Proceedings of ICEMGD 2026 Symposium: Rethinking Governance and Policy Innovation for Societal Challenges
DOI: 10.54254/2754-1169/2026.LH34963

The New Landscape of Enterprise Financial Penetrating Supervision: Corporate Risk Monitoring under Digital-Intelligent Transformation

Zhuoyan He

International Business School, Tianjin University of Finance and Economics, Tianjin, China
15620790998@163.com

Abstract. Using literature analysis, comparative analysis, and framework construction, this study examines how several research streams respond to concrete problems in enterprise financial supervision. Regulatory technology is used to explain how compliance review can move from checking documents to tracing transaction data. Big data accounting helps clarify why financial evidence now includes not only vouchers and ledgers, but also contracts, delivery records, electronic invoices, payment data, tax declarations, and system logs. Continuous auditing addresses the problem of delayed risk detection by showing how abnormal transactions may be identified during the business process rather than only after closing or reporting. Audit analytics provides methods for comparing cross-system evidence and identifying inconsistencies among business flow, invoice flow, fund flow, tax flow, and accounting flow. Enterprise risk management is used only as a supporting perspective to explain how these financial risks can be classified, escalated, reviewed, and corrected inside the enterprise. This study finds that financial risk increasingly appears as inconsistency among business flow, invoice flow, fund flow, tax flow, and accounting flow.

Keywords: Penetrating supervision, Financial risk, Regulatory technology, Audit analytics

1. Introduction

Digital-intelligent transformation is changing enterprise finance from record-keeping into process-based control. Financial information is now generated by procurement platforms, sales systems, electronic invoicing, treasury systems, tax interfaces, warehouse records, and intelligent accounting tools. This improves timeliness, but it also moves risks away from the surface of accounting documents. A transaction may appear complete in form while its real risk lies in abnormal delivery records, circular fund flows, undisclosed related parties, weak commercial substance, or tax-accounting inconsistencies.

The idea of penetrating, or look-through, supervision is rooted in the principle of substance over form. In the Chinese financial regulatory context, it has been used to identify real market participants and substantive transactions hidden behind formal arrangements [1]. Regulatory technology also shows how information technology can support monitoring, reporting, and

DOI: 10.54254/2754-1169/2026.LH34963

compliance [2]. At the same time, big data accounting research indicates that accounting and auditing evidence is expanding from structured records to broader business and external data [3-4].

Existing studies have discussed regulatory technology, accounting data, and audit analytics from different perspectives, but the connection between penetrating supervision and enterprise financial risk monitoring has not been sufficiently explained. In particular, there is still room to clarify how the idea of substance-over-form review can be applied to concrete financial risk scenarios, such as false revenue recognition, abnormal supplier payments, hidden related-party transactions, tax-finance inconsistency, and weaknesses in automated accounting rules. The significance of this study lies in two aspects. From a practical perspective, it provides a finance-oriented way for enterprises to identify risks that are difficult to discover through vouchers, invoices, or approval documents alone, especially when transaction evidence is dispersed across business, tax, treasury, and accounting systems. This is helpful for improving the authenticity of revenue, the safety of funds, the reliability of tax treatment, and the traceability of accounting records. From a research perspective, the study extends the discussion of penetrating supervision from the regulatory level to the enterprise financial process level, and offers a reference for future studies on digital financial supervision, continuous auditing, audit analytics, and transaction-substance verification. Therefore, this paper focuses on three questions: how digital-intelligent transformation reshapes financial risk, why traditional monitoring becomes insufficient, and how enterprises can reconstruct monitoring mechanisms around business flow, invoice flow, fund flow, tax flow, and accounting flow.

2. Theoretical basis and literature review

2.1. Core concepts

Enterprise financial penetrating supervision in this paper means examining financial transactions according to their economic substance rather than their formal documents. Contracts, invoices, approvals, and accounting entries may show that a transaction is procedurally complete, but they do not necessarily prove that the transaction is real, reasonable, or low-risk. Therefore, supervision should trace the business purpose, counterparty relationship, fund movement, tax treatment, accounting recognition, and actual risk bearer behind the records.

