ICS 35.080

中华人民共和国国家标准

GB/T XXXXX—XXXX
代替 GB/T 34960.2-2017

信息技术服务 治理 第2部分：实施指南

Information technology service—Governance—Part 2: Implementation guidance

（征求意见稿）

（本草案完成时间：2026-07-18）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… III
引言 …… V
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　治理实施方法 …… 1
5　治理实施框架 …… 2
6　治理主体构建 …… 3
6.1　概述 …… 3
6.2　组建 …… 3
6.3　职责 …… 3
6.4　机制 …… 3
7　治理规划 …… 3
7.1　概述 …… 3
7.2　环境 …… 4
7.3　目标 …… 4
7.4　范围 …… 5
7.5　方案 …… 5
8　治理执行 …… 5
8.1　概述 …… 5
8.2　方向 …… 5
8.3　策略 …… 7
8.4　授权 …… 8
8.5　责任 …… 10
8.6　能力 …… 11
8.7　绩效 …… 13
9　治理优化 …… 14
9.1　概述 …… 14
9.2　评价 …… 14
9.3　改进 …… 15
附录A（资料性）　人工智能治理示例 …… 17

A.1 治理目的 …… 17
A.2 治理范围 …… 17
A.3 治理主体 …… 17
A.4 治理工作 …… 18
A.5 治理交付物 …… 21
参考文献 …… 22

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 34960《信息技术服务 治理》的第2部分。GB/T 34960已经发布了以下部分：

——第1部分：通用要求；

——第2部分：实施指南；

——第3部分：绩效评价；

——第4部分：审计导则；

——第5部分：数据治理规范。

本文件代替GB/T 34960.2—2017《信息技术服务 治理 第2部分：实施指南》，与GB/T 34960.2—2017相比，除编辑性改动外，主要技术变化如下：

a） 增加了“治理实施方法”一章（见第4章）；

b） 更改了“治理实施框架”的构成以及相互关系（见第5章，2017年版的第4章）；

c） 增加了“治理主体构建”一章（见第6章）；

d） 删除了“顶层设计治理的实施”一章（见2017年版的第7章）；

e） 增加了“治理规划”一章，并将2017年版的有关内容更改后纳入（见第7章，2017年版的5.2、5.3、6.2）；

f） 删除了“管理体系治理的实施”一章（见2017年版的第8章）；

g） 增加了“治理执行”一章，并将2017年版的有关内容更改后纳入（见第8章，2017年版的6.3、6.4）；

h） 删除了“资源治理的实施”一章（见2017年版的第9章）；

i） 增加了“治理优化”一章，并将2017年版的有关内容更改后纳入（见第9章，2017年版的6.5）；

j） 增加了“人工智能治理示例”一附录（见附录A）。

本文件由全国信息技术标准化技术委员会（SAC/TC28）提出并归口。

本文件起草单位：中国电子技术标准化研究院、上海计算机软件技术开发中心、广州赛西标准检测研究院有限公司、北京赛西科技产业有限责任公司、北京可利邦信息技术股份有限公司、广东电网有限责任公司、华润数字科技有限公司、上海商学院、浪潮软件集团有限公司、北京工业大学、上海市大数据中心、中国汽车工程研究院股份有限公司、南方电网储能股份有限公司、北京国家会计学院、管易众享（北京）科技有限公司、广东粤电信息科技有限公司、中广核（深圳）运营技术与辐射监测有限公司、中电信数智科技有限公司、江苏意源科技有限公司、上海谷航信息科技发展有限公司、北京银信长远科技股份有限公司、北京神州邦邦技术服务有限公司、上海速邦信息科技有限公司、西安炎黄信息系统咨询有限公司、百信信息技术有限公司、四川久远银海软件股份有限公司、卡斯柯信号有限公司、上海浦东软件平台有限公司、北京德信永道信息技术服务有限公司、北京金山办公软件股份有限公司、上海北宙企业管理咨询有限公司、美林数据技术股份有限公司、深圳市紫金支点技术股份有限公司、青岛城市建设投资（集团）有限责任公司、华南理工大学、南京理工大学、中汽院（重庆）机器人检测技术有限公司、星环信息科技（上海）股份有限公司、上海软中智链数字科

技有限公司、北京仁科信息技术有限公司、山东城市建设职业学院、中金云链（武汉）数字科技有限公司、北京赛迪认证中心有限公司、世熠网络科技（上海）有限公司、神州数码信息系统有限公司、北京疆越科技有限公司、北京赛西科技发展有限责任公司、湖北省电子信息产品质量监督检验院、中通服咨询设计研究院有限公司、轩克科技（上海）有限公司、中电金信数字科技集团股份有限公司、北京信息科技大学、珠海金智维人工智能股份有限公司、湖南创博龙智信息科技股份有限公司、赛韵网络科技（上海）有限公司、广西财经学院、西安咸林能源科技有限公司、护航科技股份有限公司、赛西（深圳）电子信息产品标准化工程中心有限公司、深圳市标准技术研究院、广州赛宝认证中心服务有限公司、深圳市优讯信息技术有限公司、中国联合网络通信有限公司深圳市分公司、北京海鹰科技情报研究所、中国司法大数据研究院有限公司、青岛立卓智高咨询服务有限公司。

本文件主要起草人：张明英、郭鑫伟、尹正茹、宋俊典、黄胜华、叶康涛、孙勉、张绍华、杨震、俞文平、朱俊伟、杨琳、肖筱华、刘瑞慧、陈泽佳、吴恩龙、梁瑛、郑晨光、杨舸、李京、孙佩、聂兴凯、周庭梁、李世喆、张小军、杨泉、张树玲、刘颋、薛科、王会、郭浩、温利峰、田春惠、马添、吕艳、蔡毅、郝冠亚、袁龙、侯觅、唐剑飞、于海阳、王巍、戴炳荣、郭锐、徐飞、马烈、陆兴海、李良芳、王华、梁晓雁、戴鹏、尹瑞平、高艳炫、廖崇阳、冷威、徐仁彬、董雷、张飞、龚贤夫、李春梅、单小虎、金春华、李晶、田一、柏志建、李建良、廖万里、唐泽诚、高泱、李耀东、刘芳、陈文生、彭穗、钱伟峰、胡佳琳、朱永佳、王中华、徐煦、夏婷婷、曾立军、王海峰、张兴、职亮亮、赖成宇、于浩。

本文件及其代替文件的历次版本发布情况为：

——本文件于2017年首次发布；

——本次为第一次修订。

引　言

随着数字化、智能化技术的深度渗透与融合应用，各行业、各领域的信息化发展已迈入数智化转型新阶段。信息技术日益成为组织重塑核心竞争力、驱动业务模式创新、释放数据要素价值的关键引擎。有效的信息技术治理，是确保信息技术战略与组织总体战略有机统一、实现价值交付、管控系统性风险、满足合规性要求的根本保障。

本次修订旨在适应数字化转型、数据要素化及人工智能等发展带来的新挑战，借鉴国内外最新治理理念和实践成果，将信息技术治理的定位从指导信息技术的有效应用，提升为全面支撑组织数智化转型的治理框架。引导组织建立更具前瞻性、适应性和系统性的信息技术治理体系，助力组织在复杂多变的环境中，敏捷响应技术变革，有效驾驭数智化风险，持续创造业务价值，从而实现高质量、可持续发展。

GB/T 34960《信息技术服务 治理》由五部分构成。

——第 1 部分：通用要求。目的在于提出信息技术治理的通用要求，明确信息技术治理的原则、模型、过程和要素等，指导组织信息技术治理体系的建立、评价和改进。

——第 2 部分：实施指南。目的是为组织提供信息技术治理方法与框架，指导信息技术治理的规划、执行和优化。

——第 3 部分：绩效评价。目的在于指导组织建立信息技术治理的绩效评价模型，明确绩效评价方法和评价指标的建立程序，使组织能够定量或定性地评价信息技术及其应用的绩效。

