



University Procurement Data Compliance in the Digital Age

Xiaojie Huang

Zhejiang Gongshang University Hangzhou College of Commerce, Hangzhou, China
81241415@qq.com

Abstract. Digital transformation revolutionizes university procurement, promising enhanced efficiency and transparency. However, robust data compliance is crucial. This paper analyzes legal and practical data security challenges in digitally transformed university procurement. It examines risks like data breaches, misuse, non-compliant data handling, cross-border transfers, and inadequate security systems. Analyzing existing legal frameworks (Data Security Law, Personal Information Protection Law, Government Procurement Law), the paper identifies gaps and proposes improvements. Recommendations include refining data breach liabilities, clarifying data ownership, strengthening cross-border transfer oversight, issuing university-specific compliance guidelines, and bolstering technical safeguards and personnel competency. Addressing these challenges allows universities to harness digital transformation while safeguarding sensitive procurement data.

Keywords: University procurement, Digital transformation, Data compliance.

1 Introduction

Driven by the rapid advancement of information technology, digital transformation has become an inevitable choice for university procurement management. The widespread application of emerging technologies such as big data, cloud computing, and artificial intelligence is profoundly impacting traditional procurement processes, management models, and operational methods [1-2]. This presents universities with immense potential for improved efficiency, reduced costs, and enhanced transparency. However, as Luan Xiaoqi (2024) points out in "Tendering and Procurement Management," while digital government procurement is a crucial path to increased efficiency, it also introduces challenges related to data security and compliance [3]. This holds true for universities as well [4-5]. While digital transformation enhances efficiency in university procurement, it necessitates addressing new challenges arising from data security and compliance. Security incidents such as data breaches, data misuse, and cyberattacks can not only damage the reputation and interests of universities but also pose threats to national security and public interests [6]. Specifically, the digital transformation of university procurement involves a large amount of sensitive data, including but not limited to:

(1) Bidder Information: This encompasses corporate qualifications, financial status, personnel information, etc. Leakage of this information could lead to unfair competition or disclosure of trade secrets.

(2) Evaluation Expert Information: The identity, contact details, and other information of evaluation experts require strict confidentiality to ensure the fairness and transparency of the evaluation process.

(3) Tender Project Information: Information such as project budgets, technical requirements, and evaluation criteria must be properly secured to prevent leakage or tampering.

(4) Personal Information of Faculty and Students: Procurement projects involving faculty and student supplies may involve personal information, requiring strict adherence to laws and regulations such as the Personal Information Protection Law.

In this context, this study focuses on data compliance and risk prevention, holding significant theoretical and practical implications:

(1) Theoretical Level: This study aims to systematically organize and analyze current laws, regulations, policy documents, and industry standards related to data security and compliance. It seeks to construct a theoretical framework for data compliance and risk prevention in the digital transformation of university procurement, providing a theoretical foundation for future research.

(2) Practical Level: This study will propose specific improvement suggestions and solutions for the data compliance and risk prevention challenges faced by universities during digital transformation. It will offer guidance for university practices, assisting in the establishment of comprehensive data compliance management systems and risk prevention mechanisms.

(3) Policy Level: The findings of this study can provide references for government departments in formulating and improving relevant policies and regulations, promoting the healthy development of digital transformation in university procurement.

This study aims to address the following core questions:

(1) What are the main data compliance risks in the digital transformation of university procurement?

(2) How do current laws, regulations, and policy frameworks function in the digital transformation of university procurement, and what is their effectiveness?

(3) How can an effective risk prevention system be constructed to ensure the security and compliance of the digital transformation of university procurement?

This study will adopt a normative research approach. Through analysis of relevant laws and regulations such as the Data Security Law, the Personal Information Protection Law, and the Government Procurement Law, combined with the findings of relevant literature reviews, proposed theoretical frameworks, and practical case studies, it will explore the issues of data compliance and risk prevention in the digital transformation of university procurement and propose corresponding improvement suggestions.

