Certified Global Sanctions Specialist (ACAMS)

ACAMS CGSS

Version Demo

Total Demo Questions: 9

Total Premium Questions: 95

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co

dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Sanctions Regulatory Framework	36
Topic 2, Sanctions Risk Management	10
Topic 3, Sanctions Compliance Programs	10
Topic 4, Sanctions Screening	21
Topic 5, Sanctions Investigations	15
Topic 6, Mix Questions	3
Total	95

QUESTION NO: 1

A financial institution is implementing a new sanctions-list feed into its screening platform. Which controls should be performed before the institution relies on the feed in production? (Select Two.)

A. Reconciling the loaded records to the authoritative source

B. Testing that newly added and amended list entries generate expected alerts

C. Accepting the feed once the vendor confirms that transmission was successful

D. Suppressing alerts until the first monthly quality-assurance review is completed

E. Limiting the feed to names that have a complete date of birth or registration number

ANSWER: A B

Explanation:

Reconciling the loaded records to the authoritative source and **testing that newly added and amended list entries generate expected alerts** are essential controls. Reconciliation helps establish that the full source file was received, parsed, and loaded without omissions, truncation, or mapping errors. Testing with representative list entries verifies that the screening engine can detect new designations and changes to identifiers, aliases, or other data.

Simply accepting a vendor confirmation or waiting for normal alerts does not demonstrate that list data was loaded accurately or that the matching configuration is working as intended. Suppressing alerts during implementation would create an avoidable false-negative risk. List management should be documented, controlled, and subject to ongoing validation.

QUESTION NO: 2

Who must generally comply with sanctions programs?

A. Individuals and entities subject to the jurisdiction of the authority that is imposing the sanction

B. Individuals and entities globally

C. International financial institutions

D. Non-nationals outside the jurisdiction of the authority that is imposing the sanction

ANSWER: A

Explanation:

Individuals and entities subject to the jurisdiction of the authority imposing the sanction must generally comply with that authority's sanctions program. Jurisdiction is determined by the issuing authority's laws and can extend beyond simple physical location. For example, U.S. sanctions administered by the Office of Foreign Assets Control generally apply to U.S. citizens and permanent residents wherever located, persons in the United States, and entities organized under U.S. law, including their foreign branches. This means a sanctions compliance analysis should first identify the relevant jurisdictional nexus: such as nationality, place of incorporation, physical presence, or the location and nature of the activity. Similar principles apply to other sanctions authorities, whose measures bind the persons, entities, and activities within the scope established by their own legal instruments. A firm operating across borders should therefore assess every jurisdiction that may apply to its legal entities, employees, branches, transactions, and operations, rather than assuming that sanctions are universally binding or limited solely to the country where a person happens to be located. See OFAC FAQ 11 and the European Commission's sanctions guidance.

QUESTION NO: 3

What element should be included in an effective export compliance program to address sanctions risk?

A. Implementing letters of credit containing prohibited boycott terms or conditions

B. Collecting of vouchers

C. Outsourcing to freight forwarders who have excellent expertise and guidance

D. Conducting payment screening according to formalized procedures

ANSWER: D

Explanation:

Conducting payment screening according to formalized procedures is an essential control in an effective export compliance program because payments can reveal sanctioned parties, restricted financial institutions, prohibited jurisdictions, or transaction details that were not apparent at initial customer onboarding. Formalized procedures establish who must be screened, which payment and trade data must be reviewed, when screening occurs, how potential matches are escalated, and how decisions are documented. This makes sanctions controls repeatable, auditable, and capable of being consistently applied across sales, shipping, finance, and compliance functions.

Payment screening also complements screening of customers, beneficial owners, intermediaries, vessels, banks, and transaction documents. A risk-based process should use current sanctions lists and account for changes in counterparties, routing, ownership, and payment instructions throughout the life of a transaction. Where a potential sanctions concern is identified, the organization should pause the activity as appropriate and investigate or escalate it before processing the payment. OFAC identifies sanctions-list screening and ongoing compliance controls as important features of a sanctions compliance program, while BIS guidance emphasizes documented procedures and transactional screening within export compliance programs. See OFAC's Framework for Compliance Commitments and BIS Export Compliance Program Guidance.

QUESTION NO: 4

A sanctions analyst receives a letter of credit (LC) request that shows the carrier is a possible match under the Specially Designated Nationals and Blocked Persons List. Which action should the analyst take?

