多目标之间的关系。主要利益相关人士包括股东、管理人员和理事。其它利益相关人士包括雇员、供应商、顾客、银行和其它贷款人、政府政策管理者、环境和整个社区。

从公司治理的产生和发展来看，公司治理可以分为狭义的公司治理和广义的公司治理两个层次。

- 狭义的公司治理，是指所有者（主要是股东）对经营者的一种监督与制衡机制，即通过一种制度安排，来合理地界定和配置所有者与经营者之间的权利与责任关系。
- 公司治理的目标是保证股东利益的最大化，防止经营者与所有者利益的背离。其主要特点是通过股东大会、董事会、监事会及经理层所构成的公司治理结构的内部治理。
- 广义的公司治理是指通过一整套包括正式或非正式的、内部的或外部的制度来协调公司与所有利益相关者之间（股东、债权人、职工、潜在的投资者等）的利益关系，以保证公司决策的科学性、有效性，从而最终维护公司各方面的利益。
- 公司治理是指公司被管理和控制的制度。治理结构具体是指权利和职责在公司利益相关者（例如，董事会、经理人员、股东、债权人、监管机构和公司外部审计人员）之间的分配。
- 治理结构进一步指明了公司事务决策制定的规则和程序。

公司治理-董事会和审计委员会的责任

- 董事会对企业的运营和结果负有最终责任。董事会负责设定运营的整体目标，这些目标可以指导如何设计和监控控制制度。董事会的主要职责就是确保公司的运营符合股东利益最大化原则。
- 审计委员会需要具备熟练财务知识背景的独立董事。《萨班斯—奥克斯利法案》（SOX）要求审计委员会要完全由独立于组织的董事组成，这意味着委员会成员不能从组织接受任何与审计事务有关的咨询费、顾问费或其他报酬，或者与该组织或其分公司具有任何附属关系。
- 此外，至少一名审计委员会成员必须具备证券交易委员会（SEC）所认可的“财务专家”资格。

【例题·单选题】

下面哪一项不是董事会的职责（ ）。

A. 预算审批

B. 制定战略目标

C. SOX 法案规定的内控职责

D. 高管人员的选择及其职责义务的确定

【答案】C

【解析】C 选项是管理层的职责。

第 65 讲-公司治理，风险与合规性（2）

第 1 节 公司治理，风险与合规性（2）

风险与风险管理

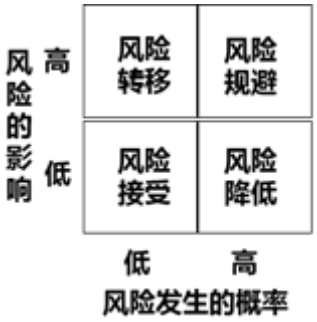
风控模型

风险管理（Risk Management）是指如何在项目或者企业一个肯定有风险的环境里把风险减至最低的管理过程。风险管理是指通过对风险的认识、衡量和分析，选择最有效的方式，主动地、有目的地、有计划地处理风险，以最小成本争取获得最大安全保证的管理方法。当企业面临市场开放、法规解禁、产品创新，均使变化波动程度提高，连带增加经营的风险性。良好的风险管理有助于降低决策错误之几率、避免损失之可能、相对提高企业本身之附加价值。

风险管理是指如何在项目或者企业一个肯定有风险的环境里把风险可能造成的不良影响减至最低的管理过程。风险管理对现代企业而言十分重要。

风险可以被有效地分析或分解成几个组成要素或组成部分。这几个要素或部分包括：

1. 损失的可能性。损失发生的概率有多大？
2. 如果发生，损失金额有多少？



风险是各种带来损失的可能性。任何企业都面临风险，风险可以通过各种形式来损害企业利益。

企业应当对风险进行评估。企业内控系统需要考虑成本效益原则。

风险的评估与从定性与定量的两个维度展开。

预期的损失值是预计的损失范围的可能性乘以预计损失发生时每个预计损失的金额。

风险类型

- 固有风险（IR）：不考虑内部控制结构的前提下，由于内部因素和客观环境的影响，企业的账户、交易类别和整体财务报表发生重大错误的可能性。
- 控制风险（CR）：内部控制没有预防或发现的风险。
- 检查（失侦）风险（DR）：审计证据没有发现虚假陈述的风险。
- 可接受的审计风险（ARR）：是指发生审计失败的概率，其公式为：ARR=IR×CR×DR。

审计风险，从外部审计的角度，审计师将风险划分为三种类型：

1. 固有风险（IR）
2. 控制风险（CR）
3. 检查（失侦）风险（DR）

如果管理层诚信度越低、财务报告使用者越多、被审计单位的财务状况越糟糕以及审计师希望在更大程度上确信财务报告没有重大虚报，可接受的审计风险就越低。

【例题 • 单选题】

一些账户余额，如养老金和租金，都是复杂计算的结果。这些账户容易产生重大虚假陈述的风险被称为（ ）。

A. 审计风险
B. 检查风险
C. 抽样风险
D. 固有风险

【答案】D

【解析】固有风险是在不考虑内部控制结构的前提下，由于内部因素和客观环境的影响，企业的账户、交易类别和整体财务报表发生重大错误的可能性。比如，复杂的计算比简单计算更容易出现虚假陈述，现金比煤的存货更容易失窃。固有风险与审计没有关系。

【例题 • 单选题】

没有被审计师审计发现错误的风险是（ ）。

A. 固有风险

B.控制风险

C.其他系统风险

D.检查风险

【答案】D

【解析】“Detection Risk”又称为失侦风险，即选项中的检查风险，指某项错误或欺诈未被审计师发现的风险。

审计师应当根据审计结论，分别出具：

1.无保留意见；

2.带有强调事项段的无保留意见；

3.保留意见；

4.否定意见；

5.拒绝表示意见的审计报告。

1.无保留意见

无保留意见审计报告，是指审计人员对被审计单位的会计报表，依照独立审计准则的要求进行审查后，确认被审计单位采用的会计处理方法遵循了会计准则及有关规定。

会计报表反映的内容符合被审计单位的实际情况；会计报表内容完整，表达清楚，无重要遗漏；报表项目的分类和编制方法符合规定要求，因而对被审计单位的会计报表无保留地表示满意。

