

Research on Financial Risk Control Based on the COSO-ERM Framework - A Case Study of Yunnan Open University

Xiaotian Zhang^{1*}

¹ Yunnan Open University, Kunming, China

*Correspondence: Xiaotian Zhang

Received: 26 June 2026; **Accepted:** 29 July 2026; **Published:** 21 August 2026

Abstract:

With the rapid development of higher education and the diversification of funding sources, university financial risk management faces increasingly complex challenges. This study, grounded in the COSO Committee's 2017 Enterprise Risk Management – Integrating with Strategy and Performance (COSO-ERM) framework, systematically analyses the current state and problems of financial risk management at Yunnan Open University—a case characterised by its dual-mode operation of “open education plus vocational education”—from five dimensions: governance and culture, strategy and objective-setting, performance, review and revision, and information, communication and reporting. Corresponding countermeasures are proposed based on the COSO-ERM framework. The research indicates that the COSO-ERM concept, which integrates risk management with corporate strategy and performance, provides universities with a systematic guide that goes beyond traditional internal control. Nevertheless, for a special organisation like an open university that concurrently performs both open and vocational education functions, adaptive adjustments must be made in light of its unique governance structure and operational characteristics. The study recommends implementation through five aspects: optimising governance structure, cultivating risk awareness, improving management systems, building digital intelligent monitoring systems, and closing the information communication loop, so as to enhance financial risk management at Yunnan Open University and offer reference for similar institutions.

Keywords:

COSO-ERM Framework, Financial Risk, Enterprise Risk Management, Open University, Dual-Mode Operation

1. Introduction

With the rapid development of China's higher education and the diversification of funding sources, the scale of funds involved in university financial management continues to expand, business scenarios multiply, and the financial risks faced become increasingly complex. University financial risk control is a systemic project: while it manifests in financial operations, its roots often lie deep in governance structures, strategic decisions, and daily operations[1]. How to effectively identify, assess,

respond to, and monitor university financial risks has become a common concern for educational authorities and university administrators.

As an important component of China's higher education system, open universities undertake the significant mission of lifelong and continuing education, and their operational models differ markedly from those of conventional universities[2]. Taking Yunnan Open University as an example, the institution operates under a management system of "one team, two plaques" (i.e., the same leadership team manages two separate legal entities) and simultaneously performs the functions of open education and higher vocational education, forming a distinctive "dual-mode" operational pattern. This unique model exposes the university to more complex financial risk challenges in terms of governance structure, resource allocation, and business processes. The university has already established information facilities such as an online financial platform and a smart campus card system, and in 2024 piloted 12 internal control policies including the Basic Internal Control Standards (Trial) and 11 internal control application guidelines. However, deficiencies remain in risk identification, assessment, and response.

The COSO Committee's 2017 Enterprise Risk Management – Integrating with Strategy and Performance (hereafter "COSO-ERM framework") elevates enterprise risk management from the traditional internal control perspective to a new level that integrates with strategy and performance. The framework emphasises embedding risk management throughout the organisation to influence strategy and performance, providing systematic guidance for establishing comprehensive risk management systems. In recent years, domestic scholars have begun applying the COSO-ERM framework to university financial risk management research. However, studies specifically targeting open universities—which bear the dual functions of both open and vocational education—remain relatively scarce. This paper takes Yunnan Open University as a case study, and based on the five elements of the COSO-ERM framework—governance and culture, strategy and objective-setting, performance, review and revision, and information, communication and reporting—systematically analyses its current financial risk management, identifies key risk issues, and designs targeted financial management countermeasures, aiming to provide theoretical reference and practical guidance for financial risk control at open universities and similar institutions.

2. Theoretical Foundations and Literature Review

2.1. Financial Risk Management Theory

Financial risk management refers to the management process by which organisations identify, assess, respond to, and monitor various risks in financial activities to safeguard the achievement of financial objectives. University financial risks typically include financing risk, investment risk, fund operation risk, budget management risk, internal control risk, etc. Unlike for-profit enterprises, universities, as public welfare public institutions, must not only focus on fund safety and utilisation efficiency but also balance multiple objectives such as educational equity and social benefits. This necessitates adaptive adjustments in both theoretical frameworks and practical approaches for university financial risk management.

