ICS 35.080
CCS L 70

中华人民共和国国家标准

GB/T 34960.1—XXXX
代替 GB/T 34960.1-2017

信息技术服务 治理 第1部分：通用要求

Information technology service—Governance—Part 1：General requirements

（征求意见稿）

（本草案完成时间：2026年7月16日）

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

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1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 34960.1—2017《信息技术服务 治理 第1部分：通用要求》，与GB/T 34960.1—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“利益相关方”的定义，更改了“治理主体、治理要素、治理域、能力”的定义，删除了“信息技术架构”的定义（见第 3 章，2017 年版的第 3 章）。

b) 更改了 IT 治理模型，将“治理主体、治理过程（评估、指导、监督）及管理体系”组成的模型，更改为由“治理目标与原则、治理主体、利益相关方、治理过程、治理要素和治理域”组成的新模型（见第 4 章，2017 年版的第 5 章）。

c) 更改了“治理原则”章节的内容，将章节名称由“治理原则”更改为“治理目标与原则”，目标包括战略一致、风险可控、运营合规和绩效提升，原则更新为权责清晰、多元协同、风控优先、过程透明、创新赋能（见第 5 章，2017 年版的第 4 章）。

d) 增加了“治理主体”一章，明确了治理主体的职责与要求（见第 6 章）。

e) 增加了“利益相关方”一章，明确了其作为治理活动全过程参与者的定位（见第 7 章）。

f) 增加了“治理过程”一章，详细规定了评估、指导、监督三个核心环节的具体要求（见第 8 章，2017 年版的第 5 章）。

g) 增加了“治理要素”一章，将原来分散的要求提炼为方向、策略、授权、责任、能力、绩效六大核心要素（见第 9 章）。

h) 删除了“信息技术治理框架”章节，修改了顶层设计、管理体系和资源三大治理域的结构化划分方式，采用以“治理域”为核心的动态构建与拓展方法（见第 10 章及附录 A、2017 年版的第 6 章）。

i) 删除了“顶层设计的治理”章节，将“战略、组织、架构”相关内容，整合并转化为“方向”、“策略”等治理要素中的具体要求（见第 9.1、9.2 章，2017 年版的第 7 章）。

j) 删除了“管理体系的治理”章节，将管理体系（如质量管理、信息安全管理、业务连续性管理等）的要求，整合并重构到“治理过程”和“治理要素”的相应条款中（见第 8 章和第 9 章，2017 年版的第 8 章）。

k) 删除了“资源的治理”章节，将“基础设施”、“应用系统”、“数据”的治理要求，进行扩展和细化，统一纳入新的治理域中（见第 10 章及附录 A，2017 年版的第 9 章）。

l) 增加了“治理域”一章，规定了治理域的构建、拓展和适配、优化和完善（见第 10 章）。

m) 增加了“资料性附录 A”，给出了管理体系、基础设施、数据、人工智能、应用系统等治理域的构建方法（见附录 A）。

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：上海市大数据中心、上海计算机软件技术开发中心、中国电子技术标准化研究院、江苏意源科技有限公司、北京可利邦信息技术股份有限公司、浪潮软件集团有限公司、金税信息技术服务股份有限公司、上海商学院、上海谷航信息科技发展有限公司、北京赛西科技产业有限责任公司、华东师范大学、神州数码信息系统有限公司、中远海运科技股份有限公司、上海银行、北京金山办公软件股份有限公司、上海翰纬信息科技有限公司、广州赛西标准检测研究院有限公司、北京直真科技股份有限公司、万达信息股份有限公司、北京仁科信息技术有限公司、北京赛迪认证中心有限公司、百信信息技术有限公司、广西博联信息通信技术有限责任公司、北京神州邦邦技术服务有限公司、山东省科技咨询中心有限公司、中通服咨询设计研究院有限公司、上海浦东软件平台有限公司、广州赛宝联睿信息科技有限公司、北京银信长远科技股份有限公司、广州赛宝认证中心服务有限公司、湖南湘创科技有限公司、上海北宙企业管理咨询有限公司、中科软科技股份有限公司、北京华胜天成科技股份有限公司、合肥博胜信息技术服务有限公司、厦门群睿信息技术有限公司、中电信数智科技有限公司、成都市工业互联网发展中心、北京德信永道信息技术服务有限公司、湖州市数据服务中心、陕西中安数信项目管理有限公司、上海软中信息技术有限公司

本文件主要起草人：杨琳、宋俊典、郭鑫伟、肖筱华、尹正茹、刘瑞慧、熊健淞、张绍华、朱俊伟、俞文平、张明英、刘辰昀、高明、王华、郝建明、单曙兵、张树玲、陈宏峰、黄胜华、聂俊平、侯秀琳、吕艳、马烈、李京、谭丽圆、梁瑛、许志国、薛科、李世喆、夏婷婷、徐莹莹、侯觅、黄建新、季寒德、张翀、陈艳、傅盛、朱爱斌、刘鹏飞、刘颋、孙勉、王珊珊、梁钢、王飞、吴超、刘亚东、王文俊、杨泉、雷唤、庞卫忠、蔡浩淼

本文件及其所代替的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》拟由五部分构成。

——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模型、原则、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。

