第二节　风险管理体系

三、内部控制的要素

2.风险评估

（1）COSO《内部控制框架》关于风险评估要素的要求

①前提：每个企业都面临诸多来自内部和外部的有待评估的风险。风险评估的前提是使经营目标在不同层次上相互衔接、保持一致。

②内容：风险评估指识别、分析相关风险以实现既定目标，从而形成风险管理的基础。由于经济、产业、法规和经营环境的不断变化，需要确立一套机制来识别和应对由这些变化带来的风险。

（2）COSO《内部控制框架》关于风险评估要素的原则

①企业制定足够清晰的目标，以便识别和评估有关目标所涉及的风险

②企业从整个企业的角度来识别实现所涉及的风险，分析风险，并据此决定应如何管理这些风险

③企业在评估影响目标实现的风险时，考虑潜在的舞弊行为

④企业识别并评估可能会对内部控制系统产生重大影响的变更

（3）我国《基本规范》关于风险评估要素的要求

①企业应当根据设定的控制目标，全面系统持续地收集相关信息，结合实际情况，及时进行风险评估

②企业开展风险评估，应当准确识别与实现控制目标相关的内部风险和外部风险，确定相应的风险承受度。风险承受度是企业能够承担的风险限度，包括整体风险承受能力和业务层面的可接受风险水平。

③企业识别内部风险，应当关注下列因素：

▷董事、监事、经理及其他高级管理人员的职业操守、员工专业胜任能力等人力资源因素

▷组织机构、经营方式、资产管理、业务流程等管理因素

▷研究开发、技术投入、信息技术运用等自主创新因素

▷财务状况、经营成果、现金流量等财务因素

▷营运安全、员工健康、环境保护等安全环保因素

▷其他有关内部风险因素

④企业识别外部风险，应当关注下列因素：

▷经济形势、产业政策、融资环境、市场竞争、资源供给等经济因素

▷法律法规、监管要求等法律因素

▷安全稳定、文化传统、社会信用、教育水平、消费者行为等社会因素

▷技术进步、工艺改进等科学技术因素

▷自然灾害、环境状况等自然环境因素

▷其他有关外部风险因素

⑤企业应当采用定性与定量相结合的方法，按照风险发生的可能性及其影响程度等，对识别的风险进行分析和排序，确定关注重点和优先控制的风险。企业进行风险分析，应当充分吸收专业人员，组成风险分析团队，严格按照规范的程序开展工作，确保风险分析结果的准确性。

⑥企业应当根据风险分析的结果，结合风险承受度，权衡风险与收益，确定风险应对策略。企业应当合理分析、准确掌握董事、经理及其他高级管理人员、关键岗位员工的风险偏好，采取适当的控制措施，避免因个人风险偏好给企业经营带来重大损失。

⑦企业应当综合运用风险规避、风险降低、风险分担和风险承受等风险应对策略，实现对风险的有效控制。
⑧企业应当结合不同发展阶段和业务拓展情况，持续收集与风险变化相关的信息，进行风险识别和风险分析，及时调整风险应对策略。

3.控制活动
（1）COSO《内部控制框架》关于控制活动要素的要求
①概念：控制活动指那些有助于管理层决策顺利实施的政策和程序。
②作用：控制行为有助于确保实施必要的措施以管理风险，实现经营目标。控制行为体现在整个企业的不同层次和不同部门中。

（2）COSO《内部控制框架》关于控制活动要素的原则
①企业选择并制定有助于将目标实现风险降低至可接受水平的控制活动
②企业为用以支持目标实现的技术选择并制定一般控制政策
③企业通过政策和程序来部署控制活动：政策用来确定期望的目标；程序则将政策付诸行动。

（3）我国《基本规范》关于控制活动要素的要求
①企业应当结合风险评估结果，通过手工控制与自动控制、预防性控制与发现性控制相结合的方法，运用相应的控制措施，将风险控制在可承受度之内。控制措施一般包括：不相容职务分离控制、授权审批控制、会计系统控制、财产保护控制、预算控制、运营分析控制和绩效考评控制等。

②不相容职务分离控制要求企业全面系统地分析、梳理业务流程中所涉及的不相容职务，实施相应的分离措施，形成各司其职、各负其责、相互制约的工作机制。

③授权审批控制要求企业根据常规授权和特别授权的规定，明确各岗位办理业务和事项的权限范围、审批程序和相应责任。企业应当编制常规授权的权限指引，规范特别授权的范围、权限、程序和责任，严格控制特别授权。常规授权是指企业在日常经营管理活动中按照既定的职责和程序进行的授权。特别授权是指企业在特殊情况、特定条件下进行的授权。