In terms of the evolution of risk management, financial risk management has progressed from single-risk response to comprehensive risk management, and from

compliance-oriented to value-oriented approaches. Traditional financial risk management emphasised post-event control and loss compensation, whereas modern financial risk management stresses the organic integration of pre-event prevention, in-process control, and post-event evaluation, with attention to the balance between risk and return and the supportive role of risk management for organisational strategy.

2.2. Overview of the COSO-ERM Framework

The COSO Committee first issued Enterprise Risk Management – Integrated Framework in 2004 and significantly revised it in 2017[3], releasing Enterprise Risk Management – Integrating with Strategy and Performance. Compared with the 2004 version, the 2017 COSO-ERM framework places greater emphasis on integrating risk management with corporate strategy and performance, highlighting that risk management should be embedded throughout the organisation and influence strategy and performance. The 2017 COSO-ERM framework consists of five interrelated elements[4]:

First, Governance and Culture – the foundational element, emphasising the importance of “tone at the top” and the supporting role of culture for effective risk management. It contains five principles: board risk oversight, establishing operating structures, defining the desired culture, demonstrating core values, and attracting, developing, and retaining capable individuals. Governance embeds risk management into organisational governance mechanisms, fundamentally setting the risk tone.

Second, Strategy and Objective-Setting – this element stresses the critical integration of ERM, strategy, and objective-setting, highlighting that effective ERM should serve as an important strategic tool. Organisations should fully consider risk factors when formulating strategy and embed risk management throughout strategy execution.

Third, Performance – this element emphasises identifying, assessing, responding to, and reporting risks related to strategy and business objectives, including risk identification, severity assessment, and risk response.

Fourth, Review and Revision – this element describes how performance evaluations reveal the operating status of the ERM process and what revisions are needed. Organisations should continuously assess the effectiveness of their risk management systems and make dynamic adjustments in response to internal and external environmental changes.

Fifth, Information, Communication and Reporting – this element emphasises that ERM is an ongoing process requiring continuous identification and sharing of risk and strategy information. Organisations should ensure that relevant risk information is effectively transmitted at appropriate levels and scopes.

3. Analysis of Financial Risk Management Problems at Yunnan Open University – A Systematic Risk Diagnosis Based on COSO-ERM Elements

3.1. Risks at the Governance and Culture Level

First, at the governance structure level, the “one team, two plaques” management system, while conducive to unified leadership, also creates blurred lines of authority and responsibility. Open education and vocational education differ in their financial

management objectives, standards, and processes, yet the same management team must simultaneously address the financial risks of both models, which may lead to a “one-size-fits-all” approach or neglect of one at the expense of the other. For example, the online fund security risk of open education tuition collection and the risk of delayed industry-university cooperation fund disbursement for vocational education differ significantly in risk nature, impact extent, and response strategies, but under the current management system there is no differentiated risk control mechanism. Although the university has formulated internal control basic standards clarifying that the objectives of internal control are to ensure the legality and compliance of teaching, research, and management service activities, the safety and effective use of assets, and the truthfulness and completeness of financial information, it still lacks systematic design in the organisational structure and governance mechanisms for risk management[5].

Second, at the organisational structure level, the university has not yet established a dedicated risk management department or a clearly designated leading risk management agency. Risk management functions are dispersed among finance, audit, business, and other departments, lacking central coordination and professional oversight. Although the 12 internal control policies piloted in 2024 have been initially established, in practice there still exists a “two-skin” phenomenon where systems and operations are not integrated.

Third, at the culture building level, the awareness of risk management among all staff needs strengthening. Some faculty and staff still regard financial risk as “the finance department’s business”, and cross-departmental risk control collaboration is poor, making it difficult to form a comprehensive defence. As the COSO-ERM framework emphasises, culture is the foundation of effective risk management, yet the university has not yet fostered an organisational culture of “everyone cares about risk, everyone participates in risk control”.