2.带有强调事项段的无保留意见

说明审计师认为被审计者编制的财务报表符合相关会计准则的要求并在所有重大方面公允反映了被审计者的财务状况、经营成果和现金流量，但是存在需要说明的事项，如对持续经营能力产生重大疑虑及重大不确定事项等。

3.保留意见；

经过审计后认为被审计单位会计报表的反映就其整体而言是公允的，但存在下述情况之一时，应出具保留意见的审计报告：

（1)个别重要财务会计事项的处理或个别重要会计报表项目的编制不符合相关会计准则或财务会计法规的规定，被审计单位拒绝进行调整。

（2）因审计范围受到重要的局部限制，无法按照独立审计准则的要求取得应有的审计证据。

（3）个别重要会计处理方法的选用不符合一贯性原则。

4.否定意见

所谓否定意见审计报告，是指审计人员经过审计后，认为被审计单位的会计报表不能公允地反映其财务状况、经营成果和现金流量情况，从而提出否定其会计报表“ 三性”（可靠性、相关性 和及时性）的审计意见的一种审计报告。

5.拒绝表示意见的审计报告

所谓拒绝表示意见审计报告，是指审计人员在审计过程中因未搜集到足够的审计证据，无法对被审计单位的会计报表发表确切的审计意见，所出具的一种不发表评价意见的审计报告，也即对会计报表不发表肯定、保留和否定审计意见的审计报告。

【例题 • 单选题】

某审计事务所在为某公司进行审计时发现了重大的错报和错误披露，但此错误并不普遍存在，则审计事务所出具什么类型的审计意见（ ）。

A.保留意见

B.无保留意见

C.否定意见

D.无法出具意见

【答案】A

【解析】对公司财务报告的审计，如果发现有重大的错报和错误披露，但此错误并不普遍存在，则审计师应当出具保留意见。注：否定意见是当审计发现公司财务报告没有按照财务准则来编制时出具的意见。

外部审计人员的职责：对内部控制的报告

《萨班斯—奥克斯利法案》的404条款也要求外部审计人员对证券被公开交易的发行人/企业的财务报告与内部控制的充分性提供证明并提交报告。

影响风险的五个主要因素

1. 独立绩效检查的频率。
2. 组织控制方法的充分性。
3. 权责想匹配的充分性。
4. 执行控制措施的连续性。
5. 物理性控制的充分性。

风险管理

本节讨论组织如何有效管理风险。这要基于 COSO 所提出的企业风险管理（ERM）框架。企业风险管理包括确定和管理可能影响企业实现目标能力的事件和情况。

根据 COSO 企业风险管理框架，风险管理的目标包括：

1. 调整风险偏好和策略
2 . 改进风险应对机制
3. 减少运营意外和损失
4. 识别和管理多重以及跨企业的风险
5. 抓住机遇
6. 改善资本部署

控制环境的组成

- 高层管理者所营造的道德氛围
- 政策和标准
- 职责分离和关键会计职能
- 编制有关控制政策和程序的文件，2002 年《萨班斯—奥克斯利法案》（SOX）的 404 条款要求上市公司要记录其内部控制。

第 66 讲-公司治理，风险与合规性（3）

第 E.1 节 公司治理，风险与合规性

内部控制

什么是内部控制？

根据 COSO 的解释，内部控制的运作体系是一种程序，该程序提供了合理的保证，使得实体能实现其与运营、报告和合规性相关的目标。

是由公司的董事会，管理层和全体员工共同实施的，旨在合理保证实现企业基本目标的一系列控制活动。

基本目标包括：

1. 经营的效率和效果
2. 财务报告及管理信息的真实可靠
3. 遵守适用法律和法规
4. 资产的安全完整
5. 企业战略

内控的定义，指明了一些基本概念：

内部控制是一个过程。这意味着内部控制本身没有结束，它属于业务流程的一部分。内部控制不仅仅是政策手册和表格，而关系到组织每个层次的人。内控受人的影响，也影响人。

内部控制只能对公司管理层和董事会提供合理的保证，而不是绝对的保证。因为：

- 人的判断可能是错误的；
- 成本和效益考虑；
- 人为失误，如简单的错误或过失；
- 两人或多人间的勾结；
- 管理人员滥用职权。

我们会涉及内部控制系统的三个维度：

1. 目标的类别；
2. 内部控制系统的组成；
3. 组织结构。

内控的目标

下面的三类目标允许组织关注可能对他们特别重要的内部控制的一些方面：

1. 运营—与既有效率又有效果地对组织资源加以利用相关的目标。
2. 报告—与财务和非财务报告的可靠性、及时性和透明度相关的目标。
3. 合规性—与遵守适用的法律和法规相关的目标。

内控的范围

控制系统的第三个维度是组织的结构，描述了一个大型组织中常见的组织结构。

1. 组织范围（即实体层面）
2. 部门层面、高层、组织中不连续的部分
3. 运营单位（即组织中可以分离的单位）
4. 职能（例如会计、营销、信息技术）

内控的五要素

根据 COSO，内部控制制度有五个组成部分：

1. 控制环境
2. 风险评估
3. 控制活动
4. 信息与沟通
5. 监控活动

控制环境	#1组织	#2董事会	#3管理层	#4员工能力	#5问责制
风险评估	#6目标	#7评估	#8舞弊	#9变革管理	
控制活动	#10降低风险	#11技术控制	#12政策		
信息与沟通	#13信息质量	#14内部沟通	#15外部沟通		
监控活动	#16持续和定期的监督	#17解决内部控制缺陷			