Digital-intelligent transformation changes the way such evidence is formed. Financial facts are now scattered across procurement systems, sales platforms, electronic invoices, online payments, tax interfaces, treasury systems, and accounting software. A single voucher can no longer reflect the whole transaction process. Risk often appears when business records, invoice data, fund flows, tax filings, and accounting entries fail to support the same transaction substance.

Risk monitoring, as used in this paper, refers to the timely identification, warning, review, and correction of financial risks during the transaction process. It should not wait until financial statements are completed. Instead, it should cover key links such as supplier creation, contract approval, order execution, delivery or receipt, invoicing, payment, accounting recognition, tax declaration, and cash recovery. In this sense, digital systems provide the evidence base, penetrating supervision provides the review logic, and risk monitoring turns that logic into a practical financial control process.

2.2. Theoretical foundations

The necessity of penetrating supervision first comes from information asymmetry. In corporate finance, managers and business departments usually know more about the real transaction

DOI: 10.54254/2754-1169/2026.LH34963

background than auditors, regulators, creditors, or investors. Digitalization does not eliminate this gap. Instead, it may turn document asymmetry into data asymmetry. When financial records are generated through business systems, tax interfaces, treasury platforms, and automated accounting rules, complete data results may still fail to show how a transaction was formed, approved, or modified. Financial supervision therefore needs to trace the process behind accounting outputs.

The principle of substance over form provides the basic review logic. Contracts, invoices, approvals, and accounting entries can prove procedural completeness, but they cannot alone prove transaction authenticity. For revenue, supervision should compare contract terms, delivery evidence, customer acceptance, invoicing, revenue recognition, cash collection, and later returns. For procurement and payment, it should examine supplier identity, goods receipt, invoice validity, payment direction, and accounting treatment. The key is whether different types of evidence support the same economic substance.

Regulatory technology, big data analysis, and continuous auditing provide the technical basis for earlier identification of risk. Data matching, rule screening, system logs, and exception alerts can help detect problems such as payment before receipt, revenue recognition without delivery evidence, abnormal invoicing, or inconsistency between tax filings and accounting records [2]. However, technology can only identify exceptions. Whether an exception reflects normal business practice or hidden financial risk still depends on professional judgment.

2.3. Research status and literature review

Existing foreign studies are mainly related to regulatory technology, big data accounting, and audit analytics. Arner, Barberis, and Buckley argue that regulatory technology is not a simple digitization of manual compliance, but a change in regulatory logic [2]. This supports the shift from document checking to data-based and substance-oriented review. Vasarhelyi, Kogan, and Tuttle, as well as Warren, Moffitt, and Byrnes, show that accounting evidence is expanding from ledgers and statements to broader business data [3-4]. These studies provide a basis for examining financial risk through transaction processes rather than through accounting records alone.

Audit analytics and continuous monitoring studies further explain how risks can be identified earlier. Cao, Chychyla, and Stewart point out that big data analytics can improve financial statement audit procedures [5]. Alles, Brennan, Kogan, and Vasarhelyi's Siemens case shows that monitoring can be embedded in business process controls, while also revealing practical issues such as rule design, alarm management, and audit trails [6]. Appelbaum, Kogan, and Vasarhelyi also emphasize the role of data-driven analytical procedures in external auditing [7]. These studies show that technology can help identify abnormal patterns, but final judgment still depends on audit evidence and professional review.

Domestic research discusses penetrating supervision mainly in financial regulation, state-owned asset supervision, and digital supervision. It stresses full-chain and full-process review, but often remains at the level of policy interpretation. Less attention is given to enterprise-level financial scenarios, such as false revenue, abnormal payments, hidden related parties, tax-finance inconsistency, and accounting estimate manipulation. Therefore, this paper links penetrating supervision with audit analytics and continuous monitoring, and develops a more finance-centered framework for enterprise risk monitoring.

