Strategic Trade Control of Transshipments: Know Your Customer-Based Best Practices for Counterproliferation

KUSHANI DE SILVA AND ROHAN PERERA[1]

Abstract

International regulations play a crucial role in enhancing understanding of counterproliferation strategies in the context of maritime security. Thus study identifies Know Your Customer (KYC)-based sanction-sound best practices in transshipment, which are essential for effectively countering proliferation and also valuable in reducing smuggling trends by enhancing end-user screening processes. Best practices have been identified through a study where data was gathered through a questionnaire completed by 30 experts from Bangladesh, China, Iraq, India, Indonesia, Jordan, Malaysia, Pakistan, Philippines, and Sri Lanka. Additionally, five experts provided insights on cross-border customs compliance and maritime security concerns. It was found that KYC-based best practices and red flag indicators are essential for identifying the final recipient or purpose of sensitive goods or dual-use goods/technologies and that national

1 **Dr. Kushani De Silva** obtained a Ph.D in Disaster Management (UK) with a special emphasis on global security. She holds a Master's in Gender studies specializing in vulnerability reduction and a Bachelor's in Agriculture Technology specializing in dual-use chemicals and agrochemical security. She is also trained on the implementation of disarmament treaties at the T.M.C Asser Institute, Netherlands and studied the application of space technology in risk reduction at the Centre for Space Science and Technology Education in Asia and the Pacific (CSSTEAP), India. She is a pricipal investigator of security risk reduction, disarmament, and counterproliferation of WMD-related research work including the present study. She is a lead Subject Matter Expert in Chemical Security at CRDF Global and the founder/CEO Gloir. K working on disarmament and counterproliferation inspirational training, education, and research programs. **Dr. Rohan Perera** received his Ph.D. in Chemistry from Wichita State University in 2004, studying the neurochemical basis for neurodegenerative diseases. In 2005, he joined the Department of Chemistry at the University of Colombo as a Senior Lecturer in Chemistry, Biochemistry, and Toxicology. In 2014, Dr. Perera served as a former Senior Program Officer at the Organisation for the Prohibition of Chemical Weapons (OPCW). During his tenure at the OPCW, he coordinated and worked on chemical safety and security management programs and analytical skills development courses managing projects, and training chemical safety and security professionals. He is also a subject matter expert affiliated with U.S. CRDF Global and a subject matter expert to Gloir. K.

licensing authorities should publish and regularly update lists of red flags, taking into account research, case reports, incidents, and emerging threats. They should also manage the risks associated with sensitive technologies, such as the cyber security of Internal Compliance Programs (ICPs).

Keywords

Know-Your-Customer, strategic trade controls, sanctions, transshipment, counterproliferation

Introduction

Maritime import-export operations have become essential in supply chains, particularly in transshipment operations. These operations involve sophisticated tactics using vessels that can be misused in ways such as the use of disinformation to submit legitimate documents, misuse of automatic identification systems for ship-to-ship transfers, and non-compliance with corporate management systems to confuse vessel ownership.

Internal Compliance Programs (ICPs) play a crucial role in transshipment. ICPs serve as a monitoring tool to prevent the transfer of strategic goods to prohibited end-users or end-uses. They are an in-house manual that consists of Standard Operating Procedures (SOPs) and internal protocols that enable the identification of emerging risks and efficiently manage them using export control-related risk reduction strategies.[21]It is important for companies to conduct self-audits, taking voluntary disclosure and incident reports into consideration. These audits help ensure that the company is gathering and analyzing information accurately with the help of capable experts. Additionally, software automation is essential for ensuring the security of delivery and efficiency of processes when dealing with largevolumes of diverse export control regulations across the globe.

Examples of useful software include risk assessment, compliance screening, export controls, and license management software. Non-compliance with the ICP can result in financial penalties, legal repercussions, reputational damage, and socio-economic and environmental losses.

The main objective of this article is to investigate and present best practices related to Know-Your-Customer (KYC)-based, sanctions compliant, and resilient strategic trade control of transshipment for countering proliferation. The best practices presented have been compiled through a systematic study whose methodology and findings are discussed. The article specifically focuses on the objective of exploring KYC-based sanction-compliant best practices for the secure handling of strategic goods and technology during transshipments. It is structured into several key sections comprising an introduction, background to KYC, ICPs, and red flags, methodology, results and discussions, findings, and conclusions.

---

2 "CBRN Proliferation Financing: A Perspective from Southeast Asia," United Nations Interregional Crime and Justice Research Institute (UNICRI), October 2023, <https://issuu.com/unicri/docs/cbrn_proliferation_financing._a_perspective_from_s>.