2 Current Status and Challenges of Digital Transformation in University Procurement

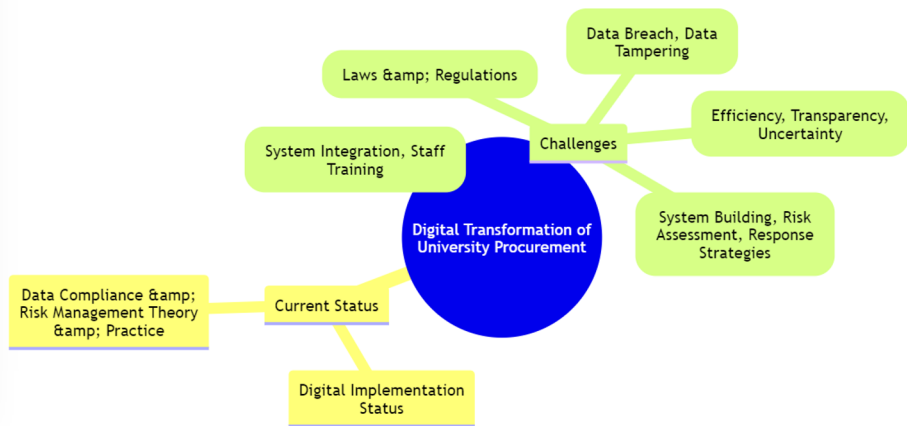


Fig. 1. Digital transformation of university procurement.

2.1 Implementation Status of Digital Transformation

Digital transformation involves using digital technologies to optimize and improve various operational and management processes within an organization [7-8]. In university procurement, this transformation has become a key approach to enhancing efficiency and transparency. However, digital transformation is not merely the application of technology; it also involves data security, compliance, and related risk management. A key focus of current research is how to effectively control risks while ensuring improved efficiency [9-10].

Existing research indicates that an increasing number of universities are adopting digital platforms and systems for procurement activities. For example, Luan Xiaoqi (2024) highlights the trend of digital government procurement and its associated data security and compliance challenges in "Tendering and Procurement Management," which are equally applicable to universities [3]. This suggests the need for universities to establish comprehensive data compliance management systems during digital transformation. While Yang Yuchun's data compliance management system and risk prevention strategies, presented in "Industrial Information Security," focus on enterprises, their analysis of data application scenarios, sharing mechanisms, and transaction mechanisms provides valuable insights for data compliance and risk prevention in the digital transformation of university procurement [7-8].

Furthermore, Zhang Lei (2022) emphasizes the importance of institutional design, including the establishment of regulatory systems and the improvement of regulatory effectiveness, in digital transformation in an article in "China Government Procurement Newspaper." This suggests that universities need to pay attention to the institutional changes brought about by digital transformation and make corresponding adjustments. Some studies also focus on specific practices of digital transformation in university

procurement, such as the application of electronic tendering platforms and blockchain technology in procurement. These practices provide concrete examples for understanding digital transformation but also reveal data security and compliance issues, such as the risks of data breaches and data tampering.

2.2 Theory and Practice of Data Compliance and Risk Prevention

In terms of the data compliance management framework, some studies propose frameworks covering various stages of the data lifecycle, including data collection, storage, use, transmission, and destruction. These frameworks emphasize the importance of data security and privacy protection and propose corresponding management measures, such as data encryption, access control, and security audits [4-5]. Regarding risk assessment models, some studies have constructed risk assessment models specifically for the digital transformation of university procurement to identify and assess potential data security risks.

These models typically consider various factors, such as technical risks, management risks, and human risks, and provide risk level classifications and response strategy recommendations. For risk response strategies, existing research proposes various strategies, including technical, management, and legal strategies [11-12]. Technical strategies involve adopting advanced security technologies such as firewalls and intrusion detection systems. Management strategies include formulating data security management systems and strengthening staff training. Legal strategies involve complying with relevant laws and regulations, such as the Cybersecurity Law and the Data Security Law.

In terms of normative research, some scholars explore how to apply the perspective of normative analysis to data compliance and risk prevention research. For example, by analyzing existing laws, regulations, and standards, they identify data compliance requirements and propose corresponding compliance strategies. By analyzing best practice cases, they summarize experiences in data compliance and risk prevention and extract actionable norms.

2.3 Main Challenges of Digital Transformation

Technical Challenges. Universities need to integrate different systems, such as financial and procurement systems, which requires overcoming technical difficulties. Staff training and technology updates are also challenges. For example, Luan Xiaoqi (2024) points out the inadequacy of platform construction and functionality and the interoperability issues between platforms [3].

