

ACAMS.CGSS-KR.v2026-04-21.q42

|                                                                                                                                   |                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| □□□□:                                                                                                                             | CGSS-KR                                                     |
| □□□□:                                                                                                                             | Certified Global Sanctions Specialist (CGSS Korean Version) |
| □□□:                                                                                                                              | ACAMS                                                       |
| □□ □□ □□□:                                                                                                                        | 42                                                          |
| □□:                                                                                                                               | v2026-04-21                                                 |
| # □□ □:                                                                                                                           | 128                                                         |
| # □□ □□□:                                                                                                                         | 420                                                         |
| <a href="https://www.krdump.com/ACAMS.CGSS-KR.v2026-04-21.q42.html">https://www.krdump.com/ACAMS.CGSS-KR.v2026-04-21.q42.html</a> |                                                             |

NEW QUESTION: 1

2018□ □□ EU□ □□□ □□□ □□□ □ □□□ □□□ EU-□□ □□ □□ □□ □□ (INSTEX)□ □□□ □□ □□□□□.

- A. □□ □□.
- B. □□□□□□.
- C. □□ □□□□.
- D. □□ □□.

Answer: B (LEAVE A REPLY)

INSTEX was established by EU member states as an operational mechanism designed to facilitate limited and compliant trade with Iran after the re-imposition of U.S. secondary sanctions in 2018. According to the Sanctions and Compliance Domains, INSTEX is categorized as a special purpose vehicle, created specifically to permit trade transactions without reliance on traditional cross-border payment routes exposed to U.S. sanctions risk. Special purpose vehicles are defined within sanctions frameworks as structured entities created to conduct or support specific categories of trade or payments where direct financial transfers are restricted or exposed to sanctions risk. INSTEX was designed to match European exporters and importers with Iranian counterparts through a barter-style internal clearing arrangement, avoiding external USD payment flows. It is not a general license, nor is it a blocking statute. It also does not constitute sanctions evasion because it was formally established, publicly announced, and structured within EU legal parameters. Its purpose was to ensure compliance while maintaining limited humanitarian and permitted trade channels.

Reference from Sanctions and Compliance Domains:

Definitions and characteristics of special purpose vehicles in sanctions environments.

Description of EU mechanisms facilitating compliant trade with sanctioned jurisdictions.

Distinction between SPVs, blocking statutes, and licensing frameworks.

Regulatory context regarding INSTEX as an EU-created structured trade mechanism.

### NEW QUESTION: 2

Which of the following is NOT a requirement for a comprehensive sanctions framework?

- A. Thorough training for staff responsible for alert review and sanctions decision-making.
- B. Sanctions and Compliance Domains specify that personnel involved in alert clearing must receive appropriate training to ensure awareness of regulatory expectations, sanctions typologies, and escalation procedures.
- C. Robust screening controls supported by documented strategy, governance, list-management processes, alert management rules, and ongoing testing.
- D. Management information reports are restricted to need-to-know distribution, and reliance on "best-efforts" is not compliant.

**Answer: D (LEAVE A REPLY)**

OFAC regulations apply broadly to US persons, which include US citizens, permanent residents, entities organized under US law, and individuals located in the United States.

These obligations apply regardless of where the US person is physically located.

Foreign companies, foreign financial institutions, or foreign persons are only obligated under OFAC regulations when a US nexus exists (e.g., US origin goods, US dollars, US-based transactions). US persons, however, must always comply.

Reference:

Definition of "US persons" under OFAC regulations.

Global applicability of OFAC rules to US citizens and permanent residents.

### NEW QUESTION: 3

Which of the following is NOT a requirement for a comprehensive sanctions framework? (2 answers)

- A. Thorough training for staff responsible for alert review and sanctions decision-making.
- B. Sanctions and Compliance Domains specify that personnel involved in alert clearing must receive appropriate training to ensure awareness of regulatory expectations, sanctions typologies, and escalation procedures.
- C. Robust screening controls supported by documented strategy, governance, list-management processes, alert management rules, and ongoing testing.
- D. Management information reports are restricted to need-to-know distribution, and reliance on "best-efforts" is not compliant.
- E. Institutions must implement structured, risk-based controls, not minimal-effort approaches.

**Answer: D,E (LEAVE A REPLY)**

A comprehensive sanctions framework requires well-designed operational controls, including thorough training for staff responsible for alert review and sanctions decision-making. Sanctions and Compliance Domains specify that personnel involved in alert clearing must receive appropriate training to ensure awareness of regulatory expectations, sanctions typologies, and escalation procedures.

Additionally, the framework must include robust screening controls supported by documented strategy, governance, list-management processes, alert management rules, and ongoing testing. These elements form core requirements of sanctions compliance programs.

Management information reports are restricted to need-to-know distribution, and reliance on "best-efforts" is not compliant. Institutions must implement structured, risk-based controls, not minimal-effort approaches.

Reference:

Requirements for sanctions training and staff competency.

Necessity of a robust sanctions screening program with strategic oversight.  
Internal governance and control expectations in sanctions frameworks.

**NEW QUESTION: 4**

□□□□ □□□ "□□□ □□□(Al-Falah Company)"□ □□□□□ □□□ □□□□□ □  
□□. □□□□□□□□ □□□ □□ □□□□ □□□ □ "□□□ □□□□□□(El-Fallah  
Investments)"□ □□ □□ □□□ □□□ □□□ □□ □□□ □□ □□□ □□□□□□.  
□□ □□ □□□ □□ □□□□□(CEO)□ □□ □□□ CEO□ □□□□ □□□□□. □□□□  
□□□□□ □□□ □□□□ □□□?

- A. □□ □□□ □□□□ □□□ □□ □□ □□□ □□□□ □□□.
- B. □□□ □□□ □□ □□ □□□ □□□ □□ □□□□ □□□□□.
- C. □□ □□ □□□□□ □□□ □□ □□□ □□ □□□□ □□□□ □□□□ □□□.
- D. □□ □□□ □□ □□□ □□□ □□□ □□□ □□□, □□□□□□ □□□□ □ □□  
□□.

**Answer: B (LEAVE A REPLY)**

Sanctions and Compliance Domains state that when entities share similar names, regions, or other characteristics with a sanctioned party - even when executive leadership differs - the institution must perform enhanced due diligence to rule out affiliation, ownership, or control links.