Know Your Customer (KYC): Ensuring Supply Chain Security

KYC should be understood as going beyond just end-user and end-use; it should also include suppliers. It is important to identify not only immediate suppliers but also subsequent levels of suppliers that make up the entire supply chain community. By maintaining a comprehensive database of suppliers and conducting a thorough stakeholder risk analysis, it is possible to better identify each supplier and create risk profiles for them. This proactive approach helps to prevent and mitigate third-party breaches, which can occur when bad actors gain unauthorized access to systems and sensitive information. Notable examples of supply chain attacks, such as those that targeted Accellion, SolarWinds, and Microsoft Exchange, serve as reminders of the importance of this practice.[3]

It is important to emphasize that Know Your Customer (KYC) and Know Your Supplier (KYS) are essential verification strategies for identifying customers and suppliers as well as assessing their suitability for business or trade transactions. Individuals and organizations should refrain from engaging in trade with individuals or entities from sanctioned or restricted countries.[4]

Despite high-level management commitment to managing supply chain risk, the percentage of risk reduction efforts decreased from 41% in 2017 to 26% in 2019.[5] This decline may help explain why it is necessary to enhance due diligence in higher supply chains. Since due diligence is a crucial risk mitigation strategy, it is important to include penalties or negative consequences for non-compliance in contract agreements. Consequently, coordinated reporting and monitoring can be strengthened.

Red Flag Indicators for Ensuring Supply Chain Security

Red flag indicators can be discussed considering end-users and end-uses, products, delivery, payment terms, and so forth and are useful for effective ICP implementation.[6] It is preferable to develop checklists for each activity as applicable to the country or organizational context.

The following are representative, though non-exhaustive, questions that could be part of the checklist:

- Are the shipped commodities compatible with the technical capacities or natural resources of the origin/destination country?

---

3 "Supply Chain Due Diligence is Faltering: Here's How to Tackle It," AML Right Source, February 20, 2020, <https://www.amlrightsource.com/news/supply-chain-due-diligence-is-faltering-heres-how-to-tackle-it/>.

4 "Strategic Trade Control Enforcement (STCE) Implementation Guide," World Customs Organization, <https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/tools-and-instruments/stce-implementation-guide/stce-implementation-guide-2023-e-final.pdf?db=web>.

5 "Supply Chain Resilience Report," Business Continuity Institute, October 2019, <https://www.thebci.org/static/e5803f73-e3d5-4d78-9efb2f983f25a64d/BCISupplyChainResilienceReportOctober2019SingleLow1.pdf>.

6 Nicole Mantei, "Export Controls: New Red Flag Checklist for your ICP," AEB, August 18, 2022, <https://www.aeb.com/en/magazine/articles/red-flags-trade-compliance-icp.php>.

- Is the shipping route appropriate for the product and destination?
- Are free trade zones or free ports utilized for the shipment?
- Was shipment clearance requested at the last minute?
- Was the bill of landing (B/L) changed?

New dimensions of capacity limitations due to global conflicts such as attacks on vessels in the Red Sea need to be understood as an emerging STC risk. For instance, major freight carriers, including Maersk and Hapag-Lloyd, suspended operations in 2024 through the Suez Canal in order to avoid the Red Sea. They are now rerouting vessels around the Cape of Good Hope, which adds 5,500 to 6,500 kilometers and seven to ten days to a typical trip between Europe and Asia. This extra distance could absorb anywhere from 700,000 to 1.9 million twenty-foot equivalent units (TEUs) of shipping capacity.[7]

Epidemics like Covid-19 or other disasters can heighten vulnerabilities of integrated supply chains due to the emergence of new and dynamic red flag indicators. Therefore, Mutual Recognition Arrangement/Agreements (MRAs) play a crucial role in planning, negotiation, and implementation of cross-border customs administration, ensuring the security of end-to-end supply chains with partner customs administrations.[8]

The main reasons for supply chain risks are unplanned IT or telecommunications outages, adverse weather, cyber-attacks and data breaches, loss of talent/skills, transport network disruption,political change, and new laws or regulations.[9] These situations can be alleviated through strengthening ICPs.

The Relationship between Internal Compliance Programs (ICPs) and Strategic Trade Controls

ICPs serve as a monitoring tool to prevent the intentional or unintentional transfer of strategic goods to prohibited end-users or for prohibited end-uses. It consists of Standard Operating Procedures (SOPs) and internal protocols to effectively identify emerging risks and manage them through export control-related risk reduction strategies. Performing a self-audit is important, which should consider voluntary disclosure, incident reports, and notes. It is crucial to have information analysis systems in place and involve knowledgeable experts. Additionally, software automation is essential for ensuring the secure and efficient delivery of processes, particularly when dealing with large volumes of diverse export control regulations.

---

7 Arvis F. Jean, Rastogi, Cordula, and Ulybina, Daria, "Will a Prolonged Rerouting of Ships from Suez Trigger a New Supply Chain Crisis?" The World Bank, January 19, 2024.

8 "AEO Mutual Recognition Strategy Guide," World Customs Organization, <https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/strategy-guide-for-aeo- mutual-recognition.pdf?db=web>.

9 "Supply Chain Resilience Report," Business Continuity Institute, 2019, <https://www.thebci.org/static/e5803f73-e3d5-4d78-9efb2f983f25a64d/BCISupplyChainResilienceReportOctober2019SingleLow1.pdf>.

