International Journal of Asian Social Science Research; Vol.3, No.4; 2026
E-ISSN: 3006-2179 P-ISSN：3006-754X
DOI: https://doi.org/10.70267/ijassr.260304.5864
Published by: Zeus Press

Building Comprehensive Compliance for Cross-Border Supply Chains Under Export Control Laws and Regulations

Guangying Zhang*

Costco (China) Investment Co., Ltd. Shanghai 201107, China

**Corresponding author: Guangying Zhang.*

Abstract

The tightening of export control regulations has laid the groundwork for unprecedented requirements around cross-border supply chain compliance. The traditional approach of conducting a static review of the parties directly involved in a transaction will not address the systemic challenges posed by the expansion of regulatory tentacles to the farthest reaches of the supply chain. Ultimately, the core of penetrating compliance lies in rethinking the logic of compliance governance, expanding the subject of compliance from individual corporations to all players in the entire chain, broadening the object of compliance from item control to end user/user verification, and shifting compliance from post-review to ongoing monitoring throughout the entire process. This framework relies upon penetrating due diligence during the admission phase, embedding compliance nodes in the circulation phase, and tracing the flow of end processes. Operational guidelines, collaborative management entities and information tracing systems provide operational support for penetrating compliance.

Keywords

export controls, cross-border supply chains, look-through compliance, legal regulations

1. Introduction

In recent years, export control legislation has exhibited two convergent tendencies: the extraterritorial reach of domestic regulations has markedly expanded, while concomitant sanctions have grown appreciably more severe. The U.S. Export Administration Regulations (EAR) exemplify this trend, leveraging the Entity List and the De Minimis Rule to project American legal strictures far beyond U.S. borders. Concurrently, China's Export Control Law, enacted in 2020, grants domestic regulatory bodies the authority to trace the trajectory of controlled items through all stages of export transactions. These normative developments, unfolding against a backdrop of intensifying geopolitical rivalry, imply that a compliance lapse at any single echelon of the supply chain carries the potential to trigger cascading repercussions across the entire network. The prevailing compliance paradigm, anchored in static due diligence directed at the contracting party, founders when confronted with opaque transactional configurations—successive resales, cross-shareholding among intermediaries, and layered distribution channels. The resultant chasm between the regulatory ambition of penetrating oversight and the operational realities of compliance practice constitutes a pressing problem

demanding scholarly attention. It is within this interstitial space that the concept of "look-through compliance" emerges—not merely as a defensive posture against enforcement risks, but as a strategic opportunity to reconfigure supply chain governance for enhanced transparency and resilience.

2. New Challenges Posed by Export Control Laws to Cross-Border Supply Chain Compliance

2.1 Traditional Compliance is Limited to Static Screening of Direct Transaction Parties

The most salient transformation in export control legislation over recent years consists in the relentless outward expansion of prescriptive jurisdiction. Novel regulatory architectures no longer rest content with scrutinising the qualifications of actors directly engaged in export transactions; rather, they impose cascading compliance duties that ripple through successive tiers of the supply chain. Under the United States' Export Administration Regulations, the interplay between Entity List affiliation rules and the De Minimis calculation mechanism effectively brings within the regulatory perimeter re-sale and re-export activities conducted by non-U.S. entities. Concomitantly, China's Export Control Law furnishes statutory grounding for end-to-end traceability of controlled articles. This jurisprudential evolution carries a pivotal implication: the exporting party's accountability persists beyond the mere handover of merchandise. Any unauthorised modification of the ultimate consignee or any diversion from the stated end-use, even if occurring at the most peripheral node of the distribution network, may furnish sufficient grounds for a determination of non-compliance.

2.2 New Regulations Require “Look-through” Oversight of Entities at the Far End of the Supply Chain

The recently revised export control regulations have recalibrated the jurisdictional scope of compliance obligations, extending beyond the bilateral exporter-immediate counterparty relationship to encompass all intermediary handlers and the ultimate recipient of the goods in question. Under this expanded normative framework, the exporting party assumes a legally cognisable duty to conduct reasonable verification of the ownership structure, operational profile, and historical receipt records of entities situated at the second tier—and conceivably deeper strata—of the supply chain. Within this enhanced standard of care, exculpatory declarations proffered by the direct contracting party no longer carry sufficient evidentiary weight to discharge the exporter's diligence obligations. Should the exporting party exhibit any deficiency in compliance scrutiny at these remote tiers, a violation determination may ensue—notwithstanding that the direct counterparty possessed all requisite credentials at the time of contracting—provided that the actual end-user or *de facto* utilisation deviates from the particulars filed with the competent authorities. The Seagate Technology case illustrates this principle [1].