内控五要素－控制环境

控制环境是指组织的管理理念和风险承受能力，它包括一个组织的完整性、道德价值观及其运作环境。

控制环境	#1组织	#2董事会	#3管理层	#4员工能力	#5问责制

管理理念与经营方式

- 风险偏好和风险的对策
- 对财务报告的态度

组织结构

- 权力与责任的分配

人力资源政策与实践

- 向员工发送有关预期道德行为、诚信、胜任能力的完整信息

人员素质

董事会或审计委员会

- 治理、指导和监督
- 审计委员会
- 外部独立董事

内控五要素－风险评估

COSO 模型包含的一个要素是确定风险发生的概率及其重要性程度。

风险分为固有风险和剩余风险。

风险评估	#6目标	#7评估	#8舞弊	#9变革管理

所有的公司，无论规模大小、结构、性质或行业，都会在组织内遇到不同等级的风险，但是事实上没有切实可行的方法可以将风险降低为零，因此管理层必须决定有多少风险需要慎重接受。

风险识别-识别影响组织目标实现的事件。

风险分析-风险=发生的概率（%）×发生后的损失（$）

舞弊三角：

该理论由美国注册舞弊审核师协会（ACFE）的创始人、现任美国会计学会会长史蒂文·阿伯雷齐特（W. Steve Albrecht）提出，他认为，企业舞弊的产生是由压力（Pressure）、机会（Opportunity）和自我合理化（Rationalization）三要素组成，就像必须同时具备一定的热度、燃料、氧气这三要素才能燃烧一样，缺少了上述任何一项要素都不可能真正形成企业舞弊。

内控五要素－控制活动

政策和程序的制定及实施有助于确保风险应对得到有效执行。

COSO 模型列出了以下控制活动：

1. 权责的划分（工作描述）
2. 交易授权系统
3. 适当的文件和记录
4. 良好的授权系统与职责分离制以保证资产安全
5. 独立审核（内审&外审）

控制活动的实例

- 职责划分：最有效但也最昂贵，下面四个职能应该由不同的部门或不同的人执行：授权/记录/资产的保管/对账。
- 正当的授权程序。
- 资产的物理控制和记录。

内控五要素－信息与沟通

COSO 模型认为相关信息必须以某种形式并在某个时间框架内进行确认、捕捉和交流，以使人们能成功地从事工作。这里假设数据交流具有安全性和准确性。

A－accurate－准确
C－complete－完整
C－cost/beneficial－性价比
U－user targeted－用户导向
R－relevant－相关性
A－authoritative（ie credible）－授权
T－timely－时效性
E－easy to use－易用性

内部信息反映企业内部情况的信息，企业内部信息很多，归纳起来主要有：

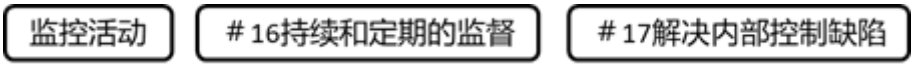
- 反映企业管理部门的信息。
- 反映企业生产活动方面的信息。
- 反映企业经济方面的信息。
- 反映生产技术方面的信息。
- 反映企业人事教育方面的信息。

外部信息是指企业以外产生但与企业运行环境相关的各种信息。其主要职能是，在企业经营决策时作为分析企业外部条件的依据，尤其在确定企业中长期战略目标和计划时起重要作用。

- 宏观社会环境信息。
- 科学技术发展信息。
- 科学技术发展信息。
- 市场信息。

内控五要素－监督活动

内部控制的所有方面都受到监控，并根据需要进行修改。监控需通过持续的管理行为、独立的评估或两者相结合的方式来实施。内部审计人员、审计委员会、披露委员会和管理层都需要参与到监控活动中来。



- 组织应选择、开展并实施持续和/或单独评估，以确认内部控制各要素的存在和持续运行。
- 持续评估通常由一线主管或职能经理来执行，他们具备胜任能力且有丰富的知识以理解被评估的事项，并且能够对获得的信息进行进一步的考察。
- 独立评估是由内部审计部门来负责实施的，它能以全新的视角去审视内部控制 5 要素是否存在且持续运行。
- 组织应评价内部控制缺陷，并及时与整改责任方沟通，必要时还应与管理高层和董事会沟通。

【例题·单选题】

COSO 内部控制要素的主要部分包括以下哪些（ ）。

Ⅰ. 内部环境 Ⅱ. 监控 Ⅲ. 控制活动 Ⅳ. 风险识别

A. 只包括Ⅰ

B. 包括Ⅰ，Ⅱ

C. 包括Ⅰ，Ⅱ，Ⅲ

D. 包括Ⅰ，Ⅱ，Ⅲ，Ⅳ

【答案】C

【解析】COSO 内部控制五要素包含：控制环境、风险评估、控制活动、信息与交流与监控活动。风险识别不是 COSO 五要素中的内容。

【例题·单选题】

以下哪个选项最好地反映了公司的控制环境良好（ ）。

A. 内审和财务人员一起工作，指导和监督财务人员的工作

B. 公司在处理业务时各部门保持职责分离

C. 企业经营目标的订立超过员工的预期

D. 企业内控政策及时口头宣布要求大家遵守

【答案】B

【解析】职责分离是公司控制环境良好的最佳体现。

【例题·单选题】

在评估企业内部控制结构的政策和程序时，主要考虑的因素是（ ）。

A. 是否能预防管理人员越权

B. 是否与控制环境相关

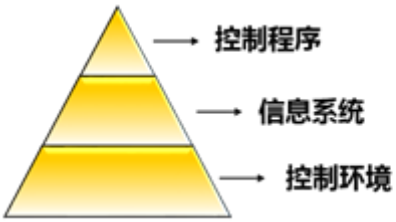
C. 是否反映管理层经营理念和经营风格

D. 是否影响财务报表的认定

【答案】D

【解析】内部控制的主要目标之一就是为财务报告的可靠性提供合理保证，即影响财务报表的认定。

内部控制的层次结构



设计（内控）系统的四大准则

1. 控制原则。控制系统有助于保护公司的资产并确保数据可靠。
2. 兼容性原则。会计系统的设计必须与企业的组织结构和人员因素保持一致。
3. 灵活性原则。会计系统必须足够灵活，交易的数量可以随组织的增长而增加。
4. 成本效益原则。会计系统所带来的好处以及所提供的信息必须等于或者大于该系统的成本。