The similarity in names ("Al-Falah" vs. "El-Fallah"), geographic proximity, and the involvement of UN-sanctioned terrorism-related activity require deeper investigation.

Compliance teams must confirm corporate records, ownership structure, purpose, and possible indirect connections before making a determination.

Automatic rejection is premature without evidence. Onboarding without further investigation is inappropriate.

Reference:

Name similarity and geographic proximity as sanctions escalation triggers.

Requirements for enhanced due diligence when possible indirect links exist.

**NEW QUESTION: 5**

□□ □□□ □□□ □□□□□ □□□ □□ □□ □□ □□□ □□ □□□ □□□□ □□  
□ □□□□ □□, □□ □□□ □□ □□ □□□ □□□ □□□?

- A. □□□ □□ □□ □□□ □□□□□ □□□ □□□□ □□ □□, □□ □□□ □□ □□  
□□□□ □□□□ □□□ □□□□ □□□.
- B. □□□ □□, □, □□ □□□ □□□□□ □□ □□□ □□□□ □□ □□□ □□ □ □  
□ □□□ □□□ □□□ □□□□.
- C. □□□ □□□ □□□ □□ □□ □□ □□□ □□, □ □□ □□□ □□□ □□□ □□□  
□.
- D. □□□ □□□ □□□ □□□ □□, □□□ □□□□ □□□□ □□□□ □□ □□□ □  
□□□ □□□.

**Answer: D (LEAVE A REPLY)**

Sanctions screening standards require that when a hit is produced by the filtering system, the institution must determine whether the alert is a true match or a false positive through a structured escalation and investigation process. The Sanctions and Compliance Domains emphasize that financial institutions must evaluate all relevant identifiers, including entity type, name, ownership, vessel IMO numbers, and additional attributes.

In the case of vessels, sanctions regulations often target vessels by name and ownership, meaning that a vessel with an identical name requires deeper investigation. Authorities such as OFAC, the EU, and the UK regularly designate vessels because of their involvement in sanctioned activities, and vessel names frequently overlap with commercial entities. Therefore, the correct investigative approach is to continue the investigation to determine the true ownership, IMO number, and whether the vessel is the sanctioned party.

Options A, B, and C describe scenarios typically associated with clear mismatches or cases where additional investigation is unnecessary because essential identifiers do not match. However, vessels require continued review due to the regulatory emphasis on vessel ownership, registration, and operational control as determining factors in sanctions risk.

Reference from Sanctions and Compliance Domains:

Requirements for detailed matching processes in sanctions screening.

Guidance on evaluating entity type, ownership, and identifiers when reviewing alerts.

Rules relating to vessel sanctions, ownership determination, and verification steps.

Procedures for identifying true matches versus false positives in sanctions screening.

#### NEW QUESTION: 6

□□ □□□ □□□ □□□ □□ □□ □□□□ □□□□□ □□□□□.

A. □□□ □□.

B. □□□□.

C. □□□.

D. □□ □□.

**Answer: C (LEAVE A REPLY)**

Sanctions and Compliance Domains explain that fuzzy logic screening includes phonetic algorithms (e.g., Soundex, Metaphone) to identify variations in the spelling or pronunciation of names. This allows a screening tool to detect near matches and transliteration differences that would not match under exact-match logic.

Inequality lists, big data, and whitelists are not fuzzy matching algorithms. Whitelists are used for reducing false positives, not matching logic.

Reference:

Use of phonetic-based algorithms in fuzzy matching.

Screening methodologies for variant spellings and transliterations.

#### NEW QUESTION: 7

OFAC (ONC) has designated various entities and jurisdictions. Which of the following is NOT a designated entity or jurisdiction?

- A. Hackers and cyber actors involved in cryptocurrency theft.
- B. Cryptocurrency exchanges facilitating illicit transactions or supporting sanctioned jurisdictions.
- C. Mixers (tumblers) known to anonymize blockchain transactions and facilitate laundering and sanctions evasion.
- D. Software developers (D) are generally not designated unless directly linked to illicit activity.
- E. Credit unions and central banks are not typical OFAC digital-asset designations.
- F. None of the above.

**Answer: (SHOW ANSWER)**

OFAC has designated:

- \* Hackers and cyber actors involved in cryptocurrency theft.
- \* Cryptocurrency exchanges facilitating illicit transactions or supporting sanctioned jurisdictions.
- \* Mixers (tumblers) known to anonymize blockchain transactions and facilitate laundering and sanctions evasion.

Software developers (D) are generally not designated unless directly linked to illicit activity.

Credit unions and central banks are not typical OFAC digital-asset designations.

Reference:

OFAC digital asset designations (e.g., mixers, DPRK cyber actors).

Sanctions risk indicators in the virtual currency sector.

### NEW QUESTION: 8

Wolfsberg emphasizes data quality as the most important factor when developing or maintaining a screening system. High-quality, accurate, complete, and consistently structured data is essential to ensure proper matching, reduce false positives, and avoid missed true matches.

- A. High-quality, accurate, complete, and consistently structured data is essential to ensure proper matching, reduce false positives, and avoid missed true matches.
- B. High-quality, accurate, complete, and consistently structured data is essential to ensure proper matching, reduce false positives, and avoid missed true matches.
- C. High-quality, accurate, complete, and consistently structured data is essential to ensure proper matching, reduce false positives, and avoid missed true matches.
- D. High-quality, accurate, complete, and consistently structured data is essential to ensure proper matching, reduce false positives, and avoid missed true matches.

**Answer: A (LEAVE A REPLY)**

The Wolfsberg Guidance on Sanctions Screening emphasizes data quality as the most important factor when developing or maintaining a screening system. High-quality, accurate, complete, and consistently structured data is essential to ensure proper matching, reduce false positives, and avoid missed true matches.

Even with strong IT capabilities or defined risk appetite, a screening system will fail if the underlying data is incomplete or inaccurate.

Reference:

Wolfsberg Guidance: primacy of data quality in sanctions screening.

Importance of accurate customer and transaction data for effective matching.

### NEW QUESTION: 9

Which of the following is a common indicator of illicit procurement?  
A. Using a shell company to procure goods on behalf of a sanctioned end-user commonly involves concealing the true final destination. Sanctions and Compliance Domains describe this as a primary evasion technique in illicit procurement chains, where shell companies mask the ultimate recipient, shipment routing, and country of origin or destination.

