

**南海发展股份有限公司**  
**内部控制手册**  
**内部控制评价工作方法论分册**

# 目录

|                          |    |
|--------------------------|----|
| 第一部分 综述.....             | 4  |
| 1.1 意义和目的.....           | 4  |
| 1.2 基本原则.....            | 4  |
| 1.3 编制依据.....            | 4  |
| 1.4 适用范围、功能和管理.....      | 5  |
| 1.5 内部控制的目标.....         | 5  |
| 1.6 内部控制有效性评估框架.....     | 6  |
| 1.7 内部控制建设和自我评价工作流程..... | 7  |
| 第二部分 风险信息的识别.....        | 8  |
| 2.1 信息收集与识别.....         | 8  |
| 2.2 风险评价.....            | 8  |
| 第三部分 项目范围的制定.....        | 10 |
| 3.1 确定评价范围的主要步骤.....     | 10 |
| 3.2 从财务报告的角度厘定项目范围.....  | 11 |

|                                   |    |
|-----------------------------------|----|
| 3.3 项目范围设定的其他考虑.....              | 15 |
| 第四部分 内部控制设计有效性评价.....             | 16 |
| 4.1 内部控制要素.....                   | 16 |
| 4.2 内部控制描述方法概述.....               | 17 |
| 4.3 内部控制分类.....                   | 17 |
| 4.4 信息系统的相关控制.....                | 18 |
| 4.5 财务报告认定.....                   | 19 |
| 4.6 内部控制设计有效性测试方法.....            | 19 |
| 4.7 评价内部控制在设计上的有效性.....           | 20 |
| 第五部分 内部控制执行有效性评价.....             | 21 |
| 5.1 内部控制执行有效性测试内容.....            | 21 |
| 5.2 内部控制执行有效性测试方法.....            | 21 |
| 第六部分 内部控制缺陷评价.....                | 23 |
| 6.1 内部控制缺陷的类型.....                | 23 |
| 6.2 《企业内部控制基本规范》对内部控制缺陷评价的要求..... | 24 |
| 6.3 内部控制缺陷的评估标准.....              | 24 |
| 第七部分 内部控制评价报告.....                | 26 |
| 7.1 内部控制评价报告的基本内容.....            | 26 |
| 7.2 内部控制评价报告披露要求.....             | 26 |

## 第一部分 综述

### 1.1 意义和目的

为了加强和规范公司的内部控制，进一步提升公司的治理水平和防范风险的能力，合理确保公司经营管理合法合规、资产安全、财务报告及相关信息真实完整，提高经营效率和效果，促进公司实现总体发展战略目标，现根据国家财政部等五部委颁布的《企业内部控制基本规范》（以下简称“《基本规范》”）及相关配套指引的要求，并结合本公司实际情况，特制定本《内部控制手册》（以下简称“本手册”）并组织实施。

### 1.2 基本原则

公司开展内部控制体系建设工作遵循以下工作原则：

（一）**全面性原则**。内部控制应当贯穿决策、执行和监督全过程，覆盖公司及其所属单位的各种业务和事项。

（二）**重要性原则**。内部控制应当在全面控制的基础上，关注重要业务事项和高风险领域。

（三）**制衡性原则**。内部控制应当在治理结构、机构设置及权责分配、业务流程等方面形成相互制约、相互监督，同时兼顾运营效率。

（四）**适应性原则**。内部控制应当与公司经营规模、业务范围、竞争状况和风险水平等相适应，并随着情况的变化及时加以调整。

（五）**成本效益原则**。内部控制应当权衡实施成本与预期效益，以适当的成本实现有效控制。

### 1.3 编制依据

本手册以财政部、证监会、审计署、银监会、保监会五部委发布的《基本规范》相关配套指引为基础，结合相关法律法规要求、行业管理以及公司制度的具体流程制度要求等作为手册编制的基础，主要包括：

- 《基本规范》及相关配套指引，包括18项《企业内部控制应用指引》、《企业内部控制评价指引》、《企业内部控制审计指引》；
- 美国COSO委员会《企业风险管理整合框架》；
- 国务院国资委《中央企业全面风险管理指引》；
- 公司现有的各项管理制度及业务流程。

## 1.4 适用范围、功能和管理

### 1.4.1 适用范围

本手册所描述的内部控制体系覆盖并适用于南海发展股份有限公司总部（以下简称“公司总部”）及佛山市南海绿电再生能源有限公司（以下简称“绿电”）的所有项目范围内涉及的相关管理部门。本手册的内部控制体系涉及公司总部与绿电的所有关键业务和管理活动。

各下属公司可参考本手册的业务流程描述结合本公司的实际情况执行相关业务流程，并根据业务流程的实际情况编写适用于本公司的内部控制手册。下属公司应比照本手册，对内部控制框架和其中涉及的业务流程进行差异分析，并就差异产生的原因进行说明。