Security Risks. Data security and privacy protection are major security risks in digital transformation. There are risks of data breaches and tampering during the extensive exchange and processing of data. The importance of data asset security and related security prevention suggestions proposed by Xiang Bangmeng et al. (2024) are worth noting for universities [13].

Compliance Issues. Digital transformation requires compliance with relevant laws, regulations, and standards, such as the Cybersecurity Law, the Data Security Law, and the Government Procurement Law. Universities need to ensure that their digital procurement processes comply with these regulations.

Management Dilemmas. Maintaining transparency and fairness while improving efficiency, and handling potential technical and managerial uncertainties during digital transformation are management dilemmas that universities need to address.

The data compliance management system and risk prevention strategies proposed by Yang Yuchun (2023) can provide references for universities [7]. Furthermore, data compliance and risk prevention themselves introduce new challenges. For example, universities need to consider how to establish effective data compliance management systems, conduct comprehensive risk assessments, and formulate effective risk response strategies.

3 Normative Analysis

A normative analysis of current laws and regulations is conducted, alongside an identification of data compliance risks inherent in the digital transformation of university procurement. The applicability and limitations of existing legal frameworks are also analyzed.

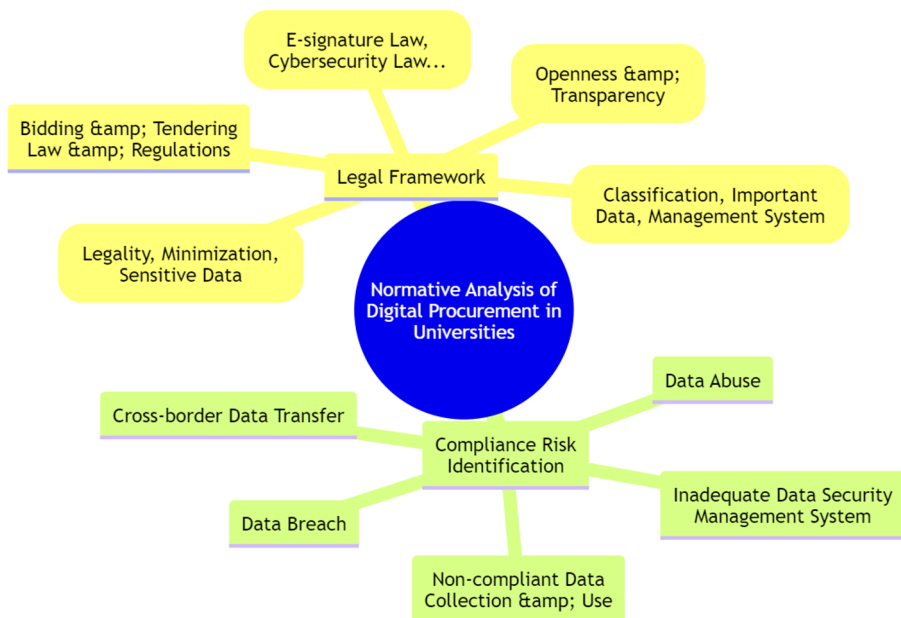


Fig. 2. Normative analysis of digital procurement in universities.

3.1 Legal Framework for Data Compliance

The following laws and regulations constitute the framework for data compliance in the digital transformation of university procurement:

Data Security Law. This law is the fundamental law in the field of data security, clarifying the obligations and responsibilities of data processors. In the digital transformation of university procurement, the following provisions are particularly important:

Data Classification and Graded Protection (Article 21). Universities need to classify and grade procurement data and implement corresponding security protection measures. For example, sensitive data such as bidder information and evaluation expert information should be classified as having a higher security level and subject to stricter protection measures.

Important Data Identification and Protection (Articles 21 and 31). Universities need to identify important procurement data and implement special protection measures. For example, data related to national security, trade secrets, and personal privacy should be identified as important data.

Data Security Management System (Articles 25, 26, and 27). Universities need to establish and improve data security management systems, including risk assessment, security review, and emergency response.

Personal Information Protection Law. This law sets clear provisions for the processing of personal information. Personal information involved in university procurement activities must strictly comply with this law. Key provisions include:

Legal Basis for Personal Information Processing (Article 11). Universities must have a clear legal basis to process personal information, such as obtaining consent from the information subject or fulfilling legal obligations.

