MINDWELL SCIENCE PRESS SDN. BHD.

Journal of Systemic Risk
Volume 1, Issue 2

RESEARCH ARTICLE

Research on the Prevention of, and Response Strategies for, ICT Supply Chain Security Risks in Telecommunications Operating Enterprises

Jiashuo Wang[1], Jianning Cheng[1], Min Zhu[2], Tiancheng Zhou[2], Yongjun Hu[3,*]

[1] *China Mobile Group Shaanxi Co., Ltd., Xi'an 710076, Shaanxi, China*
[2] *Huaxin Consulting and Design Institute Co., Ltd., Hangzhou 310051, Zhejiang, China*
[3] *Supply Chain Management Centre, China Mobile Communications Group Co., Ltd., Beijing 100033, China*

Corresponding author: Yongjun Hu, E-mail: huyongjun@chinamobile.com

Published: 28 August 2026

Abstract

With the rapid development of global informatisation, every sector of the economy has become increasingly dependent on information and communication technology (ICT) products and services, and concern for the security and stability of the ICT supply chain has risen continuously. In recent years, shifts in the global situation, trade disputes among major powers and the outbreak of the COVID-19 pandemic have had far-reaching effects on the global political and economic landscape. The ICT supply chain risks and security problems thereby induced — chip shortages and cut-offs, rises in raw material prices, "chokepoint" restrictions and power rationing and production limits — have become increasingly apparent. In this context, telecommunications operating enterprises urgently need to respond actively to the present ICT supply chain security situation and to the risks arising from it, to explore ways of strengthening their own supply chain security capacity, and to formulate more scientific and effective risk response strategies. Taking the present ICT supply chain security situation and risks as its subject, and grounding itself in the management realities and supply chain management characteristics of telecommunications operating enterprises, this article sets out the research approach and methods for risk response strategy, and proposes strategies for responding to and preventing supply chain security risks in two respects: building an end-to-end risk management system, and formulating scientific and efficient risk prevention measures. The aim is to raise supply chain management and operating capacity in an all-round way, safeguard the security and stability of the supply chain, and support the transformation and development of the enterprise's business.

Keywords: telecommunications operating enterprises; ICT supply chain; risk prevention; response strategies

* Corresponding author.

1 Introduction

The external environment in today's world is turbulent. With a new phase in the global response to the pandemic, an increasingly complex international political and economic situation, and the "rise" of trade protectionism and unilateralism, global industrial and supply chains face reconstruction. Forecasts by the relevant institutions hold that chips will remain in short supply for some time, that commodity prices will run high, that the trade war and the effects of the pandemic will be difficult to eliminate in the short term, that the contradiction between supply and demand will be difficult to resolve, and that the risk of price increases and supply delays therefore remains considerable. Trade disputes continue in the contest among major powers; some countries have gone so far as to use government power directly to compel the leading enterprises in the semiconductor chain to supply business secrets such as production capacity and core customer information, and have used statutory provisions to impose "chokepoint" restrictions on access to key technologies. Under such a severe external situation, and in order to safeguard the sustained and stable development of the economy effectively, ICT supply chain security has become a problem that must be confronted. Party and state policy has been issued repeatedly, explicitly requiring that the security and stability of both the industrial chain and the supply chain be ensured and that capacity for self-reliance and control be strengthened. In *Several Major Issues in the National Medium- and Long-Term Economic and Social Development Strategy*, General Secretary Xi Jinping stated that it is necessary to "optimise and stabilise industrial and supply chains"; the outline of the Fourteenth Five-Year Plan for National Economic and Social Development proposes to "establish a global supply chain risk early-warning system for important resources and products".

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Telecommunications operating enterprises have responded positively to the national call, advancing the construction of 5G, data centres and other infrastructure and the development of ICT business. Since the Fourteenth Five-Year Plan period began, these enterprises have extended their business development from communications into the broader space of information services; their markets have expanded from a focus on mobile to all five markets — individual, household, government and enterprise, small and medium-sized enterprises, and computing-network; and their development model has been upgraded from one driven by resource factors to one driven by innovation. Enterprises have explicitly proposed that, building on the original plan to "comprehensively implement the '5G+' programme and bring information services into every industry and to the general public", this be enriched and extended into a new information service system of "connectivity + computing power + capability" based on 5G plus a computing power network plus a smart middle platform. Under the CHBN market development strategy, demand for ICT equipment and software continues to rise, imposing higher requirements on the security and stability of the supply chain. Yet in the face of rising procurement costs, lengthening supply cycles and a markedly increased risk of supply cut-off in the ICT supply chain, the contradiction between high business demand and weak business support capacity has become prominent, and perfecting ICT supply chain security management has become an important task for telecommunications operating enterprises.

In summary, ICT supply chain security has become a major difficulty facing the development of telecommunications operating enterprises. It is necessary, in the light of enterprises' actual business conditions and their internal and external resources, to propose measures for responding to and preventing supply chain security problems, to enhance enterprises' supply chain risk and security management capacity, to respond to current risks promptly and effectively, to strengthen the anticipation and prevention of risk, to raise supply chain management and operating capacity in an all-round way, to safeguard the security and stability of the supply chain, and to support high-quality development. The main content of this article is as follows. Against the current macro-environment of the industry, and at international and domestic level, and against enterprises' internal and external management requirements, it focuses on the ICT supply chain security risks induced by changes in the security situation — global shifts, trade disputes among major powers, epidemic prevention and control — namely chip shortages and cut-offs, rises in raw material prices, "chokepoint" restrictions, and power rationing and production limits. Covering the whole ICT supply chain process, and using internal and external personnel surveys, basic data analysis and industry report research, and taking account of the business characteristics of telecommunications enterprises — high product continuity, a position downstream in the supply chain, and centralised management — it proposes strategies for each link of the whole ICT supply chain process. It sets out strategies for responding to and preventing supply chain security risks in two major respects: building an end-to-end risk management system, and formulating scientific and efficient risk prevention measures. The aim is to clear the "blockages" and connect the "breaks", and to enhance the company's capacity for supply chain risk and supply chain security management.