### 1.4.2 功能

本手册是一套科学、系统的内部控制体系建设方法和标准，是公司建设并实施内部控制体系的纲领性文件。本手册对公司领导、公司所属各部门的管理层及员工具有约束力，各相关人员应当遵循手册中对其工作职责的定义及描述，保持内部控制的有效性，保证公司战略目标的实现。

本手册明确了内控控制建设与自我评价工作目标、基本工作原则、工作流程以及关键业务流程等内容，是指导公司开展年度内部控制建设和自我评价工作的关键项目成果，公司每年应遵循本手册的工作原则和流程，组织相关部门及下属公司开展内控建设与自我评价工作。

### 1.4.2 管理与维护

公司董事会审计委员会办公室（以下简称“审计办”）对本手册进行规范管理，以确保其有效、完整、统一和适用。由审计办组织编写，公司董事会审计委员会（以下简称“审计委员会”）审议，公司董事会批准后正式发布实施。

本手册的修订、维护由审计办负责。每年，审计办将根据相关法律法规的要求、内外部审计对公司内部控制的评价、公司内控管理中出现的新问题等，对本手册进行修订，审计委员会审议，经公司董事会批准执行。

本手册是公司重要文件，属公司机密。各部门/公司应按相关要求正确使用，未经允许，不得复印，不得对外泄露。在使用过程中遇到疑难问题，及时向审计办咨询。

## 1.5 内部控制的目标

《企业内部控制基本规范》对内部控制定义如下：

**内部控制：**是企业董事会、监事会、经理层和全体员工实施的、旨在实现控制目标的过程。

内部控制的目标为：

- 提高经营的效率和效果；
- 合理保证财务报告和相关信息的真实完整；
- 合理保证公司经营管理合法合规；
- 合理保证资产安全；
- 促进公司实现发展战略。

1.6 内部控制有效性评估框架

按照《企业内部控制基本规范》及相关配套指引中的要求，内部控制的整体框架包含以下五大要素：

- **内部环境** - 是公司实施内部控制的基础，一般包括治理结构、机构设置及权责分配、内部审计、人力资源政策、企业文化等；
- **风险评估** - 是公司及时识别、系统分析经营活动与实现内部控制目标相关的风险，合理确定风险应对策略；
- **控制活动** - 是公司根据风险评价结果，采用相应的控制措施，将风险控制在可承受度之内；
- **信息与沟通** - 是公司及时、准确地收集、传递与内部控制相关的信息，确保信息在公司内部、公司与外部之间进行有效沟通；
- **内部监督** - 是公司对内部控制建立与实施情况进行监督检查，评价内部控制的有效性，发现内部控制缺陷，应当及时加以改进。

根据内部控制的整体框架，公司的内部控制自我评价工作具体分为以下两个层面的内容：

- **公司层面内部控制，主要包括以下流程：**

|         |         |           |
|---------|---------|-----------|
| 1. 组织架构 | 4. 社会责任 | 7. 全面预算   |
| 2. 发展战略 | 5. 合同管理 | 8. 内部信息传递 |
| 3. 人力资源 | 6. 企业文化 | 9. 信息系统   |

- 流程层面内部控制，主要包括以下流程：

|          |           |             |              |
|----------|-----------|-------------|--------------|
| 1. 资金管理  | 6. 固定资产管理 | 11. 财务报告    | 16. 安全环保     |
| 2. 投资管理  | 7. 无形资产管理 | 12. 人工与福利   | 17. 信息系统一般控制 |
| 3. 筹资管理  | 8. 工程项目管理 | 13. 税费管理    |              |
| 4. 采购与付款 | 9. 销售与收款  | 14. 费用管理    |              |
| 5. 存货管理  | 10. 研究与开发 | 15. 生产与成本管理 |              |

## 1.7 内部控制建设和自我评价工作流程

下图显示的是以风险为导向的内部控制建设和自我评价工作的基本工作流程，本手册的余下部分将对此工作流程进行详细地讲解。



## 第二部分 风险信息的识别

### 2.1 信息收集与识别

风险信息的收集与识别工作，是企业每年开展风险管控工作的起点，通过收集、识别和更新本年度企业的各项风险信息，可以更有效的协助企业开展年度风险管控工作，明确工作内容和工作重点。

企业应定期通过调查问卷、访谈及研讨会等形式向各业务单位和职能部门收集相关风险信息，识别新产生的风险信息，整理汇总并记录其衍生的风险，最终形成/更新《风险清单》。具体步骤包括：

- 1) 从战略、财务、市场、运营以及法律风险等方面广泛收集与本企业相关的重要信息，并以此作为编制《风险评估调查问卷》及开展风险信息收集工作的起点；
- 2) 由公司各业务单位和职能部门配合按要求，收集本部门涉及的风险信息，填写《风险评估调查问卷》并及时将其报送给审计办；
- 3) 审计办负责将业务部门上报的风险信息进行识别、汇总和归纳，筛选有用的风险信息，编制/更新《风险清单》初稿；
  - 与业务部门各级管理层展开访谈，确认风险信息；
  - 根据访谈结果对《风险清单》进行最终整理，形成本年度的《风险清单》；
  - 风险确认方法可采用调查问卷、小组讨论、访谈等形式。