信息技术服务 治理 第1部分：通用要求

1 范围

本文件确立了信息技术治理（以下简称：IT治理）的模型与原则，规定了治理主体、利益相关方、治理过程，治理要素和治理域等IT治理通用要求。

本文件适用于：

a) 各类组织建立、实施、评价和改进其 IT 治理体系。

b) 开展信息技术审计。

c) 研发、选择和评价 IT 治理相关的软件或解决方案。

d) 第三方对组织的 IT 治理能力进行评价。

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 20269 信息安全技术 信息系统安全管理要求

GB/T 31496 信息技术 安全技术 信息安全管理体系 指南

GB/T 34960.5 信息技术服务 治理 第 5 部分：数据治理规范

GB/T 44109 信息技术 大数据 数据治理实施指南

GB/T 45081 人工智能 管理体系

GB 45438 网络安全技术 人工智能生成合成内容标识方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息技术治理 information technology governance

专注于信息技术体系及其绩效和风险管理的一组治理规则，由领导关系、组织结构和过程组成，以确保信息技术能够支撑组织的战略目标。

[来源：GB/T 29264—2012，2.6]

3.2

治理主体 governance body

对组织信息技术使用的绩效和合规承担最终责任，并行使评估、指导和监督职能的个人或团体。

3.3

利益相关方 stakeholder

对组织信息技术治理活动拥有责任、期待或利益，并能影响或受其影响的个人、群体或组织。

3.4

治理要素 governance element

实施信息技术治理所涉及的关键治理对象或组件。治理主体通过评估、指导、监督这些要素，将治理意图转化为具体的活动和成果。

3.5

治理域 governance domain

按照特定层次或功能划分的治理范围，是治理过程和治理要素的集合。它帮助组织对信息技术治理活动进行结构化、系统化的分类。

3.6

能力 capability

完成任务或履行角色责任所需知识、技能、经验及其他相关资源的组合。

4 治理模型

IT治理模型由治理目标与原则、治理主体、利益相关方、治理过程、治理要素和治理域组成，见图1。

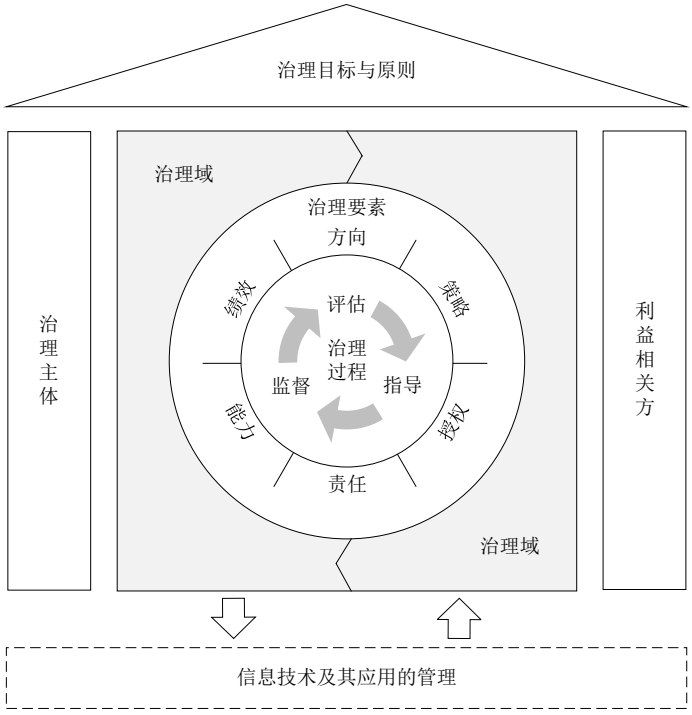

图1 IT治理模型

治理目标是组织发展目标的组成部分，包括战略一致、风险可控、运营合规和绩效提升。

治理原则是治理主体开展治理过程中所遵循的基本原则，包括权责清晰原则、多元协同原则、风控优先原则、过程透明原则和创新赋能原则。

治理主体是开展治理活动的责任主体。治理主体以治理目标为指引、治理原则为基准，构建治理过程和治理要素的映射，对治理域进行治理。

利益相关方是治理活动的全过程参与者，是信息技术价值实现和利益承载的主体，是IT治理的多层次责任体系的组成部分。

治理过程是IT治理的核心机制，是治理主体履行职责、开展治理的行动框架，包括评估、指导、监督三个环节。

治理要素是IT治理的核心组件，是组织构建IT治理体系的重点，作为连接治理主体与治理域的桥梁，包括方向、策略、授权、责任、能力和绩效六个方面。

治理域是按照层次或功能划分的治理范围，承载具体的治理活动。治理主体围绕业务领域、应用场景、安全管控等差异化需求，从顶层设计、管理体系和资源三个维度对治理域进行构建、扩展和适配、优化和完善。治理域的构建见附录A。

本文件对虚线框内内容不作规定。

5 治理目标与原则

5.1 治理目标

组织应明确IT治理目标，确保其与组织发展目标、业务发展目标和IT发展目标保持一致。IT治理目标的制定应由组织治理层或高级管理层主导，并符合以下要求：

a) 战略一致：制定与组织战略一致的信息技术战略，建立评估与监督机制，确保 IT 治理过程贯穿治理要素，有效支撑业务目标实现与创新变革。
b) 风险可控：明确风险偏好与容忍度，指导建立覆盖全生命周期的 IT 风险管理机制，主动识别、评估并管理 IT 相关风险，防范重大财务损失、声誉损害、监管处罚及法律制裁。
c) 运营合规：对当前及未来的 IT 使用进行监督，确保运营合规性与风险状况符合既定期望，并对第三方提供的 IT 服务实现有效监管。
d) 绩效提升：确保 IT 投资与新一代信息技术的价值实现，优化资源配置，提升组织绩效与可持续发展能力。