2 Characteristics of the ICT Supply Chain of Telecommunications Operating Enterprises and Analysis of Security Risks

2.1 ICT business products and supply chain characteristics of telecommunications operating enterprises

As growth in the traditional communications market slows, ICT business has gradually become an important direction of transformation for telecommunications operating enterprises. Their ICT business is directed mainly at the individualised needs of group customers, integrating and developing as necessary network communication services, information content applications and information technology products to form a "one-stop solution" of "communication services (CT)" plus "informatisation applications (IT)", providing customers with services that are more service-oriented, integrated, professional and systematic — an organic combination of traditional communications, internet applications and IT applications. At the product level, taking the ICT business segments of China's three major operators together, the ICT products and services of telecommunications operating enterprises comprise four areas: information content applications (Information), communication network applications (Communication), information technology products (Technology), and other information services.

At the supply chain level, the ICT supply chain is a network-chain structure formed by many upstream and downstream organisations connected to one another. Compared with a traditional supply chain, the ICT supply chain covers more links and a wider scope, and therefore carries more security risks; it is characterised by global distribution, a whole-life-cycle character, complexity of products and services, and diversity of suppliers. In the ICT supply chain of a telecommunications operating enterprise, the enterprise occupies a mid- and downstream position in the ICT industrial chain. Its upstream consists mainly of communications equipment vendors, hardware suppliers and software suppliers, with the core suppliers at the very top being semiconductor chip manufacturers; its downstream consists of final consumers and users.

As regards supply chain management objectives, the supply chain management of telecommunications operating enterprises currently focuses on three areas — demand management, procurement management and logistics management

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

— and in the course of continuous reform and development has been characterised by a search for balance between raising supply chain efficiency and building resilience. Supply chain management pursues intensive, standardised and informatised development, establishing efficient, intensive and standardised systems in procurement and logistics management and emphasising optimal efficiency. China Mobile, for example, has built a two-tier procurement management mechanism of "horizontal centralisation, vertical concentration" covering every unit of the group, and has established a unified and complete institutional system; through intensive management — demand aggregation, coordination of demand and procurement, product standardisation and logistics integration — it has given full play to economies of scale, with marked results in cost reduction and efficiency improvement. But an intensive management model measured by cost and quality often gives rise to greater management difficulty and lower sensitivity to changes in demand, which to some extent affects the stability of the supply chain.

2.2 The ICT security risk situation and management status of telecommunications operating enterprises

The risk points and areas of concern in the current ICT supply chain security management of telecommunications operating enterprises are concentrated mainly in the field of information technology products, involving chiefly hardware equipment such as data processing equipment, data storage equipment, servers, routers, switches, and various information and communication terminals, and software products such as commercial standardised software. As regards the situation faced: chips will remain in short supply for some time, commodity prices will run high, the trade war and the effects of the pandemic will be difficult to eliminate in the short term, the contradiction between supply and demand will be difficult to resolve, and the risk of price increases and supply delays therefore remains considerable. Trade disputes continue in the contest among major powers; some countries have gone so far as to use government power directly to compel leading enterprises in the semiconductor chain to supply business secrets such as production capacity and core customer information, and to force through statutory provisions restricting access to key technologies — and such phenomena are becoming more rather than less frequent.

Against this background, and in the light of the industry characteristics of telecommunications operating enterprises and the characteristics of their product supply chains, the impact of procurement supply chain security risks is manifested mainly in the following four respects.

(1) Reduced procurement volumes. Black swan events such as the pandemic, China–US trade friction and the Russia–Ukraine conflict have dealt a severe blow to the production and supply of semiconductors and integrated circuits, affecting communications equipment, network equipment, servers and other products alike, and have had a major impact on the normal conduct of procurement business.

(2) Increased procurement costs. Rising raw material prices, shutdowns and production stoppages have pushed up upstream production costs and reduced production efficiency, while downstream demand and safety stocks have increased. In an overall environment of demand exceeding supply, procurement prices for ICT products have continued to climb, greatly increasing procurement costs.

(3) Lengthened transport cycles. To prevent and control COVID-19, traffic control measures were adopted at home and abroad, regions under key epidemic prevention and control admitted and released nothing, cross-border transport became still more difficult, and the whole transport network was riddled with "blockages", with a considerable impact on the timeliness and cost of logistics and transport.

(4) Weak business support. The complex and severe external environment has had a negative effect on procurement business and logistics warehousing in many respects, and the risk of dependence on external demand has grown. The supply chain, the "great artery" of enterprise development, has been unable to provide the necessary inputs in good time, so that existing ICT assets have been idle.

Under severe changes in the external security situation and their risk impacts, supply chain security management has risen to the level of corporate strategy, and supply chain management must place further emphasis on building resilience — that is, on enhancing the supply chain's capacity to respond to risk through a series of measures such as digital and intelligent empowerment and ecosystem collaboration. China Mobile, for example, has mapped the chokepoints in key areas such as 5G, transmission, IT and basic software, and through investment leverage, procurement strategy guidance, diversified supply and inventory redundancy has driven the industrial chain to tackle core technologies, so as to respond further to the risk of supply interruption. But building supply chain resilience with the aim of enhancing stability requires considerable cost input and appropriate redundancy, and this to some extent sacrifices supply chain efficiency.

The supply chain management of telecommunications operating enterprises must therefore seek a balance between supply chain efficiency and resilience, and must strengthen research on response strategies for ICT supply chain security risks, so as further to withstand supply chain risk and safeguard the healthy and effective development of the company's business.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

3 Approach and Methods for Research on ICT Supply Chain Risk Response Strategies

The overall research approach and methods for ICT supply chain risk response strategy fall into four steps. The first step is to collect external materials, in order to understand the current domestic and international market environment and the present state of security problems, to understand current policy and the latest research findings in the field, and to study the theoretical models commonly used in risk management, so as to provide theoretical and data support for the research that follows. The second step is to survey the internal situation of the enterprise, establishing its strategic positioning, its current procurement situation, the basic circumstances of its suppliers, the extent to which demand is met, its business support capacity, and its supply chain security management measures. The third step, after internal and external materials have been comprehensively reviewed and integrated, is to discuss and select the most appropriate research model, so as to identify the key problems precisely and to determine their impact on supply chain security. The fourth step is to give the analytical results and the response strategies, so as to achieve preventive and responsive management of supply chain risk.