DOI: 10.54254/2754-1169/2026.LH34963

3. Digital-intelligent transformation and the new landscape of penetrating supervision

3.1. Reshaping of enterprise financial risk forms

Digital-intelligent transformation changes both the generation and recording of enterprise financial risk. In the traditional environment, review usually begins with vouchers, ledgers, financial statements, and approval documents. In the digital environment, risks may arise earlier in procurement, sales, logistics, invoicing, treasury, tax, and accounting systems. Once orders, delivery records, invoices, payment instructions, or journal entries are automatically processed, problems may enter the financial system before manual review takes place. Financial risk is therefore not only a reporting issue, but also a process issue.

This change is especially clear in financial shared services and intelligent accounting. Shared service centers standardize reimbursement, payment, accounting, and reporting, but formal process completion may hide weak business substance. An expense claim may have an invoice and approval record, yet lack a clear business purpose. A supplier payment may follow the required procedure, while the supplier itself may be newly created, inactive, or related to internal personnel. Intelligent accounting also creates dependence on system rules. If invoice classification, expense recognition, bank matching, or automatic journal-entry rules are poorly designed, the system may repeatedly produce incorrect accounting results. Monitoring should therefore examine not only individual entries, but also rule design, exception handling, and system logs.

Business-finance-tax integration further makes financial risk appear as inconsistency among business flow, invoice flow, fund flow, tax flow, and accounting flow. A wrong delivery date may affect revenue cut-off, invoicing, tax declaration, and receivable analysis. A false procurement record may lead to improper cost recognition, input tax treatment, and payment approval. In this context, complete documents are only the starting point of verification. For revenue, the key is whether contract terms, delivery evidence, customer acceptance, invoicing, revenue recognition, cash collection, and later returns support the same transaction. For procurement, the key is whether supplier identity, goods receipt, invoice validity, price reasonableness, payment direction, and accounting treatment are consistent.

3.2. Limitations and challenges of traditional financial risk monitoring

Traditional financial risk monitoring faces clear limitations in the digital-intelligent environment. First, many reviews still take place after monthly closing, annual reporting, external audit, or regulatory inquiry. Although post-event review can identify errors, it often comes too late to prevent losses. Suspicious payments may already have been made, false revenue may have affected performance results, and tax-finance inconsistencies may have been submitted to the tax system. When risks are formed during transaction execution, after-event review is no longer sufficient.

Second, transaction evidence is often scattered across different systems and departments. Procurement, sales, treasury, tax, logistics, legal, and accounting records may each show only part of the transaction. Finance departments may see invoices and journal entries, but not delivery records, bank payments, contract changes, or tax declarations. Without data connection, it is difficult to judge whether the whole transaction chain is consistent, which may create blind spots for false transactions, repeated payments, abnormal reimbursements, and hidden related-party arrangements.

Third, digital systems also increase review difficulty. Financial staff may not fully understand automated rules, while technical staff may not know their accounting or tax effects. Abnormal transactions may therefore be hidden behind standard system procedures. In high-volume

DOI: 10.54254/2754-1169/2026.LH34963

transactions, traditional sampling is also limited, because some risks become visible only when similar payments, suppliers, receivables, or invoices are compared together.

The deeper problem is that traditional monitoring often treats compliance as document completeness. A contract, invoice, approval record, and accounting voucher may pass formal review, but they do not necessarily prove economic substance. Penetrating supervision therefore needs to focus on whether documents, system data, tax records, and fund flows support the same business reality.

3.3. New meaning of penetrating risk monitoring

Under digital-intelligent transformation, penetrating risk monitoring no longer starts only from completed accounting entries. Its focus moves forward to the transaction process. Revenue, procurement, payment, tax declaration, and accounting recognition should be reviewed as connected links, because an error in one link may affect the reliability of the whole financial record.