内控的终极目标——一项关键的控制及目标：保护资产

内部控制的目的是为企业整体目标的实现提供合理的保证，包括下列五个方面。

- 资产的保护（safeguarding）
- 合规性（compliance）
- 组织目标和使命的实现（accomplishment）
- 报告（尤其是财务报告）的可靠性（reliability）
- 经营效率（efficiency）

“人事”（人力资源）控制

1. 招聘、选择、录用和监督优秀员工
2. 引导、培训、发展和绩效检查
3. 结合、轮换和休假

内部控制的类型

预防性控制

预防性控制有助于防止挪用资产和不当使用资产。

检测性控制

检测性控制通过一旦错误发生就对其进行检测来对预防性控制提供支持。

纠正性控制

纠正性控制可以改正采用检测性控制识别出来的问题。

指令性控制

与预防性控制、检测性控制以及改正性控制形成对照，指令性控制是为了产生积极结果而设计的指令。

补充性控制

补充性控制也称为缓和性控制，用来弥补控制结构中其他方面的不足。

内部控制的局限性

即使设计良好的控制系统也可能会失效。可能会对设计良好的系统造成伤害的重要威胁包括：

1. 管理层不执行相关的控制。

2. 员工之间、员工与外部人（如顾客或供应商）之间相互勾结。

3. 其他固有的缺陷包括失误、误解、判断上的错误以及对控制的成本 / 效益的权衡（即完美的控制成本太昂贵而无法实施）。

第 67 讲-公司治理，风险与合规性（4）

第 1 节 公司治理，风险与合规性（4）

内部控制

内部控制的相关法律法规

从美国企业和财务视角来看，企业内部控制的要求来自于：

1.《美国海外贪腐防治法》（FCPA）

2.《萨班斯 - 奥克斯利法案》（SOX）

《美国海外贪腐防治法》（FCPA）

《美国海外贪腐防治法》（FCPA）于 1977 年推出，针对在美国上市的公司，由美国证券交易委员会（SEC）全面监管。（旨在防范）

1.不道德海外商业行为 - 禁止向海外政府和官员行贿。

2.防止潜在的洗钱，与资产流失行为 - 要求制作保存账目，记录和账户，并维护一个内部会计控制系统。该系统应能为以下方面提供合理的保证：

1.交易按照管理层的一般授权或具体授权来执行。

2.必要时记录交易，以便使得财务报表的编制符合公认会计原则（GAAP）或其他适用标准的要求，并维持资产会计责任。

3.只有获得管理层的一般授权或具体授权，才被允许接触资产。

4.在合理的时间间隔内将记录的资产与实有资产相比较，并采取适当的措施处理二者之间的差异。

《萨班斯 - 奥克斯利法案》 - 对事务所的要求

- 21 世纪初的安然等公司的财务丑闻，促成了《萨班斯 - 奥克斯利法案》（SOX）于 2002 年 7 月 30 日正式签署实施。
- 法案包含了影响上市公司及其高管，以及审计师。
- 同时美国证监会成立“上市公司会计督察机构 PCAOB“ 对上市公司的审计师事务所进行监管与督察。