3.1 Collection of external materials

Key external materials are structured, and big-data review and integration are carried out, so as to achieve a full-data description of key external events and to provide data support for the research. Internet sources are searched (as shown in Table 1) to collect relevant international events, including the impact of repeated waves of COVID-19 on the supply chain, the impact of the Russia–Ukraine conflict, and the impact of the associated earthquakes and other natural disasters on raw material supply. Physical books are consulted to screen the available models — situational models, macro-environment models, neural network models and others — and the theoretical model selected for the research is determined in the light of actual conditions. Third-party materials and databases are consulted to collect policy and standards documents such as the *Information Security Technology — ICT Supply Chain Security Risk Management Guide*, the *TAF Association Standard — Network Product Supply Chain Security Requirements* and the *5G Supply Chain Security Assessment Guide*, and to consult reports and research literature such as the *Research Report on New Risks to ICT Supply Chain Security*, *Analysis of ICT Supply Chain Security Risks and Typical Events*, and *The Russia–Ukraine Conflict Disturbs the Semiconductor Supply Chain: Longer Chip Lead Times and Price Rises Introduce Uncertainty*. Drawing on the theoretical findings of existing scholars, and combining them with information on external events, the external materials are reviewed using the relevant theoretical models.

Table 1 Source channels for materials

Channel	Examples
Official websites	Ministry of Commerce of China; Ministry of Foreign Affairs of China; United Nations Conference on Trade and Development
WeChat official accounts	China Institutes of Contemporary International Relations; China Institute of International Studies; Chinese Academy of International Trade and Economic Cooperation, Ministry of Commerce; Institute of World Economics and Politics, Chinese Academy of Social Sciences; Institute of International Relations, Tsinghua University
News portals	People's Daily Online; Xinhua Net; China Going Global Network; Xiakedao; Global Times; The Paper
Research institutions / securities firms	iResearch Consulting; Deloitte Consulting; Ernst & Young Consulting

3.2 Analysis of the internal situation

The analysis of the internal situation is based chiefly on survey work. The survey work is divided, according to its sequence in time, into four stages: preparation, survey, consolidation of requirements, and output of the survey report. The specific process is shown in Figure 1.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

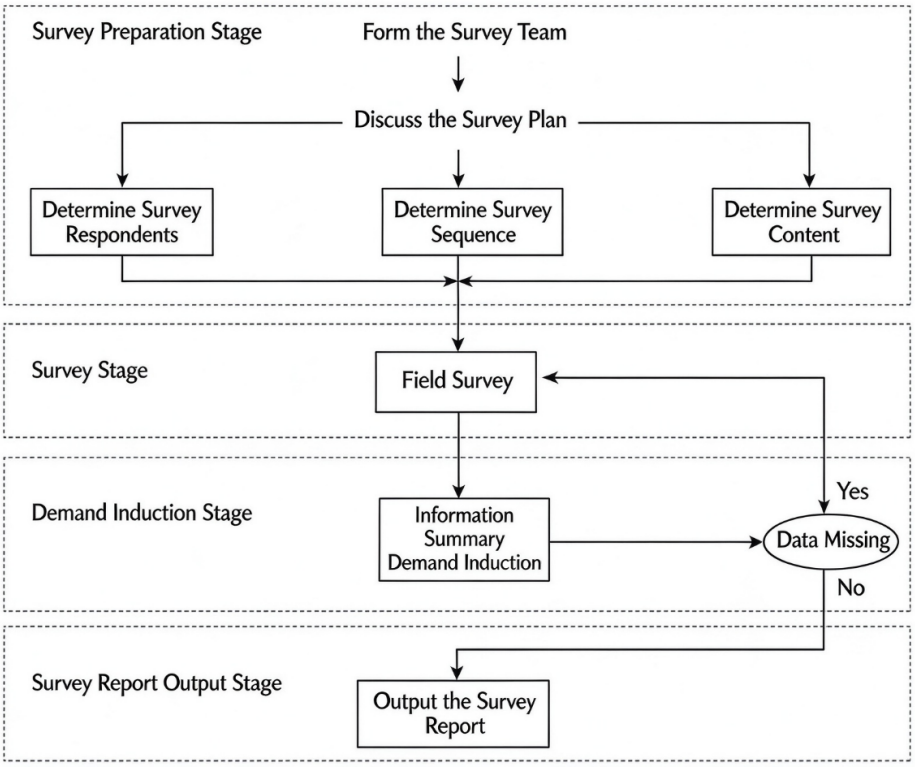


Figure 1 Process of the survey scheme

Following the sequence described above, the project managers and related business staff of the company's internal procurement department were surveyed on matters such as the timeliness of supplier deliveries and changes in procurement costs; the leaders of the demand departments were surveyed on the extent to which business requirements were met; the finance department was consulted on the fund management process for ICT projects and on business-finance statistical statements; and the leaders of the strategic development department were consulted on the company's future strategic planning for ICT business. By consolidating, organising and analysing the materials obtained at the survey stage, the present state of the operating enterprise's network communication business, information technology business and other ICT support services was reviewed; the characteristics of key ICT products — hardware such as switches, routers and load balancers, and software such as databases — were established; and the circumstances of the products and their suppliers were analysed. Finally, in the light of the enterprise's actual situation, a comprehensive analysis was made of its strategic positioning, its current procurement situation, the extent to which demand is met, its business support capacity and its supply chain security management measures, laying the foundation for assessing security risks.