Research institutions should share best practices and consider export controls risks within their company's risk registry. They should also provide targeted training and awareness to individuals involved in the handling of exports, supplies, brokering, or publishing controlled goods, software, and technology maintenance. Collaborative projects with the relevant supply chain community, such as the insurance community, can be beneficial. These projects can include clauses in business agreements that address non-compliance and violations. Non-compliance can result in financial penalties, legal consequences, and damage to reputation. Examples of non-compliance activities are provided below.

- Not having SOPs or procedures to follow
- Insufficient administrative procedures to practice or not practicing existing procedures
- Failure to follow SOPs or operational procedures
- Not having required certification/licenses to handle operations
- Failure to report to relevant authorities about suspicious activities

Transshipment Risks Beyond Physical Operations

Transshipment risks are often viewed considering physical operations. Nevertheless, reporting requirements, non-existent global transshipment guidelines, and privately owned ports and terminals act as non-physical compliance risks. This is illustrated below.

Reporting Requirements

It is important to generate, observe, and accept reports in a standardized manner with SOPs. For example, transshipment-related documents must contain notifications/authorization, declarations, observer reports, and landing reports. It is essential to report red flags to state authorities of both vessels by any relevant coastal, port, national, regional, or international organization. Red flag reporting and SOPs should be developed and not only be limited to strategic or dual-use goods and technologies but also consider the misuse potential of new goods and technologies within the country's context. This challenges global security norms.

Global Guidelines for Transshipments

The need for global transshipment guidelines for catching fish was identified many years ago.[10] Nevertheless, equally important transshipment guidelines should be developed, including best practices for handling strategic and/or dual-use goods and technology. Clear definitions, formalized documentation procedures with SOPs, and the use of technologies for the physical monitoring of transshipments have become essential in this regard.

Privately Owned and Operated Ports and Terminals as a Barrier

Oversight and enforcement measures could be challenged when ports and terminals are not

10 "Transshipment: A Closer Look: An In-Depth Study in Support of the Development of International Guidelines," Food and Agriculture Organization, 2020, <https://www.fao.org/3/cb2339en/cb2339en.pdf>.

owned by the government. Little or no oversight of domestic or foreign-flagged vessels landing, transshipping, or receiving port might lead to inadequate information on the volume and composition of the goods transshipped. This can create economic, social, and environmental losses. The role of voluntary non-state sector organizations is pivotal in raising awareness and training on vulnerability-sensitive risk-reduction compliance strategies.[11,12]

Sometimes, it becomes evident that state-owned ports and terminals suffer from poor oversight This is particularly noticeable when there are gaps in the enforcement and implementation of the International Convention for the Prevention of Pollution from Ships (ICP) and when shippers fail to share relevant details. A recent incident exemplifying this issue occurred in May 2021 at Colombo Port in Sri Lanka, where the express pearl transshipment disaster took place. This disasterresulted in the leakage of 25 metric tons of nitric acid and approximately 50 billion plastic pellets into the environment, causing not only environmental damage but also significant socioeconomiclosses.

Methodology

This section describes the sample selection, data collection, and analysis for the study upon which the best practices identified in this article was performed..

Sample Selection, Data Collection and Analysis

The study purposefully selected 10 Asian countries that have STC mechanisms, including customs regulations and procedures that comply with the World Customs Organization. These countries are also a part of international disarmament treaties and have established systems for transshipment handling.

Additionally, the countries had experts who were willing to contribute to the study. Data collection lasted for eight weeks, during which an expert perception survey was conducted. The survey targeted 30 experts from the following 10 Asian countries: India, Bangladesh, Malaysia, Philippines, Iraq, Pakistan, Jordan, China, Indonesia, and Sri Lanka. Furthermore, five expert interviews were conducted with individuals (EX1, EX2, EX3, EX4 & EX5) from the European and Asian region and Brazil. Data analysis was carried out using Excel and thematic content analysis techniques. Data interpretational techniques included concept maps, percentages, and literature arguments.

Results and Discussion

This section describes the best practices highlighted by the experts in light of KYC, sanctions,