——第 4 部分：审计导则。目的在于指导组织建立信息技术审计体系，加强信息技术在审计领域应用的治理，规范信息系统审计，以完成组织的信息技术治理目标。

——第 5 部分：数据治理规范。目的是为各类组织提供数据治理框架，指导组织进行数据治理的顶层设计，对治理域中的数据管理体系、数据价值体系进行治理，并对数据治理过程进行规范。

GB/T 34960.2—2017 发布实施已近十年，与信息技术服务治理有关的理论研究和实践以及国家标准都发生了变化。首先，信息技术服务治理原理与方法研究不断深入，逐步建立起以治理要素为基础、以治理域为载体，依托治理阶段和治理活动驱动闭环，构建组织治理实施方法。其次，随着信息技术服务治理实践的逐渐深入以及新技术的应用，新的治理需求不断产生。鉴于此，确有必要修订完善 GB/T 34960.2—2017，以不断适应国内外相关标准的新变化以及信息技术服务治理实践发展的新需求，确保支撑信息技术服务治理工作的国家标准体系整体协调。

本次对 GB/T 34960.2—2017 的修订，重点考虑了信息技术服务治理的实施方法和框架，明确了治理主体的组建、职责与机制，并进一步清晰地提供了治理规划、执行和优化阶段的实施指引。通过确立实施方法和框架，让实施信息技术服务治理时有据可依，从而提高实施的质量和效率，更好地促进信息技术服务交付、技术交流及合作。

信息技术服务 治理 第2部分：实施指南

1 范围

本文件描述了信息技术治理（以下简称：IT治理）的实施方法，确立了IT治理实施框架与主体，提供了IT治理实施规划、执行和优化的指南。

本文件适用于：

——组织内部开展IT治理的实施；

——IT治理相关软件或解决方案实施落地的指导；

——第三方开展IT治理评价的指导。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34960.1 信息技术服务 治理 第1部分：通用要求

GB/T 34960.3 信息技术服务 治理 第3部分：绩效评价

3 术语和定义

GB/T 34960.1界定的术语和定义适用于本文件。

4 治理实施方法

治理实施方法以评估、指导和监督活动为主要活动，以治理要素为管控内容，以治理域为对象，按照治理规划、治理执行、治理优化三个阶段，指导治理实施工作，见图1。

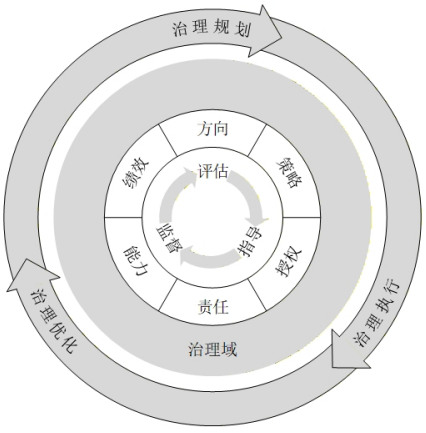

图 1 IT 治理实施方法

图 1 中“评估—指导—监督”部分与其他部分的关系说明如下：

a） 评估：通过评估各要素运行现状，识别偏差和风险，为后续治理工作提供评估结果；

b） 指导：结合治理规划与评估结果，完善治理制度体系与实施策略，明确各治理要素管控内容，为治理实施提供指导；

c） 监督：动态监控各治理要素，核验治理成效，确定风险、偏差和改进事项，并将监督结果反馈至治理优化阶段。

5 治理实施框架

基于第 4 章规定的治理实施方法，组织组建治理主体，明确其职责和机制。治理主体承担评估、指导和监督职责，分阶段对治理域进行治理实施，见图 2。

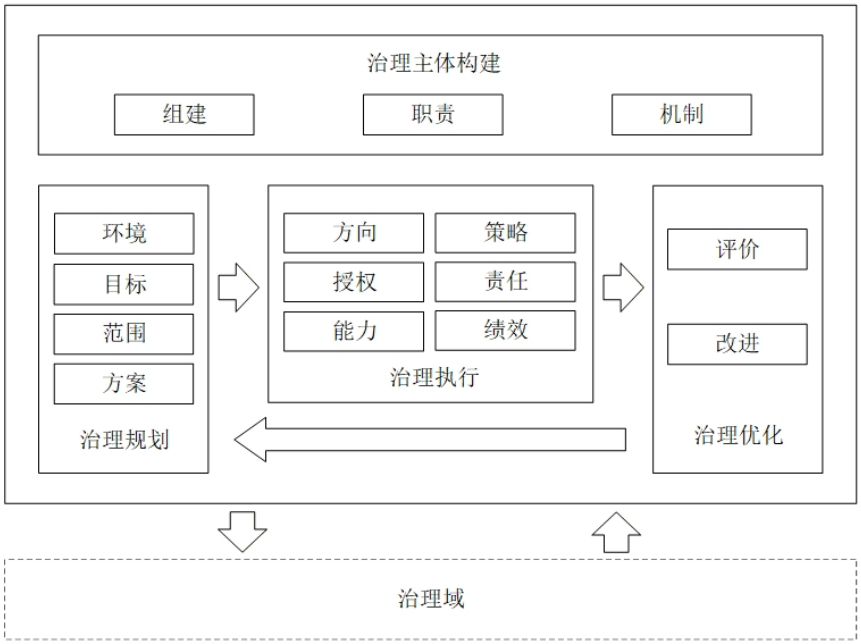

图 2 IT 治理实施框架

治理实施过程包括治理规划、治理执行和治理优化三个阶段：

a） 治理规划：对治理实施进行策划，通过环境分析、驱动力和利益相关方识别，确定治理目标和范围，识别治理域，形成治理方案；

b） 治理执行：在治理规划基础上，执行治理方案，围绕方向、策略、授权、责任、能力、绩效六项治理要素开展评估、指导、监督活动；

c） 治理优化：对组织治理实施工作情况进行评价，识别偏差并持续改进。

人工智能治理作为治理实施的应用示例参见附录 A。

6 治理主体构建

6.1 概述

组织宜结合治理目标和利益相关方期望，组建治理主体，分配职责和权限，并建立运行机制。治理主体行使评估、指导和监督职能，对组织 IT 使用的绩效和合规承担最终责任。

6.2 组建

组织宜在开展 IT 治理实施前，组建治理主体。组建宜考虑治理主体需求、组建方式以及定期评估：

a） 治理主体组建的考虑因素包括：
   1） 组织战略规划和业务发展的要求；
   2） 组织的特征，如组织规模、服务范围和复杂度、服务模式、服务能力、供应关系等；
   3） 治理目标、价值要求和风险管控；
   4） IT 全生存周期活动的治理需要；
   5） 利益相关方参与治理的需要。
b） 采用设立专门机构或依托现有机构或建立跨部门机构等方式组建；
c） 定期评估治理主体，并在内外部环境发生重大变化时及时评估，必要时进行调整。

6.3 职责

组织宜沟通并确定治理主体的相关职责和权限，厘清其与业务管理、风险合规、数据管理、信息安全等各类管理工作的分工边界，形成可获取的文件化信息，并在组织内传达。治理主体的层级、职责和权限宜包括：

a） 决策层提出治理要求，审定治理方向、策略和目标，审批重大事项（包括重大决策、重大投入、重要变更等）；
b） 执行层将治理要求转化为治理相关的制度、流程和衡量指标，并开展治理活动；
c） 监督层独立开展合规检查和成效核验活动，并督促整改。

6.4 机制

组织宜建立、实施、保持并持续改进治理主体的运行机制，并使运行机制与组织运营模式、监管要求相匹配。运行机制可包括：

a） 决策机制，如议事规则、决策程序、审批授权机制等；
b） 执行机制，如治理评估、工作指导、监督检查机制等；
c） 协作机制，如工作流程、沟通协同、信息报告机制等；
d） 管控机制，如重大事项审批与监管机制、风险治理机制、问责机制等。

7 治理规划

7.1 概述

在治理规划阶段，治理主体宜通过环境分析，识别治理的驱动力和利益相关方，明确治理目标，确定治理域，制定涵盖治理组织架构、运行机制、实施计划、保障措施等内容的治理方案。