3.3 Supply chain security risk assessment

The focus of security risk assessment is to identify the critical problems and to assess their impact. The risk probability–impact matrix model is used to carry out risk rating, concentrating on the risks of greatest concern and supporting graded, classified and precisely targeted measures.

The risk probability–impact matrix is used mainly for qualitative risk analysis in project risk management. It assesses the risks in a project along two dimensions — the probability that the risk will occur, and the degree of impact the risk would have on objectives — dividing both the probability of occurrence and the impact on the project into five grades: rather low, low, medium, high and very high. Impact is plotted on the horizontal axis and probability on the vertical axis, giving a 5 × 5 matrix by which events are rated. Risk rating helps guide risk response: a risk in the high-risk region must be met with priority and active decision-making measures; one in the medium-risk region may be placed on a watch list or covered by a contingency reserve; and one in the low-risk region may be dealt with when it occurs.

3.4 Analysis of recommended strategies

On the basis of the review of external events affecting security and of the enterprise's internal circumstances, and for the risk events of different grades identified in the preceding step, strategies are proposed with reference to the research methods of earlier scholars and to commonly used research models.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

For the security risk events of different grades and categories arrived at by the assessment, the six-W analytical method (what, why, where, when, who, how) is used to pose questions from six angles — the cause of the risk, the object affected by the risk, the place where the risk occurs, the time at which the risk occurs, the personnel involved, and the method of response. The impact of risk events on supply chain security is divided into four broad categories: impact on procurement volume, impact on procurement cycle, impact on procurement cost, and impact on business support. Strategies are then proposed in two respects: building an end-to-end risk management system, and formulating more efficient risk prevention measures.

Finally, the Deming cycle is used to strengthen the verification and updating of the risk register, the risk probability–impact matrix and the risk response strategies. The Deming cycle divides quality management work into four stages: Plan, Do, Check and Act. In management activity, work is first planned according to the relevant standards, then implemented according to process and system, the results of implementation are checked against the plan, and finally deviations are dealt with — successful results being incorporated into the standards and unsuccessful ones left for the next cycle to resolve. Specifically, for the measures drawn up by the six-W method, the measures must be strictly implemented and their results verified, and effective measures must have their standards consolidated. Problems unresolved in a given Deming cycle enter the next, going round and round and rising spirally, until the prevention and management of supply chain risk is finally achieved.

4 Strategies for Responding to ICT Supply Chain Security Risks in Operating Enterprises

4.1 Building an end-to-end risk management system

4.1.1 Perfecting the organisational structure of supply chain security management

(1) Establishing a department-level supply chain security management group. Taking practical account of the problems encountered throughout the whole process of material procurement and supply, warehousing and logistics, and operation, maintenance and decommissioning, a department-level supply chain security management group is established, responsible for the day-to-day monitoring and management of supply chain security risks and for reporting major risks in good time. Its duties are as follows.

(i) To be responsible for formulating, executing, evaluating and perfecting the department-level supply chain risk management system. (ii) To guide departments in collecting and organising supply chain risk information, to be responsible for consolidating that information, and to carry out the publication of monitoring, analysis and results data on comprehensive risk early-warning information in each domain. (iii) To provide supply chain risk management strategies and solutions for risks below the moderate level, and to be responsible for organising their implementation and for day-to-day monitoring of those risks. (iv) To evaluate the effectiveness of the management of risks below the moderate level and to propose improved risk response measures where these are deficient. (v) To guide and supervise subordinate bodies in carrying out supply chain risk management work. (vi) To be responsible for monitoring and reporting major risks.

(2) Establishing an enterprise-level joint supply chain security management body. An organisational structure led by the general manager and linking the supply chain department, the finance department, the demand departments and other departments is built, so as comprehensively to strengthen supply chain security risk management, to establish a unified and efficient risk management organisational system at company level, and to organise and coordinate day-to-day risk management work. Its duties are as follows.

(i) To establish and perfect a working mechanism for coordinating supply chain risk management among the business departments, and to organise the drafting of detailed rules for the division of risk management work between the risk management division and the relevant business divisions, together with methods for contact and cooperation. (ii) To approve the company-level response plans for major supply chain risks and the annual risk management work report. (iii) To keep abreast of the major supply chain risks facing each department of the company, to understand the current state of risk management, and to issue decisions that effectively control risk. (iv) To determine the company-level overall objectives and management policy for supply chain risk management, and to approve management strategies and management solutions for major risks. (v) To approve the judgement mechanisms, judgement criteria and management measures for important decisions, major events and key business processes relating to the company's supply chain risk, and to correct and deal with conduct that violates the provisions on risk management. (vi) To supervise and guide the development of supply chain security risk management work in each department of the company. (vii) To be responsible for other major matters relating to supply chain security risk management.

(3) Establishing a supply chain security expert think tank. Relying on the "chain leader" position that telecommunications operating enterprises hold within the industry, members are invited from enterprises upstream and downstream in the supply chain and industrial chain, technology providers, university professors, industry associations and research institutes.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Focusing on manufacturing and logistics, a supply chain security management expert pool is built to provide support chiefly in judging global supply chain security trends, risk management, planning for informatisation support, establishing mechanisms for information exchange and sharing, formulating standards and norms, and training supply chain security management personnel. While providing support for the enterprise's supply chain security management, the pool "forges a bond" for the coordinated development and stable supply of the whole industrial chain.

4.1.2 Perfecting supply chain security management mechanisms

(1) Risk identification. The more changeable the environment, the more uncertainty and risk there is about what may happen in future. Risk identification attends to the question "what could go wrong?", and forms an accurate and complete risk register through forward-looking, predictive and hypothetical thinking. First, supply chain security risk identification is carried out periodically. Project managers, project team members, operations managers, supply chain risk experts, other project managers and customers are convened periodically to collect multi-dimensional information from the enterprise's joint supply chain security management body, external risk management think tanks and end users, and to analyse fully the sources, causes and events of risk, identifying the circumstances that may have a major impact on objectives and the nature of that impact. Second, an enterprise supply chain security risk register is built. Covering the whole project process — planning and design, procurement and supply, warehousing and logistics, and operation, maintenance and decommissioning — a supply chain security risk database is constructed which on the one hand supports risk assessment and response and on the other is updated qualitatively, monitoring supply chain security risks in real time. An example of a supply chain security risk register is shown in Table 2.