Principle of Minimum Necessity (Article 12). Universities' collection and use of personal information should be limited to the minimum scope necessary to achieve the processing purpose, avoiding excessive collection.

Sensitive Personal Information Protection (Articles 28 to 30). Universities need to adopt stricter protection measures for sensitive personal information, such as ID numbers and biometric information.

Government Procurement Law and its Implementing Regulations. This law and its regulations govern government procurement activities and provide guidance for

university procurement. While not directly addressing data compliance, its principle of openness and transparency implicitly sets requirements for data management.

Tendering and Bidding Law and its Implementing Regulations. This law and its regulations govern tendering and bidding procedures and indirectly address data security and compliance.

Other Relevant Laws and Regulations. The Electronic Signature Law, the Cybersecurity Law, the Regulations on the Security Protection of Critical Information Infrastructure, etc., also set requirements for data security and compliance in the digital transformation of university procurement.

3.2 Data Compliance Risk Identification in University Procurement

Based on the above legal framework and the actual situation of the digital transformation of university procurement, the main data compliance risks include:

Data Breach Risk. Sensitive data, such as bidder information, evaluation expert information, and tender project information, may be leaked due to system vulnerabilities, human error, or malicious attacks, causing significant losses.

Data Misuse Risk. Unauthorized access, use, or tampering with data, such as modifying evaluation results or disclosing trade secrets.

Non-compliant Data Collection and Use Risk. Collecting or using personal information without the consent of the information subject or beyond the necessary scope, violating the Personal Information Protection Law.

Cross-border Data Transfer Risk. Conducting cross-border data transfer without complying with relevant regulations, potentially leading to data security risks.

Inadequate Data Security Management System Risk. Lack of a comprehensive data security management system, making it difficult to effectively control data security risks.

3.3 Correspondence between Compliance Risks and Legal Norms and Improvement Suggestions

Table 1. Compliance Risks and Legal Norms and Improvement Suggestions.

Compliance Risk	Relevant Laws and Regulations	Limitations of Laws and Regulations	Improvement Suggestions
Data Breach Risk	Data Security Law, Personal Information Protection Law	Lack of specific penalties for data breaches in university procurement.	Refine legal liabilities for data breaches and increase penalties. Clarify the responsible parties and penalty standards for different data breach scenarios. Consider incorporating specific provisions related to procurement data.
Data Abuse Risk	Data Security Law, Criminal Law	Ambiguous definition and penalties for data abuse.	Clearly define the boundaries of data abuse and refine penalties. Establish different penalty standards for various abusive behaviors (e.g., tampering, unauthorized access).
Non-compliant Data Collection and Use Risk	Personal Information Protection Law	Lack of specific guidance for universities on legally collecting and using personal information in procurement.	Issue guidelines to instruct universities on legally collecting and using personal information. Specify what information can be collected during procurement and how to obtain authorization.
Cross-border Data Transfer Risk	Data Security Law, Personal Information Protection Law	Complex and inefficient approval process for cross-border data transfer.	Simplify the approval process and improve efficiency. Develop a dedicated approval process for university procurement scenarios or provide more convenient online approval channels.
Inadequate Data Security Management System Risk	Data Security Law	Lack of specific guidance for universities on establishing data security management systems.	Issue model texts of data security management systems for universities to reference. Provide different model texts for various types of universities and allow adjustments based on specific circumstances. Include best practices and specific controls relevant to procurement processes.

Through the above normative analysis, it can be seen that existing laws and regulations have certain limitations in the digital transformation of university procurement. Further improvement of relevant laws and regulations, strengthening of supervision, and enhancement of universities' own awareness and capabilities in data security compliance are necessary to effectively prevent data compliance risks and ensure the smooth progress of the digital transformation of university procurement.

4 Data Compliance and Risk Prevention Challenges Faced by Digital Transformation of University Procurement

While enhancing efficiency and transparency, the digital transformation of university procurement also brings new challenges in data compliance and risk prevention. This chapter will combine the aforementioned literature review and normative analysis to delve into these challenges.