教材中，主要提到了三个“责任人”在法规下被要求的责任。

1. 管理层的责任；

2. 审计师的责任；

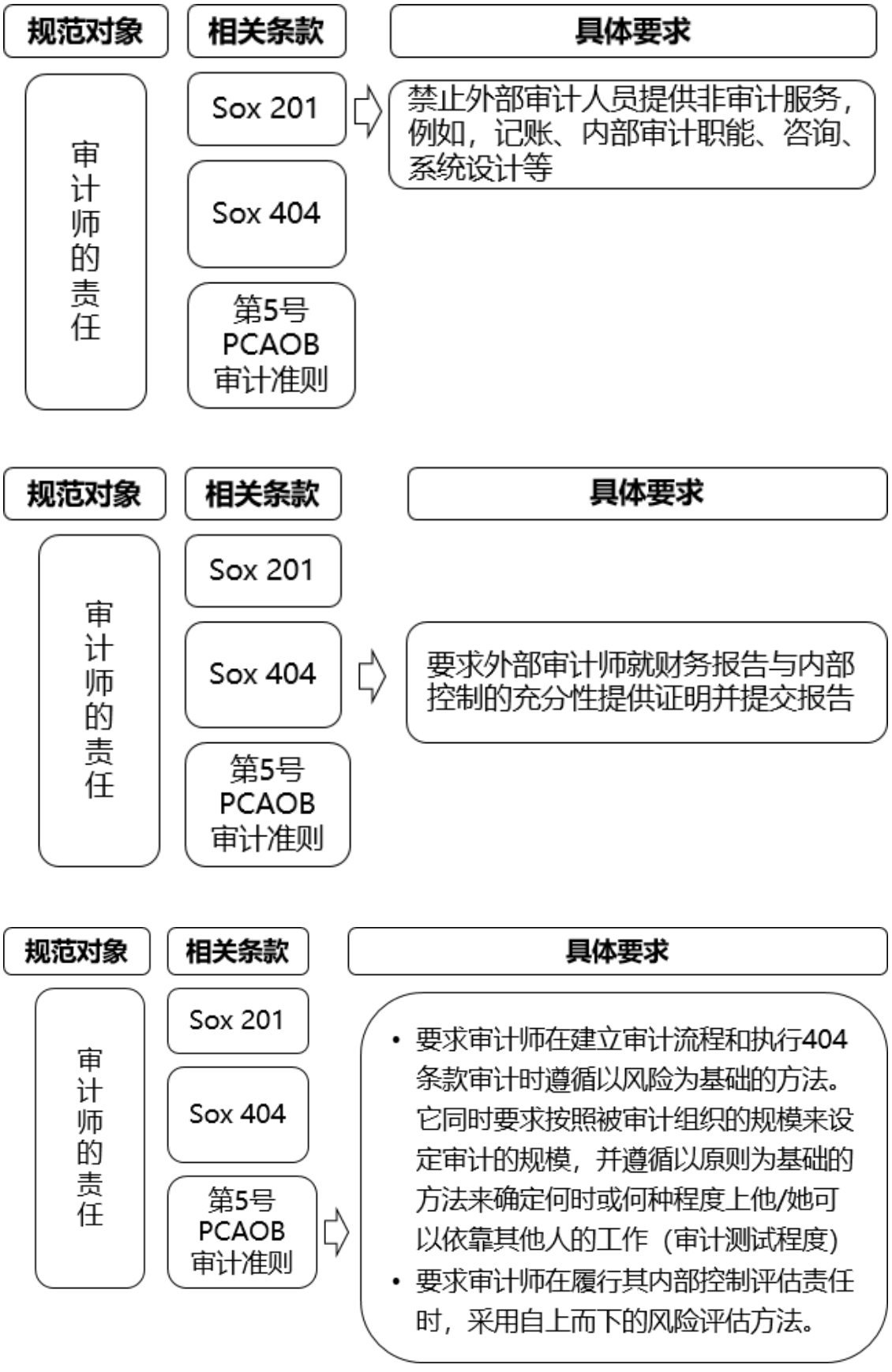
3. 审计委员会的责任。

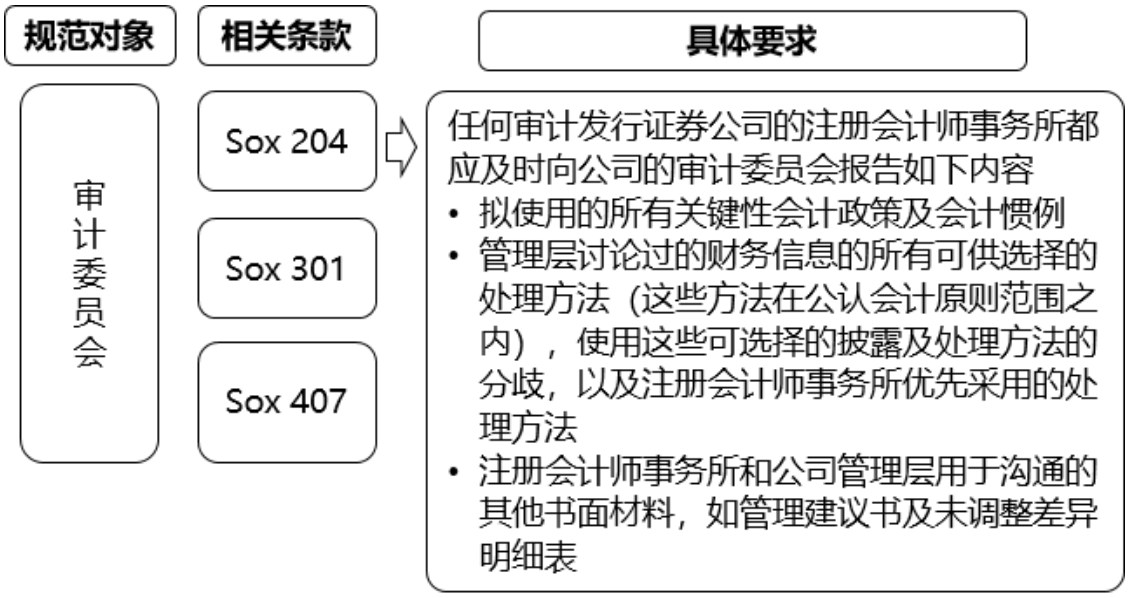
《萨班斯 – 奥克斯利法案》

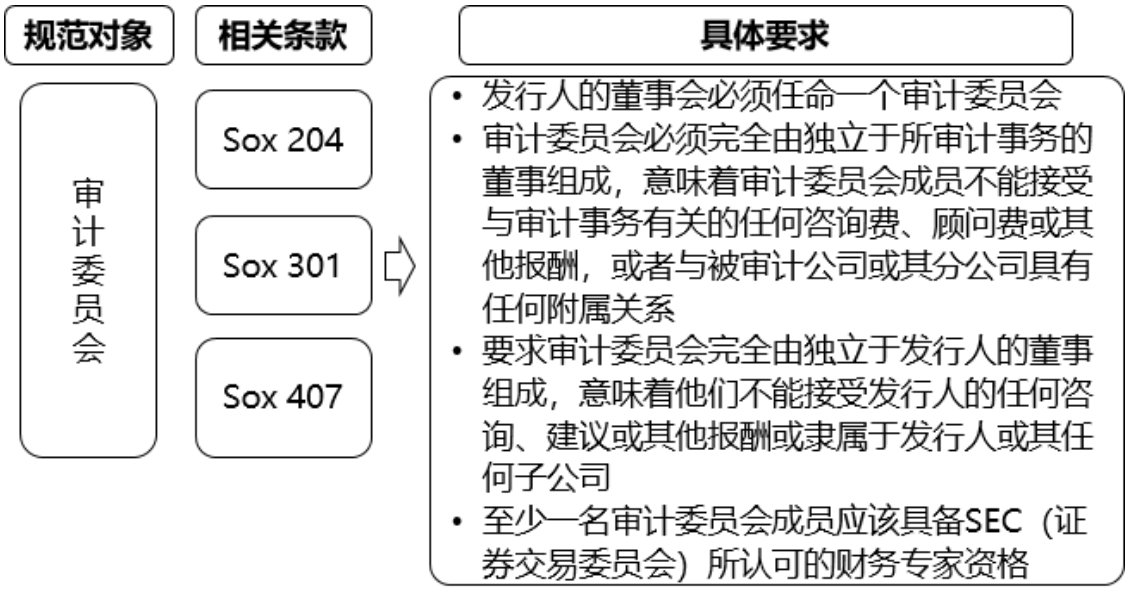
规范对象	相关条款	具体要求
管理层的责任	Sox 203	要求公司至少5年更换一次负责审计的审计合伙人
	Sox 302	
	Sox 404	