A. Using a shell company to procure goods on behalf of a sanctioned end-user commonly involves concealing the true final destination. Sanctions and Compliance Domains describe this as a primary evasion technique in illicit procurement chains, where shell companies mask the ultimate recipient, shipment routing, and country of origin or destination.

B. Consolidation of goods and changes in ownership structure may occur in other schemes but the key deceptive tactic in this question is the concealment of the actual final destination.

C. Reference: Illicit procurement and diversion typologies involving shell companies. Concealment of end-users and destination as a sanctions evasion indicator.

D. Consolidation of goods and changes in ownership structure may occur in other schemes but the key deceptive tactic in this question is the concealment of the actual final destination.

**Answer: A (LEAVE A REPLY)**

Using a shell company to procure goods on behalf of a sanctioned end-user commonly involves concealing the true final destination. Sanctions and Compliance Domains describe this as a primary evasion technique in illicit procurement chains, where shell companies mask the ultimate recipient, shipment routing, and country of origin or destination.

Consolidation of goods and changes in ownership structure may occur in other schemes but the key deceptive tactic in this question is the concealment of the actual final destination.

Reference:

Illicit procurement and diversion typologies involving shell companies.

Concealment of end-users and destination as a sanctions evasion indicator.

#### NEW QUESTION: 10

Which of the following is a common indicator of illicit procurement?  
A. Using a shell company to procure goods on behalf of a sanctioned end-user commonly involves concealing the true final destination. Sanctions and Compliance Domains describe this as a primary evasion technique in illicit procurement chains, where shell companies mask the ultimate recipient, shipment routing, and country of origin or destination.

A. Using a shell company to procure goods on behalf of a sanctioned end-user commonly involves concealing the true final destination. Sanctions and Compliance Domains describe this as a primary evasion technique in illicit procurement chains, where shell companies mask the ultimate recipient, shipment routing, and country of origin or destination.

B. Consolidation of goods and changes in ownership structure may occur in other schemes but the key deceptive tactic in this question is the concealment of the actual final destination.

C. Reference: Illicit procurement and diversion typologies involving shell companies. Concealment of end-users and destination as a sanctions evasion indicator.

D. Consolidation of goods and changes in ownership structure may occur in other schemes but the key deceptive tactic in this question is the concealment of the actual final destination.

**Answer: (SHOW ANSWER)**

Using a USD-denominated account creates a US nexus, because USD transactions must clear through the US financial system. Routing payments through USD accounts while obscuring the sanctioned jurisdiction or buyer is a known sanctions-evasion technique. This is especially true in cases involving comprehensive sanctions (e.g., Iran, North Korea, Cuba), where attempts to hide identifying information in payment orders show intent to evade regulatory controls.

Reference:

OFAC guidance on US nexus in USD transactions.

Evasion indicators including concealment of sanctioned jurisdictions or parties.

#### NEW QUESTION: 11

Which of the following is a common indicator of illicit procurement?  
A. Using a shell company to procure goods on behalf of a sanctioned end-user commonly involves concealing the true final destination. Sanctions and Compliance Domains describe this as a primary evasion technique in illicit procurement chains, where shell companies mask the ultimate recipient, shipment routing, and country of origin or destination.

A. Using a shell company to procure goods on behalf of a sanctioned end-user commonly involves concealing the true final destination. Sanctions and Compliance Domains describe this as a primary evasion technique in illicit procurement chains, where shell companies mask the ultimate recipient, shipment routing, and country of origin or destination.





Sanctions and Compliance Domains specify that when a transaction shows significant sanctions or illicit-trade red flags, a bank must avoid executing the transaction if it risks breaching sanctions restrictions. If the bank identifies discrepancies, counterfeiting indicators, or potential sanctions violations, the transaction must be rejected unless a blocking requirement applies.

Blocking applies only when a sanctioned party or property interest is identified. In this scenario, because there are red flags but no confirmed designated person, the appropriate action is to reject the transaction and file the relevant report with the competent authority. Banks should not process the transaction and investigate later, nor should they disclose red-flag details to customers. Reporting requirements prohibit tipping-off in such regulatory contexts.

Reference from Sanctions and Compliance Domains:

Guidance on rejection versus blocking in trade finance risks.

Reporting obligations when red flags indicate possible sanctions exposure.

Prohibition on providing details of internal investigations to customers.

#### NEW QUESTION: 15

□□□□□□□(OFAC)□ 50% □□□ □□, □□□□□□(SDN) □□□ □□□□ □□ □  
□□ □□□ □□ □□□ □□□□□? (□ □□□ □□□□□.)

A. SDN□ □□ 98%□ □□□ □□

B. SDN□ 35% □□□ □□□□ □□ SDN□ 15% □□□ □□□ □□

C. SDN□ 20% □□□ □□□□, □□ SDN□ 25% □□□ □□□ □□

D. SDN□ 12% □□□ □□□□, □□ SDN□ 18% □□□ □□□□, □ □□ SDN□ 28%  
□□□ □□□ □□

E. SDN□ 45% □□□ □□□□ □□ SDN□ 3% □□□ □□□ □□

F. 10□□ SDN□ □□□□ □□□, □ SDN□ 4%□ □□□ □□□ □□

**Answer: A,B,D (LEAVE A REPLY)**

Under the OFAC 50% Rule, an entity must be treated as a Specially Designated National (SDN) - even if not named on the SDN List - when:

One SDN owns 50% or more of the entity, OR

Multiple SDNs collectively own 50% or more of the entity (ownership must be aggregated).

Applying this rule:

A: 98% ownership by a single SDN → Blocked (exceeds 50%).

B: 35% + 15% = 50% aggregate ownership by two SDNs → Blocked (meets 50%).

C: 20% + 25% = 45%, which does not meet the threshold → Not blocked.

D: 12% + 18% + 28% = 58% aggregate ownership by SDNs → Blocked (exceeds 50%).

E: 45% + 3% = 48%, which is below 50% → Not blocked.

F: 10 SDNs × 4% = 40%, which is below 50% → Not blocked.

Thus, only A, B, and D meet or exceed the 50% aggregate ownership requirement defined by OFAC.