④会计系统控制要求企业严格执行国家统一的会计准则制度，加强会计基础工作，明确会计凭证、会计账簿和财务会计报告的处理程序，保证会计资料真实完整。企业应当依法设置会计机构，配备会计从业人员。从事会计工作的人员，必须取得会计从业资格证书。会计机构负责人应当具备会计师以上专业技术职务资格。大中型企业应当设置总会计师，设置总会计师的企业，不得设置与其职权重叠的副职。

⑤财产保护控制要求企业建立财产日常管理制度和定期清查制度，采取财产记录、实物保管、定期盘点、账实核对等措施，确保财产安全。企业应当严格限制未经授权的人员接触和处置财产。

⑥预算控制要求企业实施全面预算管理制度，明确各责任单位在预算管理中的职责权限，规范预算的编制、审定、下达和执行程序，强化预算约束。

⑦运营分析控制要求企业建立运营情况分析制度，经理层应当综合运用生产、购销、投资、筹资、财务等方面的信息，通过因素分析、对比分析、趋势分析等方法，定期开展运营情况分析，发现存在的问题，及时查明原因并加以改进。

⑧绩效考评控制要求企业建立和实施绩效考评制度，科学设置考核指标体系，对企业内部各责任单位和全体员工的业绩进行定期考核和客观评价，将考评结果作为确定员工薪酬以及职务晋升、评优、降级、调岗、辞退等的依据。

⑨企业应当建立重大风险预警机制和突发事件应急处理机制，明确风险预警标准，对可能发生的重大风险或突发事件，制定应急预案、明确责任人员、规范处置程序，确保突发事件得到及时妥善处理。

【多选题】隆盛信托投资公司自成立以来，结合业务特点和内部控制要求设置内部机构，明确职责权限，将权力和责任落实到责任单位，同时综合运用风险规避、风险降低、风险分担和风险承受等风险应对策略，实现对风险的有效控制。根据我国《企业内部控制基本规范》，该公司的上述做法涉及的内部控制要素有（　）。
A.风险评估
B.控制环境
C.信息与沟通
D.控制活动

答案：AB
解析：“综合运用风险规避、风险降低、风险分担和风险承受等风险应对策略，实现对风险的有效控制”属于风险评估，选项 A 正确。“结合业务特点和内部控制要求设置内部机构，明确职责权限，将权力和责任落实到责任单位”属于控制环境，选项 B 正确。

【单选题】凌云公司近年来不断加强企业内部控制体系建设，在董事会下设立了审计委员会。审计委员会负责审查企业内部控制，监督内部控制的有效实施和内部控制自我评价情况，协调内部控制审计及其他相关事宜。根据 COSO《内部控制框架》，凌云公司的上述做法属于内部控制要素中的（　）。
A.风险评估
B.控制活动
C.监控
D.控制环境

答案：D
解析：企业应当在董事会下设立审计委员会。审计委员会负责审查企业内部控制，监督内部控制的有效实施和内部控制自我评价情况，协调内部控制审计及其他相关事宜等。根据 COSO
《内部控制框架》，属于控制环境的范畴，选项 D 正确。

4.信息沟通
（1）COSO《内部控制框架》关于信息与沟通要素的要求
①公允的信息必须被确认、捕获并以一定形式及时传递，以便员工履行职责。
②信息系统产出涵盖经营、财务和遵循性信息的报告，以助于经营和控制企业。
③信息系统不仅处理内部产生的信息，还包括与企业经营决策和对外报告相关的外部事件、行为和条件等。

④有效的沟通从广义上说是信息的自上而下、横向以及自下而上的传递。所有员工必须从管理层得到准确的信息，认真履行控制职责。员工必须理解自身在整个内控系统中的位置，理解个人行为与其他员工工作的相关性。员工必须有向上传递重要信息的途径。同时，与外部诸如客户、供应商、管理当局和股东之间也需要有效的沟通。

（2）COSO《内部控制框架》关于信息与沟通要素的原则
①企业获取或生成和使用相关的高质量信息，以支持内部控制其他要素发挥效用
②企业于内部沟通的内部控制信息，包括内部控制目标和职责范围，必须能够支持内部控制的其他要素发挥效用

③企业就影响内部控制其他要素发挥效用的事项与外部方进行沟通

（3）我国《基本规范》关于信息与沟通要素的要求

①企业应当建立信息与沟通制度，明确内部控制相关信息的收集、处理和传递程序，确保信息及时沟通，促进内部控制有效运行。

②企业应当对收集的各种内部信息和外部信息进行合理筛选、核对、整合，提高信息的有用性。企业可以通过财务会计资料、经营管理资料、调研报告、专项信息、内部刊物、办公网络等渠道获取内部信息。企业可以通过行业协会组织、社会中介机构、业务往来单位、市场调查、来信来访、网络媒体以及有关监管部门等渠道获取外部信息。