5.2 治理原则

组织需制定IT治理原则，以支撑治理目标的实现。IT治理包含但不限于以下原则：

a) 权责清晰原则：IT 治理是公司治理的重要组成部分，宜明确 IT 决策的权力与责任分配，由最高决策者承担 IT 治理的最终责任，决策层为 IT 治理主体。
b) 多元协同原则：建立由内部监督部门、重要业务部门、信息技术管理部门、财务部门、合规及风险管理部门等多元主体共同参与的 IT 治理机构，确保各方协同治理。
c) 风控优先原则：明确组织对安全与风险的偏好及容忍度，建立覆盖全生命周期的风险管理机制，主动识别、评估并管理 IT 相关风险，防范重大财务损失、声誉损害、监管处罚及法律制裁。
d) 过程透明原则：建立定期的沟通机制，确保 IT 治理全过程的透明性与可追溯性，通过业务与 IT 的深度融合，使利益相关方充分理解 IT 投资预期收益、清晰认知潜在风险及应对措施。
e) 创新赋能原则：建立信息技术应用的战略对齐机制、制度保障体系、创新文化和持续改进机制，通过 IT 赋能业务模式变革、技术进步与管理效能提升，驱动组织可持续发展。

6 治理主体

组织应确定IT治理主体，构建权责清晰、层级分明的治理组织，确保IT治理体系的有效运行与持续改进，IT治理主体应：

a) 明确治理的核心，确保 IT 治理目标与组织战略、价值创造及风险管理策略一致，构建治理过程的闭环机制，评估内部外环境与风险，监督 IT 规划的实施执行与绩效，确保 IT 投入与业务匹配。

b) 确定治理的原则，作为治理准则和决策框架，涵盖风险偏好、合规、绩效与持续改进，引导管理层平衡创新与安全，确保信息技术及其应用的合规可控。
c) 保障利益相关方的参与，建立沟通参与机制，明确角色权责，定期评价并改进，确保各方对 IT 投资、风险与收益形成共识。
d) 构建跨职能的治理机制，构建治理过程与治理要素的映射矩阵，形成分工明确、责权清晰的治理过程。
e) 开展治理任务的实施，划分清晰可行的治理域，通过治理要素细化治理域的具体活动和任务。

7 利益相关方

组织应确定利益相关方，全面系统地识别、理解并响应其合理期望与需求，确保IT治理的透明性和全面性，至少应：

a) 建立动态识别机制，指导建立并维护利益相关方识别流程，系统性识别所有内外部利益相关方，定期或在环境发生重大变化时更新清单，确保无遗漏。
b) 制定利益相关方的差异化参与策略，明确参与目的、范围、目标群体、沟通渠道、频率及所需资源，针对不同关注点和任务采用差异化沟通。
c) 建立期望收集与冲突平衡机制，通过正式渠道收集利益相关方期望，评估其对 IT 战略、价值目标及风险偏好的影响，识别期望冲突并建立平衡与优先排序机制。
d) 构建闭环反馈机制，确保信息在合适时间以合适方式传递给合适受众，并将其作为持续改进治理的重要输入。

8 治理过程

8.1 评估

治理主体应持续评估信息技术应用现状与趋势、治理机制及组织目标的适配性，识别差距和风险，形成评估结论，支撑组织治理能力的不断提升，至少应：

a) 建立评估机制。建立常态化、系统化、全面化的评估机制，结合内外部环境压力与业务战略，明确评估边界与目标，确定必须覆盖的治理域，使评估活动支撑治理决策。
b) 组建评估组织。识别利益相关方，联合管理层、IT 部门与业务部门、内审及风险合规团队，必要时引入外部专家或第三方机构，共同开展评估活动，明确各方权责。
c) 采集评估数据。建立数据采集责任矩阵，定期采集涵盖组织战略、治理域、风险与合规控制、资产治理、运营与服务绩效、数据质量与过程能力、利益相关方与治理文化等方面的数据，并保证采集数据质量及评估依据的客观性与完整性。
d) 开展差距分析。依据治理目标、法律法规、内部策略及行业基准，开展战略对齐、控制执行及风险合规等方面的差距分析，并明确差距分析的实施频次、方法与标准。
e) 评估治理成效。对信息技术战略与业务战略的对齐度、组织架构与流程的合理性、服务交付质量、重大投资决策、资源投入规范性、风险管控有效性及绩效表现等进行综合评估，发现治理体系中的有效举措，识别存在的问题。
f) 形成评估结果。规范记录评估活动，确保评估结果具备规范性、准确性、真实性、完整性与可追溯性，为指导和监督活动提供依据；将评估结果及时传递至治理主体，为制定和优化信息技术战略、资源配置策略及风险应对措施提供数据支撑。

8.2 指导

治理主体应基于评估结果，立足组织全局，围绕治理要素和治理域，制定或调整战略、策略、原则、资源配置及决策规则，为当前及未来信息技术应用提供方向，使信息技术战略深度融入组织战略，至少应：

