Research on Strategies for the Intelligent Transformation of Enterprise Finance from the Perspective of Internal Control

Feipeng Liu*

Shaanxi Vocational & Technical College, Xi'an 710038, China
**Corresponding author: lfp131025@163.com*

Abstract: *The intelligent transformation of finance based on data, algorithms, and platforms will lead to changes in the generation, flow and use of financial information which causes problems in internal control such as changes in control location, deviations in automated judgment, and division of human-machine responsibilities. From the perspective of internal control this paper discusses technology application and organizational adjustment, functional changes in control elements, and the coordination relationship between control and technology; identifies control gaps in process automation, control failure in data centralization and automated judgment, and responsibility-division risks in human-machine operations; then proposes intelligent financial governance arrangements in the control environment, embedding controls in risk assessment and information communication, and feedback and capability-update strategies in monitoring and evaluation. It aims at explaining that internal control should be coordinated with the intelligent transformation of finance and provide a solution for control requirements enter system configuration and system operation support control execution.*

Keywords: *internal control; intelligent transformation of finance; changes in control location; intelligent control embedding; coordination relationship*

Introduction

The intelligent transformation of finance enhances the efficiency of financial information processing and decision support while changing the position-based approval, voucher review, and hierarchical supervision that traditional internal control relies on. Certain control actions (approval, review, supervision) no longer rely solely on positions and paper vouchers but are transferred into system rules, data interfaces, and model outputs. Existing research mainly focuses on any single aspect of technology application or management change without systematically explaining how to adaptively reconstruct internal control along with data flows, algorithmic models, and human-machine collaboration scenarios[1-2]. Studying the intelligent transformation of enterprise finance from the perspective of internal control can answer questions such as: How to keep the control objective under an intelligent context? How to embed control activities into algorithms and platforms? How to distribute control responsibilities between humans and systems? It has necessary significance since process automation will bring control gaps; data centralization and automated judgment brings control failure that is hard to detect; human-machine collaboration leads to difficulty in responsibility tracing. These risks should be analyzed by taking into account the functional changes in control elements and coordination mechanisms, thus forming a strategy system for governing arrangements, control embedding, and monitoring update.

1. Theoretical Framework for the Intelligent Transformation of Enterprise Finance from the Perspective of Internal Control

1.1 Technical Architecture and Organizational Impact of the Intelligent Transformation of Finance

Intelligent transformation of finance transforms how financial problems are handled at links including data entry, rule-based judgment, platform invocation and manual confirmation. Data is organized according to financial data by means of interfaces, master data and metadata management; rules and models are applied for voucher recognition, risk alerting and predictive analysis; platform

services offer unified support via financial shared services, data middle platforms and cloud services[4] and distributed, real-time and model-based features transform the generation and usage of financial information. Links create connections between data transfer, model invocation and service reuse that transform financial information from record results inside one system into data assets flowing over platforms. Openness and configurability of technology applications provide interface points where control activities enter systems expanding the scope of control together with data flows.

Impact on organizations includes restructuring of financial functions, allocation of positions, relationship between authority and responsibility[1]; Process automation and shared services reduce repetitive operational positions, increase the number of roles for data management, model management, exception handling, and business partnership; Expand the scope of control from inside departments to cross-organization data interaction and platform collaboration. The allocation of human-machine collaboration allocates routine tasks to be programmed and exceptions to be manually judged: Hierarchical compression of control, the transparency of control information move the inspection time from fixed times to inspections within processes with immediate feedback. Decision-making authority, execution authority, and supervision authority within the organization combines under the intervention of intelligent systems; Control responsibilities of financial entities extends from position responsibilities to system configuration, model supervision, data quality management, and control relationships have multi-agent distribution characteristics.

1.2 Functional Evolution of Internal Control Elements in the Intelligent Finance Context

Functional change of internal control elements within intelligent finance is reflected by adapting objects, methods and focus: In the control environment we have data management, algorithm management and model risk handling while in control culture we have data quality awareness and norms for using intelligent systems; For risk assessment we need model monitoring, anomaly detection and scenario simulation with risk sources being data bias, algorithm opacity, interface security, model changes and interruption of automated processes as well as the assessment frequency shifts from periodic to continuous. Changes in control elements are interrelated – changes in the control environment create new objects of interest for risk assessment, the result of risk assessment guides the rule configuration of control activities, and the operational data of control activities form a content basis for information and communication[2].

