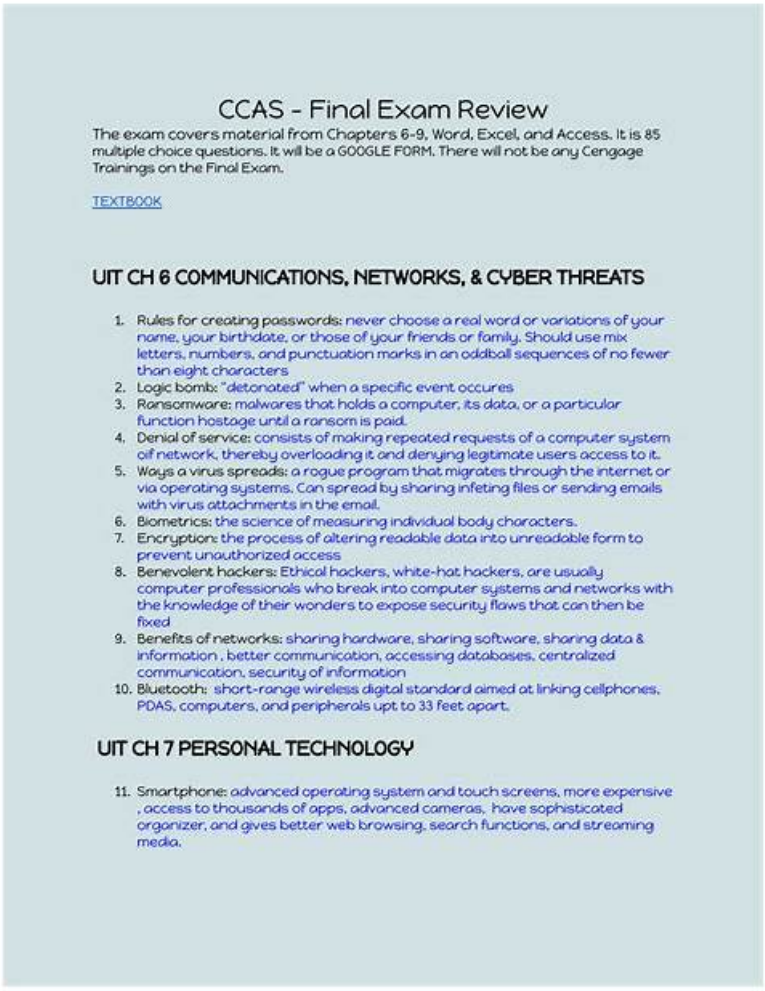
Valid CCAS Test Materials, CCAS Exam Reference



CCAS - Final Exam Review

The exam covers material from Chapters 6-9, Word, Excel, and Access. It is 85 multiple choice questions. It will be a GOOGLE FORM. There will not be any Cengage Trainings on the Final Exam.

TEXTBOOK

UIT CH 6 COMMUNICATIONS, NETWORKS, & CYBER THREATS

1. Rules for creating passwords: never choose a real word or variations of your name, your birthdate, or those of your friends or family. Should use mix letters, numbers, and punctuation marks in an oddball sequences of no fewer than eight characters
2. Logic bomb: "detonated" when a specific event occures
3. Ransomware: malwares that holds a computer, its data, or a particular function hostage until a ransom is paid.
4. Denial of service: consists of making repeated requests of a computer system oif network, thereby overloading it and denying legitimate users access to it.
5. Ways a virus spreads: a rogue program that migrates through the internet or via operating systems. Can spread by sharing infeting files or sending emails with virus attachments in the email.
6. Biometrics: the science of measuring individual body characters.
7. Encryption: the process of altering readable data into unreadable form to prevent unauthorized access
8. Benevolent hackers: Ethical hackers, white-hat hackers, are usually computer professionals who break into computer systems and networks with the knowledge of their wonders to expose security flaws that can then be fixed
9. Benefits of networks: sharing hardware, sharing software, sharing data & information , better communication, accessing databases, centralized communication, security of information
10. Bluetooth: short-range wireless digital standard aimed at linking cellphones, PDAS, computers, and peripherals upt to 33 feet apart.