a) 明确战略与顶层设计。依据评估发现的短板与差距，明确信息技术战略方向、中长期规划、指导原则及策略指令，审批信息技术总体架构与技术演进路径，使治理决策与组织战略目标一致。
b) 确立组织与权责体系。构建清晰的信息技术治理组织架构，明确界定治理主体、管理层及执行层的职责边界、权限与问责机制，落实信息技术应用中的责任体系，使决策权与执行权有效匹配。
c) 统筹决策与资源配置。建立科学的信息技术投资决策机制，明确资源分配、投资优先级及风险管控策略，统筹配置资金、人员、技术及数据等资源，指导重点项目建设与资源合理投入。
d) 发布执行准则与准入审批规则。建立覆盖治理域的战略执行传导机制，向管理层及执行层提出工作准则；针对高风险、高价值、高投入事项，制定审批规则，明确审批门槛、权限及例外管控机制。
e) 设定风险阈值与合规边界。明确信息技术应用必须遵循的内外部法律法规、政策规定及伦理要求，指导设定可接受的信息技术风险阈值，确立合规底线与安全红线。
f) 核准价值目标与能力建设。建立以价值为导向的治理基准，指导构建与战略相匹配的信息技术能力体系、绩效评价体系，倡导治理文化，使信息技术投入转化为可度量的业务价值，推动数智化转型与人工智能等创新应用。
g) 动态调适与协同贯通。结合治理实践成效与发展趋势，指导优化信息技术战略、政策及治理框架，使指导工作紧密衔接评估输入并支撑监督核查。

8.3 监督

治理主体应对信息技术治理的执行过程与成效实施全过程监督，建立常态化跟踪核查、动态指标监控、偏差预警问责、定期审计验证及结果闭环回流机制，以促进组织目标达成，至少应：

a) 监督战略对齐与适配性。监督信息技术战略与业务战略的一致性，核查战略规划执行及治理域的落地成效，持续监控战略绩效指标，定期审视战略适配性，对重大偏差及时预警并启动整改，确保信息技术战略有效支撑组织发展。
b) 监控能力稳定与可持续性。监控信息技术支持能力的可持续性与稳定性，常态化核查各领域技术支撑的落地情况，持续监测资产运行状态与业务保障指标，识别并推进补齐能力缺口，驱动信息技术能力持续满足组织战略需求。
c) 监督合规与制度执行。监督信息技术治理活动符合法律法规、合同及内部制度要求，动态跟踪法律法规更新并开展合规审查，常态化监控政策制度、治理机制及指标体系运行情况和执行效果，对违规行为启动预警、限期整改与问责，构建合规管理闭环。
d) 监控风险管控与内部控制。监控信息技术风险管理与内部控制的有效性，常态化核查风控内控措施的落地情况，评估风险全流程管控质量及伦理风险，对重大风险偏差落实整改，使风险可控并夯实组织信任基础。
e) 监督资源管理与价值产出。监督信息技术资源全生存周期管理的规范性，常态化校验资源管理执行情况，监控资源运行的稳定性与价值产出指标，审查资源配置的合理性与优化成效，对管理偏差进行整改优化，使资源投入合规且持续产出预期价值。
f) 定期审计验证。建立 IT 审计制度，制定定期审计计划，结合内外部审计资源，对治理域的规划、构建、运行及成效开展独立、系统、周期性的审计。审计范围应覆盖战略一致性、资源管理、风险管控、合规执行及绩效产出等关键领域，明确审计程序、方法及准则，确保审计证据

充分、结论客观。形成审计报告。明确发现问题和改进建议，跟踪审计整改落实情况，将审计结果纳入考核与问责，确保审计闭环有效运行。

g) 监督结果闭环与持续改进。监督授权机制与问责安排的有效性与清晰度，常态化核查权责落地与协同问责情况，对违规偏差启动问责并整改。将常态化监督发现、审计验证结果及整改情况全面回流至评估环节，作为治理体系优化的重要输入，推动治理机制、绩效指标及治理方法的持续改进。

9 治理要素

9.1 方向

治理主体应结合业务定位、核心价值及利益相关方期望等，明确IT应用符合组织的价值导向，至少应：

a) 建立 IT 治理方向管理机制，包括信息收集与分析、治理方向设计、部署实施、定期评审与优化等。

b) 收集组织战略、业务规划、监管要求、风险偏好、利益相关方诉求等信息，作为 IT 治理方向评估、制定和监督的依据。

c) 结合 IT 对组织发展和能力的影响，以及组织对 IT 使用需求和 IT 支持的价值产生模式等，明确 IT 提供持续服务和创造价值的方向。

d) 明确 IT 治理工作的整体边界和核心导向，开展 IT 治理方向顶层设计，与组织发展和核心价值保持一致，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。

e) 评估 IT 治理方向及目标与组织战略、能力目标的一致性。

f) 围绕 IT 治理方向，明确可测量、可执行、可验证的阶段性 IT 治理目标，支撑 IT 治理方向落地见效。

g) 遵循相关监管要求，规范人工智能等 IT 技术应用中的伦理原则与规范，将伦理要求贯穿于 IT 应用全过程。

h) 指导并推动 IT 治理方向及治理目标在治理域的贯彻落实，准确理解与一致执行。

i) 监督内外部环境变化、组织战略调整及监管要求更新等重大变化，识别方向偏离，并及时动态优化调整。

9.2 策略

治理主体应制定IT治理策略体系，以体现决策规则，资源配置、行动准则等策略指引，至少应：

a) 规范 IT 治理策略制定、批准、发布、执行、修订、监督与验证的相关活动要求。

b) 构建 IT 治理策略体系，明确指导原则、行动框架与边界、决策规则和监督标准等，统筹 IT 资源、管控 IT 风险、以实现 IT 价值最大化。

c) 提出 IT 治理策略的行动准则，包括市场变化应对、项目与客户选择、资源调整与分配、风险偏好与防控、利益相关方期望与影响等，且保持行动之间协同一致。

d) 明确 IT 可接受使用与行为规范，制定针对外部供应商及合作伙伴的 IT 获取与外包策略，约束和指导利益相关方对 IT 的使用，防范合规与安全风险。

e) 明确 IT 治理策略行动的责任与义务，提供必要的资源与能力保障，指导 IT 治理策略在组织内被准确理解、有效传达和一致执行。

f) 定义可用于支持系统自动配置的策略参数，增强 IT 治理策略的动态适应性，推动治理策略向数字能力的直接转化与自动执行。

g) 记录并保留 IT 治理策略制定过程中的决策依据和解释说明，包括对备选方案的分析与选择，支持治理决策的可追溯性。
h) 评估 IT 治理策略与组织治理目标、治理方向、战略目标保持一致，并遵守相关行业监管和合规要求。
i) 监督 IT 治理策略的执行偏差、合规违规等情况，并持续更新策略文件，完善管理机制。

