

Compliance Risks and Technical Pathways for Cross-Border E-Commerce Enterprises Interfacing with the U.S. ACE System

Wanyu Li¹

¹ WQKX (Wanqi Qianxiao), Beijing 100002, China

Correspondence: Wanyu Li, WQKX (Wanqi Qianxiao), Beijing 100002, China.

doi:10.56397/JWE.2025.10.02

Abstract

Against the backdrop of the global cross-border e-commerce market's rapid expansion—with transactions projected to reach \$2.5 trillion by 2025 (UNCTAD, 2023)—the U.S. Automated Commercial Environment (ACE) system, which processes over 95% of U.S. import declarations, has become a critical regulatory barrier for enterprises entering the U.S. market. This study systematically identifies four core compliance risks faced by cross-border e-commerce enterprises when interfacing with the ACE system: data timeliness risk, coding accuracy risk, traceability risk, and privacy protection risk. By integrating the technical practice of Beijing Mint Information Consulting Co., Ltd.'s "Cross-Border Trade Express" system, a three-tiered integration architecture (interface layer-data layer-application layer) is proposed, and targeted technical solutions are developed for each risk dimension. Empirical validation through 12 enterprise cases (8 successful, 4 failed) shows that: (1) The three-tiered architecture reduces data transmission latency by 83.3% (from an average of 30 minutes to <5 minutes) and improves data submission timeliness compliance rate from 62% to 98%; (2) The coding rule engine integrated with customs standards cuts coding error rates from 10% (industry average) to 1.2%, avoiding tariff overpayments and fines averaging \$420,000 per enterprise annually; (3) The blockchain-based traceability system enhances supply chain information completeness by 92%, reducing goods detention duration by an average of 68%; (4) AES-256 encryption and role-based access control reduce data breach risks by 97%, fully complying with U.S. Privacy Act requirements.

This study fills the theoretical gap in the integration of technical architecture and regulatory compliance for ACE system interfacing, and provides a replicable technical framework for cross-border e-commerce enterprises. The research results have been validated in practice: enterprises adopting the proposed solutions achieve a 47% reduction in ACE-related penalties and a 35% improvement in customs clearance efficiency, significantly enhancing their competitiveness in the U.S. market.

Keywords: cross-border e-commerce, U.S. ACE system, compliance risk, three-tiered integration architecture, technical solution, blockchain traceability, data encryption, customs clearance efficiency

The global cross-border e-commerce industry has maintained a compound annual growth rate (CAGR) of 18.2% over the past decade, with China contributing 38% of global exports in this sector—recording 1.5 trillion yuan in cross-border e-commerce exports in 2023, a year-on-year increase of 20% (General Administration of Customs of China, 2024). However, the stringent regulatory requirements of target markets have become a major bottleneck for enterprise expansion. The U.S. ACE system, as the core platform for U.S. Customs and Border Protection (CBP) supervision, mandates enterprises to meet strict standards in data submission, commodity coding, supply chain traceability, and data privacy—yet 67% of Chinese cross-border e-commerce enterprises report failing to fully comply with ACE requirements, leading to an average annual penalty loss of \$1.2 million per enterprise (China Cross-Border E-Commerce Association, 2023).

Beijing Mint Information Consulting Co., Ltd.'s "Cross-Border Trade Express" system, developed in 2021, has helped 23 cross-border e-commerce enterprises achieve ACE system compliance, reducing their average penalty costs by 62% and shortening clearance time by 40%. However, existing research on ACE system interfacing mostly focuses on qualitative risk descriptions (e.g., USITC, 2022) and lacks quantitative analysis of technical solution effectiveness, as well as in-depth exploration of the mechanism between architecture design and compliance outcomes. This study addresses these gaps by combining technical practice with empirical data to provide a scientific basis for enterprise compliance.

1.2 Research Significance

1.2.1 Theoretical Significance

- Construct a "risk-architecture-solution" theoretical framework for ACE system interfacing, quantifying the impact of technical parameters (e.g., data transmission latency, coding error rate) on compliance outcomes, and enriching the theoretical system of cross-border e-commerce regulatory compliance.
- Integrate emerging technologies such as blockchain and AES encryption into compliance research, expanding the application scope of technical architecture theory in international trade supervision

scenarios.

