

# 内部控制管理手册

## 体系框架分册

中国石油天然气股份有限公司

二〇〇八年一月

# 目 录

公司简介 .....	
手册说明 .....	
<b>1 总论</b> .....	
1.1 概述 .....	
1.2 内部控制体系框架 .....	
1.3 组织结构、职责与权限 .....	
<b>2 控制环境</b> .....	
2.1 概述 .....	
2.2 诚信与道德价值观 .....	
2.3 发展目标 .....	
2.4 管理理念与企业文化 .....	
2.5 风险管理策略 .....	
2.6 董事会及下属委员会 .....	
2.7 组织结构 .....	
2.8 权利和责任分配 .....	
2.9 人力资源政策与措施 .....	
2.10 员工胜任能力 .....	
2.11 反舞弊机制 .....	
<b>3 风险评估</b> .....	
3.1 概述 .....	
3.2 建立风险评估机制 .....	
3.3 建立并完善风险管理体系 .....	
<b>4 控制活动</b> .....	
4.1 概述 .....	
4.2 控制活动的实施 .....	
<b>5 信息与沟通</b> .....	
5.1 概述 .....	
5.2 信息 .....	
5.3 沟通 .....	
5.4 信息系统总体控制 .....	
5.5 信息系统应用控制 .....	
5.6 信息披露 .....	
<b>6 监督</b> .....	
6.1 概述 .....	
6.2 持续监督 .....	
6.3 独立评估 .....	
6.4 缺陷报告 .....	
附件 《内部控制管理手册》（地区公司分册）编制规范 .....	

## 公司简介

中国石油天然气股份有限公司（简称“中国石油”）是于 1999 年 11 月 5 日在中国石油天然气集团公司（简称“中油集团”）重组过程中，按照中华人民共和国公司法成立的股份有限公司。在重组过程中，中油集团向中国石油注入了与勘探和生产、炼制和营销、化工产品和天然气业务有关的大部分资产和负债。

中国石油是中国销售额最大的公司之一，广泛从事与石油、天然气有关的各项业务，包括：

- 1) 原油和天然气勘探、开发、生产和销售；
- 2) 原油和石油产品的炼制、运输、储存和销售；
- 3) 基本石油化工产品、衍生化工产品及其他化工产品的生产和销售；
- 4) 天然气、原油和成品油的输送及天然气的销售。

中国石油发行的美国存托股份、H 股及 A 股于 2000 年 4 月 6 日、2000 年 4 月 7 日和 2007 年 11 月 5 日分别在纽约证券交易所、香港联合交易所有限公司及上海证券交易所挂牌上市。

中国石油的财务业绩优良，2004 年、2005 年和 2006 年的净利润分别为 1038 亿元人民币、1333 亿元人民币和 1422.24 亿元人民币。

公司注册中文名称：中国石油天然气股份有限公司

公司英文名称：PetroChina Company Limited

公司法定代表人：蒋洁敏

公司董事会秘书：李怀奇

公司法定地址：中国北京东城区安德路 16 号洲际大厦

邮政编码：100011

电话：(8610) 84886270

传真：(8610) 84886260

上市地点：上海证券交易所（A 股，股票代码为“N 石油”）、香港联合交易所有限公司（H 股，股票代码为“HK00857”）和纽约证券交易所（ADS，股票代码为“PTR”）。

# 手册说明

## 关于《内部控制管理手册》

### 目的、意义及原则

编制和实施《内部控制管理手册》（以下简称《手册》），是为了遵循国内及上市地法律法规，进一步完善现代企业制度和法人治理结构，确保公司各项工作规范、有序运行，最大限度地减少或规避风险，提高公司的经营管理水平。

通过编制《手册》，建立一套科学、系统的内部控制体系建设的方法和规范，为公司内部控制体系建设、运行和维护提供指引，并作为建立、运行及评价内部控制体系的依据。从而确保公司上下从思想上、认识上对内部控制体系保持高度统一，以进一步实现行为上的统一。

《手册》编写遵循以下原则：

- 1) 选用 COSO 内控框架进行体系设计；
- 2) 以风险管理为核心的内部控制体系建设；
- 3) 满足国内外监管要求。

### 法律依据

《手册》编写依据的法律法规。

国内法律法规：

- 1) 《中华人民共和国会计法》及配套法规；
- 2) 企业会计准则；
- 3) 《中华人民共和国审计法》；
- 4) 《审计署关于内部审计工作的规定》；
- 5) 《中央企业内部审计管理暂行办法》；
- 6) 《中央企业全面风险管理指引》。

国外法律法规：

- 1) 《萨班斯—奥克斯利法案》；
- 2) 《与财务报表审计协同进行的对于财务报告内部控制的审计》；
- 3) 与财务报表审计相结合的财务报告内部控制审计以及相关的独立性规定和一致性修正案（审计准则 5 号）；
- 4) 有关财务报告内部控制管理层报告规则的修订（解释性指南）。

### 标准：

- 1) COSO 内部控制框架；
- 2) COSO 企业风险管理整体框架。

### 适用范围

本《手册》所描述的内部控制体系覆盖并适用于：

- 1) 本公司所有部门和所属单位；
- 2) 本公司内部控制体系所涉及的所有业务和管理活动。

### 贯彻实施的责任和要求

《手册》已经建立了一套科学、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。为保证内部控制体系“设计有效、执行有力”，公司所属各单位要认真组织实施，严格遵照执行。

各地区公司要充分认识内部控制体系建设工作的长期性和艰巨性，把建立和有效运行内部控制体系作为本单位的重要工作，建立长效机制，指定专职管理部门或专职管理岗位，履行内部控制职能，切实做到实施有力。

为推动《手册》的贯彻执行，提高《手册》的使用效果，内部控制部每年至少举办一次《手册》使用培训。各地区公司要有计划地做好本单位的培训，将内控工作要求传达到每个员工、每个岗位，确保执行到位。

各地区公司要按照《内部控制管理手册》（地区公司分册）编制规范（见附件）的要求，修订、完善和细化本单位的分册。

各地区公司内控管理部门要对本单位内部控制体系运行情况进行检查和督促，公司内部控制部将定期组织考核并进行通报。

## 使用指南

### 内容指引

本《手册》包括六个分册，即《体系框架分册》、《控制环境分册》、《风险评估分册》、《控制活动分册》、《信息与沟通分册》及《监督分册》。

1)《体系框架分册》，描述了内部控制体系组织结构与职责，较为全面地阐述了内部控制体系的建设目标，并以 COSO 内控框架为指引，从控制环境、风险评估、控制活动、信息与沟通和监督等五个方面对内控关注要点及相应措施进行了较为全面、系统的阐述；

2)《控制环境分册》，描述了控制环境的概念，并从诚信与道德价值观、发展目标、管理理念与企业文化、风险管理策略、董事会及下属委员会、组织结构、权利和责任分配、人力资源政策与措施、员工胜任能力以及反舞弊机制等十个方面对内控关注要点、措施进行了阐述；

3)《风险评估分册》，描述了风险和风险评估的基本概念以及风险的分类，从建立风险评估目标、风险评估机制、建立并完善风险管理体系三个方面对内控关注要点及相应措施进行了阐述，并汇编了风险评估的相关方法、规范及管理制度；

4)《控制活动分册》，描述了控制活动的概念及分类，对公司控制活动的实施进行了概括，并汇编了关键控制管理文件；

5)《信息与沟通分册》，描述了信息与沟通的概念及要素，从信息、沟通、信息系统及信息披露等五个方面对内控关注要点及相应措施进行了阐述；

6)《监督分册》，描述了监督的概念及要素，并从持续监督、独立评估和缺陷报告三个方面对内控关注要点及相应措施进行了阐述，并汇编了相关管理制度及规范。

### 使用要求

本《手册》是公司重要文件，属公司机密。各单位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，及时向内部控制部咨询。

### 管理与维护

内部控制部对《手册》进行规范管理，以保证其有效、完整、统一和适用。

### 编写与发布

《手册》由内部控制部组织编写，内控体系建设委员会审定，股份公司行文发布。

### 发放

1)《手册》须按发放范围统一发放。发放范围由内部控制部提出，经管理层批准执行。一般包括总裁、副总裁、机关职能部门、专业分公司、地区公司及其下属单位等。

2)《手册》包括纸质版和电子版两种。电子版的配发范围为业务流程管理信息系统的覆盖范围；纸质版的配发范围为公司所属单位及特殊使用者。

### 维护

《手册》的维护是一项长期性、经常性的重要工作，需要各单位高度重视，积极参与，大力配合。

《手册》的修订、维护由内部控制部负责。每年，内部控制部将根据国内和上市地新出台的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以及地区公司反馈的意见及建议等，对《手册》进行修订，经总裁批准执行。

各地区公司应指定专职管理部门负责本单位《手册》的日常管理和维护。对《手册》日常使用过程中发现的问题，应认真记录并及时反馈给内部控制部。

内部控制部应及时掌握《手册》的执行情况，并采取有效措施确保内部控制管理体系的有效运行。

## 关键术语和定义

### COSO

COSO 是自愿性的私人组织，致力于通过强化商业道德、建立完善有效的内部控制和法人治理结构以提高财务报告的质量。1985 年，由美国注册会计师协会（AICPA）、会计协会（AAA）、财务经理协会（FEI）、内部审计师协会（IIA）、管理会计师协会（IMA）联合创建了反虚假财务报告委员会。该委员会旨在探讨

财务报告中舞弊产生的原因，并寻求解决措施。两年后，该委员会提出了很多有价值的建议。基于该委员会的建议，其赞助机构成立了 COSO 委员会，专门研究内部控制问题。

## COSO 框架

### 1) COSO 内部控制—整体框架

反虚假财务报告委员会于 1987 年签署了报告，号召研究并制定一个统一的内部控制框架。1992 年 9 月，COSO 委员会提出了报告《内部控制——整体框架》(1994 年进行了增补)，即 COSO 内部控制框架。COSO 内部控制框架被广泛地选择作为构建和完善内部控制体系的标准，是因为：虽然 COSO 内部控制框架并非唯一的内部控制框架，但却是美国证券交易委员会唯一推荐使用的内部控制框架，《萨班斯—奥克斯利法案》第 404 条款的“最终细则”也明确表明 COSO 内部控制框架可以作为评估公司内部控制的的标准。

COSO 框架提出五个互相关联的组成要素，根据公司的规模和结构，公司可采用不同的方式来实施这些组成要素，但是所有公司都必须涉及这五个组成要素。因此，在对内部控制进行评估时，管理层必须考虑以下每个组成要素：

**控制环境：**控制环境是内部控制体系的基础，是有效实施内部控制的保障，直接影响着公司内部控制的贯彻执行、公司经营目标及整体战略目标的实现。控制环境确定了公司的总体态度，是内部控制所有其他组成要素的基础。控制环境包括职业道德、员工的胜任能力、管理理念和经营风格、组织结构、权利和责任的分配、人力资源政策与措施、董事会与审计委员会以及反舞弊等内容。

**风险评估：**风险评估是识别及分析影响公司目标实现的风险的过程，是风险管理的基础。在风险评估中，应识别和分析对实现目标具有阻碍作用的风险。

**控制活动：**控制活动是确保管理层的指令得到贯彻执行的必要措施，存在于整个机构内所有级别和职能部门。包括批准、授权、查证、核对、经营业绩评价、资产保全措施和职责分工等活动。

**信息与沟通：**信息与沟通是公司经营管理所需的信息被识别、获得并以一定形式及时地传递，以便员工履行职责。信息不仅包括内部产生的信息，还包括与公司经营决策和对外报告相关的外部信息。畅通的沟通渠道和机制使公司的员工能及时取得他们在执行、管理和控制公司经营过程中所需的信息，并交换这些信息。

**监督：**监督是对内部控制体系有效性进行评估的持续过程，包括持续监督、独立评估和缺陷报告等。

### 2) COSO 企业风险管理—整体框架

最近数年，企业风险管理成为焦点而受到突出关注，需要一个强有力的框架以有效地识别、评估和管理风险。2004 年 9 月，COSO 委员会发布《企业风险管理整体框架》，在内部控制的基础上，扩展、提供了一个更强有力的框架，更广泛地专注企业的全面风险管理。该框架不会取代内控框架，而是将内控框架与其融合为一体。公司仍可以决定依靠这个企业风险管理框架去满足企业内控的需要，通过采用更全面的风险管理方法使企业持续发展。

企业风险管理由八项相互关联的要素组成，来自管理层经营企业的方式，并融入管理过程本身。这些要素包括：

**内部环境：**内部环境包含了一个企业的基调，为该企业管理层和员工审视和应对风险的方式制定基础，包括风险管理理念和风险容量、诚信和道德价值观以及他们进行经营活动所处的环境。

**目标制定：**在管理层能够识别影响目标实现的潜在事件之前，企业必须已制定目标。企业风险管理确保管理层使制定目标的流程到位，并保持选择的目标支持企业的使命并与此并行不悖，同时这些目标也与企业的风险容量相一致。

**事件识别：**必须识别出影响企业实现目标的各种外部和内部事件，并区分风险和机遇。可以在管理层制定企业战略或目标的过程中对机遇加以考虑。

**风险评估：**应对风险进行分析，考虑其发生的可能性和影响，以作为确定应如何管理风险的基础。还应对企业固有风险及残存风险进行评估。

**风险反应：**管理层选择风险反应方案：规避风险、接受风险、减少风险或分担风险，采取一系列措施使风险维持在企业的风险承受度和风险容量范围之内。

**控制活动：**确立和实施政策和程序，以有助于确保风险反应方案得以有效地贯彻执行。

**信息与沟通：**相关信息以某种形式和在一定时限内被识别、获得和传达沟通，以便使员工履行自己的职责。从广义上讲，有效的沟通也应自上而下、自下而上地进行，贯穿整个企业。

**监督：**监督整个企业风险管理过程，并根据需要作出修改。通过持续性监督活动、独立评估或两者兼而有之来完成监督。

## 内部控制

COSO 内部控制框架认为，内部控制是受公司董事会、管理层和其他人员影响，为实现经营的效率和

效果、财务报告的可靠性、相关法规的遵循性等目标而提供合理保证的过程。

### **企业风险管理**

COSO 企业风险管理整体框架认为，企业风险管理是一个受到企业董事会、管理层和其他人员影响的过程，这个过程从企业战略制定一直贯穿到企业的各项活动中，旨在识别那些可能影响企业的潜在事件并管理风险使之在企业的风险容量之内，从而合理确保企业实现其既定目标。

### **PCAOB**

PCAOB 是美国上市公司会计监管委员会的英文缩写。

美国上市公司会计监管委员会（PCAOB）是根据 2002 年 7 月 30 日美国总统乔治·布什签署的《萨班斯—奥克斯利法案》成立的。其宗旨在于通过准备独立、准确的审计报告来保护投资者的利益，从而进一步保护公众的利益。根据美国联邦法律规定，PCAOB 有权制定一系列准则来指导和约束上市公司的审计。联邦法律还要求 PCAOB 每年向 SEC 和美国国会中主管 PCAOB 的委员会同时提交报告。

### **对财务报告的内部控制**

财务报告的内部控制是由公司主要管理人员和财务管理人员或者执行类似职能的人员设计和监督的，由公司董事会、管理层及其他人员实施，并能合理确保财务报告的可靠性，以及向外部相关方提供的财务报表的编制符合公认会计准则的一个流程。该流程涉及对交易进行记录、记录的维护以及对未经授权的收购、使用或处置公司资产的行为进行防范或检测的措施。

### **设计方案的有效性**

当内部控制能够满足内控目标，并能防止或发现可能导致财务报表发生重大错报或舞弊时，财务报告内部控制的设计方案就是有效的。

### **运行有效性**

当设计恰当的内控按设计运行，并且执行内控的相关人员具备有效执行控制所需的权限和资格时，对于财务报告的内部控制的运行是有效的。

# 1 总 论

## 1.1 概 述

### 1.1.1 框架编制的目的

通过确定内部控制体系建设目标，明晰内部控制体系建设的范围和内容，为公司建设以风险管理为核心内容的内部控制体系提供指引，以建立统一、规范、有效的内部控制体系，增强公司风险防范能力，为公司战略发展提供合理保障。

### 1.1.2 框架编制的原则

- 1) 合法性原则。以国内及上市地法律法规为准绳，结合公司实际建立内部控制体系。
- 2) 完整性原则。以 COSO 内部控制整体框架为基础，融合 COSO 企业风险管理整体框架的主要内容，结合国家监管部门的基本要求，全面开展内部控制体系建设，覆盖全部业务和部门。
- 3) 继承性原则。在公司现有管理体系的基础上，依托已有管理优势，建立内部控制体系。
- 4) 效率性原则。在保证体系设计合理性的前提下，提高公司运营效率和效益。

### 1.1.3 框架编制的依据

国资委《中央企业全面风险管理指引》；《萨班斯—奥克斯利法案》；美国上市公司会计监管委员会（PCAOB）发布的相关审计准则；《COSO 内部控制整体框架》；《COSO 企业风险管理整体框架》及公司相关管理规定。

### 1.1.4 框架编制的思路与方法

在现有内控体系框架的基础上，结合《COSO 企业风险管理整体框架》的主要内容，按照国资委《中央企业全面风险管理指引》的基本要求，增加控制目标和体系建设内容，汲取国内外其他公司内部控制体系建设的先进经验，根据公司管理实际编制内部控制体系框架。

### 1.1.5 体系框架的实施

框架明确了公司内控工作任务，是制定内控工作规划的依据。框架确定的工作目标将在今后分年度实施。

## 1.2 内部控制体系框架

### 1.2.1 内部控制体系建设的总体目标

公司内部控制体系建设的总体目标是：建立以风险管理为核心内容，涵盖公司经营管理各领域，较为完善、运行有效的内部控制体系，为公司战略发展提供合理保障。

### 1.2.2 内部控制体系建设指导思想

充分认识公司建设内部控制体系工作的严肃性、重要性和紧迫性，以《萨班斯—奥克斯利法案》的颁布为契机，以国资委发布的《中央企业全面风险管理指引》为指导，以提高公司管理水平为动力，依托已有的管理优势，适应公司国际化发展要求，开展以风险管理为核心内容的内部控制体系建设，为公司战略发展提供合理保障，从而树立和维护公司在国际资本市场诚信、稳健和安全的良好形象。

### 1.2.3 框架的主要内容



### 1.2.3.1 控制环境

控制环境确立公司风险管理的总体态度，是内部控制体系的基础，是有效实施风险管理的保障，直接影响内部控制体系的执行、公司经营目标及整体战略目标的实现。风险管理是受公司董事会、管理层和其他人员影响的过程，这个过程从公司战略制定一直贯穿到企业的各项活动中，旨在识别那些可能影响公司目标的潜在因素并予以管理，使之在公司的风险容量之内，从而为公司实现其目标提供合理保证。

控制环境包括诚信与道德价值观、发展目标、管理理念与企业文化、风险管理策略、董事会及下属委员会、组织结构、权利和责任分配、人力资源政策与措施、员工胜任能力以及反舞弊机制等内容。

1) 诚信与道德价值观：建立涵盖公司各个层面的员工职业道德规范，体现公司诚信与道德价值观念，树立员工诚信价值观。

2) 发展目标：制定公司战略目标，并在此基础上制定相关经营目标、报告目标和合规性目标。

3) 管理理念与企业文化：确立公司管理理念，体现公司的经营管理风格；确立公司风险管理理念，体现公司认知经营管理风险所共有的信念和态度。

继承和发扬公司企业文化，体现公司的经营宗旨、价值观念和行为规范；将风险管理文化融入企业文化建设全过程，树立和传播正确的风险管理理念，增强守法意识和诚信意识，将风险管理意识转化为员工的共同认识和自觉行动，提高全员风险意识。

公司高级管理人员应在继承和发扬风险管理文化中发挥表率作用，中层管理人员应继承和发扬风险管理文化的骨干作用。

4) 风险管理策略：公司围绕发展战略，确定风险容量、风险承受度、风险管理有效性标准，体现公司风险管理的总体策略，并据此制定风险反应方案。

公司确定针对发展战略的风险容量，体现公司在战略制定与实施过程中愿意承受的风险范围和风险水平，反映公司的风险偏好。公司针对特定目标，制定具体的风险承受度，体现在实现特定目标过程中公司对差异的可接受程度。公司确定风险容量和风险承受度，要正确认识和把握风险与收益的平衡，防止忽视风险，片面追求收益或者单纯为规避风险而放弃发展机遇。风险承受度与风险容量保持一致。

公司根据风险管理的总体目标，制定风险管理有效性标准。

5) 董事会及下属委员会：董事会的设立符合国内外法律法规的规定。董事会负责督导公司内部控制体系的建立和实施，督导公司将风险管理融入战略管理之中，监督公司以风险管理为核心内容的内部控制工作。

董事会下属的审计委员会的设立符合国内外法律法规的规定，负责监督内部控制体系运行与评价情况。

6) 组织结构：建立规范的法人治理结构，优化组织结构，明确部门权责并细化落实到各个岗位，规范组织机构编制管理工作。

建立内部控制体系运行网络。建立健全公司内部控制管理组织体系，明确内部控制组织体系的职责分工，形成包括董事会、审计委员会、管理层、内控体系建设委员会、内部控制管理部门、其他职能部门及各业务单位在内的内部控制管理组织体系。各单位根据实际情况，按规定设置内部控制管理机构或管理岗位负责内部控制日常管理工作。内部控制管理工作应与其他管理工作紧密结合，把内控管理的各项要求融入企业管理和业务流程中。

7) 权利和责任分配：建立完善的公司权责管理体系，制定完善的授权管理文件。

8) 人力资源政策与措施：建立完善的公司管理人员任用选拔、管理考核和激励监督等方面的政策。

9) 员工胜任能力：健全全员职业培训和技能考核机制，持续提高员工的综合素质和工作能力。

10) 反舞弊机制：制定反舞弊相关制度，建立反舞弊机制。持续开展舞弊风险评估，建立舞弊风险数据库。制定反舞弊控制措施，持续开展舞弊调查并进行违规处理。监督反舞弊机制运行效果并逐步予以完善。

### 1.2.3.2 风险评估

风险是指未来的不确定性对公司实现其目标的影响。风险评估是识别及分析影响公司目标实现的因素的过程，是风险管理的基础。在风险评估中，既要识别和分析对实现目标具有阻碍作用的风险，也要发现对实现目标具有积极影响的机遇。

公司制定完善的风险评估规范，明确风险评估的程序和方法，规范公司风险评估工作。公司风险评估工作由内控部门组织有关职能部门和业务单位实施。

1) 风险评估范围

公司针对战略目标、经营目标、报告目标、合规性目标，分别确认风险评估的范围。

## 2) 风险评估的基本程序

(1) 信息收集。围绕公司战略目标和相关目标以及风险管理要求,相关职能部门、业务单位和内控管理部门广泛、持续收集与公司风险及风险管理相关的内部、外部各种信息,包括收集历史数据和未来信息,关注宏观经济与经营环境、竞争对手、新技术与新产品、海外经营、公司重组、业务整合、会计政策、信息系统、资本运作等方面已经发生和将要发生的变化情况。公司对收集的数据、信息和变化情况进行必要的筛选、提炼、对比、分类、组合,形成与公司风险管理相关的信息资料库并不断更新,以便进行风险评估。

(2) 风险识别。风险识别是指查找公司各项重要经营管理活动及其重要业务流程中存在的实现目标的风险和机遇的过程。公司分别从公司层面、业务活动层面,动态识别影响公司战略目标及相关目标实现的、内部和外部的各种不确定性因素。带负面影响的因素代表风险,需要对其分析和应对;带积极影响的因素代表机遇,在制定目标和政策实施过程中对其加以考虑并把握。

① 公司层面风险识别。公司从战略发展的角度,识别公司层面面临的所有重大的不利因素和有利因素,从而识别风险,发现机遇。这些因素来自外部和内部两个方面,外部因素主要包括政治因素、经济因素、社会因素、自然环境因素等;内部因素主要包括基础设施因素、员工因素、流程因素和技术因素等。

② 业务活动层面风险识别。公司制定业务流程描述规范,建立流程目录并用流程图对所有业务进行直观描述。在业务流程描述的基础上,以业务流程步骤为主线,全面识别影响目标实现的相关因素。