The control activities are included in rule bases, workflows and smart contracts to realize automatic verification, real-time interception and dynamic authorization; Information and communications transmit data flow between business systems, financial platforms and decision-making terminals which have multi-node and dispersed features; Monitoring is based on continuous auditing, analyzing operation records and inspecting logs, changing from sampling inspection to full inspection, focusing from result deviation to process deviation and system behavior. Change of elements does not mean substitution: Manual judgment takes charge of confirming exceptions and dealing with complex situations while intelligent systems take over rule execution and real-time monitoring, changing internal control from hierarchical approval to system rules, platform records and continuous inspection, extending control scope to data sources and model use. Linkages of control elements get closer under an intelligent context, when adjusting one will cause response and adaptation of others.

1.3 Coordination Mechanism Between Internal Control and the Intelligent Transformation of Finance

It has been established the mutual coordination between internal control and the intelligent transformation of finance[3-4], which provides the internal control with data foundation, algorithmic tools and platform carriers for control activities enter into business processes and achieve a real-time response when the intelligent transformation provides the internal control with objective constraints, responsibility framework, and risk boundaries for technology application obtainting an institution support on data quality, model reliability and clarity of authority and responsibility. The coordination relationship is reflected as follows: 1) Consideration of construction objectives takes into account efficiency, information reliability and asset security simultaneously; 2) Organization structure matching control responsibilities, data management, model approval and internal auditing have their own responsibilities respectively; 3) All process links are connected continuously forming continuous records so that transaction occurrence, data generation, model judgment, manual review, and monitoring feedback can be connected together, and control location advance to in-process and pre-event stages[4].

The Coordination mechanism includes feedback and update: Abnormal data, model deviation and records of manual intervention in control operations feed back to system optimization and institutional adjustment, which leads to updating of control rules and algorithm parameters. The internal control and intelligent transformation of finance is not a one-way adaptation process, it's an analysis that control requires entering technical configuration, technical operation supporting control execution, and organization coordinating human-machine relations. The stability of the coordination relationship depends on continuously matching control rules with technical architecture, change in control objectives, changes in technical conditions and evolution of organizational capabilities driving the coordination mechanism into new states. It provides an analytical foundation for further risk identification and strategy construction.

2.Identification of Internal Control Risks in the Intelligent Transformation of Enterprise Finance

2.1 Migration of Control Nodes Triggered by Intelligent Process Reengineering

Intelligent process reengineering: Process automation, end-to-end integration, rule-driven operations which move the traditional control location (authorization approval, voucher review, segregation of duties) embedded into manual links to process rules, parameter settings, interface validation; trigger from manual to event-driven; timing from post-event to in-process and pre-event. The change of control locations leads to control gaps because original controls based on paper documents, manual signatures, hierarchical approval are weakened by automated processes whereas new algorithmic rules, parameter configurations, interface permissions do not have full control coverage[1]. Increased configurability of control rules result in dispersed responsibilities for maintenance of rules – without synchronization mechanisms between process changes and rule updates there is no substance behind control locations existing just in form.

Control locations affect control distance and control visibility. Cross-system and cross-platform processes spread out control activities across different technical modules with fragmented control responsibility by location distribution which makes it impossible for supervisory entities to have a full control trail. Exception handling, manual intervention and rollback mechanism of process automation without clear control rules will create control bypass paths. Control frequency and control granularity is synchronous: Real time validation instead of periodic review; When control rule updates lag behind process changes, there exists a risk of disconnecting rules from business. Focus on location, trigger condition, permission configuration and log retention to identify if control coverage adjusts synchronously as process reengineering and whether control trail can be fully reconstructed in dispersed processes.

2.2 Control Failure Risks Arising from Data Centralization and Algorithmic Decision-Making

When financial data, business data and external data converge on a platform or data middle platform, centralized data assets emerge and alter the structure of control dependence[5], data permission, interface security and master data quality are the basic conditions for effective control: without identity verification and access scope restriction at interfaces, bulk data is read, modified or erroneously transmitted out of its authority, making the expansion of control failure goes from local level to system levels; duplicate master data with inconsistent standards and unclear source records make it difficult for control entities to track data sources and change process, affecting the completeness and reliability of control evidence. Centralized data improves the capability of data correlation analysis but expands the aggregation scope of sensitive information, increasing the scope and concealment of control failures.