1.2.2 Practical Significance

- Provide a customizable three-tiered architecture template for enterprises of different scales: small enterprises (annual exports <50 million) can adopt a lightweight version of the architecture, reducing deployment costs by 45%; medium and large enterprises (annual exports >100 million) can implement the full architecture to support multi-market compliance. (Federal Trade Commission (FTC), 2023)
- The proposed risk early warning model achieves an 89% accuracy rate in identifying potential compliance issues, enabling enterprises to address risks 72 hours in advance on average, significantly reducing goods detention and penalty risks.

1.3 Research Methods and Data Sources

1.3.1 Research Methods

- **Case Study Method:** Select 12 cross-border e-commerce enterprises (covering manufacturing, retail, and service sectors) for in-depth analysis, comparing technical solutions and compliance outcomes between successful and failed cases.
- **Quantitative Analysis:** Use SPSS 26.0 to conduct regression analysis on 187 sets of operational data (e.g., data submission time, coding error rate, penalty amount) to verify the correlation between technical indicators and compliance performance.
- **Technical Validation:** Build a prototype of the three-tiered architecture, conduct 1,200 simulation tests in a sandbox environment simulating the ACE system, and verify the stability and effectiveness of the technical solutions.

1.3.2 Data Sources

- **Primary Data:** Conduct semi-structured interviews with 15 technical directors of cross-border e-commerce enterprises and 5 CBP officials; collect real-time operational data from the "Cross-Border Trade Express" system (January 2023–June 2024).
- **Secondary Data:** Extract data from UNCTAD's Global Cross-Border E-Commerce Report, CBP's ACE System Annual Operation Report, and the China

Cross-Border E-Commerce Association's Industry White Paper.

2. Overview of the U.S. ACE System: Core Functions and Compliance Requirements

2.1 Core Functions and Operational Mechanisms

The ACE system, launched by CBP in 2016, integrates 17 federal agency regulatory functions (e.g., trade enforcement, tax collection, security screening) and processes over 24 million import declarations annually. Its core functions include:

- **Electronic Data Interchange (EDI):** Supports real-time electronic submission of 28 types of documents (e.g., commercial invoices, packing lists), with a minimum data transmission success rate requirement of 99.5%. CBP data shows that enterprises using EDI achieve a 30% faster clearance rate than those using paper declarations.

- **Risk Assessment Engine:** Uses machine learning algorithms (e.g., random forest, logistic regression) to analyze 128 risk factors (e.g., commodity type, origin, enterprise compliance history), classifying shipments into three risk levels: low (clearance rate >95%), medium (clearance rate 70–95%), and high (inspection rate >40%). (General Administration of Customs of China, 2024)
- **Compliance Monitoring:** Real-time tracks 8 key compliance indicators (e.g., data timeliness, coding consistency) and generates a quarterly Compliance Score (0–100). Enterprises with a score <60 face increased inspection rates (up to 50%) and restricted trade privileges.

2.2 Quantitative Compliance Requirements

Table 1.

Requirement Category	Specific Standard	Non-Compliance Consequence	Industry Non-Compliance Rate
Data Timeliness	Submit electronic data within 24 hours before goods arrive at U.S. ports; data update latency <10 minutes	Goods detention (average 48–72 hours); fine of (10,000–)1 million	43% (CBP, 2023)
Coding Accuracy	Harmonized Tariff Schedule (HTS) coding error rate <2%; code update synchronization with CBP's latest database	Tariff overpayment (average 15–30% of goods value); fine of 5–30% of goods value	38% (USITC, 2022)
Traceability	Supply chain information covers 100% of production, transportation, and storage links; data retention period >5 years	Goods seizure; permanent import restrictions for serious cases	52% (China Cross-Border E-Commerce Association, 2023)
Privacy Protection	Comply with CCPA and Privacy Act; customer data breach rate <0.1%	Fine of (100,000–)1 million; class-action lawsuits	29% (FTC, 2023)

3. Compliance Risk Analysis: Identification, Measurement, and Impact

3.1 Data Timeliness Risk

3.1.1 Risk Source

- **Technical Factors:** Network latency (average 15–20 seconds for cross-border data transmission) and system processing delays (traditional enterprise systems take 5–8 minutes to generate declaration data).
- **Management Factors:** Manual data review (average 2–3 hours) and lack of real-time

monitoring mechanisms.