3.2. Risks at the Strategy and Objective-Setting Level

First, at the strategic positioning level, there is insufficient integration between the strategic objectives of the “dual-mode” operation and risk management. The COSO-ERM framework stresses embedding risk management throughout the strategy-formulation and execution process, but currently the university’s strategic planning and risk management remain disconnected. The two modes—open education and vocational education—differ in their positioning, development goals, and resource allocation, yet there is no matching differentiated risk management strategy.

Second, at the objective-setting level, the university’s financial risk management objectives are not sufficiently clear and specific. Although the internal control system states objectives such as compliance, asset security, and information truthfulness, it has not established a risk appetite and risk tolerance system aligned with the “dual-mode” strategy. The 12 internal control policies piloted in 2024 mainly focus on business process standardisation and lack a mechanism for systematic risk identification and assessment from a strategic perspective.

Third, at the level of integrating risk and strategy, the university has not established a closed-loop mechanism that feeds risk assessment results back into strategic decision-making. Risk assessments in key areas such as research fund management, student admissions, and infrastructure projects are often perfunctory and cannot effectively support strategic decisions.

3.3. Risks at the Performance Level

First, in risk identification, the university has not constructed a routine, full-coverage risk identification mechanism tailored to the “dual-mode” operation. Major risks for open education include fund security in online tuition collection, student status management, and copyright of online teaching resources; for vocational education, major risks include industry-university cooperation funding, practical training base construction, and student internship management. The risk points of the two modes differ significantly, but current risk identification is often generalised and consolidated, lacking refined identification of the unique risks under the “dual-mode” conditions[6].

Second, in risk assessment, the university has not established a systematic risk assessment mechanism. There is no quantitative analysis of risk probability and impact, and risk grading lacks scientific basis. As required by the “Performance” element of the COSO-ERM framework, organisations should systematically identify, assess, and respond to risks associated with strategic objectives, but currently the university’s risk assessment work is still in its infancy.

Third, in risk response, the university lacks differentiated response strategies for different risk levels. Although control activities in budget management, revenue management, expenditure management, and asset management have been initially established, the systematicness and pertinence of control measures are insufficient. Budget preparation is dominated by the finance department with low participation from business departments; budget execution lacks rigid constraints; expenditure review is not strict enough, and accounting treatment is not sufficiently standardised.

3.4. Risks at the Review and Revision Level

First, in internal supervision, the independence and effectiveness of internal audit need strengthening. Internal audit risk assessments may become formalistic, and the application of audit results is inadequate, failing to form an effective rectification closed-loop.

Second, in system updating, some management policies have not been promptly updated to reflect policy changes and business developments. For example, risk control provisions for new financing instruments such as green bonds and REITs are absent. The risk database is blank, and historical risk events have not been systematically archived and analysed, leading to repeated occurrences of similar risks.

Third, in continuous improvement, the university has not established a regular evaluation and dynamic adjustment mechanism for the internal control system. As emphasised by the “Review and Revision” element of the COSO-ERM framework, organisations should use performance evaluations to gain insight into the operation of the ERM process and make timely revisions. However, the current risk management system lacks a mechanism for self-improvement and continuous enhancement.

3.5. Risks at the Information, Communication and Reporting Level

First, in information systems, there are information silos among the financial system, asset system, academic affairs system, etc., with no real-time data sharing and interoperability, leading to a disconnect between financial accounting and business management. For example, information asymmetry between project progress and

financial payments may cause mismatches between fund disbursement and project completion [7].

Second, in information transmission, the chain from risk discovery to decision-making is too long, resulting in poor response timeliness. Risk signals detected by frontline staff are difficult to communicate promptly to management, and management struggles to obtain a complete picture of key risk points.

Third, in communication mechanisms, cross-departmental communication is inefficient. There is no routine communication mechanism between the finance department and business departments, and information sharing lags. Risk reporting lacks depth, often merely listing financial indicators without in-depth analysis of causes or recommendations. The COSO-ERM framework emphasises that ERM is an ongoing process requiring continuous identification and sharing of risk and strategy information, but the current information communication mechanisms at the university cannot meet this requirement.

