Research on the Construction of Early Warning Mechanism and Closed-Loop Management System of College Students' Telecommunication Network Fraud from the Perspective of Integrated Governance

Chuanjie Liu, Yutong Deng, Jiaming Cui
Department of Public Security Management, Beijing Police College, Beijing, China

Abstract: Telecommunication network fraud has become a prominent form of crime in the digital age, and college students have become the main victims because of their lack of social experience and frequent network use. Academic circles have accumulated rich governance tools from multiple dimensions, but there are theoretical integration and systematic framework construction faults in the research. From the perspective of risk management theory, this paper reveals the basic pattern of "rich tools but lack of framework" at present, and identifies three major integration dilemmas: decentralized governance tools, fuzzy distribution of rights and responsibilities, and static process management. Based on enterprise risk management theory and PDCA cycle, an integrated theoretical framework is constructed, which includes five core elements: governance environment and organizational basis, risk identification and evaluation, risk coping strategies, control activities and implementation mechanism, information communication and supervision improvement. A multi-subject power and responsibility system based on the three-tier structure of "risk owner-risk controller-risk supervisor" is designed. The closed-loop realization path and performance evaluation index system of planning, execution, inspection and treatment are explored. This study provides a systematic management solution to get rid of the dilemma of campus anti-fraud fragmentation.

Keywords: Telecommunication Network Fraud; College Students; Risk Management; Theoretical Framework; Realization Path

1. Introduction

Telecommunication network fraud has become a prominent problem endangering social security and stability. According to the 53rd Statistical Report on China's Internet Development by China Internet Network Information Center, by the end of December 2023, the number of Internet users in China had reached 1.092 billion, of which students accounted for 21.5%. At the same time, all kinds of telecommunication network fraud cases continue to be high, and college students have become the key target group of fraudsters because of their relatively insufficient social experience, high frequency of network use and easy access to personal information. According to the data of the Criminal Investigation Bureau of the Ministry of Public Security, in 2023, public security organs across the country cracked 437,000 cases of telecommunication network fraud, among which the proportion of cases involving school students can not be ignored, and it shows a trend of younger age and higher education. Faced with this grim situation, although the Ministry of Education, the Ministry of Public Security and other departments have jointly issued several documents to deploy anti-fraud work, and various forms of publicity and education activities have been carried out in colleges and universities around the country, the cases of college students being deceived are still repeated, and the governance efficiency needs to be improved urgently. The researchers pointed out that telecom fraud in colleges and universities has the characteristics of intelligent means, strong concealment, high incidence of new students, significant differences in motivation of victims and generally weak prevention ability, which seriously infringes on the rights and interests of college students and affects the safety and stability of campus [1].

From the perspective of academic research, the academic community has launched a wide range of discussions from a multi-dimensional

perspective. Criminology focuses on improving the cost of crime through legal punishment, and advocates perfecting the legal system and building a collaborative protection platform [2]; From the perspective of information technology, we are committed to developing intelligent early warning models to identify fraudulent behaviors, using algorithmic models to identify fraudulent phone calls and phishing websites, and building risk portraits based on user behavior data; From the perspective of psychology, the cognitive bias and psychological weakness of victims are deeply analyzed, and the constituent dimensions of college students' vulnerability to telecommunication network fraud are concerned [3]; From the perspective of public management, it calls for multi-subjects to cooperate and co-govern, emphasizing that public security organs, university administrators and other relevant responsible persons should actively participate in governance and form a joint force of governance [4]. These studies touched on the key links of governance from different aspects, and accumulated a wealth of governance tools and paths.

However, from the perspective of management science, especially risk management theory, there are obvious gaps in theoretical integration and systematic framework construction in the existing research: although there are many countermeasures, they are isolated from each other and cannot be integrated into an organic risk management system with clear rights and responsibilities, closed process, auditability and sustainable improvement. The lack of this theory directly leads to the "fragmented governance" at the practical level-technical early warning has produced risk signals, but no one has followed up; Psychological education has a huge investment, but it is difficult to evaluate its effectiveness; Multi-subject collaboration has become a slogan, but it lacks the definition of rights and responsibilities and the assessment mechanism. The reason is that the governance practice is caught in a "collective action dilemma": although each subject has the willingness to participate, it lacks the mechanism guarantee of collaborative landing. Researchers found that one of the fundamental reasons for preventing telecommunication network fraud in colleges and universities at present is the lack of coordination of social security management, the imperfect school safety education system and the poor cooperative education mechanism between home and school [5]. This means that the current governance lacks not tools, but a top-level framework that can organically integrate decentralized tools; What is lacking is not the idea, but a management mechanism that can turn the idea into action.

Based on the above analysis, this study attempts to answer the following three interlocking core questions: First, how to build an integrated theoretical framework for college students' telecommunication network fraud governance? Second, under this framework, how to design a multi-agent power and responsibility system? Third, how to establish the operation mechanism and realization path of the continuous self-improvement of the driving system ?