---

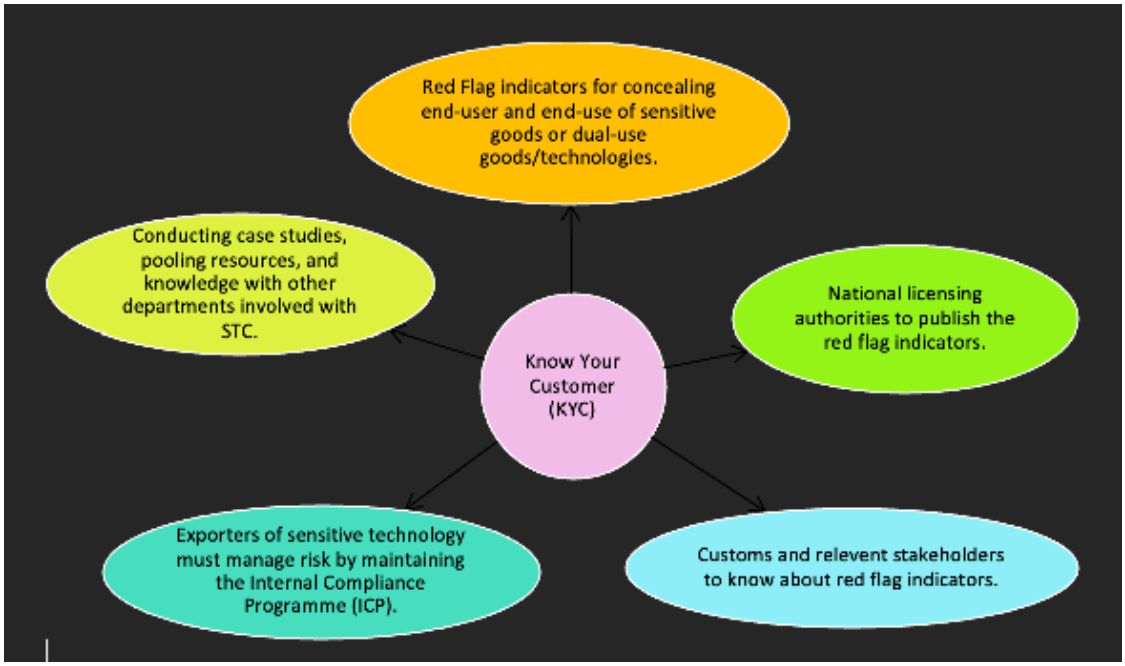
11 "Global Study on Transshipment: Regulations, Practices, Monitoring and Control," Food and Agriculture Organization, June 2018, <http://www.fao.org/fileadmin/user_upload/COFI/COFI33Documents/SBD15en.pdf>.

12 Food and Agriculture Organization, "Voluntary Guidelines for the Marking of Fishing Gear," May 18, 2018, <https://www.fao.org/fileadmin/user_upload/COFI/COFI33Documents/MX136_COFI_2018_Inf30en.pdf>.

STC, digital information-sharing, cyber security, and accountability.

KYC Based on Transshipment Best Practices (Experts' Opinions)

Figure 1: KYC-based transshipment best practices concept map (Survey data, 2023)



As per Figure 1, the following aspects were highlighted by experts as STC-sensitive KYC best practices in handling transshipments.

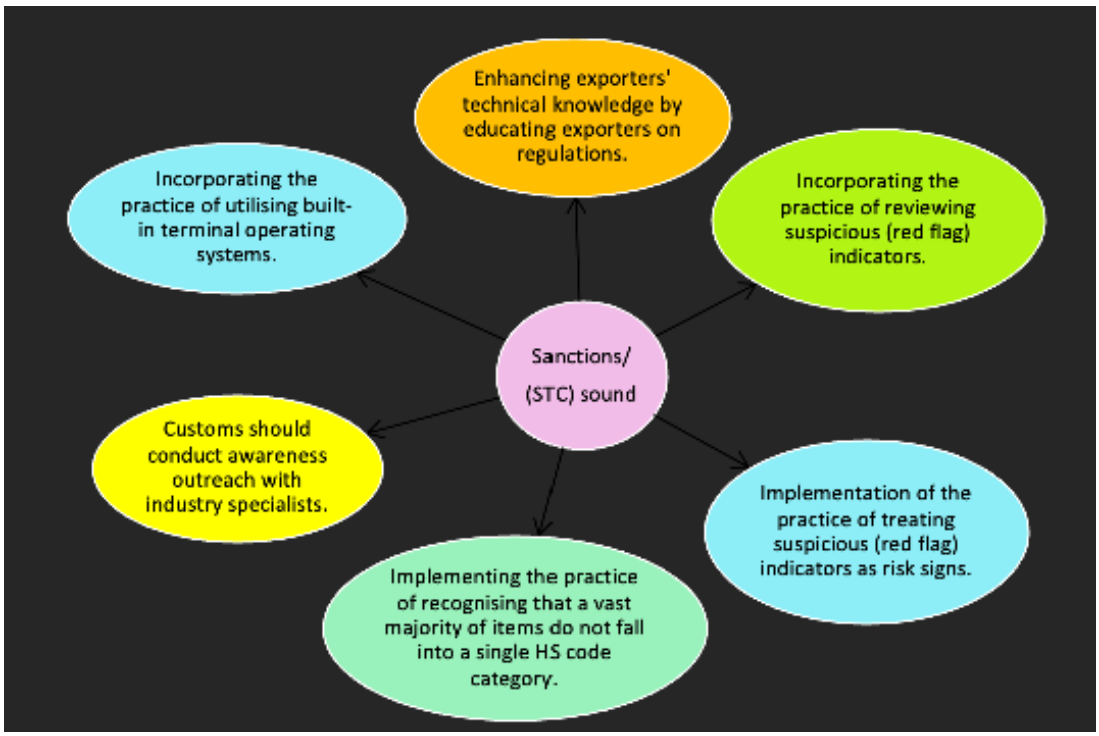
- Red flag indicators for concealing ultimate end-user or end-use of sensitive goods or dual-use goods/technologies (83.33%).
- National licensing authorities should publish a list of red flag indicators (93.33%).
- Red flag during transshipment is a must that relevant stakeholders, including customs, should be aware of (96.66%).
- Sector-specific awareness by customs and licensing authorities is essential (89.99%)
- It is essential to have industry and academic institutions outreach efforts to prevent the proliferation of export-controlled technology and components (93.32%).
- Case studies and pooling resources and knowledge with other departments involved with Strategic Trade Control (STC) are essential (93.33%).
- Those who export sensitive technologies must manage risks related to compliance and enforcement by maintaining the Internal Compliance Programme (ICP) to address the risks, for example, identifying and classifying controlled goods, and risky trading partners and locations (93.32%).