UIT CH 7 PERSONAL TECHNOLOGY

11. Smartphone: advanced operating system and touch screens, more expensive , access to thousands of apps, advanced cameras, have sophisticated organizer, and gives better web browsing, search functions, and streaming media.

2026 Latest TestInsides CCAS PDF Dumps and CCAS Exam Engine Free Share: https://drive.google.com/open?id=1KiExxDidaCTYOU8j3X6wszXY5KjnDVo2

One of the reason for this popularity is our study material are accompanied by high quality and efficient services so that they can solve all your problems. We guarantee that after purchasing our CCAS test prep, we will deliver the product to you as soon as possible about 5-10 minutes. So you don’t need to wait for a long time or worry about the delivery time has any delay. We will transfer our CCAS Test Prep to you online immediately, and this service is also the reason why our CCAS study torrent can win people’s heart and mind.

Compared with the other CCAS exam questions providers' three months or five months on their free update service, we give all our customers promise that we will give one year free update on the CCAS study quiz after payment. In this way, we can help our customers to pass their exams with more available opportunities with the updated CCAS Preparation materials. You can feel how considerate our service is as well!

>> Valid CCAS Test Materials <<

CCAS Exam Reference - CCAS Valid Exam Registration

The experts in our company are always keeping a close eye on even the slightest change on the CCAS exam questions in the field. Therefore, we can assure that you will miss nothing needed for the CCAS exam. What's more, the latest version of our CCAS Study Materials will be a good way for you to broaden your horizons as well as improve your skills. You will certainly obtain a great chance to get a promotion in your company.

ACAMS CCAS Exam Syllabus Topics:

Topic	Details
Topic 1	• AML Foundations for Cryptoasset and Blockchain: This section of the exam measures skills of Anti-Money Laundering (AML) Officers and Crypto Compliance Specialists. It covers foundational knowledge of AML principles tailored to the cryptoasset and blockchain environment, introducing the regulatory landscape, typologies of financial crime, and the evolving risks associated with cryptoassets.
Topic 2	• Risk Management Programs for Cryptoasset and Blockchain: This section measures expertise of Compliance Managers and Risk Officers in developing and implementing risk management frameworks specifically for the crypto sector. It includes procedures for assessing crypto-related financial crime risks, designing controls, monitoring compliance, and adapting to emerging threats within the cryptoasset ecosystem.
Topic 3	• Cryptoasset and Blockchain: This domain targets Blockchain Analysts and Crypto Risk Managers. It focuses on understanding cryptoasset technologies, blockchain fundamentals, and their operational characteristics. Candidates learn about cryptoasset transaction flows, wallets, exchanges, smart contracts, and the challenges these present to financial crime prevention.

ACAMS Certified Cryptoasset Anti-Financial Crime Specialist Examination Sample Questions (Q24-Q29):

NEW QUESTION # 24
Which activity is most commonly associated with mixing and tumbling as a method of laundering cryptoassets?

- A. Rapid purchase and sale of different cryptocurrencies
- B. Use of IP address concealing software
- C. Frequent transactions to high-risk jurisdictions via different virtual asset service providers
- D. Presence of unknown or disguised source of funds

Answer: D

Explanation:
Mixing and tumbling services are used to obscure the origin of funds by blending multiple transactions, resulting in unknown or disguised sources of funds. This is a classic money laundering technique.
Rapid trades (B), IP address obfuscation (C), and transactions to high-risk jurisdictions (D) are separate or related risks but not direct indicators of mixing/tumbling.

NEW QUESTION # 25
How should an investigator use transaction history to determine whether cryptoassets were previously involved in money laundering?

- A. Assess other assets held by the cryptoasset owner.
- B. Assess the cryptoasset addresses' receiving exposure to illicit activity.
- C. Assess the identity of the cryptoasset owner.
- D. Assess the jurisdiction where the transactions took place.