Reference:

OFAC "50 Percent Rule" Guidance: Entities owned 50% or more, directly or indirectly, singly or in the aggregate by one or more SDNs, are considered blocked.  
OFAC Ownership and Control Interpretive Guidance detailing aggregation of SDN ownership percentages.

**NEW QUESTION: 16**

□□□ □□□ □□ □□□□□.

- A. □□□ □□□ □□□□ □□□□□ □□□ □□□□ □□□□□.
- B. □□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□□.
- C. □□□ □□ □□□□ □□ □□□□ □□□□□ □□□□□□□.
- D. □ □□□ □□□□ □□ □□□ □□□□□.

**Answer: D (LEAVE A REPLY)**

Transliteration is defined as converting writing from one script into another while preserving pronunciation as closely as possible. In sanctions screening, transliteration is important because sanctioned parties may appear in multiple scripts (e.g., Cyrillic, Arabic, Mandarin) and the automated screening system must recognize these variations.

While option B focuses specifically on converting non-Latin scripts into Latin, sanctions screening requires a broader definition that applies to any script-to-script conversion relevant to matching names globally. Thus, the correct definition is the general conversion of text from one script into another.

Reference from Sanctions and Compliance Domains:

Definition of transliteration in sanctions screening and name-matching methodologies.

Need for script conversion to support accurate detection of sanctioned parties across language systems.

**CGSS-KR** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CGSS-KR □  
□! DumpTop □ □□ **CGSS-KR** □□ □□□ □□□□□□, DumpTop CGSS-KR □□  
□□□ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□  
DumpTop CGSS-KR □□□ □□□□□. <https://www.dumptop.com/ACAMS/CGSS-KR-dump.html> (103 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

**NEW QUESTION: 17**

□□ □□□ □□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□ □□□□□?

- A. □□□ □□
- B. □□ □□
- C. □□ □□
- D. □□□ □□

**Answer: D (LEAVE A REPLY)**

Sectoral sanctions target specific sectors of a foreign country's economy, such as defense, energy, mining, or financial services. These sanctions apply to persons or entities operating within those sectors and often restrict specific types of transactions (e.g., certain financing or technology transfers).

Comprehensive sanctions cover entire jurisdictions. Individual or corporate sanctions apply to specific persons or companies but are not sector-based.

Reference:

Definition of sectoral sanctions using economic sector targeting.

Distinction between sectoral and comprehensive sanctions.

### NEW QUESTION: 18

□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□□? (□ □□ □□)

A. □□□□ □ □□ □□

B. □□ □□□□ □□□ □□ □□□ □□ □□

C. □□ □□□ □□ □□

D. □□ □□□□ □ □□□

E. □□□□ □□□ □□□

F. □□ □□□ □□□

**Answer: A,B,D (LEAVE A REPLY)**

Sanctions and Compliance Domains explain that model validation for sanctions screening systems must include:

- \* Governance and management oversight, ensuring independent review, escalation paths, and proper control structures.

- \* Identification and verification of all data sources, ensuring that all required and relevant reference data feeds are included in screening.

- \* Matching algorithms and thresholds, which require testing, calibration, and validation to ensure accurate detection of potential sanctions matches.

Storage capacity, automation, or multiple administrators are operational considerations but not core components of model validation.

Reference:

Requirements for model governance and oversight.

Validation of data sources and matching logic.

Threshold testing and system calibration expectations.

### NEW QUESTION: 19

□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□□ □ □□□ □□□□.

A. □□ □.

B. □□ □□.

C. □□ □□.

D. □□□□ □□.

**Answer: (SHOW ANSWER)**

Sanctions and Compliance Domains state that screening calibration must be tied directly to a financial institution's sanctions risk assessment, which evaluates products, customer base, geography, delivery channels, and transaction volume. Sensitivity adjustments must be justified by an institution's assessed sanctions exposure.

Staff levels or training do not determine screening thresholds; these are operational considerations. Management commitment supports governance but does not form the technical basis for calibration decisions.

Reference:

Screening calibration tied to sanctions risk assessments.

Threshold adjustments must reflect actual sanctions exposure and transaction characteristics.

**NEW QUESTION: 20**

□□ □□□□ □□ □□ □□□ □□ □□□□□. □□ □□, □□ □□□ □□ □□ □ □□ □□ □□□ □□□□ □□□□ □□□ □□□□. □□□□ □□ □□□ □□ □□ □ □□□ □□□?

- A. □□□□ □□□□□.
- B. □□ □□□□□ □□□□□.
- C. □□ □□□ □□ □□□□ □□ □□ □□□ □□□□□.
- D. □□□ □□□□□.

**Answer: C (LEAVE A REPLY)**

In sanctions compliance frameworks applied globally by bodies such as OFAC, the EU, the UN, the UK, Canada, and Australia, transactions involving humanitarian goods, including medicine and medical supplies, are treated under specific regulatory categories. These frameworks include humanitarian exemptions, general licenses, and permitted transactions for medical or health-related items. The standard compliance expectation requires an analyst to determine whether the activity is already authorized before taking restrictive action.

The Sanctions and Compliance Domains specify that when a transaction involves potential humanitarian goods, the analyst must confirm whether a general license or exemption applies. General licenses commonly authorize exports of medicines, medical devices, and humanitarian materials to sanctioned jurisdictions. The rule requires verification of these authorizations prior to escalation, rejection, or requesting a specific license.

If a general license exists for the type of goods or activity, the transaction may proceed in accordance with regulatory conditions. Only when no exemption or general license applies should a specific license be sought. Therefore, the correct immediate step for the analyst is to check applicable general licenses or exemptions related to medical exports.

Reference from Sanctions and Compliance Domains:

Regulatory requirements relating to humanitarian exemptions under sanctions programs.

General license structures for medical and humanitarian goods in sanctions regimes.

Compliance procedures directing analysts to verify authorizations or exemptions before rejecting or escalating transactions.

Standard sequencing: determine applicability of general licenses or exemptions prior to requesting a specific license.

**NEW QUESTION: 21**

Which of the following is a recognized sanctions evasion technique?