2. The Existing Model and Limitations of College Students' Telecommunication Network Fraud Governance

2.1 The Existing Governance Model and Its Risk Management Positioning

The existing research has accumulated a wealth of governance tools and paths to solve the problem of telecommunication network fraud. From the perspective of risk management, these studies have touched on different links of risk management process, but they have not been connected in series by unified risk management logic. Mainly can be summarized as the following four modes:

2.1.1 Crime deterrence and judicial punishment mode

This model is a traditional and mainstream governance path, and its internal logic lies in restraining criminal motives by increasing the cost of crime, which belongs to the links of "post-event response" and "loss control" in risk management. The research focus includes the improvement of legal regulation, the improvement of investigation and crackdown technology, and the "full chain" attack on the criminal industry chain. Part of the research introduces the cost-benefit theory of criminal economics, and advocates that the "punishment cost" can be improved by increasing punishment and recovering the proceeds of crime. From the perspective of risk management, this model provides the ultimate legal authority of governance and a rigid means of afterwards remedy, which constitutes the bottom line guarantee of the risk response system. However, its role is obviously lagging behind, and it is a

typical "after-the-fact response", and its contribution to the front-end links of risk management such as risk identification, risk assessment, prevention in advance and intervention in the event is extremely limited.

2.1.2 Technology empowerment and accurate early warning mode

This model relies on big data, artificial intelligence and other technologies, and its core logic lies in realizing pre-identification and dynamic early warning of risks through real-time monitoring and intelligent analysis, corresponding to the "risk identification" and "risk monitoring" links in the risk management process. The research focuses on the identification of fraudulent phone calls and phishing websites by using algorithm models, and the construction of risk portraits and event maps based on user behavior data to deconstruct and dynamically warn the victimization process in stages. The advantage of this model is that it improves the accuracy and timeliness of risk identification, and can realize automatic and large-scale risk scanning, which is the technical support for building an active risk management system. However, it is essentially a manifestation of "instrumental rationality", and it is good at finding "risk points", but it lacks the management logic to transform risk points into specific action instructions of various responsible subjects within the organization, that is, it has completed "identification" but failed to connect "response".

2.1.3. Victim prevention and psychological intervention mode

This model shifts the focus of management to the potential victim, who bears the risk of fraud. Its logic lies in reducing the probability of risk by eliminating or strengthening the psychological vulnerability of individuals, corresponding to the links of "risk mitigation" and "control activities" in risk management. The researcher conducted in-depth interviews with college students by qualitative research methods, and found that college students' vulnerability to telecommunication network fraud consists of four dimensions: telecommunication network risk preference, telecommunication network information processing and vigilance, telecommunication network interaction compliance and telecommunication network interaction self-control. The countermeasures emphasize the development of accurate publicity and education based on audience analysis. The advantage of this model is that it touches the root of the risk, aims to improve the individual's "risk immunity" and is the most cost-effective basic risk mitigation strategy. However, its effect is highly dependent on the effective delivery of content and individual's subjective acceptance, and it is difficult to quantify the effect and cover it comprehensively in organizational management, that is, the effectiveness of "control activities" is difficult to be objectively measured and continuously optimized.

2.1.4. Collaborative governance and ecological governance model

Facing the complexity and cross-domain of fraud, this model puts forward the most systematic concept. Its management logic lies in recognizing that a single subject cannot cope with complex risks, and it is necessary to integrate the forces of public security organs, financial institutions, telecommunications enterprises, universities, communities and other parties to form a joint force of risk management. The study puts forward the concepts of ecological governance and holistic governance, advocates the construction of a responsible community, and emphasizes that we should pay attention to the application of multi-center governance theory to promote the participation and linkage governance of public security organs, universities, students and relevant departments. From the perspective of risk management, this model touches on the core issue of risk management organizational structure design, that is, "who will manage risks". However, the existing research mostly stays at the level of concept advocacy and macro-principles, and provides few management design schemes for the operational core issues of risk management system design such as specific organizational structure, division of powers and responsibilities, information flow process and assessment and accountability mechanism of collaborative governance. The differences between the above four models in risk management link positioning, main contributions and internal management limitations can be summarized as shown in Table 1

3. The Integration Dilemma of Existing Research

The above four models jointly draw a governance picture of "rich tools but lacking framework". If we look at it from the perspective of risk management theory, these scattered

governance tools expose the following three interrelated and structural integration dilemmas:

First, governance tools are scattered in all aspects of risk management and lack an integrated top-level framework. As shown in Table 1, the four models correspond to different links in the risk management process: judicial punishment focuses on "post-event response", technical early warning focuses on "risk identification", psychological intervention focuses on "risk mitigation", and the concept of coordination touches on "organizational structure". Each of these tools contributes to a specific link, but there is no organic and institutionalized connection channel between them. How does technical early warning automatically trigger psychological intervention? How can the case of judicial attack be fed back to the optimization of risk identification model? How can the risk management performance of all parties be evaluated in a unified way? The existing research fails to answer these questions, the fundamental reason is the lack of a top-level risk management framework that can embed risk management elements such as "identification-evaluation-response-monitoring-improvement" into the same set of organizational structure and operation process according to unified management logic. Various governance measures are like pearls scattered at all nodes of the risk management process, and a main line of management is urgently needed to connect them in series into a complete "risk management necklace".