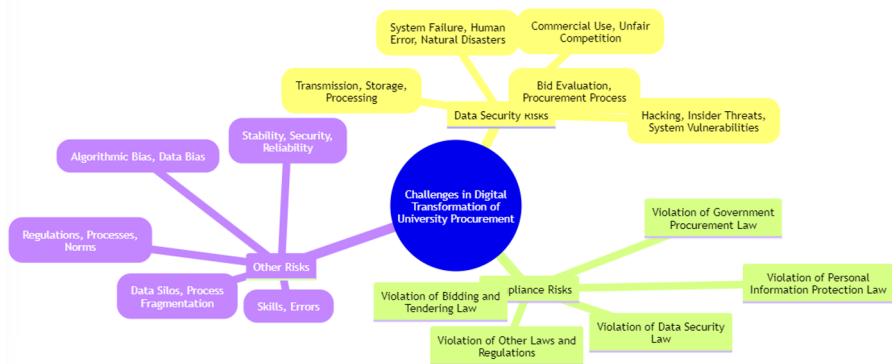


Fig. 3. Challenges in digital transformation of university procurement.

4.1 Data Security Risks

Data security risks are one of the most prominent challenges in the digital transformation of university procurement. Specifically, they manifest as:

Data Breaches. Digital platforms store a large amount of sensitive data, such as bidder information, expert reviewer information, and procurement project information. Data breaches can severely damage the university's reputation, bidders' rights, and fair market competition. For example, hacker attacks, malicious leaks by internal personnel, and system vulnerabilities can all lead to data breaches.

Data Tampering. Tampering with procurement data can lead to unfair evaluation results, loss of control over the procurement process, and even corruption. For example,

maliciously tampering with bidding documents or modifying evaluation scores can significantly impact procurement outcomes

Data Loss. System failures, human error, or natural disasters can lead to the loss of important procurement data, affecting the normal conduct of procurement activities and causing economic losses.

Data Misuse. Collected procurement data being used for unauthorized purposes, such as commercial use or unfair competition, infringing on the rights of data subjects.

Data Integrity Risks. Data may be corrupted or damaged during transmission, storage, and processing, leading to incomplete or inaccurate data and affecting the reliability of decision-making.

4.2 Compliance Risks

The digital transformation of procurement must adhere to a series of laws and regulations. Universities may face the following compliance risks in practice:

Violation of the Data Security Law. Failure to fulfill data security protection obligations, such as not establishing data security management systems, not taking necessary security technical measures, and not conducting data security risk assessments.

Violation of the Personal Information Protection Law. Unauthorized collection, use, or disclosure of personal information, or failure to take necessary measures to protect personal information security. For example, excessive collection of bidder personal information or failure to inform the data subject of the purpose of collection.

Violation of the Government Procurement Law and its Implementing Regulations. Failure to conduct electronic bidding and tendering according to regulations, or improper management of procurement data. For example, the electronic bidding and tendering platform not meeting requirements or incomplete procurement data.

Violation of the Tendering and Bidding Law and its Implementing Regulations. Failure to conduct tendering and bidding activities according to regulations, such as discriminatory clauses in tender documents or lack of transparency in the bid evaluation process.

Violation of other relevant laws and regulations. Such as the Electronic Signature Law and the Cybersecurity Law.

4.3 Other Risks

In addition to data security and compliance risks, the digital transformation of procurement in universities also faces other potential risks:

Technical Risks. Risks exist in the stability, security, and reliability of digital platforms. For example, system failures, cyberattacks, and software vulnerabilities may affect the normal operation of the platform.

Management Risks. The lack of sound digital transformation management systems and processes leads to management chaos and inefficiency. For example, the lack of data management norms, personnel training, and supervision mechanisms.

Operational Risks. Staff lacking professional skills or making operational errors can lead to data errors and system failures. For example, accidental data deletion or system misoperation.

Ethical Risks. Algorithmic discrimination and data bias may lead to unfair procurement results and raise ethical controversies.

Integration Risks. Difficulties in effectively integrating new digital procurement systems with existing systems can lead to data silos and process fragmentation.

Universities need to fully recognize the challenges brought about by digital transformation, actively take measures to strengthen data security and compliance management, improve risk prevention and control mechanisms, and ensure the smooth progress of digital transformation to ultimately achieve the goals of improving efficiency, reducing costs, and ensuring fair competition.