A. Use secondary sources to obtain more identifiers and information.

B. File a report to the regulator and reject the LC.

C. Immediately reject the LC and list the company name internally.

D. Immediately reject the payment and close the customer account.

ANSWER: A

Explanation:

Use secondary sources to obtain more identifiers and information. is the appropriate first action because the screening result is only a possible match, not yet a confirmed sanctions nexus. In trade finance, a carrier-name alert can be ambiguous because vessel and company names may be similar, abbreviated, transliterated, changed, or associated with multiple entities. The analyst should investigate promptly using reliable internal and external sources to resolve the alert. Relevant identifiers can include the vessel's IMO number, flag, ownership and management details, port-call history, registration information, address, country of incorporation, and other distinguishing corporate data. The transaction documentation, including the LC application and transport documents, should also be reviewed for information that helps establish or disprove identity.

This investigation supports a defensible true-match or false-positive determination before the institution decides how to handle the LC. OFAC's sanctions-list search guidance emphasizes using additional identifying information to distinguish a listed party from a non-listed party with a similar name. In particular, vessel identification should rely on stable identifiers such as the IMO number rather than a name alone. See OFAC FAQ 14 and the OFAC SDN List resources.

QUESTION NO: 5

A data quality review will often attempt to identify which issues? (Select Three.)

A. Data placed in incorrect fields, such as names placed in address fields

B. Use of separate first and last name fields

C. Default values for date fields

D. Data using all upper case letters instead of mixed case

E. Hispanic names with both paternal and maternal last names

F. Duplicate records

ANSWER: A C F

Explanation:

Data quality review is a core control for sanctions-screening effectiveness because screening engines can only evaluate the information supplied to them. **Data placed in incorrect fields, such as names placed in address fields** is a material issue: field-specific matching logic may not apply the expected name-screening rules when identifying information is misclassified. **Default values for date fields** should also be identified because placeholder or system-generated dates can impair the reliability of date-of-birth comparisons, a key attribute used to distinguish true matches from false positives. **Duplicate records** are likewise a data-quality concern because they can create redundant alerts, obscure the completeness of a customer or payment population, and make case management and audit reconciliation less reliable. A sound review tests whether relevant data is complete, accurate, appropriately mapped, and consistently available to the sanctions filter, then routes identified defects through remediation and governance processes. These practices align with OFAC's expectation that sanctions compliance programs include appropriate internal controls and routine testing or auditing, including controls commensurate with the institution's sanctions risk profile. See OFAC's Framework for Compliance Commitments and the FATF Recommendations.

QUESTION NO: 6

A bank is offering a credit line for a trade transaction to a commercial client that is based in a country that shares its border with a sanctioned country. To which should a financial institution apply enhanced due diligence? (Select Two.)

A. The ultimate beneficial owners of the exporter and importer.

B. The shipment details because there are countries subject to international sanctions in the client's region.

C. Public domain searches of the client to confirm the client's industry.

D. The commercial terms of the credit to ensure the terms are not prohibited under Sectoral Sanctions' extension of debit or credit arrangements.

E. The pricing of the goods to see if they are reasonably in line with market value, determined through publicly available sources.

ANSWER: A B

Explanation:

The ultimate beneficial owners of the exporter and importer require enhanced due diligence because sanctions exposure can be concealed through complex ownership structures, intermediaries, or entities acting for designated persons. The institution should establish and verify who ultimately owns or controls each party to the trade, screen those persons against relevant sanctions lists, and understand whether any ownership or control relationship creates a sanctions nexus. This is particularly important where a transaction involves a jurisdiction bordering a comprehensively sanctioned country, as geographic proximity can elevate the risk that apparently non-sanctioned parties are being used to facilitate restricted activity.

The shipment details also require enhanced due diligence. Trade documentation and logistics information can reveal whether goods may be diverted, transshipped, or routed through neighboring jurisdictions to reach a sanctioned destination. A sanctions-focused review should assess the parties involved in transport, the goods description and quantity, ports and countries of loading and discharge, the proposed route, end use, and end user. These checks help the bank determine whether the stated transaction is consistent with the actual movement of goods and whether a sanctioned-country nexus may be obscured. This approach aligns with the risk-based controls described in OFAC's Framework for Compliance Commitments and the trade-finance risk indicators discussed by FATF.