4. Countermeasures for Financial Risk Management at Yunnan Open University Based on the COSO-ERM Framework

4.1. Optimise Governance Structure and Build a Risk Governance System with Clear Authority and Responsibility

Targeting the risks at the governance and culture level, we should start with optimising the governance structure and establish a risk governance architecture that matches the “dual-mode” operation[8].

First, improve the governance structure under the “dual-mode”. On the basis of the existing “one team, two plaques” management system, clarify the financial management responsibilities and authority of the open education and vocational education business lines. Establish a differentiated risk management mechanism, developing separate risk control plans for open and vocational education to avoid a “one-size-fits-all” approach.

Second, establish a three-tier risk management organisational structure. It is recommended to set up a risk management committee led by the university’s top leadership as the highest decision-making body for risk management. Establish a risk management office within the finance department to coordinate and promote daily risk management work. Appoint risk management liaisons in each business department to be responsible for departmental risk management, forming a “university – department – position” three-tier architecture.

Third, improve the “Three Major and One Important” decision-making mechanism (i.e., major decisions, major cadre appointments, major project arrangements, and large-sum fund use). Implement collective decision-making on major economic matters to ensure that risks of significant decisions are fully assessed and effectively controlled. Clarify risk management responsibilities and establish a performance appraisal mechanism that incorporates risk management outcomes into departmental and individual performance evaluations.

4.2. Cultivate Risk Awareness and Foster a Participatory Risk Culture

Targeting the risks at the governance and culture level, integrate risk management concepts into campus culture building and construct a risk-prevention atmosphere with full participation.

First, embed risk management concepts into campus culture. Through internal control training sessions, risk case teaching, scenario simulation drills, etc., enhance the risk awareness and identification capabilities of all staff. Help faculty and staff understand that financial risk is not only the responsibility of the finance department but a shared duty of all employees.

Second, establish a risk management performance appraisal mechanism. Incorporate risk management results into departmental and individual performance appraisals, transforming risk management from a “soft constraint” into a “hard indicator”. Through appraisal orientation, encourage all departments to proactively identify and prevent financial risks in their operational areas.

Third, foster a positive atmosphere of “everyone cares about risk, everyone participates in risk control”. Encourage frontline employees to proactively report risk hazards and establish a reward mechanism for risk reporting. Recognise and reward employees who identify major risk hazards or propose effective risk prevention recommendations, stimulating the enthusiasm and initiative of all staff in participating in risk management.

4.3. Improve Management Systems and Establish a Comprehensive, Full-Process Institutional Framework

Targeting the risks at the strategy and objective-setting level and the performance level, start with institutional construction to improve the financial management system covering the entire process of “dual-mode” operation[9].

First, embed risk management into strategic planning. Clearly define the strategic positioning and objectives of financial risk management in the university’s strategic plan. In light of the “dual-mode” characteristics, establish a risk appetite and risk tolerance system, setting differentiated risk tolerance standards for open education and vocational education respectively. When making major strategic decisions, conduct risk assessments concurrently to ensure that risk management is aligned with strategy execution.

Second, establish a routine risk identification and assessment mechanism. Systematically identify risk points across six major business areas: revenue, expenditure, budget, final accounts, projects, and monetary funds. Pay special attention to the unique risks under the “dual-mode” conditions, using methods such as risk matrices to conduct quantitative assessments of probability and impact, and develop risk registers and risk maps.

Third, strengthen the budget management system. Establish a “full participation, full-process control, full-coverage” budget management system. Increase the participation of business departments in budget preparation and reinforce the rigid constraints of budget execution. Establish a budget execution progress notification and early warning mechanism to promptly analyse and correct budget deviations.

Fourth, standardise revenue and expenditure and asset management systems. Strictly implement approval procedures for fee collection and standardise the invoice management process. Establish a robust expenditure management system to strictly verify the authenticity and legality of expenditure items. Establish a full-life-cycle

asset management system, regulating the acquisition, use, maintenance, and disposal of fixed assets, and conduct regular asset inventories to ensure consistency between accounting records and physical assets.