2.3 Expanded Liability for Violations is Driving a Transformation in Compliance Models

Export control legislation exhibits a conspicuous expansion in liability allocation, with enforcement actions increasingly directed not solely at the principals executing the export transaction, but also at intermediaries, freight forwarders, and even downstream consumers implicated in the chain of custody. Regulatory agencies have simultaneously elevated the due diligence threshold expected of exporters, imposing an ongoing duty of care that operates irrespective of where in the supply chain the offending conduct occurs. Under this reconfigured liability regime, an exporter cannot evade legal consequences merely by demonstrating that the violation was perpetrated by a remote party; absent affirmative proof that it has discharged its reasonable oversight functions, the exporter remains exposed to enforcement measures. The legacy compliance playbook—predicated largely upon contract execution and documentary verification at discrete transactional milestones—no longer affords a tenable defence in this more exacting enforcement environment. The ZTE case—in which the U.S. Department of Commerce in 2016 determined that the company had routed telecommunications equipment to Iran through shell companies and third-party carriers—illustrates how liability has diffused from direct actors to all supply chain participants. The penalties imposed on ZTE itself, as well as on the intermediaries and freight forwarders involved, confirm that any compliance lapse at any tier can trigger cascading accountability across the entire network [2].

3. System Framework for Building Penetrative Compliance in Cross-Border Supply Chains

3.1 Compliance Entities: Expanding from a Single Enterprise to All Relevant Parties Across the Chain

The existing framework for export control compliance concentrates compliance obligations solely on a single entity of the exporter, with other supply chain participants only assuming limited cooperation obligations rather than independent compliance responsibilities. Recent legislation has included remote intermediaries, freight forwarders, technology transferors, and even end-users in the potential scope of accountability, with exporters bearing *de facto* integrated responsibility for the actions of all parties involved in the entire chain. Compliance entities must therefore expand from a single enterprise to include all stakeholders in the entire chain, including suppliers, distributors, logistics service providers, and end-users. Each entity at every link in the chain must assume corresponding compliance obligations within their business scope. The responsibility radius faced by exporters in compliance management has expanded to include not only ensuring compliance with their own behavior, but also assuming substantive review and supervision responsibilities for the compliance capabilities and consequences of remote entities. This shift has led to the definition of compliance entities no longer being based on contractual relationships, but rather on the actual control over the flow of items. The burden of compliance obligations has shifted from a single enterprise to a multi-center responsibility network.

3.2 Compliance Targets: Extending from Controls on Goods to Verification of End Users and End Uses

Traditional export control practices strictly limits compliance to the items themselves, and the core task of compliance work is to confirm whether the classification code of the exported items matches the license requirements. The recent legislation has elevated the importance of end-users and end uses to the same level as item control, and the obligation of exporters to verify the identity background, business scope, and item usage plan of the recipient has been elevated to a statutory independent compliance requirement. Once the item is delivered, the deviation between its actual user and declared use constitutes the core source of compliance risk, and the technical parameters of the item itself have not changed in any way. The compliance object extends from static item attributes to dynamic dimensions of people and use. The exporter needs to simultaneously complete the triple task of item compliance judgment, receiver background review, and usage rationality evaluation. Any single dimensional omission may cause the entire export behavior to deviate from the compliance track.

3.3 Compliance Methods: Shifting from Post-Event Reviews to Dynamic Monitoring Throughout the Entire Process

The existing operation of export control compliance regards the review as an independent process that occurs at a specific point in time. The compliance department declares the end of the review after completing item classification, license verification, and transaction party screening between order signing and goods delivery. Recent law enforcement cases have revealed that compliance risks do not condense at the moment of transaction, as changes in equity in remote links of the supply chain, adjustments to end-user business scope, or resale of items may trigger violation recognition several years after contract signing. The compliance approach must therefore shift from node based review to dynamic monitoring covering the entire process of order generation, production stocking, shipment customs clearance, in transit tracking, and post delivery flow monitoring, with corresponding compliance checkpoints set up at each stage. The exporter must continue to monitor the actual receipt and use of the items after delivery, regularly update the background information of remote entities, and compare it with the regulatory list. The endpoint of compliance management is no longer marked by the receipt of goods [3].

4. Implementation Pathways for Penetrative Compliance in Cross-Border Supply Chains

4.1 Entry Stage: Establishing Penetrative Due Diligence Procedures for Suppliers

Due diligence conducted during the supplier admission stage constitutes the first line of defense to penetrate compliance, and its operational depth directly determines the size of risk exposure in subsequent stages.