QUESTION NO: 7

A financial institution provides banking services to cryptocurrency exchanges. One of their clients is a cryptocurrency exchange that specializes in offering privacy coins and provision of a tumbler/mixer service. Which sanctions-related risk should be considered?

A. Privacy coins provide anonymity on the blockchain but can be screened for sanctions compliance by the exchange.

B. Privacy coins provide enhanced anonymity features that negate the requirements for sanctions screening.

C. A tumbler/mixer service mingles cryptocurrency making it difficult to perform effective sanctions screening.

D. The cryptocurrency exchange can rely on the financial institution to perform due diligence on their clients.

ANSWER: C

Explanation:

A tumbler/mixer service mingles cryptocurrency making it difficult to perform effective sanctions screening. This is the key sanctions risk because mixers pool, split, and redistribute virtual currency in ways that can obscure the source, destination, ownership, and transactional path of funds. That loss of traceability impairs a financial institution's ability to identify whether a transaction involves blocked persons, sanctioned jurisdictions, or wallets associated with illicit activity. When an exchange offers both privacy-enhancing assets and mixing services, its exposure is elevated because the institution may have less reliable information for transaction monitoring, customer due diligence, and investigation of alerts.

OFAC has specifically identified virtual-currency mixers as services that may be used to obfuscate transactions and has imposed sanctions on mixer-related activity where it facilitated laundering by malicious cyber actors. A risk-based sanctions compliance program for an institution serving such an exchange should therefore account for the limitations on blockchain tracing, the exchange's controls and customer base, geographic exposure, and the capacity to detect and escalate suspicious or potentially sanctioned activity. OFAC's guidance on virtual currency sanctions compliance is available at OFAC Sanctions Compliance Guidance for the Virtual Currency Industry, and its mixer-related enforcement information is available at OFAC's Tornado Cash designation notice.

QUESTION NO: 8

The Office of Foreign Assets Control has designated which types of high-risk persons or entities in the digital asset ecosystem? (Select Three.)

A. Persons hacking and stealing cryptocurrency

B. Cryptocurrency exchanges

C. Mixers

D. Software developers

E. Credit unions

F. Central banks

ANSWER: A B C

Explanation:

Persons hacking and stealing cryptocurrency, cryptocurrency exchanges, and mixers are correct because OFAC has used its sanctions authorities against each of these types of actors or services when they support cyber-enabled theft, money laundering, ransomware activity, or sanctions evasion. For example, OFAC has designated cyber actors, including North Korea-linked actors, involved in theft and laundering of virtual currency. These designations demonstrate that digital-asset theft is not merely a technical or fraud concern; it can be a sanctions nexus when the responsible persons or organizations are listed.

OFAC has also designated virtual-currency exchanges that facilitated payments or laundering connected to illicit actors. In addition, OFAC has sanctioned virtual-currency mixers, including services alleged to have processed funds associated with malicious cyber actors and other illicit activity. These actions require regulated firms to screen customers and transactions, identify exposure to listed digital-wallet addresses and associated entities, and block or reject transactions as applicable under OFAC rules. OFAC's virtual-currency sanctions guidance and its announcements concerning cyber-related designations provide the relevant compliance context. See OFAC FAQs: Virtual Currency and OFAC's Tornado Cash designation announcement.

QUESTION NO: 9

Which has an obligation to accept and carry out UN Security Council Resolutions?

A. All members of the UN

B. Only permanent members of the Security Council

C. Only members of the Security Council

D. Only countries that are targets of the resolution

ANSWER: A

Explanation:

All members of the UN have the Charter-based obligation to accept and carry out decisions of the UN Security Council. Article 25 of the UN Charter expressly provides that UN Members agree to accept and carry out Security Council decisions in accordance with the Charter. This collective obligation is foundational to the Security Council's role in maintaining international peace and security. In the sanctions context, when the Security Council adopts a binding resolution, particularly acting under Chapter VII, each UN Member State must take the measures needed within its own legal framework to implement the resolution. Those measures may include asset freezes, travel bans, arms embargoes, trade restrictions, or other targeted financial sanctions. Implementation is therefore a responsibility extending across the UN membership, rather than being limited to states sitting on the Security Council, its permanent members, or states specifically named in a sanctions regime. The precise domestic legal steps can differ among jurisdictions, but the international obligation derives from UN membership and the Charter commitment. Article 103 further establishes the primacy of Charter obligations where they conflict with obligations under another international agreement. See Article 25 of the Charter of the United Nations and the UN Security Council's overview of Security Council actions.