Those who were neutral or disagreed on the points mentioned above responded by comparing the existing situation in their countries and working environments to assess the extent to which the best practices mentioned above had been implemented. In other words, they too recognized the importance of implementing these best practices in their working environments.

Strategic Trade Controls/Sanctions

According to the experts surveyed, the best practices associated with strategic trade controls and sanctions can be summarized as follows:

Figure 2. Sanctions/STC sound transshipment best practices concept map from survey data



Based on the perception survey, the majority of experts strongly identified the need to enhance experts' knowledge on sanctions/STC. They also highlighted the importance of reviewing suspicious indicators and treating them as risk signs, promoting exporters to rely on more comprehensive technical details for export control, and investing more in terminal operations and customs awareness outreach as best practices.

- Enhancing exporters' technical knowledge by educating exporters on regulations (100%).
- Incorporating the practice of reviewing red flag indicators to identify elements of a shipment requiring heightened compliance checks or verification (93.33%).
- Implementation of the practice of treating red flag indicators as risk signs for the prevention of unauthorized diversion of exports to a sanctioned or blacklisted entity (90%).

- Recognition that a vast majority of items do not fall into a single Harmonized System (HS) code category, prompting exporters to rely on more comprehensive technical details for export control (86.66%).

- Customs should conduct awareness outreach with industry specialists regarding the application of the correct tariff codes (93.33%).

- Incorporating the practice of utilizing built-in terminal operating systems to facilitate informed decision-making and enhance security management (83.33%).

Furthermore, the expert interviews reflected ways that ICPs can be used to make STC effective with KYC compliance.

The Importance of ICPs for Resilient KYC-Based Sanction-Compliant STC of Transshipments

According to EX1, the Internal Compliance Program (ICP) can be viewed as a framework of coordinated corporate processes to support the export compliance function for the following reasons:

- Risk management: An ICP provides a systematic approach to identify, assess, and manage risks associated with export controls. This includes risks related to the unauthorized export of controlled goods, technology, or services.

- Regulatory compliance: An ICP helps ensure a company complies with all applicable export control laws and regulations. This includes understanding and adhering to licensing requirements, export restrictions to certain countries or entities, and record-keeping obligations.

- Corporate governance: An ICP is an integral part of good corporate governance. It demonstrates a company's commitment to ethical business practices and corporate responsibility. It also helps foster a culture of compliance within the organization. The above points were also highlighted by EX3 and EX4.

Furthermore, EX2 explained the Internal Compliance Program (ICP) as a:

> *"set of internal policies and procedures to ensure compliance with national or international laws and regulations in the framework of trade controls. To this extent an ICP is not only a matter of interest for the export compliance function in an organization but should involve the whole chain of the internal functions engaged in trade activities, starting from the top-level management, that should be committed to compliance, passing through the sales sectors, the shipping departments, and so on".*

The Importance of a Communication Plan for Resilient KYC-Based Sanction Resilient STC of Transshipments

EX1 described that a communication plan for communicating with relevant stakeholders on

compliance procedures, guidelines, regulatory updates, contact information, and protocols/ standards of communication is indeed crucial due to following reasons:

- Clarity and consistency: A well-defined communication plan ensures that all stakeholders consistently receive the same information. This helps prevent misunderstandings and ensures that everyone remains aligned with compliance procedures and guidelines.

- Timely updates: Regulatory environments can change rapidly. A communication plan ensures that stakeholders are informed about these changes promptly, allowing them to adjust their practices accordingly.

- Responsibility and accountability: Clear communication about contact information and communication protocols clarifies who is responsible for what, which is crucial for accountability.

EX2, EX3, EX4, and EX5 also highlighted similar points.