A. Structuring transactions to avoid reporting thresholds.

B. Using shell companies to obscure the true ownership of a transaction.

C. Using multiple payment methods to avoid detection.

D. Using intermediaries to route transactions through high-risk jurisdictions.

**Answer: (SHOW ANSWER)**

"Stripping" refers to removing, altering, or replacing material information from payment messages, invoices, or trade documents to conceal a sanctioned party, vessel, location, or jurisdiction. It is a recognized sanctions evasion technique used by actors seeking to bypass automated screening.

Examples include removing the sanctioned port name, omitting the ultimate consignee, or deleting identifying references.

This is distinct from structuring (option A), price manipulation (B), or dual messaging (C).

Reference:

Sanctions evasion typologies involving manipulation or removal of identifying information.

Trade and payment message alteration risks.

**NEW QUESTION: 22**

Which of the following is a recognized sanctions evasion technique?

A. Structuring transactions to avoid reporting thresholds.

B. Using shell companies to obscure the true ownership of a transaction.

C. Using multiple payment methods to avoid detection.

D. Using intermediaries to route transactions through high-risk jurisdictions.

**Answer: (SHOW ANSWER)**

OFAC guidance clarifies that blocking virtual currency means preventing any access, transfer, or withdrawal of the asset by the sanctioned party. The entity holding the virtual currency must:

Deny access to the wallet or virtual asset, and

Report the blocked property to OFAC in accordance with reporting rules.

Virtual currencies are not "returned" (A), not necessarily moved to a pooled wallet (B), and are not converted to fiat unless authorized (C).

Reference:

OFAC Virtual Currency Guidance on blocking and reporting.

Requirements for preventing access to digital assets belonging to sanctioned persons.

**NEW QUESTION: 23**

Which of the following is a red flag for sanctions exposure? (Select all that apply.)

- A. Payment made to a sanctioned entity.
- B. Payment made to a sanctioned entity, but the payment is made to a third party.
- C. Payment made to a sanctioned entity, but the payment is made to a third party.
- D. Payment made to a sanctioned entity, but the payment is made to a third party.

**Answer: (SHOW ANSWER)**

Sanctions and Compliance Domains outline that references to sanctioned ports, locations, or shipping routes in payment instructions require further investigation. Even when the transaction parties are not located in a sanctioned jurisdiction, involvement of a sanctioned port or movement of prohibited goods can trigger sanctions exposure.

The correct approach is to obtain supporting documents such as shipping documents, invoices, bills of lading, and routing information to confirm whether the shipment, goods, transport path, or third parties have any sanctioned involvement. Approving or rejecting a payment without verification contradicts sanctions screening standards.

Reference from Sanctions and Compliance Domains:

Requirements to investigate references to sanctioned locations in trade or payment messages.

Guidance on obtaining underlying documents to assess sanctions exposure.

Expectations for verifying goods, ports, and shipment paths.

**NEW QUESTION: 24**

Which of the following is a red flag for sanctions exposure? (Select all that apply.)

- A. Payment made to a sanctioned entity.
- B. Payment made to a sanctioned entity, but the payment is made to a third party.
- C. Payment made to a sanctioned entity, but the payment is made to a third party.
- D. Payment made to a sanctioned entity, but the payment is made to a third party.

**Answer: C (LEAVE A REPLY)**

A key sanctions-evasion red flag in trade documents is reluctance or refusal to disclose end-use or end-user information. This may indicate diversion to a sanctioned jurisdiction, entity, or prohibited program (e.g., proliferation).

Expiration dates (D) are irrelevant to sanctions. Payment timing and product suitability (A, B) are normal commercial behaviors and not sanctions red flags.

Reference:

Trade-based sanctions-evasion indicators (concealed end-user/end-use).  
Red flags involving incomplete or intentionally vague documentation.

**NEW QUESTION: 25**

□□ □□□ □□ □□ □□□ □□□□□. □□ □□□ □□□ □□ □□□□□.

- A. □□ □□□ □□ □□□ □□ □□□ □□□ □ □□.
- B. □□□□ □□□ □□□ □□□ □□□□ □□□□□.
- C. □□□ □□, □□, □□□ □□□□□.
- D. □□□ □□□□, □□□□ □□□ □□□ □□□□ □□ □□□ □ □□□□.

**Answer: C (LEAVE A REPLY)**

UN sanctions are imposed by the UN Security Council as part of its mandate to maintain international peace and security. They are intended to influence behavior, prevent conflict, suppress terrorism, and stabilize global security conditions.

While asset freezes and travel bans are common measures (option D), they are examples, not the fundamental reason for imposing sanctions. Option C describes the overarching purpose.

Reference:

UN Security Council mandate under the UN Charter.

Objectives of UN sanctions in global peace and security.

**NEW QUESTION: 26**

□□ □□□ □□ □□ □□ □□□□ □□□□ □□□ □□□□□?

- A. □□ □□□ □□ SWIFT □□□ □□ □□□□ □□□□ □□ □□/□□ □□□ □□□ □□□□□.
- B. □□ □□□ □□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□□□ □□□□ □.
- C. □□ □□□ □□ □□ □□□□□ □□ □□ □□ □□□ □□□□□.
- D. □□ □□□ □□□□□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□ □□□ □□□□.

**Answer: D (LEAVE A REPLY)**

Sanctions and Compliance Domains outline that institutions must maintain effective and reliable sanctions screening systems. This includes screening all incoming and outgoing payment messages, and institutions may not rely solely on correspondent banks for sanctions controls. Screening tools must also be capable of detecting alternative spellings, transliterations, and name variations of sanctioned parties.

Sanctions list updates must be incorporated immediately or as soon as practicable after publication. Monthly updates would be considered insufficient.

The use of controlled internal whitelists, combined with proper governance, periodic review, and controlled threshold calibration, is an accepted method used to reduce false positives while maintaining compliance integrity. Threshold adjustments must always follow documented validation, testing, and oversight procedures.

### Reference from Sanctions and Compliance Domains:

Requirements for screening all payment messages, including incoming SWIFT transfers.

## System expectations for matching name variations and alternative spellings.

## Regulatory expectations for timely list updates.

Recognition of whitelist use and threshold calibration as acceptable screening optimization methods.

**NEW QUESTION: 27**

EU □□ □□□ □□□□□. (□ □□□ □□□□□.)