7.2 环境

7.2.1 内外部环境

治理主体宜对内外部环境进行分析，考虑因素包括：

a） 法律法规与政策；
b） 国内外经济形势与市场环境；
c） 高新技术变革与重大技术创新；
d） 人工智能、云计算等新技术应用的安全风险；
e） 内外部审计、监督、评估的要求；
f） 组织的 IT 供应链生态；
g） 组织的业务现状与发展规划；
h） 组织的技术资源储备与治理能力。

7.2.2 驱动力

治理主体宜基于环境分析的结果，识别并明确治理的驱动力，考虑因素包括：

a） 组织战略规划和业务发展的要求；
b） 风险管控的要求；
c） 利益相关方诉求及其优先级；
d） 技术变革与创新驱动；
e） 成本优化与价值创造的要求；
f） 治理框架优化的要求；
g） 与组织文化、愿景、价值观相一致的要求。

7.2.3 利益相关方

治理主体宜识别并明确治理的利益相关方，考虑因素包括：

a） 利益相关方的责权利；
b） 利益相关方的支持程度；
c） 利益相关方对治理过程的作用；
d） 治理过程对利益相关方产生的影响。

7.3 目标

7.3.1 治理目标

治理主体宜结合组织的战略目标确定治理目标，考虑因素包括 ：

a） 战略对齐：治理能支撑业务战略的实现；
b） 价值交付：治理能实现预期价值，并控制相应成本；
c） 风险管理：识别并控制治理的相关风险，满足安全合规和业务连续性要求；
d） 资源优化：高效整合与利用 IT 资源；
e） 绩效度量：通过指标监控和评估治理绩效。

7.3.2 需求分析

治理主体宜按照下列步骤分析治理需求：

a） 综合分析 IT 的核心诉求、合规要求、预算边界和可接受的创新风险，形成治理需求基线；

b） 梳理现有 IT 资源和内部能力，识别能力短板与冗余；
c） 将现有资源和能力与治理需求基线进行对标，识别与治理目标的偏差及治理方向；
d） 梳理利益相关方的核心诉求；
e） 分析各类需求对业务的影响程度、实施的紧迫程度和难易程度，建立需求优先级排序规则；
f） 建立需求跟踪与持续改进机制。

7.4 范围

治理主体宜基于治理目标和治理需求分析结果，按照下列步骤确定治理范围：
a） 将治理目标逐层拆解为关键能力要求，评估当前 IT 能力的满足程度，识别存在能力缺口且计划重点建设或优化的治理对象；
b） 分析现有 IT 能力中的问题点和风险点，归纳出治理对象；
c） 结合组织所属行业特征、经营规模及现有治理水平，梳理出治理对象涉及的治理域；
d） 分析治理域之间的依赖和协同关系，确定治理范围，并通过利益相关方的确认；
e） 建立治理范围动态调整机制，根据内外部环境变化及时变更治理范围。

7.5 方案

治理主体宜根据治理目标，明确职责、机制、流程、活动和计划，并评估治理实施的风险与阻力，形成治理方案。治理方案宜包括下列内容：
a） 治理主体的职责、人员要求等；
b） 决策、授权、沟通、绩效评价、监督、持续改进等机制；
c） 利益相关方及其沟通参与策略；
d） 遵循治理过程、覆盖治理要素的治理实施流程；
e） 治理实施计划，覆盖时间安排、主要任务、阶段目标、职责分工、资源需求等内容；
f） 治理过程中潜在的风险和机会，及其应对措施和预案；
g） 治理过程中所需的保障措施及其有效性评估机制，保障措施覆盖组织、人力、技术、资金、机制、安全等方面。

8 治理执行

8.1 概述

治理主体宜在治理执行过程中，遵循治理方案开展工作，围绕治理要素对确定的治理域进行评估、指导和监督。

8.2 方向

8.2.1 评估

治理主体宜评估治理方向与治理域的适配性、可行性、可追溯性，以及伦理风险，评估步骤宜包括：
a） 收集组织战略、业务规划、监管要求、风险偏好、利益相关方诉求、内外部环境变动、行业技术趋势、IT 架构现状、数字化能力现状，形成治理方向台账；
b） 将治理方向与组织战略、业务目标、行业最佳实践、监管细则逐项分析，识别 IT 持续服务和创造价值的方向与治理目标的适配性、可行性和可追溯性，并形成差异分析结果，分析维度包括：

1） 适配性：评估治理方向与组织战略的适配性，分析当前 IT 定位、价值导向的偏离程度；
2） 可行性：评估人力、预算、技术、周期约束下的目标落地概率，识别资源不足、技术瓶颈、跨部门协同障碍等风险；
3） 可追溯性：记录治理方向偏差的具体表现、触发环节、影响范围、关联业务域等。

c） 评估人工智能伦理风险：

a） 梳理人工智能应用场景，对照伦理原则逐项核查；
2） 识别数据滥用、算法偏见、隐私泄露、安全失控等伦理风险点，输出伦理风险评估报告。

8.2.2 指导

治理主体宜基于治理规划和评估结果，输出可执行、适配的治理方向，执行步骤宜包括：

a） 校准阶段方向：依据评估结果与战略调整，确定治理域的各阶段治理方向，形成经过审批的阶段方向文件；
b） 明确阶段治理目标：
1） 基于阶段治理方向，明确可测量、可执行、可验证的阶段 IT 治理目标，确定长期路线、中期目标、年度重点，并与组织战略、能力目标对齐；
2） 分解目标达成的量化指标、时间节点、责任部门、验收标准等。
c） 明确 IT 定位：结合 IT 对组织发展的影响、业务对 IT 的需求、价值产生模式，界定 IT 的战略定位、价值贡献边界、核心能力建设清单、服务支撑模式等，明确 IT 提供持续服务和创造价值的方向；
d） 规划 IT 投资方向：围绕治理方向和 IT 定位，确定 IT 投资的优先级；
e） 确定 IT 投资预算：基于 IT 的价值导向和投资优先级，聚焦核心业务数字化、关键技术升级、安全能力建设、治理体系完善、人工智能伦理保障等领域，编制年度 IT 投资预算，明确资金分配比例、重点项目清单、投入产出预期等；
f） 制定人工智能伦理规范：
1） 依据监管要求，制定人工智能应用伦理原则与规范；
2） 明确增进人类福祉、尊重生命权利、公平公正、风险可控、公开透明、隐私安全、可控可信等人工智能伦理原则；
3） 将人工智能伦理要求嵌入人工智能应用全生命周期，形成监督与执行细则。
g） 规范管理机制：依据 IT 治理方向管理机制，规范执行信息收集与分析、治理方向设计、部署实施、定期评审与优化的相关活动，留存归档过程文件；
h） 编制成果文件：编制 IT 治理章程、治理方向及人工智能伦理指引性等文件，成果性文件发布至各部门，并形成全员统一认知。

8.2.3 监督

治理主体宜动态监控治理方向执行情况，响应重大变化并纠偏优化，监督检查宜包括：

a） 建立监督检查全流程：
1） 依据 IT 治理方向管理机制，覆盖方向制定、边界裁剪、目标落地、投资执行、伦理治理、迭代调整全环节，开展自查、专项检查和年度审计；
2） 核查各治理域运行的合规性、目标达成情况，形成监督检查报告。
b） 校验动态一致性：动态校验治理方向、目标、原则与组织战略、业务目标、能力目标、监管要求的一致性，对比评估数据，识别偏差并记录；

c） 响应重大变化：当外部环境、组织战略、监管要求、行业技术发生重大变化时，启动方向校准审批流程，重新开展评估、修订方向、调整目标、更新路径；动态优化治理体系，形成重大变更专项报告；