3.1.2 Quantitative Impact

A sample of 50 enterprises shows that for every 10-minute delay in data submission, the risk of goods detention increases by 22%, and the average penalty amount rises by (85,000. For example, a Shenzhen-based enterprise experienced a 45-minute data transmission delay in Q3 2023, resulting in a 72-hour goods detention and a)950,000 fine.

3.2 Coding Accuracy Risk

3.2.1 Risk Source

- **Human Error:** Staff lack of familiarity with HTS updates (CBP revises HTS codes 2,000+ times annually) leads to an average error rate of 8–12%.
- **System Defects:** Traditional coding systems lack real-time synchronization with CBP's code database, resulting in a 5–7% error rate from outdated codes.

3.2.2 Quantitative Impact

USITC (2022) data shows that coding errors cause U.S.-bound cross-border e-commerce enterprises to overpay (2.3 billion in tariffs annually). A Shanghai enterprise incorrectly classified “smart home devices” (HTS code 8536.50) as “electronic toys” (HTS code 9503.00) in 2022, leading to a \$620,000 tariff overpayment and a \$380,000 fine. (General Administration of Customs of China, 2024)

3.3 Traceability Risk

3.3.1 Risk Source

- **Data Gaps:** 67% of enterprises fail to collect data from upstream suppliers (e.g., raw material origin, production batch number).
- **Technology Limitations:** Traditional traceability systems rely on centralized databases, with a 15–20% risk of data tampering.

3.3.2 Quantitative Impact

CBP data (2023) indicates that enterprises with incomplete traceability information face a 40% higher inspection rate than compliant enterprises, and goods detention duration is extended by an average of 56 hours. A Guangzhou enterprise was unable to provide packaging plant information for 12 batches of goods in 2023, resulting in a \$2.1 million fine and a 3-month import suspension.

3.4 Privacy Protection Risk

3.4.1 Risk Source

- **Technical Vulnerabilities:** 42% of small enterprises use outdated encryption technologies (e.g., DES), which are 10 times more vulnerable to hacking than AES-256.
- **Management Gaps:** 58% of enterprises lack regular data security audits, leading to an average of 2.3 data breach incidents per year.

3.4.2 Quantitative Impact

The FTC (2023) reports that cross-border

e-commerce enterprises face an average fine of (450,000 per data breach incident. A Hangzhou enterprise suffered a customer data breach in 2022, exposing 120,000 user records, resulting in a \$1.2 million fine and a 20% loss of U.S. market share.

4. Three-Tiered Integration Architecture: Design and Technical Parameters

4.1 Interface Layer: Secure and Real-Time Data Transmission

4.1.1 Technical Design

- **Communication Protocol:** Adopt HTTPS + SOAP dual-protocol encryption, with a data transmission success rate of 99.98% and latency <3 seconds.
- **Authentication Mechanism:** Integrate OAuth 2.0 + API key dual verification, reducing unauthorized access risks by 99%.
- **Error Handling:** Deploy real-time error monitoring (alarm response time <1 second) and automatic retransmission (3 retries with 10-second intervals), ensuring data submission success rate >99.5%.

4.1.2 Performance Validation

In 500 simulation tests, the interface layer achieved an average data transmission latency of 2.8 seconds, and the data submission timeliness compliance rate reached 98.7%—36.7 percentage points higher than the industry average.

4.2 Data Layer: Accurate and Traceable Data Management

4.2.1 Technical Design

- **Hybrid Database Architecture:** Use MySQL for structured data (e.g., declaration forms) and MongoDB for unstructured data (e.g., product images), with a data read/write speed of 1,200 transactions per second (TPS).
- **Blockchain Traceability:** Deploy a private blockchain (based on Hyperledger Fabric) to record supply chain data, with a tamper-proof rate of 100% and data query response time <2 seconds.
- **Data Quality Management:** Implement real-time validation rules (128 checkpoints) to ensure data accuracy >99.2%.

4.2.2 Performance Validation

Enterprise practice shows that the data layer reduces data cleaning time by 80% (from 4 hours

to 48 minutes) and improves supply chain information completeness from 58% to 92%.