**A.** EU □□□□ □□□□ □□ □□□□.

**B. EU** ☐☐☐ ☐☐☐ 45% ☐ ☐☐☐ ☐ EU ☐☐☐ ☐☐☐ ☐ ☐☐☐ ☐.

C. ☐ ☐ EU ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ EU ☐ ☐ ☐.

**D. EU □ □ □ □ □ □ □ □ EU □ □ □.**

**E. EU □□□□ □□□ □□ □□□□□ □□□ EU □□ □□□ □□.**

**Answer: A,E (LEAVE A REPLY)**

EU Restrictive Measures apply to all persons and entities within the territory of the EU, including airspace and territorial waters, and to any vessel or aircraft under the jurisdiction of an EU Member State. This establishes that sanctions obligations extend to vessels registered under EU jurisdictions regardless of location.

EU sanctions also apply to all legal persons, entities, and bodies incorporated or constituted under the law of an EU Member State, even when those entities operate entirely outside EU territory. Legal incorporation under EU law creates an ongoing obligation to comply with EU sanctions.

EU ownership by itself does not trigger sanctions applicability, so a non-EU company that is 45% owned by an EU national does not fall under EU Restrictive Measures. Additionally, arrangements such as double-taxation conventions or participation in customs union agreements do not extend the territorial or legal applicability of EU sanctions to non-EU jurisdictions.

### Reference from Sanctions and Compliance Domains:

Territorial applicability of EU sanctions, including vessels and aircraft under Member State jurisdiction.

Applicability to companies incorporated under EU Member State law regardless of geographic operations.

## Legal and territorial definitions outlining the scope of EU Restrictive Measures.

**NEW QUESTION: 28**

□□□ □□ □□ □□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□ □□□ □□  
 □□ □□□ □□□□ □□□□. □□□□□ □□ □□□ □□ □□□ □□□ □□□□ □  
 □□? (□ □□ □□)

**A.** □□□□ □□□□ □□ □□□.

**B.** □□□□□ □□□ □□ □□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□□

**C.** □□□□□□ □□□ □□□□ □□ □□□□□□ □□□ □□□ □□□□□.

D. □□□ □□□ □□ □□ □□ □□□ □□□ □□ □□□ □□□□ □□□ □□□  
□□□ □□□ □□□□□.

E. □□□□□ □□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□□ □□□□□ □□□□□ □□ □□ □□.

**Answer: A,B (LEAVE A REPLY)**

Enhanced due diligence is required when trade transactions involve jurisdictions near sanctioned countries due to the increased risk of transshipment, diversion, and sanctions evasion.

Sanctions and Compliance Domains highlight two core focus areas:

- \* verifying the identities and ultimate beneficial owners of all involved parties, and
- \* validating the shipment details, including routing, goods description, and movement patterns.

These elements are critical where geographic proximity raises sanctions exposure. While reviewing commercial terms and pricing may be part of general trade finance due diligence, the primary sanctions-specific EDD requirements focus on beneficial ownership and shipment details.

### Reference from Sanctions and Compliance Domains:

Enhanced due diligence expectations for trade involving high-risk regions.

## Requirements to verify UBOs to detect potential sanctioned ownership.

Importance of shipment route verification to detect diversion to sanctioned jurisdictions.

**NEW QUESTION: 29**

□□□□□□□(ONA)□ 50% □□□ □□ □□□ □□ C□ □□□□□? (□ □□□ □□□ □□.)

**A.** □□□ □□ X□ □□ A□ 50%□ □□□□□. □□ A□ □□ C□ 50%(1□)□ □□□□  
□. □□□ □□ X□ □□ C□ 1□□ □□ □□□□□.

**B.** □□□ □□ X□ □□□ A□ 50%, □□□ B□ 50%□ □□□□□. □□□ A□ B□ □□ □□□ C□ 25%□ □□□□□.

**C.** □□□ □□ X□ □□ A□ 50%(1□)□ □□□□ □□□□. □□ A□ □□ B□ 50%(1□) □□□□□ □□□□. □□ B□ □□ C□ 50%(1□)□ □□□□ □□□□.

**D.**  $\frac{1}{4}$   $\frac{1}{4}$   $\frac{1}{4}$  A  $\frac{1}{4}$   $\frac{1}{4}$   $\frac{1}{4}$  B  $\frac{1}{4}$  50%  $\frac{1}{4}$   $\frac{1}{4}$   $\frac{1}{4}$   $\frac{1}{4}$ .  $\frac{1}{4}$   $\frac{1}{4}$  B  $\frac{1}{4}$   $\frac{1}{4}$   $\frac{1}{4}$  C  $\frac{1}{4}$  50%  $\frac{1}{4}$   $\frac{1}{4}$   $\frac{1}{4}$ .

E.  $\frac{1}{4} \times \frac{1}{4} \times \frac{1}{4} = \frac{1}{64}$ ,  $\frac{1}{4} \times \frac{1}{4} \times \frac{1}{4} = \frac{1}{64}$ .  $\frac{1}{64} \times \frac{1}{64} = \frac{1}{4096}$ .

**F.** □□□ □□□ A□ □□□ B□ 49.99%□ □□□□ □□□□. □□□ B□ □□□ C□ 49.99%□ □□□□ □□□□.

**Answer: A,C,D (LEAVE A REPLY)**

The OFAC 50% Rule states:

- \* Any entity owned 50% or more - directly or indirectly - by an SDN or SDN-owned entity is itself automatically blocked.

\* Ownership is cumulative through all tiers.

Apply the rule:

✓ A - Blocked Person X has direct + indirect ownership in Entity C exceeding 50% → Blocked.

✓ C - Ownership cascades: SDN → A → B → C; each at 50%. Result: Entity C is blocked.

✓ D - Blocked Entity A (>50%) → owns B (>50%) → owns C (>50%). All downstream entities are blocked.

Not blocked:

\* B = 25% + 25% = 50% but SDN does not directly own A or B - the SDN owns A and B, but A and B each are not blocked themselves because ownership is not aggregated across separate entities unless they hold shares. Therefore, C is not blocked.

\* E = Only 25% flows into Entity C.

\* F = Neither ownership chain reaches 50%.

Reference:

OFAC 50% Rule on direct and indirect ownership.

OFAC guidance on cascading ownership and aggregation requirements.