(3) 风险评价。风险评价是评估风险对公司实现目标的影响程度和风险发生可能性的过程。公司针对固有风险和残存风险,运用定性和定量的方法,对公司层面和业务活动层面风险发生的可能性和影响程度进行分析、评价,并按照风险排序标准和方法,确定风险重要性水平,识别公司重大风险,确定风险管理的优先顺序。

(4) 风险反应。风险反应是公司针对风险发生的原因、风险重要性水平,考虑风险之间的关系并把握机遇,运用风险组合观,选择风险反应方案的过程。风险反应方案包括回避风险、减少风险、分担风险、接受风险。

## 3) 风险数据库

公司按照规定的程序和方法,开展公司层面风险和业务活动层面风险评估后,结合风险因素、重要性水平和风险反应方案,编制与维护公司层面风险数据库和业务活动层面风险数据库。

### 1.2.3.3 控制活动

控制活动是确保管理层关于风险应对方案得以贯彻执行的政策和程序。控制活动存在于公司所有级别的分支机构和职能部门,包括授权、批准、查证、核对、报告、内部审计、重大风险预警、企业法律顾问、经营业绩评价和资产保全措施等活动。

公司应根据风险管理策略,针对各类风险或每一项重大风险制定相关的规章制度、控制政策和控制措施,确保风险控制在风险承受度的范围内。

公司针对风险建立的规章制度、控制政策和控制措施,要满足合规的要求,坚持经营战略与风险策略一致、风险控制与运营效率及效果相平衡的原则,针对重大风险所涉及的各管理及业务流程,制定涵盖各个环节的全流程控制措施;对其他风险所涉及的业务流程,要把关键环节作为控制点,采取相应的控制措施。

公司应当按照各有关部门和业务单位的职责分工,组织实施控制措施。

1) 针对公司层面风险,按照风险反应方案,建立相应的公司层面风险控制政策,制定公司统一的规章制度,统驭业务活动层面控制。

2) 针对业务活动层面风险,以公司层面控制政策为导向,规范业务流程,制定业务活动层面风险控制措施。

(1) 控制现状描述与分析。制定风险控制文档编制规范和模板,对业务流程进行风险控制分析,编制风险控制文档(RCD),对控制的合理性、完整性进行分析。

(2) 规范、统一业务流程。根据风险控制分析结果,补充、完善相关控制,规范、统一流程步骤、控制规范和记录表单,建立规范、统一的业务流程。

(3) 建立关键控制。建立完善的关键控制确认方法,确定所有业务流程的关键控制并建立关键控制管理文件。

(4) 强化自动控制。通过实施信息系统自动控制,固化流程操作程序,提高控制执行效率和效果。

3) 财务会计报告流程。建立健全财务会计报告流程,完善财务会计报告相关制度。

4) 建立并实施经营管理活动分析评价制度。各级管理层开展经营管理活动分析,对经营管理情况实施审核和监督。

### 1.2.3.4 信息与沟通

信息与沟通是公司经营管理所需的信息被识别、获得并以一定形式及时地传递，以便员工履行职责。信息不仅包括内部产生的信息，还包括与公司经营决策和对外报告相关的外部信息。畅通的沟通渠道和机制使公司的员工能及时取得他们在执行、管理和控制公司经营过程中所需的信息。公司建立符合发展战略并与经营管理活动一体化的信息系统，为公司风险管理提供足够的信息资源和顺畅的沟通渠道。

#### 1) 信息资源收集。

公司持续不断地识别、收集、整理与归纳来自内部与外部、经营与管理的各种信息。针对不同的信息来源和信息类型，明确各种信息的收集人员、收集方式、传递程序、报告途径和加工与处理要求，确保经营管理各种信息资源得到及时、准确、完整收集。

2) 信息沟通渠道。公司建立横向和纵向相互通畅、贯穿整个公司的信息沟通渠道，确保公司目标、风险策略、风险现状、控制措施、员工职责、经营状况、市场变化等各种信息在公司内部得到有效的传达。

公司建立适当的渠道，与公司的相关方如供应商、客户、律师、股东、监管机构、外部审计师，就相关信息进行必要的外部沟通。

3) 信息披露。公司制定完善的信息披露管理制度，明确重大事项的判定标准和报告程序，确定披露事项的收集、汇总和披露程序，符合资本市场监管要求。

#### 4) 信息系统

公司将信息技术应用于风险管理各项工作，运用信息系统对经营管理进行过程控制和信息的采集、存储、加工、分析、测试、传递、报告和披露等，实现对各种风险计量和定量分析、定量测试；能够适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并进行重大风险预警；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。

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。

(1) 建立信息系统总体控制。建立包括信息系统的控制环境、信息安全、项目建设管理、系统变更管理、系统运行维护、最终用户操作等六方面内容的信息系统总体控制规范与规章制度。

(2) 建立信息系统应用控制。全面识别应用系统相关风险，建立完善的应用系统控制规范，对应用系统的输入、处理和输出进行有效控制。公司信息系统提供的信息应达到一致性、准确性、及时性、可用性和完整性的目标。公司确保信息系统稳定运行和安全，并根据实际需要不断进行改进、完善或更新。

(3) 建立流程管理信息系统。建立统一业务流程管理平台，实现业务流程语言、设计规范、管理制度、控制措施、流程发布的统一管理，建成满足全面风险管理，具有开放性、可拓展性的流程管理信息系统。

### 1.2.3.5 监督

监督是对内部控制体系有效性进行评估的持续过程。包括持续监督、独立评估和缺陷报告等。公司应以重大风险、重大事件和重大决策、重要管理及业务流程为重点，对内控体系的有效性实施监督。

1) 持续监督。公司制定内部控制体系运行与维护管理制度，定期维护《内部控制管理手册》，将内部控制工作纳入公司各级管理层业绩考核，构建内部控制体系运行长效机制。

公司各级管理部门、流程责任部门，在体系日常运行中，实施自我监督和自我检查，并将检查、检验报告报送内控管理部门。

2) 独立评估。以风险为导向，建立完整的测试规范，定期对各部门和业务单位内部控制体系有效性进行检查和监督。

3) 缺陷报告。建立健全缺陷报告管理机制，制定缺陷认定规范，明确上报内控缺陷的程序。

## 1·3 组织结构、职责与权限

### 1·3·1 目的

通过建立分工合理、职责明确、报告关系清晰的组织结构，明确内控管理决策机构、管理机构、执行机构和监督机构的责任和义务，确保本公司内部控制的职责、权限及其相互关系得到规定和沟通，使本公司内部控制体系得到有效运行。

### 1·3·2 机构

公司内部控制和风险管理体系工作，在总裁领导下形成决策、管理、执行、监督四个层次的管理架构：

1) 决策机构：内控体系建设委员会是公司内部控制和风险管理工作的决策机构；

2) 管理机构：内部控制部作为公司内部控制体系日常管理部门和委员会的办事机构；

3) 执行机构：总部各部门、专业分公司、地区公司作为执行层，按照内部控制和风险管理体系的统一要求，具体组织落实；

4) 监督机构：审计部门行使监督职能，负责对体系运行状况实施测试监督。

为加强对内部控制体系管理工作的组织和领导，各地区公司成立相应的内控体系建设委员会。内控体系建设委员会由各单位有关领导和部门负责人组成，由总经理担任内控体系建设委员会主任。内控体系建设委员会下设办公室。

### 1.3.3 职责与权限

#### 1.3.3.1 公司内控体系建设委员会主要职责

1) 审定内部控制体系框架及实施计划。

2) 审定内部控制体系建立、测试和评估方案，对内部控制体系建设工作进行安排、部署。

3) 协调解决内部控制体系建设工作中的重大问题。

4) 审查批准对各部门、专业分公司和地区公司进行内部控制体系建设的考核方案，并组织实施。

5) 负审定需要提交董事会或管理层解决的重大事项。

6) 督导、督促公司内部控制体系的建立、完善和运行。

#### 1.3.3.2 内部控制部主要职责

1) 根据国家有关法律、法规及相关规定，负责组织制定集团公司、股份公司内部控制及风险管理制度、标准及方法；

2) 负责编制集团公司、股份公司内部控制及风险管理体系建设规划、体系框架，并组织实施；

3) 负责组织集团公司、股份公司风险评估工作，确定重大风险，建立风险数据库；

4) 负责组织和协调集团公司、股份公司业务流程相关工作管理；

5) 负责组织集团公司、股份公司风险控制设计及实施，负责内部控制及风险管理体系日常维护；

6) 协调内、外部审计测试，组织开展运行评价、改进测试和缺陷评估。负责组织内部控制及风险管理体系运行监督考核；

7) 代拟股份公司管理层内部控制评估报告，协助董秘局处理对外披露相关事宜；

8) 负责集团公司、股份公司内部控制及风险管理业务培训。

#### 1.3.3.3 公司各部门、专业分公司、地区公司职责

1) 审计部负责内部控制体系执行有效性的监督，组织实施管理层测试，其主要职能包括：

(1) 编制管理层测试计划和方案，经管理层批准后组织实施；

(2) 按照审计规定和公司发布的内部控制体系评价规范，每年定期组织实施管理层测试，对测试结果进行汇总、确认和分析，并分别向管理层和审计委员会汇报；

(3) 对被测试单位（股份公司机关、专业公司、地区公司）出具测试报告。

2) 监察部、审计部负责建立和完善反舞弊工作机制。

3) 信息管理部负责公司信息系统总体控制和应用控制管理制度的建立、运行维护工作。

4) 法律部负责公司规章制度和法律风险的综合管理

5) 公司各部门、专业公司按照内部控制和风险管理体系的各项要求，具体负责本部门、专业公司内控体系建设、运行、维护等工作的具体实施。

6) 地区公司内控建设是股份内控体系的组成部分。地区公司按照《内部控制管理手册》的要求，具体负责本公司内部控制体系建设、运行、维护等工作，并对特殊风险和业务流程制定专门管理办法。

地区公司的内部控制管理接受公司内部控制部领导。

## 2 控制环境

### 2.1 概述

#### 2.1.1 概念

控制环境确立公司风险管理的总体态度，是内部控制体系的基础，是有效实施风险管理的保障，直接影响内部控制体系的执行、公司经营目标及整体战略目标的实现。

#### 2.1.2 要素

控制环境包括诚信与道德价值观、发展目标、管理理念与企业文化、风险管理策略、董事会及下属委员会、组织结构、权利和责任分配、人力资源政策与措施、员工胜任能力以及反舞弊机制等内容。

##### 2.1.2.1 诚信与道德价值观

一个公司的目标及目标实现的方式基于该公司的优先选择、价值判断和管理层的经营风格。这些优先选择和价值判断反映出公司管理层的诚信及其信奉的道德价值观。

##### 2.1.2.2 发展目标

公司制定发展目标,作为风险评估的前提条件，只有先确立了目标，管理层才能针对目标确定风险，并采取必要的行动来管理风险。公司制定战略目标，并在此基础上制定相关经营目标、报告目标和合规性目标。

战略目标：与高层次目标有关，支持公司的使命并与此相一致。

经营目标：与公司资源利用的效率和效果、防止公司不因灾害性风险或人为失误而遭受重大损失有关。

报告目标：与为公司经营管理和对外披露提供信息的可靠性有关。

合规性目标：与公司对适用法律和法规的遵循性有关。

公司发展目标可以分为公司层面目标和业务活动层面目标。公司层面目标是指公司的总目标和相关战略规划，与高层次资源的分配和优先利用相关。业务活动层面目标是总目标的子目标，是针对公司业务和管理活动的更加专门化的目标。

##### 2.1.2.3 管理理念与企业文化

管理层的管理理念和企业文化会影响公司的管理方式，包括面对各种风险的态度。管理层的管理理念和企业文化还表现在：管理层对财务报告的态度，在现在可替代的会计准则选择方面是保守的还是激进的，进行会计核算时是否遵循谨慎性原则，对待数据处理、会计职能及人事管理方面的态度如何等。

继承和发扬公司企业文化，体现公司的经营宗旨、价值观念和行为准则；将风险管理文化融入企业文化建设全过程。

##### 2.1.2.4 风险管理策略

公司围绕发展战略，确定风险容量、风险承受度、风险管理有效性标准，体现公司风险管理的总体策略，并据此制定风险反应方案。

##### 2.1.2.5 董事会及下属委员会

控制环境和“高层管理基调”受到公司董事会及下属委员会的重大影响。影响因素包括：董事会和审计委员会相对于管理层的独立性、其成员的经验和职业道德水平、参与和监督公司活动的范围以及其行为的适当性；影响因素还包括董事会和审计委员会对涉及公司计划或业绩等问题的询问和质疑程度以及管理层解决这些问题的程度，董事会和审计委员会与内、外部审计师的交流和沟通程度。

#### 2.1.2.6 组织结构

公司的组织结构提供了一个构架，在此构架中为实现公司目标对公司活动进行规划、执行、控制和监督。建立一个相关的公司组织结构的主要内容包括：确定权责的关键领域以及建立适当的报告负责部门。公司根据自身的需要来确定其组织结构。公司组织结构的适当性在相当程度上取决于公司的规模及其活动的性质。

#### 2.1.2.7 权利和责任分配

包括对公司经营活动的权限和职责分配、建立上下级报告关系和授权协议。它涉及到鼓励个人和团队主动提出和解决问题的程度以及他们被授予的权限，还涉及到描述适当的开展业务的政策、骨干员工的知识和经验以及为履行职责而提供的资源。

#### 2.1.2.8 人力资源政策与措施

人力资源政策引导员工达到公司期望的职业道德水平和胜任能力。人力资源工作涉及员工聘用、定岗、培训、评价、晋升、考核、薪酬等活动。

#### 2.1.2.9 员工胜任能力

胜任能力应反映出员工完成工作任务所需要的知识和技能。工作任务需要具备什么样的知识和技能的员工来完成，通常是管理层根据公司的目标和实现这些目标的战略和计划，在胜任能力和成本之间进行平衡后做出的决策。

#### 2.1.2.10 反舞弊机制

反舞弊机制不仅需要满足合法性要求，而且应该具有预防性和及时性，受到公司管理层的直接监督和重视。它强调审计、监察等部门的作用，主要包括进行舞弊风险分析、评估并测试反舞弊控制设计和执行的有效性、执行舞弊违规调查并提出整改意见等工作。

## 2.2 诚信与道德价值观

### 2.2.1 职业道德规范的制定及推行

#### 2.2.1.1 内控关注要点

管理层应该向员工传达职业道德规范，并且必须不折不扣地执行。员工应该知晓和理解这些规定。管理层应该在言谈和行动中表现出对职业道德规范一丝不苟的遵循。具体包括：

- 1) 职业道德规范是全面的，针对利益冲突、非法或其他不当付款、反不正当竞争准则、内幕交易等。
- 2) 公司对职业道德规范进行有效的宣传推广。
- 3) 员工知晓什么行为是可接受的，什么是不可接受的，以及当遇到不当行为时应该采取的行动。

#### 2.2.1.2 措施

- 1) 建立并推行高级管理人员的职业道德规范。

(1) 公司制定《中国石油天然气股份有限公司高级管理人员职业道德规范》，并使其与《国有企业领导人员廉洁从业若干规定（试行）》、《中国石油天然气股份有限公司章程》、企业精神与宗旨、企业核心经营理念成为公司对各层管理人员，包括董事在内的，特别是高级管理人员的主要道德准则。

(2) 公司制定《中国石油天然气股份有限公司高级管理人员职业道德建设制度》，将对高级管理人员职业道德规范的宣传作为职业道德建设的重要工作内容：

①公司总裁是公司职业道德的倡导者，践行的表率，也是公司职业道德建设的第一责任人。总裁通过公开信函把公司高级管理人员职业道德规范介绍给全体高级管理人员并提出努力执行的希望和要求，并在每年工作会上宣讲高级管理人员职业道德规范；同时对职业道德建设提出要求。

②公司将职业道德建设列入公司高级管理人员的培训内容，通过印发学习资料、把职业道德建设

列入部分培训班的学习内容、利用网络或开设职业道德建设学习栏目等多种形式开展培训。

③公司要求新提升聘任的高级管理人员及时学习职业道德规范。

④公司每年组织高级管理人员签订“职业道德规范确认书”，并将签订的责任书报企业文化部。

2) 建立并推行员工职业道德规范。

(1) 公司制定《中国石油天然气股份有限公司员工职业道德规范》，与《中国石油天然气集团公司企业文化建设纲要》成为适用于全体员工的职业道德规范。

(2) 公司制定《中国石油天然气股份有限公司员工职业道德建设制度》，对员工职业道德规范的宣传是公司职业道德建设的重要工作内容：

①总裁通过文件、讲话等不同形式把公司员工职业道德规范介绍给全体员工，并提出践行的希望和要求。公司每年的工作会议上均有宣讲职业道德的内容，并对员工提出遵守职业道德规范的要求。

②将职业道德建设列入公司员工的培训内容，通过印发学习资料，把职业道德建设列入员工培训的常规学习内容，以及利用网络及其他形式进行职业道德建设学习宣传。

③对新员工开展关于职业道德规范方面的岗前教育培训，并在劳动合同中纳入遵守公司职业道德规范的内容。

3) 对员工遵守职业道德规范情况进行监督。

公司监察部和人事部等部门根据公司管理层的授权，对公司员工遵守职业道德规范的情况进行监督。员工违反职业道德规范的任何行为，除依照国家法律、上市监管地规则进行处理外，公司可以根据有关文件规定对其处分直至解除劳动合同。

#### 2.2.1.3 文档性记录

1) 中国石油天然气股份有限公司总裁致高级管理人员的信。

2) 中国石油天然气股份有限公司高级管理人员职业道德规范确认书。

3) 培训记录。

4) 会议材料（领导讲话材料）、会议纪要（或记录）等。

### 2.2.2 “高层管理基调”的建立

#### 2.2.2.1 内控关注要点

“高层管理基调”的建立包括详尽的道德指导和在公司上下沟通程度的指导。具体包括：

1) 通过一言一行，在公司范围内传达对职业道德规范的遵循。

2) 员工感觉到被同仁敦促做正确事情的压力。

3) 管理层对存在问题的迹象予以适当关注。

#### 2.2.2.2 措施

1) 董事会负责对公司高级管理人员的职业道德规范遵守情况进行监督，并授权公司总裁负责实施。公司管理层定期对高级管理人员职业道德规范的充分性和有效性做出评价，根据评价情况或董事会的要求做出修改。

2) 公司职业道德建设强调从“一把手”做起，总裁通过文件、讲话等不同形式把职业道德规范的要求传达给全体员工，并提出践行的希望；同时，通过领导干部廉洁从业检查、建立健全信访举报机制以及公示办法，在公司范围内传达管理层对职业道德规范的要求。

3) 公司根据《中国石油天然气股份有限公司劳动合同管理暂行办法》和相关业绩考核办法等多项规章对员工实施管理，对出现的违规行为进行处理，敦促员工遵守职业道德规范。

#### 2.2.2.3 文档性记录

1) 会议材料（领导讲话材料）、纪要（或记录）等。

2) 对员工违规的处理材料等。

### 2.2.3 与利益相关方的关系

#### 2.2.3.1 内控关注要点

管理层与员工、供应商、客户、投资者、债权人、保险公司、竞争对手和审计师等进行交往时，是否采用高的道德标准，并且要求其他人同样遵守道德标准。具体包括：与客户、供应商、员工和其他相关方的日常业务建立在诚实和公允的基础上。

#### 2.2.3.2 措施

1) 公司视诚信为立身之本、发展之基、信誉之源，要求在对外交往中也应遵循“平等互利、诚实守信”的原则。

2) 公司在《中国石油天然气股份有限公司高级管理人员职业道德规范》中强调高级管理人员应当公平对待员工、客户和供应商，不得通过操纵、隐瞒、滥用专用信息或对重大事实进行不实陈述等做法，不公平地对待上述人员。

3) 公司在《中国石油天然气股份有限公司员工职业道德规范》中规定：员工不得接受可能影响商务决策和有损独立判断的有偿馈赠，严禁为商务目的而以任何手段向政府官员提供、给予或承诺给予金钱和其他有价值的物品。

4) 公司设立举报电话、网上举报中心和电子举报信箱，鼓励全体员工和合作方检举任何所获知或遇到的违规行为。

#### 2.2.3.3 文档性记录

客户投诉、举报记录。

### 2.2.4 违规处理

#### 2.2.4.1 内控关注要点

针对违反政策和道德标准的情况采取适当的措施，具体包括：

- 1) 管理层对违规行为应进行回应。
- 2) 对违规行为要进行处理，处理的原则和结果应在公司上下进行传达。
- 3) 员工确信如果违规要承担后果。

#### 2.2.4.2 措施

1) 公司注重对员工违规情况的管理，主要通过审计、信访举报、民主监督等渠道进行。依据《中国石油天然气股份有限公司劳动合同管理暂行办法》等相关管理文件对员工违法违规行为进行处理。公司通过将需要接受处罚的违规行为写入劳动合同，使员工明确违规必定要受到处罚。对员工违规的处理主要采取批评教育、组织谈话、纪律处分等形式，处理结果在适当范围内进行通报。对重大违规事件还在公司范围内进行典型案例剖析，开展警示教育。

2) 公司制定管理人员违纪违规处理等相关规定，强化监督约束机制，规范管理人员行为，维护公司合法权益，保障公司健康发展。

#### 2.2.4.3 文档性记录

- 1) 信访案件情况通报。
- 2) 案例分析和警示教育宣传材料。
- 3) 对员工违规的处理材料等。

### 2.2.5 管理层对干预或逾越既定控制的态度

#### 2.2.5.1 内控关注要点

管理层对干预或逾越既定控制的态度，具体包括：

- 1) 管理层就需要进行干预的情形和进行干预的频率订立方针。
- 2) 管理层对控制制度的干预被适当地记录和解释。
- 3) 明确禁止管理人员逾越既定控制。



#### 2.2.5.2 措施

- 1) 公司的管理制度对各项业务的管理职责进行了界定,明确了部门及相关人员的职责和权利。
- 2) 公司通过岗位职责描述和权限指引的方式对各级管理人员的职责和权限进行详细描述,敦促员工按程序办事。
- 3) 管理层为了合法的目的而发生偏离既定的规章和程序的情形被详细记录。
- 4) 公司明确禁止管理人员违反公司的规定,鼓励对违纪违规行为进行举报,并予以保密。

#### 2.2.5.3 文档性记录

- 1) 风险控制文档。
- 2) 员工岗位职责描述。
- 3) 有关干预的记录。

### 2.2.6 实现目标的压力

#### 2.2.6.1 内控关注要点

确定合理的绩效目标,特别是短期目标;工资与绩效目标实现的挂钩程度是合理的。具体包括:

- 1) 不存在偏激的奖惩制度,影响员工对道德标准的遵守。
- 2) 升职和工资不能仅基于短期绩效目标的实现程度。
- 3) 实施控制以减少其他形式存在的诱惑。

#### 2.2.6.2 措施

1) 公司注重建立以业绩为基础的激励机制,针对不同层次的员工,分别制定《中国石油天然气股份有限公司总裁班子年度业绩考核办法》、《中国石油天然气股份有限公司高级管理人员业绩考核办法》、《中国石油天然气股份有限公司总部机关部门和专业公司中级管理人员绩效考核暂行办法》、《中国石油天然气股份有限公司中层以下管理人员业绩考核指导意见》和《中国石油天然气股份有限公司操作服务人员绩效考核指导意见》等制度,形成了较为系统规范的业绩考核评价体系。

2) 公司通过与高级管理人员签订业绩合同的方式,将高级管理人员应完成的主要任务量化为关键业绩指标,并严格按业绩合同和考核规定进行考核。业绩指标的选择和目标值的确定注重短期与长期目标相结合,即与公司总体发展战略、生产经营目标一致,并结合实际,具体明确,重点突出,覆盖受约人的主要工作内容。

3) 公司建立中级管理人员激励约束机制,通过与中级管理人员签订绩效合同的方式,将中级管理人员应完成的主要任务量化为关键绩效指标,并严格按绩效合同和考核规定进行考核。即与公司总体发展战略、生产经营目标一致,并结合实际,具体明确,重点突出,覆盖受约人的主要工作内容,确保公司战略目标和相关政策有效实施。