### 2.2 风险评价

在进行风险评价之前，审计办需要对识别的风险进行分析与确认，并更新《风险清单》。步骤如下：

- 1) 识别无效风险：根据风险识别的结果，识别现有《风险清单》中失效的风险，并将其从《风险清单》中删除。失效的风险主要包括：定义和描述不清晰的风险、重复的风险、分类错误的风险和不合实际的风险等。

- 2) 向总部各部门下发更新的《风险清单》，部门负责人负责审阅更新后的《风险清单》，以确定是否覆盖了影响各专业部门业务目标实现的风险，如是，则在《风险清单》中注明“无额外风险”，如否，则在《风险清单》增加尚未包括的风险，报送审计办。

在完成了风险分析后，由审计办组织相关部门对风险进行评估，评估结果上报审计办分管领导。该阶段的工作内容包括：

1. 风险评估的准备工作：

- 根据汇总的《风险清单》的内容确定参与本次风险评估的人员范围及名单，确定风险评估的工作计划安排；
- 将更新后的《风险清单》和风险评估标准与说明及时下发；
- 组织风险评估培训，向相关人员讲解本年度的风险评估工作流程、工作安排、风险评估的方法，对风险评估标准与说明进行讲解。

2. 风险评估的执行主体是各级风险责任部门，风险评估活动主要是以更新的《风险清单》为起点，针对实际情况对风险进行评估，组织相关责任人按照《风险评估标准与说明》进行评分，由审计办对评分结果进行汇总，对风险进行排序并将评估结果更新到《风险清单》中。

3. 根据风险发生的可能性和影响程度评价标准，从定量和定性两个角度对企业各类风险进行评价，需要企业目前面临的重大风险，并在运营管理及内部控制管理中给予足够的关注。

## **第三部分 项目范围的制定**

### **3.1 确定评价范围的主要步骤**

从内部控制的目标出发，即：合理保证公司经营管理合法合规、资产安全、财务报告及相关信息真实完整、提高经营效率和效果及促进公司实现发展战略，参照《企业内部控制基本规范》及相关配套指引的要求，并结合公司的实际经营状况和业务特点，采用以风险为导向的工作方法，结合年度风险识别与评价工作的结果，将对公司经营运作有重大影响的关键风险点及业务流程纳入项目评价范围。内部控制自我评价的方式、范围、程序和频率，由公司根据经营业务调整、经营环境变化、业务发展状况、剩余风险水平等确定。

3.2 从财务报告的角度厘定项目范围

从财务报告角度厘定内部控制评价工作范围时，公司的内部控制评价人员应当考虑量化与非量化的因素。确定评价范围的主要步骤如下：

- 决定合并财务报表层次的重要性水平；
- 识别合并财务报表层次的重要会计科目及披露信息；
- 重要业务流程和重要业务单元配对。

3.2.1 确定量化考虑因素

确定量化考虑因素即确定合并财务报表的重要性水平与可容忍误差，即确定“金额重大”的水平标准。这里需要理解什么是“重要性水平”与“可容忍误差”、它们之间的关系如何：

- **重要性水平**：是指用金额额度表示的会计信息错报与漏报的严重程度，若该错报、漏报未被揭露足以影响会计信息使用者的判断或者决策。
- **可容忍误差**：是指可接受的总体中的最大误差。
- **重要性水平与可容忍误差的关系**：一般可容忍误差值为重要性水平的 50%或 75%。例如：对于连续多年财务报告数据趋势稳定、可持续经营假设不受质疑的成熟企业，往往采用重要性水平的 75%作为可容忍误差值。

根据国际通行的惯例，可以参考税前利润、税息折旧及摊销前利润、所有者权益、总资产、总收入等五个指标来确定重要性水平，这五个指标各自均有较为明确的判断标准，公司内部控制评价人员应当结合公司的实际情况来选用其中一个指标以作为确定当期财务报告相关内部控制评价范围的量化标准。五项指标的判断标准如下：

| 参考指标                   | 判断标准                                                           | 是否适用于公司                                 |
|------------------------|----------------------------------------------------------------|-----------------------------------------|
| 税前利润<br>5%-10%         | 税前利润是最为通用的参考标准。适用于连续多年盈利，且没有异常事件影响常规盈利趋势的企业。                   | 适用。公司连续多年盈利，且发展稳健，故适用税前利润作为计划重要性水平计算依据。 |
| 税息折旧及摊销前利润<br>(EBITDA) | 在少数情形下，一个企业发行公开交易的债券但没有发行公开交易的股票，EBITDA 可以作为一个适用的标准。（国内企业较少采用） | 不适用。公司是上市公司，已公开发行股票。                    |