d） 监督人工智能伦理执行：

1） 跟踪人工智能应用全生命周期伦理执行效果；

2） 核查数据合规、算法公平、隐私保护、安全可控、透明可解释等要求落实情况；

3） 对伦理偏差问题进行整改。

e） 纠正与优化：

1） 对发现的方向偏离、目标未达成、执行不到位、伦理不合规等问题，分析根因，制定整改措施，明确整改时限，跟踪整改效果；

2） 整改完成后更新治理文件、优化管理机制，形成闭环管理。

8.3 策略

8.3.1 评估

治理主体宜评估治理策略体系的一致性、合规性、完整性、可执行性、执行规范性、专项适配性，识别外部要求可控性与偏差问题，评估内容宜包括：

a） 评估治理策略体系：将治理策略与治理方向进行对比分析，并形成差异分析结果，分析维度宜包括：

1） 一致性：评估治理策略与治理方向、组织战略、业务目标、治理目标的一致性，识别偏差；

2） 合规性：依据行业监管要求及治理章程，评估策略的符合性；

3） 完整性：评估价值导向、指导原则、行动框架、决策规则等策略层级的完整性；

4） 可执行性：评估策略在市场、项目、资源、风险、利益相关方等维度行动准则的覆盖度、可执行性；

5） 执行规范性：评估策略参数、版本管理、变更及废止机制的规范性、可追溯性；

6） 专项适配性：评估新兴技术、新型架构、通用组件、安全管控等专项策略的适配性、时效性与完备性。

b） 评估外部要求可控性：评估外部供方、合作方、外包机构执行策略的约束有效性、可追溯性与风险可控性；

c） 识别偏差与问题形成基线：识别策略滞后、不适配、冲突、空白等问题，形成策略评估报告与优化基线。

8.3.2 指导

治理主体宜基于治理规划和评估结果，通过策略构建、资源统筹、规则适配、变更管控、参数量化、冲突处置等策略的全周期管理，输出可执行、可验证的策略指引，执行步骤宜包括：

a） 锚定顶层关系：明确治理策略与治理目标、治理方向、组织战略的对应关系，确定治理策略的顶层设计；

b） 建立策略体系：建立顶层策略、专项策略、行动细则的分层治理策略体系，并规范治理策略体系的版本管理、发布审批、更迭记录等；

c） 统筹资源配置：以业务价值为核心，统筹传统 IT 资源与新型信息化资源配置，动态调整策略体系，并分层落实至各治理域；

d） 制定行动准则：围绕市场、项目、资源、风险、利益相关方等维度，制定统一行动准则与场景化执行规则，明确跨部门协同边界、责任与流程；
e） 明确变更规则：明确策略变更触发场景、发起主体、启动条件与审批流程，建立变更管控规则；
f） 标准化治理参数：制定标准化、可度量的治理参数，明确参数与业务迭代、技术演进、风险变化的适配规则；
g） 规范专项策略：划定新兴技术、新型架构、通用组件、安全管控等专项策略范围，统一专项策略编制、评审、发布与维护；
h） 明确冲突处置流程：明确策略冲突识别、研判、处置流程，规范新旧策略、跨领域策略的冲突管理与协调；
i） 确保执行统一：明确策略的传达途径、适用范围以及对治理主体及利益相关方的执行约束，统一各方认知与执行标准；
j） 规范管理机制：实施策略全生命周期管理，规范修订、审批、发布、生效、执行、监督、验证、废止的相关活动，留存归档过程文件；
k） 编制成果文件：编制治理策略文件，包括但不限于各阶段治理行动准则或方针、专项治理准则等。成果性文件发布至各部门，形成全员统一认知。

8.3.3 监督

组织宜动态监控策略落实情况，预警、纠偏并持续迭代，监督检查宜包括：

a） 建立监督检查全流程：
   1） 依据策略管理机制，覆盖策略宣贯、规则落地、参数执行、变更管控、冲突处置、版本管理等环节，开展定期检查、专项核查和年度评审；
   2） 核查各治理域策略执行情况，形成监督检查报告。
b） 校验动态一致性：
   1） 定期校验策略体系、层级架构、行动准则、治理参数与治理方向、组织战略、业务目标、监管要求的一致性；
   2） 识别策略滞后、不适配、冲突、空白问题并记录，持续适配组织治理需求。
c） 响应重大变化：当监管要求、业务模式、技术架构发生重大变化时，启动策略校准审批流程，重新开展评估、修订体系、调整规则、更新参数；动态优化治理策略，形成重大变更专项报告；
d） 纠正与优化：
   1） 对监督中发现的执行偏差、规则失效、适配不足、合规风险等问题，分析根因，制定整改措施，明确整改时限，跟踪整改效果；
   2） 整改完成后更新策略文件、完善管理机制，形成闭环管理。

8.4 授权

8.4.1 评估

治理主体宜识别授权体系现状、边界、风险，开展一致性、完整性、合规性、匹配性、可追溯性等多维度的授权体系评估，评估内容宜包括：

a） 将授权体系与组织治理架构、权责体系、权限配置等进行对比分析，分析维度宜包括：
   1） 一致性：对比授权架构、分级权限、责任划分与组织架构、组织战略、治理方向、风险偏好等的一致性；

2） 完整性：对比岗位、系统、数据、功能、决策、接口、跨治理域等授权边界的覆盖情况；
3） 合规性：核查权限配置是否符合最小权限、权责对等、职责分离、数据安全、隐私保护要求；
4） 匹配性：权限设置与业务复杂度、风险等级、组织规模等因素的匹配性，与授权相关的监督、审计、追责机制匹配性；
5） 可追溯性：授权申请、审批、变更、回收、审计全流程可追溯程度。

b） 评估过度授权、权限冗余、权限外溢、自动化决策权限失控、不当跨生态授权等风险。

8.4.2 指导

治理主体宜根据治理规划和评估结论，完善授权制度、定义与划分授权架构并指导新技术授权的管控，执行步骤宜包括：

a） 确立授权原则：确立并发布授权基本原则，包括战略对齐、权责对等、最小权限、职责分离、可监督、可追溯、动态适配；
b） 设计分级授权架构：建立决策、执行、监督三级授权清单，明确授权层级、权限范围、决策边界、审批权限、责任边界等相关内容；
c） 制定域级授权规则：按治理域明确授权事项、权限分级、审批流程、操作规范、留痕要求、异常升级路径等；
d） 建立动态权限管理：权限与岗位职责、业务需求、风险等级动态联动，定期清理冗余、回收闲置、调整失衡权限；
e） 管控新技术与自动化授权：遵循“先授权、后上线”原则，严格控制自动化、智能化功能授权，关键高风险操作保留人工复核；
f） 规范跨生态授权：对利益相关方，如供应商、合作方、监管方等，授予必要最小权限，限定并控制范围、期限、用途、数据访问边界；
g） 建立管理机制：建立并实施需求识别、方案设计、申请审批、授权实施、变更管控、回收注销、审计追溯、风险处置等授权管理机制；
h） 编制成果文件：编制授权清单、审批流程、权限变更规范、追溯记录的标准化授权文件，或固化在 IT 系统中，统一发布并执行。

8.4.3 监督

治理主体宜对授权的执行、风险、效果及持续改进等内容进行监督，监督检查宜包括：

a） 建立监督检查全流程：
1） 覆盖权限配置管理、申请审批、变更回收、跨生态授权、新技术授权、日志记录、留痕追溯等环节，开展定期检查、专项核查和年度评审；
2） 核查各治理域权限执行情况，形成监督检查报告。

b） 动态校验权限匹配度：
1） 定期校验已授权权限、岗位职责、授权文件、治理目标、监管要求的一致性；
2） 核对实际权限与岗位职责的匹配度，清理冗余、回收闲置、纠正错配权限；
3） 识别越权、权限外溢、配置失效等问题并记录。

c） 响应重大变化：
1） 当组织架构、业务流程、技术架构、监管要求、战略发生重大变化时，启动授权校准审批流程；

2） 重新开展评估、调整架构、更新并固化权限、优化管控规则；
3） 动态优化授权体系，形成重大变更专项报告。

d） 纠正与优化：
1） 重点监督高权限账号、自动化工具、跨生态访问、智能化授权决策行为，设置异常告警并处置；
2） 对权限滥用、越权、配置不当、流程缺陷、权限配置失效等问题，分析根因，制定整改措施，明确整改时限，跟踪整改效果；
3） 整改完成后更新授权文件、完善管理机制、优化系统配置、落实追责问责，形成闭环管理。