4) 公司将业绩考核作为确定员工薪酬、奖惩及任用的依据,使激励机制与约束机制相结合,达到责、权、利相统一。

#### 2.2.6.3 文档性记录

- 1) 业绩合同。
- 2) 业绩考核评价文档资料等。

## 2.3 发展目标

### 2.3.1 内控关注要点

#### 2.3.1.1 公司层面的目标

一个公司要达到有效控制就必须建立目标。公司层面的目标包括公司期望实现目标的总体说明,并有相关的战略规划支持。

- 1) 公司层面的目标提供对公司期望达到的主要目标的充分说明和指导,它们应当与公司直接相

关。

- 2) 公司层面目标的生效应与员工及董事会沟通。
- 3) 公司层面目标与战略计划的关联性和一贯性。
- 4) 公司计划和预算与公司层面目标、战略计划及当前情况的一致性。

#### 2.3.1.2 业务活动层面的目标

业务活动层面的目标来自公司的总目标和战略计划，并与之相联系，是随着具体对象和最终期限不断制定的。这些目标应针对每个重要活动并与其他活动保持一致：

- 1) 业务活动层面的目标与公司目标及战略计划一致。
- 2) 各个活动目标之间的一致性。
- 3) 所有重要业务流程与业务活动层面目标的相关性。
- 4) 业务活动层面目标的具体性。
- 5) 资源的充足性。
- 6) 确定决定公司整体目标实现与否的重要因素。
- 7) 管理层参与制定公司目标以及他们对目标的负责程度。

### 2.3.2 措施

#### 2.3.2.1 公司层面的目标

- 1) 制定公司层面的目标并向员工传达。

公司在中长期业务发展规划中明确长远发展目标和发展规划。规划分为公司规划、专业分公司规划、地区公司规划、专项规划和区域规划。

公司通过培训、宣传手册、领导报告等形式将公司层面目标传达给员工。

- 2) 制定支撑公司实现总体目标的规划。

公司在对外部环境、行业、竞争对手进行分析，对内部资源能力、优劣势及机会与威胁进行分析的基础上制定中长期业务发展规划。中长期业务发展规划主要指按国家统一部署编制的五年计划和十五年长远规划，以及公司根据市场变化而滚动编制的五年业务发展计划，包括专业分公司、地区公司各级业务发展计划。

- 3) 制定年度计划与预算。

公司根据中长期业务发展规划，制定年度投资计划、年度生产经营计划等。公司制定《中国石油天然气股份有限公司规划计划工作管理暂行办法》，明确规定计划编制的内容、程序及相关要求。

公司编制年度预算，对预算经营年度的经营目标及相应措施做出预期安排。公司制定《中国石油天然气股份有限公司预算管理暂行办法》，对预算编制的基本原则、预算的内容、编制依据及程序等进行明确规定。

公司的年度计划和预算总体上符合中长期业务发展规划确定的效益目标、投资方向和投资结构。

公司的年度计划和预算由相关部门汇总并综合平衡后，报董事会审批，以保证计划和预算与公司目标相一致。

#### 2.3.2.2 业务活动层面的目标

- 1) 通过上下沟通将公司总体目标和规划分解至业务活动层面。

公司业务活动的具体目标来源于公司总体目标和规划，并且根据公司总体目标和规划进行分解。

各单位根据本单位的实际情况和公司的总体目标要求提出本单位的业务活动目标，并经过公司管理层的审核，通过上下不断的沟通最终确定业务和职能单位的目标。

各单位的年度计划和预算也采用上下沟通的方式来确定。

年度计划的确定过程为：

- (1) 公司计划部门根据发展战略和董事会、管理层的总体要求提出年度计划编制要求。
- (2) 各业务和职能部门结合本单位的实际情况，提出本单位的业务活动计划。
- (3) 公司计划部门进行汇总并综合平衡，提出年度计划，经董事会批准后下发执行。

预算确定的过程为：

(1) 公司预算管理委员会根据经董事会批准的公司年度经营目标确定下一年度的预算目标，并将预算目标分解至各业务和职能部门。

(2) 公司各单位在全面分析以前年度预算执行情况的基础上, 根据对下一预算年度经营环境的变化、年度经营目标和部门计划, 编制下一预算年度的预算草案, 交本部门主管领导审核后报预算管理部门。

(3) 公司预算管理部门对各单位的预算进行汇总并综合平衡, 并提出年度预算, 经董事会批准后下发。

公司的业绩指标分为: 效益类、营运类、控制类指标。对于关键业绩指标, 有一定的衡量标准。各单位再将其目标分解至各子业务活动中, 保证各项业务活动都有具体的目标。

为保证业务活动具体目标之间的一致性, 公司管理层不断采取措施审查各业务活动的具体目标, 根据业务活动的具体情况及发现的问题不断进行补充和完善, 业务活动的目标每年更新一次。

2) 配置相应的资源以保证业务活动层面目标的实现。

公司在确定各个业务活动目标之后, 将公司的资源如财务、人事、设施、技术等资源以计划和预算的形式分解至各单位, 以保证各单位能够有实现其业务活动的目标资源。

3) 制定具体业务活动目标。

公司在确定各业务和职能部门的目标后, 各单位的主管领导通过工作计划等形式再将其目标分解至各具体业务活动中, 并明确相应岗位的目标。

### 2.3.3 文档性记录

- 1) 中长期业务发展规划。
- 2) 公司五年业务发展规划。
- 3) 年度投资计划。
- 4) 年度生产经营计划。
- 5) 公司年度预算。
- 6) 业绩合同。

## 1.4 管理理念与企业文化

### 2.4.1 业务风险的接受程度

#### 2.4.1.1 内控关注要点

公司接受业务风险的态度, 包括:

- 1) 在介入新业务前, 是否经过仔细的风险和收益分析后才采取行动。
- 2) 是否经常介入风险特别高的业务, 还是在接受风险方面非常保守。

#### 2.4.1.2 措施

1) 公司在管理业务风险方面, 制定了《中国石油天然气股份公司对外投资管理暂行办法》、《中国石油天然气股份有限公司短期投资管理办法》、《中国石油天然气股份有限公司短期投资管理实施细则》等制度规范。

2) 大力继承和发扬良好的风险管理文化, 树立和传播正确的风险管理理念, 将风险管理意识转化为员工的共同认识和自觉行动。风险管理文化建设应与薪酬制度、人事制度相结合。公司高级管理人员应在继承和发扬风险管理文化中发挥表率作用, 中层管理人员应继承和发扬风险管理文化的骨干作用。

公司将在以后的内控体系建设中, 将风险管理文化建设融入到企业文化建设全过程中, 逐步树立和传播正确的风险管理理念, 增强员工的守法意识和诚信意识。

#### 2.4.1.3 文档性记录

投资计划及相关审批资料。

### 2.4.2 关键人员的更换频率

#### 2.4.2.1 内控关注要点

关键部门人员（例如：经营、会计和数据处理等部门）的更换频率，具体包括：

- 1) 管理层和监督层人员是否存在过高的更换频率。
- 2) 关键岗位员工是否存在突然辞职，或辞职提前通知期较短的现象。

#### 2.4.2.2 措施

1) 公司确保持管理层、监督职能人员的稳定，杜绝人员频繁更换，保持公司财务、信息等系统员工队伍稳定。

2) 公司在《中国石油天然气股份有限公司劳动合同管理暂行办法》中规定：对于知识产权、科研成果归属问题悬而未决的，或从事的重要工程、设计、研究项目或重要生产（工作）任务尚未完毕，离开会给用人单位造成重大损失的员工，用人单位可以拒绝其提出解除劳动合同的要求。

### 2.4.3 管理层对数据处理、财务报告等的态度

#### 2.4.3.1 内控关注要点

管理层对数据处理和会计职能的态度，以及对财务报告和资产安全可靠性的关注。具体包括：

- 1) 财务职能被认为仅仅是公司的“计数中心”，还是公司各种经营管理活动的控制中心。
- 2) 所选用的会计准则是否追求财务报告利润最高。
- 3) 如果会计职能为分散管理，地区公司负责人是否对报告结果签字确认。
- 4) 基层单位的财务部门是否与总部的财务部门有工作汇报关系。
- 5) 重大资产，包括知识资产和信息被严格地保护，防止未经授权的接触。

#### 2.4.3.2 措施

##### 1) 财务管理。

公司财务部具有财务管理和监督职能，涉及资金管理、资产管理、价格管理、债务管理、税收管理以及财务制度管理等多个方面。

财务总监作为公司管理层成员参与主要经营活动的决策。

##### 2) 会计政策的选用。

公司财务部按照《会计法》、《企业会计准则》、《企业会计制度》及国际会计准则、美国会计准则的要求，制定适合本公司的财务会计制度，并根据政策和准则的变化及时修订。

公司会计政策前后各期保持一致，而且公司所有的合并报表单位的会计政策均与公司保持一致。

公司按国际会计准则、美国会计准则对外披露财务会计报告。

##### 3) 财务报告制度的建立。

公司实行会计一级集中核算的财务模式，即在全公司采用一套账进行会计核算。行政上，地区公司财务人员隶属地区公司，向地区公司总经理负责；业务上，在公司财务部和专业分公司的指导下开展工作。地区公司执行公司统一的财务会计制度。

公司财务部统一编制公司财务会计报告。

##### 4) 资产安全管理。

公司制定涉及油气资产及固定资产、资金、存货等资产的管理规定，明确资产安全管理办法，并注重对财务信息和知识产权的保护。

#### 2.4.3.3 文档性记录

财务分析材料。

### 2.4.4 高级管理人员相互交流的频率

#### 2.4.4.1 内控关注要点

高级管理人员和各级业务部门管理人员相互交流的频率，特别是在双方处于不同的地域时。具体包括：

- 1) 高级管理人员经常访问分支机构及不同地区的下属机构。
- 2) 经常召开公司或区域性的管理层会议。

#### 2.4.4.2 措施

1) 公司颁布实施《中国石油天然气股份有限公司领导办公制度》，注重高级管理人员之间的沟通：

(1) 公司每年召开两次工作会，贯彻落实股东大会、董事会决议，研究公司改革、发展、增效大计，总结年度（半年）工作，对下一年度（半年）工作做出部署。参会人员包括公司领导成员、监事会成员、机关职能部门和专业分公司主要负责人、地区公司经理。

(2) 公司每季度召开一次经营形势分析会，重点研究上一季度和年初以来公司主要生产经营指标完成情况、生产建设和投资完成情况、预算执行情况、存在的主要问题、解决措施和下一步工作安排。参会人员包括：总裁、高级副总裁、副总裁、财务总监、总地质师，规划计划部、财务部、审计部和各专业分公司领导及财务负责人等。

(3) 公司管理层每周举行工作例会，各专业分公司、地区公司每周召开生产经营协调会，通报上周生产经营情况，协调解决有关问题，确定本周主要工作安排。

(4) 公司总裁根据需要组织召开总裁办公会，并根据会议内容确定会议列席人员。

2) 公司高级管理人员定期走访调研基层单位。

#### 2.4.4.3 文档性记录

- 1) 会议安排。
- 2) 会议纪要。

## 2.5 风险管理策略

公司围绕发展战略，确定风险容量、风险承受度、风险管理有效性标准，体现公司风险管理的总体策略，并据此制定风险反应方案。

公司确定针对发展战略的风险容量，体现公司在战略制定与实施过程中愿意承受的风险范围和风险水平，反映公司的风险偏好。公司针对特定目标，制定具体的风险承受度，体现在实现特定目标过程中公司对差异的可接受程度。公司确定风险容量和风险承受度，要正确认识和把握风险与收益的平衡，防止忽视风险，片面追求收益或者单纯为规避风险而放弃发展机遇。风险承受度与风险容量保持一致。

公司根据风险管理的总体目标，制定风险管理有效性标准。

公司将在以后的内控体系建设中，围绕公司的发展战略，逐步确定公司风险容量、风险承受度和风险管理有效性标准，制定公司风险管理策略。

## 2.6 董事会及下属委员会

### 2.6.1 独立性

#### 2.6.1.1 内控关注要点

董事会或审计委员会独立于管理层，可以对管理层的决策提出必要的质疑。具体包括：

董事会对管理层的决定（如战略决策、重大交易）进行推断并提出置疑，对前期运营结果进行质询（如预算执行差异）。

#### 2.6.1.2 措施

1) 公司董事会的构成及独立性符合国内公司法。根据公司章程, 公司董事会由 13 名董事组成, 设董事长 1 名, 副董事长 2 名。13 名董事中有 4 名董事同时是公司执行机构成员, 1 名董事是公司内部员工代表, 另有 3 名董事为独立非执行董事。公司的独立非执行董事由董事会提名, 并由股东大会选举产生。董事会设秘书 1 人。公司设董事会秘书局, 其工作由董事会秘书负责。董事会的构成不完全符合美国有关法规的要求, 公司根据豁免条例, 就差异部分进行了披露。公司董事会向股东大会负责, 按照《中国石油天然气股份有限公司章程》、《中国石油天然气股份有限公司董事会工作手册》履行对管理层战略决策、重大交易、预算执行差异质疑等职责。

2) 公司建立独立董事制度, 独立非执行董事未在本公司担任任何职务, 但出席公司董事会会议, 参与讨论决策有关重大事项; 以其丰富的专业知识和经验, 就公司规范运作和有关经营工作提出意见; 对关联交易是否符合上市地监管部门的要求提供公正、合理性的意见, 确保关联交易的公平合理, 为公司的日常业务即按一般商业调控推行的资产重组及关联交易等进行审核, 并发表独立意见。

3) 董事会每年至少召开四次例会, 且经 1/3 以上董事、董事长或总裁均可提议召开临时董事会会议。

4) 公司董事会下设审计委员会, 审计委员会由 4 名成员组成, 3 名为独立董事。审计委员会设主任委员 1 名, 由董事会从独立董事中提名产生。审计委员会按照《中国石油天然气股份有限公司审计委员会组织和工作规则》履行其监督职责, 其决议须经独立董事表决通过。按照《审计委员会的工作程序和自评指引》内容, 从权力、组织—成员、组织—会议、内部控制、财务报告、法规的遵循、外部审计、内部审计、反舞弊控制、委员会的汇报职责、业绩评价和章程等十二个方面 65 项内容, 评估审计委员会职责完成情况。

#### 2.6.1.3 文档性记录

董事会会议记录。

### 2.6.2 董事会 / 专门委员会

#### 2.6.2.1 内控关注要点

对于特定事务, 必要时建立董事会专门委员会, 以关注和处理相关重要事件, 他们在专业和资历方面能够有效地处理相关的重要问题。

#### 2.6.2.2 措施

公司董事会下设 4 个专门委员会: 审计委员会, 投资与发展委员会, 考核与薪酬委员会, 健康、安全与环保委员会。

董事会的专门委员会全部由董事组成, 其中审计委员会由 4 名成员组成, 3 名成员是公司独立董事, 有 1 名成员具有会计或相关财务管理专长; 考核与薪酬委员会的成员中独立非执行董事占多数, 并担任主任委员。

董事会的专门委员会主要职责是为董事会进行决策提供支持。参加专门委员会的董事, 按分工侧重研究某一方面的问题, 并为公司管理水平的改善和提高提出建议。

### 2.6.3 董事的知识和经验

#### 2.6.3.1 内控关注要点

董事的知识和经验。具体包括: 董事拥有足够的知识、行业经验和时间, 以有效地开展工作。专门委员会人数充分, 足以处理专业性、重大性事务。

#### 2.6.3.2 措施

1) 公司在《中国石油天然气股份有限公司章程》中规定了董事的任职资格。

2) 公司慎重地选择董事、各专门委员会成员的人选：由持有公司股份 5% 以上的股东提名董事候选人名单，由董事会授权董事长汇总董事候选人，在股东会上投票表决选举产生。董事的知识和经验丰富，独立董事具有很高的威望，能为董事的监督提供质量保障。

3) 公司对董事会及专业委员会的会议议程进行规定，保证与议题相关的议案、文件等资料能够提前送达相关人员，使其有足够的时间了解议案并做出正确判断。

## 2.6.4 与内、外部审计师等的会面频率和接触

### 2.6.4.1 内控关注要点

财务负责人、会计人员、内部审计和外部审计人员会面的频率和时间。审计委员会每年审核内部和外部审计师的工作范围。

### 2.6.4.2 措施

1) 审计委员会会议每年至少召开四次，审计委员会主任委员可以应外部独立审计师或内部审计师的要求召开会议。审计委员会成员认为有必要，可随时提议召开会议。会上听取财务部、审计部、独立审计师的汇报，在认真讨论后，就审核结果形成一份书面的审阅意见书。

2) 审计委员会负责审核外部审计师的资质（包括合伙人和审计人员的背景和经验）及其独立性，确保其负责合伙人的定期轮换符合相关法律法规；对外部审计师的表现进行年度审核，会同监事会向股东大会提出聘用、续聘、解聘外部审计师及其审计服务费用的建议；根据现行法律法规和其他监管要求的变化，审核外部审计师提议的本年度审计范围和方法，评估其工作内容和程序是否客观、有效，并预批准该等审计服务；制定有关外部审计师提供非审计服务的政策，确保该等非审计服务不会影响其独立性或客观性，审核并批准外部审计师向公司提供非审计服务的事项及其费用；与外部审计师讨论双方认为必须单独讨论的事项，保证外部审计师在需要时与审计委员会有畅通的沟通渠道；每年从外部审计师处获得关于其内控质量及其可能存在的重大缺陷和不足的报告；审核公司雇用外部审计师事务所职员及前职员的政策，并监督其落实情况。

3) 审计委员会根据国内外适用规则，检查、监督内部审计部门的工作，检查内部审计部门职能发挥的有效性，保证其在公司内控制度中能够充分发挥作用；与管理层和内外部审计师协调并共同审核公司内部控制和风险管理及风险审核的质量、充足性和效力，以及在内部控制中存在的重要缺陷或重大弱点；检查公司的营运、财务及会计政策及实务。

4) 审计委员会定期听取有关反舞弊方面的情况汇报，监督员工对有关会计、内部控制、审计事项或舞弊方面的举报和投诉。

5) 审计委员会每年至少与公司外部审计师、内部法律顾问会晤一次。审计委员会行使职权时有权聘请独立的法律、会计或其他顾问（外部顾问）为其提供咨询服务。

### 2.6.4.3 文档性记录

审计委员会会议记录。

## 2.6.5 信息的及时性和充分性

### 2.6.5.1 内控关注要点

为董事会或审计委员会提供信息的及时性和充分性，以便及时监督管理层的目标和战略、公司的财务状况和经营成果，以及重大协议的条款等。具体包括：

1) 董事会定期收到关键信息，例如财务报告、主要的市场动向、重大合同和谈判信息。

2) 董事相信其得到了适当的信息。

### 2.6.5.2 措施

1) 公司制定《中国石油天然气股份有限公司董事会工作手册》，规定董事会全体董事有权获得为履行职责所需的公司信息。公司设董事会秘书和董事会秘书局，负责协调董事会和各委员会对所需信息的收集工作。公司定期向董事会成员提供日常信息，如快讯、生产运行月报等。

2) 董事会每年至少召开四次例会，董事会例会议程的议案和文件至少在会议召开前七个工作日送达各位董事。除上述例会外，经 1/3 以上董事、董事长或总裁提议，公司召开临时董事会会议。临时董事会的议案和文件至少在会议召开前两个工作日送达各位董事。

3) 审计委员会定期从公司管理层和法律顾问等有关方面了解可能对公司财务报告产生重要影响的法规遵循事项的更新信息。

4) 公司对外信息披露遵循《中国石油天然气股份有限公司信息披露控制和披露程序的原则》，董事会秘书局负责会同公司有关部门，做好对外信息披露工作。

#### 2.6.5.3 文档性记录

1) 董事会成员收到的信息记录。

2) 审计委员会成员收到的信息记录。

### 2.6.6 获知和调查不正当行为

#### 2.6.6.1 内控关注要点

关注董事会或审计委员会对敏感信息、调查和不正当行为进行评价的充分性和及时性（例如，高级职员的出差费用、重大诉讼、监管机构的调查、挪用或滥用公司资产、违反内部贸易规章、政治性付款、非法报酬等）。具体包括：

1) 存在告知董事会重大问题的程序。

2) 信息得到及时沟通。

#### 2.6.6.2 措施

1) 公司建立并不断完善出现紧急事项时召开董事会会议的机制和重大事件汇报的程序。

2) 审计委员会建立相关程序，接收、保留及处理公司获悉的有关会计、内部会计控制或审计事项的投诉；接收、处理员工有关会计或审计事项的投诉或匿名举报，并保证其保密性。

3) 审计委员会定期向董事会汇报，汇报事项包括有助于董事会及时了解可能影响公司财务状况及经营业务的重要事项。

#### 2.6.6.3 文档性记录

会议记录。

### 2.6.7 “高层管理基调”的审核

#### 2.6.7.1 内控关注要点

建立适当的“高层管理基调”。具体包括：

1) 董事会及下属委员会充分参与、评价“高层管理基调”的有效性。

2) 董事会 / 审计委员会采取行动以保证适当的“基调”。

3) 董事会明确地强调管理层应该遵守职业道德规范。

#### 2.6.7.2 措施

1) 公司董事会对高级管理人员遵守职业道德规范的情况进行监督，并授权公司总裁负责实施和监督规范的遵守情况。

2) 公司管理层定期对高级管理人员职业道德规范的充分性和有效性做出评价，并根据评价情况和董事会的要求做出修改。



3) 监事会按照《公司法》及《中国石油天然气股份有限公司监事会组织和议事规则》、《中国石油天然气股份有限公司章程》，行使对包括董事在内的公司高层管理人员进行职业道德规范遵守情况的监督。

## 2.6.8 监督管理层对审计发现的跟进

### 2.6.8.1 内控关注要点

董事会或审计委员会依据其发现，采取适当的措施，包括特殊调查。具体包括：

- 1) 董事会或审计委员会向管理层就需采取的具体行动下达指令。
- 2) 如果需要，董事会或审计委员会进行监督和跟踪处理。

### 2.6.8.2 措施

1) 公司制定《董事信息反馈制度》，董事会秘书局在每次董事会后，整理会议记录的同时，将各位董事在会议期间及在各专业委员会会议上提出的意见和建议进行归纳、整理和分类，并按程序报批同意后，送公司管理层。

2) 根据董事会开会和闭会期间董事提出的意见和建议，管理层责令有关部门对相关问题进行研究并提出具体整改措施。

3) 董事会秘书局负责收集、汇总董事会及专门委员会提出的要求、意见和建议的落实情况，并以董事信息反馈的形式呈报各位董事。

### 2.6.8.3 文档性记录

- 1) 董事信息反馈。
- 2) 审计委员会相关资料。

## 2.7 组织结构

### 2.7.1 组织结构适应信息流通和权力集中程度

#### 2.7.1.1 内控关注要点

公司组织结构的适当性，以及其提供管理活动必要信息流的能力。具体包括：

- 1) 考虑公司经营业务的性质，公司的组织结构按照适当集中或分散的管理方式设置。
- 2) 组织结构有利于信息的上传、下达和各业务活动间的传递。

#### 2.7.1.2 措施

1) 公司按照《公司法》的要求，参照国际大型石油公司的通行做法，结合公司实际，建立规范的法人治理结构（包括股东大会、董事会、监事会和总裁负责的管理机构），即建立起资产所有权、经营权分离，决策权、执行权、监督权分立，股东会、董事会、监事会并存的法人制衡管理机制。

2) 公司的经营管理实行一级法人、分公司为主的体制，分级授权管理，权责统一，逐级负责。公司的行政管理实行两级管理体制，即股份公司—地区公司；业务管理实行三级管理体制，即股份公司—专业分公司—地区公司。

3) 公司组织机构编制管理遵循“科学先进、实事求是；职责清晰、精干高效；统一归口、分级管理；规范程序、严格审批”的原则。

4) 建立内部控制体系运行网络。按照国资委《中央企业风险管理指引》的规定，逐步建立健全公司内部控制管理组织体系。明确内部控制组织体系的职责分工，形成包括董事会、审计委员会、管理层、内控体系建设委员会、内部控制管理部门、其他职能部门及各业务单位在内的内部控制管理组织体系。各单位根据实际情况，按规定设置内部控制管理机构或管理岗位负责内部控制日常管理工作。内部控制管理工