9.3 授权

治理主体应明确授权边界和授权方案，规范授权行为和匹配权责，适配组织管理模式，至少应：

a) 建立 IT 治理授权原则，遵循战略对齐、权责对等、最小权限、可监督、可验证、动态适配等原则。
b) 建立 IT 治理授权管理机制，包括授权需求识别、授权方案设计、授权实施、变更管控、授权监督与审计等要求。
c) 评估授权范围与组织发展、风险偏好的匹配度，确保授权体系与组织发展相适应。
d) 明确 IT 治理的决策层、执行层、监督层的分级授权和责任使用，划分各分级主体的授权范围、决策边界，使责权对等并与组织架构保持一致。
e) 围绕 IT 治理活动和关键控制点，明确治理域授权的具体事项、分级权限及对应审批流程，支撑授权机制在 IT 治理各环节落地执行。
f) 明确 IT 可接受使用行为规范、身份认证与访问控制标准，保障 IT 资源高效、安全与合规利用。
g) 监督授权机制、授权边界及授权执行的一致性，识别权限冗余、越权与配置失效等问题。
h) 结合组织战略调整、业务流程优化、监管要求更新及信息安全风险变化等情况，优化授权方案，持续适配组织 IT 治理与业务发展需求。

9.4 责任

治理主体应明确IT治理责任事项、责任主体、职责权限、协同机制、问责规则等要求，且责任履行结果可验证，至少应：

a) 建立 IT 治理责任管理机制，明确责任事项识别、责任配置、责任履行、监督验证、追溯问责和责任调整的流程、职责及要求。
b) 构建责任体系与责任矩阵，配置相应的责任主体、履职标准及跨域协同关系，确保利益相关方在治理活动中的职责、权限与资源配置对等一致。
c) 评估责任体系与组织战略、业务目标、风险控制及合规要求的匹配度，识别履职情况偏差。
d) 明确治理域活动中的职责、权限配置、责任要求，以及沟通协同机制等。
e) 将责任要求嵌入 IT 治理制度、业务流程及绩效体系，制定履职标准，指导责任要求在 IT 服务中被准确理解与一致执行。
f) 明确问责触发条件、责任认定标准与处置措施，规范过程记录与归档，实施责任认定、原因分析、整改验证的闭环管理。
g) 监督责任履行状态、目标达成情况进行确认，并将履职情况纳入考核，及时调整不适宜的授权与责任。
h) 结合组织战略调整、业务变化、技术变化、利益相关方反馈等情况，开展责任校准，优化责任体系。

9.5 能力

治理主体应识别和构建支撑治理与管理所需的能力组合，在风险可控的前提下，并将能力转化为可衡量的业务价值，至少应：

a) 建立能力的管理机制，明确能力识别、评估、构建、监督、优化的过程和责任等要求。
b) 通过深入理解内外部环境、利益相关方期望和组织文化，洞察组织战略和业务需求，识别能力需求，盘点能力现状，分析现有能力现状与差距，进行内外部的能力协同与整合，形成对当前及未来所需能力视图。
c) 明确 IT 治理能力框架，开展覆盖顶层设计，保持与组织战略及治理方向的一致性，确定能力目标与建设路径。
d) 聚焦实现组织治理目标和战略目标的核心能力要素，指导并形成能力策划，确定能力核心要素的执行计划和沟通协调机制等。
e) 围绕能力策划，制定阶段性、可测量、可执行、可验证的能力建设目标，支撑治理方向落地见效，且与组织战略目标及治理目标保持一致。
f) 为能力建设提供必要的资源保障，并遵循相关监管与合规要求。
g) 在能力建设全过程中，应与内外部利益相关方保持充分沟通，以获取其理解、支持和反馈，确保能力建设符合预期。
h) 监督能力建设情况，以及能力绩效达成情况及能力满足状态，并驱动能力持续提升。
i) 当组织发生重大变化时，重新开展能力评估，优化能力框架和能力策划。

9.6 绩效

治理主体应建立绩效体系和绩效指标，并开展有效的绩效监测，至少应：

a) 建立绩效管理机制，明确绩效管控原则、绩效指标设置、监测指标、绩效信息收集与分析、预警与改进、绩效结果应用等要求。
b) 收集分析组织战略、业务规划、监管考核、内控标准及利益相关方期望等信息，使 IT 绩效评价契合组织价值导向，作为制定绩效要素与指标体系、更新绩效基准的依据。
c) 明确 IT 治理绩效管控边界与核心导向，并形成覆盖治理域的绩效体系。
d) 建立绩效评价指标体系，包括 IT 治理自身衡量指标、IT 运营管理指标和 IT 性能衡量指标等，绩效指标设置需具备可量化、可监测、可预警性。
e) 遵循监管要求，将合规管控、数据安全、科技伦理、风险整改等要求纳入绩效评价范畴，将管控要求贯穿 IT 绩效管理全过程。
f) 结合组织结构和授权范围，建立绩效指标分级管控机制，确保绩效指标责任到人，与授权、责任体系保持一致，指导有效传达并在组织内形成共识。
g) 建立绩效指标监测与预警机制，实时或定期采集绩效数据，跟踪目标达成情况，对异常指标和重大风险及时预警。
h) 评估治理域绩效落地现状与成效，以及绩效体系与组织发展的适配性、可行性。
i) 监督治理域绩效执行，并通过绩效结果优化资源配置、落实奖惩问责，持续优化绩效体系。
j) 当组织内外部环境、战略及监管要求变化时，启动绩效校准，并更新绩效体系。