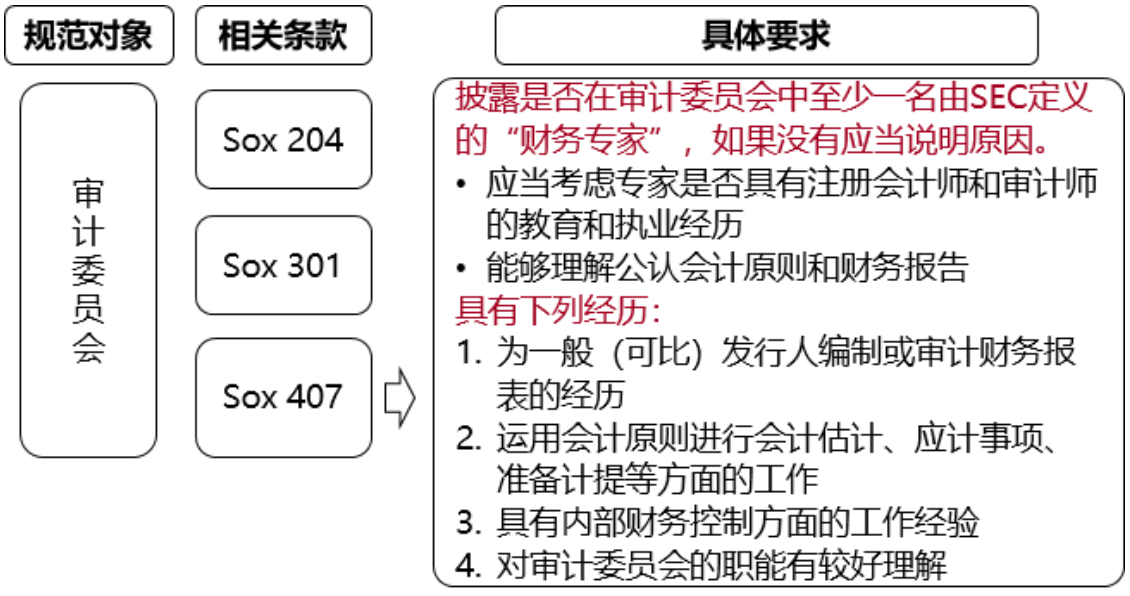
规范对象	相关条款	具体要求
管理层的责任	Sox 203	• 要求上市公司的CEO和CFO核实公司的季度和年度财务报告，并要求公司管理层设计和实施内部控制，确保可靠财务报告的编制 • 要求公众公司主要经理人对公司财务报告的准确性和完整性做出保证，进而保证财务报告的真实性
	Sox 302	
	Sox 404	

规范对象	相关条款	具体要求
管理层的责任	Sox 203	• 要求制定和实施内部控制制度，并由外部审计师进行审计 • 管理层必须在文件中证明他们评估内部控制结构和流程的效果符合要求 • 要求管理层每年都要证明：管理层负责内部控制；内部控制已设计到位，并能对财务活动提供充分的披露；已就内部控制的有效性进行评估 • 要求会计年报中必须包含内部控制自评报告和管理层提供建立和维护内部控制结构的充分性的责任声明
	Sox 302	
	Sox 404	


规范对象
相关条款
具体要求
审计师的责任
Sox 201
Sox 404
第5号PCAOB审计准则
禁止外部审计人员提供非审计服务，例如，记账、内部审计职能、咨询、系统设计等
规范对象
相关条款
具体要求
审计师的责任
Sox 201
Sox 404
第5号PCAOB审计准则
要求外部审计师就财务报告与内部控制的充分性提供证明并提交报告
规范对象
相关条款
具体要求
审计师的责任
Sox 201
Sox 404
第5号PCAOB审计准则
• 要求审计师在建立审计流程和执行404条款审计时遵循以风险为基础的方法。它同时要求按照被审计组织的规模来设定审计的规模，并遵循以原则为基础的方法来确定何时或何种程度上他/她可以依靠其他人的工作（审计测试程度）
• 要求审计师在履行其内部控制评估责任时，采用自上而下的风险评估方法。