Automation of judgment refers to the assignment of some judgment tasks to execute on models. Control activities refer to the linkage among model training, parameter tuning and result output. Opaque bases for model judgment, inappropriate sample selection, untimely model update, and bias in feature selection cause deviation of output results away from control objectives which are difficult to find out through traditional sampling review. The solidified rules of automated decision-making leave abnormal scenarios and edge cases uninvolved in manual judgment intervention, conceal and accumulate control failure. Lack of model version management and no approval for retraining leads to detached automated judgment from control supervision. Risk identification includes: data management, algorithm explanation, model monitoring and decision review; assess coverage and response capability of control activities when there's data centralization and automated judgment; determine whether it can

be identified and corrected in time regarding model output deviations[5].

2.3 Risks in the Allocation of Control Responsibilities in Human-Machine Collaboration Scenarios

For human-machine collaboration, routine transactions, data validation, and initial judgments are entrusted to intelligent systems while exceptions, complex judgment, and final confirmation tasks are done by humans[3], Control responsibilities shift between humans and systems based on task allocation rules, permission settings, and interaction design. Without a clear rule for allocating tasks, manual reviews will become mere formality leading to form automation bias in which operators tend to follow the output of the system and reduce their own judgment. Without clear records of attributing responsibility between system recommendations and human decisions, tracking the control responsibilities when deviation occurs is difficult. With intelligent systems taking over some function of control execution, control responsibilities interweave from position responsibilities to system configuration responsibility, model supervision responsibility, and manual review responsibility with the integrity of the responsibility chain facing challenges.

Risk of control responsibilities allocated reflects the inconsistency of permissions and capabilities in human-machine collaboration scenarios: intelligent systems take over some functions for executing controls but human control entities should have the capability like data interpretation, model understanding, and anomaly identification; without them leads to ineffective implementation of control activities. Incomplete information shown on interactive interfaces or inconspicuous warning prompts makes difficulty for humans' judgments with solid foundations. Incomplete preservation of system logs, operation records, and decision bases makes monitoring and evaluations lacking in verifiability. Risk identification needs to focus on task allocation, permission configuration, capability matching, interaction design, and responsibility tracing mechanisms; determine whether the control responsibilities under human-machine collaboration conditions are clear, executable, and verifiable; assess if the allocation of responsibilities could be dynamically adjusted according to changes of task complexity and system autonomy[3].

3. Strategy Construction for the Intelligent Transformation of Enterprise Finance from the Perspective of Internal Control

3.1 Optimization of the Intelligent Financial Governance Structure at the Control Environment Level

Optimization of intelligent financial governance structure refers to distribution of authority and responsibility, managing data and algorithms, handling model risks: Organizations build their own cross-functional governance architecture by integrating finance, information technology, data management, and internal auditing in a control responsibility network; clearly defining data ownership, model approval authority, parameter adjustment authority, and exception handling authority. Data management responsibilities and algorithm management responsibilities integrated into the financial governance system as an authorization chain from data standards and model admission to result review. Governance changes from hierarchical approval to platform-based, matrix-based, and specialized division of labor with the control environment covering all processes of data assets and the process of algorithm use.

The optimization of the control environment includes personnel competence, control culture and incentive and constraint mechanisms: Financial personnel should have data literacy, understanding of models, anomaly detection; Position integration combines financial judgment with technical operation. Control culture focuses on data quality, algorithm transparency, responsible traceability; norms for using intelligent systems, approval of model changes, recording manual interventions are embedded in the code of conduct. Incentive and constraint mechanisms relate to allocation of responsibilities; Data quality, model monitoring, control execution is part of performance evaluation which constitutes a control environment with clearly defined authority and responsibility, matching capabilities, effective supervision[1].

3.2 Intelligent Control Embedding Strategies at the Risk Assessment and Information and Communication Levels

Intelligent control embedding employs risk lists, rule bases, and continuous monitoring; advancing

control rules into transaction initiation, data entry, and process nodes[2][4]; transition risk assessment from periodic to continuous via anomaly detection, scenario simulation, and model monitoring detecting data bias, algorithm changes, interface security, and process interruption; enter workflow, smart contract, and interface validation by configuring control rules automatically verifying, intercepting and authorizing dynamically; establish approval and version management for risk threshold, control parameter, and exception rules; run control activities concurrently with business activities. The depth of control embedding must match the degree of process automation: automatic control implements rule-driven links but manual intervention interfaces are still present in judgment-intensive links coordinating rule-based control and manual judgment.

