数据安全治理视角下企业合规管理体系构建与实践

张宝宝[1]　孟　震[2]　韩伟华[3]
1.云盾智慧安全科技有限公司　北京　100037
2.沈阳市和平区汉口街　辽宁沈阳　110001
3.石家庄市长安区跃进路　河北石家庄　050032

摘　要：在数字经济快速发展的背景下，数据已成为企业核心生产要素之一，同时也成为合规风险高度集中的领域。数据安全事件频发、法律监管日趋严格，使企业合规管理面临前所未有的挑战。本文立足数据安全治理与企业合规管理的内在关联，系统分析企业在数据安全合规方面面临的现实困境，深入探讨数据安全治理融入企业合规管理体系的逻辑基础与实施路径，并从制度设计、组织运行和实践保障等层面提出具有可操作性的体系构建思路，以期为企业实现合规经营与高质量发展提供理论支持与实践参考。

关键词：数据安全治理；企业合规；合规管理体系；风险防控；数字经济

引言

随着信息技术的广泛应用和数字化转型的持续推进，企业在生产经营过程中对数据资源的依赖程度不断加深。数据在提升经营效率、优化决策支持的同时，也带来了数据泄露、滥用和合规失范等一系列风险。合规管理指的是为了有效防控合规风险并倡导合规经营价值观而进行的一系列管理活动。这包括制定合规制度、完善相应的管理措施，并通过内部组织架构的搭建，确保合规要求能够在企业各个层级得到有效执行。合规管理的核心要素包括计划、组织、决策、执行和控制。在经营过程中，由于企业对当地相关部门下发的法律法规文件学习不够，与当地劳务、税务、消防、环保等部门沟通协调较少，给企业带来法律风险和管理隐患。近年来，国家层面不断完善数据安全与个人信息保护相关法律法规，对企业数据处理活动提出了更加明确和严格的合规要求。在此背景下，传统以业务合规或财务合规为主的企业合规管理模式，已难以全面覆盖数据安全领域的复杂风险。如何从数据安全治理视角出发，系统构建企业合规管理体系，实现数据安全与合规管理的深度融合，成为企业治理实践中亟需研究的重要课题。

一、数据安全治理与企业合规管理的理论关联

（一）数据安全治理的内涵及其治理目标

数据安全治理是指企业在法律法规、行业规范和内部制度框架下，对数据全生命周期进行系统管理和风险控制的过程，其核心目标在于保障数据的合法性、完整性、保密性和可用性。从治理层面看，数据安全并非单一的技术问题，而是涵盖制度建设、组织管理和文化培育等多个方面的综合性治理议题。通过数据安全治理，企业能够在合法合规的前提下实现数据价值的合理利用，为可持续发展提供稳定支撑。

（二）企业合规管理体系的功能定位

企业合规管理体系是指企业为防范合规风险、确保经营活动符合法律法规和内部规范要求而建立的系统性管理机制。其功能不仅体现在风险防控层面，还体现在规范经营行为、提升治理水平和塑造企业形象等方面。随着监管环境的变化，合规管理的范围逐步由传统领域向数据安全、信息保护等新型领域拓展，合规管理体系亟需与数据安全治理形成有效衔接。

（三）数据安全治理融入企业合规管理的必然性

从现代企业治理逻辑看，数据安全风险已成为企业整体合规风险体系中不可忽视的重要组成部分。数据处理活动贯穿企业研发、生产、营销和管理等各个业务环节，一旦在数据采集、存储或使用过程中出现治理缺位，极易引发法律责任、监管处罚和声誉损失，甚至影响企业的正常经营秩序。因此，将数据安全治理系统纳入企业合规管理体系，是应对复杂风险环境的必然选择。通过合规管理框架对数据安全风险进行统一识别、评估和应对，有助于打破部门壁垒，形成协同治理机制，推动企业由被动应对监管要求向主动防控和系统治理转变。这种融合不仅体现了合规管理向前端延伸和精细化发展的趋势，也反映了现代企业治理由单一合规向综合风险

治理升级的必然方向。

二、数据安全治理背景下企业合规管理面临的现实问题

（一）数据安全合规意识与治理能力不足

在企业数据管理实践中，部分企业对数据安全合规的认识仍停留在应付检查或满足最低合规要求的层面，缺乏系统性和前瞻性的治理思维。企业管理层对数据安全风险的重视程度不足，未能将数据治理纳入整体战略管理中，导致数据安全和合规管理在组织架构和资源配置上处于边缘位置。例如，一些企业虽然配备了信息安全团队，但团队人力和预算有限，缺乏跨部门协调权，无法有效支持业务部门的数据安全需求；同时，日常决策中未充分考虑数据合规风险，使数据使用、存储和共享过程中存在隐患。