8.5 责任

8.5.1 评估

治理主体宜评估治理责任偏差，以及对责任配置和履行现状开展一致性、匹配性、完整性、有效性的评估，评估内容宜包括：

a） 评估责任偏差：评估越权、失职、渎职、责任悬空、权责错配、追责不严、追溯失效等偏差；
b） 评估履职情况：将责任配置和履行现状进行对比分析，分析维度宜包括：
1） 责任一致性：责任体系与组织架构、业务流程、技术架构、治理目标、风险事件、监管要求等的一致性；
2） 责任完整性：各治理域、关键岗位、核心活动的责任配置覆盖情况，识别责任空白、交叉、重叠、模糊等问题；
3） 权责匹配性：评估决策层、执行层、监督层的职责边界、责任类型、协同关系与治理目标、授权范围、岗位职责的匹配性；
4） 履职有效性：评估履职与协同的有效性，识别缺位、推诿、敷衍、协同失序、责任悬空、履职不到位等问题。

8.5.2 指导

治理主体宜基于治理规划和评估结果，对治理责任的分配、履行、协同、调整、问责等事项做出安排，执行步骤宜包括：

a） 确立责任原则：确立并发布责任基本原则，包括权责对等、一岗双责、履职留痕、协同配合、失责必追等；
b） 构建责任矩阵：构建全域责任矩阵，明确各治理域的关键活动，明确核心岗位的责任主体、协同关系等；
c） 规范履职标准：明确履职时限、工作流程、操作规范、成果交付、留痕要求、异常升级路径等；
d） 建立协同责任机制：界定跨部门、跨岗位、跨域协同责任边界、配合要求、沟通机制、争议处置规则等；
e） 设置并更新责任规则：明确责任要求、履职标准及跨主体协同细则，根据组织架构变革、业务迭代、技术升级与治理目标变化，实施动态更新；
f） 设置问责与追溯规则：明确问责触发条件、责任认定标准、处置措施、追溯流程、记录规范、结果应用机制；

g） 编制成果文件：编制责任清单、履职手册、协同规范、问责细则、追溯记录模板，统一发布并执行。

8.5.3 监督

治理主体宜对治理责任履行和整改情况进行监督检查和改进，监督检查宜包括：

a） 建立监督检查履职情况：
   1） 依据责任管理机制，定期开展履职检查，覆盖责任配置、履职执行、协同配合、异常处置、留痕记录、追溯归档各环节，开展定期检查、专项核查和年度评审；
   2） 核查各治理域的责任履行情况，形成监督检查报告。

b） 动态校验履职一致性：
   1） 采集职责履行数据，定期校验责任配置、履职行为、履职成果、授权范围、治理目标、协同要求的一致性；
   2） 识别缺位、推诿、越权、协同失序、责任悬空、履职不到位等问题并记录。

c） 响应重大变化：
   1） 当组织架构、业务流程、治理目标、技术架构、风险事件、利益相关方需求等发生重大变化时，启动责任校准审批流程；
   2） 重新开展评估、调整边界、更新要求、优化协同机制，形成重大变更专项报告。

d） 纠正与优化：
   1） 跟踪责任偏离情形、问责落实情况、整改措施落实情况及整改结果，对履职不到位、责任偏离、协同不畅、整改不力、追责不严等问题，分析根因，制定整改措施，明确整改时限，跟踪整改效果；
   2） 整改完成后更新责任文件、完善管理机制，形成闭环管理。

8.6 能力

8.6.1 评估

治理主体宜识别治理能力需求、评估能力现状与差距，形成能力视图，评估步骤宜包括：

a） 识别内外部能力需求：理解内外部环境、利益相关方期望和组织文化，洞察组织战略和业务需求，评估战略、业务、监管、技术、风险、利益相关方期望等，明确能力总体需求；

b） 盘点能力现状：评估现有能力水平，包括管理、技术、安全、风险、数据、工具、人才、流程等；

c） 分析能力差距：对比治理需求与能力现状，识别能力短板与瓶颈，评估能力与治理目标、管控范围、业务规模、数字化成熟度、风险等的匹配性，并结合业务发展阶段与组织战略需要，形成能力建设范围；

d） 确定能力优先级：结合价值、风险、紧迫性、资源约束等，确定能力建设优先级；

e） 形成能力视图：明确能力建设、共享、复用或获取方式，形成当前及未来所需能力视图。

8.6.2 指导

治理主体宜基于治理规划和评估结果，聚焦战略落地所需治理核心活动要素，构建分级分类、差异化的能力体系，指导并形成能力建设策划，执行步骤宜包括：

a） 构建能力框架：基于能力视图，构建支撑治理与管理所需的能力要素，并在决策层、监督层和执行层上形成能力框架，整合内外部资源进行能力协同，确定能力目标与建设路径；

b） 确定核心能力要素要求：明确各治理域的核心能力要素的要求，包括能力等级、达标标准、衡量指标等，形成能力管理的基础；
c） 策划能力建设：制定短期、中期、长期能力建设计划，明确核心能力要素提升目标、任务分解、任务实现方式、责任人与协同人、时间安排、资源保障、IT 部署、人才培养和沟通协调等事项；
d） 实施能力建设：依据当期治理重点、风险等级、资源投入等，按计划推进能力建设，并根据治理范围、管控强度、业务需求的变化情况，动态提升组织能力；
e） 保持利益相关方沟通：在能力识别、构建和评估的全过程中，与利益相关方保持沟通，就目标、方案、进展及成效收集其理解、支持和反馈的意见；
f） 采用智能化工具：以智能化工具为核心赋能手段，统筹部署并迭代策略引擎、监控平台、人工智能治理组件与自动化流程工具，依托智能化能力，减少重复性人工操作；
g） 规范管理机制：规范实施能力管理机制，包括能力识别、评估、构建、监督、优化的相关活动，留存归档过程文件；
h） 编制成果文件：编制能力管理计划、能力指标体系、能力指标达成情况跟踪、能力实施情况报告、履职手册、协同规范等文件，将成果性文件发布至各部门。

8.6.3 监督

治理主体宜动态监控能力落地效果、目标匹配度与业务价值转化，监督能力绩效达成情况及能力满足状态，纠偏并持续迭代。监督检查宜包括：

a） 监督检查能力建设情况：定期开展能力执行情况检查，覆盖能力规划落地合规性、任务完整性、执行有效性，形成能力实施报告，内容包括：
   1） 能力建设目标的达成情况；
   2） 能力与治理目标的匹配度；
   3） 能力提升的实际进展；
   4） 能力当前的满足状态；
   5） 未达标的环节及待解决的问题。
b） 动态校验与监测能力：
   1） 定期校验能力建设目标、能力落地成效与组织战略、治理目标、业务目标、技术迭代、监管要求的一致性；
   2） 监督能力绩效达成情况及能力满足状态，采集能力落地运行数据，分析能力建设对治理目标、管理要求、业务价值转化和风险防控成效的支撑情况，识别能力低效滞后、资源错配、支撑不足等问题并记录。
c） 响应重大变化：当组织战略、治理目标、业务范围、技术环境、监管要求或风险状况发生重大变化时，启动能力落地校准审批流程，重新开展能力评估，优化能力框架，调整能力策划，形成重大变更专项报告；
d） 纠正与优化：
   1） 针对能力低效滞后、资源错配、支撑不足、目标偏离等问题，开展根因分析，制定落地整改方案，明确整改时限，跟踪落地成效；
   2） 整改完成后更新相关文件，调整资源配置，并持续提升能力。

8.7 绩效

8.7.1 评估

治理主体宜收集绩效信息，开展绩效体系适配性、完整性、合理性评估，评估步骤宜包括：

a） 收集绩效相关信息：收集组织战略、治理目标、业务目标、监管考核、内控合规、运营数据、人工智能落地成效、各治理域绩效数据及利益相关方期望等信息，并动态更新绩效基准；

b） 分析绩效现状：对标治理落地现状与绩效管控需求，核查现有考核口径、指标覆盖、目标值，梳理指标缺失、口径不统一、权责与绩效错配等问题，形成差异清单；

c） 评估绩效体系：对绩效体系运行现状进行对比分析，分析维度包括：

1） 适配性：评估绩效框架与治理方向、治理目标、授权规则、责任划分、能力建设、组织结构、业务发展和核心价值的匹配程度，明确治理绩效管控边界与核心导向，保持绩效导向与组织发展一致；

