文章类型：论文| 刊号（ISSN）：3082-8295(O) / 2630-4759(P)

智能财务共享中心的数据安全治理与合规性研究

张萌
黑龙江工商学院
DOI:10.12238/ej.v8i6.2684

[摘　要] 智能财务共享中心凭借集成化、信息化的手段,极大增强了财务管理的效率与精准性。伴随数据规模的扩大与信息技术的迅猛发展,数据安全治理及合规体系成为核心挑战。数据泄露、违规操作与合规风险,不仅对企业财务稳定构成威胁,还可能引发法律责任与声誉损失。为实现智能财务共享中心的长久稳定运作,必须搭建一套有效的数据安全治理机制与合规性管理体系。解决这一问题的关键,在于数据安全技术的持续创新,以及合规性管理框架的系统完善。
[关键词] 智能财务共享中心；数据安全治理；合规性管理；隐私保护；集成治理
中图分类号：F253.7　**文献标识码：**A

Research on Data Security Governance and Compliance of Intelligent Financial Shared Center

Meng Zhang
Heilongjiang University Of Business And Technology

[Abstract] Intelligent financial sharing center by means of integration, informatization, greatly enhance the efficiency and precision of financial management, with the expansion of data scale and the rapid development of information technology, data security governance and compliance system become the core challenge, data leakage, illegal operation and compliance risk is a threat to enterprise financial stability, but also may cause legal responsibility and reputation loss, to realize intelligent financial sharing center for a long time, must set up an effective data security management mechanism and compliance management system, the key to solve the problem for data security technology innovation and the integrity of the compliance management framework.
[Key words] intelligent financial sharing center; data security governance; compliance management; privacy protection; integrated governance

引言

智能财务共享中心凭借信息技术,实现了财务管理业务的集中与自动化操作,旨在提升财务运作的效率与精准度。伴随信息化进程的稳步推进,智能财务共享中心逐渐成为企业财务管理的重要组成部分,助力财务职能的转型与升级。

然而,数据泄露以及合规性风险也逐渐凸显,企业面临复杂的安全与合规形势。在此背景下,本研究聚焦于探究如何通过数据安全治理与合规性管理,实现智能财务共享中心稳定、安全的运营模式,这在理论与实践层面均具有重要意义。本研究采用案例研究与文献分析的方法,为企业提供实用的安全合规解决方案。

1 智能财务共享中心的数据安全管理框架

1.1数据安全治理的概念与重要性

数据安全治理依靠构建合理的组织架构、制定有效的政策制度、采用先进的技术手段和实施严格的流程管控,保障数据在存储、传输及处理过程中不被非法侵入、泄露、篡改或丢失,其核心意义在于保障数据的完整性、机密性与可用性。从智能财务共享中心角度看,数据安全治理不仅关系到财务信息的防护,还涉及法律合规、企业声誉以及客户信任等范畴。随着财务信息化进程的加速,所面临的安全形势诸如黑客攻击、内部信息外泄和技术短板等问题日益增多。

1.2数据安全风险识别与评估

数据安全风险识别是指针对潜在威胁财务共享中心数据安全的因素进行识别,涵盖诸如黑客攻击、数据泄露、系统故障等情形。企业可采用定性与定量分析模式、SWOT分析等工具,评估风险的严重程度。关键环节包括风险识别、评估、控制与应急响应。针对不同类型的风险,企业需规划相应的应对策略,并定期开展风险审查与更新活动,以切实降低潜在威胁。

文章类型：论文| 刊号（ISSN）：3082-8295(O) / 2630-4759(P)

1.3数据安全技术的应用与创新

在智能财务共享中心中,数据安全技术的应用至关重要。敏感数据可通过加密技术进行保护,即使数据被截取,也无法轻易完成破译操作。防泄漏技术通过限制数据的传输、复制与使用,有效防止信息泄露；访问控制与身份认证技术则确保只有获得授权的用户才能访问数据。随着人工智能与大数据技术的不断进步,智能监控与威胁检测技术依托实时数据分析与机器学习,可预判潜在安全威胁,进一步提升数据防护水平。