### NEW QUESTION: 30

□□ □□□ □□ □□ □□□ □□□□□? (2□ □□)

A. □□ □□ □□

B. □□□□ □□□ □□ □ □□ □□ □□

C. □□ □□ □□

D. □□ □□□□

E. □□ □□□ □□□

Answer: ([SHOW ANSWER](#))

Sanctions investigations rely primarily on the factual evidence contained in transaction activity and on authoritative, government-issued sanctions lists. Transaction details provide information on counterparties, payment paths, goods, and purpose. Official blocked-person lists such as OFAC, EU, UN, and national export-control lists provide the authoritative basis for sanctions matching. News, social media, and internal correspondence may supplement context but are not primary sources.

Reference:

Transaction activity as primary investigative data.

Mandatory reliance on official sanctions and export-restriction lists.

### NEW QUESTION: 31

□□ □□□□ □□ □□□□□ □□□□□□ □ □□□□ □□□ □□□ □□□□ □□□  
□□□□ □□□(LC) □□□ □□□□□. □□□□ □□ □□□ □□□ □□□?

A. 2□ □□□ □□□□ □ □□ □□□□ □□□ □□□□.

B. □□ □□□ □□□□ □□□□ LC□ □□□□□.

C. LC□ □□ □□□□ □□ □□□ □□□□□ □□□□□.

D. □□ □□□ □□□□ □□ □□□ □□□□.

**Answer: A (LEAVE A REPLY)**

Sanctions and Compliance Domains state that when a potential sanctions match occurs, the first step is to conduct a proper investigation to determine whether the alert is a true match or false positive. This includes obtaining additional identifiers such as addresses, IMO numbers, registration numbers, or corporate details.

Immediate rejection or reporting is only appropriate after confirming a true match.

Premature rejection without verification violates due diligence expectations. Closing the customer account is not justified without confirmed sanctions involvement.

Reference:

Investigation procedures for potential sanctions matches.

Requirements to gather additional identifiers before determining match status.

**CGSS-KR** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ CGSS-KR □  
□! DumpTop □ □□ **CGSS-KR** □□ □□□ □□□□□□, DumpTop CGSS-KR □□  
□□□ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□  
DumpTop CGSS-KR □□□ □□□□□. <https://www.dumptop.com/ACAMS/CGSS-KR-dump.html> (103 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

### NEW QUESTION: 32

□□ □□□ □□□□ □□□ □□□ □□□ □□□□□? (□ □□ □□)

A. □□ □□□ □□□□□ □□ □□□ □□□ □□□□□.

B. □□□ □□□ □□ □□ □□□ □□□ □□□□□.

C. □□ □□□ □□ □□□ □□□ □□□ □ □□ □□□□□.

D. □□ □□□ □□□□□□ □□□ □□□□.

E. □□ □□□□□□□ □□□□□□ □□ □□□ □□□□ □□□ □□□.

**Answer: (SHOW ANSWER)**

UN sanctions require agreement among multiple countries, making them more difficult to enact than unilateral national sanctions. The UN Security Council must reach consensus, and all five permanent members must avoid using their veto power. Any negative vote by a permanent member blocks the resolution entirely.

This requirement for global political alignment is the primary barrier to rapid sanctions adoption. UN sanctions are neither autonomous nor inherently ineffective, and they do not exist to intervene in domestic affairs but to protect international peace and security under Chapter VII of the UN Charter.

Reference:

UN Security Council voting procedures and veto rules.

Multilateral consensus requirements for adopting UNSC sanctions.

**NEW QUESTION: 33**

Wolfsberg □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □  
□ □ ? (□ □ □ □)

- A.** □□ □□□ □□□□ □□□□ □□□ □□□□□ □□□□ □□ □□□□
- B.** □□□□ □□□ □□□ □□ □□□□ □□ □□ □□
- C.** □□□□ □□ □□ □□□ □□□□ □□□ "□□ □□" □□□ □□□□ □□□ □□□ □□□.
- D.** □□ □□□□ □□□ □□□ □□ □□ □□□□ □□□ □□□□□.
- E.** □□□□ □ □□ □□□ □□□ □□ □□ □□□□□ □□ □□□□ □□□□ □□□ □□□ □□□□□.

**Answer: C,E (LEAVE A REPLY)**

The Wolfsberg Guidance identifies that effective sanctions screening depends on high-quality, risk-relevant reference data. Institutions must regularly review and remove outdated or irrelevant data to avoid generating unnecessary alerts and ensure screening outputs remain meaningful. Maintaining accurate and current data reduces noise and increases the productivity of alerts.

The Guidance also emphasizes that institutions may use "good guy lists" to reduce false positives, but these lists must be maintained in a controlled way to ensure they do not unintentionally suppress alerts that could indicate sanctions risk. Proper governance must accompany good-guy lists so that risk-relevant entities are not excluded from screening. The Guidance does not support reducing thresholds to generate more alerts, nor does it promote removing low-risk parties without structured criteria. It also does not recommend manual jurisdiction-specific screening as a method of improving alert quality.

### Reference from Sanctions and Compliance Domains:

Wolfsberg principles on management of reference data for sanctions screening.

## Guidance on proper use and governance of "good guy lists."

Recommendations for ensuring alerts remain relevant, accurate, and risk-based.

**NEW QUESTION: 34**

□□ □□□ □□□ EU □□ □□□ □□, □□ □□□ □□□ □□□ □□□□ □□ □□  
□ □□□ □ □□□□?

- A.** □ □ □ □
- B.** □ □
- C.** □ □ □ □
- D.** □ □ □ □ □ □

**Answer: A (LEAVE A REPLY)**

EU best practices allow processing of payments that fall under permitted exemptions such as basic needs and reasonable living expenses. These may include essential subscriptions such as newspapers or communication services, provided proper authorization or notification is followed.

Salary payments generally require strict conditions and may not be allowed directly for designated persons. Taxi rides and luxury purchases are not considered basic or essential needs and cannot be processed.

Reference:

EU restrictive measures exemptions for basic needs and essential services.

Conditions for processing payments for designated persons.

### NEW QUESTION: 35

"□□ □□"□ □□□□ □□□ □□□□□? (2□ □□)

- A. □□ □□□ □□□□ □□
- B. □□□ □□□□ □□
- C. □□□ □□□ □□
- D. □ □ □□□□ □□□□ □□
- E. □□□ □□ □□□ □□ □□

**Answer: (SHOW ANSWER)**

Sanctions and Compliance Domains identify "weak aliases" as variations of names that do not robustly identify an individual. These include:

- \* Nicknames - informal or shortened versions ("Alex" vs. "Aleksandr"), often used for concealment.
- \* Names with numbers - identifiers that are easily fabricated and not tied to legitimate naming conventions.