2） 可行性：结合绩效数据采集条件、系统支撑能力、人员配置现状、组织授权范围和跨域协同条件，评估绩效落地实施难度，识别数据缺口、系统短板、跨域考核协同障碍等风险，形成风险清单；

3） 可控性：评估绩效指标是否支持量化取值、动态监测及异常预警，管控绩效过程。

d） 复盘历史绩效：汇总历史绩效达成数据、偏差事项、整改记录、资源配置调整情况和奖惩问责结果，留存过程记录，分析偏差原因并总结经验，并更新绩效基准、指标阈值和考核规则。

8.7.2 指导

治理主体宜建立绩效基准与实施规则，通过指标构建、分解目标、规则标准化、系统固化形成可执行、可量化、可验证的绩效管控文件，执行步骤宜包括：

a） 设计绩效机制：依据治理目标和评估结果，进行绩效全周期管理，明确绩效管控原则、绩效指标设置、监测指标、预警机制、绩效信息收集与分析、预警与改进、绩效结果应用等要求；

b） 建立全域绩效体系：面向治理域，围绕治理目标和治理要素，建立绩效体系，明确绩效指标、统计口径、计算逻辑、数据来源、基线阈值、权重配比、责任主体等内容；

c） 明确分级管控机制：结合组织架构、授权边界、岗位职责、各治理域业务特征，建立绩效指标分级管控机制，分级设定绩效目标和考核频率，差异化配置组织、部门、岗位及相关责任主体的考核指标，绩效指标责任到人，并与授权、责任体系保持一致；

d） 明确指标类型和要求：绩效指标体系包括治理自身衡量指标、IT 运营管理指标、IT 性能衡量指标等，指标设置具备可量化、可监测、可预警性，并支撑绩效评价、绩效分析和绩效改进；

e） 遵循监管要求：遵循相关监管要求，将数据安全、科技伦理、风险整改等要求纳入绩效评价，并贯穿绩效管理全过程；

f） 明确考核细则：明确考核计分标准、达标判定条件、例外事项处置规范、申诉管理要求等内容；

g） 智能化绩效管理：将指标参数、考核规则、预警阈值、数据采集规则和结果输出规则内嵌固化至智能化治理引擎，依托智能化能力，刚性执行规则、自动运算、动态监测和实时预警；

h） 落实绩效应用：以绩效考核结果为依据，合理配置资源、落实奖惩问责，持续迭代绩效要素与考核体系；

i） 编制成果文件：编制绩效管理文件、绩效考核文件等，将成果性文件发布至各部门，并形成全员统一认知。

8.7.3 监督

治理主体宜动态监控绩效落地执行与指标达成，纠偏并迭代优化，监督检查宜包括：

a） 建立监督检查全流程：

1） 依据绩效管理制度开展阶段自查和考评，覆盖指标运维、目标落地、数据采集、系统核算、考核应用等环节；

2） 核查治理域绩效执行合规性、数据真实性、指标达成水平、责任落实情况和结果应用情况，形成绩效监督报告。

b） 动态校验适配性：定期校验绩效指标、考核目标与组织战略、治理方向、权责配置、能力建设要求、监管合规要求和业务发展变化的适配性，对照绩效基准识别指标滞后、目标偏离、口径失效等问题并记录；

c） 响应重大变化：组织结构、战略方向、业务目标、监管政策、内外部环境或治理目标重大调整时，启动绩效校准审批流程，重新开展评估、修订指标、优化目标、更新系统配置，形成重大变更专项报告；

d） 绩效异动预警管控：根据绩效规则自动化运算结果，对异常指标和重大风险预警，从策略落地、履职执行、资源保障、能力配套、智能赋能等维度分析绩效未达标根因，对重大绩效风险触发预警并跟踪处置；

e） 纠正与优化：

1） 针对指标不达标、规则不合理、执行偏差等问题，开展根因分析，制定整改方案，明确整改责任、整改措施和整改时限，验证实施效果；

2） 结合整改成果、绩效监测结果与年度治理变化，迭代指标、目标阈值、考核规则、预警机制和结果应用方式等。

9 治理优化

9.1 概述

治理主体宜搭建治理体系常态化评价与改进机制，结合治理实施过程运行状态、治理成效反馈信息，对治理的方向、策略、授权、责任、能力、绩效进行系统性优化，保持治理体系与业务发展的动态适配状态。

9.2 评价

9.2.1 治理主体宜定期开展治理体系综合评价，排查治理规划、体系设计落地执行环节的差距、短板及潜在风险。

9.2.2 评价由治理主体或其授权职能机构落地实施，评价结果报送决策层；重要治理事项可委托第三方机构开展独立评价。

9.2.3 综合评价宜不少于每年一次；治理体系发生重大变更后开展专项评价；对核心治理指标实施常态化动态监测。

9.2.4 评价指标体系宜综合运用指标测量、数据分析、访谈问卷、专家评审等方式，依据 GB/T 34960.3 并结合组织实际情况构建。评价内容宜覆盖下列方面：

a） 战略目标达成性：核查业务战略的达成情况及治理实施全过程，评估治理工作与组织整体业务战略的对齐深度、核心业务需求的匹配程度，并据此评估治理对战略目标实现的实质贡献，优化战略目标；

b） 价值交付成效性：核查业务价值的实际体现与治理全流程的成本投入情况，覆盖各类资源成本。对照治理过程规划的成本预算与管控标准，评价成本支出的合规性、合理性与可控性，并综合评估治理过程的整体投入产出效益；

c） 风险管控实效性：复盘治理全流程各类风险处置情况，核对风险识别覆盖完整性、风险研判精准度、防控措施落地效果以及风险处置闭环完成质量，判定组织风险管控能力，优化风险治理机制；

d） 资源利用充分性：核查治理全流程中 IT 全要素资源的整合、调配与利用情况，评估资源配置的合理性、资源共享的协同性以及资源复用的高效性，优化资源配置；

e） 组织绩效达成性：核查治理主体各层级的绩效达成情况，包括各层级绩效指标的运行状况，并验证绩效评价机制本身的科学性与实用性。综合评价治理绩效管理体系的整体效能，优化绩效体系；

f） 治理域完备性：核查治理域识别划分的全面性、分级的合理性、适配的准确性以及运行的规范性，评估治理边界的清晰度，并综合评估治理能力覆盖的广度与深度，优化治理架构与体系；

g） 治理要素执行有效性回顾：复盘方向、策略、授权、责任、能力、绩效等核心治理要素，核查各要素评估、指导与监督全流程的落地情况，结合复盘结果研判整体治理成效，优化各治理要素协同运行机制。

注：评价结论以治理结果的达成情况为核心判断依据，治理要素全过程执行复盘内容作为过程性参考资料，不单独作为最终评价结论的判定依据。

9.3 改进

改进工作按照下列步骤开展：

a） 反馈意见归集：系统汇总治理实施相关内外部反馈信息（包括治理评价结果、治理绩效偏差、内外部审计结果、合规检查、风险事件复盘、利益相关方诉求、外部监管意见，以及数据治理、云治理、人工智能治理等专项领域的运行反馈）。归集范围覆盖决策层、监督层、执行层及全部治理域；

b） 改进事项梳理：对反馈信息及现存问题开展根源分析，梳理治理成效偏差内容，划定具体改进事项。对照治理目标，从战略对齐、价值交付、风险管理、资源优化、绩效度量等维度进行成因研判，结合方向、策略、授权、责任、能力、绩效六项治理要素完成问题归类，并依据影响范围、严重程度划分改进事项优先级；

c） 制定改进计划：根据组织业务发展要求及资源约束，针对高优先级的改进事项，制定改进措施，并落实责任主体、资源需求、完成时限和验收标准。改进内容包括修订治理制度、调整授权规则、优化流程节点、提升人员能力、部署或升级治理工具等；