Table 2 Example of a supply chain security risk register

Life-cycle stage	Risk factor	Risk description
Planning and design	Insufficient forward-looking design	Equipment may be at end of life; it must be purchased from the project-approval standpoint, but faces the risk of inevitable obsolescence
	Deviation in design requirements	Because of the pandemic, survey work was not thorough, and machine-room preparation time and machine-room capacity were not accurately established
	Technological dependence	Problems of network interconnection and group requirements lead to inevitable dependence on particular technologies and vendors
Production and supply	Reduced vendor capacity	Shortages of raw materials and components, production limits and power rationing, and the impact of COVID-19 reduce production capacity
Warehousing and logistics	Longer transport times	Because of the international and domestic political situation, the optimum transport route is interrupted and transport personnel cannot take up their posts in time, so that in-transit times lengthen
Operation, maintenance and decommissioning	Ageing equipment	Products are at the end of their life cycle, and vendors reduce capacity or even cease production
	Equipment replacement	Because of supply cut-offs and similar factors, existing equipment must be upgraded to accommodate new equipment, requiring a replacement cycle

(2) Risk assessment. Supply chain security risks are assessed along two dimensions — the probability that the risk will occur and the impact it would have if it did — and are ranked by priority and importance, providing a basis for subsequent risk management action and guiding the formulation of graded risk response measures. The more accurate the analysis, the more targeted the subsequent measures, the lower the cost of response, and the greater the effectiveness of risk management. First, risk probability analysis is carried out: through deductive analysis the causes of hazardous events are identified, and the frequency of hazardous events is predicted from hazard data and expert judgement. Second, risk impact assessment is carried out: all potential consequences arising from hazardous events are identified (including but not limited to those listed below), multi-dimensional factors are taken into comprehensive account, and all possible final outcomes are established.

(i) Urgency: the period within which response measures must be taken if the risk is to be met effectively. (ii) Proximity: how long it will be before the risk affects one or more project objectives. (iii) Latency: the possible period between the occurrence of the risk and its impact. (iv) Manageability: the ease with which the occurrence or impact of the risk can be managed. (v) Controllability: the degree to which the consequences of the risk can be controlled. (vi) Monitorability: the

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

ease with which a risk that has occurred or is about to occur can be monitored. (vii) Connectivity: the degree to which the risk is associated with other risks. (viii) Strategic influence: the potential positive or negative effect of the risk on the organisation's strategic objectives.

(3) Graded risk response. Combining the results of the supply chain risk probability–impact assessment, a risk traffic-light matrix is constructed to manage risks by grade and category and to determine the priority allocation of the enterprise's resources in each area (as shown in Figure 2). Risk is controlled by grade according to the following principles: first, the greater the impact of a risk and the higher its probability, the higher the level of control; second, a lower level must at the same time control the risks for which the level above is responsible, implementing specific measures level by level. The details are as follows.

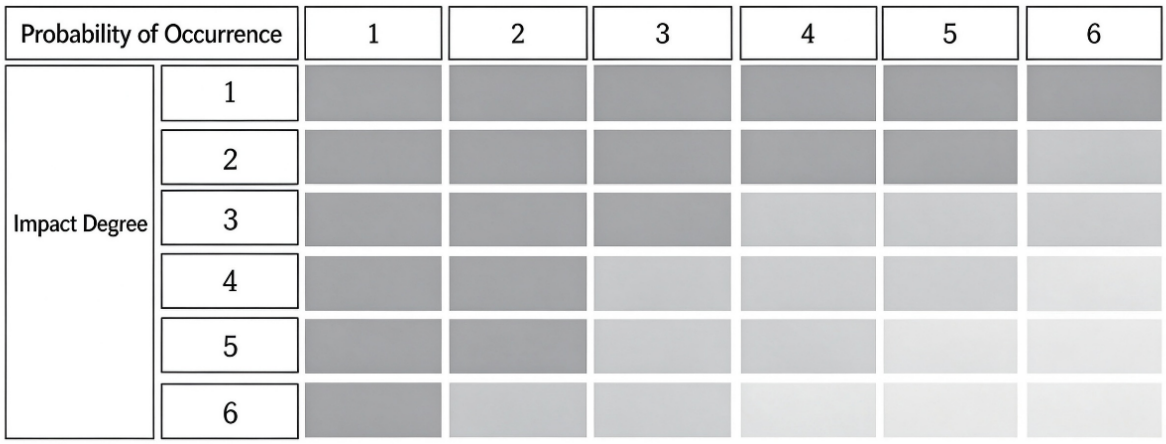


Figure 2 Risk traffic-light matrix

First, green risks. These are chiefly hazards of slight impact and low probability — ones requiring attention or that may be neglected, and that are acceptable. For green risks the department-level supply chain security management group should pay attention and take charge of control and management; no additional control measures are required, and solutions with the better investment payoff should be given priority provided no extra cost is incurred, after which continuous monitoring ensures that the control measures remain effective and the risk level is maintained where it is, the whole process being properly recorded.

Second, yellow risks. These are chiefly hazards of moderate degree and significance, requiring measures to be taken as soon as possible to control and rectify them. For yellow risks the enterprise-level joint supply chain security management group should immediately pay attention and take charge of management and control, while the department-level supply chain security management group should formulate and perfect management systems and regulations to control the risk, strive to reduce both its probability and its impact, carefully determine, plan and control the cost of preventing the risk, and implement risk-reduction measures within a specified period. Where serious harm may result, further assessment should be carried out to establish the likelihood of harm and whether existing control measures need improvement.

