



SANCTIONS COMPLIANCE – PREVENTING ILLICIT TRANSPORTATION OF ADVANCED CONVENTIONAL WEAPONS (ACWS) AND COMPONENTS

**Practical Recommendations for the Transport and
Logistics Sector of Georgia**



Tbilisi
2024



CENTER FOR STRATEGY AND DEVELOPMENT

CSD is one of the leading independent think tanks in the country. Our values are based on the principles of equality, freedom, respect, accountability, and transparency. Our goals are to support Georgia's national security, strengthen the country's principles of effective and democratic governance, support its European and Euro-Atlantic integration, and create the conditions for Georgia's sustainable development.

With the support of the U.S. Department of State's Office for Cooperative Threat Reduction (CTR), CSD has been conducting several initiatives to enhance Georgia's capacity to identify and respond and ACW (Advanced Conventional Weapons) threats. Strengthen sanctions compliance implementation and programs.

DISCLAIMER:

This manual was composed with the generous support of the U.S. Department of State. The views and opinions expressed in this document are those of the author and do not necessarily reflect or represent the views and opinions of the Center for Strategy and Development (CSD) or the U.S. Department of State.

TABLE OF CONTENTS

ACRONYMS	01
FOREWORD AND OVERVIEW	02
CONTEXT AND OBJECTIVES OF THE DOCUMENT	04
● Definition And Examples Of Advanced Conventional Weapons	05
● Georgian Context	09
THE IMPORTANCE OF MANAGING YOUR COMPANY IN THE SANCTIONS AND NON-PROLIFERATION ENVIRONMENT	10
● Existing Sanctions Regimes	10
● Consequences of Non-Compliance	11
● Compliance Implications For Logistics	12
BASICS OF SANCTIONS COMPLIANCE	13
● Types of Sanctions	13
● How to Identify and Avoid Sanctioned Entities	13
● Managing Red Flags During Business Operations	14
● Maritime Related Red Flags	15
IMPLEMENTING A COMPLIANCE GUIDANCE	17
● Transaction Diagram	19
● Risk Assessment Checklist	20
PRACTICAL STEPS FOR COMPLIANCE	21
DUE DILIGENCE AND MONITORING	23
KEY TRAINING AREAS FOR EMPLOYEES	24

ACRONYMS

ACSS	Association Of Certified Sanctions Specialists
ACW	Advanced Conventional Weapons
AEW&C	Early Warning And Control
ATGMS	Anti-Tank Guided Missiles
BIS	Bureau Of Industry And Security
CAATSA	Countering American Adversaries Through Sanctions Act
CIS	Community Of Independent States
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
EU	European Union
KYC	Know Your Customer
KYCC	Know Your Customer's Customer
MANPADS	Man-Portable Air Defense Systems
METI	Japanese Ministry Of Economy, Trade And Industry
OFAC	Office Of Foreign Assets Control
SDN	Specially Designated Nationals
STS	Ship-To-Ship
WMD	Weapons Of Mass Destruction



Since 2022 Center for Strategy and Development (CSD) has conducted multiple trainings, published documents, and has consistently engaged with the Georgian Logistics sector, aimed at enhancing sectoral resilience to illicit Advanced Conventional Weapons (ACW) transactions. These activities were done with the explicit aim of increasing awareness of the existing sanctions and restrictive regimes that affect the economic security of the region and organizations within.

Throughout the two years of activity, there were multiple instances of CSD being made aware of attempts at suspicious transactions, clients or end/users, often shared by the organizations and companies involved. In discussions, various logistics companies highlighted the potential methods utilized by some clients to obfuscate the cargo or the final recipient of the item. Suggestions of PDF document forgery and methods to avoid the detection by sophisticated pieces of software. Logistics sector representatives often underlined that while the state may not be participating in current sanctions mechanisms, businesses and crucially, the logistic sector must ensure that it's compliant with the restrictive regimes placed upon individuals connected to the Russian military complex. Additionally, In discussions with the major logistics companies in Georgia, their current methods of detection, KYC, KYCC and other compliance methods were explored, indicating gaps that were necessary to overcome.

This document aims to support logistics sector companies and organizations to further investigate their internal compliance policies, offer operational and process updates and encourage constant improvement in sanctions compliance measures based on open-source and widely available information. Allowing businesses to make informed decisions based on risk analysis and a full picture of the possible dangers of any uncertified transaction.

Context and Objectives of the Document

This module explores the sanctions environment surrounding advanced conventional weapons, defining the term, exploring different components that need to be monitored and underlining Georgia's role, responsibilities, and the overall context

The Importance of Managing Your Company in The Sanctions and Non-Proliferation Environment

The module contains information about the existing sanctions regimes, OFAC, UNSCR, EU and other sanctions. Exploring the potential consequences of non-compliance and the implications of the sanctions regimes and compliance for the logistics sector.

Basics of Sanctions Compliance

The module understates the types of sanctions that are enacted against foreign entities and gives actionable recommendations for logistics companies to conduct screening and due diligence.

Implementing A Compliance Guideline

The module overviews multiple compliance processes, a general, company-wide guidance to ensure compliance. A transactions diagram to guide the relevant compliance officer through pre-transaction checks and a risk assessment checklist for compliance officers

Practical Steps for Compliance

The module offers general recommendations for a company and its compliance officers, covering an overview of the compliance program and the tools necessary for its implementation. It also includes two types of risk matrices.

Due Diligence and Monitoring

The module emphasizes the importance of due diligence and ongoing monitoring in a sanctions compliance program. Providing guidelines for implementing effective monitoring systems to prevent violations and manage risks.

Key Training Areas for Employees

The module covers essential training areas for compliance officers, including types of sanctions, relevant authorities and more. It addresses the key components for an effective compliance officer.