|                       |                                                                                           |                              |
|-----------------------|-------------------------------------------------------------------------------------------|------------------------------|
| 所有者权益（净资产）<br>1% - 5% | 在某些情况下，当企业的经营水平及盈利状态不佳，资产折现力及偿付能力将成为关注点；或者，某些非公众公司，财务报告的使用者更关心所有者权益的情况下，所有者权益可以作为一个适用的标准。 | 不适用。公司连续多年盈利，且发展稳健；且公司是上市公司。 |
| 总资产<br>0.5%-1%        | 在少数情况下，当所有者权益呈快速缩小的状态，采用一个非常小比例的总资产值作为判断标准是可行的。                                           | 不适用。公司所有者权益较稳定。              |
| 总收入<br>0.5%-1%        | 当企业处于正常运营且有正的营业收入时，若上述其他标准均不适用，可采用总收入作为判断标准。                                              | 不适用。公司已符合适用税前利润标准的条件。        |

确定重要性水平与可容忍误差等量化标准均应当以年度化的合并财务报表作为计算的基准。如何确定量化标准的计算与应用请详见下表：

|                          |                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 财务报表层面的<br>量化基准——计划重要性水平 | <ul style="list-style-type: none"> <li>由于内部控制自我评价项目往往在会计年度中期就开始进行，难以等到会计年度完结出具合并财务报表数据后才启动，故判断重要性水平时，需要将中期合并财务报表进行年度化处理后作为“计划重要性水平”，以指导项目范围的制定。该计划重要性水平需要在年度合并财务报表出具后，根据年度报表的实际数据再次测算，确定最终的重要性水平值，比对其与“计划重要性水平”的差异，并对内部控制评价的范围进行修订。</li> <li>计划重要性水平=年度化的合并财务报表税前利润 x 5%<br/>（例如：半年度合并财务报表的税前利润为 36,500 万，则年度化的税前利</li> </ul> |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                            |                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 重要会计科目的<br>量化基准——可<br>容忍误差 | 润为 36,500 万 ÷ 6 个月 × 12 个月=73,000 万, 计划重要性水平=73,000 万 × 5% = 3,650 万)                                                                                                     |
|                            | <ul style="list-style-type: none"> <li>可容忍误差=计划重要性水平 × 75%<br/>(沿用上例: 可容忍误差=3,650 万 × 75% =2,737.5 万)</li> <li>超过此量化基准的为重要会计科目, 此等科目必须记录“与财务报告相关的内部控制”, 并进行测试。</li> </ul> |

除了指导项目范围的制定外, 重要性水平与可容忍误差还将作为项目后期对发现的内部控制缺陷进行性质认定的量化评估标准。

### 3.2.2 确定非量化考虑因素

确定非量化考虑因素即相关会计科目是否由于具有某些特殊的性质而需要给予特别关注, 即确定“性质重大”的水平标准。在识别重要会计科目、财务报表附注、披露项目与它们相关的财务报表认定时, 公司内部控制评价人员在内在考虑量化因素的同时, 需要考虑以下的非量化因素:

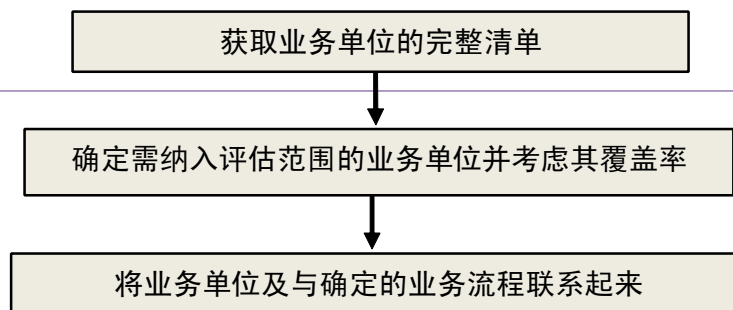
- 相关交易的数量和复杂性;
- 会计科目的性质特殊;
- 会计核算和报告披露要求的复杂性;
- 易遭人为操纵或舞弊而导致损失;
- 账户余额牵涉主观判断;
- 会计科目中反映出来的由经营活动所引起的重大或有负债的可能性;
- 存在关联方交易。

### 3.2.3 确定纳入评估范围的重要会计科目与财务报表附注

根据已经确定的量化和非量化考虑因素, 识别应纳入评估范围的重要会计科目与财务报表附注。

### 3.2.4 决定多业务单位或工作地点的覆盖比例

公司内部控制评价人员应当根据重要性原则, 根据量化的标准选取重要的业务单位纳入评价范围。因此, 在识别重要会计报表科目、财务报表附注及业务流程的风险之后, 公司内部控制评价人员需确定重要的业务单位(这里统称合并报表的母公司及控股子公司为“业务单位”), 并决定其内部控制评价的覆盖率。确定过程如下:



单个重要的业务单位至少满足以下任何一个资产负债表或利润表的量化指标：

- 超过合并报表总收入的 5%；
- 超过合并报表净资产的 5%；
- 超过合并报表税前利润的 5%；
- 超过合并报表总资产的 5%。

除根据以上量化指标以识别单个重要业务单位，还应考虑到个别业务单位的特有风险以识别特有风险单位。在确定单个重要业务单位和特有风险单位后，我们还需考虑已确定的单位占已选择的量化指标，即合并报表总收入、净资产、税前利润、总资产的百分比。确定覆盖百分比的参考标准如下：

| 参考比率   | 业务单位                 | 内部控制评价程序                                                                                                                   |
|--------|----------------------|----------------------------------------------------------------------------------------------------------------------------|
| 50-70% | 单个重要的业务单位、特有<br>风险单位 | <u>单个重要的业务单位</u><br><br>对所有已识别的重要会计科目及财务报表附注的相关重要流程和内部控制进行记录和测试，并测试公司层面的控制，除非其重要会计科目余额小于合并报表合并余额的 5%。<br><br><u>特有风险单位</u> |

| 参考比率   | 业务单位                  | 内部控制评价程序                                              |
|--------|-----------------------|-------------------------------------------------------|
|        |                       | 对其特有风险所关联的重要会计科目及财务报表附注的相关重要流程和内部控制进行记录和测试，并测试公司层面控制。 |
| 30-40% | 单独来说不重要，但合并起来是重要的业务单位 | 评估及测试公司层面的控制，如果公司层面的控制不存在，考虑获取其它证据或对该业务单位本身的控制进行测试。   |
| <10%   | 非重要业务单位               | 不需测试。                                                 |

### 3.2.5 识别业务流程并将其与重要会计科目和披露信息配对

将根据量化和非量化考虑因素选取的重要会计科目与本文1.3章节“内部控制有效性的评价架构”中确定的流程层面业务流程进行配对。例如：销售与收款流程与应收账款和主营业务收入会计科目配对。

### 3.2.6 将重要业务流程和重要业务单位配对

最后，公司内部控制评价人员需要将重要业务流程与重要业务单位配对，得出将要进行评估和测试工作的具体范围。

## 3.3 项目范围设定的其他考虑

在公司以财务报告角度初步厘定项目范围后，还应结合年度战略目标、管理层重点关注的领域、风险评估结果、外部经营环境变化、业务发展情况及实际经营运作情况等因素，对内控评价项目范围进行适当调整，以确保工作范围的完整性和合理性。

## 第四部分 内部控制设计有效性评价

### 4.1 内部控制要素

内部控制是指由企业董事会、监事会、经理层和全体员工实施的、旨在实现控制目标的过程，其包括每个重要流程及子流程的交易发起、审批授权、记录、处理和报告的过程。

- **发起**——因一项交易的发生而产生的应承担的权力或义务、增加的资产或负债，即交易记录的起点。
- **审批授权**——在交易执行或记录之前，有独立的审批授权，对业务的执行进行授权批准。
- **记录**——每项交易一旦发起，必须在交易的过程中将相关的控制过程及关键控制点进行记录。
- **处理**——必须正确执行交易过程中的信息，以确保交易记录的准确性。
- **报告**——营运过程中产生信息的汇报过程。

## 4.2 内部控制描述方法概述

在内部控制评价工作过程中，凡是在财务报表上所有重要科目和披露的认定所对应的控制及信息技术系统的一般控制都需要进行记录。

在编写控制描述时，对于每个控制点的描述要注意要描述出五个方面内容（5W）：

- **Who** 谁是该控制的执行者
- **When** 控制在什么时间发生
- **What** 如何实施该控制
- **Where** 控制体现在什么地方
- **Why** 该控制的目的

在记录被纳入工作范围的流程时，公司内部控制评价人员可以通过以下方式识别流程层面的主要控制点：

- 审阅现行的管理制度；
- 询问有关责任人控制情况；
- 进行穿行测试；
- 将内部控制设计与《企业内部控制基本规范》和其它内部控制资料进行比较和差异分析。

内部控制评价人员应使用标准的工作底稿模版记录内部控制描述，在工作过程中将现有的过程、政策、方法、操作守则、业务流程和业务负责人等内容进行详细记录。

## 4.3 内部控制分类

根据控制的具体实现方式的区分，我们可将内部控制细分为**手工控制**、**自动化控制**和**依赖自动化的手工控制**。

- **手工控制**——是指那些运行时不需要依赖于信息系统环境的控制。
- **自动化控制**——是指应用于单个交易处理的完全由系统自动执行的控制（应用程序控制），包括诸如编辑检查、确认、计算、转换和授权等控制。应用程序控制还可有效增强不相容职责的分离，并有效提高控制活动的效率和效果。
- **依赖自动化的手工控制**——是指人通过基于信息系统生成的信息来进行控制，因此它是人与电脑相结合的产物。由于依赖自动化的手工操作很大程度上依赖电脑系统生成的信息报告，保证电脑系统生成信息的完整性和准确性尤为重要。