10 治理域

10.1 基本规则

治理域的构建、拓展和适配、优化和完善，应遵循以下基本规则：

a) 战略对齐：治理域的管控目标、架构逻辑及演进方向，应与组织经营战略、数智化发展目标及顶层 IT 规划保持一致，确保 IT 治理活动始终服务于业务成果实现与价值创造。
b) 边界唯一：清晰界定各治理域的管控范畴、职责边界及协同接口，确保治理域之间界面清晰，实现无管控重叠、无治理空白。建立治理域间的协调联动机制，明确跨域问题的升级路径与裁决规则，避免部门间推诿和资源浪费。
c) 权责适配：逐域明确治理责任主体及其在评估、指导、监督各环节中的具体职责。建立权责对等的履职机制和可追溯的问责制度，确保治理要求能够有效传导、落地执行，避免权责脱节或虚置。
d) 要素贯穿：治理要素通过治理活动的有效开展，系统性作用于各治理域。治理主体应在治理域规划、构建、拓展及优化的各环节中，明确治理要素的承载载体与传导路径，确保治理要素通过治理活动在各治理域内实现有效落地与协同运转，避免因要素传导不畅或过程缺失导致治理失效。
e) 动态兼容：治理域应具备对业务模式变革、新技术引入及外部政策法规更新的动态响应能力。建立常态化的环境感知与适配调整机制，确保治理域能够及时适应内外部变化，实现持续演进和自我优化，保持治理体系的前瞻性和有效性。
f) 成本平衡：合理权衡治理成本投入、资源配置与全域治理效益之间的关系，在满足合规底线、风险可控和价值实现的前提下，科学设定治理域的颗粒度和管理密度。避免因过度治理造成资源浪费和效率损耗，亦防止因治理缺位引发风险敞口和责任缺失，实现治理效能的最优化。

10.2 构建方法

治理主体应结合行业属性、组织规模、业务模式、技术架构及监管合规等要求，按照治理域的基本规则，从顶层设计、管理体系和资源三个维度开展独立或组合的治理域构建，至少应：

a) 构建覆盖战略、组织和架构的顶层设计治理域。依据组织数智化转型愿景与业务战略，明确 IT 治理的总体目标、价值主张和推进路线图，保障顶层设计对下层治理域的战略牵引。
b) 构建覆盖资源统筹、协同推进、价值交付和风险可控的管理体系治理域。以决策、执行、监督三级权责为主线，建立分层分级的治理流程与制度体系；强化跨部门协同与资源配置统筹；健全价值交付管理机制，确保 IT 投入与业务成效的量化关联；将安全、隐私、伦理及合规要求嵌入治理全过程，形成闭环管控。
c) 构建覆盖基础设施、数据、算法、人工智能等的技术和资源治理域。面向新一代信息技术创新应用场景，建立技术资源全生命周期管理规则；针对数据要素化趋势，完善数据资产、数据质量、数据流通与安全治理机制；针对人工智能及算法应用，明确可解释性、公平性、鲁棒性及人工监督等治理要求；统筹云、网、边、端等基础设施，确保资源弹性供给与持续演进。

10.3 构建流程

治理主体开展治理域的策划、构建、评审和实施，至少应：

a) 依据组织战略及数智化转型目标，系统识别内外部环境与利益相关者需求，明确 IT 治理的总体范围和愿景。从顶层设计、管理体系、资源三个维度划分治理域，界定各治理域的职责边界，评估治理要素与治理域之间的适配性，确保覆盖完整、权责清晰且无重叠盲区。
b) 针对各治理域，明确承担评估、指导、监督职能的责任主体，制定差异化的管控细则和操作规范，将治理域逐层分解为可量化、可执行的治理要点，形成治理要点清单。构建责任分配矩阵，清晰界定决策、执行、支持、咨询等环节中各角色的职责与权限，确保责任落实到位，并建立跨域协同机制。

c) 开展治理域的合规性评审，对照法律法规、行业监管要求、内部管理制度及数智化伦理准则，验证治理域设计的合理性和合规性，识别并评估潜在风险。评审通过后，正式发布 IT 治理域体系文件，并将其纳入组织统一的 IT 治理体系进行管理，确保所有治理活动的过程记录完整、可审计、可追溯。

d) 建立治理域运行状态的持续监测、绩效评估与反馈改进机制，定期审视治理域的有效性、效率及价值贡献。及时收集运行数据与改进建议，当业务战略调整、新技术落地应用或外部监管环境发生重大变化时，动态调整治理域范围、管控措施及责任分配，确保治理域始终适配组织数智化发展需求，实现持续演进与优化。