5 Improvement Suggestions

While the digital transformation of university procurement enhances efficiency and convenience, it also brings new challenges in data compliance and risk prevention. To ensure successful transformation and effectively mitigate risks, this study proposes the following improvement suggestions from the perspectives of laws and regulations, technical safeguards, management systems, and personnel competency:

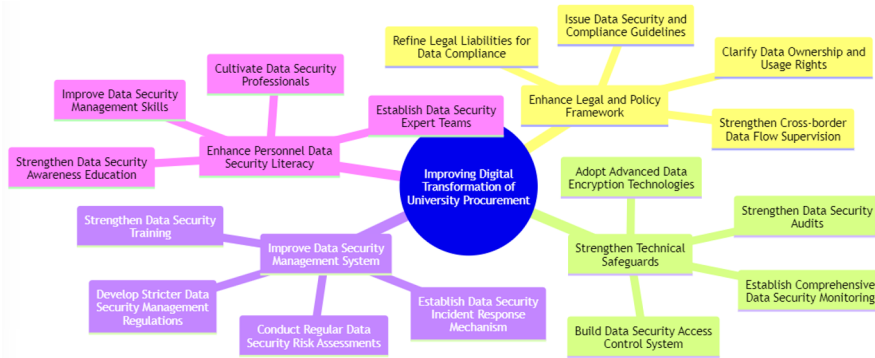


Fig. 4. Improving digital transformation of university procurement.

5.1 Improve the Legal and Policy Framework

Existing laws, regulations, and policies have some shortcomings in the digital transformation of university procurement. A more comprehensive policy framework needs to be constructed:

Refine the legal responsibilities for data compliance. Drawing on the Data Security Law and the Personal Information Protection Law, formulate detailed rules specifically for data security in university procurement, refine the legal responsibilities for data breaches and misuse, clarify the severity of penalties, increase the cost of violations, and deter potential violations. For example, clearly define the responsible parties and penalty standards for different levels of data breach incidents, and detail the penalty amounts or other penalty measures.

Clarify data ownership and usage rights. Formulate university procurement data management measures, clarify the ownership and usage rights of different types of data (e.g., bidder information, bid evaluation expert information, tender documents), and avoid issues such as unclear data ownership and data misuse. Standardize data sharing and exchange mechanisms to ensure the legal and compliant circulation of data. For example, clarify the approval process for data sharing and data format requirements.

Strengthen the supervision of cross-border data flow. For procurement data involving cross-border transmission, strictly comply with relevant national laws and regulations, such as the Cybersecurity Law and the Data Exit Security Assessment Measures, conduct security assessments before cross-border data transmission, and take necessary security measures, such as data masking and encrypted transmission, to ensure data security and compliance. The approval process and responsible parties for cross-border data transmission should be clearly defined.

Issue data security compliance guidelines for universities. Issue specific data security compliance guidelines for the characteristics of the digital transformation of university procurement, providing more specific guidance and operating standards for universities, covering security requirements for all stages of the data lifecycle, and providing best practice cases to facilitate implementation by universities. The guidelines should include specific operating procedures and technical specifications, such as specific algorithms for data encryption and key management specifications.

5.2 Strengthen the Construction of Technical Safeguards

Technical safeguards are the foundation of data compliance and risk prevention. Universities need to build a multi-layered technical safeguard system:

Adopt more advanced data encryption technologies. Adopt more advanced encryption algorithms and technologies, such as homomorphic encryption and blockchain technology, to encrypt sensitive data during storage and transmission, ensuring data confidentiality. At the same time, explore the application of privacy computing technology in procurement scenarios to achieve data "availability without visibility." For example, research how to use homomorphic encryption technology to perform statistical analysis on encrypted data.

Establish a more comprehensive data security monitoring system. Establish a real-time data security monitoring system to comprehensively monitor data access, use, and storage, and timely detect and warn of potential security risks. For example, deploy intrusion detection systems (IDS), security information and event management systems (SIEM), and combine artificial intelligence technology for security event analysis and prediction. Establish an alert mechanism and emergency response process for security incidents.

Strengthen data security audits. Conduct regular data security audits to evaluate the effectiveness of data security measures and make timely improvements. The audit content should cover both technical and management aspects, and an audit report should be generated with improvement suggestions. For example, regularly analyze data access logs to identify abnormal access behavior.