其中自动化控制可以分为**信息系统一般控制**和**应用控制**两部分。

- **信息系统一般控制**——强调的是信息系统所处的整体信息技术环境，是其它任何基于信息系统的控制措施的基础。信息系统一般控制的目标是实现信息系统的安全性、可靠性和有效性。
- **信息系统应用控制**——是指在业务流程中基于信息系统的控制措施。一般涵盖对某一特定系统功能的访问权限，对数据输入、处理及输出的控制等。信息系统应用控制的目标是实现相关应用系统操作数据的真实性、完整性和合规性。

根据控制的具体功能区别，我们可将内部控制细分为**预防性控制**和**发现性控制**。

- **预防性控制**——发生于差错出现之前，正常情况下适用于单笔交易或系统设置。
- **发现性控制**——发生于差错出现之后，正常情况下适用于多笔交易。

#### 4.4 信息系统的相关控制

信息技术控制分为**信息系统一般控制**及**信息系统应用控制**两部分。**信息系统一般控制**：强调的是信息系统所处的整体信息技术环境，是其它任何基于信息系统的控制措施的基础。信息系统一般控制为作用于数据中心和网络运行，操作系统软件采购与维护，访问安全和应用程序系统的采购、开发和维护的控制。这些控制适用于大型机、小型机和最终用户的环境中。其主要涵盖程序开发控制、程序变更控制、程序及数据的访问控制、系统运行控制以及最终用户运算五方面。

- **程序开发控制**——合理确保对与日常经营活动密切相关的重要程序的更改，在被移至生产环境之前是经过授权与适当测试的。另外，有关的控制按期望实施并支持财务报告的要求，其中还应包括公司对信息安全和数据处理完整性等方面的要求。
- **程序变更控制**——能合理确保对与日常经营活动密切相关的重要程序的更改，在被移至生产环境之前是经过授权与适当测试的。
- **程序及数据的访问控制**——能合理确保系统与子系统上建立了适当的安全性措施来防止数据的未授权使用，披露，更改，破坏和流失。
- **系统运行控制**——管理层制定、记录并遵循了关于系统运作的标准流程：包括实施批处理作业以及对安全与信息处理事件的监控与反应。
- **最终用户运算**——合理确保终端用户所使用的电子表格与自主开发的程序所提供数据的完整性、准确性和可靠性。数据的未授权使用，披露，更改，破坏与流失得到合理的预防。

**信息系统应用控制：**是指在业务流程中基于信息系统的控制措施。一般涵盖对某一特定系统功能的访问权限，对数据输入，处理及输出的控制等。原则上需将信息系统依据信息技术环境进行归类，按类对控制进行描述，但需要保证该归类能够包括所有涉及以上关键业务流程中定义为关键控制点的信息系统情况。

#### 4.5 财务报告认定

与财务报告相关控制还需要确保每个重要的会计科目符合下列财务报表认定的要求：

- **存在与发生**——资产负债表所列的各项资产、负债、权益在资产负债表日是否存在，损益表所列的各项收入和费用在会计期间是否确实发生。需要注意的是“存在或发生”认定所需要解决的问题是，管理当局是否把那些不应包括的项目（如不存在的项目或不曾发生的交易结果）记入了会计报表，但并不涉及所报告的金额是否正确。
- **完整性**——在会计报表中应列示的所有交易和项目是否都列入了。这里需注意，有关“完整性”的认定所要解决的问题是，管理当局是否把应包括的项目给遗漏或省略了，并不涉及所报告的金额是否正确。可见，“完整性”认定与“存在与发生”认定正好相反，它主要与会计报表的组成要素的低估有关。即“该记账的没记”。
- **估价与分摊**——资产与负债、交易或事件以适当的金额记录。收入与费用于适当的期间内分摊。
- **权利与义务**——在某一特定日期，各项资产是否确属公司的权利，各项负债是否确属公司的义务，需注意该认定只与资产负债表的组成要素有关。
- **表达与披露**——会计报表上的特定组成要素是否被适当地加以分类、说明和披露。

#### 4.6 内部控制设计有效性测试方法

通过执行**穿行测试**来对内部控制设计有效性进行评价。

**穿行测试：**即对完整业务流程轨迹按交易流程进行模拟跟踪，需要审阅及复印交易所涉及的实际交易单据、凭证、对账单及其它有关文件，每年都需要对项目范围内的主要流程进行穿行测试。在穿行测试中，应在每类重大交易中选择一笔交易，从其业务起点追溯至业务的终结，确保在流程各个环节获取的文档要能勾稽起来。

#### 4.7 评价内部控制在设计上的有效性

在考虑内部控制设计有效性时，项目组成员需判断其内部控制设计是否可以防范/规避有关风险（例如需要处理什么风险？控制如何进行？频率是否足够？员工技能或经验是否可以有效操作）。透过与流程负责人或相关系统负责人访谈以了解各重要流程的内部控制，通过穿行测试确认内部控制的真实性，用以评价现有内部控制在设计上能否确保控制措施可以涵盖相关的风