In addition, EX2 explained that:

> *"a communication plan for communicating with relevant stakeholders the commitment to compliance, is something important, sometimes crucial, in engaging new customers or for letting know to other relevant stakeholders, including national and/or international authorities (e.g., licensing, enforcement, financial, etc.), to what extent a company is committed to compliance and to better explain the way how it is taken into consideration and ensured by all the internal functions. So not only how much a company is committed, but how commitment is being ensured also."*

Digital Information to Ensure Secured Information-Sharing and Dual-Screening (e.g., Manifest and Invoices) with the Support of Relevant Stakeholders of Transshipment Handling

According to EX1 "updating digital information securely is crucial for effective transshipment handling. Here are three best practices:

- Data encryption: All sensitive data, including manifests and invoices, should be encrypted during transmission. This ensures that even if the data is intercepted, it cannot be read without the decryption key.

- Access control: Implement strict access control measures. Only authorized personnel should have access to sensitive information. This can be managed through user roles and permissions in the information tracking systems.

- Regular updates and patches: Keep all systems, such as ASYCUDA, maritime traffic monitoring systems, and terminal operating systems, up to date with the latest patches and updates. This helps to protect against known vulnerabilities that could be exploited.

In addition, regular audits and staff training on data security can further enhance the security of information-sharing in transshipment handling. In addition, blockchain could be used to secure

data and match them with that provided by different stakeholders and automatically assess its consistency.
EX3 and EX4 also agreed on the above points. Furthermore, EX4 mentioned that the following was critical:

- Establish clear roles and responsibilities: Clearly define who is responsible for updating digital information and how this information should be shared.

- Implement data access controls: Implement data access controls to ensure that only authorized personnel can access sensitive information.

- Use secure communication channels: Use secure communication channels, such as encrypted email or file transfer protocols, to share sensitive information.

- Monitor data integrity: Regularly monitor data integrity to ensure that information is accurate and complete.

EX2 highlighted that the:

> *"clearness and completeness of documentation is one of it, to put enforcement authorities (and licensing authorities as well) in the best position to understand what is being shipped. Such documentation should include technical information (description of the goods, datasheet, and so on), and commercial information (e.g., invoice, purchase orders, contracts, etc.), to clearly understand not only what is related to the goods, but also identify the entities involved in the transaction and the shipment, including anyone which is a part of the strategic goods supply chain".*

Strengthening the Accountability of Shippers and Exporters to do their Jobs According to the Provisions of the License

EX1 mentioned that "strengthening the accountability of shippers and exporters is crucial for ensuring compliance with licensing provisions. Based on my experience, the most critical way to achieve this can be described as follows:

- Training and education: Regular training sessions can ensure that shippers and exporters understand the provisions of the license and understand their responsibilities. This should include training on the consequences of non-compliance.

- Audits and inspections: Regular audits and inspections can help to monitor compliance and identify any areas of concern. This not only holds shippers and exporters accountable but also provides an opportunity for continuous improvement.

- Penalties for non-compliance: Establishing clear penalties for non-compliance can deter and encourage adherence to license provisions. This could range from fines to suspension or revocation of the license.

- Promote compliance programs such as Authorized Economic Operators (AEO): In this

case, to avoid duplicating efforts and controls, it should also be explored whether it is possible to have a kind of mutual recognition or synergy between ICP and AEO."

EX2 mentioned that exchanging information between licensing and customs authorities is important especially regarding the respect of license provisions. EX2 also emphasized the significance of engaging with shippers and exporters through outreach activities, training programs, and the publication of information.

EX4 highlighted the importance of conducting pre-shipment audits. For instance, these audits help ensure that shippers and exporters comply with license requirements. Penalties for non-compliance, such as fines or license suspension, should also be imposed. Additionally, providing training and guidance to shippers and exporters on how to comply with license requirements is crucial.

Ways Customs Identify and Implement Operational Best Practices Related to Integrated Supply Chain Security Management with Relevant Stakeholders

According to EX3, customs should identify and implement operational best practices related to integrated supply chain security management with an emphasis on the following:

- Develop standardized procedures for supply chain security management and ensure their consistent implementation (training/adequate staff).
- Use modern technology, such as risk assessment algorithms and tracking systems, to increase supply chain security.
- Collaborate with industry stakeholders to share best practices and jointly tackle supply chain security challenges.
- Introduce modern monitoring equipment such as night vision cameras, drones, and scanners.

EX3 and EX4 propose the development of a global convention or treaty for transshipment compliance. This convention would establish minimum standards and guidelines. It is crucial to consider the contexts of both developed and developing countries equally when designing the convention and proposed systems. Additionally, a communication plan should be developed to promote a culture of integrity surrounding the convention.

EX3 highlights the sensitivity of transshipment information in terms of competitiveness, both politically and economically. Many developing countries have transshipment hubs that must include transshipment audits as a mandatory component of their supply chain security management.