10.4 拓展和适配

治理主体应结合组织数智化发展战略及内外部环境变化，围绕业务领域拓展、应用场景创新、安全合规管控等差异化需求，在已构建的治理域基础上，开展治理域的拓展和适配工作，至少应：

a) 持续跟踪业务战略调整、新兴技术应用及风险形态演变，识别新增治理需求，适时增设新治理域；同时，评估新设治理域与已有治理域之间的依赖关系和管控衔接，确保新旧治理域协同一致。

b) 结合法律法规、外部监管、内部管控等需求的变化，及时审视现有治理域的覆盖充分性和边界合理性；必要时对治理域进行重构，重新定义治理边界、治理要点和职责分工，确保治理域持续有效，并与原有治理域实现无缝适配。

c) 围绕业务深入发展和治理活动场景化落地需求，在现有治理域框架下，拓展治理对象的内涵和外延，结合不同业务领域的差异化需求，制定领域级或场景级的治理细则，实现治理要求的精准化、差异化落地。

10.5 优化和完善

治理主体应建立常态化的治理域评估与优化机制，通过评估、指导和监督的闭环过程，对治理域的设计、覆盖范围、治理内容进行持续完善，至少应：

a) 定期评估各治理域在组织职责划分、管控流程设计及管控对象覆盖等方面的交叉重叠情况，识别职责冲突、流程冗余等问题，实施治理域的优化调整，及时适配管理体系变革、技术迭代创新及安全监管要求的动态变化，提升治理体系整体运行效率。

b) 针对业务变化快、技术迭代频繁、管控要求高的重点领域（如数据治理、人工智能等），建立更加敏捷的评估节奏，根据技术发展成熟度和应用风险等级，将治理域进一步细化为子域或专项治理模块，确保治理要求能够精准匹配业务和技术创新需求。

c) 对因业务下线、技术水平落后、外部监管取消或内部管理流程重构等原因不再产生实质性管控需求的治理域，及时启动裁撤评估，从业务价值、管控效能和资源投入三个维度综合研判其存续必要性；确认裁撤后，同步完成资产清理、风险遗留评估及合规责任闭环评审，确保裁撤过程平稳有序，治理对象始终处于受控状态。

附 录 A
（资料性）
治理域的构建

A.1 概述

本附录用于说明管理体系、基础设施、数据、人工智能、应用系统等治理域的治理定位、场景特征、治理要点及扩展方向，为各类组织治理域的构建、拓展和适配、优化和完善提供参考。

A.2 管理体系治理

A.2.1 治理定位

IT管理体系治理域是IT治理核心域，覆盖质量、环境、内控、合规等一体化管理体系；横向独立于业务、数据、资产治理域，纵向承接顶层治理指令、下沉末端业务执行，遵守体系合规红线。IT管理体系治理域聚焦体系合规闭环、流程适配落地、权责清晰履职、风险压降可控，短期保障审核合规、中期压缩治理成本、长期构建长效治理机制，破解体系文件与实际脱节、整改碎片化、权责模糊痛点，支撑组织有效运营与安全合规。

A.2.2 场景特征

具有制度约束性、流程穿透性、审核周期性、整改闭环性、跨部门强协同等特点，管理体系的风险多集中在体系与执行脱节、配置流程失控、权责交叉缺位、台账资料缺失、整改落实不闭环、内审体系不规范等方面。

A.2.3 治理要点

在顶层设计方面，宜建立管理体系策划、运行、审核、整改、迭代的全生命周期治理架构，明确归口管理、业务执行、内审监督、安全合规权责；在资源统筹方面，实行体系文件、岗位权责、审核台账、问题清单统一台账与标准化集约管控；在协同推进方面，打通归口部门、业务部门、内审部门、合规部门、第三方审核机构联动机制；在价值交付方面，提升体系落地率、压缩合规整改成本、保障体系审核、贴合安全合规等要求；在风险合规方面，重点落实ISO体系强制条款、国标管控要求、内审合规、过程留痕、问题销号管控要求。

A.2.4 扩展方向

可结合一体化融合管理体系、数字化内审管控、合规内控联动、供应链体系共管等新型治理场景，细化形成二级治理模块，补充文件基线、过程运行基线、内审核查基线、问题整改基线、管理评审基线等管控要求。

A.3 基础设施治理

A.3.1 治理定位

基础设施治理域覆盖物理设施、云资源、网络、算力、存储、安全设备等基础设施对象，聚焦资源可靠、运行稳定、集约可控。

A.3.2 场景特征

具有底层支撑性、资源密集性、高可用性要求、运维持续性、故障传导性强等特点，风险多集中在运行中断、配置失控、资源超配、边界暴露、运维不规范等方面。

A.3.3 治理要点

在顶层设计方面，宜建立基础设施全生命周期运维治理架构，明确建设、运维、安全、调度权责；在资源统筹方面，实行算力、存储、带宽、设备资源统一台账与集约调度；在协同推进方面，打通建设部门、运维部门、安全部门、业务使用部门的联动机制；在价值交付方面，以提升资源利用率、降低运维成本、保障业务连续性为核心价值目标；在风险合规方面，重点落实网络安全、等级保护、运维合规、访问可控要求。

A.3.4 扩展方向

可结合云原生、超算算力、灾备体系、物联网终端设施等新型基础设施，细化形成二级治理模块，补充硬件基线、配置基线、巡检基线、容灾备份等管控要求。

A.4 数据治理

A.4.1 治理定位

数据治理域覆盖数据采集、传输、存储、共享、使用、销毁全过程，统筹数据治理组织、制度、流程、资源与环境建设，聚焦数据质量、数据安全、数据合规、数据价值释放，实现数据治理标准化落地、全流程闭环管控与数据要素资产化运营。