Table 1. Risk Management Orientation and Inherent Limitations of Existing Main Governance Models

Governance model	Risk management link positioning	Main contribution	Internal management limitations
Crime deterrence and judicial punishment	Post-event response and loss control	Provide ultimate legal protection and disciplinary deterrence	Lag in management stage: it is an after-the-fact response, and lacks embedding in the process before.
Technology empowerment and accurate early warning	Risk identification and dynamic monitoring	Improve the accuracy and timeliness of risk identification.	Absence of management subject: after identifying risks, it is unclear who, what process and what action to take.
Victim prevention and psychological intervention	Risk mitigation and control activities	Reduce the probability of risk from the root cause	Fuzzy management effect: it is difficult to quantify and optimize the effectiveness of control activities.
Collaborative governance and ecological governance	Risk management organizational structure design	Put forward the systematic concept of pluralistic co-governance	Management mechanism is vague: lack of specific organizational structure, division of powers and responsibilities and process design.

Second, multi-subject participation has become a consensus, and there is a lack of a clear risk management power and responsibility allocation mechanism. Although collaborative governance has become the consensus of academic and practical circles, the basic management problem of "who is responsible for which part of risk management" is far from clear in the campus scene. What roles do the student affairs department, security department, counselors, departments, information technology centers, student associations and even individual students play in the anti-fraud risk management system? Are they risk owners, risk controllers or risk supervisors? Where are the boundaries of their respective powers and responsibilities? When a fraud case occurs, which link of risk management should be traced back? The existing research on the basic issues of risk management of these organizations is almost zero. Fuzzy responsibility will inevitably lead to prevarication, scattered resources and delayed response, which makes it difficult to escape the "collective action dilemma" in practice and cannot be transformed into effective risk management execution.

Third, the governance practice is characterized by movement, lacking the risk management closed loop that drives the system to improve itself. An effective risk management system must be a living system capable of continuous learning and dynamic adjustment, and its core lies in establishing a closed-loop process of "risk identification, risk assessment, risk response, monitoring and review, and continuous improvement". At present, many campus anti-fraud work shows the characteristics of "sports" and "activity", lacking standardized and

streamlined operation mode and data-based evaluation and feedback mechanism. Most of the existing studies focus on the "response" link, and seriously ignore the "monitoring review" and "continuous improvement". How effective is the risk management of the governance system? How effective are the risk control measures? How to measure the input-output ratio? How to dynamically adjust the risk response strategy according to the evolution of fraud methods? Due to the lack of an independent and powerful audit evaluation and feedback improvement mechanism, that is, the "inspection" and "handling" links in the closed loop of risk management, the whole governance system cannot realize self-evolution, and it is always in a state of passive response and exhaustion.

4. The Construction of the Theoretical Framework of Integrated Risk Management

4.1 An Overview of Integrated Governance Theory

The theory of integrated governance originates from the response of the public management field to the dilemma of "fragmented governance", emphasizing the construction of an integrated governance system through cross-departmental cooperation, resource integration and process reengineering [6]. The core essence of this theory includes: first, the multi-coordination of governance subjects, breaking departmental barriers to form a joint force; The second is to manage the overall allocation of resources to avoid repeated investment and waste of resources; The third is the closed-loop design of governance process to ensure the complete chain from problem identification to effect evaluation; Fourth, the governance mechanism is continuously improved, and dynamic optimization is realized through feedback and learning [7]. The theory of integrated governance provides an important theoretical resource for solving the dilemma of "fragmented governance" in the current campus anti-fraud work.

4.2 Enterprise Risk Management (ERM) Framework and Its Applicability

Enterprise Risk Management, ERM) is a systematic framework for enterprises to integrate risk management into all levels and activities of the organization in order to achieve strategic goals. Enterprise Risk Management-Integrated Framework issued by COSO is one of the most influential risk management standards in the world, which puts forward that risk management should run through the organization's strategic formulation and daily operation, including eight interrelated elements: internal environment, goal setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring [8].

It is of great theoretical applicability and innovative value to introduce ERM framework into the field of college students' telecommunication network fraud governance. First, integration. ERM requires that scattered risk management activities be brought into a unified framework system, which is the top-level design thinking needed to get rid of the current fragmentation dilemma of governance tools, and can bring the originally separated elements such as judicial deterrence, technical early warning and psychological intervention into a unified management logic. Second, organizational embeddedness. ERM regards risk management as a continuous process in which all employees participate in the organization, and requires clear risk management responsibilities of all levels and departments, which provides a theoretical basis for designing the power and responsibility system of multiple subjects on campus [9]. Third, closed-loop management. ERM ensures the continuous optimization of the risk management system through the complete process of "goal setting-risk identification-risk assessment-risk response-control activities-information communication-monitoring-improvement", which is the logical closed loop needed to establish the self-improvement mechanism of the drive system [10]. Fourth, the adaptability of the scene. The core principles of ERM can be adapted to all kinds of organizational scenes, which provides a theoretical possibility for creatively transplanting mature enterprise risk management theory to the special non-profit and educational organization on the university campus.