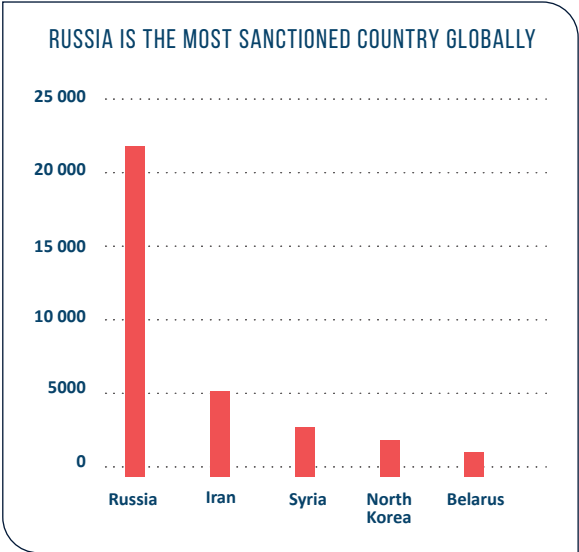
Useful Resources to Detect Sanctioned Companies or Individuals

Within the annex, online resources that allow free access to conduct screening and monitoring activities are listed, containing both consolidated and nonconsolidated lists from western countries, organizations.

CONTEXT AND OBJECTIVES OF THE DOCUMENT



Russia’s escalation of the occupation of Crimea into a full-scale war in Ukraine caused a cascade of restriction regimes that have culminated into one of the most extensive sanctions implementation regimes in history. Today, Russia has more than 20,000 entities subject to international sanctions, becoming by far the most sanctioned country globally,¹ spearheaded by around 50 countries. Amongst its many goals, the restrictions imposed aim to limit Russia’s ability to finance the war and hinder the production of advanced conventional weapons (ACW).²



Sanction regimes differ, and coordinated cooperation is of utmost importance. Financial and logistics companies are subject to the greatest risks, therefore additional care is taken to raise awareness amongst these sectors.

Non-compliance with sanctions regimes is among the most significant risks many private sector entities face. The threat of secondary sanctions underlines the need for stronger compliance systems and measures.

In the wake of these developments, compliance with the ACW-related sanctions regimes has become critically important for private sector entities, especially in countries neighboring or those with significant business ties to Russia. A firm’s ability to quickly and accurately identify illicit transactions and take appropriate steps to address the respective risks is critical to ensuring unhindered operation and maintaining regulatory compliance. Considering the significant effects of noncompliance such as frozen assets, restricted or banned exports, seized property, and denied visa travel – the private sector needs to be vigilant in their compliance with these regimes.³

Knowledge of existing sanctions regimes and their proper enforcement needs to be improved particularly in the transport and logistics sectors. This document aims to provide practical advice to transport and logistics companies in Georgia regarding the enforcement of the sanctions imposed against Russia.

¹ “About 20,000 Sanctions Slapped on Russian Economy by Collective West — MFA.”
² Singapore Ministry of Foreign Affairs, “Sanctions and Restrictions Against Russia in Response to Its Invasion of Ukraine.”
³ OFAC, “SANCTIONS ADVISORY Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia’s Military-Industrial Base.”

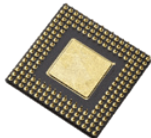


DEFINITION AND EXAMPLES OF ADVANCED CONVENTIONAL WEAPONS AND COMPONENTS

Current sanctions against Russia aim to limit its ability to import critical system components and high-performance machine tools, significantly affecting its capacity to manufacture advanced conventional weapons. Despite these sanctions, Russia and its allies have developed sophisticated networks to bypass restrictions and acquire necessary weapons and components to sustain their defense-industrial complex.

ACW encompasses a broad range of weapons systems, including Man-Portable Air Defense Systems (MANPADS), Anti-Tank Guided Missiles (ATGMs), major weapons systems, heavy military equipment like tanks, aircraft, and missiles, sensors, lasers, and precision-guided munitions. While some firms may encounter complete or partial weapons systems, they are more likely to face challenges related to the export, sale, or transfer of components.⁴

U.S. measures also target Russian military end-users by adding them to the Department of Commerce’s Entity List, effectively blocking their access to most items under the Export Administration Regulations (EAR), including specific electronics, sensors, and telecommunications and computer processing supplies. Sanctions may also cause Russian defense companies to face higher interest rates on loans and increased prices for materials and components.

Although sanctions may take time to significantly impact due to the long lead times required for weapons system production, there is evidence that they have affected Russia's ability to manufacture key systems, such as precision-guided munitions. For example, Russian media reports delays in the next-generation airborne early warning and control (AEW&C) aircraft, the A-100 Premier, due to delays in electronic component deliveries like microchips.

TYPE OF COMPONENT	IMAGE/REPRESENTATION	USAGE
Microelectronics/microchips		Communications equipment, UAS, precision long-range munitions
Semiconductors		Defense-related components (computers, sensors, switches, amplifiers)
Bearings		Tanks, aircraft, submarines, other military systems

⁴ United States Department of State, “Advanced Conventional Weapons.”

Connectors, fasteners, trans-formers, casings, transistors, insulators		Basic components that constitute the electronics systems in a conventional weapon system
Engines, vehicle parts		Defense-related components (computers, sensors, switches, amplifiers)
Composite material		Tanks, aircraft, submarines, other military systems
COMMODITY		EXPORT CONTROL CLASSIFICATION NUMBER
Aircraft Parts and Equipment		ECCN 9A991
Antennas		ECCN 7A994
Breathing Systems		ECCN 8A992
Cameras		ECCN 6A993
GPS Systems		ECCN 7A994
Inertial Measurement Units		ECCN 7A994

Integrated Circuits		ECCN 3A001, 3A991, 5A991
Oil Field Equipment		ECCN EAR99
Sonar Systems		ECCN 6A991
Spectrophotometers		ECCN 3A999
Test Equipment		ECCN 3B992

Some components are clearly intended for military use based on their type or grade. However, many weapons are manufactured using dual-use components that were not initially designed for or do not seem to have illegal purposes.