Traditional supplier surveys are limited to requesting business registration information and filling out standardized questionnaires, and this level of data collection has little screening value for identifying hidden associations and potential compliance risks of remote entities. Penetrating due diligence requires extending the investigation level to the shareholder structure of suppliers, actual controllers, and their affiliated entities, with a particular focus on whether there is a shareholding relationship or personnel overlap with regulated entities. The exporter shall embed the entity list, industry sanction list, and end-user blacklist issued by regulatory agencies into the standard comparison process for supplier access, and design differentiated investigation depth based on this. For suppliers in high-risk areas, the compliance department needs to further collect information on their upstream and downstream counterparties to assess the possibility of items being resold to sensitive entities after processing. The scope of investigation has expanded from first tier suppliers to second and even third tier nodes. After the admission review is completed, a regular review mechanism must still be established. The compliance status of suppliers continues to change with the dynamic adjustment of the regulatory list and changes in their own business conditions. A one-time admission approval does not constitute permanent compliance endorsement.

4.2 Transit Stage: Embedding Compliance Screening into Contracts, Orders, and Logistics Nodes

The compliant design of contract terms constitutes the first control node in the circulation process, and the exporter shall include restrictive clauses on the use of items and binding agreements on non resale without permission in the sales contract. The order generation stage triggers the automatic launch of the compliance screening program, and the compliance department must verify whether the recipient and end-user information stated in the order differs from the information retained in the admission process. Logistics nodes are located in high-risk areas for compliance risks, and cross checking the item names, quantities, and final destinations in the customs declaration information is particularly crucial before the goods are shipped. The warehouse receipts and bill of lading information provided by logistics service providers must be consistent with the export declaration content [4]. If there is a change in the transshipment port or adjustment of the recipient's information during the transit of goods, the compliance department must reassess whether these changes affect the validity of the original compliance judgment. The transmission of compliance information between various circulation nodes by the exporting party cannot be ignored. The supplier information collected in the admission process and the user information verified in the order stage should be coherent and traceable. Any disconnection at any node may result in a break in the compliance chain.

4.3 End-Point Stage: Trace Final Destinations Through Contractual Obligations and Document Verification

The core dilemma of the end stage lies in the sharp increase in the likelihood of discrepancy between the actual usage scenario and the declared purpose of the item once it is no longer under the physical control of the exporter. The root cause of this dilemma is not the lack of compliance willingness of the exporter, but the physical barrier of the verification capability naturally formed by the information asymmetry at the remote level. Faced with this barrier, the exporter must use contractual constraints as the institutional basis for information acquisition, and explicitly include obligation clauses in the sales contract for downstream distributors and end-users to regularly report the usage status of items. The design of such clauses must specify specific reporting content, frequency, and breach of contract liability in case of non-performance, only then can abstract legal rights be transformed into enforceable commercial constraints. The contract terms merely provide a basis for rights, and the actual traceability still relies on the operability of document verification. After the delivery of the goods, the exporter should request the recipient to provide the import declaration issued by the customs, the final delivery certificate issued by the carrier, and the acceptance report of the item installation site in sequence, and cross compare the above three documents with the end-user information filled in during the export declaration. If the item passes through multiple intermediaries before reaching the end user, the exporter must collect the contract number and property transfer certificate for each level of transfer in reverse along the supply chain, so that every ownership change can be covered by a complete written record. When downstream entities refuse to cooperate with the provision of documents or when there is a logical contradiction in the documents submitted, the exporting party shall immediately activate the suspension of supply clause in the contract and simultaneously initiate internal review procedures. If it is verified that the

items have flowed into the controlled entity or sensitive use, it shall be required to return the goods or terminate subsequent cooperation in accordance with the contract agreement. The binding force of the contract and the traceability provided by the documents together constitute the management loop of the end link, and any lack of alignment between the two will lead to the breakage of the traceability chain.

5. Supporting Measures for Cross-Border Supply Chain Penetrative Compliance

5.1 Developing Tiered, Actionable Compliance Guidelines

Frontline compliance officers daily confront a significant gap between the regulatory provisions' principled language and the transaction realities. This gap makes it increasingly difficult for these employees to translate abstract regulatory norms into concrete behaviors because there is little operational basis for doing so.

The content of guidance material should have a three-level hierarchy, allowing for distinct levels of role-specific guidance. For instance, the section addressed to senior management would include a statement of the overall penetration compliance risk framework; this serves to provide senior management with a general understanding of the relationship between penetration compliance risk and business interests in order to aid in making decisions regarding resource allocations to compliance programs. The section for middle-management compliance employees would provide operational procedures for compliance-related processes. This would help middle management define specific tasks that need to be performed and how to properly evaluate the performance of those tasks. The section for employees in frontline operational roles would contain enough detail that, for example, an employee now has the operational knowledge necessary to complete the filling out of a form, will be able to archive a document and report to their manager the existence of an anomaly, etc. Each layer's content must correlate to the true responsibilities of positions — senior executives need not understand the specifics of operational entities, while front-line employees need not consider global risk exposure strategically [5].