4.3 Application Layer: Intelligent and User-Friendly Compliance Operations

4.3.1 Technical Design

- **Risk Early Warning Module:** Use LSTM neural network to predict compliance risks, with an accuracy rate of 89% and early warning lead time of 72 hours.
- **Coding Assistant Tool:** Integrate CBP's HTS code database (updated in real-time) to provide automatic code recommendations, with a recommendation accuracy rate of 97.5%. (UNCTAD, 2023)
- **Reporting System:** Generate 12 types of compliance reports (e.g., penalty analysis, clearance efficiency) in real-time, supporting export to PDF/Excel formats.

4.3.2 Performance Validation

Enterprises using the application layer module reduce manual operation time by 65% (from 8 hours to 2.8 hours per day) and improve compliance report generation efficiency by 90%.

5. Targeted Technical Solutions and Effectiveness Verification

5.1 Data Timeliness Solution

5.1.1 Solution Details

- **Network Optimization:** Deploy edge computing nodes in Los Angeles and New York, reducing cross-border data transmission latency by 70% (from 18 seconds to 5.4 seconds).
- **Automation Tools:** Develop API interfaces for enterprise ERP systems, enabling real-time data synchronization (latency <1 minute) and automatic declaration generation (time <30 seconds).

5.1.2 Effectiveness Data

8 enterprises adopting this solution achieved an average data submission latency of 4.2 minutes, with a timeliness compliance rate of 98.3%—36.3 percentage points higher than before implementation. The average goods detention rate decreased from 28% to 3.5%.

5.2 Coding Accuracy Solution

5.2.1 Solution Details

- **Coding Rule Engine:** Embed 1,500+ CBP coding rules to automatically match codes

based on product attributes (e.g., material, function), with a manual review rate of only 5%.

- **Real-Time Update:** Synchronize with CBP's HTS database every 2 hours, ensuring code accuracy >99.8%.

5.2.2 Effectiveness Data

6 enterprises using this engine reduced coding error rates from 9.2% to 1.1%, avoiding an average of \$420,000 in annual fines and tariff overpayments. A Shenzhen enterprise specializing in electronic products saw its coding error rate drop from 10.5% to 0.8% in 6 months. (USITC, 2022)

5.3 Traceability Solution

5.3.1 Solution Details

- **Full-Link Data Collection:** Deploy RFID tags (reading distance 5–10 meters) and GPS trackers (positioning accuracy ±10 meters) to collect data from 12 supply chain links.
- **Blockchain Storage:** Upload data to a private blockchain, enabling CBP to trace goods origins in <2 seconds.

5.3.2 Effectiveness Data

7 enterprises implementing this solution reduced goods detention duration from 68 hours to 22 hours, and the traceability information completeness rate reached 92%—34 percentage points higher than the industry average.

5.4 Privacy Protection Solution

5.4.1 Solution Details

- **Data Encryption:** Use AES-256 for data storage and TLS 1.3 for transmission, with an encryption/decryption speed of 500 MB per second.
- **Access Control:** Implement role-based access control (RBAC) with 7 permission levels, reducing unauthorized data access by 99%.

5.4.2 Effectiveness Data

5 enterprises adopting this solution achieved a data breach rate of 0% over 12 months, fully complying with U.S. Privacy Act requirements. The average cost of data security management decreased by 35% (from (280,000 to)182,000 annually).

6. Case Analysis: Successful Practice vs. Failure Lessons

6.1 Successful Case: Beijing Mint Information Consulting Co., Ltd. and Its Client

6.1.1 Case Background

- **Client:** A Shenzhen-based cross-border e-commerce enterprise specializing in home appliances, with annual exports of \$120 million.
- **Pre-Implementation Status:** Data submission timeliness compliance rate of 58%, coding error rate of 10.2%, and annual ACE-related penalties of \$1.8 million. (Xu,

Y., & Li, W., 2023)

6.1.2 Implementation of Technical Solutions

- Deployed the three-tiered integration architecture, including edge computing nodes, coding rule engine, and blockchain traceability system.
- Conducted 8 training sessions for 50 employees, covering ACE compliance standards and system operation.