Broadly speaking, the types of components that could be used by military end-users for ACW and should be subject to additional scrutiny by firms include the following:

Thrusters (Marine)		ECCN 8A992
Underwater Communications		ECCN 5A991
Vacuum Pumps		ECCN 2B999
Wafer Fabrication Equipment		ECCN 3B001, 3B991

Wafer Substrates



ECCN 3C001 through 3C006

Many of these components are made by companies in the U.S., Germany, the Netherlands, the U.K., Taiwan, and Japan among others, but could be found anywhere due to the prevalence of re-exporters and freight forwarding services.

Some sanctions regimes, such as those adopted by the EU, have specific bans on transactions involving certain dual use goods, including the following:

- Toy/Hobby Drones
- Complex Generator Devices
- Laptop Computers And Computing Components
- Printed Circuits
- Radio Navigational Systems
- Radio Remote Control Apparatus
- Aircraft Engines And Parts Of Engines
- Cameras And Lenses
- Drone Engines
- Camouflage Gear
- Additional Chemical/Biological Equipment
- Riot Control Agents.



Georgia does not produce Advanced Conventional Weapons (ACW's) or their components. However, attention should be paid to Russia's procurement of ACW components through third countries, known as trans-shipment hubs. This process involves various front companies and fraudulent end-users who acquire microelectronics and other components under legitimate pretenses before forwarding them to sanctioned end-users in Russia. These intermediaries often operate from jurisdictions that make it challenging for sellers and manufacturers to identify and avoid firms connected to sanctioned entities. This situation highlights the importance of a strong internal compliance system and procedures.

GEORGIAN CONTEXT

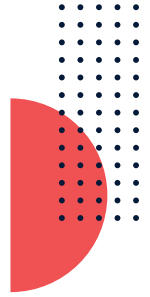
Even without any specific evidence, it is reasonable to assume that Georgia – like its neighbors – would be a desirable hub or transit country for Russia, requiring significant vigilance on the part of the Georgian financial and logistics sectors.

Russia has direct borders with 14 countries (Norway, Finland, Estonia, Latvia, Lithuania (via the Kaliningrad), Poland (via the Kaliningrad), Belarus, Ukraine, Georgia (including occupied territories Abkhazia and Tskhinvali region), Azerbaijan, Kazakhstan, China, Mongolia and North Korea, also maritime boundaries with Japan and USA). Georgia benefits from free trade regimes with EU, China, Turkey and CIS countries, is ranked top 10 in the global Ease of Doing Business Index, enjoys top positions in the Economic Freedom Index and has access to the open sea (Black Sea) connecting Georgian ports with EU harbors. All these factors highlight the risks Georgia and Georgian companies face, as both the location and the business environment suit it to be a transshipment hub.

Georgia has a legal framework in place to prevent certain types of illicit transactions, called the “Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism.” This law is focused on UN Security Council Resolutions imposing sanctions related to money laundering, foreign terrorist financing, and proliferation financing, as these sanctions regimes are legally binding and apply to Georgia. A governmental commission on these resolutions is led by the Ministry of Justice and sanctioned persons and entities can be found on the Ministry’s website. This does not, however, apply to bilateral (non-UN) sanctions, like the sanctions and controls discussed in this document.

There are several ways that goods can be transported between Georgia and Russia. Currently, Georgia and Russia are linked by road, with the only operational border crossing point functioning in Kazbegi. As per statistical data, the transportation rate along that route has increased significantly in recent years. Detection of the sanctioned goods along this route is mainly left to the Georgian customs service, as most Georgian road transportation companies have little understanding of the sanction’s regimes. Rail transportation of goods is less common, as there is no direct rail connectivity between Georgia and Russia. Rail transportation does occur via Azerbaijan though, whose rail service is operated and maintained by the Russian industry. There are direct flight connections between Georgia and Russia. Georgian cargo airlines display a better understanding of sanctions and have implemented processes in place to detect and prevent illicit transactions. There is no regular maritime connectivity between Russia and Georgia, however, chartered vessels may be accepted in Georgian Ports, subject to checking relevant sanctions lists.

THE IMPORTANCE OF MANAGING YOUR COMPANY IN THE SANCTIONS AND NON-PROLIFERATION ENVIRONMENT



EXISTING SANCTIONS REGIMES

There are several bilateral and multilateral sanctions and export control regimes in effect today that impose obligations on private-sector firms. Many prior weapons-related sanctions regimes have focused exclusively on Weapons of Mass Destruction (WMD) production materials. This includes the robust UN sanctions targeting North Korea's and, until recently, Iran's proliferation financing. Russia's annexation of Crimea, Ukraine in 2014, followed by its further invasion of rest of Ukraine in 2022, dramatically altered the sanctions landscape, especially by imposing severe sanctions targeting individuals and entities engaged in ACW-related transactions.

The United States was the first to adopt sanctions against Russia after Russia's 2014 invasion of Crimea, Ukraine. These sanctions, implemented by the Office of Foreign Assets Control (OFAC), apply to specific sectors, prohibit transactions with designated nationals, and ban investments and export/import of goods related to Crimea. In 2017, the Countering American Adversaries Through Sanctions Act (CAATSA) went into force. Section 231, administered by the U.S. Department of State, addresses transactions with the Russian intelligence and defense sectors, allowing the United States to act against any individual or entity engaged in the manufacture, sale, or delivery of Russian advanced conventional weapons.⁵

Notably, CAATSA enables the U.S. to penalize any entity, including non-American ones, that engage with illicit entities. These sanctions aim to reduce Russia's economic sophistication, hinder military modernization, and limit access to dual-use items. The Department of Commerce's Bureau of Industry and Security (BIS) restricts Russia's access to critical goods, including microelectronics and aircraft components. The European Union has imposed significant parallel sanctions against Russia, starting in 2014. As of July, 2024, the EU had approved fourteen packages of sanctions against Russia. These sanctions have several measures specifically targeting Russia's advanced conventional weapons industry. The EU sanctions are specifically aimed at limiting Russia's capacity to manufacture new weapons and repair the existing ones, as well as disrupting its ability to transport material. These sanctions target Russian entities to cut off their access to sensitive dual-use and advanced technology items. A number of other countries, including the UK, Japan, and Australia, have implemented sanctions against Russia.