5.2 Establishing a Mechanism for Synergy Between Compliance and Supply Chain Management

The compliance and supply chain management (SCM) departments have historically worked independently, with the compliance department tasked with identifying risk and ensuring regulatory compliance, while the supply chain department is primarily concerned with cost control and delivery efficiency as their major performance measurement methods. The difference between the two departments' methods of assessment has caused ongoing resistance at the operational level when trying to embed compliance requirements into the supply chain's operations. Building a collaborative linkage mechanism requires the elimination of the information barriers between the two departments. The procurement department must, at the same time, obtain compliance feedback from the compliance department concerning suppliers during the supplier development process while also including the supplier's compliance history in the supplier admission evaluation system. In a similar vein, the logistics department must collaborate with the compliance department to confirm the regulatory limitations associated with ports and transshipment points prior to developing transportation plans. When integrating compliance into the SCM process, the SCM and compliance departments should establish a routine structure of meetings where both departments can share information concerning regulatory developments and the SCM process. Through these meetings, the SCM department can inform the compliance department of new or changing regulations affecting SCM, and the compliance department can provide SCM with a summary of compliance issues experienced by the SCM department within its operational functions. Furthermore, compliance incidents would be evaluated together to identify and address SCM management weaknesses that were exposed by such incidents. The success of the collaborative mechanism will also be related to how well the enterprise has defined the authority of the compliance function and the value placed on compliance metrics within the performance measurement systems of both departments [6].

5.3 Leveraging Information Systems to Ensure Data Logging and Traceability

When putting in place information systems for the purpose of complying with the requirements of building compliance, these information systems must provide more than just passive storage of data. The principal value of information systems lies in integrating compliance-related data from disparate business processes into a

structured chain of evidentiary records. In order for the compliance department to provide rapid access to the complete body of information, including supplier investigation records, background verification records of transactions, criteria for the classification of goods, and comparison of end-user documents, information systems must not only be designed with the data fields and associated logic considered in the system's initial design, but also should cover all of the process data associated with each transaction in the exportation of goods, such as records of suppliers' changes of equity structure, history of the transaction of intermediaries, and operation logs of each logistics node throughout the entire supply chain, all of which must be included in the system's required collection scope. In addition, the system must have the capability to store all original shipping documents as attachments and provide for their indexing to facilitate retrieval through multiple forms of matching practices, including but not limited to fuzzy and exact match queries [7].

6. Conclusion

The goal of compliance construction is to move beyond merely meeting formal obligations to managing actual risk through changes in the governance of a cross-border supply chain. When companies utilize a more extensive due diligence effort, as well as incur transition costs associated with implementing the necessary information systems to enable this, they now also have an opportunity to address potential vulnerabilities in the underlying supply chain infrastructure. The primary purpose of international trade compliance is to create a flexible supply chain that is able to quickly adapt to changes in the regulatory environment within legal limits; therefore, the successful transition of compliance by using it as an underlying architecture for all supplier relationships will rely on the strategic trade-offs made between compliance expenditures versus enterprise risk exposure, and the ability of the regulatory environment to provide clarity and facilitate effective commercial transactions.

References

[1] Yu Zhen, Shang Yu, Li Xue. The Impact of U.S. Commercial Control Lists on Innovation by Chinese Enterprises: Based on Supply Chain Mechanisms [J]. World Economic Research, 2024, (5): 48–62+135.

[2] Jiang Daxing. Trade Controls/Trade Retaliation and Cross-Border Corporate Governance—How Did the ZTE Case Distort the Evolution of Corporate Governance? [J]. Dongyue Luncong, 2020, 41(2), 113–126+192.

[3] Cheng Hui, Xing Zhengjun. The Current Status and Future Trends of U.S. Export Controls on China Amid U.S.-China Strategic Rivalry [J]. International Economic Cooperation, 2025, 41(1): 23-32+91.

[4] Rasador S G ,Cunha M A .The new security grey zone: export controls, emerging technologies and US-China technological rivalry[J].The Pacific Review,2025,38(6):1020-1048.

[5] Gao X ,Guo C ,Hu A .Export controls and stock price fluctuations of affiliated companies: Empirical evidence from the US entity list against China[J].Economic Analysis and Policy,2026,89965-985.

[6] He H ,Chen P ,Huang X , et al.The influence of the U.S. export controls against China on the resilience of Chinese corporates.[J].PloS one,2025,20(9):e0331222.

[7] Wei Ping, Zhang Chaorui. U.S. Export Controls on High-Tech Products to China and Their Impact on Bilateral Trade [J]. Industrial Technology and Economics, 2018, 37(1): 76-85.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.