作应与其他管理工作紧密结合，把内控管理的各项要求融入企业管理和业务流程中。

公司将进一步修订和完善风险管理规范，明确规定董事会、公司总裁、内部控制管理部门、公司审计委员会及内审部门、其他职能部门和业务单位内部控制管理职责。

#### 2.7.1.3 文档性记录

组织结构图。

### 2.7.2 关键管理人员的知识和经验

#### 2.7.2.1 内控关注要点

关键管理人员具备执行相关职责的知识和经验。具体包括：负责的管理人员技能素质满足要求，具备执行其业务必备的知识、经验并接受适当培训。

#### 2.7.2.2 措施

1) 公司制定《中国石油天然气股份有限公司经营管理者职务竞聘试行办法》、《关于进一步推进地区公司领导班子行政副职竞聘上岗工作的安排意见》、《关于股份公司总部机关开展岗位竞聘实施意见》等一系列规章制度，选人用人机制实现经营管理者由单一的组织配置向组织配置与市场配置相结合的转变，确保管理人员的技能素质满足要求，具备执行其业务必备的知识、经验。

2) 公司制定《中国石油天然气股份有限公司关于选拔领导人员实行任前公示的暂行办法》，通过公司报纸、有线电视、网络等媒体发布公告或召开会议等方式，对经营管理者实行任前公示，增加选拔任用的透明度。

3) 公司注重对经营管理者的培养，通过针对性培训、轮岗交流、挂职锻炼等形式提高管理者素质。

#### 2.7.2.3 文档性记录

- 1) 竞聘选拔材料。
- 2) 公示文稿。

### 2.7.3 汇报机制的适当性

#### 2.7.3.1 内控关注要点

确立的汇报机制是有效的，能够保证管理人员获得与其责任和权限有关的信息。经营活动的管理人员有与相关的高级管理人员进行沟通和交流的通畅渠道。

#### 2.7.3.2 措施

1) 公司通过分级管理的组织结构和员工岗位职责描述对汇报关系进行了清晰的定义。机关职能部门向上级请示、报告工作，要先按照公司领导的工作分工向分管领导请示、报告，再根据请示报告类别，按照行政两级（股份公司—地区公司）或业务三级（股份公司—专业分公司—地区公司）管理体制向对口的上级请示、报告。正常情况下不得越级请示、报告工作。

2) 公司注重高层管理人员之间的沟通，建立相应的沟通和交流渠道并确保其畅通，如定期召开公司工作会、经营形势分析会，各职能部门负责人也有机会参加总裁办公会等高层会议，公司总部、专业分公司和地区公司定期举行工作例会，管理层定期或不定期走访调研基层单位等，使负责经营活动的管理人员能够与相关的高级管理人员进行沟通和交流。

3) 公司为员工向管理层反映问题和建议提供多种渠道，如员工代表大会制度、座谈会、接待日等。

#### 2.7.3.3 文档性记录

- 1) 各类请示报告材料。
- 2) 员工代表大会会议材料。

## 2.7.4 组织结构变化的适应性

### 2.7.4.1 内控关注要点

组织结构会在何种程度上随环境的变化而变化。具体包括：管理人员定期根据变化的业务或行业环境来评价公司的组织结构。

### 2.7.4.2 措施

1) 公司制定《中国石油天然气股份有限公司机构编制管理办法》，明确人事部为公司机构编制业务的归口管理部门，地区公司人事部门为本单位机构编制业务归口管理部门，并明确界定了股份公司和地区公司机构编制管理的范围。

2) 管理部门根据公司总体发展战略和管理定位及外部环境的变化，定期评价现有组织结构的合理性；需要做出调整的，管理部门组织评估、论证并提出机构编制调整方案，按照规定程序审批后实施。

### 2.7.4.3 文档性记录

- 1) 机构编制调整请示、审批材料。
- 2) 机构编制调整文件。

## 2.7.5 职员人数足够

### 2.7.5.1 内控关注要点

存在足够数量的员工，特别是管理人员。具体包括：

- 1) 管理人员拥有足够的时间来有效地履行职责。
- 2) 管理人员能够将工作分派给其下属，避免出现大量加班，以完成本可以由多名员工完成的工作。

### 2.7.5.2 措施

1) 为确保劳动力资源合理配置，公司针对工种（岗位）颁布相应的劳动定员定额标准，制定《中国石油天然气股份有限公司劳动定员定额标准化管理暂行办法》，并确保其得到有效实施。

2) 公司确定人员编制，以核准的工作量和生产任务为前提，以科学先进的劳动定员定额标准为依据，先定任务、定职责、定岗位，后定编制，并按编制配备人员，确保公司任用足够数量的员工和管理人员，保证各项业务工作顺利进行。

3) 公司颁布实施《中国石油天然气股份有限公司油气田地区公司组织结构设置指导规范》、《中国石油天然气股份有限公司炼化地区公司组织结构设置指导规范》、《中国石油天然气股份有限公司关于领导班子职务设置和职数管理的暂行规定》等制度，明确组织机构和相关岗位的设置标准，确保管理岗位人员配备的适当性。

4) 公司定期分析员工队伍结构和总量状况，确定下属公司的劳动用工总量，每年对各地区公司下发年度员工总量控制计划。

### 2.7.5.3 文档性记录

- 1) 劳动定员定额标准文件。
- 2) 年度用工总量控制计划文件。

## 2.8 权利和责任分配

## 2.8.1 责任分配与授权

### 2.8.1.1 内控关注要点

根据公司的目标、经营职能和监管要求，分配责任和授权，包括信息系统的责任和变化的授权。具体包括：

- 1) 职权和职责被授予公司内的员工。
- 2) 决策的责任与其职权和职责相对应。
- 3) 对员工进行授权和分配职责时，应充分考虑适当的信息。

### 2.8.1.2 措施

1) 公司根据经营目标、职能和监管要求，颁布实施《中国石油天然气股份有限公司机关部门职能及专业分公司职责范围》，并补充实施《关于集团公司和股份公司两个机关审计部实施整合的通知》、《关于成立集团公司、股份公司预算管理委员会和预算管理办公室的通知》、《关于成立集团公司、股份公司内部控制部的通知》、《关于成立预算管理办公室及调整财务部主要职责有关问题的通知》、《关于集团公司和股份公司规划计划部实施整合有关问题的通知》、《关于成立集团公司、股份公司物资采购管理部的通知》、《关于撤销质量安全环保部设立安全环保部和质量管理与节能部的通知》、《关于集团公司和股份公司两个机关维护稳定职能及资本运营部实施整合的通知》，明确公司各机关职能部门和专业分公司的职责。

2) 公司在明确管理层、部门职责的基础上，组织实施员工岗位职责描述，将职责分解到具体岗位；同时公司编制权限指引，以适应公司一级法人为主的经营体制，更好地落实分级授权制度。通过岗位职责描述和权限指引，公司对职责权限进行适当分配。

3) 公司规范信息系统（系统及业务系统）的授权，由应用相关信息系统的机关职能部门、专业分公司、地区公司根据不同的职责分别设置和维护用户授权。

公司目前编制的权限指引，主要针对财务报告控制有效性的关键控制，尚未涵盖公司主要业务流程，公司将在以后的内控体系建设过程中，逐步建立涵盖公司各主要业务流程的权限指引。

### 2.8.1.3 文档性记录

- 1) 员工岗位职责描述。
- 2) 权限指引。

## 2.8.2 数据、会计等员工技能的充分性

### 2.8.2.1 内控关注要点

数据处理和会计职能部门的员工应具备与公司规模、业务活动和系统相适应的技能水平。具体包括：从数量和经验两个方面考虑，公司拥有足够的员工以完成其职责。

### 2.8.2.2 措施

1) 公司配置充足的财务和信息系统的管理人员，所配置人员具备胜任工作需求的基本技能，能够满足公司生产经营业务活动的需要。

2) 公司规定使用网络财务管理信息系统的单位，应设置专职信息系统管理员；有条件的单位设置专门的信息系统组织机构，并任命负责人，负责财务管理信息系统的管理和维护。

3) 信息管理部门配合人事部门，统筹信息技术培训计划，组织多种形式不同层次的培训，包括对各级信息管理部门员工的培训。公司组织信息技术应用复合型培训，使信息管理人员更多地掌握公司其他领域的知识，有效地提高管理和决策水平。

4) 公司编制《中国石油财务培训纲要》作为指导公司财务人员培训工作的纲领性文件；同时，公司为财务人员提供项目性培训和开放性培训，系统化、规范化地开发财务人员的职业潜能，全面提高财务人员的业务能力和职业道德素质。

### 2.8.2.3 文档性记录

培训记录。

## 2.8.3 责任分配与授权的恰当性

### 2.8.3.1 内控关注要点

授权和所分配的责任相吻合。具体包括：

- 1) 完成工作所需要的权力与高级管理人员参与的程度应存在适当的平衡。
- 2) 授予合适级别的员工纠正问题或实施改进的权力，并且此授权也明确了所需的能力水平和权力界限。

### 2.8.3.2 措施

1) 公司对业务活动的权限，根据不同的业务性质，在机关职能部门、专业分公司和地区公司之间有所划分；根据业务活动的重要性程度，按不同层次进行审批。公司对业务权限进行梳理和规范，形成公司整体的权限指引，并及时进行维护更新。

2) 公司通过对岗位职责描述的规范、完善，明确各个岗位在处理有关业务时所具备的权力。

3) 公司规定授权人有权对受托人履行授权的行为进行监督、检查，发现受托人不适当履行授权的情形，应及时给予批评并及时纠正。对受托人未尽职责造成失误或损失的，应撤销授权。

### 2.8.3.3 文档性记录

权限指引。

## 2.9 人力资源政策与措施

### 2.9.1 人力资源政策和程序

#### 2.9.1.1 内控关注要点

雇佣、培训、晋升和员工薪酬的政策及程序，具体包括：

- 1) 现有人力资源政策和程序可以招聘并发展有能力、可信的人员，能够支持有效的内部控制体系。
- 2) 对招聘和培训合适人员的关注程度是适当的。

#### 2.9.1.2 措施

1) 公司通过与员工订立劳动合同的形式确立劳动关系，并依据《劳动法》和《中国石油天然气股份有限公司劳动合同管理暂行办法》等管理规定对员工实施必要的管理。人事部门通过组织开展竞聘或招聘活动，对关键岗位和紧缺人才进行选拔。招聘程序一般包括资格初审、专业知识和素质测评、专业答辩和专家组评审等必要程序。

2) 公司针对总裁班子成员、高级管理人员、中层及以下管理人员、操作人员分别制定考核制度，形成较为系统、规范的业绩考核评价体系，对员工履行职责、完成任务的情况实施全面、客观、公正、准确地考核，并以此作为确定员工薪酬、奖惩及任用的依据。

3) 公司制定《中国石油天然气股份有限公司员工教育培训工作暂行规定》等相关规章制度，每年制定并下达培训工作计划，有针对性地组织业务和操作技能培训，确保员工技术素质和业务能力达到岗位要求。

4) 公司制定《中国石油天然气股份有限公司薪酬总额与业绩指标挂钩办法》、《中国石油天然气股份有限公司完善基本工资制度实施方案》、《中国石油天然气股份有限公司高级管理人员年薪制管理办

法（试行）》等制度，建立内部薪酬激励和约束机制，调动员工的积极性和创造性，增强公司的市场竞争力。

5) 根据总体战略，公司每年通过对包括招聘、培训、考核、薪酬、职务晋升等制度在内的人力资源政策进行调整，使之能够有效地支持公司战略的实施。

#### 2.9.1.3 文档性记录

- 1) 员工的《劳动合同》文本。
- 2) 业绩考核文档资料。
- 3) 培训计划及记录。
- 4) 员工职务晋升、薪酬调整文档资料。

### 2.9.2 员工责任和目标

#### 2.9.2.1 内控关注要点

员工（包括新员工）应意识到他们的工作职责和公司对他们的期望。

#### 2.9.2.2 措施

1) 公司组织实施的员工岗位职责描述，明确岗位的相应责任、职责和权限，使员工能从中了解工作职责和公司对他们的具体要求。

2) 公司对新员工进行岗前教育培训，包括应知应会的知识和技能、安全常识、公司规章制度要求等，帮助其了解岗位职责，并使其达到岗位要求的基本技能素质。

3) 公司与高级管理人员签订业绩合同，明确其需要承担的指标和责任。

4) 公司组织员工定期进行工作总结，评价员工工作表现，分析员工当前的成绩、经验与不足，对下阶段工作进行安排，使员工意识到所负的责任和公司对他们的期望。

#### 2.9.2.3 文档性记录

- 1) 员工岗位职责描述。
- 2) 业绩考核文档资料。

### 2.9.3 违规行为的纠正措施

#### 2.9.3.1 内控关注要点

对违背政策和程序的行为的校正，具体包括：

- 1) 管理层对工作失职采取适当的措施。
- 2) 对违背政策的行为有适当的纠正措施。
- 3) 员工应明白未照章执行的行为最终将被纠正。

#### 2.9.3.2 措施

1) 公司制定管理人员违纪违规处理等相关规定，并对重要控制制度和强制性规范进行宣贯。

2) 公司对发现的违规行为及时进行制止，并按公司的有关规章制度要求进行处理。

3) 相关职能部门对本职能领域内出现的重大违规事项的发生与处理情况进行警示教育。

#### 2.9.3.3 文档性记录

对员工违规的处罚材料等。

### 2.9.4 道德标准的遵从

#### 2.9.4.1 内控关注要点

人力资源政策与相应的道德标准一致，对职业道德规范的遵从是员工评价的一项标准。

#### 2.9.4.2 措施

公司人事部门定期对相关人力资源政策进行全面的检查，评价政策是否与公司职业道德规范相符，并据此对人力资源政策进行修订。

#### 2.9.4.3 文档性记录

人力资源政策。

### 2.9.5 核查候选人的背景

#### 2.9.5.1 内控关注要点

核查候选人的背景，特别要考虑公司不能接受的行为或活动，具体包括：

- 1) 对频繁更换工作和职业背景相差很大的候选人要仔细核查。
- 2) 雇佣政策要包括对犯罪记录的调查。

#### 2.9.5.2 措施

公司以档案材料审查作为核查候选人背景的主要举措。公司制定《中国石油天然气股份有限公司干部人事档案管理暂行办法》，确保员工档案资料的管理和使用规范、安全。公司在选拔任用或招聘处室干部以及关键岗位的人员时，通过核查人事档案、单位鉴定等方式对其政治素质、技能资格水平等多方面进行考察，并形成专门材料。对频繁更换工作和职业背景相差很大的候选人，进行仔细核查。

#### 2.9.5.3 文档性记录

人事档案。

## 2.10 员工胜任能力

### 2.10.1 岗位职责描述

#### 2.10.1.1 内控关注要点

管理层应当以正式或非正式的岗位描述，或其他方式分析并定义各岗位的具体工作任务，考虑员工在履行工作时运用判断的程度和对该工作的相应监督程度。

#### 2.10.1.2 措施

公司通过开展“五定”工作，对各岗位的岗位职责进行规范，形成较为全面的“岗位规范”文本，并以此作为各岗位履行职责和行使职权的依据。在此基础上，根据内部控制建设需要，公司制定《关于进一步规范员工岗位职责描述的通知》，对员工岗位职责描述的形式和涵盖要素内容等进行进一步规范。

#### 2.10.1.3 文档性记录

- 1) 员工岗位职责描述。
- 2) 岗位规范。

## 2.10.2 分析胜任工作所需要的知识和技能

### 2.10.2.1 内控关注要点

管理层应分析并确定员工胜任工作所需的基本知识和技能，并有证据表明员工具备工作所需的基本知识和技能。

### 2.10.2.2 措施

1) 针对公司管理的实际需要和现实状况，公司通过“员工岗位职责描述”明确对各岗位所需能力和知识的基本要求，如学历、专业技术职务、任职资格、专业背景、工作经验（经历）和操作水平等基本任职条件要求。

2) 公司通过对员工实施考核评价，找出员工素质与任职岗位的差距，并进行业务、技能培训等，及时提高员工的能力和水平。

3) 公司按照不同的岗位要求，组织员工进行岗位培训，并随公司经营战略、运作方式的变化与发展，适时进行适应性岗位培训。

### 2.10.2.3 文档性记录

- 1) 员工岗位职责描述。
- 2) 培训计划和记录等。

## 2.11 反舞弊机制

### 2.11.1 内控关注要点

1) 管理层有效地设计、实施公司反舞弊程序和控制，针对规避财务报告内部控制的行为和其他欺诈行为，采取适当的措施。

2) 董事会及下属委员会监督公司反舞弊程序和控制。

3) 建立并推行道德准则。

4) 建立道德热线 / 检举揭发机制。

5) 雇佣和晋升时进行背景调查。

6) 建立舞弊调查程序并实施恰当的补救措施。

7) 进行舞弊风险分析。

8) 为减少已识别的舞弊风险应该设计并实施有效的控制活动。

9) 对反舞弊相关信息进行收集和分享并适当培训。

10) 管理层对反舞弊程序和控制的质量持续监控和定期评估。

### 2.11.2 措施

1) 公司审计部与监察部建立联合反舞弊工作机制。

(1) 反舞弊工作协调配合的组织形式。

按照《关于建立股份公司反舞弊协调小组和舞弊风险评估小组的通知》、《关于调整股份公司反舞弊协调小组和舞弊风险评估小组的通知》，公司成立由审计、纪检监察、内部控制有关人员组成的反舞弊协调小组，负责组织协调审计、监察等部门的反舞弊工作，以加强反舞弊审计、监察中的协调与配合。股份公司反舞弊协调小组领导由审计部、监察部和内部控制部领导担任，地区公司反舞弊协调小组由分管领导牵头。

(2) 受理舞弊举报工作程序。

公司设立信访举报机制，由监察部负责受理在会计、财务控制或审计等方面的违规和舞弊行为的举报，并进行相应的调查。

对于在会计、财务控制或审计等方面的违规和舞弊行为的举报，公司根据不同情况做出相应处理：属一般性问题的，由审计部进行反舞弊审计；属重大问题或涉及公司高级管理人员的，由监察部与审



计部及时沟通，研究调查处理办法，报主管领导同意后，组成联合调查组进行反舞弊审计与调查；对缺乏具体线索和内容的，分析潜在的违纪或舞弊风险，并由审计部在反舞弊审计中加以关注。

### （3）反舞弊审计调查结果的处理程序。

反舞弊审计与调查结束后，对已构成违纪但情节轻微且未给公司造成损失的，由审计部或监察部对违纪单位和人员进行批评教育或给予通报批评，需要组织处理的，由人事部门组织处理；对已构成违规违纪且情节较重或给公司造成重大经济损失的，移交监察部追究有关单位和人员的纪律责任；对触犯法律构成犯罪的，由监察部移交司法机关处理。

#### 2) 公司建立反舞弊情况通报制度。

按照《关于建立股份公司反舞弊协调小组和舞弊风险评估小组的通知》、《关于调整股份公司反舞弊协调小组和舞弊风险评估小组的通知》和《中国石油天然气股份有限公司审计部与监察部在反舞弊工作中加强协调配合的组织形式与工作程序》，股份公司反舞弊协调小组定期召开反舞弊情况通报会，通报反舞弊工作情况，确定向审计委员会汇报反舞弊有关情况，研究反舞弊工作中出现的新情况、新问题，研究部署反舞弊工作；根据舞弊风险发生的可能性和重要性水平，提出加强和改进公司内部控制的建议。反舞弊情况通报会原则上每个季度召开一次，遇有重要情况或重大问题时，随时召开，并向管理层和审计委员会汇报。地区公司反舞弊协调小组向股份公司反舞弊协调小组报告情况。

按照《审计委员会工作章程》，审计委员会定期听取审计部有关反舞弊方面的情况汇报，监督员工对有关会计、内部控制、审计事项或舞弊方面的举报和投诉。

#### 3) 进行舞弊风险分析。

公司制定《中国石油天然气股份有限公司舞弊风险评估办法》，公司舞弊风险评估小组是舞弊风险分析评估的组织领导机构；各地区公司、科研院所舞弊风险评估小组或反舞弊协调小组负责本单位的舞弊风险分析与评估工作。

公司监察部每半年汇总审计、监察部门查证属实的舞弊问题，向舞弊风险评估小组报告，并提交舞弊问题分析报告；地区公司发现的舞弊风险，经本单位风险评估小组评估和反舞弊协调小组确认后，报公司舞弊风险评估小组办公室。

舞弊风险评估小组根据舞弊问题实际发生情况和分析报告，以现有的业务循环中风险数据库为基础，结合案例分析，对该舞弊情形进行描述，分析其易发生的领域，评估其发生的可能性和重要性水平，确定相对应的流程和控制，并形成舞弊风险评估报告，提交反舞弊协调小组和公司管理层。

舞弊风险评估报告经公司反舞弊协调小组和管理层同意后，由监察部根据舞弊风险评估报告的内容，对舞弊风险数据库进行相应调整。

#### 4) 建立反舞弊数据库。

公司根据《中国石油天然气股份有限公司舞弊风险数据库管理规定》，由审计部、监察部、内部控制部共同建立了《股份公司舞弊风险数据库》，主要记录公司潜在的舞弊风险和发生的舞弊问题。

总部机关其他部门、专业公司的领导和相关人员，地区公司领导及纪检监察、审计、内控、财务、人事等部门领导和相关人员具有查询数据库舞弊风险的权限。

数据库管理员每半年对舞弊风险、舞弊问题等有关情况进行分析、汇总，提交公司舞弊风险评估小组进行评估。

舞弊风险数据库舞弊风险部分每年更新一次，舞弊问题部分待公司舞弊风险评估小组确认后随时更新。

#### 5) 对最高管理层的监督。

监事会按照《公司法》及《中国石油天然气股份有限公司监事会组织和议事规则》、《中国石油天然气股份有限公司章程》，对公司高级管理人员执行公司职务的行为进行监督，向股东大会独立报告公司高级管理人员的诚信及勤勉尽责表现。

#### 6) 其他方面。

公司建立并推行分别针对高级管理人员和全体员工的职业道德规范，并对遵守情况进行监督。具体内容参见第1·2节。

公司制定内部审计规范——舞弊审计，对舞弊审计的对象、依据、程序、方式、方法和要求等进行规范。公司组织与反舞弊工作相关的培训，安排信访管理与初核、案件检查、内部控制与反舞弊等方面的课程。

#### 7) 反舞弊自评工具——反舞弊程序和控制评价表。

反舞弊程序和控制评价表包括要素、标准、最佳实践、执行情况、跟进措施、责任部门等6方面内容。具体自评内容是从框架五要素控制环境、风险分析、控制活动、信息与沟通、监督展开的18项内容评估审计部、监察部、董秘局、企业文化部、财务部、信息管理部、人事部及内部控制部等部门各自承担的反舞弊工作完成情况。

### 2.11.3 文档性记录

- 1) 投诉报告。
- 2) 解决投诉的程序。
- 3) 对事件报告的记录。
- 4) 反舞弊数据库。

## 3 风险评估

### 3.1 概述

#### 3.1.1 风险

##### 3.1.1.1 概念

风险是指未来的不确定性对公司实现其目标的影响，所有公司，无论规模、结构和行业性质，都面临着诸多来自内部和外部的风险，影响公司既定目标的实现。

##### 3.1.1.2 风险的类型

公司面临的风险可以分为公司层面风险和业务活动层面风险。

1) 公司层面风险。

导致公司层面风险的因素包括外部和内部两个方面。

(1) 外部因素主要体现在：

- ①技术发展——影响研发的性质和时机；
- ②不断变化的客户需求和期望——影响产品开发和定价；
- ③竞争——影响营销和服务活动；
- ④新的法律和法规——影响经营政策和策略；
- ⑤自然灾害——可能造成损失；
- ⑥经济形势的变化等——影响融资、资本支出和扩张决策。

(2) 内部因素主要体现在：

- ①信息系统运行的中断——影响经营运转；
- ②员工的素质以及培训、激励方法——影响控制理念；
- ③管理层职责的改变——影响某些实施控制的方式；
- ④公司经营活动的性质、员工对资产的接触途径——产生挪用；
- ⑤董事会或审计委员会无法有效履行其职责——可能为管理层轻率的行为提供机会。

2) 业务活动层面风险。

业务活动层面风险是指与公司的主要生产经营活动及管理职能有关的风险，包括采购、生产、市场营销、销售、技术开发以及研发、人力资源管理、财务管理等业务和管理活动中存在的风险。