Build a data security access control system. Implement role-based access control (RBAC) and the principle of least privilege to restrict user access to data and prevent unauthorized access and data breaches. Combine multi-factor authentication technology to enhance system security. For example, set different data access permissions for users with different roles and use two-factor authentication for identity verification.

5.3 Improve Data Security Management Systems

Sound management systems are an important guarantee for data compliance and risk prevention. Universities need to establish and improve the following management systems:

Develop more stringent data security management systems. Develop data security management systems covering the entire data lifecycle, clarifying the responsibilities and obligations of each stage, and ensuring the standardization and institutionalization of data security management. For example, develop data classification and grading management systems and data security incident response systems. Establish corresponding assessment mechanisms to ensure the effective implementation of the systems.

Strengthen data security training. Regularly conduct data security training for relevant personnel to enhance their data security awareness and skills, enabling them to effectively identify and respond to data security risks. Training content should be tailored to the needs of different positions, such as encryption technology training for technical personnel and data security management system training for management personnel. Evaluate the effectiveness of the training.

Establish a data security incident response mechanism. Establish a comprehensive data security incident response mechanism, clarifying the incident handling process and responsible personnel, ensuring timely and effective handling of data security incidents, and conducting post-incident analysis and improvement. For example, develop a contingency plan for data breach incidents and conduct regular drills.

Conduct regular data security risk assessments. Regularly assess the data security risks in the digital transformation of university procurement, identify potential risks, and formulate corresponding countermeasures. Risk assessments should be combined with actual situations, using both qualitative and quantitative methods. For example, regularly conduct vulnerability scanning and penetration testing on the system.

5.4 Enhance Personnel Data Security Literacy

Personnel competency is a key factor in data compliance and risk prevention. Universities need to take multiple measures to enhance personnel data security literacy:

Strengthen data security awareness education. Enhance the data security awareness of all faculty and staff through various forms, such as lectures, training, and publicity, making them aware of the importance of data security and consciously complying with data security management systems. Case studies can be used to enhance the relevance

and effectiveness of education. For example, regularly carry out data security themed publicity activities.

Improve data security management skills. Provide professional skills training for data security management personnel, such as data encryption technologies, risk assessment methods, and incident response processes, to improve their data security management capabilities. Encourage them to obtain relevant professional certificates, such as CISP and CISSP. Provide practical opportunities, such as participating in the emergency handling of security incidents.

Cultivate data security professionals. Universities can establish data security related majors or courses to cultivate data security professionals and provide talent support for the digital transformation of university procurement. Cooperate with enterprises to carry out internship and training programs to improve students' practical abilities. For example, cooperate with security vendors to establish joint laboratories.

Establish a data security expert team. Form a data security expert team to provide consultation and guidance for the digital transformation of university procurement, assisting universities in formulating and implementing data security strategies. The expert team can be composed of internal and external experts. For example, hire renowned experts in the industry as consultants.

Through the implementation of the above improvement suggestions, the level of data compliance in the digital transformation of university procurement can be effectively enhanced, data security risks can be reduced, and the smooth progress of university digital transformation can be guaranteed, ultimately achieving the modernization and standardization of university procurement activities. Future research can further focus on specific practical cases and conduct comparative analysis of the digital transformation paths of different universities.

6 Conclusion

6.1 Research Conclusions

This study delves into the key issues of data compliance and risk prevention in the digital transformation of university procurement. The study finds that while digital transformation enhances efficiency and convenience, it also brings unprecedented data security challenges to university procurement. The lack of a sound legal and regulatory framework, insufficient technical safeguards, incomplete management systems, and the lack of personnel data security literacy are the main problems currently faced by universities.

The main findings of this study include:

Legal and Regulatory Level. The existing legal and regulatory framework lacks specificity and operability for data security issues in the digital transformation of university procurement, and needs further refinement and improvement, especially in the supervision of cross-border data flow.

Technical Safeguards Level. Universities need to build a more robust technical safeguard system, including adopting more advanced encryption technologies, establishing more comprehensive monitoring and access control systems, and strengthening data security audits.

Management System Level. A sound data security management system is key to ensuring data compliance. Universities need to develop more stringent data security management systems and strengthen the training and assessment of relevant personnel.

Personnel Competency Level. Enhancing the data security literacy of personnel is crucial. It is necessary to strengthen data security awareness education, improve data security management skills, and cultivate data security professionals.