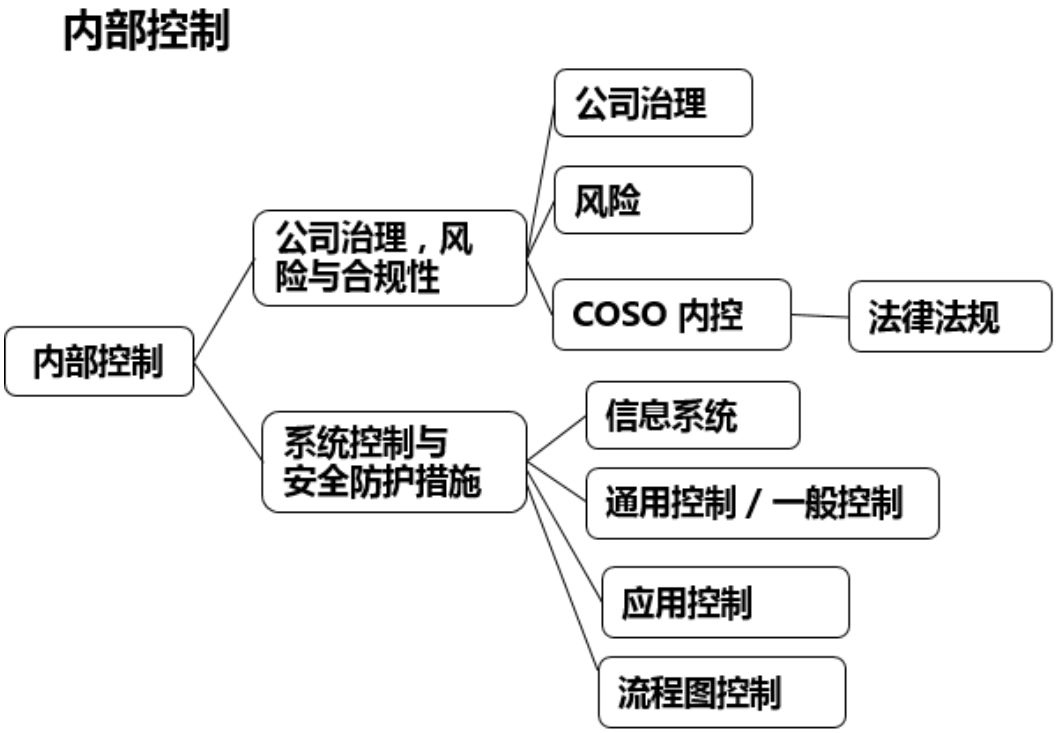
【例题 • 单选题】

根据萨班斯奥克斯利法案（SOX）的要求，下列各项描述都是正确的，除了（ ）。

A.管理层需要声明对公司内部控制负责
B.管理层声明设计内部控制程序是审计委员会的责任
C.管理层声明需要对内部控制的评估工作负责
D.需要有独立的外部审计对内部控制进行审计
【答案】B
【解析】设计内部控制不是审计委员会的责任，而是管理层的责任。
【例题 • 单选题】
根据萨班斯奥克斯利法案对公司的要求，公司最高管理层的职责有哪些（ ）。
A.负责建立和维护内控系统并做出声明
B.管理层负责对外与法律人士沟通
C.管理层和审计委员会的职责不需要独立
D.管理层兼任公司的独立董事
【答案】A
【解析】最高管理层需要负责建立和维护内控系统，并为此做出声明。
【例题 • 单选题】
以下行为都违反了“美国海外贪腐防治法”，除了（ ）。
A.为了更快取得外国政府的批准文件，赠送给外国官员的小礼物
B.把款项直接付给外国政府官员
C.帮助外国政府官员安排住宿
D.与外国的海关人员联系过关事宜
【答案】D
【解析】A、B、C选项内容都违反了“美国海外贪腐防治法”，D选项没有违反。
【例题 • 单选题】
美国萨班斯奥克斯利法案中第404条款要求上市公司管理层（ ）。
A.证明管理层没有舞弊行为
B.评估风险报告中的内控
C.设计内部控制
D.披露内部控制的重大变化
【答案】D
【解析】404条款要求管理层每年都要证明：管理层负责内部控制；内部控制已设计到位，并能对财务活动提供充分的披露，已就内部控制的有效性进行评估。要求会计年报中必须包括内部控制自评报告和管理层提供建立和维护内部控制结构的充分性的责任声明。B选项，并非评估风险报告中的内控，而是对“内部控制的有效性”进行评估。C选项，该条款要求管理层证明内部控制已经设计到位，而非要求管理层设计内部控制。404条款要求如果企业的内部控制发生了重大变化，管理层需要披露。

第68讲-系统控制安全防护措施

第2节 系统控制和安全防护措施



信息系统

系统控制和安全防护措施

信息是任何公司的关键资产，内部控制必须保护这项资产。存储在计算机系统上的信息遭遇丢失或不准确的可能原因如下：

- 计算机或网络崩溃 / 自然灾害或盗窃
- 输入或应用程序出现人为错误 / 对输入数据的篡改
- 对记录或程序的故意更改 / 破坏
- 软件缺陷
- 计算机病毒和蠕虫 / 特洛伊木马程序和其他计算机系统威胁

常见的信息系统控制措施

信息系统通常分为两大功能：财务会计信息系统和运营信息系统。

1. 财务会计：信息系统为管理人员生成企业的财务报表、预算和成本报告。

2. 运营信息：系统收集与各种业务活动有关的信息并为管理人员生成报告。

与信息系统相关的风险

1. 输入操纵（输入错误数据）。

2. 程序变更（通过天窗绕过安全系统变更程序）。

3. 直接修改文件；数据被盗；蓄意破坏。

4. 病毒（将一种恶意软件植入电脑程序、数据文件中，当执行该恶意软件时，它会对电脑程序、数据文件或电脑硬盘产生破坏作用）。

5. 木马程序（在一些明显无害程序或数据中包含恶意或有害代码的程序，进而控制或对它选择的文件产生破坏作用）。

6. 钓鱼软件（通常以精心设计的虚假网页引诱用户上当，达到盗取用户名、密码、信用卡信息或社会安全号码等目的）。

常见的信息系统控制措施

信息系统控制措施由通用控制和应用控制组成。

通用控制（也称为普适控制，一般控制）是与计算机技术或信息技术（IT）功能相关的控制。它们包括：

1. 组织、人员和运营控制

2. 系统开发控制

3. 网络、硬件和设备控制

4. 备份和灾难恢复控制

5. 会计控制

通用控制 / 一般控制

组织、人员和运营控制

职责分离

职能与组织的其他职能相分离。

职能内的系统开发（应用程序员、分析师）、操作（计算机操作员、输入/输出操作员）和技术支持（网络管理员、数据库管员、安全管理员、系统程序员）相互分离。

休假规定

要求特定职位的人员定期休假一定时间。

在这种机制下，任何账户欺诈行为都很快会被发现。

计算机访问控制

用户授权。

访问权限。

实施跟踪异常访问或异常使用。

系统开发控制

系统开发生命周期四阶段：

分析：了解系统本身、确立合适的设计规格（注：内审不能参与系统分析）。

设计：确立系统规格，用书面形式详细记录各项规格要求。

实施：系统通过测试，得到用户接受并批准对外发布后，由原有系统向新系统转换。

维护：监控新系统的运行，确保其达到设计目的（定期在应用低峰的时段维护）。

数据安全

数据通过一个逻辑的安全系统被保护，这也被称为**逻辑访问控制**。

- 只有授权的用户有权访问数据；
- 权限的水平应该适用于工作需求；
- 数据的修改应伴随着一个完整的审计跟踪流程；
- 未经授权的访问应被拒绝并报告。

密码控制

- 密码加密；
- 制定天数要求强制更改密码；
- 要求密码的结构（强度）；
    - 至少有四个字节，由数字或字母组成；
    - 永远不要设置过于简单的密码，这样别人就可以很容易地把它们猜出来。

访问授权

- 磁条门禁卡
- 生物特征验证系统

计算机中心设计

- 不显眼的位置
- 空调的能力
- 湿度和温度监测

备份和灾难恢复控制

应急计划和灾难恢复

- 一个灾难恢复计划必须落实在公司的最高水平
- 一个有足够能力从灾难中恢复的组织，应具备：
    - 异地储存关键数据，程序，操作系统和文档
    - 一个灾难事件中的详细应对步骤的规划文件
    - 异地加工场所
    - 关键应用程序列表
    - 运行文档
    - 电信信息
    - 主要员工的姓名和电话号码