EX1 emphasizes that customs can identify and implement operational best practices related to integrated supply chain security management. This can be achieved through collaboration with relevant stakeholders. Effective communication channels should be established with importers, exporters, carriers, and warehouse operators to identify potential risks and implement security measures. Regular meetings, workshops, and training sessions can facilitate this process. The

implementation of the Authorized Economic Operator (AEO) program serves as an example of such practices.
Furthermore, EX1 highlighted the following regarding risk assessment and management:

> *"Customs should conduct regular risk assessments to identify vulnerabilities in the supply chain. This involves analyzing data from various sources, including cargo reports, intelligence reports, and stakeholder feedback. The findings can then be used to implement risk-based controls and procedures. Also, use of technology: implementing advanced technologies such as automated tracking systems, data analytics, and AI can enhance supply chain security, blockchain, etc. These technologies can help in real-time tracking of goods, anomaly detection, and predictive analysis."*

EX2 stated that post-shipment verification is an important aspect of the periodical revision of certifications granted to economic operators. They also stated the need for focused and unique outreach activities and exchange of information with relevant stakeholders via roundtables, open hearings, and so forth.

Licensing Authorities to Adopt/Update/Develop Red Flag Indicators

According to EX1, an effective alert system is vital for implementing continuous monitoring of stakeholders' feedback and the impact of training. EX2 emphasized that the most relevant best practice is the development of a KYC policy in every company, which may include the adoption of ICPs by companies and stakeholders (including consultants and customs brokers). From this perspective, the entrance of new customers into a market could raise a red flag, as well as the knowledge of the industry in the country of destination or the availability of a large amount of money for purchasing items. Furthermore, unusual delivery options or requests for an unusual path to the country of destination can also be red flags.

EX4 stated that the collection and analysis of data on past shipments to identify patterns that may indicate non-compliance is crucial. Consulting with experts from Customs, law enforcement, and other relevant agencies to identify potential red flag indicators is also important. It is further recommended to regularly update red flag indicators to reflect changes in the law, regulations, and business practices. Red flag indicators should be considered as short-term risk assessment components for building a compliance culture with integrity.

EX3 explained that regularly reviewing and updating red flag indicators based on emerging risks and trends in strategic trade is pivotal. Collaboration with intelligence agencies and industry experts to obtain information on possible threats and vulnerabilities is also necessary. Additionally, developing a feedback mechanism to report and address false positives and false negatives in red flag indicators to refine their accuracy (including the introduction of machine learning or artificial intelligence) is recommended.

Findings

Based on the study, this section delinestes best practices related to KYC, sanctions, and transshipment handling that make strategic trade controls effective as a counterproliferation

strategy.

KYC Best Practices

1. During transshipment, it is essential for all relevant stakeholders including customs to be aware of red flags. These indicators are crucial for detecting attempts to conceal the ultimate end-user or end-use of sensitive goods or dual-use goods/technologies.

2. National licensing authorities should publish a list of red flag indicators. Additionally, sector-specific awareness by customs and licensing authorities is essential.

3. To prevent the proliferation of export-controlled technology and components, industry and academic institution outreach efforts, case studies, pooling of resources, and knowledge with other departments involved with STC are essential.

4. Those who export sensitive technologies must manage risks related to compliance and enforcement by maintaining the ICP to address the risks, for example, identifying and classifying controlled goods, and risky trading partners and locations.

Sanctions-Compliant Best Practices

1. Enhancing exporters' technical knowledge by educating them on regulations is crucial. For instance, customs should conduct awareness outreach programs targeting industry specialists. These programs should focus on topics such as applying the correct tariff code and encouraging exporters to rely on more detailed technical information for export control. This is important because the majority of items cannot be categorized under a single HS code.

2. Incorporating the practice of reviewing suspicious (red flag) indicators to identify elements of a shipment that require heightened compliance checks or verification and combining it with the practice of utilizing built-in terminal operating systems, can facilitate informed decision-making and enhance security management.

3. Implementation of the practice of treating suspicious (red flag) indicators as risk signs is aimed at preventing the unauthorized diversion of exports to a sanctioned or blacklisted entity.

Resilient STC Best Practices

1. ICP should be viewed as a framework of coordinated corporate processes and be published on the companies' intranet pages and include advanced cyber security mechanisms.

2. A communication plan for communicating with relevant stakeholders on compliance procedures and practices is essential.

3. Strengthening the accountability of shippers and exporters by providing them with competency-based training is critical.

4. Customs should identify and implement operational best practices related to integrated supply chain security management.

5. Licensing authorities must update and develop further suspicious (red flag) indicators based on the case reports/studies.

The ICP can be seen as a framework of coordinated corporate processes that aid the export compliance function. It is necessary to develop a communication plan to ensure resilient KYC-based sanction-compliant STC of transshipments. Additionally, measures must be taken to secure digital information, promoting secure information-sharing and dual-screening (e.g., manifests and invoices) with the involvement of relevant transshipment handling stakeholders. The accountability of shippers and exporters should be strengthened to ensure compliance with licensing provisions. Customs authorities should implement operational best practices related to integrated supply chain security management in collaboration with relevant stakeholders, and licensing authorities should adopt/update/develop red flag indicators.