4.3 The Core Elements of the Framework and the Logical Relationship

Based on ERM framework and integrated governance theory, the integrated governance framework of college students' telecommunication network fraud constructed in this study contains six core elements, and its

logical relationship is shown in Figure 1.

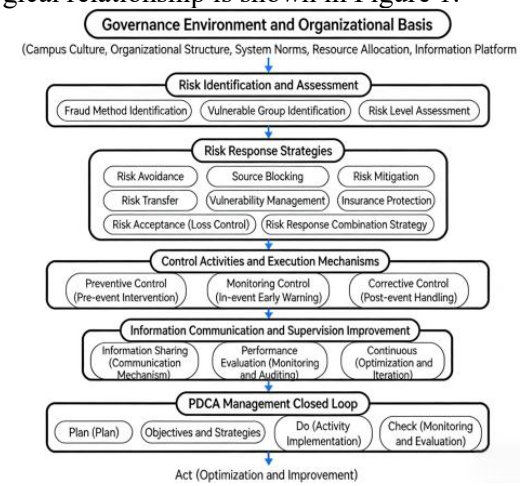

Figure 1. Theoretical Framework of Integrated Risk Management of College Students' Telecommunication Network Fraud

4.3.1 Governance environment and organizational foundation

Governance environment is the foundation of the framework operation and determines the implementation effect of other elements. In the campus scene, it mainly includes: first, campus culture, that is, the degree of cognition and attention of teachers and students to fraud risks; The second is the organizational structure, that is, the establishment of institutions that undertake anti-fraud duties and their subordinate relations; Third, the system norms, that is, relevant rules and regulations and operating procedures; The fourth is the allocation of resources, that is, the manpower, material resources and financial resources invested; The fifth is the information platform, that is, the technical system that supports the collection and processing of risk information.

4.3.2 Risk identification and assessment

Risk identification and assessment is the starting point of the governance process, aiming at systematically identifying the fraud risks faced by the campus and evaluating its level. Specifically, it includes three links: first, the identification of fraud methods, tracking and judging the evolution trend of various fraud methods (single rebate, impersonating customer service, fake shopping, etc.); The second is the identification of susceptible population, which identifies the characteristics and distribution of high-risk students based on behavior data; The third is risk grade assessment, which comprehensively classifies the risks based on factors such as the harm degree of fraud, the size of susceptible population and the perfection of prevention and control measures, so as to provide a basis for subsequent response.

4.3.3 Risk coping strategies

Choosing coping strategies based on risk assessment results can be divided into four categories by referring to ERM framework: first, risk avoidance, which is blocked from the source by cutting off the source of risk, such as blocking fraudulent apps and websites; Second, the risk is released slowly, reducing the probability or influence degree of the risk, such as carrying out anti-fraud publicity and education to enhance students' "immunity"; Third, risk transfer, through insurance and other mechanisms to transfer losses, such as the establishment of campus anti-fraud special insurance; The fourth is risk acceptance, which keeps monitoring the risks with slight impact. In practice, it is necessary to adopt a combination strategy for different risks.

4.3.4 Control activities and implementation mechanism

Control activities are the procedures that translate coping strategies into concrete actions. According to the time sequence of risk occurrence, it is divided into three categories: first, preventive control (pre-intervention), including freshmen's anti-fraud entrance education, normalized publicity and promotion, and targeted reminder of high-risk groups; The second is monitoring control (early warning in the event), including abnormal transaction monitoring, fraud-related information filtering, and abnormal behavior identification of students; Third, corrective control (after-the-fact disposal), including the freezing of funds, psychological crisis intervention, case resumption summary, etc. The three types of control are interlocking to form a complete control chain.

4.3.5 Information communication and supervision improvement

Information communication and supervision improvement are the guarantee to ensure the sustained and effective operation of the framework. Including three aspects: first, the information sharing mechanism, the establishment of risk information sharing channels between various departments in the school, schools and external institutions (public security, finance, communications, etc.); The second is the performance evaluation system, which designs scientific indicators to quantitatively evaluate the governance effect; The third is to continuously improve the

mechanism, and continuously optimize risk management strategies and control activities based on performance evaluation and supervision and audit findings.

4.3.6 PDCA management closed loop

The above five elements are organically integrated and dynamically optimized through PDCA cycle. The task of the Plan stage is to set risk management objectives, formulate risk coping strategies and control activity plans; The task of the implementation (Do) stage is to implement control activities and risk response plans; The task of the Check stage is to monitor the implementation of control activities, evaluate the performance of risk management and identify existing problems; The task of the Act stage is to take improvement measures to optimize the risk management system in view of the problems found in the inspection. After completing a cycle, the improvement measures will be incorporated into the next round of plans to achieve a spiral rise.