The significance of this study lies in:

Providing improvement suggestions for universities. This study proposes specific improvement suggestions from the perspectives of laws and regulations, technical safeguards, management systems, and personnel competency, providing practical guidance for universities to enhance data compliance and risk prevention capabilities.

Promoting the digital transformation of universities. By addressing data compliance and risk prevention issues, the smooth progress of university digital transformation can be ensured, ultimately achieving the modernization and standardization of university procurement activities.

Filling the research gap. This study focuses on data security issues in the emerging field of digital transformation of university procurement, filling the gap in related research and providing a foundation for future research.

6.2 Future Research Directions

Future research can delve into the following aspects:

In-depth research on specific legal issues. For example, conduct in-depth research on specific legal issues in cross-border data flow, such as data sovereignty and jurisdiction, and propose more specific legal suggestions.

Research on the application of emerging technologies. For example, delve into the application potential of emerging technologies such as blockchain, privacy computing, and federated learning in university procurement data security and risk prevention, and explore more effective technical solutions.

Comparative research on the transformation paths of different universities. Conduct comparative analysis of the digital transformation paths of different types of universities, summarize best practices, and provide references for other universities.

Research on quantitative data security risk assessment models. Construct quantitative data security risk assessment models to provide a more scientific basis for universities to conduct risk assessments and make decisions.

Research on university procurement data security standard systems. Research and develop university procurement data security standard systems to standardize data security management and enhance the overall security level of the industry.

Through the exploration of the above future research directions, the data compliance and risk prevention system in the digital transformation of university procurement can be further improved, providing stronger support for the sustainable development of universities.

References

1. Abdurrahman, A., Gustomo, A., & Prasetyo, E. A. (2024). Enhancing banking performance through dynamic digital transformation capabilities and governance, risk management, and compliance: Insights from the Indonesian context. *The Electronic Journal of Information Systems in Developing Countries*, 90(2), e12299
2. Cai, L., & Zhang, J. (2024). On the Construction of New Capabilities for Digital Transformation of Universities: Processes, Foundations, and Initiatives. *Chongqing Second Normal University Journal*, 2024(4).
3. Luan, Xiaoqi. (2024). Exploration of Digital Transformation in Government Procurement. *Bidding and Procurement Management*, 2024(5).
4. Li, Y. (2024). Research on the Digital Transformation Path of Applied Private Universities. *Jiangsu Science and Technology Information*, 2024(19).
5. Qi, J., Gou, N., & Zhang, G. (2024). A Review of Research on the Digital Transformation of Universities in China. *Higher Education Forum*, 2024(7).
6. Razorenov, Y. I., & Vodenko, K. V. (2021). Innovative development of the national university system in Russia: trends and key elements. *International Journal of Sociology and Social Policy*, 41(1/2), 253-262.
7. Yang, Y. (2023). Research on Data Security Compliance and Risk Prevention and Control in Digital Transformation. *Industrial Information Security*, 2023(5).
8. Zan, Y. (2022, March 11). Optimize Government Procurement Governance by Borrowing Digital Transformation. *China Government Procurement News*.

9. Xu, L. (2024). Research on the Impact of Government Procurement on Enterprise Green Technology Innovation under the Background of Digital Transformation. [Doctoral dissertation, Shandong Normal University].
10. Zhang, J., Yu, D., & Yan, Z. (2024). Can Government Digital Procurement Promote Enterprise Digital Transformation? - Analysis Based on Government Procurement Big Data and the BERT Model. *Finance Research*, 2024(11).
11. Alshammari, T. M., Alsubait, S. I., Alenzi, K. A., & Almalki, Z. S. (2023). Estimating the potential economic impact of the Wasfaty program on costs of antidiabetic treatment: an initiative for the digital transformation of health. *Saudi Pharmaceutical Journal*, 31(6), 1029-1035.
12. Gong, J. (2024). Research on the Collaborative Innovation Mechanism of Industry-University-Research in the Digital Transformation of Universities in Guizhou. *High Technology and Industrialization*, 2024(9).
13. Xiang, B., Shao, Y., Lin, J., & Chen, T. (2024). Analysis of Data Asset Security Risks and Prevention and Control in Government Digital Transformation. *Computer Knowledge and Technology*, 2024(9).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