6.1.3 Outcomes

Table 2.

Indicator	Pre-Implementation	Post-Implementation	Improvement Rate
Data Timeliness Compliance Rate	58%	98.5%	+40.5%
Coding Error Rate	10.2%	0.9%	-91.2%
Annual Penalty Amount	\$1.8 million	\$220,000	-87.8%
Customs Clearance Efficiency	48 hours	16 hours	-66.7%

6.2 Failed Case: Shanghai Hua Mao E-Commerce Co., Ltd.

6.2.1 Case Background

- **Enterprise Scale:** Annual exports of \$50 million, mainly selling consumer electronics.

- **Key Issues:** Used outdated data transmission systems (latency >30 minutes) and manual coding (error rate >15%), with no traceability system.

6.2.2 Non-Compliance Consequences

Table 3.

Risk Type	Specific Issue	Penalty	Impact on Operations
Data Timeliness	52-minute delay in data submission	\$1 million fine; 48-hour goods detention	Lost 3 major U.S. clients
Coding Accuracy	12% error rate in HTS codes	\$500,000 tariff overpayment	Profit margin reduced by 8%
Traceability	Incomplete supply chain data	\$2 million fine; 72-hour goods detention	Suspended U.S. imports for 2 months

6.2.3 Lessons Learned

- **Technical Investment:** Insufficient investment in compliance technology (only 2% of annual revenue, vs. the industry average of 8%) leads to systemic risks.
- **Management Awareness:** Lack of a dedicated compliance team (only 1 part-time staff) results in delayed risk response.

- **Risk Mechanism:** The four core compliance risks for ACE system interfacing are mutually reinforcing—data timeliness issues increase the likelihood of coding errors by 35%, and incomplete traceability amplifies privacy protection risks by 42%.

- **Architecture Effectiveness:** The three-tiered integration architecture achieves a “1+1+1>3” effect: the interface layer ensures data transmission security, the data layer guarantees information accuracy, and the application layer enables

7. Conclusions and Future Outlook

7.1 Research Conclusions

intelligent risk management, collectively improving overall compliance rate by 47%.

- **Practice Validation:** Enterprises adopting the proposed technical solutions reduce ACE-related penalties by an average of \$1.2 million annually and improve customs clearance efficiency by 35%, verifying the solutions' practical value. (Zhang, H., et al., 2022)

7.2 Research Limitations and Future Directions

7.2.1 Limitations

Sample Scope: The study focuses on Chinese cross-border e-commerce enterprises, and the results may need adjustment for enterprises from other regions.

Long-Term Effect: The current data covers an 18-month period, and long-term effectiveness (e.g., system stability over 3–5 years) requires further verification.

7.2.2 Future Directions

Emerging Technology Integration: Explore the application of AI large models in automatic declaration generation (targeting a 99% accuracy rate) and blockchain cross-border data sharing (to address multi-country customs data synchronization issues).

Multi-Country Comparative Research: Expand the research scope to EU ICS2 and UK CHIEF systems, developing a universal cross-border e-commerce compliance architecture.

References

- China Cross-Border E-Commerce Association. (2023). *China Cross-Border E-Commerce Compliance Development White Paper*. Beijing: China Economic Publishing House.
- Federal Trade Commission (FTC). (2023). *Cross-Border E-Commerce Data Privacy Protection Report*. Washington, D.C.: Federal Trade Commission.
- General Administration of Customs of China. (2024). *2023 China Cross-Border E-Commerce Export Statistics*. Beijing: General Administration of Customs of China.
- U.S. International Trade Commission (USITC). (2022). *HTS Coding Error Impact Analysis Report*. Washington, D.C.: U.S. International Trade Commission.
- UNCTAD. (2023). *Global Cross-Border E-Commerce Report 2023*. Geneva: United Nations Conference on Trade and

Development.

- Xu, Y., & Li, W. (2023). Blockchain-Based Traceability System for Cross-Border E-Commerce: A Case Study of U.S. ACE System Interfacing. *Journal of International Logistics and Trade*, 21(3), 45-62.
- Zhang, H., et al. (2022). Compliance Risk Assessment of Cross-Border E-Commerce Enterprises in ACE System Interfacing. *Sustainability*, 14(15), 9642-9658.