The relationship between these six elements can be understood as follows: the governance environment is the base, which supports the operation of the whole system; Risk identification and assessment is the entrance, providing input for follow-up activities; Risk coping strategy is the decision-making center, which decides "what to do"; Control activity is to execute the arm and turn the decision into action; Information communication and supervision improvement is a neural feedback system to ensure that the system can perceive its own state; PDCA management closed loop is the driving engine, which promotes the continuous evolution of the system. The six elements support and embed each other to form an organic whole.

5. Multi-Agent Risk Management Responsibility System Design

Under the integrated risk management framework, it is the key link to turn the theoretical framework into operational governance practice to clarify the risk management responsibilities of all relevant subjects. Based on the thought of "three lines of defense" in internal control theory and the characteristics of campus organization, this study designs the following multi-agent risk management responsibility system.

5.1 The Basic Principles of the Design of the Power and Responsibility System

5.1.1 The principle of risk responsibility and power equivalence

The subject responsible for risk management should be endowed with corresponding decision-making power and resource allocation power to ensure the matching of power and responsibility. Equivalence of power and responsibility is the basic principle of organizational design, and it is also the premise to ensure the effective operation of risk management system.

5.1.2 The principle of hierarchical responsibility and coordination

Subjects at different levels bear different risk management responsibilities, and at the same time establish an effective coordination mechanism to form an overall synergy. Hierarchical responsibility means reasonable division according to the functional orientation and resource capacity of each subject; Collaboration means forming an organic whole through information sharing and process convergence.

5.1.3 The principle of incentive compatibility

The design of power and responsibility should make each subject realize the overall risk management goal naturally while pursuing their own goals and avoid conflicts of interest. Incentive compatibility requires that risk management performance be included in the assessment system of each subject, so that risk prevention and control become the "responsibility" of each subject.

5.2 Multi-Subject Risk Management Role Positioning

Based on the difference of risk management functions, the relevant subjects on campus can be divided into three levels: risk owner level, risk controller level and risk supervisor level.

5.2.1 Risk owner layer, that is, the front-line subject directly facing risks

The subject at this level directly faces the fraud risk and is the first bearer and the first line of defense of the risk. Mainly includes:

Individual students: As the ultimate risk taker, they are responsible for improving their risk awareness and identification ability, observing safety regulations and reporting suspicious situations in time. Students' risk awareness and behavior habits are the first pass of risk prevention and control.

Peer organization (class, dormitory, community): responsible for daily mutual reminding and

information transmission, and giving play to the supervision and support role of "people around". Peer organizations have the advantages of being close to students and responding quickly, and are the "nerve endings" of risk perception.

Counselor: As a group of teachers who have the closest contact with students, they are responsible for students' daily safety education, abnormal behavior observation and preliminary intervention. Counselors have both teacher status and first-line experience in student work, and are the bridge connecting students and management departments.

5.2.2 Risk controller layer, that is, functional departments that provide professional support

The main body at this level undertakes the professional functions of risk management and provides support and guidance for risk owners. Mainly includes:

Student affairs department: take the lead in formulating the school's anti-fraud work plan and policy, organize anti-fraud publicity and education activities, and coordinate the risk disposal related to student affairs. The academic department is the overall organization of student affairs management, and plays a coordinating role in anti-fraud work.

Security department: responsible for campus security monitoring, fraud clues verification, and docking linkage with local public security departments. The security department has the professional function of security and is the command center of emergency response.

Information Technology Center: responsible for the construction and operation of technical early warning system and providing technical support for network security. The technical support of the information technology center provides the infrastructure for risk identification and monitoring.

Faculty: Implement the anti-fraud requirements of the school, carry out targeted education in combination with the characteristics of disciplines and majors, and pay attention to high-risk students in the college. As a secondary unit, the department undertakes the main responsibility of risk management of the unit and cooperates with the overall deployment of the school.

5.2.3 Risk supervisor layer, that is, independent evaluation and audit institutions

The main body at this level is independent of the risk management implementation system and is responsible for supervising and evaluating the effectiveness of risk management activities. Mainly includes:

School-level audit/supervision department: independently evaluate the operation efficiency, audit resource allocation and use efficiency of the school-wide anti-fraud risk management system. Audit department does not participate in daily management and can maintain an objective and neutral supervision perspective.

Risk Management Committee (inter-departmental): coordinating the school's risk management, reviewing major risk response plans, and supervising the performance of each department. The Risk Management Committee is composed of many departments, and can examine the risk management work from a global perspective. Based on the above role positioning, this study designed a multi-agent risk management responsibility system (see Table 2).