Third, red risks. These are chiefly high hazards and major risks, for which measures must be formulated for control and management. For risks at red level and above, the enterprise-level joint supply chain security management group should take charge of control and management as a priority and should actively mobilise resources such as the external supply chain security management think tank to formulate risk response measures jointly. If the risk will affect work in progress, emergency measures should be taken at once, risk management needs should be judged in good time, and risk management objectives, policy, indicators, plans, resource allocation plans and governance deadlines should be set according to those needs, until the risk is reduced.

(4) Risk management supervision. Risk management is a continuous process. Following the Deming cycle, project work is continually supervised through risk process monitoring, so as to determine whether the status of risks has changed, whether risk response has been effective, and whether new risks have appeared, and to assess the effectiveness of risk management. First, an analysis of the effectiveness of risk management is carried out: since risk grades and priorities may change over time and with the external environment, risk reviews are organised periodically and risks are reassessed or quantified. Second, an analysis of the effectiveness of risk response is carried out: the effectiveness of the risk response measures used to deal with risks and their root causes is checked, assessed and recorded; the cost and benefit of risk response are compared against the response objectives; the gap between outcome and objective is established; and where necessary an independent external risk team may be invited to carry out an assessment. Third, an analysis of derivative risk

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

is carried out: the derivative risks brought about by taking response measures (including secondary and consequential risks) are analysed — for example, the increase in procurement cost caused by enlarging safety stocks — and risk assessment and risk response are revisited.

4.2 Formulating more efficient risk prevention measures

4.2.1 Market insight and demand forecasting at the demand-planning stage

(1) Strengthening market insight. Research on trends in the supply market should be actively carried out, the circumstances of the upstream industrial chain and supply chain established, the demand side and the supply side connected, and the information gap narrowed. First, ICT supplier capacity should be established. For first-tier suppliers, a supplier management system should be established and perfected, covering management standards, management principles, quality requirements, delivery requirements, service requirements, resource allocation and cost control. Data on the maximum production capacity in a normal working cycle, whether existing capacity can be increased, delivery volumes and on-time delivery rates, together with their trends, should be established, so as to lock in key materials in advance and secure key projects. Second, the industrial chain of "bottleneck" products should be established. Covering the whole life cycle — product design and testing, production and manufacture, transport and circulation, and operation and maintenance — end-to-end informatised and digital management covering key components and raw materials should be built, so as quickly to detect, anticipate and pinpoint the changes in supplier and component capacity, and the risks, that may be triggered by shifts in the external environment. Targeted market surveys should be conducted, changes in the upstream supply chain grasped in good time, and the delivery priority of the enterprise's orders secured. Third, supplier sourcing should be extended. Through relevant online media, professional conferences and lectures, and industry gatherings, a thorough and comprehensive understanding of products and markets should be gained, information collected from many angles, supply channels and varieties actively broadened, substitute equipment and suppliers cultivated and held in reserve, and a complete, well-ordered directory of supply chain security vendors established, with adaptation work on the existing network carried out in advance to avoid disruption to live services when equipment is replaced.

(2) Strengthening demand forecasting. Building on the existing graded and classified material supply management system, the demand management of key materials and of materials susceptible to the effects of the pandemic should be strengthened, with active response and early intervention. First, the material supply management system should be refined: applying a grid-based approach, material management units should be made smaller, material planning managed by region and by category, the advantages of one-off centralised procurement and of small-scale, high-frequency procurement combined, the procurement model optimised, and the timeliness of demand response improved. Second, intelligent demand analysis should be strengthened: using big-data and other technologies, and drawing on historical material-use data, trend-line analysis and linear regression should be used to strengthen the analysis of material consumption patterns, business development trends and price fluctuation patterns. On the one hand this allows medium- and long-term demand forecasts for at-risk materials, guiding the establishment of safety reserves for them; on the other it allows factors such as procurement lead time, safety stock levels and procurement lot sizes to be taken comprehensively into account in support of procurement strategy, improving the accuracy of demand, moving the demand-planning threshold forward, advancing advance stocking and off-peak stocking, and preparing procurement and redundancy reserves in advance. Third, coordination between procurement and demand should be strengthened: the demand side should raise the frequency of demand feedback and actively collect material requirements, while the procurement side should strengthen supervision of suppliers, obtain supplier capacity information in good time and compare it with future delivery plans, calculating the match between supply and demand and giving early warning of supply risk.

4.2.2 Advancing the construction of a collaborative ecosystem at the sourcing and procurement stage

(1) Adhering to a diversification strategy. Supply chain diversification is an effective means of dispersing security risk. By advancing diversification across the whole process — from the design of communication services to the procurement of equipment and the procurement of suppliers — the risk that any one supplier or ICT product will encounter supply problems is reduced, and where necessary procurement volumes are shifted between different suppliers and different ICT products. First, alternative chip solutions for ICT products should be appropriately increased: starting from the source, from the network architecture design stage, the coupling between network architecture and ICT products should be enhanced, more than two solutions should be available for major equipment, key components of some equipment should be diversified, and the flexibility of supply further improved. Second, a supplier diversification strategy should be maintained: by advancing the distribution of factories across regions, the risk of inability to produce and supply caused by power rationing, the pandemic, natural disasters and other contingencies is mitigated; sole suppliers and suppliers with a single production base should be reduced; the number of winning suppliers may be increased according to market conditions; and

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

a sound system of multiple suppliers for key products should be built, continuously improving the continuity and stability of the supply chain. A flexible and convenient mechanism for adjusting supply shares should be formulated, so that when a supplier's winning share does not match its actual capacity — for instance, where some suppliers are capacity-constrained while others have spare capacity — shares are adjusted according to a pre-set adjustment scheme.