险，能否达到预期的控制目标。若发现有任何不足之处，会把相关缺陷记录至缺陷报告，然后逐一评价其潜在的影响。

内部控制如在设计上存在缺陷，将不会对其进行执行有效性评估，需待整改完成后，再次评估内部控制设计有效性认定为有效后，方可考虑进行内部控制执行有效性评估。

## 第五部分 内部控制执行有效性评价

### 5.1 内部控制执行有效性测试内容

对内部控制在执行有效性测试的内容包括控制措施是否按设计一贯的有效执行和控制执行人员是否具备相应的职权或资格。控制测试仅针对关键控制进行。**关键控制**：是指对公司日常经营运作具有深入的影响的控制，关键控制的失败将直接影响到公司相关控制目标的实现。

### 5.2 内部控制执行有效性测试方法

通过执行**控制测试**来对初步评价为有效的关键控制的执行有效性进行评价。

**控制测试**：即记录主要内部控制的遵循情况，涉及管理层审核、职责与权限的划分、授信对账及差错报告等重要内部控制点，需审阅（包括在计算机系统中审阅）有关文件及单据。

#### 抽样基准及可允许测试失效样本数量

##### 抽样基准

| 内部控制实施的频率       | 每年样本数量范围                        |
|-----------------|---------------------------------|
| 每年（一般为年终）       | 1 个                             |
| 每季度             | 2 个                             |
| 每月              | 2 个                             |
| 每周              | 5 个                             |
| 每天              | 25 个                            |
| 反复持续进行(一天内发生多次) | 25 个                            |
| 不定时             | 覆盖全年实施相关内部控制整体数量的 10%，但不超过 25 个 |

### 可允许失败的样本数量

| 控制测试样本量 | 发现的操作缺陷数量 | 跟进方法                                                           |
|---------|-----------|----------------------------------------------------------------|
| 1—20 个  | 1 个       | 控制失效，不再测试。                                                     |
| 25 个    | 1 个       | 扩大样本量（剔除原有样本重新抽取 15 个样本）进行测试。如未发现其他差异，控制仍然有效。如再发现差异，控制失效，不再测试。 |
| 25 个    | >1 个      | 控制失效，不再测试。                                                     |

若在扩大样本量后仍发现错误：

- 记录样本测试失败的详细情况及原因，并要求公司进行整改。
- 考虑针对该控制是否还有其它的补偿控制可以依赖。如果有可以信赖的补充或者替代性控制，可以考虑对其进行测试以弥补关键控制的缺失。

保持足够的书面文档支持内部控制评价工作的进行非常重要，因此项目组成员必须完成测试记录，内容包括：

- 被测试单位/部门；
- 测试负责人员和测试日期；
- 关键控制点内容；
- 样品数量和抽样方法；
- 测试步骤；
- 测试样本关键信息；
- 测试结论。

## 第六部分 内部控制缺陷评价

### 6.1 内部控制缺陷的类型

在进行内部控制设计有效性和执行有效性评价后，需把识别到的内部控制缺陷按照其类型进行分析。如发现内部控制的有效性出现问题，需向流程负责人了解有没有补偿控制。如果有补偿控制，测试员须要针对补偿控制进行测试。以下为发现内部控制缺陷时的相关处理程序：

- 将不能通过测试的情况分类（一般缺陷、重要缺陷或重大缺陷）；
- 报告有关情况、对公司的影响、短期及长期的解决方案；
- 以风险为出发点，从内部控制缺陷发生可能性和影响程度两个方面来确定哪些内部控制缺陷构成了重大缺陷或重要缺陷。

内部控制缺陷根据其性质主要分为**设计缺陷**和**执行缺陷**。

- **设计缺陷**：指的是内部控制措施在设计上本身就存在漏洞或控制缺失，控制措施无法将风险降低到可接受的最低水平。
- **执行缺陷**：指的是控制措施在设计上本身是有效的，但控制执行人并未按规定将控制活动一贯的有效执行。

内部控制缺陷按其后果的严重性和发生的可能性还可以分为三大类：**重大缺陷**、**重要缺陷**和**一般缺陷**。

- **重大缺陷**：是指一个或多个控制缺陷的组合，可能导致公司严重偏离控制目标的情形。结合公司实体风险评价的结果，仅高风险领域的关键控制点的内部控制缺陷才可能产生重大缺陷。
- **重要缺陷**：是指一个或多个控制缺陷的组合，其严重程度和经济后果低于重大缺陷，但仍有可能导致公司偏离控制目标的情形。
- **一般缺陷**：是指除重大缺陷、重要缺陷之外的其他控制缺陷。