2 智能财务共享中心的合规性要求与挑战

2.1国内外合规性法规与标准

智能财务共享中心的合规性管理工作需要依照国内外相关法规及行业标准,《个人信息保护法》督促企业切实守护个人数据隐私,保证数据合规透明,欧洲《通用数据保护条例》(GDPR)给数据处理及跨境流动设立了高规格标准,突出数据主体的知情同意与删除权利。美国《萨班斯-奥克斯利法案》(SOX)要求企业构建精准的财务报告体系,加快数据透明化步伐,以《支付卡行业数据安全标准》(PCIDSS)等为范例的行业标准,对财务共享中心的数据合规性提出了具体要求。

2.2合规性管理的框架与流程

政策制定、组织结构安排、风险识别与评估等,共同构建起合规性管理的框架。合规性管理流程应将对业务流程的审查、合规性监控、反馈及报告机制纳入其中。企业需要依据相关法律法规的要求,结合财务共享中心业务的实际情况,设计恰当的合规监控体系与内部审计机制。

2.3合规性与安全性的协调与平衡

在当代智能化财务共享中心中,合规性与数据安全常常存在矛盾。合规性要求数据的存储与处理需符合监管准则,而数据安全技术则聚焦于防范数据泄露。为协调二者之间的矛盾,企业应寻求恰当的平衡点,确保在数据存储、访问与传输活动中,采用合适的数据安全技术,以同时满足安全性与合规性的双重要求。

3 智能财务共享中心数据安全与合规性的集成治理模型

3.1集成治理的概念与必要性

集成治理被定义为整合数据安全管理和合规性管理,构建一个统一、高效的治理体系,从而保障企业在保护数据的同时,符合法律法规的要求。集成治理呈现出跨部门协同、技术与政策结合、全流程管控等特性。从智能财务共享中心的角度来看,集成治理可实现数据安全与合规性的深度融合,避免因管理层次分散以及职责不明所引发的风险。数据安全和合规性的结合,体现在共享中心对敏感财务数据的严格把控,以及对合规要求的及时响应,确保所有财务操作在法律规定的框架内进行,并通过实施安全技术,保障数据的机密性与完整性。

3.2集成治理模型的构建

构建数据安全与合规性集成模型的步骤,首先要明确治理目标与要求,厘定合理的治理政策,实现企业整体管理体系中数据安全与合规性的一致性。政策、流程与技术是集成模型的关键组成部分,企业需设定统一的数据安全及合规性标准；应构建一整套合规与安全管理流程,以保障数据在处理、存储及传输阶段的合规性。技术层面则涉及采用先进的加密技术、访问控制以及风险评估工具等,作为守护数据安全的技术手段。集成治理框架的设计应根据企业规模、业务需求,并结合合规性要求,构建一个层次清晰、职责明确、操作可行的综合管理体系。

3.3集成治理模型的实施与评估

集成治理模型实施步骤囊括政策宣传与培训、系统工具部署、治理流程执行及监督检查等事项,在实施操作阶段,企业需为员工实施定期培训,保证员工领悟且依照数据安全与合规要求操作,治理流程需结合智能财务共享中心独特特点开展优化工作。成效评估方法与工具可借助定期内部审计、风险评估、合规性报告等手段评估治理成效,发现存在的弱项,遭遇的挑战有政策执行不力、技术手段落后以及合规性与安全性标准频繁变化等状况,应对这些挑战需加大跨部门协作,不断升级治理程序,并及时实现技术与政策体系的更新。

4 智能财务共享中心中的数据隐私保护与法律责任事项

4.1数据隐私保护的法律框架

从全球范围看,数据隐私保护法律逐步完备,《个人信息保护法》规定企业收集、使用、存储个人数据时必须获得明确同意,且实施保护手段,欧盟的《通用数据保护条例》(GDPR)切实强调数据主体的知情权、访问权和删除权。美国《加利福尼亚消费者隐私法案》(CCPA)进一步扩充了消费者的控制权,在智能财务共享中心,企业面临的隐私挑战包含员工、客户及供应商数据的合规处理,尤其在跨境数据流动及第三方服务出现的时候,隐私保护合规要求愈发严格。