(2) Actively advancing business collaboration. Long-term, deeply cooperative strategic partnerships should be built, replacing short-term advantage with long-term stable collaboration; cooperation attitudes and behaviour should be coordinated honestly and flexibly; supply chain management should be extended to suppliers and even to suppliers' suppliers, synchronising cross-supply-chain participants into a single logical enterprise; and the efficiency and cost advantages of supply chain integration should be brought into play. First, a collaboration portal should be built: the use and analysis of data resources should be strengthened, an informatised supplier collaboration management platform constructed, more efficient communication channels built on digital means, and — taking key process nodes and quality management as the point of entry — more structured and refined overall control promoted. The degree of supply chain information sharing should be increased, system interconnection with strategic suppliers extended, the language systems of design, procurement, engineering and maintenance connected, timely matching of supply and demand achieved, and the efficiency of the whole supply chain process improved. Second, a raw material price linkage mechanism should be explored. Drawing on the raw material price linkage mechanisms that telecommunications operating enterprises have established for batteries, communications cable and similar products, chip and wafer prices and communications equipment prices can be bundled and linked with chip prices, so that when raw material prices change substantially the prices of the relevant products are adjusted, thereby eliminating the supply risk caused by raw material price movements and safeguarding material supply.

(3) Actively leading the supply chain ecosystem. The procurement model should be innovated: using the special position that telecommunications enterprises occupy in the industrial chain and supply chain, the "chain leader" role should be played well, the strong driving and integrating capacity of "chain leader" enterprises in the supply chain and industrial chain brought fully into play, and the coordinated and mutually beneficial development of small and medium-sized enterprises upstream and downstream led and promoted. First, small and medium-sized suppliers should be actively supported, with help in many forms — funding subsidies, joint research and development, test scenarios and priority pilots. Guided by enterprise demand, the integration of "investment + research and development + procurement" should be explored, targeted technology development and targeted commercialisation of results promoted, close linkage between the actors and links of the industrial chain advanced, a sound symbiotic ecosystem of industrial chain development formed, and the enterprise's own technological capability held in reserve with a "spare tyre" mentality. Second, the formation of a domestic industrial chain ecosystem should be actively promoted: in response to the national call, and for "chokepoint" core components and products, the proportion of domestically produced chips and equipment procured should be appropriately increased, the industrial chain guided to continue independent research and to increase investment in innovation, the conquest of a group of landmark core technologies with independent intellectual property accelerated, the iterative upgrading of domestic software and hardware products advanced in an orderly way, and domestic software and hardware moved from being "usable" to being "good to use", building a domestic industrial ecosystem.

4.2.3 Improving response agility at the warehousing and logistics stage

(1) Strengthening logistics management along the chain. Digitalisation and online operation should be promoted across every link of the whole chain from production site to project site. Through technical cooperation with upstream and downstream supply chain nodes — procurement units, production enterprises, supplying units, logistics enterprises and actual carriers — collaborative logistics management should be achieved, and risk information such as delivery delay or interruption and logistics delay or interruption obtained in good time, with early warning and handling. First, a one-stop, end-to-end logistics management system should be built: relying on the supply chain collaboration ecosystem, management of supplier logistics and third-party carrier logistics should be strengthened, multi-point collaboration in logistics operations advanced, orders, logistics and inventory displayed visually, information on vehicle dispatch, goods in transit and goods receipt grasped in good time, effective supervision and monitoring of the dispatch, transport and arrival links achieved, control over supplier arrival and project arrival information strengthened, on-time arrival rates established, and early warning given of risks such as dispatch delay and logistics delay. Second, an emergency logistics system should be built without delay: for contingencies such as the pandemic, a fast-responding, seamlessly connected functional logistics network chain should be built; on the basis of precise warehouse management, inventory turnover control in supply chain logistics management should be achieved, providing the basis and support for transfers between warehouses; arrival should be tracked in good time; efficient and scientific planning of logistics routes and rational regulation of logistics resources should be supported; logistics activity should be matched to the distribution of demand; and efficient circulation of logistics should be secured.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

(2) Optimising the internal warehousing model. Safety stock management should be strengthened, with subdivided management by region, by category and by priority; for key and core ICT equipment, "demand–inventory–plan" linkage across the whole chain should be achieved; and by informatised means, changes in the external market should be responded to in good time and safety stock managed dynamically. First, flexible allocation of materials should be secured: through combinations of modes such as "inventory materials + materials at temporary storage points" and "list + flexible dispatch", materials should be dispatched to the nearest point, internal coordination of materials strengthened, the operating capacity of the regional divisions enhanced, common and critical materials shared and co-distributed, redundant inventory at multiple levels reduced, and multi-level joint supply and cross-provincial material dispatch promoted. Second, inventory status should be monitored intelligently: centralised management of the national warehouse network should be achieved, ensuring that inventory risk is visible, controllable and traceable; by judging the life cycle of products, analysing the direction of orders, and taking account of the delivery rate and flexibility of procurement supply, safety stock rules should be updated dynamically, the balance point between "inventory holding cost" and "stock-out cost" found, a reasonable dynamic inventory strategy drawn up, "inventory–order" response strategies prepared in advance, possible risks warned of, and the risk of overstocking and of stock-out reduced.

4.2.4 Maximising resource utilisation efficiency at the material-use stage

(1) Putting existing materials to work. In the face of the industrial and supply chain "bottlenecks" caused by shocks such as the Russia–Ukraine conflict and the contest among major powers, and where the security risk to the supply chain of key equipment may persist for a long time, supply chain stability should be secured as a priority where supply chain advancement cannot be guaranteed. First, stranded materials should be brought into service: for materials left stranded by the need to secure procurement margins and safety stock levels, the principle of "use whatever can be used" should be upheld, the value of over-stocked materials fully activated, value extracted from what is otherwise a "burden", the pooling role of the regional warehouses used, and the redeployment of redundant materials strengthened. Second, "retired" equipment should be given a "second term of service": through reverse logistics, recovery and reuse should be promoted, with second use where function and safety are unaffected; "retired" equipment that has reached the end of its life cycle or been displaced by upgrading should, after overhaul, testing and maintenance and having passed inspection, be "re-employed"; and for "medically retired" equipment that cannot be repaired because some components are damaged, those components should be dismantled and the others recombined, supporting emergency use in contingencies.