d） 实施改进措施：按照既定改进计划组织实施，落实责任主体、资源配置与时间节点等要求，统筹改进活动与日常治理运行协调推进；

e） 验证改进效果：对已实施的改进措施进行效果验证，评价其有效性与适宜性。验证方式采用试运行、二次评估或审计复查等。若改进效果未达预期，则重新开展事项分析与方案调整；

f） 赋能反馈：总结改进过程中沉淀的经验，归集典型案例与最佳实践，更新治理规划目标、范围和方案。

附 录 A
（资料性）
人工智能治理示例

A.1 治理目的

人工智能治理宜统筹发展和安全，在促进人工智能创新发展的同时，有效管控其风险，体现社会公平、包容与可持续发展，有利于人类共同福祉。治理目的宜体现下列内容：

——战略对齐：人工智能投资和活动支撑组织业务战略，使人工智能应用与业务目标保持一致；
——价值交付：人工智能系统能够实现预期的商业价值和社会价值，同时有效控制成本；
——风险管理：识别并控制人工智能技术应用的各类风险，满足安全、合规要求与伦理准则，保障业务连续性；
——资源优化：资源整合与充分利用，持续优化人工智能全要素资源（如数据、算法、算力、人才等）；
——绩效度量：监控人工智能应用绩效指标，评估人工智能应用质效和治理绩效，持续改进人工智能系统的运行。

A.2 治理范围

组织可根据人工智能治理需求，界定治理实施范围，治理范围包括：

——全应用场景治理：对内运营（如风控、营销、人力、运维等）、对外服务（如用户交互、客服、推荐等）、产品嵌入（如软硬件集成、行业解决方案等）及高风险场景（如医疗、教育、金融、交通、公共安全等）；
——人工智能系统治理：包括对机器学习、深度学习、大语言模型、生成式人工智能、智能体等的治理；
——全生存周期管理：覆盖人工智能系统从规划、开发、测试、部署、运行、优化、下线各阶段的管控措施；
——全要素资源治理：统筹治理数据合规与质量、算法模型可解释性与公平性、算力效能、人才培养等；
——风险与合规治理：算法安全、数据安全与隐私保护、伦理合规、公平性与无偏见、可解释性、鲁棒性与抗攻击、供应链风险、知识产权与内容合规、人工智能系统可观测性与审计证据留存等。

A.3 治理主体

人工智能治理主体的治理工作要点，包括：

a） 治理主体构建宜考虑战略与业务发展、组织规模与应用复杂度、治理目标、全生存周期治理需要、内外部相关方参与、风险监管要求、技术变革驱动等多种因素。治理主体宜专门设立，依托 IT 治理机构，组织开展跨部门协调。治理主体宜吸纳技术、业务、安全、法律、合规等多元代表，建立跨职能协同机制，确保治理决策的系统性、全面性和连贯性，并明确跨职能团队的议事规则与决策程序。
b） 明确各层级职责与权限，各层级职责与工作内容见表 A.1。

表 A.1 人工智能治理主体各层级职责与工作内容

治理主体	职责与工作内容
治理领导小组 （决策层）	确定治理方向，明确治理策略，审定整体治理规划、专项治理方案、治理标准规范； 统筹协调跨部门治理工作； 审批重大整改事项、资源投入； 审定治理结果与优化方案
专项治理工作组 （执行层）	编制人工智能治理实施细则、年度治理计划； 落实人工智能治理落地、问题排查、整改闭环； 开展治理工作、数据统计、台账管理； 开展人工智能系统伦理审查和算法备案管理工作； 组织培训、自查、复盘等工作； 明确每项治理任务对应的执行人、协同人及汇报路径； 负责人工智能系统的合规评估与持续监测
监督考核组 （监督层）	监督治理全过程合规性、进度真实性、整改有效性； 开展专项审计与个人信息保护合规审计、抽查核验，确保审计覆盖人工智能系统全生存周期，落实治理成效、工作考核、追责问责； 监督治理优化措施落地

c） 建立和完善运行机制：

1） 决策程序、审批权限、报告关系、议事规则；

2） 有效沟通机制，明确跨部门沟通与协同接口；

3） 授权、评估、指导、监督、报告、问责及持续改进机制；

4） 重大事项（模型上线、算力投入、算法变更、风险处置等）审批与监督机制。

A.4 治理工作

A.4.1 治理规划

人工智能治理规划的方案实施要点，包括：

a） 分析内外部环境，分析因素可包括：法律法规与政策、市场环境、技术变革（大模型、多模态、智能体及多智能协同等）、人工智能安全风险、审计监督要求、供应链生态、业务现状与规划、技术资源储备与管理能力；

b） 人工智能现状研判，全面排查人工智能现存问题、短板、风险隐患、合规缺口、发展需要等；

c） 识别治理驱动力，识别因素可包括：战略与业务发展要求、风险管控需求、利益相关方诉求、技术变革驱动、成本优化与价值创造、治理框架优化、企业文化与价值观；

d） 识别相关方及其作用，识别算法使用者、受决策影响的群体、监管机构、模型供应商、数据提供方、内部业务部门等；分析其责权利、诉求、对治理活动的作用及受影响程度；

e） 明确治理目标，结合治理要求、业务需求、行业标准、伦理规范，制定短期目标（或整改目标）、中长期规范化和智能化治理目标，覆盖战略对齐、价值交付、风险管理、资源优化、绩效度量五个维度；

f） 界定治理范围并识别治理域，拆解治理目标为关键能力要求，识别能力缺口与痛点，梳理治理域（如数据、算法模型、应用、算力资源、合规与伦理等）；分析治理域依赖关系与协同要求，确定实施优先级；

g） 确定治理域并建立动态识别机制，经相关方确认后作为治理实施和监督依据；根据内外部变化（法规、技术等）及时重新识别治理域；

h） 制定治理方案，包括建立治理主体及岗位职责；明确决策、授权、沟通、绩效评价、监督、持续改进等机制；制定相关方沟通与参与策略；按评估、指导、监督规划实施流程；针对治理域明确六项要素（方向、策略、授权、责任、能力、绩效）的治理活动；进行治理任务分解，制定实施计划（任务、时间安排、阶段目标、职责分工、资源配置）；评估风险与阻力并制定应对措施；

i） 规划保障措施，规划组织、人力、技术、资金、机制、安全等保障措施，并持续评估其有效性。

A.4.2 治理执行

人工智能治理实施宜在六项治理要素（方向、策略、授权、责任、能力、绩效）以及评估—指导—监督治理活动的基础上，结合人工智能治理域的典型落地场景，转化为下列六个方面的关键实施活动，指导组织有效开展人工智能治理的执行工作，见表 A.2。

表 A.2 人工智能治理域关键实施活动

任务	活动内容
人工智能全域场景摸排建档	全面梳理组织所有人工智能模型、人工智能应用、第三方人工智能工具、人工智能训练项目等，统计归属部门、研发主体、应用场景、使用范围、训练数据来源、上线时间、运维责任人，建立人工智能资产与应用台账，形成可追溯的资产管理基线； 建立人工智能应用场景分级清单，按高风险（核心业务领域）、中风险、低风险进行分类标注，为差异化管控提供依据；风险等级评定方法，可参照相关法规对人工智能风险场景的界定要求； 盘点现有治理制度、审批流程、岗位职责与人工智能资产的匹配情况，识别未覆盖的人工智能应用和治理盲区，形成治理域补缺清单
人工智能专项风险排查	聚焦合规风险（如未审批上线、超范围应用、不符合监管政策等）、数据风险（如训练数据来源不合规、包含敏感信息、数据泄露等）、算法风险（如算法偏见、逻辑漏洞、输出失真、不可解释等）、应用风险（如人工智能滥用、违规生成内容、业务决策风险等）、运行时风险（如模型性能漂移、智能体自主决策偏差与行为异常、智能体责任归属不清、人工智能系统间交互失控与越权等）、人工智能供应链风险（如第三方人工智能服务、预训练模型、开源组件的数据流向不透明、模型版本不受控、责任边界模糊等）六大维度，采用风险登记册记录风险信息、评级、处置措施和状态，实现风险清单化闭环管理； 遵照相关法规建立合规要求清单，逐项核查算法备案、内容标识、安全评估等义务履行情况，记录伦理风险（数据滥用、偏见、隐私泄露等）； 评估现有授权体系的有效性，排查过度授权、越权操作、权限外溢等风险点，特别是高权限账号和自动化决策工具的权限配置
人工智能问题分类整改	对未审批、违规上线的人工智能应用立即暂停使用，补齐准入审批和备案手续；对不合规训练数据立即清理、替换或脱敏；对存在偏见、漏洞的算法及时迭代优化和校验测试；对超范围、高风险场景收紧权限、规范应用边界； 对整改过程进行能力复盘，识别因技能不足或工具缺失导致的问题，制定专项培训或工具部署计划，避免同类问题复发； 采用 PDCA 闭环整改跟踪表记录问题来源、措施、责任人、时限和验证结果，确保每项问题闭环