③企业应当将内部控制相关信息在企业内部各管理级次、责任单位、业务环节之间以及企业与外部投资者、债权人、客户、供应商、中介机构和监管部门等有关方面之间进行沟通和反馈。信息沟通过程中发现的问题，应当及时报告并加以解决。重要信息应当及时传递给董事会、监事会和经理层。

④企业应当利用信息技术促进信息的集成与共享，充分发挥信息技术在信息与沟通中的作用。企业应当加强对信息系统开发与维护、访问与变更、数据输入与输出、文件储存与保管、网络安全等方面的控制，保证信息系统安全稳定运行。

⑤企业应当建立反舞弊机制，坚持惩防并举、重在预防的原则，明确反舞弊工作的重点领域、关键环节和有关机构在反舞弊工作中的职责权限，规范舞弊案件的举报、调查、处理、报告和补救程序。企业至少应当将下列情形作为反舞弊工作的重点：
▷未经授权或者采取其他不法方式侵占、挪用企业资产，牟取不当利益

▷在财务会计报告和信息披露等方面存在的虚假记载、误导性陈述或者重大遗漏等
▷董事、监事、经理及其他高级管理人员滥用职权
▷相关机构或人员串通舞弊

⑥企业应当建立举报投诉制度和举报人保护制度，设置举报专线，明确举报投诉处理程序、办理时限和办结要求，确保举报、投诉成为企业有效掌握信息的重要途径。举报投诉制度和举报人保护制度应当及时传达至全体员工。

5.监控
（1）COSO《内部控制框架》关于监控要素的要求
①内部控制系统需要被监控，即对该系统有效性进行评估的全过程。可以通过持续性的监控行为、独立评估或两者结合来实现对内控系统的监控。

②持续性的监控行为发生在企业的日常经营过程中，包括企业的日常管理和监督行为、员工履行各自职责的行为。
③独立评估活动的广度和频度有赖于风险预估和日常监控程序的有效性。内部控制的缺陷应该自下而上进行汇报，性质严重的应上报最高管理层和董事会。

（2）COSO《内部控制框架》关于监控要素的原则
①企业选择并制定有助于将目标实现风险降低至可接受水平的控制活动
②企业为用以支持目标实现的技术选择制定一般控制政策
③企业通过政策和程序来部署控制活动：政策用来确定所期望的目标；程序则将政策付诸行动

（3）我国《基本规范》关于内部监督要素的要求
①企业应当根据本规范及其配套办法，制定内部控制监督制度，明确内部审计机构（或经授权的其他监督机构）和其他内部机构在内部监督中的职责权限，规范内部监督的程序、方法和要求。

②企业应当制定内部控制缺陷认定标准，对监督过程中发现的内部控制缺陷，应当分析缺陷的性质和产生的原因，提出整改方案，采取适当的形式及时向董事会、监事会或者经理层报告。
内部控制缺陷包括设计缺陷和运行缺陷。企业应当跟踪内部控制缺陷整改情况，并就内部监督中发现的重大缺陷，追究相关责任单位或者责任人的责任。

③企业应当结合内部监督情况，定期对内部控制的有效性进行自我评价，出具内部控制自我评价报告。内部控制自我评价的方式、范围、程序和频率，由企业根据经营业务调整、经营环境变化、业务发展状况、实际风险水平等自行确定。

④企业应当以书面或者其他适当的形式，妥善保存内部控制建立与实施过程中的相关记录或者资料，确保内部控制建立与实施过程的可验证性。

考点 5　风险管理信息系统★
企业的管理信息系统在风险管理中发挥着至关重要的作用。
企业应将信息技术应用于风险管理的各项工作，建立涵盖风险管理基本流程和内部控制系统各环节的风险管理信息系统，包括信息的采集、存储、加工、分析、测试、传递、报告、披露等。

1.信息采集方面
企业应采取措施确保向风险管理信息系统输入的业务数据和风险量化值的一致性、准确性、及时性、可用性和完整性。
2.信息存储方面
企业应建立良好的数据架构，解决好数据标准化和存储技术问题。信息加工、分析和测试方面。

3.信息加工、分析和测试方面
风险基础信息经风险管理信息系统加工和提炼，成为可进行分析的风险管理信息。风险管理信息系统应能够进行对各种风险的计量和定量分析、定量测试；能够实时反映风险矩阵和排序频谱、重大风险和重要业务流程的监控状态。

4.信息传递方面
风险管理信息系统应实现信息在各职能部门、业务单位之间的集成与共享，既能满足单项业务风险管理的要求，也能满足企业整体和跨职能部门、业务单位的风险管理综合要求。
5.信息报告和披露方面
风险管理信息系统能够对超过风险预警上限的重大风险实施信息报警；能够满足风险管理内部信息报告制度和企业对外信息披露管理制度的要求。

本节小结