Table 2. Multi-agent Risk Management Responsibility System

level	main body	Core responsibilities	Power-responsibility boundary
Risk owner	Individual student	Improve risk awareness and identification ability, abide by safety regulations, and report suspicious situations in time.	Conduct self-discipline and information reporting, and do not undertake professional risk management and control responsibilities.
	Peer organization	Remind each other and transmit information daily, and play the supervisory role of "people around"	Informal support network, no coercive power
	Counselor	Daily safety education, abnormal behavior observation and preliminary intervention	Discovery and preliminary disposal, referral of professional problems
Risk controller	Student affairs	Take the lead in formulating the school's anti-fraud work plan and	Policy formulation and overall coordination, student affairs disposal

	department	organizing education activities.	
	Security department	Campus security monitoring, fraud-related clue verification, and public security docking linkage	Safety professional functions, emergency response command
	Information technology center	Technical early warning system construction and operation and maintenance, network security technical support	Technical support, do not assume the responsibility of education management.
	department	Implement school requirements, carry out targeted education, and pay attention to high-risk students.	The main responsibility of the unit, with the overall deployment of the school.
Risk supervisor	School-level audit/supervision department	Independently evaluate the effectiveness of risk management system and audit the efficiency of resource use.	Independent supervision, not involved in daily management.
	Risk management Committee	Coordinate the risk management of the whole school and consider major plans.	Inter-departmental deliberation and coordination, without specific implementation responsibilities.

The innovation of this power and responsibility system lies in transforming the original general concept of "collaborative governance" into specific role orientation and power and responsibility boundaries, so that each subject can clearly define "who am I", "what should I do" and "where is the boundary". At the same time, the design of three-tier architecture ensures a complete closed loop of risk management: the risk owner is responsible for daily perception and initial disposal, the risk controller provides professional support and system intervention, and the risk supervisor independently evaluates and promotes improvement. The three have their own functions and cooperate with each other to form an organic whole.

6. The Realization Path of Risk Management Closed Loop

After constructing an integrated risk management framework and clarifying the power and responsibility system, the key is to establish an operating mechanism that drives the system to continuously improve itself. Based on PDCA cycle theory, this study designs a management closed-loop realization path with four links.

6.1 The Planning Process

The core task of the planning link is to set clear governance objectives and formulate scientific risk response strategies and implementation plans based on the results of risk identification and evaluation. In the practice of campus anti-fraud, this link should be embodied as the following work:

6.1.1 Preparation of annual anti-fraud work plan

At the beginning of each year, led by the student affairs department, together with the security department and the information technology center, based on the data of campus fraud cases in the previous year (including the type of cases, the amount involved, the distribution of victims, etc.) and the risk assessment results, the Annual Campus Anti-fraud Work Plan is compiled. The contents of the plan need to be clear: the annual governance objectives (such as reducing the incidence rate of rebate cases by 10% and increasing the awareness rate of students' anti-fraud knowledge to 90%), key tasks (such as launching the "anti-fraud publicity month" in the spring semester and organizing the "first anti-fraud lesson for freshmen" in the autumn semester), resource allocation schemes (such as special funds for anti-fraud publicity and the budget for upgrading the early warning system), division of responsibilities (specific responsibilities of each functional department) and time. After the plan is completed, it shall be submitted to the school safety work leading group for deliberation and implementation.

6.1.2 Dynamic tracking of fraud techniques and optimization of coping strategies

Based on the data of the evolution trend of fraud techniques provided by the anti-fraud center of public security organs, a dynamic tracking mechanism of campus fraud techniques is established. Aiming at the high-incidence types (such as single rebate, pretending to be customer service, and false shopping), the combination

strategy of "evasion+slow release" is adopted: on the one hand, the blocking of fraudulent apps and phishing websites is strengthened through technical means, and information dissemination is blocked from the source; On the other hand, carry out accurate publicity and education for susceptible people. For new fraud methods (such as AI face-changing fraud, false investment and wealth management), it is necessary to complete the judgment and formulate the response plan within 48 hours, and adjust the focus of publicity and education in time.

6.2 Implementation Link

The core task of the implementation link is to carry out control activities in a hierarchical and classified manner according to the established plan. Combined with the actual anti-fraud work on campus, control activities can be divided into the following three categories:

6.2.1 Preventive control: build the source defense line

The goal of preventive control is to block risks before they occur. Specific measures include: First, the anti-fraud education should be included in the compulsory course for freshmen, and the mode of "online course+offline lecture+knowledge test" should be adopted to ensure the full coverage of freshmen; The second is to establish a normalized publicity and push mechanism, relying on campus WeChat WeChat official account, class group, dormitory electronic screen and other channels to push the latest fraud cases and prevention knowledge every week, focusing on high-risk types such as brushing rebates and impersonating acquaintances; Third, based on students' consumption behavior data (such as frequently checking part-time job information, abnormal game recharge, etc.), identify high-risk student groups, and counselors will carry out "one-on-one" accurate reminders, and if necessary, interview parents for joint intervention. The key of preventive control lies in "accurate identification" and "normal maintenance".

6.2.2 Monitoring control: strengthening early warning

The goal of supervisory control is to find out the risks that are happening in time. Specific measures include: First, relying on the "National Anti-Fraud Center" APP of the public security organs and the campus anti-fraud early warning system, real-time monitoring of abnormal login, suspicious links and fraud-related information, and pushing early warning information immediately when abnormalities are found; The second is to establish a daily observation mechanism for counselors to observe students' abnormal emotions and behaviors (such as sudden large loans and frequent suspicious phone calls) through heart-to-heart talks and visits to dormitories, and report any abnormalities in time; The third is to establish information reporting channels for class safety officers and dormitory leaders, and require the backbone of students to report suspicious situations to counselors or security offices within one hour. The key of monitoring control lies in "timely perception" and "quick linkage".