4.2隐私保护技术的应用与创新

为应对隐私保护带来的挑战,智能财务共享中心采用了多种技术手段。例如,数据脱敏及匿名化技术可在不影响数据分析合理开展的基础上,删除或模糊个人身份信息,从而降低隐私泄露的潜在风险。数据加密、权限控制与访问审计等技术,保障仅授权人员可访问敏感数据,同时在数据传输过程中也进行加密保护。随着人工智能和区块链技术的引入,隐私保护变得更加智能化与自动化,显著提升了数据保护的效率与安全的综合水平。

4.3数据泄露与法律责任

数据泄露可能导致严重的财务损失,同时伴随着法律后果。企业在发生数据泄露后,必须立即通知受影响的用户,并采取补救措施。《个人信息保护法》要求企业在向监管部门报告泄露事件后,及时告知相关风险。若企业未履行隐私保护义务,可能面临罚款、诉讼及声誉损失等法律后果。为防范数据泄露事件及合规责任风险,企业需建立完善的数据安全管理制度,定期开展安全相关培训,实施有效的技术防护手段,并制定应急响应预案,以减少法律隐患。

5 智能财务共享中心数据安全治理的未来趋势与优化路径

5.1数据安全技术的发展趋势

随着云计算、大数据和人工智能的发展，数据安全技术正逐步向智能化与自动化方向迈进。云计算要求财务共享中心提升云环境下的数据安全保护水平；大数据则要求采取高效的风险识别与防护手段；人工智能的引入提升了安全防护的智能化程度，借助机器学习与自动化防御手段，提高了威胁识别与响应的速度。诸如区块链等新兴技术，为数据验证提供了全新的安全解决方案。

5.2合规性监管的未来走向

全球合规性监管将进一步聚焦于数据隐私保护与跨境数据流动管理。伴随着《通用数据保护条例》(GDPR)等法规的实施，未来的合规性要求将更加严格，尤其是在跨境数据流动这一领域，企业必须按照统一的合规标准行事。针对人工智能和大数据的应用，监管机构将努力在推动技术创新与实施数据保护之间寻求平衡，促使技术进步与数据安全同步推进。

5.3数据安全与合规性优化路径

智能财务共享中心应建立持续优化的数据安全与合规管理体系，按既定周期更新技术、政策与流程。企业应推进安全合规文化建设，增强员工的合规意识，提升全员的责任感。同时，需加大对先进数据保护技术的投资，结合最佳实践，提升数据治理与安全管理的质量，确保财务共享中心在技术与法规快速变化的背景下，持续完善安全合规工作。

6 结语

综上所述，针对智能财务共享中心数据安全治理与合规性的研究表明，集成治理模型对于维护财务数据安全、确保符合法规准则具有重要意义。通过提升数据保护技术水平与优化合规管理机制，企业能够有效抵御各类风险。随着技术的跃进与法规的变动，企业必须持续探索数据隐私保护与跨境合规问题。未来的研究可重点关注智能技术应用与合规监管的协同优化，推动财务共享中心安全合规体系的创新与变革。

[参考文献]

[1]朱敏.基于BP神经网络技术的智能财务研究[J].会计之友,2021(18):38-42.

[2]董木欣,徐玉德.国有企业数字化转型中的数据安全与治理路径——基于信息生态视域[J].财会月刊,2022(13):132-136.

[3]陈伟晓.高校财务共享服务中心建设研究[J].商业会计,2022(23):99-102.

[4]郝义飞.集团企业财务共享中心数据安全治理研究[D].扬州大学,2023.

[5]胡璐.数字经济背景下高校智能财务共享中心建设——以H大学为例[J].财政监督,2024(14):86-91.

作者简介：

张萌(2003--),女,汉族,黑龙江安达市人,本科,研究方向：会计学。