表 A.2 人工智能治理域关键实施活动（续）

任务	活动内容
人工智能全流程治理固化	建立“需求评审、合规审核、数据校验、算法测试、上线审批、场景管控、迭代优化、下线退役”等全生存周期治理流程，嵌入 RACI 矩阵明确各环节角色，将治理要求固化到管理制度和系统中； 制定人工智能伦理规范与算法合规管理规则，明确偏见定义、可解释性分级、人工干预规则、备案及内容标识义务，并建立规则变更审批与冲突处置流程； 部署智能化治理工具（如模型资产盘点、可解释性分析、偏见检测、安全测试等），建立模型漂移检测和性能劣化自动告警、回滚机制； 明确各治理主体职责边界，构建责任矩阵，规范履职标准与跨部门协同，对数字员工等自动化决策实体指定名义责任人，设置问责与追溯规则； 为每个智能体分配可追溯的唯一身份标识，明确名义责任人，建立智能体权限的生存周期管理机制（如准入授权、动态调整、定期复审、及时回收等）；记录智能体操作的行动人/智能体身份标识、时间戳、输入输出参数和执行结果，实现全链路可审计、可追溯
人工智能全要素资源治理	数据资源治理：建立训练数据全生命周期管理规范，覆盖采集、标注、清洗、脱敏、存储、使用、销毁各环节；建立数据质量评估体系和来源合法性审查机制；实施分级分类管控和数据血缘追溯； 算法模型资源治理：建立算法模型资产目录和全生命周期管理制度，涵盖开发、测试、部署、监控、迭代、退役各阶段；部署模型评估测试体系（如准确性、公平性、鲁棒性、可解释性等）和持续监控机制（如漂移检测、自动告警、版本管理等）；根据智能体的角色和自主等级实施分级授权和差异化管控，建立多智能交互规则和冲突处置机制，智能体的自主决策须记录到审计系统，重大决策保留责任人最终审批通道； 算力资源治理：建立算力资源台账和调度分配机制，按业务优先级实施差异化配额；引入虚拟化技术提升利用率；建立算力成本核算与分摊机制并部署资源监控告警；建立算力能耗监控与管理机制，跟踪人工智能系统的能源消耗和碳排放数据，制定算力资源优化配置策略，推动绿色人工智能实践； 人才资源治理：建立人工智能治理人才能力模型，制定分层培训计划（如战略、操作、审计等）；组建跨学科治理团队；建立人才储备与梯队培养机制，持续跟踪行业动态提升专业水平
人工智能应用常态化监管	定期核查人工智能模型运行状态、训练数据合规性、算法输出准确性、场景应用规范性；建立人工智能风险预警机制，对异常输出、违规应用、数据风险实时预警处置；定期开展合规自查和专项审计，范围涵盖人工智能系统的算法验证、数据安全、决策偏差、伦理合规和运行绩效等方面，对于处理大规模个人信息或涉及高风险决策的人工智能系统，按法规要求执行监管，形成从发现到整改再到验证的闭环； 设定并动态监测人工智能治理成效指标（如高风险算法备案率、偏见测试覆盖率、用户申诉响应时效、模型安全事件闭环率、智能体身份覆盖率（已身份化智能体占总数比例）、智能体权限合规率、智能体审计日志完整率等），对指标偏差进行归因分析并按优先级触发改进； 建立定期复盘机制，从合规检查、安全评估、用户投诉、模型事故等渠道收集反馈，沉淀可复用的规则库、检查清单和培训材料

A.4.3 治理优化

人工智能治理优化的治理工作要点，包括：

a） 基于治理复盘机制，定期开展治理成效自评，从战略对齐、价值交付、风险管控、资源利用、绩效达成等维度评估治理体系的完备性与人工智能运行效果，识别治理短板与不足；

b） 采集人工智能运行和治理数据，分析系统运行情况，从合规检查、安全评估、用户投诉、模型事故、算法备案退回、偏见检测异常、内部审计、监管意见等渠道系统收集反馈数据和信息，覆盖制度运行、风险管理、数据质量、算法模型、智能体运行等领域的运行情况，形成偏差报告；

c） 基于偏差报告，结合政策更新、技术升级、业务迭代等，以及风险管理过程中的风险识别、分析、处置、监控闭环要求，分析薄弱环节的根本原因，按影响范围和严重程度确定治理改进优先级；

d） 针对高优先级缺陷，明确责任主体、资源、时限和验收标准，通过调整审批规则、优化检测阈值、升级治理工具、完善培训体系、修订伦理准则等措施落实改进，补齐能力短板；

e） 采用量化指标（如风险处置率、模型安全事件闭环率、偏见测试覆盖率、制度执行符合率等）评估改进成效，未达预期则重新分析调整，确保缺陷闭环；

f） 持续推进治理能力提升，将优化改进中的经验教训和最佳实践，反馈至治理规划环节，进行校准方向、修订策略、完善指标、迭代算法等，形成可复用的治理规则库、检查清单和培训材料，推动治理能力持续提升。

A.5 治理交付物

人工智能治理交付物见表 A.3。

表 A.3 人工智能治理交付物

交付物	说明
《人工智能治理章程》	明确治理原则、组织架构、职责分工和运行机制
《人工智能伦理准则》	规定公平、透明、安全、隐私保护、可问责等核心伦理原则
《人工智能风险管理规程》	建立风险识别、评估、分级、处置的标准化流程
《人工智能系统清单与风险分级台账》	记录全组织人工智能系统及其风险等级
《人工智能应用影响评估报告》	对高风险人工智能应用开展上线前影响评估并形成报告
《人工智能治理成效报告》	按周期统计绩效指标达成情况，包含偏差分析和归因结论
《人工智能治理能力建设档案》	培训计划、参训记录、能力评估结果及工具部署文档

参 考 文 献

[1] GB/T 19668.1—2023 信息技术服务 监理 第1部分：总则

[2] GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[3] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[4] GB/T 22081—2024 信息技术 安全技术 信息安全控制实践指南

[5] GB/T 24353—2022 风险管理 指南

[6] GB/T 24405.1—2022 信息技术 服务管理 第1部分：规范

[7] GB/T 26317—2010 公司治理风险管理指南

[8] SJ/T 11445.2—2012 信息技术服务 外包 第2部分：数据（信息）保护规范

[9] 《企业内部控制基本规范》 中华人民共和国财政部［财会〔2008〕7号］2008年5月22日

[10] 《中央企业全面风险管理指引》 国务院国有资产监督管理委员会［国资发改革〔2006〕108号］2006年6月6日

[11] 《商业银行信息科技风险管理指引》 中国银行业监督管理委员会［银监发〔2009〕19号］2009年6月1日

[12] 《证券基金经营机构信息技术管理办法》 中国证券监督管理委员会 证监会令〔第152号〕 2018年12月19日

[13] 《保险公司信息系统安全管理指引（试行）》 中国保险监督管理委员会［保监发〔2011〕68号］2011年11月16日

[14] ISO/IEC 38500:2024 Governance of information technology for the organization

[15] OECD Principles of Corporate Governance. OECD, 2004

[16] Report of the Committee on the Financial Aspects of Corporate Governance. Sir AdrianCadbury, London, 1992, ISBN0852589131

[17] ISACA Cobit5.0 Control Objectives for Information and related Technology, ISACA, April 10, 2012