此外，员工的数据安全意识和合规意识普遍不高。一些员工仅关注完成业务目标，而忽视数据操作规范，例如随意使用个人邮箱传输敏感信息、将客户数据存储在非授权平台等行为，增加了数据泄露和违规风险。缺乏整体性的培训和文化引导，使企业难以形成自上而下、全员参与的数据安全治理合力。这种意识和能力不足不仅削弱了制度执行力，也增加了企业潜在法律责任和声誉风险，制约了企业数字化转型和业务创新的可持续发展。

（二）合规管理制度与数据治理实践脱节

尽管部分企业已建立数据安全和合规管理制度，但制度多以原则性规定为主，缺乏与具体业务流程的紧密结合，导致在实践中难以落地。例如，制度可能要求“保护客户数据隐私”，但未明确在日常业务操作中如何分类、加密、传输和存储数据，也未规定各岗位具体责任和操作标准，使员工在执行过程中无法准确把握合规要求。

在实际操作中，数据安全要求往往难以嵌入业务流程。例如，销售、市场或研发部门在日常数据使用中，由于制度指引不够具体或缺乏操作指南，可能出现数据共享随意、访问权限管理混乱或敏感信息外泄等问题。同时，合规制度与技术保障手段之间的衔接不够紧密，缺少数据监控、日志分析和审计机制，使违规行为难以及时发现和纠正。制度与实践之间的脱节，不仅影响了合规管理体系的运行效果，也使企业在面对监管审查、客户信任和市场竞争时处于不利地位。

综上所述，数据安全合规意识与治理能力不足，以及合规管理制度与业务实践脱节，是当前企业数据治理面临的两大主要问题。这要求企业在制度建设和文化培育上同步发力，强化管理层对数据安全的战略重视，提高员工合规意识，并将制度嵌入业务流程与技术体系之中，实现制度、技术和文化的协同联动，从而提升企业数据治理的整体效能和合规管理水平。

三、数据安全治理视角下企业合规管理体系的构建路径

（一）以数据安全风险为导向完善合规管理框架

在数字化转型不断深化的背景下，数据已成为企业核心资产之一，其安全性直接关系到企业的合规水平和可持续发展能力。因此，企业在构建合规管理体系时，应以数据安全风险为重要导向，将其系统纳入整体风险管理与内部控制框架之中。具体而言，企业需要对数据全生命周期进行系统梳理，覆盖数据采集、传输、存储、加工、使用、共享以及销毁等各个环节，识别其中可能存在的合规风险点和安全隐患。在此基础上，结合相关法律法规和行业规范，将抽象的数据安全要求转化为清晰、可操作的合规标准和管理制度，明确不同类型数据的分类分级管理要求。通过将数据安全风险前置并制度化嵌入合规管理体系，有助于提升企业对数据治理领域关键风险的识别和防控能力，使合规管理框架更加完整和具有针对性。

（二）推动数据安全治理与业务流程深度融合

合规管理的成效不仅取决于制度设计的完善程度，更关键在于制度能否在实际业务运行中得到有效落实。为此，企业应推动数据安全治理要求与业务流程的深度融合，在业务流程设计和优化过程中同步嵌入数据安全和合规控制要求。通过在流程节点中明确数据使用权限、操作规范和责任主体，将合规要求细化为具体的操作指引和工作标准，使员工在日常业务活动中能够“按流程办事、按规范用数”。这种将数据安全治理融入业务流程的方式，有助于减少制度与实践之间的脱节，避免合规要求停留在文件层面。同时，也能够促使员工逐步形成合规意识，使数据安全治理由外在约束转变为内在自觉，从而提升合规管理在实际运行中的稳定性和有效性。

（三）强化组织保障与专业支持机制

健全的组织保障和专业支持机制，是数据安全治理与合规管理有效运行的重要前提。在组织层面，企业应进一步明确数据安全治理与合规管理的职责分工，理顺管理层、职能部门和业务单元之间的权责关系，建立跨部门协同工作机制，确保数据安全要求在各业务领域得到统一理解和有效执行。同时，应结合企业规模和业务