Information and Communication Strategy: Unified Data Definition, Real-Time Interaction and Explainable Feedback. The data middle platform and financial platform are information hub with standard interface between business system, model service and decision making terminal for full transmission of control information inside process. Visual dashboard, Intelligent Alert and Semantic interaction improve information accessibility; Model output has rationale explanation, confidence level and scope of impact to assist manual judgment. Abnormal information, Control Deviation and Intervention Record constitutes a feedback loop which will transmit back to rule optimization, model adjustment and responsible entities as a multi-node, feedback capable information and communication structure. Information and Communication Mechanism should distinguish routine control information from exception control information: Routine control information enters into process in a standardized way while exception control information triggers manual attention by alert and interaction so that control information can be effectively transmitted and responded at different levels and among different entities[2][4].

3.3 Dynamic Feedback and Capability Iteration Strategies at the Monitoring and Evaluation Level

Technical supports for monitoring and evaluation: Continuous auditing, analyzing operation records, inspecting logs; extend monitoring from sampling inspection to full transaction inspection, model behavior and system logs[2][5]; Evaluate control effectiveness through control rule coverage, anomaly interception rate, manual review ratio and model deviation level (combination of process indicators and result indicators) in an evaluation system. Involves monitoring of data flow and algorithm usage, monitoring of model training, parameter tuning, version update and result output, detection of control bypass, rule lag and responsibility breakpoints. Design of monitoring and evaluation indicators should take into account balancing the standardization of control execution with the timeliness of control response, establishing a comparable evaluation standard between automated control and manual control, so as to make monitoring results reflect the overall operating state of the control system.

The dynamic feedback and capability iteration strategy involves monitoring, analysis, feedback and adjustment: abnormal data, deviation in models and manual intervention records produced by control operations feed back to control rule base, model parameters and institutional arrangements leading to update of control rules and algorithm retraining; capability iteration includes personnel capability, model capability, and organizational capability improving the level of human-machine collaborative control via updating knowledge base, skills training and role reconstruction. By linking monitoring and evaluation results with governance structure, risk assessment, and information and communication can continuously evolve internal control during finance's intelligent transformation that matches control objectives with technical environment dynamically. Iteration mechanism needs clarifying categorized processing pathway for feedback information, integrate control rule adjustments, model parameter optimization and institutional revisions into different decision-making processes, turning monitoring and evaluation from a static compliance inspection to dynamic capability building[5].

Conclusion

This paper establishes a theoretical basis for intelligent transformation of finance through internal control: identifying changes in control locations in process automation, failures of control caused by data centralization and automated judgment, as well as risks involved in allocation of control responsibilities in human-machine collaboration scenarios, proposing strategic arrangements at three levels (control environment, risk assessment and information and communication, and monitoring and evaluation), demonstrating that there is no one-way adaptation from internal control to intelligent transformation of finance – control requirements need to be configured into the system, system operation data needs to support adjusting controls, and control rules have to constantly adapt along with

data sources and models' use. Future research could consider connecting model explanation and control evidence, defining control boundaries when cross-organizational data interact, designing mechanisms for coordination of update of control rules and algorithm parameters, and dynamic evolution of allocation of control responsibilities under increasing autonomy of intelligent systems, which will further enrich the explanatory power and strategic space of internal control theory in the context of intelligent finance.

References

[1] Zong Wenjuan. Research on Financial Internal Control under Financial Intelligence. Journal of Jiamusi University (Natural Science Edition), 2022, 40(2): 149 - 151.
[2] Yang Yuwen. Research on the Construction of Intelligent Finance and Internal Control. China Management Informatization, 2022, 25(11): 121 - 124.
[3] Lu Xingfeng. Exploration of a New Financial Management Model with Multi-dimensional Collaboration among "Human, Machine, and Object" under Intelligent Finance. Finance and Accounting Monthly, 2021(12): 57 - 65.
[4] Zhao Lijin, Hu Xiaoming, Zhang Xuedong. Construction Framework and Implementation Path of Financial Intelligence under the Background of Digital Economy. Finance and Accounting Communications, 2021(10): 107 - 111.
[5] Lu Huan. Exploration of Enterprise Internal Control Risks and Prevention in the Environment of Big Data and Artificial Intelligence. Market Modernization, 2021(20): 93 - 95.