Fifth, establish differentiated risk response mechanisms. Based on risk assessment results, develop differentiated response strategies for high-, medium-, and low-risk categories. Implement key controls in high-risk areas such as research fund management, student admissions, infrastructure projects, and industry-university cooperation, ensuring effective risk control in these critical domains[10].

4.4. Promote Digital and Intelligent Transformation and Build an Intelligent Risk Monitoring System

Targeting the risks at the information, communication and reporting level, fully apply modern information technology to advance the digital and intelligent transformation of financial risk management.

First, promote information system integration and data sharing. Break down information silos and achieve interoperability among financial, asset, academic affairs, OA, and other systems. Build a unified financial information management platform to enable real-time data sharing and cross-validation, eliminating the disconnect between financial accounting and business management.

Second, establish an intelligent risk monitoring system. Leverage big data technology to build a real-time early warning system for risk monitoring. Dynamically monitor key risk indicators, set warning thresholds, and achieve early detection, early warning, and early disposal of risks. When risk indicators trigger the warning line, automatically initiate risk response procedures.

Third, explore the application of artificial intelligence in risk management. Use AI to improve the efficiency and accuracy of risk identification and assessment. Explore the application of machine learning in risk prediction and anomaly detection, using data models to make forward-looking risk projections, thereby providing scientific evidence for management decisions.

4.5. Smooth Information Communication and Establish a Closed-Loop Risk Management Mechanism

Targeting the risks at the review and revision level and the information, communication and reporting level, construct an efficient and smooth information communication and continuous improvement closed-loop management mechanism[11].

First, establish an internal control effectiveness evaluation mechanism. Regularly conduct internal control self-assessments and independent evaluations to assess the effectiveness of the risk management system. Timely rectify identified issues, forming a closed loop of “assessment – feedback – rectification – re-assessment”. Establish a dynamic system update mechanism to track national policy changes and industry trends in a timely manner, and periodically review and revise various management policies.

Second, establish a risk monitoring, early warning, and knowledge management mechanism. Dynamically monitor key risk indicators and set warning thresholds. Build a risk database to systematically archive and analyse historical risk events, forming a complete closed loop of “risk identification – risk assessment – risk

response – risk monitoring – risk reporting – risk feedback”, ensuring that similar risks do not recur.

Third, establish a routine cross-departmental communication mechanism. Regularly convene joint meetings between the finance department and business departments, establish a risk information sharing platform, and enable timely transmission and coordinated handling of risk information. Optimise the risk information transmission process, shorten the chain from risk discovery to decision-making. Establish a graded risk reporting system to ensure that risks of different levels are quickly communicated to the appropriate decision-making levels.

Fourth, improve the risk reporting system. Design risk report templates to conduct in-depth analysis of risk causes and provide targeted recommendations. Enrich the content of risk reports to not merely list financial indicators but to reveal underlying management deficiencies and institutional defects, offering valuable decision-making references for management.

5. Conclusions

Based on the COSO Committee’s 2017 Enterprise Risk Management – Integrating with Strategy and Performance framework, this paper systematically analysed the current state and problems of financial risk management at Yunnan Open University under its “dual-mode” operation from five dimensions—governance and culture, strategy and objective-setting, performance, review and revision, and information, communication and reporting—and proposed targeted countermeasures from five aspects: optimising governance structure, cultivating risk awareness, improving management systems, promoting digital and intelligent transformation, and smoothing information communication.