Middle names, titles, or long names are normal cultural variations and not considered weak aliases for screening purposes.

Reference:

Alias risk classification in sanctions screening.

Use of weak identifiers such as nicknames and numeric elements.

### NEW QUESTION: 36

□□ □□□ □□□□ □□, □□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □ □□□□.

- A. □□ □□□□ □□□□ □□□ □□□ □□□□□.
- B. □□□ □ □□□□ □□□ □□□□ □□ □□□ □□□□□.
- C. □□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.
- D. □□ □□□ □□□□ □□ □□□□ □□□ □□□.

**Answer: A (LEAVE A REPLY)**

Sanctions and Compliance Domains state that sanctions clauses in trade contracts are used to:

- \* clarify prohibited activities,
- \* define obligations of the parties in case sanctions become applicable, and
- \* ensure business partners understand compliance expectations.

Routine list updates or daily refreshes do not automatically trigger lookbacks. New sanctions programs may require enhanced forward-looking monitoring, but only missing or newly uncovered data affecting past screening results justify a historical lookback.

Reference:

Requirements for lookbacks when gaps in screening data are discovered.

Identification of previously missing identifiers as a trigger for retrospective review.

**NEW QUESTION: 39**

Which of the following is a primary governance function? (Select all that apply)

A. Reporting based on "lack of penalty" (D) is not a risk-based governance indicator.

B. Human resources actions (A) are not a primary governance function. Reporting based on "lack of penalty" (D) is not a risk-based governance indicator. Zero-tolerance statements (E) do not constitute governance processes and may conflict with risk-based management expectations.

C. Senior management ensuring adequate resources to investigate violations, identify weaknesses, and remediate control gaps.

D. Updating the sanctions risk assessment to incorporate findings and root causes from prior incidents.

E. Zero-tolerance statements (E) do not constitute governance processes and may conflict with risk-based management expectations.

**Answer: (SHOW ANSWER)**

A sound governance framework, according to Sanctions and Compliance Domains, includes:

\* Senior management ensuring adequate resources to investigate violations, identify weaknesses, and remediate control gaps.

\* Updating the sanctions risk assessment to incorporate findings and root causes from prior incidents.

Human resources actions (A) are not a primary governance function. Reporting based on "lack of penalty" (D) is not a risk-based governance indicator. Zero-tolerance statements (E) do not constitute governance processes and may conflict with risk-based management expectations.

Reference:

Governance expectations under OFAC Framework for Compliance Commitments.

Requirements for resource allocation and risk assessment updates.

**NEW QUESTION: 40**

Which of the following are requirements for resource allocation and risk assessment updates? (Select all that apply)

A. Reporting based on "lack of penalty" (D) is not a risk-based governance indicator.

B. 200%

C. 300%

D. 100% of the total

**Answer: (SHOW ANSWER)**

Sanctions and Compliance Domains and regulatory authorities such as OFAC, EU, and OFSI require institutions to update sanctions lists as quickly as possible after a new designation or change is published.

Weekly, biweekly, or monthly cycles are insufficient and can result in missed designations. Financial institutions must adopt systems that update sanctions lists promptly to maintain compliance and avoid facilitating prohibited transactions.

Reference:

Regulatory expectation for immediate or prompt sanctions list updates.

Screening list management best practices for timeliness and accuracy.

#### NEW QUESTION: 41

Which of the following is a prohibited tipping-off practice?

A. Informing a customer that their funds are under investigation, impairing regulatory or law-enforcement action. Institutions must implement controls to prevent it.

B. Informing a customer that their funds are under investigation, without revealing investigative details.

C. Informing a customer that their funds are under investigation, without revealing investigative details.

D. Informing a customer that their funds are under investigation, without revealing investigative details.

**Answer: A (LEAVE A REPLY)**

Sanctions and Compliance Domains explain:

\* Tipping-off is prohibited, as it may alert a customer that they are under investigation, impairing regulatory or law-enforcement action. Institutions must implement controls to prevent it.

\* Notification, however, refers to permitted communication - such as informing a customer that their funds were frozen - when required or allowed by law (e.g., EU asset-freeze requirements), without revealing investigative details.

Tipping-off and notification serve entirely different purposes. Regulatory frameworks explicitly warn entities against tipping-off but do allow certain forms of notification that comply with legal obligations.

Reference:

Regulatory prohibition on tipping-off.

Permitted customer notifications regarding asset freezes or legal procedures.

#### NEW QUESTION: 42

EU export sanctions restrictions apply to goods and services originating from Cuba or other embargoed jurisdictions. Under US OFAC regulations, Cuban-origin goods and services are prohibited from being exported to the EU.

A. Goods and services

B. Goods and services

C. Goods and services

D. Goods and services

**Answer: B (LEAVE A REPLY)**

Cigars, particularly those originating from Cuba or other embargoed jurisdictions, fall under both EU and US export sanctions restrictions. Under US OFAC regulations, Cuban-origin

goods-including cigars-are strictly prohibited from import, export, resale, or re-export by US persons. EU sanctions may also restrict trade with embargoed or designated jurisdictions. Textbooks, toys, and art reproductions generally do not fall under export prohibitions unless tied to dual-use concerns or specific jurisdictions, which is not indicated here. Cigars present the most direct and well-established sanctions risk.

Reference:

US OFAC Cuban Assets Control Regulations on Cuban-origin goods.

EU and US export controls covering embargoed jurisdictions and prohibited commodities.

**CGSS-KR** ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ CGSS-KR ☐  
☐! DumpTop ☐ ☐☐ **CGSS-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop CGSS-KR ☐☐  
☐☐☐ ☐☐☐☐☐☐☐☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐ ☐☐  
DumpTop CGSS-KR ☐☐☐ ☐☐☐☐☐. [https://www.dumptop.com/ACAMS/CGSS-KR-](https://www.dumptop.com/ACAMS/CGSS-KR-dump.html)  
[dump.html](https://www.dumptop.com/ACAMS/CGSS-KR-dump.html) (103 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)