#### 3.1.2 风险评估

##### 3.1.2.1 概念

风险评估是识别及分析影响公司目标实现的因素的过程，是风险管理的基础。在风险评估中，既要识别和分析对实现目标具有阻碍作用的风险，也要发现对实现目标具有积极影响的机遇。

##### 3.1.2.2 风险评估的范围

公司针对战略目标、经营目标、报告目标、合规性目标，分别确认风险评估的范围。目前主要是针对财务报告目标开展了风险评估工作，在以后的体系建设中，将逐步针对战略目标、经营目标、报告目标和合规性目标，按照全面风险管理的要求，开展公司风险评估工作。

##### 3.1.2.3 风险评估的基本程序

1) 信息收集。

围绕公司战略目标和相关目标以及风险管理要求，相关职能部门、业务单位和内控管理部门广泛、持续收集与公司风险及风险管理相关的内部、外部各种信息，包括收集历史数据和未来信息，关注宏观经济与经营环境、竞争对手、新技术与新产品、海外经营、公司重组、业务整合、会计政策、信息系统、资本运作等方面已经发生和将要发生的变化情况。公司对收集的数据、信息和变化情况进行必要的筛选、提炼、对比、分类、组合，形成与公司风险管理相关的信息资料库并不断更新，以便进行风险评估。

公司制定《风险评估规范》，明确收集风险管理信息的具体要求，包括收集战略风险、经营风险、报告风险和合规性风险等方面与公司风险和风险管理相关的内、外部各种信息。

公司目前尚未建立针对风险评估的信息收集机制，将在以后的内控体系建设中，对风险评估规范进行修订，明确规定风险评估信息收集的具体要求，建立风险评估信息收集机制。

## 2) 风险识别。

风险识别是指查找公司各项重要经营管理活动及其重要业务流程中存在的的影响目标实现的风险和机遇的过程。公司分别从公司层面、业务活动层面，动态识别影响公司战略目标及相关目标实现的、内部和外部的各种不确定性因素。带负面影响的因素代表风险，需要对其分析和应对；带积极影响的因素代表机遇，在制定目标和政策实施过程中对其加以考虑并把握。

(1) 公司层面风险识别。公司从战略发展的角度，识别公司层面面临的所有重大的不利因素和有利因素，从而识别风险，发现机遇。这些因素来自外部和内部两个方面，外部因素主要包括政治因素、经济因素、社会因素、自然环境因素等；内部因素主要包括基础设施因素、员工因素、流程因素和技术因素等。

(2) 业务活动层面风险识别。公司制定业务流程描述规范，建立流程目录并用流程图对所有业务进行直观描述。在业务流程描述的基础上，以业务流程步骤为主线，全面识别影响目标实现的相关因素。目前，在风险识别方面，暂未考虑有关公司发展机遇的问题，在以后的内控体系建设中，将关注公司发展机遇。

## 3) 风险评价。

风险评价是评估风险对公司实现目标的影响程度和风险发生可能性的过程。公司针对固有风险和残存风险，运用定性和定量的方法，对公司层面和业务活动层面风险发生的可能性和影响程度进行分析、评价，并按照风险排序标准和方法，确定风险重要性水平，识别公司重大风险，确定风险管理的优先顺序。

公司制定《风险评估规范》，明确风险评估的定性与定量的具体方法。如定性方法包括问卷调查、集体讨论、专家咨询、情景分析、政策分析、行业标杆比较、管理层访谈、由专人主持的工作访谈和调查研究等，定量方法包括统计推论、计算机模拟、失效模式与影响分析、事件树分析等；明确规定风险定量评估时，应当统一风险度量 and 度量模型；明确规定运用风险坐标图对多项风险进行比较，确定风险排序的方法。

识别风险后，需要采用定量或定性的方法对风险进行分析，分析的内容主要有：

- (1) 分析风险发生的可能性（或频率、概率）；
- (2) 分析风险可能产生的影响；
- (3) 确定风险的重要性水平。

目前，确定风险的重要性水平主要是以定性分析为主、定量分析为辅，公司将在以后的内控体系建设中，完善定量分析的方法，逐步建立起定性定量相结合的风险分析方法。

## 4) 风险反应。

风险反应是公司针对风险发生的原因、风险重要性水平，考虑风险之间的关系并把握机遇，运用风险组合观，选择风险反应方案的过程。风险反应方案包括回避风险、减少风险、分担风险、接受风险。

在评估了相关风险之后，管理层确定如何应对风险，制定风险反应方案。

风险反应方案包括以下几种：

- (1) 回避风险——退出产生风险的各种活动；
- (2) 减少风险——采取行动减少风险的可能性或影响；
- (3) 分担风险——通过将风险转移或者分担部分风险来减少风险的可能性和影响；
- (4) 接受风险——不采取任何行动去影响风险的可能性或影响。

在考虑做出风险反应的过程中，管理层需要评估风险反应对风险可能性和影响的效应以及成本和收益，并选择一种风险反应方案。

公司制定《风险管理规范》（试行），对不同类别的风险的反应策略作出规定。一般情况下，对于战略、经营、报告、合规性等风险，可采取回避风险、减少风险、接受风险等方法。对于能够通过保险、期货、对冲等手段减少风险的，可以采用风险转移等方法；明确要求按照风险管理的优选顺序，合理安排风险管理资金预算和其他风险管理资源。

## 3.2 建立风险评估机制

### 3.2.1 内控关注要点

公司的风险评估程序应该从公司层面和业务活动层面两个角度识别风险，并分析其相关影响。风险评估程序还应该考虑会影响目标实现的内部因素和外部因素，对这些风险因素进行分析，从而为风险管理提供依据。

- 1) 识别外部风险的机制是否健全；

- 2) 识别内部风险的机制是否健全;
- 3) 为业务活动层面的每一个重要目标识别相关的重要风险;
- 4) 风险分析程序的全面性和相关性, 包括: 分析风险发生的可能性(或频率、概率)、分析风险可能产生的影响、确定风险的重要性水平, 并决定应采取的行动;
- 5) 存在一种可以预见、识别并对影响公司目标实现的事件或活动发生反应的机制;
- 6) 存在一种识别和处理那些对公司有巨大深远影响的、应该引起管理层关注变革的机制。

### 3.2.2 措施

公司制定《风险管理规范》(试行)、《风险评估规范》, 对风险管理的机构及职责、风险管理的原则及要素、风险评估的程序和方法、控制设计的程序和方法进行明确的规定; 明确规定公司开展持续性风险评估工作。

公司定期或当发生以下情况之一时, 及时组织进行风险评估: 内部控制体系建立时; 新产品开发时; 新业务介入时; 新系统应用时; 内控政策和目标修改时; 业务流程发生较大变化时; 组织机构变革时; 法律法规、监管要求发生变化时; 经济周期性波动时; 行业发生变革时; 同业发生新的案例时; 其他认为需要时。同时针对风险评估的结果组织相关部门制定风险反应方案。

#### 3.2.2.1 公司层面风险评估措施

##### 1) 公司层面风险的识别。

##### (1) 从外部专家处获得公司层面风险的意见。

公司管理层从法律顾问、外部审计师等方面获得有关公司层面风险的意见, 分析后在年报中予以披露。公司已经识别并在年报中披露的公司层面风险主要包括:

- ①汇率风险;
- ②商品价格风险;
- ③行业风险;
- ④原油储备下降风险;
- ⑤灾害风险;
- ⑥大股东控制公司经营政策风险;
- ⑦同行业竞争风险;
- ⑧资金风险;
- ⑨法律风险。

##### (2) 相关管理部门识别公司层面风险。

公司在管理过程中采取一定措施来识别影响公司目标实现的公司层面风险, 并针对这些风险制定相应的控制措施。

在公司制定发展规划过程中, 公司的规划部门对公司所处的内外部环境进行分析, 从而识别可能存在的风险。

##### ①外部环境分析。

a.宏观环境分析: 如对政治的、经济的、社会的、法律的、技术的因素进行分析, 识别这些因素中影响战略目标实现的风险。

b.行业分析: 对所在行业的特性、产品发展方向及市场走向进行广泛的行业研究, 探索所在行业对手过去成功的或失败的案例, 确定最有影响力的行业因素, 评估行业竞争程度, 确定公司在本行业的战略方向, 分析对手动向, 评估对本行业带来的影响。对行业的这些因素进行分析后, 识别这些因素中影响战略目标实现的风险。

c.竞争态势分析: 对公司的直接竞争者、供应商、购买者、替代品、潜在进入者进行分析, 识别这些竞争性因素中影响战略目标实现的风险。

d.对公司所处的市场环境和客户进行分析, 识别市场环境以及客户中存在的风险因素。

##### ②控制环境分析。

对外部环境进行分析的同时, 公司也对自身的资源和能力进行分析, 分析公司资源和能力的现状是否能够支撑公司战略目标的实现, 分析的内容包括:

a.公司是否有足够的人力资源, 如关键管理人员、技术人员等是否能够满足实现战略目标的需要, 是否存在人力资源不足的风险;

b.公司是否有足够的财务资源，如是否有充足的现金流、一定的融资能力等来满足实现战略目标的需要，是否存在财务资源不足的风险；

c.公司在无形资源，如品牌商誉、技术资源等方面是否能够满足实现战略目标的需要，是否存在无形资源不足的风险；

d.公司的各项管理能力，如营销、生产、技术开发的能力等方面是否能够满足实现战略目标的需要，是否存在管理能力不足的风险。

(3) 其他风险识别方法。

公司管理层通过检查业务、参加行业联合会、利用顾问和其他专业人员获取特定信息；公司逐步加强与国内外大石油公司、知名咨询机构的沟通，获取更多、更全面的信息，从而更全面、更准确地识别公司层面风险，进而采取合理的应对措施。

2) 对公司层面风险进行分析。

内部控制部组织开展风险评估工作，对已经识别的风险采用定性的方法进行风险分析，分析风险发生的可能性（或频率、概率）以及风险可能产生的影响，确定风险的重要性水平。

3) 制定风险反应方案。

相关业务部门针对识别的风险，制定风险反应方案。对不同的风险，确定是采用规避风险、减少风险、分担风险的风险反应方案，还是接受风险。

### 3.2.2.2 业务活动层面风险评估措施

对于业务活动层面风险评估，公司目前只对影响财务报告目标实现的风险（财务报告错报、资产安全受到威胁和舞弊）进行风险评估，具体有以下措施。

1) 确定重要会计科目和披露事项。

根据美国上市公司会计监管委员会（以下简称“PCAOB”）颁布了审计准则第5号——“与财务报表审计相结合的财务报告内部控制审计以及相关的独立性规定和一致性修正案”（以下简称“PCAOB 审计准则”）的要求，管理层在每年对股份公司财务报告的内部控制体系进行评价并向美国证监会报告的过程中，需要首先确定与股份公司国际会计准则财务报告相关的重要会计科目和披露事项，以及这些重要会计科目和披露事项可能出现重大错报的原因及相关财务报表认定，并以此为基础进一步确定与重要会计科目和披露事项相对应的业务流程，即重要业务流程，作为设计相关财务报告的内部控制体系的基础和依据。

每年3月份，根据股份公司上一年度国际会计准则的合并财务报告及相关附表，初步确定当年重要会计科目和披露事项，并以此为基础确认重要业务流程。对于当年可能发生的重大业务变化，如进行的重大收购、兼并活动，重大的项目投产等，内部控制部在年底财务报告生成以后，根据年度财务报告的相关数据对初步确认的重要会计科目和披露事项进行更新，确保重要会计科目和披露事项的完整性。

2) 确定重要业务流程。

公司以财务报告为切入点对业务进行梳理，确定公司治理、管理结构、发展规划、经营计划等三十三类业务为内部控制体系建设涉及的主要业务，基本涵盖了公司各个方面的经营管理活动；并以此制定通用流程目录，下发各地区公司。各地区公司在保证一级、二级、三级流程基本不变的基础上，结合本单位的具体业务进行修改和完善。

内部控制部在确定重要会计科目和披露事项的基础上进一步确定与重要会计科目和披露事项相对应的业务流程，即重要业务流程。

为了形成公司统一的流程描述文本，公司制定“流程描述规范”，对流程描述进行规范和统一。

公司每年在进行重要会计科目和披露事项确认的同时，对重要业务流程进行更新确认。

3) 财务报表认定。

在完成重要会计科目和披露事项的确认及其与业务流程的对应后，股份公司应确认和记录相关的财务报表认定，并测试与这些财务报表认定有关的内部控制。相关的认定是那些对于会计科目是否得到公允反映起着决定性意义的认定。只有满足了重要会计科目财务报表认定，才能保证财务报告内部控制的有效性。财务报表认定是管理层进行风险评估进而确保财务报告内部控制体系设计有效的基础。因此，必须对重要会计科目的财务报表认定进行确认和记录。

财务报表认定包括存在与发生、完整性、估价与分摊、权利与义务、表达与披露五个方面。

内部控制部除在内部控制体系建设阶段开展此项工作外，以后年度将在每年3月份开展一次财务报表认定工作，为每年进行的财务报告内部控制体系的更新维护做好准备。

4) 对业务流程进行风险评估。

(1) 信息收集。

(2) 风险识别。

根据公司实际，内部控制部采用多种方法对业务流程中影响财务报告目标实现的风险进行识别。

（3）风险评价。

内部控制部组织开展风险评估工作，对已经识别的风险采用定性或定量的方法进行风险分析，分析风险发生的可能性（或频率、概率）和风险可能产生的影响，并确定风险的重要性水平。

（4）建立风险数据库。

公司按照规定的程序和方法，开展公司层面风险和业务活动层面风险评估后，结合风险因素、重要性水平和风险反应方案，编制与维护公司层面风险数据库和业务活动层面风险数据库，将识别的风险形成风险数据库，并根据公司经营环境的发展变化，对风险数据库进行不断地更新与维护。

### 3.2.3 文档性记录

- 1) 公司中长期发展规划；
- 2) 风险数据库；
- 3) 通用业务流程目录；
- 4) 重要业务流程目录。

## 3.3 建立并完善风险管理体系

公司建立风险管理组织架构，形成包括明确风险管理的职责划分，建立并不断完善风险管理制度、风险评估方法和工具，以及风险报告系统的组织体系。

内控部门负责受理公司内部及外部关于改进风险管理的建议和意见，监督并定期评估风险管理体系的运行情况，并根据评估结果及时做出相应整改。评估内容主要包括以下事项：

- （1）风险管理系统是否达到预期效果；
- （2）风险管理程序是否合理；
- （3）风险信息及其采集方法是否有效；
- （4）是否有新的风险管理知识、技术、方法产生。

## 4 控制活动

### 4.1 概述

#### 4.1.1 概念

控制活动是确保管理层关于风险应对方案得以贯彻执行的政策和程序。控制活动存在于公司所有级别的分支机构和职能部门，包括授权、批准、查证、核对、报告、内部审计、重大风险预警、经营业绩评价和资产保全措施等活动。

#### 4.1.2 控制活动的分类

控制活动按照不同的分类标准可以划分为不同的类型。

##### 4.1.2.1 按控制活动的目标分类

按控制活动的目标可以分为以下几类：

- 1) 战略目标控制活动：指能够满足战略目标实现的控制活动。
- 2) 经营目标控制活动：指能够满足经营活动效率与效果目标的控制活动。
- 3) 报告目标控制活动：指能够满足报告目标的控制活动。
- 4) 合规性目标控制活动：指能够满足合规性目标的控制活动。

##### 4.1.2.2 按控制活动的内容分类

按控制活动的内容划分，控制活动可分为公司层面控制和业务活动层面控制。

###### 1) 公司层面控制。

公司层面控制是管理层确保在公司内部各个领域获得适当、有效控制的重要机制。主要包括：

(1) 控制环境范围内的内部控制，包括道德准则的建立与推行、高层管理者基调、检举揭发机制、权限和职责分工、审计委员会、IT 环境与组织以及人力资源政策等；

- (2) 反舞弊程序与控制；
- (3) 风险评估流程；
- (4) 集中化的处理和程序；
- (5) 监督，包括持续监督、独立评估和缺陷报告；
- (6) 经营活动分析、审核；
- (7) 期末财务报告流程；
- (8) 统一的规章制度。

###### 2) 业务活动层面控制。

业务活动层面控制是指直接作用于公司生产经营业务活动的具体控制，亦称业务控制，如业务处理程序中的批准与授权、审核与复核，以及为保证资产安全而采用的限制接近等控制。

##### 4.1.2.3 按控制活动的作用分类

按控制活动的作用划分，控制活动可分为预防性控制和发现性控制。

###### 1) 预防性控制。

预防性控制是指为防止错误和非法行为的发生，或尽量减少其发生机会所进行的一种控制。

###### 2) 发现性控制。

发现性控制是指为及时查明已发生的错误和非法行为，或增强发现错误和非法行为机会的能力所进行的各项控制。

##### 4.1.2.4 按控制活动的手段分类

按控制活动的手段划分，控制活动可分为人工控制和自动控制。

###### 1) 人工控制。

人工控制是以人工方式执行的控制。

###### 2) 自动控制。

自动控制是由计算机等系统自动执行的控制。

### 4.2 控制活动的实施



#### 4.2.1 内控关注要点

- 1) 针对公司的每一项业务活动都有必要和恰当的政策和程序。
- 2) 已确定的控制行为得到恰当的执行。

#### 4.2.2 措施

公司制定风险管理制度，明确规定公司通过法定程序指导和监督全资及控股子公司建立和实施内部控制体系；明确规定控制活动（措施）外包的原则性规定，应注重成本与收益的平衡、外包工作的质量、自身商业秘密的保护以及防止自身对控制活动（措施）外包产生依赖性风险等。

4.2.2.1 针对公司层面风险，按照风险反应方案，建立相应的公司层面风险控制政策，制定公司统一的规章制度，统驭业务活动层面控制。

公司应根据风险管理策略，针对各类风险或每一项重大风险制定相关的规章制度、控制政策和控制措施，确保风险控制在风险承受度的范围内。

公司针对风险建立的规章制度、控制政策和控制措施，要满足合规的要求，坚持经营战略与风险策略一致、风险控制与运营效率及效果相平衡的原则，针对重大风险所涉及的各管理及业务流程，制定涵盖各个环节的全流程控制措施；对其他风险所涉及的业务流程，要把关键环节作为控制点，采取相应的控制措施。

公司应当按照各有关部门和业务单位的职责分工，组织实施控制措施。

公司应定期总结分析风险反应方案、控制措施的有效性和合理性，结合实际不断修订和完善。

公司针对各项生产经营活动，制定采购、生产、销售、服务等业务活动方面的管理规程；针对各项管理活动，制定财务、人事、行政、质量安全环保、监察、审计、法律事务、资本运营等管理活动方面的管理规程。此外，公司还对某些业务活动制定操作规程，如财务部制定的《中国石油会计手册》，明确规定会计政策、会计科目、主要业务会计核算、内部购销往来核对及结账、财务会计报告等与会计核算有关的政策和程序以及会计政策。地区公司普遍建立QHSE管理体系，从加强制度建设入手，针对管理上的漏洞和死角，及时建立和完善相关规章制度，用制度规范各项管理工作。按照“集约化经营、专业化管理”的思路，进一步完善管理体制和工作机制，理顺工作程序，明确工作职责和标准。在生产、现场、安全以及定额、计量、标准化、信息管理等方面，加大工作力度，提高管理水平，有效规范各项管理。

4.2.2.2 针对业务活动层面风险，以公司层面控制政策为导向，规范业务流程，制定业务活动层面风险控制措施。

（1）控制现状描述与分析。制定风险控制文档编制规范和模板，对业务流程进行风险控制分析，编制风险控制文档（RCD），对控制的合理性、完整性进行分析。

公司通过建立风险控制文档进行差异分析，查找现有控制的差距和不足，然后补充和完善现有控制措施，以达到防范风险的目的；同时，为进一步补充、修订制度提供依据。

风险控制文档（RCD）用于确认、记录每个流程及每个步骤中存在的风险和已建立的控制，并与相应的制度和控制实施证据相对应。风险控制文档的控制重点强调：与财务会计报表和附注的真实性、准确性有关的控制，防止舞弊、欺诈行为的控制以及资产安全的控制。

具体的执行步骤是：

- 1) 建立风险控制文档编制规范。

为了统一和规范风险控制文档的编制，公司制定“风险控制文档编制规范”，明确风险控制文档中各项目的描述要求。

- 2) 建立业务流程的风险控制文档。

内控部门组织相关部门对业务流程上的风险和控制进行描述，形成风险控制文档，并由有关业务主管部门的相关人员确认，以保证风险控制文档中描述的内容能够反映实际业务执行情况。

- 3) 分析查找差距，补充和完善现有控制措施。

内控部门组织相关部门对风险控制文档进行分析，查找现有控制措施的缺失和不足，由相关部门进行整改，并补充、修订相关制度。

（2）规范、统一业务流程。根据风险控制分析结果，补充、完善相关控制，规范、统一流程步骤、控制规范和记录表单，建立规范、统一的业务流程，在以后的内控体系建设中，将逐步建立起涵盖各主要业务领域的规范、统一的业务流程。

（3）建立关键控制。建立完善的关键控制确认方法，确定所有业务流程的关键控制并建立关键控制管理文件。

关键控制，是在相关流程中影响力和控制力相对较强的一项或多项控制，其控制作用是必不可少和不可替代的。如果缺少该项控制，将在很大程度上直接导致财务风险的产生。

公司确认关键控制的目的是：将确认的关键控制作为控制活动的重点，对其实行全面、严格的管理，以防范重要风险。关键控制也为公司管理层测试内部控制体系的完整性和有效性提供统一的范围和标准；同时将其作为公司提供的内部测试基础性资料，以满足外部审计师评估、测试公司内部控制体系的完整性和有效性。

确认关键控制的步骤为：

1) 在确认重要风险和关键控制目标的基础上确认关键控制。

公司成立工作小组，在开展风险控制分析并编写风险控制文档（RCD）的基础上，寻找影响公司目标实现的重要风险，并针对这些重要风险，确认关键控制。

2) 建立“关键控制文档”。

在确认关键控制的基础上，建立“关键控制文档”。

3) 关键控制的审定、审批和执行。

组织公司相关部门的负责人、地区公司的总会计师、外部内控专家对初步确认的关键控制进行审定，最终确认公司的关键控制，报公司内控体系建设委员会审批后执行。

(4) 强化自动控制。通过实施信息系统自动控制，固化流程操作程序，提高控制执行效率和效果。

#### 4.2.2.3 财务会计报告流程。

建立健全财务会计报告流程，完善财务会计报告相关制度。主要包括以下几方面的内容：

1) 编制财务会计报告的前期工作；

2) 地区公司财务会计报告流程；

3) 股份公司财务会计报告流程；

4) 财务会计报告复核；

5) 财务会计报告对外披露及考评。

#### 4.2.2.4 建立并实施经营管理活动分析评价制度。

各级管理层开展经营管理活动分析，对经营管理情况实施审核和监督。

公司制定了《财务分析管理规定》，明确了财务分析的职责、内容、具体方法和程序。财务分析的内容包括：损益类指标分析、资产负债类指标分析、现金流量指标分析。在财务分析的方法上，采用因素分析法、比较分析法等，重点对财务报表中影响利润指标的价格因素、销量因素、成本因素及其他费用的变化进行分析；同时通过财务分析对财务报表的真实性进行核实。

#### 4.2.3 文档性记录

文档性记录包括以下内容：

1) 财务分析报告；

2) 财务会计报告流程；

3) 风险控制文档（RCD）编制规范；

4) 风险控制文档；

5) 关键控制文档。

## 5 信息与沟通

### 5.1 概述

#### 5.1.1 概念

信息与沟通是公司经营管理所需的信息被识别、获得并以一定形式及时地传递，以便员工履行职责。信息不仅包括内部产生的信息，还包括与公司经营决策和对外报告相关的外部信息。畅通的沟通渠道和机制使员工能及时取得他们在执行、管理和控制公司经营过程中所需的信息。公司建立符合发展战略并与经营管理活动一体化的信息系统，为风险管理提供足够的信息资源和顺畅的沟通渠道。