The research shows that Yunnan Open University has laid a certain foundation for financial risk management, including information facilities such as an online financial platform and a smart campus card system, and the pilot of 12 internal control policies in 2024. However, under the special context of “dual-mode” operation, the university still exhibits significant deficiencies in governance and culture, strategy and objective-setting, performance, review and revision, and information, communication and reporting. The root causes of these problems lie in: first, the “one team, two plaques” governance structure leads to blurred boundaries of risk management responsibilities; second, there is an adaptability challenge between the core logic of the COSO-ERM framework—designed for the corporate sector—and the public welfare attributes of universities; third, the risk assessment mechanism has not been differentiated to address the unique risks of the “dual-mode” operation. The five countermeasures proposed in this paper—optimising governance structure, cultivating risk awareness, improving management systems, promoting digital and intelligent transformation, and smoothing information communication—are interrelated and mutually supportive, collectively constituting a comprehensive financial risk management system based on the COSO-ERM framework. This study provides a valuable reference for financial risk management at open universities and similar institutions.

Future research can be deepened in the following directions: first, conducting quantitative assessments of Yunnan Open University’s financial risks using empirical data; second, carrying out comparative studies across regions and university types to distil differentiated paths of financial risk management under different operational

models; third, exploring the in-depth application of new technologies such as big data and artificial intelligence in university financial risk monitoring; and fourth, examining the applicability of non-financial risk indicators such as ESG in university financial risk assessment.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this article.

Funding

This work was supported by the The 2025 Yunnan Open University scientific research fund project ‘Research on Risk Assessment of the Dual-mode School-running of Yunnan Open University Based on the COSO Framework’ (Project Number: 25YNOUZ30).

References

- [1] Lin, P.P. Research on the Source Governance Mechanism of University Financial Risks Based on Value Chain Analysis. *Commercial Accounting*, 2026, 13, 102-106.
- [2] Lei, X.L. Research on Prevention and Control of University Financial Risks——Taking University A in Hubei Province as an Example. *Innovation World Weekly*, 2026, 10, 65-67.
- [3] COSO. Enterprise Risk Management — Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission, 2017.
- [4] Barreto, K.A.; Callado, A.A.C.; Callado, A.L.C. Internal control under the approach of COSO ERM framework components: A study in a higher education institution. *Revista Ambiente Contábil*, 2023, 15(2), 202-223. DOI: 10.21680/2176-9036.2023v15n2ID33077.
- [5] Silveira, J.S.; Carvalho, R.F.; Peleias, I.R.; Fernandes, F.C. Internal control and risk management: The perception of financial managers in private higher education institutions. *Revista CRCSC*, 2025. DOI: 10.16930/2237-766220253513.
- [6] Syahrullah, Y.; Nashida, A.A.; Prakoso, I.; Nando, F.T. Risk mitigation through integration COSO-Enterprise Risk Management and ISO 31000 in higher education. *International Journal of Educational Management and Innovation*, 2025, 6(2), 202-218. DOI: 10.12928/ijemi.v6i2.11547.
- [7] Asad, A.; Mehmood, S.; Hussain, S.; Amir, M. Analysis of risk management in higher education institutions. *International Research Journal of Management and Social Sciences*, 2023, 4(3).
- [8] Chen, R. Research on the Construction of Internal Control System in Universities and the Improvement of Governance Structure. *Value Engineering*, 2012, 35, 219-221. DOI: 10.14018/j.cnki.cn13-1085/n.2012.35.076.

- [9] Chen, Y.Q. Research on Optimization of Internal Control Construction in Universities Based on the COSO-ERM Framework: A Case Study of T University. *Shanghai Management Science*, 2025, 6, 92-97.
- [10] Syahrullah, Y.; Nashida, A.A.; Prakoso, I.; Nando, F.T. Risk mitigation through integration COSO-Enterprise Risk Management and ISO 31000 in higher education. *International Journal of Educational Management and Innovation*, 2025, 6(2), 202-218. DOI: 10.12928/ijemi.v6i2.11547.
- [11] Lin, X.T. Optimization of the Collaborative Mechanism of “Discipline Inspection, Patrol, Finance, and Audit” in Universities from the Perspective of Financial Supervision. *Green Finance and Accounting*, 2026, 2, 41-45. DOI: 10.14153/j.cnki.lsc.2026.02.004.



© 2026 by the author(s); licensee International Technology and Science Publications (ITS), this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (<http://creativecommons.org/licenses/by/4.0/>)