Strategies Support the Implementation of Best Practices

Training first response units to liaise with all relevant stakeholders about possible incidents/accidents and carrying out regular mock drills, while strengthening cyber security for secure information exchange, are essential strategies to be implemented along with best practices. Furthermore, it is pivotal for STC authorities to have regular meetings in line with agencies such as the Ministry of Foreign Affairs, Industry, and Trade to enhance their understanding. In the long run, incorporating counterproliferation into formal, informal, and non-formal education is

important. For example, the university syllabus can include modules on ethics and strategic trade. Additionally, technology like radio frequency identification (RFID) and global positioning system (GPS) can be used to track the movements of cargo in real-time, preventing diversions during transshipment operations. Radio frequency identification (RFID) refers to a wireless system comprised of two components: tags and readers.

Track lock or T-star is a tracking device that can monitor transportation activities, such as tracking the precise location of transport containers during consignment. Currently, in developing countries, it is primarily used for monitoring the transportation of radioactive or nuclear materials.

In terms of issuing licenses for the transportation of dual-use goods, for example, in Sri Lanka, the Sri Lanka Atomic Regulatory Council (SLAERC) obtains all necessary information on individuals involved in transportation as part of their prior assessment of trustworthiness. They also gather information on vehicles to ensure they meet the required safety and security standards for transporting materials of security concern. Additionally, transport security tabletop exercises are conducted to provide hands-on experience in real-case scenarios.

The Sri Lanka Atomic Energy Regulatory Council (SLAERC), which succeeded the Sri Lanka Atomic Energy Authority, was established on January 1, 2015, through the Sri Lanka Atomic Energy Act No. 40 of 2014. As per the Act, SLAERC is required to prepare a transport security

plan and develop human resources within the organization, including those involved in transport activities.[13]

It is understood that some of the containers with dangerous cargo are stored in the port premises for longer periods as they have not been cleared by customs. As these containers are vulnerable to smuggling and explosions, it is essential to have a proper mechanism in place to remove and store them in separate safe locations. It would be better to establish a separate common body to make decisions on dangerous cargo issues within the country, with a strong intelligence service to monitor existing mechanisms and identify potential risks. Recruiting enough qualified staff and implementing screening technologies with maintenance capacities are crucial.

Summary

It has been found that implementing KYC-based, sanctions-compliant resilient strategic trade best practices is crucial for countering proliferation and preventing illicit trade. For KYC-based best practices, it is important to have red flag indicators that can help identify the ultimate end-user or end-use of sensitive goods or dual-use goods/technologies. National licensing authorities should publish and regularly update red flag lists based on research, case reports, incidents, emerging threats, and so on. Managing risks associated with sensitive technologies is essential through maintaining ICP with cyber security and developing a communication plan to coordinate with relevant stakeholders on compliance procedures and practices. Competency-based training and awareness are also necessary.

Implementing KYC-based, sanctions-compliant resilient strategic trade control best practices becomes pivotal when addressing supply chain security concerns in transshipment. Additionally, establishing a single window concept, introducing awards/rewards/special grants, conducting stakeholder analysis, developing standard operating procedures, creating a steering committee, and establishing a treaty or convention to set minimum standards for transshipment compliance are identified as important best practices.

Conclusions

Implementing KYC-based and sanction-sound management strategies can support resilient STC. When it comes to KYC-based best practices, red flag indicators play a crucial role in identifying the ultimate end-user or end-use of sensitive goods or dual-use goods/technologies. To ensure effectiveness, national licensing authorities should publish and regularly update red flag lists, taking into account research, case reports, incidents, emerging threats, and so on. Managing risks associated with sensitive technologies is essential through the maintenance of ICP with cyber security. ICP is vital for the resilient implementation of KYC-based sanction-compliant STC for transshipments. This approach also helps address the challenge of political influence in decision-making, which remains a hurdle to the implementation of risk reduction-based technical best practices.

---

13 U. W. K. Haryantha de Silva, "Sri Lankan Experience on Security of Radioactive Materials in Transport from a Regulator's Perspective," International Conference on Nuclear Security, 2020, <https://conferences.iaea.org/event/181/contributions/15756/contribution.pdf>.

Best practices also include treating red flag indicators as risk signs, utilizing built-in terminal operating systems to facilitate informed decision-making and enhancing security management, and by enhancing exporters' technical knowledge through education on regulations, including sanctions.

The development of a communication plan is crucial for coordinating and communicating with relevant stakeholders about compliance procedures and practices. It is also important to include politicians and other relevant stakeholders in the communication plan and foster a culture of integrity. A communication plan for resilient KYC-based sanction-compliant STC of transshipments helps identify the needs of stakeholders and enables the implementation of training and awareness programs to enhance their capacity.

Acknowledgments

The author would like to thank the experts from Customs, Strategic Trade Control, Ports, Chemical Biological Radiological Nuclear Energy (CBRNE), Environmental Protection authorities, and related operational focal points who have contributed to the present study. Any errors in content or analysis are nevertheless solely those of the author.