A.4.2 场景特征

具有流动性强、多源汇聚、多级共享、隐私敏感、易复制、可复用等特点，风险集中在数据泄露、违规共享、质量不满足需求、权责不清、台账缺失、溯源困难等方面。大规模利用场景下还存在数据体量庞大、格式复杂、跨域流转频繁、治理环境动态变化等特征，易出现治理规则落地不到位、治理评价缺失、改进机制失效等衍生风险。

A.4.3 治理要点

在顶层设计方面，建立数据分级分类、标准规范、质量管控、安全防护等一体化治理体系，明确数据所有者、经营者、使用者、监督者权责矩阵，同步配套治理方针、制度文件与考核机制；在资源统筹方面，对数据资产目录、数据资源池、元数据、主数据、数据标准等统一规划与集约管理；在协同推进方面，建立数据提供方、运营方、使用方、监管方协同权责与问题闭环机制，适配内外部治理环境变化；在价值交付方面，以数据赋能业务分析、精准决策、流程优化、数据资产化为价值导向，定期开展治理成效评估，持续挖掘数据要素价值；在风险合规方面，落实数据安全、个人信息保护、数据共享出境、合规审计等法定要求，落实访问控制、数据脱敏、加密防护、操作留痕、责任追溯等管控措施。

A.4.4 扩展方向

可细化为数据标准治理、数据质量治理、数据安全治理、数据共享治理、数据资产治理等细分模块，针对涉密数据、个人信息、重要数据、行业核心数据增设管控规则；扩展数据治理环境、治理过程、治理评价模块，完善治理内审、管理评审、持续改进机制；针对大数据、数据湖、数据中台、跨域数据流通等新型场景，新增治理规划、落地执行、成效考评、迭代优化管控基线，构建规划、执行、评价、改进的闭环治理体系，适配不同业务形态与数据规模的精细化治理需求。

A.5 人工智能治理

A.5.1 治理定位

人工智能治理域包含算法、模型、应用、算力与高质量数据集等治理工作，覆盖模型研发、训练、部署、推理、迭代、下线全流程，搭建常态化管理体系，聚焦算法可信、模型安全、结果可控、应用合规，保障人工智能安全、可靠、可控运行。

A.5.2 场景特征

具有算法黑箱、动态迭代、数据依赖、结果不确定性、技术迭代快、伦理风险突出等特点，风险集中在算法偏见、模型失控、训练数据污染、输出不可控、滥用误用、伦理失范等方面，生成式人工智能场景还存在内容伪造、信息误导、溯源困难等衍生风险，需要对全流程标识、人工复核、应急处置提出刚性约束。

A.5.3 治理要点

在顶层设计方面，建立人工智能研发、上线、运行、迭代、退出的全流程治理制度与审查机制，明确治理组织、岗位职责、伦理审查、风险管控权责；在资源统筹方面，统筹算法、算力和数据的统一管理，衔接数据治理相关规范，保障训练数据合规、完整、可用；在协同推进方面，构建技术研发、业务应用、安全合规、伦理审查、监督审计多方协同治理机制；在价值交付方面，以智能提效、风险管控、服务优化、创新发展为核心价值目标；在风险合规方面，落实算法备案、安全评估、伦理审查、内容标识、风险监测与应急处置规则，防范内容滥用、数据泄露、算法违规等风险。

A.5.4 扩展方向

可细分大模型治理、算法治理、训练数据治理、AI应用治理、AI伦理治理等模块，针对生成式人工智能、决策式人工智能、行业专用模型制定差异化适配规则。结合现有国家标准与监管政策，补充模型基线、算法安全基线、训练数据安全基线、内容标识管控基线、伦理审查基线等管控要求，延伸覆盖AI运维、模型变更、故障处置等细分治理场景。

A.6 应用系统治理

A.6.1 治理定位

应用系统治理域面向软件系统和平台、业务应用的功能性、稳定性、安全性开展治理，覆盖系统建设、上线、运行、变更、运维、退役全生命周期，聚焦系统可用、功能合规、运行稳定、迭代可控。

A.6.2 场景特征

业务耦合度高、变更频繁、用户覆盖面广、直接支撑业务流程运转，风险集中在代码漏洞、权限失控、变更无序、功能缺陷、运维滞后、业务中断等方面。

A.6.3 治理要点

在顶层设计方面，建立应用系统全生命周期治理与版本、变更、权限、台账管理制度；在资源统筹方面，统筹系统账号、授权资源、服务资源、版本资源统一管理；在协同推进方面，建立业务部门、研发运维部门、安全管理部门、用户主体的协同联动机制；在价值交付方面，以支撑业务流程顺畅、提升业务效率、降低业务运行风险、保障服务可用性为价值目标；在风险合规方面，落实软件安全、漏洞整改、权限最小化、日志审计、变更管控合规要求。

A.6.4 扩展方向

细分业务系统治理、平台软件治理、微服务治理、终端应用治理等细分领域，针对重要业务系统、核心交易系统、对外服务系统提升治理强度与审查频次。

参 考 文 献

[1] GB/T 19001—2016 质量管理体系 要求
[2] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[3] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求
[4] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[5] GB/T 26317—2010 公司治理风险管理指南
[6] GB/T 32923—2016 信息技术 安全技术 信息安全治理
[7] ISO/IEC 38500:2024 Governance of information technology for the organization
[8] ISO/IEC 38505-1:2017 Governance of IT — Governance of data — Part 1: Application of governance to data