6.2.3 Corrective control: Deal with it afterwards

The goal of corrective control is to reduce the losses caused by risks. Specific measures include: first, establish a rapid dissuasion mechanism. After receiving the early warning, counselors and security personnel need to get in touch with students within 30 minutes, and if necessary, contact parents to jointly discourage the ongoing transfer behavior; The second is to establish a linkage mechanism with public security organs and financial institutions, and immediately start the fund stop payment procedure for the cases that have been sent, and strive for the "golden 30 minutes" stop payment time; The third is to establish a psychological crisis intervention mechanism for deceived students, and the mental health education center will intervene within 24 hours to carry out psychological counseling and prevent secondary injuries. The key of corrective control lies in "quick response" and "professional disposal".

The three types of control activities form a progressive relationship: preventive control strives to "not happen", monitoring control strives to "find early" and corrective control strives to "reduce losses". The three are connected with each other to form a complete control chain.

6.3 Inspection Link

The core task of the inspection link is to objectively evaluate the effectiveness of risk management activities and identify existing problems and improvement space.

6.3.1 Design of performance evaluation index system

In order to objectively measure the effect of campus anti-fraud work, this study designed a

performance evaluation index system including three dimensions: outcome index, process index and perception index (see Table 3).

Table 3. Risk Management Performance Evaluation Index System

dimension	evaluating indicator	data source
Outcome index	Incidence rate of fraud cases (from/thousand people)	Security department case statistics
	The amount involved in fraud cases	
	Number of students cheated	
Process index	Coverage rate of anti-fraud publicity and education	Activity record of the department of learning and engineering
	Accuracy of early warning information	Statistics of information technology center
	Average time of rapid response	Security department disposal record
	Discourage success rate	
Perceptual index	Awareness rate of students' anti-fraud knowledge	questionnaire survey
	Students' satisfaction with anti-fraud work	
	Security evaluation	

Results indicators directly reflect the effectiveness of governance, including the incidence rate of fraud cases, the amount involved, the number of deceived people, etc. Process indicators measure the quality of work input and implementation, including the coverage of anti-fraud publicity and education, the accuracy of early warning information, the average time of rapid response, the success rate of dissuasion, etc. Perceptual indicators reflect the subjective experience of teachers and students, including students' awareness rate of anti-fraud knowledge, satisfaction with anti-fraud work, and evaluation of campus security, which can be obtained through annual questionnaires.

6.3.2 Monitoring and auditing mechanism

Monitoring audit is an important means to ensure the performance evaluation. Specifically, it includes: first, monthly monitoring, in which the student affairs department summarizes the data of various indicators on a monthly basis, forms the Monthly Anti-fraud work briefing, and submits it to the members of the school safety work leading group to find abnormal fluctuations in time; The second is quarterly evaluation. The school safety work leading group holds special meetings every quarter to analyze the effectiveness of the work, study outstanding problems, and deploy the next stage of key work; The third is the annual audit. The school-level audit department independently audits the use of anti-fraud special funds, the implementation of the system, and the performance of various departments every year, issues audit reports, and puts forward suggestions for improvement, which are included in the annual assessment of the department.

6.4 Processing Link: Continuous Improvement Mechanism Based on Problem Orientation

The core task of the treatment link is to turn the problems found in the inspection into improvement actions and promote the continuous optimization of the governance system.

6.4.1 Problem analysis and rectification

In view of the problems found in monthly monitoring, quarterly evaluation and annual audit, organize thematic analysis and trace the root causes of the problems. Problems should be analyzed by tools such as "5Why Analysis" to dig deep into the institutional and institutional roots. For example, if it is found that certain types of fraud cases continue to be high, it is necessary to ask: Is publicity and education not in place? Is the early warning system invalid? Or is the response mechanism lagging behind? On this basis, formulate rectification measures, clarify the responsible department and completion time limit, establish rectification ledger, and track the implementation of rectification. After the rectification is completed, we should organize a "look back" to ensure that the problem is truly solved.

6.4.2 Experience summary and promotion

Summarize the successful dissuasion cases and refine the replicable experiences and practices. For example, in a successful dissuasion, how did the counselor find the abnormality of the students in time? Which form of student

participation is the highest in a publicity and education activity? These experiences should be promoted through inter-school communication and case compilation, so that the point experience can be transformed into the surface ability.

6.4.3 System optimization and iteration

According to the problem rectification and experience summary, timely revise and improve the relevant system norms. For example, if there is a delay in the transmission of early warning information, the information flow process should be optimized; If it is found that it is difficult to identify a certain type of fraud, the early warning model algorithm should be updated. At the same time, according to the results of performance evaluation, dynamically adjust the allocation of resources to ensure investment in key areas. System optimization should become a normal working mechanism.