#### 5.1.2 要素

##### 5.1.2.1 信息资源收集

这里所说的信息是指来源于公司外部及内部，与公司经营相关的财务及非财务信息。公司持续不断地识别、收集、整理与归纳来自内部与外部、经营与管理的各种信息。针对不同的信息来源和信息类型，明确各种信息的收集人员、收集方式、传递程序、报告途径和加工与处理要求，确保经营管理各种信息资源得到及时、准确、完整收集。

按信息来源不同，可将公司内部控制重点关注的信息分为内部信息和外部信息。

1) 内部信息主要包括：财务信息、经营信息、规章制度信息、综合信息等。主要获取渠道有：机关职能部门的调研报告；财务会计报告；信息员搜集、反映的情况；群众来信来访、员工直接向上级沟通的信息；内部刊物、资料；公司局域网；各种会议提案、记录、纪要等。

2) 外部信息主要包括：国家法律法规，国内外监管机构信息，以及客户、供应商、竞争对手的信息等。获取渠道主要有：国家部委和外部监管方的文件；期刊杂志；中介机构；互联网；广播、电视；公司采购及销售部门收集的市场和价格信息；驻外办事处提供的信息；外部来信来访；参加行业会议、座谈交流等多种渠道。

##### 5.1.2.2 信息沟通渠道

沟通是指信息在公司内部各层次、各部门之间以及公司与客户、供应商、监管者和股东等外部环境之间的传递。

建立有效沟通，公司需要从沟通环境、沟通渠道、沟通方式及沟通反馈多方面进行建设。有效沟通的特点表现为：沟通频率高、方式随意；沟通深入且平等；具有沟通所需的物质条件；完善的沟通制度和系统；全方位的信息共享。

建立横向和纵向相互通畅、贯穿整个公司的信息沟通渠道，确保公司目标、风险策略、风险现状、控制措施、员工职责、经营状况、市场变化等各种信息在公司内部得到有效的传达。

建立适当的渠道，与公司的相关方如供应商、客户、律师、股东、监管机构、外部审计师，就相关信息进行必要的外部沟通。

##### 5.1.2.3 信息披露

信息披露是指公司为确保符合中国证券监督管理委员会、纽约证券交易所、香港联合交易所和美国证券交易委员会的要求以及其他监管要求，向所有市场参与者和监管部门提供及时、有序、一致、准确、完整、可靠和可信的公司信息。

制定完善的信息披露管理制度，明确重大事项的判定标准和报告程序，确定披露事项的收集、汇总和披露程序，符合资本市场监管要求。

##### 5.1.2.4 信息系统总体控制

信息系统总体控制适用于企业在信息技术的开发、实施、运行、维护及管理等方面的控制，它可以更好地保护企业的信息资产，可以提高信息系统对业务的支撑力度，增强企业信息系统的运行效力。信息系统总体控制通常包括控制环境、信息安全、项目建设管理、系统变更管理、信息系统日常运作、最终用户操作等。

##### 5.1.2.5 信息系统应用控制

信息系统应用控制包括应用软件中的电算化步骤以及用以控制不同种类交易处理的相关手工操作程序。这些控制结合在一起，可以保证系统中的财务和其他信息的安全性、完整性、准确性和有效性。

信息系统总体控制和应用控制是相互关联的。信息系统总体控制是应用系统控制的基础，应用系统控制依赖于信息系统总体控制，信息系统总体控制和应用控制共同保证信息处理的完整性和准确性。

制定《风险管理规范》（试行），规定建立企业管理信息系统与风险管理信息系统的统筹规划。

#### 5.1.2.6 流程管理信息系统

目前，公司已启动流程管理信息系统建设，并将在今后的内控体系建设逐步建立起可支持手册信息化管理、业务流程管理、内控测试以及满足全面风险管理要求的流程管理信息系统。实现业务流程语言、设计规范、管理制度、控制措施、流程发布的统一管理，建成满足全面风险管理，具有开放性、可拓展性的流程管理信息系统。

## 5.2 信息

### 5.2.1 内控关注要点

#### 5.2.1.1 获取信息并向管理层报告

1) 公司应该完善获取外部相关信息的机制，以随时掌握有关市场状况、竞争对手的动态、立法或监管的要求以及经营环境的变化等；

2) 对于实现公司目标的重要内部信息应得到确认并定期汇报；各级管理人员能够得到他们履行职责所需要的内、外部信息。

#### 5.2.1.2 及时向适当的人员汇报足够的信息

1) 各级管理人员能够及时得到分析信息以便判断需要采取什么措施；

2) 向不同级别的管理人员汇报详细程度不同的信息；

3) 对信息进行适当的汇总，以满足进一步详查的需要；

4) 及时获取和传递信息，以利于有效监控有关事件和活动，并对经济、行业因素和控制问题进行迅速反应。

#### 5.2.1.3 建立信息技术总体规划

1) 指定专门部门负责识别不断产生的信息需求；

2) 信息的需求和优先次序由具有完全责任的管理层来决定；

3) 订立与战略决策相联系的长期信息技术总体规划。

#### 5.2.1.4 管理层对信息系统的支持态度

为建立或改进信息系统提供足够的、必要的资源（包括但不限于管理人员、分析员、具备必要能力的编程人员）控制措施。

### 5.2.2 措施

#### 5.2.2.1 内部信息收集与传递

1) 内部政策信息收集与传递。

(1) 企业价值观、道德和行为期望。

公司根据《中国石油天然气集团公司企业文化建设纲要》要求，统一企业精神和核心经营管理理念、企业宗旨，并通过广泛深入地宣讲，引导员工践行。

公司制定《中国石油天然气股份有限公司高级管理人员职业道德规范》、《中国石油天然气股份有限公司高级管理人员职业道德建设制度》和《中国石油天然气股份有限公司员工职业道德规范》、《中国石油天然气股份有限公司员工职业道德建设制度》，以公司文件形式下发，并利用网络等形式进行宣传。

公司每年的工作会议有宣讲职业道德的内容，对员工提出遵守职业道德规范的要求。新加入公司的员工要进行公司职业道德规范等内容的岗前培训。

(2) 公司的战略性经营目标。

公司在年度工作会议上提出战略性经营目标，并通过与高级管理人员签订业绩合同的方式将经营目标层层分解。

(3) 财务政策及程序。

公司制定和完善统一的财务、会计、价格、资产和资金等方面的管理制度、办法和工作规范，并宣贯执行。

财务会计政策发生变更时，按权限经过相关人员审批后，一般通过文件形式进行通知（或转发国家部门的文件），并规定文件下发之日起执行或某固定时间执行。

财务会计政策及程序以文件、会计手册形式发布。

(4) 人力资源政策。

公司通过开展“五定”工作和岗位职责描述，对各岗位职责进行了规范，使员工理解自己的职责和工作程序。

公司通过宣贯《中国石油天然气股份有限公司总裁班子年度业绩考核办法》、《中国石油天然气股份有限公司高级管理人员业绩考核办法》、《中国石油天然气股份有限公司中层及以下管理人员业绩考核指导意见》和《中国石油天然气股份有限公司操作服务人员绩效考核指导意见》等制度和实施细则，敦促员工正常履行自己的职责。

2) 其他内部信息的收集与传递。

公司各单位对收集、产生的各种信息进行必要的加工与分析，以满足向各级管理人员提供详细程度不同的有效信息。

(1) 财务信息。

地区公司编制本单位的财务报表，在公司规定的时间内报送财务报表。财务部同期对比进行财务分析，并分总部、四个专业分公司，分别对主要经营指标进行对比分析，报公司领导。

(2) 经营信息。

专业分公司和地区公司按照统计报表的要求，每月（或每周）通过统计信息系统自下而上地提供统计资料，公司规划计划部对主要经营指标进行对比分析，形成月、季、年度生产经营运行监测报告报公司领导，形成简报上报国家有关部委。

(3) 规章制度信息。

规章制度管理部门负责规章制度信息的收集、汇编，并通过规章制度管理信息系统，实现信息共享。

(4) 综合信息。

审计部门搜集内审方面的相关信息，地区公司审计部门向审计部每年上报审计计划和工作总结，每季上报审计工作统计报表。

监察部门搜集信访、违规、舞弊的信息，对于重大、紧急情况要严格执行重大情况报送制度，及时报送公司监察部。

总裁办公室负责公司重要综合管理信息的收集编发，开展专题调研，及时掌握所属公司和机关的工作动态，为领导决策提供信息参考。

其他机关部门、专业分公司负责职权范围内管理信息的收集、编发和制度制定，开展专题调研，及时掌握所属范围内的工作动态。

地区公司按照上级的信息需求及时提供各种所需的信息。

(5) 员工提供的信息。

公司各级纪检监察部门设立举报电话、网上举报中心和电子举报信箱并对外公布，设立专门的举报接待室，在员工比较集中的地方还需设立举报箱，以给员工提供信息举报、不服处分或处理申诉的渠道，并根据实际情况对员工的举报进行保密、保护和奖励。

公司组织开展合理化建议活动，听取员工的合理化建议和意见。

(6) 信息系统产生的信息。

公司信息系统提供相关信息，机关职能部门、专业分公司和地区公司根据各自权限共享这些信息。

#### 5.2.2.2 外部信息的收集与传递

1) 法律法规信息。

机关职能部门、专业分公司和地区公司在各自业务范围内搜集相关法律法规等信息，主要来源有国家部委的文件、期刊杂志、互联网、专业法律信息服务商及中介机构等，并通过公司局域网发布。

国外法规信息发生变化，由公司境外律师、驻外办事处等通过备忘录的形式提供给法律事务部等

有关部门。

2) 政策信息和监管机构信息。

机关职能部门、专业分公司和地区公司搜集国家相关政策、国内外监管机构的各种信息，通过公文形式和公司局域网进行发布。

3) 从客户、供应商、经营伙伴、投资者处获得的信息。

电子商务部、专业分公司和地区公司采购及销售部门通过供需见面会或订货会、谈判、签订合同等形式搜集产品信息、市场需求信息、竞争对手信息等，经分析整理后及时传递至相关部门。

董秘局、财务等部门搜集与证券机构或投资银行等第三方机构在业务往来中和公司相关的信息，经分析整理后及时传递至相关部门。

公司领导通过各种渠道从经营伙伴、投资者处获得的相关信息，以工作例会或外事简报方式进行发布。

### 5.2.2.3 信息报告

1) 例行报告。

各级人员按照公司分级管理的组织结构和岗位职责，定期向上级反映其管辖部门或其所在岗位的工作情况。

机关职能部门向上级请示、报告工作，要先按照公司领导的工作分工向分管领导请示、报告，再根据请示报告类别，按照行政两级（股份公司—地区公司）或业务三级（股份公司—专业分公司—地区公司）管理体制向对口的上级请示、报告。正常情况下不得越级请示、报告工作。

2) 实时报告。

除例行报告外，公司按照《中国石油天然气股份有限公司事故统计报告制度》、《中国石油天然气股份有限公司纪检监察部门信访举报工作规定》、《中国石油天然气股份有限公司事故应急管理规定》、《中国石油天然气股份有限公司事故责任追究暂行规定》、《中国石油天然气股份有限公司监察部门参与事故调查处理的暂行办法》等制度的有关规定，形成重大信息传递的机制。

3) 专题报告。

公司各部门根据业务需要，就某一专题及时向上级领导汇报情况。

4) 综合报告。

公司各部门定期向上级领导全面汇报本部门的工作情况，主要包括工作总结、计划安排等内容。

### 5.2.2.4 信息技术总体规划

公司成立信息技术委员会，主任由总裁担任，副主任由信息工作主管副总裁担任，委员由公司有关领导、总部有关职能部门和专业分公司主管领导担任。信息技术委员会根据公司整体发展战略，组织确定公司信息技术发展总体目标和战略规划。

对于重大信息技术项目，信息技术委员会委托专家小组进行项目技术论证。

### 5.2.3 文档性记录

相关的信息收集、传递文档。

## 5.3 沟 通

### 5.3.1 内控关注要点

#### 5.3.1.1 向员工传达其职责和控制责任的有效性

1) 沟通方式应能实现沟通的目的；

2) 员工应清楚他们的行为要达到的目标，以及他们的工作对于实现这些目标有什么作用；

3) 员工应清楚自己的职责与他人的职责如何相互影响。

#### 5.3.1.2 公司内部是否充分交流

企业内部沟通的充分性，信息的完整性和及时性，以及使人们有效履行职责的信息充足性。

#### 5.3.1.3 沟通渠道应开放有效

公司应存在与所有有关方面的反馈机制，对相关方的建议、投诉和收到的其他情况建立记录并

给予有效处理；必要的信息应向上级汇报并采取相应的跟进措施。

#### 5.3.1.4 外部相关方了解公司职业道德规范的程度

- 1) 与外部的重要信息交流应由相应的管理人员进行；
- 2) 供应商、客户和其他方面应清楚公司在与其往来的活动中，员工应遵循的职业道德规范；
- 3) 在与外部的日常交往中公司强调员工应遵循的职业道德规范；
- 4) 其他公司员工的不良行为应向适当人员汇报。

#### 5.3.1.5 管理层收到外部信息后应采取及时和适当的应对措施

- 1) 公司应善于接受他人就产品、服务或其他方面反映的问题，对此进行调查并采取适当的行动；
- 2) 在与客户交易或事项的财务记录中出现的错误应给予及时的纠正，并且就产生错误的根源进行调查和纠正；
- 3) 应由经授权的当事人以外的人员处理收到的投诉，并采取适当的行为与原始信息提供者进行跟踪和沟通；
- 4) 管理层应清楚投诉的性质以及数量。

### 5.3.2 措施

#### 5.3.2.1 内部沟通

- 1) 明确的职责和有效的控制。

各部门定期组织对本部门员工进行相关岗位培训，使员工清楚其行为要达到的目标及自己的职责与他人的职责如何相互影响。

人事部门根据公司制定的各种业绩考核办法组织对各级人员的业绩考核，并及时将考核结果反馈给被考核人，有效检查各级人员对其职责的理解和有效性控制。

- 2) 内部沟通与交流。

管理层定期向董事会就最新的业绩、发展、风险、重要事件或事故等问题进行汇报。

公司管理层定期或不定期召开各种会议，及时与相关职能部门领导、专业分公司、地区公司负责人就生产、运营等情况进行沟通、交流。

财务部门定期向各部门交流和通报财务状况、经营成果等。

财务部门定期将应收账款情况反馈给销售部门和清欠办公室。

生产企业与销售企业定期沟通。

电子商务部、各专业分公司和地区公司采购部门定期组织与其他业务部门就采购需求、价格信息、采购经验等方面的沟通与交流。

员工除了通过正常的向其直属上级汇报工作的沟通渠道外，还可以通过各种方式与本单位主要领导进行直接沟通。公司各机关职能部门总经理的联系方式公布在通讯录上，员工可以通过电话、邮件、面谈等方式直接进行沟通、交流。

公司员工可以通过书信、电话、走访等形式，向纪检监察部门反映党员、监察对象违反党纪、政纪的问题以及有关意见、建议和要求；同时，公司规定对信访件的处理时限和办结率及查报结果的要求，对信访举报属实，查处后为公司挽回或减少重大损失的，将酌情奖励举报人。

公司组织开展合理化建议活动，鼓励员工对公司管理、生产、研发等方面提出的合理化建议，并对有突出贡献的单位和个人，给予适当的奖励。

#### 5.3.2.2 外部沟通

- 1) 对外职业道德规范的宣传。

公司积极参与社会公益事业，以实际行动宣传公司精神和经营理念，并在国内外影响较大的报刊、杂志上进行公司形象和产品品牌的宣传。

公司通过各种新闻媒体深入报道各单位涌现出来的各种先进事迹、先进人物和先进管理经验，对公司干部、员工爱岗敬业、无私奉献的精神进行宣传报道。

公司销售、采购部门员工在同客户、供应商的日常工作中，向客户、供应商解释公司的道德规范。公司鼓励员工在发现其他公司员工的不良行为时，及时向公司适当人员汇报。

- 2) 与客户沟通。

专业分公司、地区公司销售部门建立客户座谈会制度和客户走访制度，定期与客户进行座谈和走访，听取客户对销售政策的意见和建议，收集客户需求和客户对销售单位的意见，强化售后服务，并



制定相应政策，解决销售工作中存在的问题。

专业分公司、地区公司销售部门通过产品订货会、研讨会，了解客户对产品或服务的设计以及质量方面的要求，并反馈给相关部门。

专业分公司、地区公司设立专职人员处理在销售活动中的商务纠纷。

3) 与供应商沟通。

电子商务部、专业分公司和地区公司采购部门通过供需见面会或订货会、谈判、签订合同等形式与供应商就产品或服务的设计、质量、市场需求等问题进行沟通。

4) 与律师的信息沟通。

法律事务部负责香港、美国及国内公司法律顾问的年度聘用工作，在进行年报起草、信息披露等事项时及时与前述律师进行信息沟通。

公司根据需要，聘请律师参与有关重大项目服务和法律纠纷的处理，并随时与律师沟通处理进展情况。

5) 与股东、监管者、外部审计师的沟通。

公司按照《公司法》的规定召开股东年度会议和股东临时会议，保证股东权益。根据《中国石油天然气股份有限公司章程》和上市地的监管规定依法披露公司信息，通过季度、中期和年度报告等方式，让监管者、股东等外部相关方对公司经营状况更深入的了解。

董秘局负责同监管部门的联系，组织、准备并及时递交监管部门所要求的文件，接受监管部门下达的有关任务并组织完成这些任务。

公司管理层不定期与外部审计师召开会议，商讨界定程序的相关事宜以及传达当前公司所做出的重要决定，以保证项目实施的有效性和高效性以及双方工作的协调性。

审计委员会、审计部门、财务部门、内控部门与外部审计师进行会晤和讨论，听取外部审计师有关财务报告审计、内部控制审计方面的建议。

### 5.3.3 文档性记录

- 1) 员工岗位职责描述；
- 2) 业绩考核文档资料；
- 3) 财务报告；
- 4) 审计意见书；
- 5) 客户调查问卷；
- 6) 会议纪要；
- 7) 公司年报。

## 5.4 信息系统总体控制

### 5.4.1 内控关注要点

#### 5.4.1.1 信息系统控制环境

1) 总体控制环境：控制环境是进行有效内部控制的基础，包括信息技术战略规划的制定和修订、信息技术管理组织结构、员工教育和培训等；

2) 信息与沟通：包括公司信息资产的管理、各项信息技术管理政策、制度和规范的宣贯、执行和维护等；

3) 风险评估：包括公司和业务层面的信息技术风险的识别、评估和风险的防范，并要定期回顾风险评估结果等；

4) 监控：包括公司信息技术活动的定期监督和检查，提出改进建议，采取相应的改进措施等。

#### 5.4.1.2 信息安全

1) 信息安全管理组织：包括信息安全管理机制、员工的信息安全培训以及员工入职签署遵守企业信息安全规定的声明等；

2) 逻辑安全：包括系统登录验证机制、用户账号管理、口令规则、一般用户权限管理、管理员用户权限的管理、用户权限的职责分离、用户账号和用户权限的定期审核、用户活动的监控、服务器操作系统安全设置及变更的管理和检查，以及数据的直接访问管理等；

3) 物理安全：包括进入机房的人员管理、进入机房的登记、敏感纸质系统文件的管理等；



- 4) 网络安全：包括出口的访问控制、防火墙设计、安装、配置及变更的流程和接触控制、外部网络的连接满足业务需求并记录、防火墙日志的检查、远程登录的申请和审批、财务数据通过传输时的加密、内部网络设计的审批及资料的存档、网络设计变更的管理流程等；
- 5) 计算机病毒防护：包括防病毒软件的安装、病毒定义文件的更新、定期的硬盘扫描等；
- 6) 第三方安全管理：包括合同中的安全条款以及第三方接触信息资源的审批、监控等。

#### 5.4.1.3 信息系统项目建设管理

- 1) 项目立项审批：包括立项申请的提出、可行性研究和立项申请的批复，还包括商业软件及硬件的外购等；
- 2) 项目建设方法论：包括项目启动、项目需求分析、项目设计、系统开发实施、系统测试、数据移植、系统上线、项目验收和上线后的评估等；
- 3) 项目管理：包括项目培训管理、项目文档管理、项目沟通管理、项目变更管理、项目问题管理、环境隔离等。

#### 5.4.1.4 信息系统变更管理

- 1) 变更管理：包括变更的优先级别的划分、变更申请的跟踪、未授权变更活动的管理等；
- 2) 日常变更流程：包括日常变更申请与受理、变更实施、变更测试、变更上线、变更文档管理与培训等方面；
- 3) 紧急变更流程：包括紧急变更事先获得的口头批准，事后追补的书面审批等。

#### 5.4.1.5 信息系统日常运作

- 1) 机房环境控制：包括机房的建筑标准、布线、温度、电源、防火等；
- 2) 系统日常运作监控：包括每天对应用系统、网络设备、机房状况进行的巡检，及检查结果的记录等；
- 3) 批处理作业调度管理：包括对批处理作业的审核、执行、检查、记录等；
- 4) 备份与恢复：包括备份的审批、执行、恢复、测试、记录等；
- 5) 问题管理：包括问题的解答、汇总，报告，存档等。

#### 5.4.1.6 最终用户操作

- 1) 最终用户计算机操作安全制度：包括用户计算机操作的安全制度及员工遵守该制度的声明等；
- 2) 电子表格管理：包括确定支持财务报告及披露的电子表格的清单和分类，电子表格的开发、测试、使用、变更、存储、备份、安全等。

### 5.4.2 措施

#### 5.4.2.1 信息系统控制环境

- 1) 总体控制环境。
  - (1) 公司制定信息技术总体规划，定期进行审阅和调整；
  - (2) 股份公司信息管理部作为中国石油信息化建设的牵头部门，负责企业信息化建设、指导、监督各级信息技术部门工作，建立纵向汇报、沟通和监控机制；
  - (3) 各级信息技术部门的岗位设置从安全和内部控制的角度，考虑职责分离的要求，可在重要工作岗位建立员工备份机制；
  - (4) 各级信息技术部门根据自身信息系统的特点和人员配置情况，制定相关的信息技术培训计划，落实培训工作。
- 2) 信息与沟通。
  - (1) 各级信息技术部门识别所属单位信息系统中的信息资产，确定受保护的信息资产清单，并进行分级，明确各信息资产的相关责任人；
  - (2) 各级信息技术部门应明确信息技术内控职责，负责在其管理范围内进行各项信息技术管理政策、制度和标准的宣贯工作，定期评估执行情况并解决发现的问题。
- 3) 风险评估。

公司信息管理部对公司及业务层面的主要信息技术风险进行评估，并每年定期审阅信息技术风险评估结果。当发生重大的信息技术应用或者组织结构变动时，公司信息管理部对变动情况进行风险评估，必要时调整相关风险防范措施。

#### 4) 监控。

在公司范围内，建立信息技术总体控制执行情况的测试、监督和审查制度，并根据执行情况做相应改进。

#### 5.4.2.2 信息安全

##### 1) 信息安全管理组织。

公司建立信息安全组织架构，并建立完善的汇报机制。在公司总部和地区公司等各级信息技术部门设立信息安全管理负责人，负责本单位的信息安全培训和信息技术日常工作的安全监督和检查。

##### 2) 逻辑安全。

(1) 对信息系统（包括网络系统、操作系统、数据库和应用系统等）的访问，执行访问控制原则，通过安全的登录验证机制，确保只有合法的用户才能访问适用的系统。

(2) 公司建立用户权限申请、更改、撤销的管理流程。用户和权限根据职责分离和最小权限原则进行分配和设置。

(3) 公司制定口令规则，对用户的口令及口令的使用进行管理，包括对口令设定、重新申请、口令强度、变更周期和口令管理做出明确规定。

(4) 公司建立用户账号和权限的审核流程，有正式的文档对用户获得的权限进行记录，定期审核用户账号和权限，纠正错误的权限分配，关闭无人使用的用户账号，并及时维护相关文档。