Current sanctions against Russia aim to restrict Russia's ability to import critical system components and high-performance machine tools, which will have a significant impact on Russia's ability to manufacture advanced conventional weapons. Russia and its allies, however, have sophisticated networks in place to circumvent sanctions and acquire weapons and components to allow continued manufacturing in its defense industrial complex.

⁵ "Ukraine-/Russia-Related Sanctions | Office of Foreign Assets Control."



CONSEQUENCES OF NON-COMPLIANCE

Compliance with sanctions regimes is crucial, not just as a matter of legal obligation, but also for safeguarding a company's financial health and reputation

The legal landscape surrounding sanctions is stringent and complex. Russian-related sanctions regimes are implemented to limit the Russian war machine in the production of ACW. Non-compliance with sanctions can lead to severe legal consequences. Companies found violating sanctions can face hefty fines, asset seizures, and in some cases criminal charges against their executives. For instance, several multinational corporations have faced billions of dollars in fines for sanctions violations. Beyond monetary penalties, the legal fallout can include long costly legal battles and restrictions on future business operations.

Sanctions compliance is also critical from a financial perspective. Violating sanctions can result in direct financial losses due to fines and legal fees. Banks and financial institutions are required to strictly comply with sanctions, and failure to do so can lead to loss of access to international banking systems, which are vital for global trade. The indirect financial risks are equally significant. Companies that violate sanctions will face disruptions in their supply chains, loss of business opportunities, and decreased investor confidence. Shareholders and investors are increasingly aware of the importance of compliance, and a company's failure to adhere to sanctions can lead to a sharp decline in stock prices and overall market value.

In the age of instant communication and social media, reputational damage can be swift and far-reaching. Companies that are found to violate sanctions will suffer severe harm to their reputation, both among consumers and within the business community. This reputational damage can have long-lasting effects, as trust and credibility are difficult to rebuild once lost. Public perception of a company's good profile and integrity is crucial. Consumers today are more informed and conscientious, often preferring to engage with companies that demonstrate ethical practices.

Compliance with sanctions regimes is essential for any company operating in the international arena. The legal, financial, and reputational risks associated with non-compliance are substantial and can have far-reaching consequences. Companies must invest in robust compliance programs, including regular training, thorough due diligence, KYC, and continuous monitoring of international sanctions lists. In a world where the regulatory landscape is continually evolving, a proactive approach to compliance is not just a legal necessity but a strategic imperative for long-term success.

COMPLIANCE IMPLICATIONS FOR LOGISTICS

Sanctions-related compliance in the logistics sector is critical due to the global nature of the industry and its involvement in the movement of goods across borders. However, compliance actions may cause implications and potential impacts on operations:

The most common implications are as follows:

Restricted trade with Russia, as sanctions means embargoes on specific goods. For example, oil and other sanctioned goods are prohibited from being transported to or from the Russian Federation.

Logistics companies must screen their customers, suppliers, and other partners against sanction lists to avoid dealing with restricted entities, additional actions are always linked to increased operational cost and time. Such actions are especially necessary for transactions involving high-risk regions or industries.

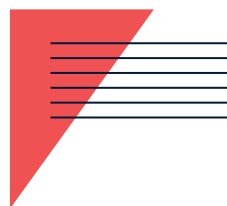
Another widespread implication is related to financial restrictions, so-called payment blockages, making it difficult to process payments related to logistics services for sanctioned entities.

From private sector customs hold-ups have been reported, predominantly in the Automobile industry, goods are held at customs for extended periods due to additional checks and documentation requirements. Some companies made route adjustments which necessitated altering existing shipping routes to avoid sanctioned territories, leading to longer transit times and increased costs.

Ongoing training for staff in sanctions regulations and the hiring of compliance experts are also additional expenses companies must bear.

In general, companies face the need of strategic adaptations, which may mean seeking alternative markets (supplier diversification) to shift focus to non-sanctioned markets to mitigate the impact of restricted trade regions.

BASICS OF SANCTIONS COMPLIANCE



TYPES OF SANCTIONS

There are various types of sanctions, each tailored to address different aspects of these issues.

Arms embargoes prevent the sale or supply of weapons and related materials.

Restrictions on admission, often referred to as travel bans, prevent targeted individuals from entering certain countries such as the EU, USA, and UK.

Asset freezing block listed persons or entities from accessing their assets in these regions, ensuring they cannot use these funds.

Economic sanctions or sector-specific restrictions can include bans on importing or exporting certain goods, investment bans, and prohibitions on providing certain services, all aimed at exerting pressure on the sanctioned entities.

HOW TO IDENTIFY AND AVOID SANCTIONED ENTITIES

Identifying and avoiding sanctioned entities is crucial for ensuring compliance with existing sanctions regimes. Sanctioned entities may include individuals, organizations, and countries that are subject to restrictions.

Governments and international organizations publish lists of sanctioned entities. Subscribing to and regularly checking these lists, such as the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list, the EU's consolidated list of sanctions is the very first step to detecting sanctioned individuals or products⁶. Later, we will discuss in more detail the useful tools for it.

Conduct thorough due diligence during the onboarding process of new clients or partners. This includes **background checks, verification of ownership structures, and ensuring that none of the involved parties are on sanction lists.**

It's important to note that sanction lists are frequently updated. Continuous monitoring of business relationships and transactions is necessary to identify any changes in the status of the entities the company or individual is dealing with. For companies, it is highly recommended to develop and enforce internal policies that control and prohibit transactions with sanctioned entities, regular training of the employees is of paramount importance as well. Apart from the activities mentioned above it is also important to maintain detailed records of due diligence efforts and compliance activities.

⁶ "Sanctions List Service | Office of Foreign Assets Control."