公司审计办应当组织相关的内部控制评价工作组综合分析内部控制缺陷的性质、产生的原因及影响程度，提出认定意见及整改方案，采取适当的形式及时向董事会、监事会或者管理层报告。公司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。重大缺陷应当由董事会予以最终认定。

进行内部控制缺陷评价时，可以将自我评价结果与外部审计师评价结果相结合，对内部控制缺陷进行最终的评价。

6.2 《企业内部控制基本规范》对内部控制缺陷评价的要求

《企业内部控制基本规范》及其《企业内部控制评价指引》对重大缺陷、重要缺陷的内部汇报及外部审计师的内部控制审计有着明确的要求。

《企业内部控制基本规范》提出企业的内部审计机构对监督检查中发现的内部控制重大缺陷，有权直接向董事会及其审计委员会、监事会报告。同时，企业应当跟踪内部控制缺陷整改情况，并就内部监督中出现的重大缺陷，追究相关责任单位或者责任人的责任。企业对于认定的重大缺陷，应当及时采取应对策略，将风险控制在可承受度之内。

《企业内部控制评价指引》要求外部审计师通过风险评估确定内部控制的特定领域存在重大缺陷的风险越高，给予该领域的审计关注就越多。外部审计师应当与企业沟通审计过程中识别的所有控制缺陷。对于其中的重大缺陷和重要缺陷，应当以书面形式与董事会或经理层沟通。外部审计师认为财务报告内部控制存在一项或多项重大缺陷的，除非审计范围受到限制，应当对财务报告内部控制发表否定意见。外部审计师出具否定意见的内部控制审计报告，还应当包括下列内容：

- 重大缺陷的定义。
- 重大缺陷的性质及其对财务报告内部控制的影响程度。

6.3 内部控制缺陷的评估标准

在评估重大缺陷、重要缺陷、一般缺陷的过程中，公司内部控制评价人员应当充分利用本手册第二部分“项目范围的制定”所提到的两个重要概念“重要性水平”与“可容忍误差”作为量化评估标准。具体评估方法如下表所示：

|      |                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 重要缺陷 | <ul style="list-style-type: none"><li>• 计划重要性水平 x 75%（即可容忍误差）</li><li>• 单一或多个内部控制缺陷的存在，可能导致无法及时地预防或发现年报或中期报告中出现上述金额或以上的重要错误。</li><li>• 所有潜在影响大于此金额会被视为重要缺陷。除了此量化基准外，在决定内部控制缺陷是否重要缺陷时，还需考虑非量化因素。</li></ul> |
| 重大缺陷 | <ul style="list-style-type: none"><li>• 计划重要性水平 x 100%</li></ul>                                                                                                                                          |

|  |                                                                                                                                                                                                        |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• 单一或多个内部控制缺陷的存在，可能导致无法及时地预防或发现年报或中期报告中出现上述金额或以上的重大错误。</li> <li>• 所有潜在影响大于此金额会被视为重大缺陷。任何重大缺陷会引致外部审计师对财务报表作出反对意见。除了量化的基准外，在决定内部控制缺陷是否重大缺陷时，还需考虑非量化因素。</li> </ul> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

某些特定的情况将表明内部控制可能存在重大缺陷的迹象，主要包括：

- 外部审计师发现董事、监事和高级管理人员舞弊。
- 企业更正已经公布的财务报表。
- 外部审计师发现当期财务报表存在重大错报，而内部控制在运行过程中未能发现该错报。
- 企业审计委员会和内部审计机构对内部控制的监督无效。

## 第七部分 内部控制评价报告

### 7.1 内部控制评价报告的基本内容

每年，公司应该在完成内部控制评价工作后，根据内部控制评价工作的结果和整改完成情况，按照《企业内部控制基本规范》及相关配套指引的要求，编制内部控制评价报告。内部控制评价报告应当分别内部环境、风险评估、控制活动、信息与沟通、内部监督等要素进行设计，对内部控制评价过程、内部控制缺陷认定及整改情况、内部控制有效性的结论等相关内容进行披露。

内部控制评价报告至少应当披露下列内容：

- （一）董事会对内部控制报告真实性的声明。
- （二）内部控制评价工作的总体情况。
- （三）内部控制评价的依据。
- （四）内部控制评价的范围。
- （五）内部控制评价的程序和方法。
- （六）内部控制缺陷及其认定情况。
- （七）内部控制缺陷的整改情况及重大缺陷拟采取的整改措施。
- （八）内部控制有效性的结论。

若存在一个或多个内部控制重大缺陷，应当得出内部控制无效的结论。内部控制评价报告应当报审计委员会审议、董事会审定批准后公布。

### 7.2 内部控制评价报告披露要求

内部控制评价报告应当报经董事会批准后对外披露或报送相关部门。企业内部控制评价部门应当关注自内部控制评价报告基准日（12月31日）至内部控制评价报告发出日之间是否发生影响内部控制有效性的因素，并根据其性质和影响程度对评价结论进行相应调整。