(5) 根据系统的重要程度，对用户的系统活动采取不同的监控措施，并及时报告异常活动。

(6) 公司建立服务器操作系统的设置和变更管理流程，并对设置进行定期审核。

(7) 公司建立应用系统数据直接访问的申请和审批管理流程，防止未经授权的数据直接访问。

##### 3) 物理安全。

(1) 所有机房采取必需的保护措施，保证进出机房的安全控制，保护措施根据实际情况可采用：电子门禁、警卫、密码、门锁等；

(2) 公司建立进入机房的安全访问和登记管理机制；

(3) 公司建立敏感纸质系统文件的管理制度。

##### 4) 网络安全。

(1) 公司建立网络设计和变更管理流程。各级信息技术部门负责本单位网络设计文档的归档管理工作。

(2) 公司建立边界网络出口的登记管理机制，内部网络与外部机构网络之间的连接经过审批和登记管理，并且边界网络出口的设置与业务需求相匹配，只允许合法的数据流通过这些连接。

(3) 在网络的内部边界和外部边界等位置，采取有效的措施实施访问控制（如进行路由过滤、配置防火墙等）。建立控制策略的设置和变更管理流程，并进行定期审核。

(4) 公司建立远程访问的管理制度，保证远程访问的安全。远程登录应通过安全可靠的方式进行。建立远程登录账号的申请和变更管理流程，并定期审核远程登录用户账号。

(5) 在外部网络中传输重要数据时采取适当的加密措施。

##### 5) 计算机病毒防护。

公司建立计算机防病毒规定，确定防病毒软件的安装范围。定期更新病毒库，定期扫描系统。

##### 6) 第三方安全管理。

(1) 第三方服务合同中包括有关遵循中国石油信息安全规定的条款，并对第三方在合同执行过程中的安全行为按照合同的要求进行监督；

(2) 建立第三方访问应用系统的申请流程，严格监控第三方对应用系统生产环境的访问；

(3) 建立第三方远程登录账号的申请流程，严格监控第三方对内部网络的远程登录。

##### 7) 信息安全事件响应。

公司建立信息安全事件的响应和升级汇报流程。

#### 5.4.2.3 信息系统项目建设管理

##### 1) 项目立项。

(1) 对公司建立项目立项审批流程；

(2) 公司建立商业软件、硬件和服务外购的管理流程。

##### 2) 项目建设方法。

(1) 公司信息系统建设项目按照系统开发生命周期法分阶段进行。

(2) 公司建立系统开发各阶段的管理制度，涵盖项目启动、项目需求分析、项目设计、系统开发实施、系统测试、数据移植、系统上线、项目验收和上线后的评估。

(3) 在系统开发过程中，开发、测试和生产环境隔离。

(4) 需求分析和项目设计文档得到业务部门的审批，关键的测试结果由最终用户签字认可。

(5) 测试后的系统源代码应有保护措施，防止未经授权的修改。

(6) 在系统上线时，采取控制措施，保证数据的准确性和完整性。数据移植结果经过数据所有者复核并签字认可。

(7) 公司建立项目验收流程，项目验收完毕由用户签署项目验收报告。系统上线一段时间后，进行上线后评估，并解决发现的问题。

### 3) 项目管理。

(1) 项目开发过程中，制定项目培训计划，并编写培训文档；

(2) 对业务用户和系统人员进行充分的项目培训；

(3) 及时收集、整理项目开发各阶段产生的项目开发文档和项目管理文档，并妥善保管；

(4) 公司建立定期向项目指导委员会汇报项目进度及其项目情况的制度；

(5) 公司建立项目的变更管理流程，以及项目的问题管理流程。

## 5.4.2.4 信息系统变更管理

### 1) 变更管理。

系统变更包括对应用系统的升级、修改、补丁安装等改变系统功能的活动，以及对操作系统升级和补丁安装、数据库 / 操作系统环境配置变化、防火墙配置修改等。

根据系统变更对业务的影响程度，界定变更活动的优先级别，并对变更活动进行跟踪。禁止一切未经授权的系统变更行为。

### 2) 日常变更。

(1) 公司建立应用系统变更和系统环境变更的管理流程，包括变更申请、受理、实施、测试、上线等几个步骤；

(2) 完整记录并更新应用系统变更和系统环境变更的相关文档。

### 3) 紧急变更。

紧急变更是指由于突发事件且情况紧急，如果不立即采取措施，按照正常变更管理流程，将会严重影响公司正常业务运作的变更需求。

紧急变更要符合以下要求：

(1) 公司建立紧急变更的管理流程，所有紧急变更应妥善记录以便事后审阅；

(2) 紧急变更完成后补填相关变更程序记录。

## 5.4.2.5 信息系统日常运作

### 1) 机房环境控制。

公司根据机房重要程度配备必要的环境控制设备，包括空调、温度湿度计、消防报警设备、防雷和防静电设备、不间断电源系统等。

### 2) 系统日常运作监控。

(1) 公司安排相关人员定期对设备运行状况进行巡检；

(2) 公司安排相关人员定期检查关键系统和设备的系统日志（如关键的应用系统、防火墙等），审查是否有错误信息或异常情况。

### 3) 批处理作业调度管理。

公司建立批处理作业的调度和变更管理流程，并进行监控和定期检查。

### 4) 备份与恢复。

公司根据应用系统的重要程度，制定系统备份和恢复策略，包括备份数据内容、备份方式、备份频率、操作方法、备份及恢复操作步骤、备份介质存放地点等。备份和恢复策略进行定期审阅。系统管理员依据策略执行备份作业，定期进行备份存储介质的恢复性测试。

### 5) 问题管理。

公司建立信息技术问题管理流程及升级汇报制度，按照问题的影响程度，对其进行分级，并根据问题的级别上报至相应的管理层。

## 5.4.2.6 最终用户操作

### 1) 最终用户计算机操作安全制度。

公司制定最终用户计算机操作安全制度，用以规范最终用户的计算机操作。

### 2) 电子表格管理（详见附件 1）。

公司识别与财务报表密切相关的电子表格，建立有关安全、版本、变更、开发、备份、逻辑检查和存档等方面的控制策略，对其进行登记、保护和管理。

上述措施详见附件 2：中国石油天然气股份有限公司信息系统总体控制矩阵。

#### 5.4.3 文档性记录

- 1) 股份公司信息技术总体规划；
- 2) 地区公司信息技术年度工作计划；
- 3) 部门、岗位职责描述；
- 4) 信息资产清单；
- 5) 会议纪要；
- 6) 信息技术培训计划、培训记录等；
- 7) 信息技术风险评估的相应文件；
- 8) 执行情况汇报、测试计划、测试报告等；
- 9) 员工遵守企业信息安全规定的声明；
- 10) 工作记录表单；
- 11) 网络设计文档及审批文件；
- 12) 与第三方供应商达成的合同或协议；
- 13) 信息系统项目建设相关文档；
- 14) 电子表格管理相关文档。

### 5.5 信息系统应用控制

#### 5.5.1 内控关注要点

##### 5.5.1.1 完整性

- 1) 所有的交易都经过处理，且只处理一次；
- 2) 不允许数据的重复录入和处理；
- 3) 例外情况的发现和解决。

##### 5.5.1.2 准确性

- 1) 所有的数据（包括金额和账户）是正确和合理的；
- 2) 例外情况被及时发现以保证交易被记录在正确的会计期间。

##### 5.5.1.3 有效性

- 1) 交易被适当授权；
- 2) 系统不接受虚假交易；
- 3) 例外情况被发现和处理。

##### 5.5.1.4 接触控制

- 1) 未经授权，不得对数据进行修改；
- 2) 数据的保密性；
- 3) 物理设备的保护。

#### 5.5.2 措施

由于公司在用的应用系统众多，而且大多数没有统一规范，为此，公司制定了《应用系统划分规范及工作指引》，该指引对在用的应用系统进行了等级划分确认。

##### 5.5.2.1 应用系统划分

- 1) 应用系统划分原则。
  - (1) 该应用系统用于进行有关重要交易事项的生成、授权、记录、处理或报告；
  - (2) 该系统是否生成关键的表单和数据供财务部门使用，直接作为记账依据或生成财务报表；
  - (3) 该系统是否生成关键的表单和数据供其他作为记账依据或生成财务报表的系统使用；

(4) 对应用系统的依赖程度，即是否有来自系统的计算结果，应用系统中是否存在相应的计算、检查、核对过程的控制。

上述应用控制是否是唯一依赖的控制措施，是否依靠存在手工控制也可以达到控制目标，弥补风险。

2) 应用系统划分标准。

(1) 第一等级应用系统。

这类应用系统是重要的与内部控制直接相关的应用系统，须满足以下条件：

- ①在公司范围内普遍使用；
- ②存在对财务报告产生重大影响的会计科目，或存在对财务报告产生重大影响的功能，或与财务系统存在接口（手工或自动）；
- ③在重大方面无法依赖手工控制。

(2) 第二等级应用系统。

这类应用系统是财务内部控制间接相关的应用系统，它生成的数据作为财务记账处理或为财务系统所使用。

对第二等级应用系统的分析思路是：首先，从录入到第一等级应用系统的重要单据和数据出发，分析、识别这些单据和数据是否来自第二等级应用系统；然后从第二等级应用系统的功能模块出发，识别系统的功能步骤，输入系统的重要单据和表单，以及系统生成的重要单据，分析是否具有有效的手工控制活动。

将同时满足以下四个标准的系统，确定为第二等级应用系统：

- ①存在对财务报告产生重大影响的功能；
- ②存在对财务报告产生重大影响的会计科目；
- ③在公司范围内普遍使用；
- ④所有重大方面可以依赖手工控制。

(3) 第三等级应用系统。

将第一等级和第二等级应用系统以外的应用系统划分为第三等级应用系统。

3) 应用系统划分结果。

依据以上划分原则，确定各等级的应用系统如下：

第一等级系统	第二等级系统	第三等级系统
财务管理系统（包括 FMIS5.0, FMIS6.0 及其他财务系统） 资产管理系统 5.0 及 6.0 资金管理系统（总部资金子系统以及地区公司独有资金结算系统） 不能通过手工控制措施满足控制目标和防范风险的企业资源规划系统（ERP 系统）	物资管理系统 销售管理系统 人力资源/薪金管理系统 能通过手工控制措施满足控制目标和防范风险的企业资源规划系统（ERP 系统）	合同管理系统 税务管理系统 投资管理系统 生产运行管理系统 工程项目管理系统 纠纷案件管理信息系统 规章制度管理信息系统 其他系统

5.5.2.2 应用系统权限管理

1) 应用系统权限管理的组成。

(1) 访问控制：是指用户能够访问哪些应用系统内的资源或执行哪些任务（或功能）的范围，从控制的角度考虑在系统中所拥有的功能权限和数据权限是否超出了其工作需要；

(2) 职责分离：职责分离是把一个业务（子）流程的工作内容分为几个职责不相容的部分并由不同的人来完成，避免因同一个人能够操作不相容职责而产生的错弊风险。

2) 应用系统权限管理的基本原则。

用户权限管理应同时满足以下基本原则：

(1) 需求导向及最小授权原则：对于用户的权限，应当以其实际工作需要为依据，且仅应当授予能够完成其工作任务的最小权限；

(2) 未明确允许即禁止：除非用户有对于权限的需求得到了相关领导的明确批准，否则不应当授予用户任何权限；

(3) 职责分离原则：任何一个用户不能同时具有两种（或两种以上）不相容的权限。

### 3) 应用系统权限控制。

(1) 公司制定《应用系统用户权限管理工作规范》并依据该规范对用户权限需求和实际分配情况进行分析，并合理设置，为定期的测试提供规范和依据。

(2) 各地区公司根据实际工作的需要定义不同的数据权限，以财务报告相关的内部控制为依据，从关键业务流程和关键控制措施出发，明确责任中心、凭证类型以及重要会计科目、报表的权限设置。

(3) 权限日常管理，是依据应用系统用户的标准功能权限和数据权限，对用户权限的申请、审批、变更、删除进行管理。

(4) 在日常管理工作中，要定期检查用户在系统中的访问权限，主要检查以下事项：

①定期或在发生变动后，检查所有用户权限的设置情况；

②对于拥有关键权限的所有用户，以更短的周期进行检查；

③在应用系统的用户权限发生变动时，按照《信息系统总体控制实施办法》中相关的流程进行变更处理。

### 5.5.2.3 应用系统自动控制

信息系统可利用数据类型校验、重复输入校验、批总量控制、序列校验、系统匹配、逐一检测、编辑校对、预定的数据列表、授权检查、有效性检查等技术控制，对应用系统的输入、处理和输出进行有效控制。

#### 1) 对输入数据的确认。

应用系统如果受到故意或意外无效数据的攻击，会导致系统故障、数据滥用或通过系统本身安全漏洞进行欺诈犯罪等事件的发生。因此应用系统采用数据确认控制将数据的输入范围控制在一个合理的范围内，即限制在系统有效处理能力之内。

(1) 定期评审关键的数据文件的内容，确保其有效性和完整性；

(2) 检查硬拷贝的输入文件，确保输入数据没有经过任何未经授权的更改；

(3) 建立错误数据的相应程序；

(4) 建立程序对于可疑的数据进行进一步检查；

(5) 规定数据输入过程中所涉及的所有人员的职责。

#### 2) 对数据内部处理的控制。

已经正确输入的数据也可能因为处理的错误或人为的改动而被破坏，因此为了保证数据在处理过程中的安全性，应对数据处理进行以下控制：

(1) 批处理控制，确保事务更新后保持数据文件的平衡一致；

(2) 确认系统产生数据的正确性；

(3) 确认数据传输过程中的完整性；

(4) 检查确保应用系统运行的时间正常；

(5) 检查确保应用系统运行的顺序正常。

#### 3) 对输出的数据进行确认。

尽管系统的输入是正确的，但输出仍然可能是错误的或是经过非法修改的。为确保输出信息的正确性，要对输出的数据进行确认，主要包括：

(1) 可信性检查，确认输出的数据是否合理；

(2) 数据一致性检查；

(3) 相应输出确认测试的程序；

(4) 数据输出过程中相关人员的责任。

#### 4) 例外处理。

相关岗位的操作人员对操作过程中出现的例外活动，根据情况自行处理或将例外事件情况及时汇报给主管领导进行处理。

### 5.5.3 文档性记录

1) 关键控制管理文档（系统控制措施）；

2) 系统权限控制文档；

3) 业务流程和应用系统目录索引；

4) 系统关系结构图；

5) 应用系统控制措施与信息处理目标（CAVR）对照表。

## 5.6 信息披露

## 5.6.1 内控关注要点

### 5.6.1.1 有效沟通

信息披露工作中涉及到的员工均能获得他们应该了解的信息，确保信息披露工作的内部沟通畅通、有效；与投资者、证券分析师和外界媒体进行良好的沟通。

### 5.6.1.2 向涉及到的员工传达其职责和控制责任

信息披露工作中涉及到的员工应对整个信息披露工作有充分的认识，明确其在信息披露工作中所承担的工作和职责；参与信息披露工作的每个岗位应由适当人选担任，以保证信息的准确传递。

### 5.6.1.3 整体支持

有效推行信息披露程序，需要管理层和所有员工的充分支持和配合，有培训或类似方式使员工能够获得最新的技术性支持材料；对于所有涉及披露流程的有关人员有专门培训，以确保他们能充分理解自身职责；对不同岗位的员工进行有针对性的培训，以确保他们有能力履行职责和应付不断更新的外部要求。

### 5.6.1.4 管理层和披露委员会的监督

管理层和披露委员会采取个别的及定期的监控流程来保证信息披露的质量；监控流程由有经验的员工进行客观、公正地执行。

### 5.6.1.5 持续改进与维护

管理层和披露委员会对信息披露工作进行改进与维护，以确保信息披露工作能够有效实施，并保证所披露资料能够满足监管要求和上市地法律、法规的要求；对于新的法规要求被提议的问题或程序执行中出现的问题，管理层应采取及时且适当的应对措施。51

## 5.6.2 措施

### 5.6.2.1 组织保障及有效沟通

#### 1) 组织机构。

公司制定《中国石油天然气股份有限公司信息披露控制和披露程序的原则》，成立了信息披露委员会，并明确其构成与职责。

信息披露委员会由负责投资者关系、披露及法律事务的副总裁、财务总监和董事会秘书组成。三人共同研究决定信息披露的重大事宜。

信息披露委员会负责考虑合并报表单位的重要性水平以及需要单独认证的业务单位的重要性水平，保持披露事项重要性水平的一致。

信息披露委员会下设披露委员会工作小组，以具体操作披露委员会的日常工作。披露委员会工作小组成员由披露委员会任命，应由（但不限于）中国石油投资者关系负责人、各业务板块披露工作负责人、法律事务部有关负责人及董事会秘书局披露工作负责人等相关人员组成。

#### 2) 职责和控制责任的传达。

公司明确涉及信息披露工作员工的职责和任职要求。

披露委员会通过指定专人负责相关披露报告中的某些章节（如诉讼、法规、竞争、财产、管理层对财务状况及经营业绩的讨论及分析、板块业务等章节）的起草 / 审阅来分配起草 / 审阅责任。

#### 3) 对外有效沟通。

在对外沟通方面，董事会秘书代表公司进行法定信息披露，公司对外发言人被授权对外发表谈话或发布新闻稿。

### 5.6.2.2 培训

披露督导组织、协调对参与编制或审核相关定期报告的披露委员会成员及其他人员（视适当者而言）就披露控制和程序进行不间断的持续性教育。包括：就美国证交会报告和披露要求以及最佳实际做法进行的相关培训等。

### 5.6.2.3 监督

1) 对定期报告的监督。

首席执行官和财务总监在认可定期报告中的披露内容前与披露委员会、独立审计师、审计委员会、高级管理层，以及外聘法律顾问和独立储量工程师（在适当范围内）进行讨论，并留有充足的时间充分审核信息、涉及事项、将做出的披露和应遵循的程序等内容。

审计委员会对财务报告和业绩公告部分进行监督、审核。

独立审计师审核财务报告的内部控制以及定期报告中的特选章节，包括：管理层对财务状况和经营业绩的讨论及分析（包括关键性会计原则、新会计标准的描述、安排资产负债表以外的披露、合同义务和或有责任及市场风险的定量和定性披露）以及其他财务披露内容。

2) 对非定期报告的监督。

对非定期报告的信息披露工作，公司根据监管规定和披露程序要求进行信息披露的监督工作，并由公司律师进行审核，董事会秘书签字确认。

#### 5.6.2.4 改进与维护

为确保信息披露内容符合监管方和上市地要求，董秘局和财务部门在确定本年信息披露内容前，与律师事务所和会计师事务所沟通，了解监管机构的最新要求，按照监管部门的要求将披露事项的增加或变动向披露委员会请示。披露委员会按照监管部门的要求，对披露事项的有关工作进行部署并上报董事长审批，工作部署包括职责分工和时间安排。

信息披露委员会审核公司过去在美国证交会报告中做出的重大披露及其他公开声明，以确定对这些披露信息是否进行更新，或更正是否适当，并根据需要及时更新、更正公司的公开披露信息。

#### 5.6.3 文档性记录

1) 披露事项有关工作部署文件。

2) 程序报告。



## 6 监督

### 6.1 概述

#### 6.1.1 概念

监督是对内部控制体系有效性进行评估的持续过程，包括持续监督、独立评估和缺陷报告等要素。

##### 6.1.1.1 持续监督

持续监督是在公司日常经营过程中进行的，包括日常的管理和监督活动，以及员工在履行职责时所采取的检查内部控制执行质量的行为。

##### 6.1.1.2 独立评估

尽管持续监督程序可以提供内部控制其他要素是否有效的重要信息，但公司有必要组织独立评估以直接检查内部控制体系的有效性，这种做法可评估持续监督程序是否有效。

独立评估就是独立于控制活动之外而采取的定期评估行为。独立评估的范围和频率，主要取决于风险评估和持续监督程序的有效性。独立评估内容包括：评估的范围和频率、评估过程、评估方法、文档记录。

##### 6.1.1.3 缺陷报告

###### 1) 内部控制缺陷

当某项控制的设计或运行不能使管理层或员工在正常行使其职责过程中及时防止或发现错报时，表明存在内部控制缺陷。内部控制缺陷包括设计缺陷和运行缺陷。

设计缺陷：当缺少实现内部控制目标必需的某项控制措施时，或者当现有内部控制的设计不适当，导致即使内部控制按照设计运行，通常也无法实现内部控制目标时，则存在设计缺陷。

运行缺陷：当设计适当的内部控制没有按设计运行，或者当执行内部控制的相关人员缺乏必要的授权或不具备实施有效控制的资格时，则存在运行缺陷。

###### 2) 缺陷类型

缺陷按照程度不同分为一般缺陷、重要缺陷和实质性漏洞。

一般缺陷：如果内部控制设计或运行无法使管理层或员工在执行指定任务的正常过程中，及时防止或发现错报，那么内部控制就存在一般缺陷。

重要缺陷：是控制缺陷或控制缺陷的集合，它会负面影响公司按照公认会计准则要求进行可靠的初始化处理、授权、记录、处理和报告对外财务数据的能力，以至于有可能导致不能防止或发现年度或中期财务报告大于不重要的错报。

实质性漏洞：是重要缺陷或重要缺陷的汇总，导致有一定可能性不能防止或发现年度或中期财务报告的重大错报。

###### 3) 缺陷报告

缺陷报告是将内部控制缺陷自下而上报告的行为。缺陷报告的内容包括：汇集和报告发现的内部控制缺陷、汇报机制的适当性、跟进评估的适当性等。

### 6.2 持续监督

#### 6.2.1 内控关注要点

持续监督主要关注以下几个方面：

- 1) 内控体系运行与维护管理；
- 2) 在日常活动中获得内部控制执行的证据；
- 3) 外部反映对内部信息的印证程度；
- 4) 定期核对财务系统数据与实物资产；
- 5) 对内外部审计师提出的关于加强内部控制的措施做出响应；
- 6) 培训、会议等对内部控制有效性的反馈；
- 7) 定期询问员工是否理解并执行了公司的职业道德规范，员工是否执行了内部控制活动；
- 8) 内部审计活动的有效性。

## 6.2.2 措施

公司应以重大风险、重大事件、重要管理及业务流程为重点，对内控体系有效性进行监督检查，并对内部控制体系维护的方法、建设标准的变更、监督与考评工作等进行规范，以保证内部控制体系安全、稳健、有效运行。公司制定《中国石油天然气股份有限公司内部控制体系管理规范》、内部控制体系评价规范等，全面规范和指导内控体系建设和监督工作。

### 6.2.2.1 内控体系运行与维护管理

公司制定内部控制体系管理规范，建立内部控制考核机制，将内部控制工作纳入各级管理层业绩考核，构建体系运行长效机制，主要措施包括：

- 1) 内部控制部根据相关情况编制公司上一年的内部控制评价报告，报内控体系建设委员会进行审核确认。
- 2) 公司管理层将内控体系评价结果纳入对总部各部门、专业分公司、地区公司及高管人员的业绩考核。
- 3) 内部控制部对地区公司内控计划完成情况进行考核。地区公司将内部控制的日常监督考核作为业绩考核的一部分，结合考核结果，实施奖惩。

公司目前内控监督考核机制尚不完善，公司将在今后的内控体系建设中，进一步修订、完善内控考核办法，将内部控制工作纳入公司各级管理层业绩考核，构建内部控制体系运行长效机制。

### 6.2.2.2 获得内部控制执行的证据

获得内部控制执行的证据是指公司在日常经营管理活动中，取得必要的、相关的证据，以证明内部控制体系发挥功能的程度，主要措施包括：

- 1) 公司管理层通过总裁办公会、财务例会等形式，收集汇总各部门的信息，监督各方面工作的进展。总部机关、专业分公司、地区公司通过财务分析等形式，汇集各方面信息，分析异常变动的原因，使潜在问题得到反映，从而对财务报表质量进行监控。
- 2) 公司总裁和财务总监签署年度报告确认其实施和维护与财务报告相关的内部控制程序的责任；同时，地区公司负责人和财务负责人对财务数据的准确性签署声明。
- 3) 总部机关、专业分公司、地区公司各部门负责对本单位的内部控制进行自我检查，并将检查、检验报告报送内控管理部门。
- 4) 地区公司对内部控制执行情况开展自我测试和评价，每年至少检查一次。地区公司内控部门牵头组织本单位综合检查组，依据《内部控制体系评价规范》的相关要求具体开展测试工作，并在测试以及评价工作结束后，模拟管理层对本单位内部控制的有效性发表声明。
- 5) 内部控制部每年 3 月份对公司重要业务单位进行确认，并随时对新增业务单位以及发生业务变化导致重要性改变的业务单位进行跟进确认。定期或不定期组织开展公司内部控制的检查和综合评价工作。
- 6) 公司审计、监察部门、质量安全环保部门制定相关制度办法，通过纪检监察信访机制、效能监察工作以及重大事故的调查工作，加强内部控制的持续监督。