By implementing these strategies, companies can effectively identify and avoid sanctioned entities. To ease this task businesses usually guide with a predefined warning list: we call it **Red Flags and Transactions of Concerns**:

MANAGING RED FLAGS DURING BUSINESS OPERATIONS

Red flag indications help companies detect and report suspicious activities more easily. Red flags can be detected with the client/end user, the product/service, the source of funds/terms of payment, and the shipment/delivery.

CLIENT BASED RED FLAGS	The customer or its address is like one of the parties found on the Commerce Department's [BIS'] list of denied persons.
	The customer or purchasing agent is reluctant to offer information about the end-use of the item.
	The customer is involved in military business.
	The customer is unfamiliar with the product's performance characteristics but still wants the product.
	The customer imposes unusual requirements for excessive confidentiality about the destination or customers or the specifications of the goods.
	The customer requires unusual and excessive confidentiality regarding the destination or the products to be delivered.
PRODUCT BASED RED FLAGS	Packaging is inconsistent with the stated method of shipment or destination.
	The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry or goods that are too advanced for the claimed end-use.
	The product's capabilities do not fit the buyer's line of business
	Discrepancies between shipped goods and their declared value, quantity, or description. Inconsistencies may arise from forged or altered documents or collusion between parties to a transaction
	Large dollar or volume purchases of items from wholesale electrical/industrial merchants, electrical parts and equipment provides or electronic parts providers.

SHIPMENT BASED RED FLAGS	Sudden unexplained changes in route, or last-minute changes to end-users or payees, such as redirection of goods to third countries that have limited restrictions on re-export to Russia or Belarus.
	Business located in transshipment countries involved in the electronics or machinery sectors especially if newly formed or with offices in Russia.
	A freight forwarding firm is listed as the product's final destination.
PAYMENT BASED RED FLAGS	The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
	The customer insists on non-conventional methods of payment (BitCoin, other Cryptocurrencies)
	Transactions involving payments being made from entities located in third-party countries not otherwise involved with the transactions and known to be a potential transshipment point for exports.
	Offer to pay prices well over normal market value for the goods or services concerned. ⁷

MARITIME-RELATED RED FLAGS

Illegal activities related to maritime transport may involve:

- ➔ Manipulating Automatic Identification Signals (AIS) to mask a vessel's name, identifying number, or next port of call.
- ➔ Disabling a vessel's AIS (this is also known as 'spoofing').
- ➔ AIS data shows a vessel engaging in indirect routing or unscheduled detours - particularly if those deviations occur in high-risk areas.
- ➔ The shipping route is abnormal for the product and destination.
- ➔ Falsifying the vessel's flag, repeatedly changing the country flagging of a vessel within a short period, or continuing to use a country's flag after a vessel has been deregistered.
- ➔ Physically altering a vessel's identifying marks, such as painting over the vessel's name or IMO number.
- ➔ Transferring cargo to another ship (usually at sea) to conceal sanctioned cargoes, entities, or destinations. STS transfers that take place in high-risk areas or at night are of special concern.

⁷ "Sanctions List Service | Office of Foreign Assets Control."

→ Falsifying cargo and vessel documents, like bills of lading, certificates of origin, invoices, insurance certificates and last ports of call, to conceal goods from a sanctioned origin or sanctioned entity.⁸

False flag operations involve the intentional misrepresentation of the flag under which a ship is operating. This tactic is used to conceal the true identity of the vessel, often employed by individuals or entities engaged in illegal activities such as smuggling or illicit trade.

Frequent changes of flag involve rapid and often repeated changes in flag registration, complicating efforts to track a vessel's movements and activities. While changing flags is a common and largely legitimate practice, close attention should be paid to the frequency of changes and the context of the flag state.⁹

Illegal actors may attempt to disguise the final destination or origin of the cargo or consignee by using indirect routes, unplanned detours, or the transit or shipment of cargo through third countries. While transit and transshipment are common in global trade, it is recommended to scrutinize routes and destinations that deviate from standard business practices as appropriate.

Ship-to-ship transshipment (STS transfers) refers to the direct transfer of cargo, goods, or materials from one ship to another while at sea. STS transfers can be conducted for legitimate purposes, such as:

- Storing cargo in floating storage
- Mixing cargoes (so-called "floating mixing")
- Transferring cargo from a large capacity vessel to a smaller one

However, STS transfers, particularly those conducted at night or in areas with a high risk of sanctions evasion or other illegal activities, are often used to circumvent sanctions by disguising the true origin or destination of the secretly transferred goods.

⁸ New Zealand Sanctions Unit, "RUSSIA SANCTIONS GUIDANCE Sanctions Evasion: Common Red Flags."

⁹ "Registration of Ships and Fraudulent Registration Matters."