6.4.4 Enter the next cycle

Incorporate improvement measures into the next year's anti-fraud work plan and start a new round of PDCA cycle. Through the repeated cycle, the spiral rise of the governance system is realized, and the risk identification is more accurate, the response is more effective, and the improvement is more timely. The above four links constitute a complete risk management closed loop (as shown in Figure 2).

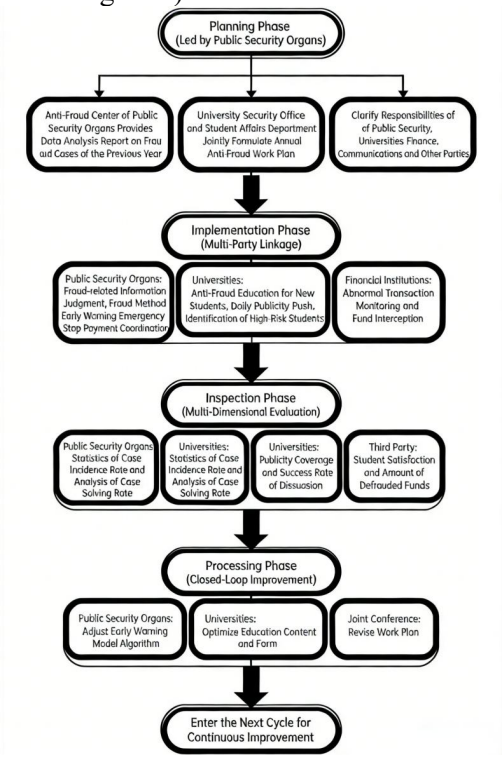

Figure 2. Path Diagram of Risk Management Closed-Loop Implementation

7. Conclusion and Prospect

From the perspective of integrated governance theory, this study aims at the basic pattern of "rich tools but lack of framework" in the current research on telecommunication network fraud governance of college students, and constructs an integrated governance framework for telecommunication network fraud for college students. The main contributions of the research are embodied in three aspects: First, an integrated theoretical framework is constructed, which includes five core elements: governance environment and organizational foundation, risk identification and evaluation, risk coping strategies, control activities and implementation mechanism, information communication and supervision improvement, and the scattered elements such as judicial deterrence, technical early warning and psychological intervention are brought into a unified management logic. Secondly, a multi-subject power and responsibility system based on the three-tier structure of "risk owner-risk controller-risk supervisor" is designed, which transforms the general concept of "collaborative governance" into a specific role orientation and power and responsibility boundary. Thirdly, it explores the realization path of closed-loop management covering four links: planning, implementation, inspection and handling, and constructs a performance evaluation index system including three dimensions: outcome index, process index and perception index, which makes the governance system change from static system design to dynamic operation mechanism.

This study provides a systematic anti-fraud governance scheme for university administrators, clarifies the division of responsibilities for functional departments such as students, security and information center, and provides a reference tool for higher authorities to evaluate the effectiveness of anti-fraud work. However, this study is mainly based on theoretical construction and logical deduction, and has not been tested by empirical analysis. Future research can test the feasibility and effectiveness of the framework through case studies, verify the scientificity of the performance evaluation index system through quantitative research, analyze the adaptation needs of different types of universities through comparative research, and observe the adjustment mechanism of the framework to adapt to new risks through dynamic tracking

research, so as to continuously improve and optimize the campus anti-fraud governance system.

References

[1] Wang Jian, Liu Yang. Compilation and Verification of College Students' Telecommunication Network Fraud Susceptibility Scale. Exploring Psychology, 2023, 43(2): 145153.

[2] Zhang Wei, Wang Xiaofeng. Research on telecom fraud early warning model based on big data. Computer Science, 2023, 50(5): 234241.

[3] COSO. Enterprise Risk Management-Integrated Framework. Fang Hongxing, Wang Hong, translated. Dalian: Dongbei University of Finance and Economics Press, 2021.

[4] Zhou Tao, Wu Fan. Research on the Application of PDCA Cycle in College Safety Management. College Education Management, 2023, 17(3): 8996.

[5] Zheng Jie, LAM Raymond. Research on the construction of college students' safety risk prevention and control system. Ideological and theoretical education guide, 2024, 32(2): 112118.

[6] Huang Wei, Xu Jing. Research on the evolution of telecom fraud based on the matter map. Journal of the china society for scientific and technical information, 2023, 42(6): 678687.

[7] Xu Ning, Gao Yuan. Research on the characteristics of college students' network behavior and risk prevention education. Youth Research, 2023, 42(4): 6775.

[8] Lin Qing, Ye Xin. Research on emergency management mechanism of colleges and universities. China Administration, 2024, 40(2): 123130.

[9] Wang Dan, Li Na. An empirical study on the effect evaluation of college students' safety education. Education Development Research, 2023, 43(11): 7885.

[10] Yang Bo, Sun Hao. The governance dilemma and countermeasures of telecommunication network fraud. Journal of Chinese People's Public Security University (Social Science Edition), 2024, 40(1): 4554.