• 软件和硬件供应商的信息

• 替代网站的备用协议

确保数据不会因为病毒、自然灾害、偷窃、删除、硬件故障以及软件故障方面的问题而丢失。

形式：定期备份；归档；灾难恢复计划。

备用站点

• 热站：设备齐全，能够在几个小时内恢复运营，数据完整性和一致性好，数据不易丢失，投资和维护成本高。

• 冷站：只配备必要的环境条件，恢复周期长，数据完整性和一致性差，投资费用和维护费用低。

• 暖站：介于冷站和热站之间。

网络、硬件和设备控制

网络控制

使经过授权的员工可以访问和使用公司的数据和程序。

1. 数据的加密和传输
2. 病毒防护与防火墙（阻止非授权访问）
3. 入侵检测系统（安全事件日志）

会计控制

确认或质疑会计分录和财务报表所记录数据的可靠性。

批次总数、控制账户、核销或取消、反馈控制（事后行为）、前馈和预防性控制（概率预测）。

【例题 • 单选题】

企业设置防火墙是用来做什么的（ ）。

A. 限制外来访问

B. 阻止病毒、木马入侵

C. 防止内部人员泄露企业机密

D. 阻止信息系统火灾侵害

【答案】A

【解析】防火墙主要是用来限制外部非法访问。

【例题 • 单选题】

某大型企业有多个子公司，为保护企业各信息数据安全，企业只对大型子公司进行数据备份，每周备份一次。考虑到数据安全性，公司拟采取更为有效的数据安全备份。以下措施中，哪一项更适合企业采用（ ）。

A. 对所有子公司进行每周备份一次

B. 对所有子公司进行每两周备份一次

C. 对大型子公司进行每两周备份一次

D. 对小型子公司进行每周备份一次

【答案】A

【解析】备份应该定时，周期不能太长。若考虑到数据的安全性，更有效的方法是对所有的子公司进行每周备份一次。

【例题 • 单选题】

A 公司要求销售人员通过 web 利用系统录入订单，采用高度复杂的防火墙。B 公司也用相同的系统录入订单，但管理层不采用防火墙，以下哪个原因能支持 B 公司不使用防火墙输入订单（ ）。

A. B 公司从未给员工授权利用互联网输入订单

B. 利用公司网络并授权员工安全使用互联网

C. 让销售人员利用企业的安全传输线在公司位置输入订单

D. 企业给销售人员进行了详细的安全性培训

【答案】C

【解析】企业安全传输线能够代替防火墙，安全性更高。

应用控制

应用控制分为三个主要的方面：

1. 输入控制
2. 处理控制

3.输出控制

应用控制的目的：

确保所有处理均得到授权，均处理完毕，以及均得到及时处理。

输入控制

目的：

在操作人员输入数据时进行检查，及时改正错误，以确保报告数据的准确性和可靠性。

常用方法：

手工方法：批控制（批号、记录数目、控制总额、数字总和）；审批机制（审批后才能输入）；双重观测（双人监督下输入）；监督程序（获得授权后输入）

自动方法：冗余数据检查（重复数据）；对未发现的记录进行测试（有效性测试、主文件检查一实时处理和批处理）；预见检查（条件关系合理性）；预见格式化屏幕（仅有某些选项可用时、单选多选）；交互编辑（字符检查、完整性检查、上下限、范围或合理性检查、通过所有编辑检查）；校验数位（所有数字运算）。

处理控制

目的：

确保系统按规定对数据进行处理，包括能够对经济业务进行正常处理；业务数据在处理过程中没有丢失、增加、重复或不恰当的改变。

常用方法：

机器处理；标准化；默认选项；批余额；运行到运行的总计（上一个输出与下一个输入一致）；余额（总账和明细账）；配比（三单匹配）；暂记待结转账户（中转科目为0）；备忘录（按时间顺序排列待处理）；冗余处理（两个人分别计算同一数据比较是否相等）；尾部标记（顺序编号的最后一个号表示记录总数）；自动错误修正（支付额超过账户余额时会自动生成付款通知）。

输出控制

目的：

保证系统生成的数据文件及报告准确和可靠。

常用方法：

与确认处理结果相关的控制（活动报告和例外报告）；与输出结果的分发和处理相关的控制（表格控制、如何分发、分发形式、密码、访问限制）。

具体形式：

对账（总额与明细）；时效（账龄）；挂起文件（未处理完成的项目）；暂记账户；定期审计（供应商确认函）；差异报告。

流程图控制

流程图是一个符号图，该图显示系统中的数据流和操作序列。

流程图的类型：

- 系统流程图；
- 程序（块）流程图；
- 分析流程图；
- 文件流程图。

【例题 • 单选题】

在提供给审计师的技术中，以下哪项对在一个信息系统中提供一个交易过程的汇总轮廓和整体描述是最有价值的（ ）。

A.交易检索

B.测试程序叠

C.软件代码比较

D.流程图

【答案】D

【解析】流程图用以对系统开发以及内部控制结构的理解。测试程序（testing program），是通过检测，可以对设备或系统的功能正确性进行测定，并在显示器上给出相应的信息。

【例题 • 单选题】

National Manufacturing 公司的数据录入人员有责任将所有公司的运输信息转换为计算机记录。当运输部门将装货单复印件发送给数据录入人员时，信息流开始形成。数据录入员将装货单信息存入便携式数据储存设备，检验员检验对比计算机记录和原始装货单。检验和修订必要的特定批次文件时，相关信息将上传至公司总部的主机。将这一系列活动更加形象化、易理解地展示出来的最有效方法是（ ）。

A. 程序流程图

B. 决策表

C. 文件流程图

D. 甘特图

【答案】C

【解析】流程图是指利用大量绘图标志代表某一过程。文件流程图形象化地展示了文件（如送货单复印件）在不同部门间的流转，是一种有效方法。

#