IMPLEMENTING A COMPLIANCE GUIDANCE



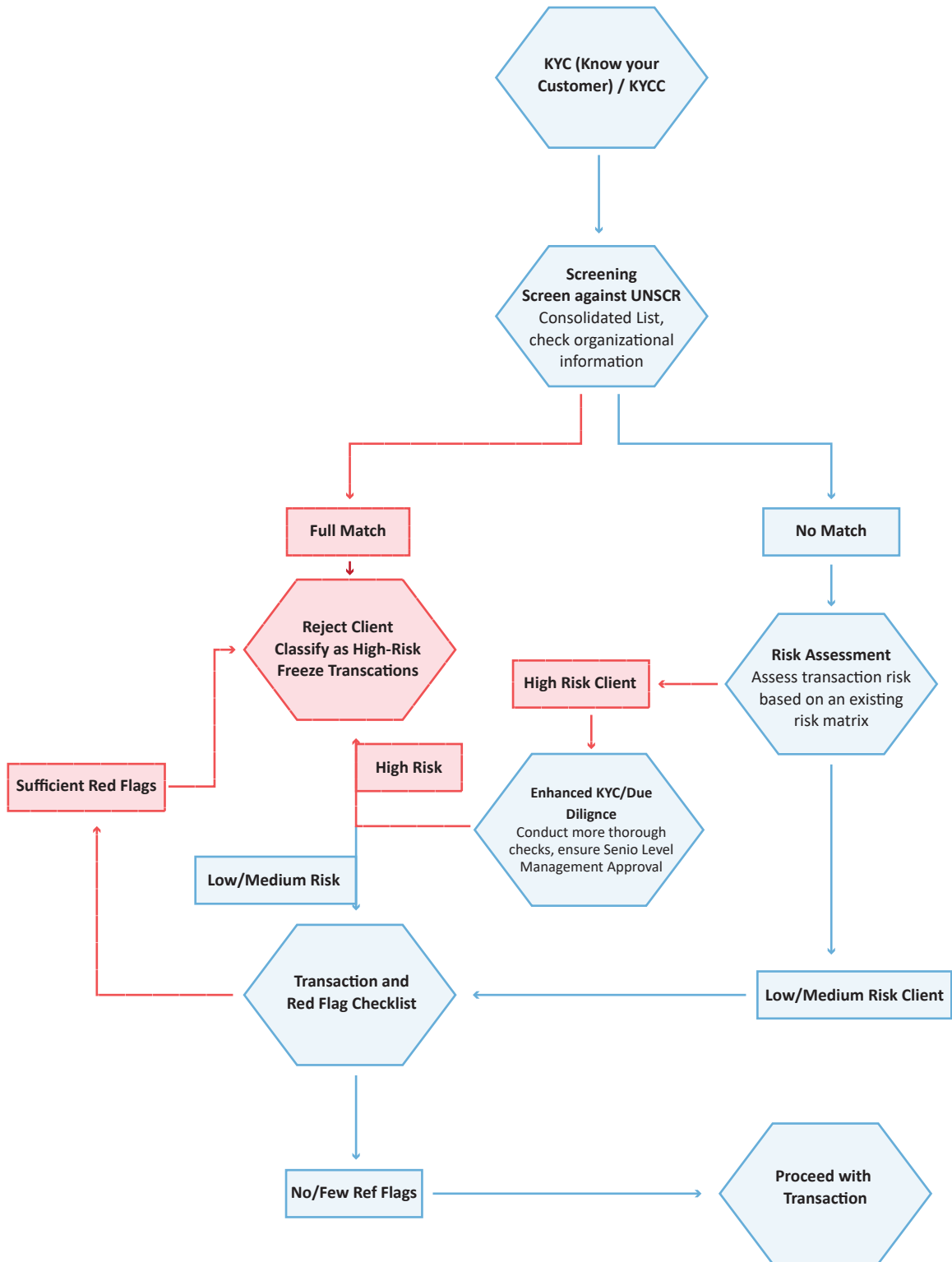
organization complies with relevant regulations. Below are recommendations, diagram and a checklist to guide you through the process:

<p>GENERAL GUIDANCE</p> <p>These steps are to ensure that an organization as a whole can deal with sanctions-related issues.</p>	<p>UNDERSTAND APPLICABLE SANCTIONS REGIMES</p>	<p>Identify and understand the sanctions regulations applicable to your organization (e.g., OFAC, UN, EU, etc.).</p>
		<p>Stay updated with changes in sanctions regulations: subscribe to official government websites, sign up for regulatory updates and alerts, join relevant associations (for example: Association of Certified Sanctions Specialists – ACSS, participation in forums, webinars and conferences)</p>
	<p>DEVELOP A SANCTIONS COMPLIANCE POLICY:</p>	<p>Advisably, companies should create a tailor-made written sanctions compliance policy focusing on industry-related risks.</p>
		<p>Ensure the policy covers all aspects of the business and is approved by senior management.</p>
	<p>TRAINING AND AWARENESS</p>	<p>Provide regular training to employees on sanctions regulations and internal compliance policies.</p>
		<p>Ensure employees understand the importance of sanctions compliance and how to identify red flags.</p>
<p>TRANSACTION RELATED</p> <p>These steps are to ensure that a transaction is done in a safe manner, following international regulations.</p>	<p>RISK ASSESSMENT:</p>	<p>Conduct a risk assessment to identify potential exposure to sanctioned entities, individuals, countries, or sectors, elaboration of risk matrix.</p>
		<p>Determine high-risk areas and transactions that require enhanced due diligence.</p>
	<p>SCREENING AND DUE DILIGENCE</p>	<p>Implement a screening program to check customers, partners, transactions, and third parties against sanctions lists.</p>
		<p>Use reliable, updated sanctions lists and automated screening tools.</p>
		<p>Conduct enhanced due diligence on high-risk entities and transactions.</p>
		<p>Conduct enhanced due diligence on high-risk entities and transactions.</p>

<p>INTERNAL MONITORING</p> <p>These steps are to ensure that an organization is safeguarded against legal ramifications.</p>	<p>RECORD KEEPING AND DOCUMENTATION</p>	<p>Maintain accurate and detailed records of all sanctions-related due diligence, screening results, and compliance decisions.</p>
	<p>REPORTING AND ESCALATION</p>	<p>Develop a protocol for reporting potential sanctions violations to the relevant authorities.</p>
	<p>REGULAR AUDITS AND REVIEWS</p>	<p>Conduct regular audits and reviews of the sanctions compliance program to identify and address any weaknesses.</p>
		<p>Update the compliance program as needed based on audit findings and changes in regulations.</p>

Implementing these recommendations will help establish a robust sanctions compliance strategy, reducing the risk of violations

TRANSACTION DIAGRAM





RISK ASSESSMENT CHECKLIST

- Does your firm know your customers and third parties?
 - Have individuals and entities been checked against sanctions lists?
 - Do you have visibility into the controlling interests behind individual customers, suppliers or other third parties?
- Does your firm know the product or service?
 - Does the product or service have a dual-use or military application?
 - Does the product or service require an export license?
 - Is the product or service subject to an embargo?
- Does your firm know the receiving country?
 - Is the receiving country Russia?
 - If not Russia, is the country a known facilitator for Russia?
- Does your firm know the end-use and end user?
 - Have you confirmed the intended end-use of the product or services?
 - Are there sanctions that might apply to that end-use?
 - Do you have an end-use/user statement and sanctions clause built into your sales contracts?
 - Can you verify whether the end user and its ultimate beneficiary are subject to sanctions?
- Does your firm know the transaction?
 - Is this an allowable transaction under sanctions and export control requirements?
 - Are there any sanctions applicable to the location of the delivery?
 - Will third parties, such as agents acting on your company's behalf or transporters moving your products, be involved in the transaction?