特点，合理配置数据安全和合规管理相关的专业人员，加强对法律合规、信息技术和业务管理等复合型人才的培养与引进。通过持续开展培训和能力建设，提升组织整体对复杂数据安全问题的识别、评估和应对能力。借助完善的组织保障和专业支持，企业合规管理体系才能在面对不断变化的数据安全风险时保持足够的韧性和适应性，切实发挥风险防控和价值保障作用。

四、数据安全治理导向下企业合规管理的实践实施重点

（一）健全数据安全合规运行与监督机制

在企业实践中，数据安全治理和合规管理的有效运行依赖于健全的监督机制。企业应建立多层次的监督体系，包括内部审计、合规检查和风险评估等环节，对数据安全和合规管理的执行情况进行持续监控。例如，可以定期开展数据使用和权限管理审计，检查员工在信息系统中对敏感数据的访问记录和操作行为是否符合公司制度要求；同时，可通过合规检查评估各部门的数据管理流程，识别潜在风险点，并提出改进措施。

此外，企业应建立动态评估机制，根据外部法律法规的更新和内部业务模式的变化，及时调整和优化数据治理制度。例如，针对新上线的业务系统或新增的数据处理环节，企业可提前进行合规评估，确保制度覆盖到所有关键环节，并通过内部管理系统记录整改措施的执行情况，实现闭环管理。通过这种全流程监督和动态调整，企业能够保证数据安全和合规管理体系持续有效运行，降低违规风险，增强信息资产保护能力。

（二）培育数据安全合规文化促进长效治理

数据安全合规不仅是制度问题，更是企业文化建设的重要内容。单靠制度约束容易出现“有章不循”的现象，而将合规理念融入企业文化，则可以形成长效治理机制。企业应通过多种形式的培训和宣传活动，帮助员工理解数据安全和合规管理的重要性。例如，可开展新员工入职培训、年度合规教育、案例分析研讨等，结合实际业务场景讲解数据违规案例及其风险，让员工在认知上形成正确的安全意识。

同时，企业可以通过日常工作中正向激励和行为规范，引导员工将数据安全和合规理念内化为日常操作习惯。例如，对在数据管理和合规执行中表现突出的团队或个人给予表彰和奖励，对违规行为进行及时纠正和反馈，使员工认识到合规不仅关乎责任，也与职业成长和企业声誉密切相关。随着合规文化的逐步深入，员工在处理数据时会更加自觉遵守制度要求，主动发现并防范潜在风险，从而降低制度执行成本，提升企业整体治理水平，实现数据安全与合规管理的长效运行。

综上所述，通过健全数据安全合规的监督机制和培育企业合规文化，企业不仅能够保障制度落实和风险可控，还能够形成自上而下的合规氛围，使数据安全治理从制度约束走向日常行为习惯，实现持续、稳健的长效管理。

结语

总体来看，在数据要素价值日益凸显的背景下，从数据安全治理视角构建企业合规管理体系，已成为企业实现稳健经营和高质量发展的重要保障。通过将数据安全治理系统融入合规管理框架，完善制度设计、强化组织保障并注重实践落实，企业能够有效防范数据安全合规风险，提升治理能力。展望未来，随着监管环境和技术条件的不断变化，企业合规管理体系仍需持续优化，在实践中不断深化数据安全治理与合规管理的融合，为数字经济时代的企业发展提供坚实支撑。

参考文献

[1]刘志云，吕铭鸿.金融机构合规管理的理性思考——兼评《金融机构合规管理办法（第二次征求意见稿）》[J].经济法论坛，2024，33（02）：202-217.

[2]杨丁晖.数字化背景下上市企业财务合规管理研究[J].国际商务财会，2024，（24）：48-51.

[3]曾辉.基园企业财税合规管理研究[J].乡镇企业导报，2024，（24）：27-29.

[4]宋芳.石化企业合规管理信息化建设实践与思考[J].石油化工技术与经济，2024，40（06）：6-9.

[5]张平，陈思，李满君，等.基于合规管理视角的电力企业数字化风控管理体系建设研究[J].企业改革与管理，2024，（24）：24-28.DOI：10.13768/j.cnki.cn11-3793/f.2024.1303.

[6]娄丹，李维玮，郑雪倩，等.北京市医疗机构合规管理专项领域调查分析[J].中国医疗保险，2024，（12）：74-80.DOI：10.19546/j.issn.1674-3830.2024.12.011.