The first change is from manual review to technology-assisted screening. Manual review remains necessary, but it cannot cover large volumes of transactions in real time. Data matching and rule screening can identify abnormal payments, inconsistent invoices, missing delivery records, or unusual fund movements, helping narrow the review scope. Professional judgment is still needed to assess the business meaning of each exception.

The second change is from single-document checking to full-chain verification. A contract, invoice, or payment record alone cannot prove transaction authenticity. Revenue monitoring should compare customer identity, contract terms, delivery evidence, invoicing, revenue recognition, cash collection, and later returns. Procurement monitoring should compare supplier qualification, purchase order, goods receipt, invoice, payment approval, and follow-up performance. Related-party risk should be judged by combining ownership, personnel, address, bank account, transaction frequency, and fund movement.

The third change is from after-event inspection to earlier warning. Before payment, the system can check supplier status, bank account consistency, goods receipt, and contract limits. Before revenue recognition, it can check delivery evidence, customer acceptance, and receivable recovery.

Therefore, the value of penetrating supervision is not simply stricter control, but deeper verification of financial substance. Enterprises need to examine whether business evidence, accounting treatment, tax treatment, and cash flow point to the same economic reality. Rules can identify clear exceptions, but issues such as related-party substance and commercial reasonableness still require professional judgment.

4. Reconstruction of corporate risk monitoring mechanisms under penetrating supervision

4.1. Digital-intelligent transformation path of risk monitoring

The transformation of financial risk monitoring should start from financial scenarios rather than technology itself. For each major risk, enterprises need to clarify the monitored object, data source, warning rule, and reviewer. Automation is meaningful only when the risk object is clear and can be expressed through data rules [6]. A practical approach is to build an independent monitoring layer above business, finance, tax, and treasury systems. This layer compares selected transaction data, generates warnings, and keeps logs, but does not modify production records. Monitoring frequency should be set according to risk level, transaction volume, and system capacity.

DOI: 10.54254/2754-1169/2026.LH34963

Data integration is the basis of this process. Business data, invoice data, fund data, tax data, and accounting data should be connected through unified master data, such as customers, suppliers, bank accounts, contracts, projects, products, and organizational units. Otherwise, duplicated supplier names, inconsistent customer records, or unmatched contract numbers may cause related-party risks, concentration risks, or abnormal transactions to be missed.

Risk indicators should be designed around specific financial scenarios. Revenue monitoring may focus on invoices without delivery, revenue without collection, abnormal period-end sales, inconsistent customer acceptance, or large post-period returns. Procurement monitoring may cover repeated invoices, payment before receipt, large transactions with newly created suppliers, or abnormal price deviations. Fund monitoring may focus on payments to inactive suppliers, frequent transfers between related accounts, or funds returning through third parties. Tax-finance monitoring should compare invoice data, accounting entries, tax declarations, and cash settlement.

After indicators are set, full-sample screening can be used in key risk areas. Its purpose is not to treat every transaction as suspicious, but to identify repeated or hidden patterns that limited sampling may overlook. Each warning should retain the triggering rule, source data, reviewer, explanation, conclusion, and corrective action. Confirmed risks may lead to accounting adjustment, payment suspension, supplier review, tax correction, or audit follow-up, while false positives should be recorded to improve rules and thresholds.

4.2. Key technical tools and risk monitoring applications

Big data analysis is mainly used to compare evidence across systems. In revenue monitoring, contracts, delivery records, invoices, journal entries, receivables, and cash collections should be reviewed together. The focus is not whether a single document is missing, but whether timing, amount, counterparty, and cash recovery support the same transaction substance. For example, period-end revenue may be acceptable when delivery, acceptance, and later collection are complete, but it becomes riskier when delivery evidence is weak, collection is delayed, or large returns occur after the reporting date. In this process, audit analytics can improve the efficiency of financial review [5].