PRACTICAL STEPS FOR COMPLIANCE



A strong compliance program for sanctions is vital for organizations involved in international operations to ensure they adhere to global sanctions regulations and avoid legal and reputational risks. Here are the core elements of such a program:

It is highly recommended to designate a Compliance Officer, whose role usually is to be responsible for developing, implementing, and overseeing the sanctions compliance program. This may include creating policies, conducting risk assessments, training employees, and monitoring compliance activities. Management of the company should give enough power to the compliance officer, so they should have the authority and resources necessary to effectively manage the program, including access to senior management and the board of directors.

Major tool for the compliance officer to perform its duties is Risk Matrix which should correspond to the industry's needs and threats. Officers should regularly assess the organization's exposure to sanctions-related risks based on its geographic footprint, customer base, product lines, and supply chain. While evaluating the risks using criteria such as country risk, customer risk, transaction risk, and product/service risk should be taken into consideration.

IMPACT CRITERIA				VULNERABILITY CRITERIA		
Score	Financial	Legal	Reputational	Score	Probability	Detectability
5	>\$100K – Real Possibility of Loss	Serious Issues Certain	Negative Press Certain	5	High Risk of Occurrence >70% over the next 12 months	No Monitoring/Safeguards – Hard to detect before failure
4	\$50K-\$100K – Real Possibility of Loss	Issues Likely	Negative Press likely	4	Significant risk of Occurrence ~50% over the next 12 months	Some Monitoring/Safeguards – Significantly difficult to detect before failure
3	\$30K-\$50K – Real Possibility of Loss	Issues Probable	Negative Press Probably	3	Moderate Risk of Occurrence	Limited Monitoring/Safeguards – Moderately Difficult to detect before failure
2	\$10K-\$30K – Possibility of Loss	Issues Possible	Negative Press Possible	2	Slight Risk of Occurrence	Good Monitoring/Safeguards – Slight risk to detect before failure
1	<\$10K Remote chance that the loss would exceed €10,000	Issues Unlikely	Negative Press Unlikely	1	Low Risk of Occurrence	Strong Monitoring/Safeguards – Highly likely to detect before failure

AN EXAMPLE OF A TAILORED RISK MATRIX

GENERAL RISK MATRIX		IMPACT				
		1	2	3	4	5
LIKELIHOOD	5	Medium/High	Medium/High	High	High	High
	4	Low/Medium	Medium/High	Medium/High	High	High
	3	Low/Medium	Low/Medium	Medium/High	Medium/High	High
	2	Low	Low	Low/Medium	Low/Medium	Medium/High
	1	Low	Low	Low	Low/Medium	Medium/High

AN EXAMPLE OF A GENERAL RISK MATRIX

Risk matrix in practice is always based on developed comprehensive policies that clearly outline the organization's stance on sanctions compliance, including prohibitions, requirements etc.

To make sure that real life application of the policies is duly enforced companies should elaborate operational guidelines covering areas such as customer onboarding, transaction monitoring, and handling potential violations. Another important aspect of good operational practice is the regular training of employees to ensure they understand sanctions regulations, the importance of compliance, and how to recognize and report potential violations. Conducting Awareness initiative campaigns also helps to keep sanctions issues top of mind and reinforces the importance of compliance.

A trained officer should be able to conduct enhanced due diligence on high-risk entities and transactions, including thorough background checks and ongoing monitoring. They must also maintain accurate records of all screening and due diligence activities. One of the major roles of an officer is conducting regular internal audits to assess the effectiveness of the compliance program and identify areas for improvement. Based on findings officers should develop response plans to address identified compliance issues, including steps for investigation, remediation, and prevention of future occurrences. In certain cases, company HR officers may implement disciplinary measures for employees who violate sanctions policies, with severity depending on the nature of the breach.

As mentioned above it is of crucial to ensure that senior management actively supports and promotes the sanctions compliance program. By integrating these core elements, organizations can establish a robust sanctions compliance program that effectively mitigates risks and ensures compliance with global sanctions regulations.

DUE DILIGENCE AND MONITORING



Due diligence and monitoring are critical components of a robust sanction's compliance program. They play a fundamental role in identifying and mitigating risks associated with conducting business in a global environment.

Proper due diligence involves comprehensive background checks on potential customers, suppliers, and business partners to identify any connections to sanctioned entities or individuals – we call it Thorough Vetting. This reduces the risk of inadvertently engaging in prohibited transactions.

Ongoing Surveillance/continuous monitoring ensures that any changes in the status of business partners or transactions are promptly detected. This includes new sanctions being imposed or existing ones being updated. Proper and functional monitoring systems should provide real-time alerts if an entity becomes sanctioned, allowing for immediate action to be taken to halt transactions or relationships. Effective due diligence mechanism can prevent the initiation of transactions with sanctioned entities, thereby avoiding potential violations and the associated legal and financial repercussions as it enables timely detection of potential violations, enabling the organization to take corrective action before a violation occurs or is detected.¹⁰

¹⁰ "What Businesses Need to Know about Sanctions Compliance?"

KEY TRAINING AREAS FOR EMPLOYEES



Key training areas on Sanctions Compliance include but are not limited to the following:

→ **Understanding Sanctions Regimes**

- a. Types of Sanctions,
- b. Differentiate between economic sanctions,
- c. Trade embargoes,
- d. Financial Restrictions,
- e. Sectoral Sanctions.

