Journal of Global Information Management
Volume 34 • Issue 1 • January-December 2026

Confronting Cross-Border Data Risks:
A Multidimensional Firm-Level Scale for an Era of Digital Fragmentation

Wanxiu Xu
https://orcid.org/0009-0007-9469-9797
University of Science and Technology, China

Xiaodong Zuo
Independent Researcher, China
Received: May 18th, 2025 | **Accepted:** January 7th, 2026

ABSTRACT

Digital sovereignty is reshaping global data governance, with the increasing fragmentation of regulatory regimes exposing firms to complex risks in cross-border data flows. However, existing research lacks theoretically grounded and empirically validated frameworks and tools from the firm perspective, limiting their practical utility in identifying and mitigating these risks. This study proposes a three-dimensional framework of cross-border data flow risk based on the institution–technology–organisation structure, with each dimension informed by institutional theory, socio-technical systems theory, and the New OLI Paradigm. An initial item pool was developed through literature review and Delphi consultation, followed by a two-stage survey with exploratory and confirmatory factor analyses, reliability, and validity testing. The resulting 12-item scale captures three key dimensions: regulatory complexity, data security and privacy, and business continuity. This framework offers both conceptual clarity and practical tools for firms navigating fragmented data environments.

KEYWORDS

Cross-Border Data Flow Risk, Institution–Technology–Organisation Framework, Scale Development, Global Data Governance, Organisational Risk Management

INTRODUCTION

In the context of digital globalization, cross-border data flows (CBDF) drive global technological collaboration, business deployment, and market operations (Brynjolfsson & Kahin, 2002). However, increasing geopolitical tensions and digital protectionism are shifting these flows from market-driven to state-driven competition over digital sovereignty (Meltzer, 2015; Mitchell & Mishra, 2019; Xu et al., 2025). The involvement of multiple actors, contextual variations, and technological uncertainty further heightens the risks faced by globally operating firms (Almuqrin, 2024; Samiee, 1984; Wang et al., 2023).

In recent years, regulatory sanctions on firms for CBDF violations have increased in both frequency and severity. Notable cases include China's 2018 sanctions on BGI and WuXi AppTec for unauthorized human genetic data transfers (Cyranoski, 2018), Didi's 2021 RMB 8.026 billion fine for data breaches tied to its U.S. IPO (Xiong, 2022), and Meta's 2023 €1.2 billion fine by the Irish Data Protection Commission for General Data Protection Regulation (GDPR) violations and the

DOI: 10.4018/JGIM.399056

suspension of European Union (EU)–U.S. data transfers (McCallum, 2023). In 2024, the United States passed the Protecting Americans from Foreign Adversary Controlled Applications Act, effectively banning TikTok (Xu et al., 2025), while South Korea fined AliExpress nearly KRW 2 billion, and the Netherlands fined Uber €290 million for CBDF violations (Lomas, 2024). In January 2025, the European Center for Digital Rights filed complaints against six Chinese tech firms—TikTok, AliExpress, SHEIN, Temu, WeChat, and Xiaomi—over unauthorized data transfers to China. These high-profile cases reflect broader regulatory scrutiny, with many firms facing operational disruptions or restrictions under national security or cybersecurity pretexts.

However, research on CBDF risks remains significantly underdeveloped. Most studies take a macro-level, national governance perspective, focusing on risks such as national security threats and data breaches, but lack a risk identification framework at the organizational level (Cheng et al., 2019; Manyika et al., 2016). Some research examines security threats across the data lifecycle stages—generation, collection, transmission, storage, processing, and sharing—offering technical insights but often failing to capture the interdisciplinary complexity of CBDF risks (Burri, 2021; von Scherenberg et al., 2024). Additionally, while a few studies acknowledge the security implications of information flows, they generally treat CBDF risks as part of broader "digital risks" without distinguishing them as a unique domain (Allison et al., 2021; Jing et al., 2018; Luo, 2021a). As a result, a coherent theoretical framework for CBDF risks, particularly at the organizational level, is lacking, which hinders the development of international risk and strategic management theories in the digital age.

Building on this research gap, the present study investigates CBDF risks faced by firms and develops a comprehensive theoretical framework. This framework supports the creation of a reliable empirical measurement scale to analyze how these risks affect organizations. The study was carried out in three steps: First, we constructed a theoretical framework for CBDF risks, drawing on classical theories to define and analyze risk dimensions; second, we identified core risk elements and developed a preliminary measurement scale through a literature review and semi-structured expert interviews; and third, we conducted a two-stage survey, using 188 valid responses for exploratory factor analysis (EFA) and 307 responses for confirmatory factor analysis (CFA) to assess the scale's reliability and validity. These efforts address the theoretical gap in CBDF risk conceptualization and provide firms with a structured framework for risk identification and management in the complex global data regulatory environment.

THEORETICAL FRAMEWORK AND DIMENSION CONSTRUCTION

Theoretical Framework

For firms engaged in cross-border operations, the fragmentation of global data governance and the growing contest over digital sovereignty have increased compliance costs and exposed core activities to multiple risks. While "CBDF risk" is widely discussed in international law, politics, and trade, it remains underdefined from a management perspective, with limited progress in its theoretical development.

The origins of the institution–technology analytical framework can be traced to the Institutional Analysis and Development framework proposed by Ostrom (2019). This framework posits that governance outcomes result not only from interactions among actors but also from the interrelationships between actors, action situations, and external systems (Ostrom, 2011). This approach has evolved into the institution–technology lens, emphasizing the reciprocal relationship between institutional environments and technological systems and their joint influence on organizational governance. It supports organizations in adjusting and optimizing internal structures to improve performance and efficiency.

This study is the first to apply the institution–technology analytical framework to identify emerging data-related risks at the firm level. Given the multidimensional and cross-cutting nature of CBDF risks, this framework provides valuable guidance for delineating risk dimensions. However, it