(2) Rational allocation of material use. In the face of the risk of price rises, shortages and even stock-outs, a more precise approach to material supply management should be adopted, so that supply is sufficient, consumption low, costs saved and waste small. First, whole-life-cycle material management should be advanced: using a "list-based" management method, "one form to the end" and "one code to the end" should be implemented, linking different enterprises, departments and systems, and monitoring the whole life cycle of materials — "requirement", "procurement", "supply", "storage", "use", "return" and "scrapping" — by full digital identity, so that the status of materials is understood in real time, the actual situation of construction use is understood, and resource allocation is more rationally achieved. Second, the method of drawing materials should be optimised: on the basis of centralised supply of standard and general-purpose parts, point-to-point supply of key and important parts should be provided in support; materials should be drawn against issue rather than pre-issued, and issued according to need; small-batch, high-frequency requisition should be encouraged; the scarcest materials should be reserved for the most important projects; and higher returns should be created with less investment.

5 Conclusions and Prospects

This article has carried out in-depth research on the risk management system and on risk response measures. In particular, for the work of responding to and preventing ICT supply chain security risks in telecommunications operating enterprises, it puts forward comprehensive recommendations for response strategy, supporting enterprises in withstanding ICT supply chain security risks. It systematically reviews the supply chain security risks experienced since 2020 and the specific measures taken in responding to them, and, integrating risk management with the whole process of business implementation, forms a complete and systematic response strategy in respect of both the risk management system and response measures, providing a reference for safeguarding the security and stability of the ICT supply chain and promoting high-quality development of the enterprise.

Because there is relatively little research material in the domestic and international literature, and because the research capability of the project team members is limited, the study has certain shortcomings. The following directions may, as the environment continues to develop, be appropriately updated and optimised and studied further. First, the effectiveness of the recommended strategies remains to be verified. Owing to time constraints, the practical effect of the response strategies has not yet been fully demonstrated, and their economic, technical and organisational feasibility still requires exploration

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

and verification — for example, whether the equipment of alternative suppliers can meet design requirements in terms of adaptation and performance, and whether network performance is affected, are questions that require further observation and, on that basis, continuous tuning. Second, the body of knowledge accumulated by the research remains to be disseminated. Research on supply chain security and stability is still a new subject, and the stable operation of supply chain security is not a problem for any single enterprise: it requires the joint efforts of the actors along the chain. The research approach and findings accumulated here can provide a reference for the study of supply chain stability in peer companies, and can be updated and optimised in the light of actual business conditions and the latest security situation, so as to promote a joint improvement in risk response capacity among the enterprises along the chain and to ensure the overall stability and efficiency of the supply chain and industrial chain.

References

[1] CHEN X H, SHANG Y M, WANG H L, et al. Research on international ICT supply chain security management with Chinese characteristics[J]. *Information Security and Communications Privacy*, 2019(4): 32-36. [in Chinese]

[2] LU T B, GUO X B, YAO P X, et al. A framework for standardization of ICT supply chain security[M]. Berlin: Springer, 2019: 1-12.

[3] MIN S, SON K. Comparative analysis on ICT supply chain security standards and framework[J]. *Journal of the Korea Institute of Information Security and Cryptology*, 2019, 29(2): 1-10.

[4] SOLDANI D. 5G and the future of security in ICT[C]//2019 29th International Telecommunication Networks and Applications Conference (ITNAC). IEEE, 2019: 1-4.

[5] Han Xiaolu, Duan Weilun, Lü Xin, et al. Analysis of and countermeasures against 5G supply chain security risks[J]. *Journal of Information Security Research*, 2021(12): 7. [in Chinese]

[6] Li Lu, Ni Ping, He Haokun, et al. Analysis of ICT supply chain security risks and typical events[J]. *Defence Science and Technology Industry*, 2019(9): 3. [in Chinese]

[7] Li Lu, Wang Kun. Research and practice in ICT supply chain security risk management[J]. *Secrecy Science and Technology*, 2020(5): 44-47. [in Chinese]

[8] Liu Yao, Chen Shanshan. The impact of COVID-19 on global supply chains and China's response: from the perspective of the dual superposition of supply-side disruption and demand-side weakness[J]. *Intertrade*, 2020(6): 53-62. [in Chinese]

[9] Li Yan. ICT supply chain security governance from the perspective of international norms[J]. *Information Security and Communications Privacy*, 2020(4): 5. [in Chinese]

[10] He Haokun, Li Lu. Research on risk identification in ICT supply chain security management[J]. *Cyberspace Security*, 2019, 10(4): 6. [in Chinese]

[11] Ni Guangnan, Chen Xiaohua, Shang Yanmin, et al. Research on and recommendations for ICT supply chain security management abroad[J]. *Strategic Study of CAE*, 2016, 18(6): 104-109. [in Chinese]

[12] Shangguan Xiaoli, Sun Yan, Li Yanfeng. Research on policies, regulations and standards for information and communication technology supply chain security[J]. *China Information Security*, 2021(10): 43-46. [in Chinese]

[13] Yin Jianfeng, Peng Aihua, Chen Jianhong, et al. Digital transformation of supply chain management in operating enterprises[J]. *Telecommunications Enterprise Management*, 2021(3): 66-67. [in Chinese]

[14] Hu Yongjun, Cheng Jianning. Reducing ICT supply chain risk to a minimum[J]. *Telecommunications Enterprise Management*, 2022(8): 30-31. [in Chinese]

[15] Cheng Jianning. The path and development trend of digital and intelligent transformation in central enterprise procurement[J]. *Telecommunications Enterprise Management*, 2021(11): 2046-2048. [in Chinese]

[16] Wang Jiashuo, Cheng Jianning, Zhou Tiancheng. Analysis of and countermeasures for ICT supply chain security in telecommunications operating enterprises under the new situation[J]. *China Tendering*, 2022, 1479(11): 70-74. [in Chinese]

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.