→ **Understanding of relevant sanctions imposing bodies**

- a. OFAC,
- b. European Union,
- c. United Nations
- d. Other Western Nations

→ **Understanding of the scope of sanctions**

- a. Application of Sanctions Based on Jurisdiction.
- b. Application of Sanctions Based on the Entity's Location.

→ **Understanding customer and transaction screening in sanctions lists, screening tools, red flags.**

→ **Understanding of sector-specific compliance related to certain industries (e.g., energy, transport, financial etc).**

→ **Understanding of proper, basic principles of record keeping and documentation.¹¹**

Special attention should be given to cargo description, including detailed descriptions of the cargo, including quantity, weight, dimensions, and any special handling requirements as well as shipping documents, such as bills of lading, packing lists, and certificates of origin.

¹¹ "Types of Sanctions the EU Adopts."

ANNEX 1 - USEFUL RESOURCES TO DETECT SANCTIONED COMPANIES OR INDIVIDUALS

Below you can find the resources available for firms to use with ACW-related sanctions. As part of this review, you can observe screening of certain individuals and entities through these resources.

OFAC LIST OF SPECIALLY DESIGNATED NATIONALS AND BLOCKED PERSONS (SDN LIST) < OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. Web: <https://sanctionssearch.ofac.treas.gov/>

BUREAU OF INDUSTRY AND SECURITY (BIS) ENTITY LIST < The Export Administration Regulations (EAR) contain a list of names of certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items. Web: <https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file>

DEPARTMENT OF STATE, CAATSA SECTION 231(E) LIST < The Department of State maintains a list identifying persons that are part of, or operate for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation for the purposes of CAATSA Section 231. Web: <https://www.state.gov/caatsa-section-231d-defense-and-intelligence-sectors-of-the-government-of-the-russian-federation/>

OFFICE OF FINANCIAL SANCTIONS IMPLEMENTATION (OFSI) OF HM TREASURY IN THE UK < The UK government publishes the UK Sanctions List, which provides details of those designated under regulations made under the Sanctions Act. Web: <https://ofsistorage.blob.core.windows.net/publishlive/2022format/ConList.html>

EUROPEAN UNION < The EU maintains a list of sanctioned individuals and entities, kept under constant review and is subject to periodic renewals by the Council. Web: <https://sanctionsmap.eu/#/main>

AUSTRALIAN DEPARTMENT OF FOREIGN AFFAIRS AND TRADE < The Australian government maintains a consolidated list of sanctioned individuals and entities. Web: <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>

JAPANESE MINISTRY OF ECONOMY, TRADE, AND INDUSTRY (METI) < The Japanese government issues an End User List, providing exporters with information on entities that may be involved in activities related to WMDs and other items. Web: https://www.meti.go.jp/english/press/2022/1104_002.html

SANCTIONS EXPLORER < combines all above-mentioned Web: <https://sanctionexplorer.org/>

UNITED NATIONS < The Consolidated List includes all individuals and entities subject to measures imposed by the Security Council. The inclusion of all names on one Consolidated List is to facilitate the implementation of the measures, and neither implies that all names are listed under one regime, nor that the criteria for listing specific names are the same. For each instance where the Security Council has decided to impose measures in response to a threat, a Security Council Committee manages the sanctions regime. Each sanctions committee established by the United Nations Security Council therefore publishes the names of individuals and entities listed in relation to that committee as well as information concerning the specific measures that apply to each listed name. Web: <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list> same link is available under the website of the ministry of justice of Georgia www.justice.gov.ge

<https://trade-integrity.org/> < is also useful tool to promoting transparency and accountability in global trade. By utilizing public and whistleblower data, in which CHPL continue to reach Russia, providing crucial insights to help companies screen their clients and prevent their goods from being diverted to the Russian military-industrial complex.

ANNEX 2 – KNOW YOUR CUSTOMER AND KNOW YOUR CUSTOMER'S CUSTOMER CHECKLIST

KYC CHECKLIST	KYCC CHECKLIST
<p>CUSTOMER IDENTIFICATION:</p> <ul style="list-style-type: none"> ● Collect identification documents (e.g., passport, ID card) ● Verify the authenticity of documents ● Obtain proof of address 	<p>CUSTOMER'S CUSTOMER IDENTIFICATION</p> <ul style="list-style-type: none"> ● Identify the key clients or partners of your customer ● Collect and verify information on your customer's customers ● Understand the nature of your customer's relationships
<p>CUSTOMER DUE DILIGENCE</p> <ul style="list-style-type: none"> ● Assess the risk profile of the customer ● Check against sanctions and watch lists ● Perform enhanced due diligence for high-risk customers 	<p>RISK ASSESSMENT</p> <ul style="list-style-type: none"> ● Assess the risk associated with the customer's customers ● Determine the level of due diligence required ● Monitor high-risk relationships closely
<p>BENEFICIAL OWNERSHIP VERIFICATION</p> <ul style="list-style-type: none"> ● Identify and verify ultimate beneficial owners (UBOs) ● Understand the ownership and control structure of the entity ● Screen UBOs against sanctions lists 	<p>MONITORING AND REPORTING</p> <ul style="list-style-type: none"> ● Track transactions and interactions involving customer's customers ● Report any red flags or unusual activities ● Document findings and actions taken
<p>ONGOING MONITORING</p> <ul style="list-style-type: none"> ● Monitor transactions for unusual or suspicious activity ● Review and update customer information periodically ● Report suspicious activities to authorities 	<p>COMPLIANCE AND DOCUMENTATION</p> <ul style="list-style-type: none"> ● Ensure compliance with all applicable laws and regulations ● Maintain detailed records of all KYCC processes ● Review and update KYCC information regularly
<p>RECORD KEEPING</p> <ul style="list-style-type: none"> ● Maintain records of customer identification and verification ● Document due diligence processes and decisions ● Keep records for the required period as per regulations 	



Authors:

Akaki Saghirashvili, Giorgi Gogvadze, Nikoloz Kipshidze

Contributor:

Levan Dolidze