### 1.2.2.3 外部反映对内部信息的印证

外部反映对内部信息的印证是指来自外部关联方的信息支持内部生成的信息或反映内部问题，主要措施包括：

- 1) 公司接受外部监管者的检查监督，及时获取反馈信息，汇总、分析检查意见，制订整改措施并检查各项措施的执行情况。
- 2) 各单位通过召开客户座谈会、检查客户的投诉记录、走访客户以及向客户公布公司监督部门的联系方式等措施，收集客户对公司的意见和建议，制定相应的政策并监督检查整改措施的执行情况。
- 3) 公司与外部单位进行往来账项的函证，并对结果进行分析处理。

### 6.2.2.4 会计记录和实物资产的定期核对

会计记录和实物资产的定期核对是指定期将信息系统所记录的数据与实物资产相比较，主要措施包括：

1) 公司制定《中国石油天然气股份有限公司资产管理暂行办法》等实物资产的管理办法,明确定期盘点的具体要求。

2) 地区公司根据上述办法制定实施细则,定期对固定资产、存货、现金、票据和有价证券等进行盘点,做到账账、账实相符。

#### 6.2.2.5 内外部审计建议的响应

内外部审计建议的响应是指管理层对内外部审计师提出的加强内部控制的建议所做出的反应,主要措施包括:

1) 审计委员会向董事会提交对公司财务报告及相关资料的审阅报告,充分考虑内外部审计师提出的事项。

2) 公司管理层对内外部审计师提出的管理建议,通过召开会议、委派调查小组等方式对缺陷进行调查、分析,并采取相应的纠正措施。

3) 根据《中国石油天然气股份有限公司内部审计工作规定》,审计部门执行公司内部审计工作,对审计中发现的问题提出管理建议:

(1) 对一般性问题,管理层授权审计部门下达审计意见书或审计决定书。被审计单位接到上述文件后,按照审计意见和决定组织实施,并将整改情况以书面形式向审计部门反馈。

(2) 对重大事项,即涉及公司重大决策、重大利益、声誉等,以及需要对其主要负责人进行处理的,经总裁(总经理)审批后,签发给被审计单位及有关部门,审计部门负责跟踪审计建议落实情况。

#### 6.2.2.6 管理层及有关部门获知内部控制的程度

管理层及有关部门获知内部控制的程度是指管理层及有关部门通过培训、会议等方式从基层了解到控制实施情况及控制缺陷的反馈情况,主要措施包括:

1) 审计委员会建立相关程序,处理下述投诉:

受理、保留及处理公司获悉的有关会计、内部会计控制或审计事项的投诉;

受理、处理员工有关会计或审计事项的投诉或匿名举报,并保证其保密性。

2) 管理层在会议或培训中询问内部控制执行情况,对大家提出的问题进行总结并提出改进措施。

3) 管理层对公司员工提出的合理化建议予以重视,并不断完善员工合理化建议机制,明确相应的责任部门、范围、征集方式、评审办法、奖励措施等内容。

4) 监察部门每年组织调研和专项检查。调研主要针对公司管理人员廉洁从业状况、管理制度的落实状况、管理的效果、存在的问题,并向管理层提出管理建议。

5) 监察部门负责受理来自于公司内、外部对违规行为的举报,并进行调查处理。

#### 6.2.2.7 定期询问员工

定期询问员工是指定期要求公司员工明确说明他们是否理解并遵守了行为规范、道德准则,以及是否开展了控制活动,主要措施包括:

1) 公司制定《中国石油天然气股份有限公司高级管理人员职业道德规范》和《中国石油天然气股份有限公司员工职业道德规范》,以书面形式下发,要求以培训等方式进行宣贯。同时,公司每年组织高级管理人员签订《职业道德规范确认书》。

新加入公司的员工上岗前的教育包括公司职业道德规范的内容。

监察部门和人事部门根据公司管理层的授权对公司员工遵守职业道德规范的情况进行监督。

2) 公司确立重要业务流程及对应的控制措施,各单位在日常工作中,就本单位员工是否执行了控制活动进行自我监督检查。

#### 6.2.2.8 内部审计活动的有效性

内部审计活动的有效性主要包括以下几个方面:执行内审活动人员的能力与水平是否合适;审计部门负责人是否按规定或应董事会、审计委员会要求报告工作;内审的职责和权限是否恰当,内审的范围、责任和计划是否恰当。主要措施包括:

1) 审计人员能力和水平。

(1) 公司在《中国石油天然气股份有限公司内部审计工作规定》中明确规定,根据需和相关规范对各级审计机构的审计人员数量、职级、专业结构进行配备,保证审计部门能够全面有效地开展工作。

(2) 公司在《中国石油天然气股份有限公司内部审计规范》中明确规定内部审计人员应该具有的资质和执业能力，制定内部审计职业道德规范，要求审计人员在办理审计事项时必须遵守。

2) 审计部门的地位及与董事会、审计委员会的接触。

(1) 公司确保审计部门拥有足够的运作资源，享有适当地位。

(2) 审计部门根据授权可以参加公司有关经营和财务管理决策会议，获知管理薄弱领域或环节、公司新的重大的经营管理活动等，从而编制内部审计计划。

(3) 审计部门对审计中发现的违反国家法律法规和公司管理规定的事项提出审计建议，做出审计决定，对审计建议、审计决定的落实情况进行跟踪监督。必要时对责任单位、责任人按有关规定提出追究责任的建议；对发现的公司内部控制管理缺陷，及时提出改进建议。

(4) 根据《中国石油天然气股份有限公司内部审计工作规定》，审计部门定期或应要求向监事会、董事会审计委员会、总裁（总经理、院长）以及上级审计机构报告工作，对重要审计发现及时报告并提出处理意见。

(5) 根据国内外适用规则，内部审计工作接受董事会、审计委员会的检查、监督，接受国家审计机关、行业协会的指导和检查，各所属专业分公司、地区公司的内部审计工作接受股份公司审计部的指导。

3) 公司制定《中国石油天然气股份有限公司内部审计工作规定》，明确内部审计的责任、范围。

### 6.2.3 文档性记录

1) 总裁办公会、财务例会等相关会议纪要；

2) 财务分析报告；

3) 年度财务报告；

4) 客户座谈会记录、客户投诉和举报记录；

5) 往来款项询证函；

6) 资产盘点报告；

7) 内部审计建设规划、年度审计工作要点、审计项目计划、年度内部审计工作总结、审计报告、审计意见书、审计决定书、整改情况说明材料；

8) 内部控制工作会议纪要；

9) 监察部门的调研报告；

10) 合理化建议记录；

11) 职业道德确认书、职业道德和行为规范的培训记录；

12) 自我监督检查及测试记录。

## 6.3 独立评估

### 6.3.1 范围和频率

#### 6.3.1.1 内控关注要点

1) 对内部控制体系适当的部分进行评估；

2) 评估是由具备必要技能的人员进行的；

3) 评估的范围、覆盖的深度和频率是足够的。

#### 6.3.1.2 措施

公司以风险为导向，制定《重要业务单位确认》、内部控制体系评价规范等，定期对总部各部门、专业公司和地区公司内部控制体系有效性进行检查和监督。

1) 对内部控制体系适当的部分进行评估，而且评估的范围与频率是足够的。

(1) 公司具体明确对公司层面控制、业务活动层面控制、信息系统控制进行独立评估。审计部和内部控制部定期对各部门和业务单位内控体系有效性进行监督评价。

(2) 审计部、内部控制部依据持续监督的结果，针对高风险领域进一步提出管理层测试范围的意见和建议。

(3) 公司管理层每年开展管理层测试，审计部和内部控制部负责组织实施对总部机关、专业分公司和地区公司的管理层测试。其中，对审计委员会、审计部的测试以及补充、更新、改进、财务报告控制测

试均由内部控制部负责组织实施。

(4) 审计部负责进行例外事项分析；内部控制部负责对控制缺陷进行分析，确认一般缺陷、重要缺陷和实质性漏洞，同时对有效性问题进行跟进整改。

(5) 内部控制部已经制定了《重要业务单位确认》，并以标准形式正式下发；以财务报告内控有效性为目标制定了内部控制体系评价规范；今后，随着体系建设涵盖的目标的扩大，内部控制部将不断充实和更新。

#### 2) 测试人员

公司审计部门代表管理层开展的管理层测试由内部审计人员参加，在人员不充足的情况下，可以在中介机构中选择合适人员。

公司内控部门代表管理层开展的测试由内部控制人员参加，在人员不充足的情况下，可以在内部控制服务市场准入单位中选择合适人员。

(1) 测试人员不能够参加自己负责的业务活动的评估。

(2) 测试人员必须具备相关专业知识和一定的经验。

### 6.3.2 评估过程

#### 6.3.2.1 内控关注要点

- 1) 评估过程由具有必要职权的高级管理人员主持；
- 2) 测试人员充分地了解公司的活动；
- 3) 了解内部控制体系应该如何运作，以及实际的运作情况；
- 4) 将评估结果与已建立的标准进行对照，并对其进行分析。

#### 6.3.2.2 措施

1) 管理层测试由公司总裁作为最高负责人，授权财务总监具体负责，总裁和财务总监对最终测试结果负责。

2) 组织参与独立评估的人员开展评估前培训，使测试人员掌握程序、标准和方法，了解被评估单位的基本情况，确保评估工作顺畅、高质、高效开展。

3) 内部控制体系评价规范具体规定测试人员如何充分了解公司的活动，如何了解内部控制体系运作以及如何将测试结果与已建立的标准进行对比分析。

### 6.3.3 评估方法

#### 6.3.3.1 内控关注要点

- 1) 评估方法包括使用核对清单、问卷或其他一些辅助工具；
- 2) 评估小组共同安排评估程序，并确保各方的努力协调一致。

#### 6.3.3.2 措施

1) 测试人员通过询问、观察、检查、再执行等方法评估公司内部控制体系的实际运作。

首先，通过审阅各种文件，询问被测试单位或部门的员工，了解员工对相关业务流程内部控制的熟悉及掌握情况。

其次，采取实地观察、审阅证据和再执行等方法，对照规定的业务流程步骤、控制点，抽取一定量的业务活动样本检查内部控制是否执行以及执行的程度。

2) 评估程序由评估小组编制，在评估工作的时间安排以及人员配合等方面与被测试单位达成一致。

### 6.3.4 文档记录

#### 6.3.4.1 内控关注要点

- 1) 具备书面的政策手册、组织结构图、工作说明、操作指南及信息系统流程图等文件；

2) 以文档记录的评估流程。

#### 6.3.4.2 措施

1) 公司按照萨奥法案和美国上市公司会计监管委员会的要求，组织对内部控制体系进行设计和记录，形成一系列文件，包括：业务流程描述、风险控制文档、风险数据库、自评表等。公司形成书面的公司章程、组织结构图、规章制度，并汇编成册。地区公司根据股份公司下发的制度文件，结合本单位实际，制定相应的实施细则。公司全面开展岗位职责描述，形成《岗位规范》文本。

2) 测试人员将评估过程及结果（包括存在的问题和已有的整改措施）进行记录，负责人复核。被评估单位对评估结果签字确认。

#### 6.3.5 文档性记录

- 1) 内部控制体系评价规范；
- 2) 管理层测试实施方案；
- 3) 评估过程记录；
- 4) 管理层测试报告；
- 5) 检查和综合评价工作报告。

### 6.4 缺陷报告

#### 6.4.1 汇集和报告发现的内部控制缺陷

##### 6.4.1.1 内控关注要点

- 1) 通过持续监督和独立评估获取；
- 2) 来源于内部或外部。

##### 6.4.1.2 措施

公司制定《中国石油天然气股份有限公司内部控制体系管理规范》，明确缺陷报告的职责、报告的内容，对缺陷报告程序及跟进措施等方面进行规范；制定《内部控制缺陷认定规范》，明确缺陷定义及分类、缺陷评估内容、方法和标准等。

##### 1) 通过持续监督和独立评估获取

①地区公司内控部门汇总本单位各部门自查情况以及自我测试结果，形成本单位的内部控制综合评价报告，报送到内部控制部。

②审计部实施管理层测试并出具管理层测试报告，抄送内部控制部。

③内部控制部负责进行缺陷认定，并撰写缺陷认定报告，上报管理层。

##### 2) 来源于内部

公司的纪检监察信访机制、效能监察工作以及重大事故的调查工作，能够汇集和发现公司包括内部控制缺陷在内的问题。具体为：

①纪检监察信访机制：监察部门通过受理公民、法人、境外人员和其他组织以举报信、来访、举报电话为形式的举报，实施监察信访的受理工作。此外，监察部还受理以电子邮件方式在公司信息网上的举报，鼓励合作方对违规行为进行检举。

②效能监察：监察部门对于在效能监察中发现的重要问题和情况，向本单位和上级监察部门报告。

③重大、特大事故报告：公司所属单位在发生重大事故后，两个小时内报总裁办值班室和专业公司生产运行处（调度处）；在发生特大事故后，立即报总裁办值班室。

④公司成立工会并建立员工代表大会制度，汇总员工代表的意见并及时反馈。

##### 3) 来源于外部

公司从外部单位获取相关信息，汇集并报告发现的控制缺陷。具体为：

①公司接受外部监管者的检查监督，汇总、分析外部监管者的检查意见，制订整改措施并检查各项措施的执行情况。

②公司每年从外部审计师获得关于其内控质量及其可能存在的重大缺陷和不足的报告。

③通过召开客户座谈会、走访客户、检查客户的投诉记录、受理客户意见或举报等方式获取有关内部控制存在缺陷的信息，进而改善内部控制状况。

4) 内部控制部依据管理层测试报告, 结合总部机关、专业分公司、地区公司持续监督的检查情况、内部控制部的综合评价以及其他内外部信息, 对公司内部控制体系进行缺陷认定, 形成公司内部控制评价报告, 经内控体系建设委员会审核确认后报董事会审议。

#### 6.4.2 汇报机制的适当性

##### 6.4.2.1 内控关注要点

- 1) 将控制缺陷向直接负责人或上一级人员汇报;
- 2) 特殊类型的缺陷向管理层和董事会汇报。

##### 6.4.2.2 措施

1) 公司审计部门根据《中国石油天然气股份有限公司内部审计工作规定》向总裁(总经理、院长)报告工作, 并及时报告重要审计发现。审计部定期或应要求向监事会、董事会、审计委员会和上级审计机构报告工作。

2) 公司监察部对管理层负责并汇报工作。地区公司监察部门同时向本单位的主管领导、总经理及上级监察部门汇报, 遇到重大事项(如重要案件的线索、重大安全事故、纪检监察部门的重要人事变动及需要请示的其他重大事项)向监察部书面请示、报告, 其他信息通过工作通报、简报、内部刊物、工作会议文件、全年工作总结和专项工作总结、纪检监察信息等方式上报。

3) 总裁办值班室在接到特重大事故报告后立即向有关领导报告, 并通知质量安全环保部和相关专业公司。对于重大事故, 总裁办值班室接到报告后立即向有关领导报告, 并通知质量安全环保部; 专业公司生产运行处(调度处)接到事故报告后立即向专业分公司领导报告。

4) 业务部门和其他控制人员在工作中发现内部控制的隐患和缺陷, 及时以书面形式向其上级主管部门和内控部门报告。

5) 内控部门向管理层随时或定期汇报新出现的风险, 或业务活动中存在着的风险控制瑕疵。涉及重要风险的控制方案及重大整改事项须报内控体系建设委员会审查。

内部控制部在对公司内部控制体系进行评价的基础上, 编制公司内部控制综合评价报告, 经内控体系建设委员会审核确认后报董事会审议。

#### 6.4.3 跟进评估的适当性

##### 6.4.3.1 内控关注要点

- 1) 识别出的错误交易或行为得到纠正;
- 2) 针对问题的根本原因进行调查;
- 3) 实施跟进, 以确保必要的整改措施得到实施。

##### 6.4.3.2 措施

1) 审计委员会就有关内部控制的重要调查结果及管理层的响应进行研究。

2) 公司管理层对外部监管者监管过程中、内外部审计中发现的内部控制缺陷授权相关部门进行调查、分析, 采取相应的纠正措施, 并检查各项措施的执行情况。

3) 公司制定《中国石油天然气股份有限公司内部审计工作规定》、《中国石油天然气股份有限公司内部审计规范》, 审计部门按照规定实施审计。审计部门根据审定的审计报告出具审计意见书, 下达审计决定, 提出管理建议等。

审计部门负责监督检查内部审计意见采纳及审计决定执行情况。

被审计单位在收到审计意见书、审计决定书两个月内, 向审计部门报告执行情况。重要项目审计决定的执行情况, 可实行跟踪检查或后续审计。

4) 监察部门对在纪检监察信访机制、效能监察工作以及重大事故的调查工作中汇集和发现公司包括内部控制缺陷在内的问题, 进行适当的处理, 实施改进措施。

(1) 公司制定《中国石油天然气股份有限公司纪检监察部门信访举报工作规定》, 对信访举报处理的责任部门、方式、程序、完成时限、处理结果反馈方式等进行明确, 确保举报事项能得到适当处理。

(2) 公司制定《中国石油天然气股份有限公司效能监察工作规定》, 对效能监察中发现的问题和效

能评价中反映的问题、找出原因、分清责任、积极整改，同时对效能监察的实施效果进行奖惩。

（3）公司制定《中国石油天然气股份有限公司监察部门参加特别重大事故调查处理的暂行办法》，明确规定：重大事故调查处理工作结束后一个月内，事故发生单位的监察部门要正式向监察部上报事故调查处理情况报告。

5）公司在发生重大事故或特重大事故后，配合政府事故调查组及时认真地调查处理事故，并落实事故调查报告中的事故处理意见和防范措施建议。

6）内控部门负责跟踪检查内外部审计提出的管理建议和内部控制改进意见的落实情况。监督、指导整改方案的实施，根据对方案实施过程和结果的监督，对控制措施的有效性、适宜性进行验证，提出改进建议，并组织有关部门对整改方案进行必要的调整，以确保风险控制目标的实现。

#### **6.4.4 文档性记录**

- 1）内部控制综合评价报告；
- 2）管理层测试报告；
- 3）客户座谈会记录、客户投诉、举报记录；
- 4）审计工作汇报材料、监察部汇报材料；
- 5）各类控制缺陷的上报材料、缺陷整改记录；
- 6）审计意见书、审计决定书；
- 7）事故调查报告；
- 8）效能监察终结报告。



# 附件

## 《内部控制管理手册（地区公司分册）》 编制规范

### 1 范围

本规范规定了股份公司《内部控制管理手册》（地区公司分册）的编制要求、体例格式和管理及维护等内容。

本规范适用于股份公司所属分公司、全资子公司及控股公司（以下称地区公司）。

### 2 规范性引用文件

无。

### 3 术语和定义

#### 3.1 《内部控制管理手册》

《内部控制管理手册》是中国石油天然气股份公司制定并发布的《内部控制管理手册》，简称股份公司《手册》。

#### 3.2 《内部控制管理手册（地区公司分册）》

《内部控制管理手册（地区公司分册）》，是股份公司所属地区公司根据《内部控制管理手册》（地区公司分册）编制规范要求，结合本公司管理实际，编制的《内部控制管理手册》（××公司分册），简称（地区公司分册）。

### 4 编制要求

#### 4.1 编制的总体要求

地区公司在全面贯彻实施股份公司《手册》的基础上，结合本单位的管理实际，编制（地区公司分册），作为股份公司《手册》的组成部分。

#### 4.2 具体编制内容

##### 4.2.1 简介。

##### 4.2.2 手册说明。

##### 4.2.3 组织结构及职责

##### 4.2.4 控制环境。

##### 4.2.4.1 组织结构图。

##### 4.2.4.2 权限指引。

##### 4.2.4.3 控制环境涉及的制度索引。

##### 4.2.5 风险评估。

##### 4.2.5.1 基本业务流程目录。

##### 4.2.5.2 重要业务流程目录。

##### 4.2.6 控制活动。

##### 4.2.6.1 风险控制管理文件。

##### 1) 业务流程图。

##### 2) 风险控制文档（包括 RCD 和 ARCD）。

- 3) 控制实施证据表单。
- 4.2.6.2 控制活动涉及的制度索引。
- 4.2.7 信息与沟通。
- 4.2.7.1 信息流汇总表。
- 4.2.7.2 业务活动与应用系统索引目录。
- 4.2.7.3 关键应用系统调研问卷。
- 4.2.7.4 关键权限与通用角色对照表 (FMIS7.0)。
- 4.2.7.5 不相容通用角色清单 (FMIS7.0)。
- 4.2.7.6 关键权限与通用角色对照表 (FA7.0)。
- 4.2.7.7 不相容通用角色清单 (FA7.0)。
- 4.2.7.8 ERP 系统职责分离矩阵。
- 4.2.7.9 人力资源系统职责分离矩阵。
- 4.2.7.10 财务关联信息系统清单。
- 4.2.7.11 财务关联信息系统手工控制。
- 4.2.7.12 财务关联信息系统流程图。
- 4.2.7.13 电子表格汇总表。
- 4.2.7.14 信息与沟通涉及的制度索引。
- 4.2.8 监督。
- 4.2.8.1 监督涉及的制度索引。

## 5 体例格式

### 5.1 封面

封面格式统一，颜色及字体、字号大小参照股份公司《手册》，式样见附录 1。

### 5.2 目录

参照股份公司《手册》。

### 5.3 正文

#### 5.3.1 正文标题部分。

第一级标题为三号黑体上下各空一行靠左齐，第二级标题为四号宋体上下各空一行靠左齐，第三级标题为五号黑体上下各空一行靠左齐，第四级标题为五号楷体上下各空一行靠左齐；各级标题的编码与标题的内容之间空一个字的距离，标题之后无标点符号。

#### 5.3.2 正文内容部分。

5.3.2.1 串文编码：串文第一级编码为 1)、2)、3) ……，串文第二级编码为 (1)、(2)、(3) ……，串文第三级编码为①、②、③……；若还需要进行级次编码，则第四级用 a、b、c……。

由于这一部分属正文内容，各级串文编码的内容叙述完后，后面要加标点（一般为句号），且段落首行前空两字，换行顶格靠左齐，字体字号均为五号宋体，标准字间距，单倍行距。

5.3.2.2 正文文字：无串文编码的正文内容段落首行前空两字，换行顶格靠左齐，字体字号均为五号宋体，标准字间距，单倍行距。

#### 5.3.3 正文体例格式编制参照股份公司《手册》。

### 5.4 图表体例格式

图名字体字号为小五号宋体，图名应居中排，图名与图之间空一行；图字均为六号宋体。表名字体字号为小五号黑体，表名也应居中排，表名与表之间空一行；表字均为六号宋体（个别地方表示强调可用黑体或其他字体，但同一张表内，所有需强调的地方其字体必须统一）。风险控制文档(RCD)编制参照《控制活动分册》2.1 风险控制文档(RCD)编制规范。

## 6 管理及维护

## 6•1 编写与发布

6•1•1 （地区公司分册）是股份公司《手册》的组成部分，由地区公司内控部门组织编写，报股份公司审查批准，地区公司行文发布。

6•1•2 （地区公司分册）发放范围由地区公司内控部门提出，经本单位管理层批准执行。

6•1•3 （地区公司分册）包括纸质版和电子版两种。

6•1•3•1 电子版的配发范围为业务流程管理信息系统的覆盖范围。

6•1•3•2 纸质版的配发范围为公司所属单位及特殊使用者。

## 6•2 更新与维护

6•2•1 （地区公司分册）由地区公司内控部门负责更新与维护。

6•2•2 每年根据股份公司《手册》的更新要求和内部控制体系运行情况，对（地区公司分册）进行修订，报股份公司备案，由地区公司总经理批准发布执行。

6•2•3 对于追加和调整的部分，地区公司内控部门适时下发补充规定，确保内部控制管理体系的有效运行。

本规范的解释权归属股份公司内部控制部。

本规范自发布之日起执行。



# 内部控制管理手册

× × 公司分册

中国石油天然气股份有限公司  
× × 公司  
二 0 0 七 年 一 月 一 日