Graph analytics helps identify hidden related-party and counterparty risks. Separate invoices or payments may appear normal, but links among shareholders, managers, employees, suppliers, customers, addresses, bank accounts, contracts, invoices, and payments may reveal abnormal relationships. A shared address alone may not prove related-party risk, but shared contacts, repeated transactions, similar bank accounts, and circular fund flows can together indicate higher risk.

Artificial intelligence and machine learning can support risk scoring, such as identifying abnormal reimbursements, unusual journal entries, suspicious payment paths, or customers with higher default risk [8]. However, model risk and weak interpretability should be considered [9]. These tools should be based on understandable financial variables and used to support, rather than replace, professional judgment.

Blockchain has a more limited role. It can improve traceability in supply-chain finance, electronic invoices, inventory pledge, and multi-party reconciliation, but it cannot prove that the original data are true. If false delivery information is entered at the beginning, blockchain only preserves the false record. Therefore, it should be combined with identity verification, logistics evidence, invoice matching, and fund-flow tracing.

Overall, different tools are suitable for different types of risks. Formalized issues, such as amount mismatches, payment before receipt, or inconsistent bank accounts, can be detected by rules. Issues involving commercial substance, concealed related parties, or abnormal fund circulation still require

DOI: 10.54254/2754-1169/2026.LH34963

professional review. The monitoring system should identify exceptions and provide evidence, but not replace financial judgment.

Table 1. Financial risk monitoring framework under penetrating supervision

Financial Process	Formalizable Check	Judgment Boundary	Warning and Follow-up
Revenue recognition	Match contract, delivery, invoice, revenue entry, receivable, and bank collection.	Assess whether delayed collection or post-period return weakens transaction substance.	If delivery, acceptance, or collection support is weak, review revenue recognition and document adjustment or explanation.
Procurement payment	Match supplier file, purchase order, receipt, invoice, approval, and payment.	Assess whether price deviation, urgent purchase, or supplier change has commercial reason.	If payment precedes receipt or supplier data are abnormal, suspend payment and review supplier risk.
Fund transfer	Trace approval, bank flow, counterparty, and subsequent return flow.	Assess whether fund movement reflects legitimate settlement or disguised occupation.	If funds return through related or third-party accounts, escalate to finance leadership and perform audit follow-up.
Related-party transaction	Compare ownership, address, phone number, personnel, bank account, and transaction frequency.	Assess whether multiple weak signals together indicate concealed control.	If shared identifiers combine with repeated transactions or circular flows, review disclosure and approval requirements.
Tax-finance consistency	Reconcile invoice data, tax declaration, accounting entry, and cash settlement.	Assess whether timing difference is reasonable under tax and accounting rules.	If tax records conflict with accounting recognition or cash flow, correct filing, adjust entry, or retain explanation.
Accounting estimate	Compare impairment, provision, or fair-value estimate with aging, market, and historical data.	Assess whether assumptions are reasonable in the business context.	If estimates deviate from evidence, recalculate assumptions and request independent review.
Data traceability	Check modification logs, approval records, access rights, and system timestamps.	Assess whether manual change has legitimate business and accounting basis.	If modification lacks authorization or audit trail, restore data, restrict access, and investigate control weakness.

As shown in Table 1, the reconstructed monitoring mechanism begins with financial risk scenarios rather than with technology labels. Duplicate payments can be detected by formalized matching rules, while hidden related-party transactions require graph analysis and professional judgment. Complex accounting estimates require data comparison, but the final judgment still depends on accounting standards, business context, and audit evidence.

4.3. Institutional safeguards for the risk monitoring system

A penetrating monitoring system first requires reliable and standardized data. Customer, supplier, bank account, contract, project, product, and organizational information should follow unified rules; otherwise, duplicated supplier names, inconsistent customer records, or unmatched contract numbers may lead to inaccurate warnings. Data ownership, correction authority, retention periods, and audit trails also need to be clearly defined so that each warning can be traced back to its source.

Data retention should be based on evidence needs rather than simple accumulation. Short-term exceptions may only require follow-up records, while receivables, payables, supplier behavior, and related-party transactions often need longer historical data. Retention rules should therefore balance legal requirements, evidence value, risk type, data sensitivity, and confidentiality concerns.