Answer: B

Explanation:
In the context of AML/CFT frameworks for cryptoassets, the investigation of transaction histories involves blockchain analysis tools to trace the flow of funds to and from crypto addresses. Specifically, it is essential to assess whether the addresses involved have had prior exposure to illicit activities such as known darknet marketplaces, ransomware payments, or sanctioned entities. This form of "address screening" helps identify potentially tainted cryptoassets.
The DFSA AML Module and associated guidance emphasize that transaction monitoring for cryptoassets requires analyzing the provenance of funds, not just ownership. While identifying the owner is part of customer due diligence (CDD), the transactional exposure itself reveals laundering risks embedded in the chain of transfers.
Extract from DFSA AML Module and COB Module on Crypto Business Rules:
"Transaction monitoring systems must include blockchain analysis to detect suspicious activity related to crypto tokens, including

tracing transactions against known illicit sources."
"Enhanced due diligence (EDD) is required when a cryptoasset transaction involves addresses or wallets with a history of illicit activity."
"Risk-based approaches must integrate forensic review of transaction histories to assess financial crime risks in crypto asset transfers"【AML/VER25/05-24: Sections 6.3, 7.3, 13.3; COB/VER45/05-24: Sections 6.13, 15】.
Therefore, assessing the receiving exposure of cryptoasset addresses to illicit activity (Option C) is the most direct and effective method to detect laundering.

NEW QUESTION # 26
Which term describes converting one cryptoasset into another without first converting to fiat?

- A. Layering
- B. Integration
- C. Structuring
- D. Chain hopping

Answer: D

Explanation:
Chain hopping involves moving between blockchains to make tracing harder, often exploiting regulatory gaps.

NEW QUESTION # 27
A compliance officer at an exchange who is conducting an annual risk assessment identifies an increased volume of transactions to and from unhosted wallets. Based on Financial Action Task Force guidance, which inherent risk rating would be most appropriate for the compliance officer to assign to such activities?

- A. High
- B. Negligible
- C. Low
- D. Moderate

Answer: A

Explanation:
The Financial Action Task Force (FATF) guidance on Virtual Assets and Virtual Asset Service Providers (VASPs) explicitly highlights that transactions involving unhosted wallets (wallets not held or controlled by a regulated entity) pose a high inherent risk for money laundering and terrorist financing. This is because unhosted wallets are more difficult to monitor and control, lack identifiable customer information, and are often exploited for illicit activities.
The DFSA AML Module, aligned with FATF recommendations, mandates that Relevant Persons incorporate this risk into their business-wide risk assessments. The increased volume of transactions to and from unhosted wallets should therefore be assigned a high inherent risk rating to trigger enhanced controls such as enhanced due diligence (EDD) and transaction monitoring.
Supporting extracts include:
FATF Guidance on Virtual Assets (October 2021) states: "Unhosted wallets or transactions with them represent a high risk of ML/TF due to limited or no access to identifying information." DFSA AML Module (AML/VER25/05-24) Section 4.1 & 6.1 on Risk-Based Approach: mandates firms to assess and rate risks posed by customers and products, explicitly including virtual assets and unhosted wallets as high risk.
COB Module also requires heightened controls and disclosures when dealing with transactions involving unhosted wallets【AML/VER25/05-24: Sections 4.1, 6.1, COB/VER45/05-24: Sections 6.13, 15.6】.
Thus, option D (High) is the correct risk rating.

NEW QUESTION # 28
Which statement describes what a staff member should do If suspicious activity is identified?

- A. Report the suspicious activity immediately to the financial investigation unit.
- B. Report the suspicious activity immediately to the designated Money Laundering Reporting Officer
- C. Monitor the customer's transactions for the next 6 months to analyze the customer's behavior
- D. Inform the customer of concerns about the suspicious activity to obtain clarification.

Answer: B

Explanation:
Staff must report any suspicious activity immediately to the designated Money Laundering Reporting Officer (MLRO) or equivalent within their organization. The MLRO is responsible for assessing the suspicion and deciding on escalation to the relevant authorities. Informing customers (A) could compromise investigations. Reporting directly to financial investigation units (B) is not the staff member's role. Monitoring transactions without reporting (D) delays required action and risks regulatory non-compliance.
DFSA AML Module and FATF Recommendations emphasize timely internal reporting to designated officers as the first step in managing suspicious activity.

NEW QUESTION # 29
.....