Audit work should also be linked with daily monitoring. Internal audit can review indicator design, data interfaces, warning handling, and corrective actions. External auditors may use monitoring results as supporting evidence, but they still need to evaluate system reliability and

DOI: 10.54254/2754-1169/2026.LH34963

underlying data. Continuous monitoring improves process evidence, yet it cannot replace independent assurance [6].

Finally, warnings should be classified by amount, frequency, severity, evidence strength, and responsible department. High-risk issues, such as payment to unverified suppliers or revenue recognition without delivery evidence, should be escalated promptly. Repeated medium-risk issues should be reviewed together, while low-risk exceptions can support process improvement. Even when third-party platforms or models are used, the enterprise remains responsible for rule design, model validation, data security, and exception handling.

5. Conclusion

This paper examines enterprise financial penetrating supervision under digital-intelligent transformation. The main finding is that financial risk is increasingly reflected in inconsistencies among business flow, invoice flow, fund flow, tax flow, and accounting flow. As a result, document-based review alone is no longer enough to judge the substance of financial transactions.

Penetrating supervision should focus on full-chain verification rather than stricter formal control. Enterprises need to connect transaction data, set clear risk rules, screen key risk areas, classify warnings, retain audit trails, and arrange professional review. Digital tools can support this process, but they must be used together with accounting standards, tax rules, audit evidence, and professional judgment. This study is limited by its reliance on literature analysis and framework construction. It does not include empirical testing or company-level case data. Future research may further examine industry-specific indicators, warning thresholds, model validation, and the practical effectiveness of penetrating monitoring systems.

References

[1] Chang, Jian. "On Look-through Supervision and Reform of China's Supervision System." Journal of Huazhong University of Science and Technology (Social Science Edition), 33(1), 2019: 111-117. DOI: 10.19648/j.cnki.jhustss1980.2019.01.14.

[2] Arner, Douglas W., Barberis, Janos, and Buckley, Ross P. "FinTech, RegTech, and the Reconceptualization of Financial Regulation." Northwestern Journal of International Law & Business, 37(3), 2017: 371-413.

[3] Vasarhelyi, Miklos A., Kogan, Alexander, and Tuttle, Brad M. "Big Data in Accounting: An Overview." Accounting Horizons, 29(2), 2015: 381-396. DOI: 10.2308/acch-51071.

[4] Warren, J. Donald, Moffitt, Kevin C., and Byrnes, Paul. "How Big Data Will Change Accounting." Accounting Horizons, 29(2), 2015: 397-407. DOI: 10.2308/acch-51069.

[5] Cao, Min, Chychyla, Roman, and Stewart, Trevor. "Big Data Analytics in Financial Statement Audits." Accounting Horizons, 29(2), 2015: 423-429. DOI: 10.2308/acch-51068.

[6] Alles, Michael G., Brennan, Gerard, Kogan, Alexander, and Vasarhelyi, Miklos A. "Continuous Monitoring of Business Process Controls: A Pilot Implementation of a Continuous Auditing System at Siemens." International Journal of Accounting Information Systems, 7(2), 2006: 137-161. DOI: 10.1016/j.accinf.2005.10.004.

[7] Appelbaum, Deniz A., Kogan, Alexander, and Vasarhelyi, Miklos A. "Analytical Procedures in External Auditing: A Comprehensive Literature Survey and Framework for External Audit Analytics." Journal of Accounting Literature, 40, 2018: 83-101. DOI: 10.1016/j.acclit.2018.01.001.

[8] Issa, Hussein, Sun, Ting, and Vasarhelyi, Miklos A. "Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation." Journal of Emerging Technologies in Accounting, 13(2), 2016: 1-20. DOI: 10.2308/jeta-10511.

[9] Financial Stability Board. Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications. Financial Stability Board, 2017. Available at: https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/.