

CFtA® EXAM

SAMPLE MULTIPLE CHOICE QUESTIONS

THE CFtA® PROGRAM

“ Your pathway into fintech innovation, ethics, and global financial systems.

The Chartered Fintech Associate (CFtA) is the foundational professional certification of the Global Fintech Institute, designed for early-career professionals, graduates, and practitioners building their grounding in fintech.

The program equips candidates with a structured understanding of the fintech landscape — from the architecture of the traditional financial system, to the role of data, artificial intelligence, blockchain, and cybersecurity in shaping modern financial services, to the ethics and governance frameworks that anchor responsible practice.

Candidates progress through eight curriculum chapters and sit a single-level examination comprising multiple choice questions. Successful candidates earn the CFtA designation, positioning them as informed, industry-relevant practitioners in a sector defined by rapid change.

The CFtA sits alongside the Chartered Fintech Professional (CFtP) as part of GFI's two-tier certification framework. Together, the designations support the professional development of individuals across the spectrum — from those entering the field to those leading institutional transformation.

The sample questions on the following pages reflect the structure, depth, and subject coverage of the CFtA examination.

More information:

globalfintechinstitute.org/programmes/cfta

QUESTIONS

CHAPTER 1 OVERVIEW OF FINTECH

Question 1

What is a 'neobank'?

- A. A bank that specializes only in foreign exchange
- B. A traditional bank that has launched a mobile app
- C. A digital-first bank-like service with no physical branches

Question 2

Which of the following is an example of a Fintech 1.0 development?

- A. Robo-advisers
- B. Automated Teller Machines (ATMs)
- C. Decentralized Finance (DeFi)

CHAPTER 2 THE TRADITIONAL FINANCIAL SYSTEM

Question 3

What does 'information asymmetry' mean in the context of the financial system?

- A. When data systems between banks are not synchronized
- B. When one side of a transaction has more information than the other side
- C. When regulators have access to more data than market participants

Question 4

What is 'hedging' as a risk management mechanism?

- A. Spreading investments across different assets to reduce exposure
- B. Collecting premiums from many individuals to compensate those who suffer losses
- C. Using financial contracts such as options and futures to offset potential future losses

Question 5

A fintech payment app shows users an instant 'payment successful' message. Which of the following statements best describes the accuracy of this message?

- A. It confirms only that authorization has been granted; clearing and settlement may still be pending
- B. It accurately reflects the complete economic settlement of funds between all parties
- C. It means the merchant has already received the funds in their bank account

CHAPTER 3 DATA IN FINTECH: HOW INFORMATION BECOMES PRODUCTS, DECISIONS, AND TRUST

Question 6

What is 'open banking'?

- A. A system where banks publish all customer data publicly for transparency
- B. Arrangements that allow customers to permit approved third parties to access certain banking data through secure interfaces
- C. A model in which all banks share a single unified database

Question 7

What is 'data governance' in the context of fintech?

- A. Government regulations that ban fintech firms from collecting data
- B. The technical encryption standards applied to financial databases
- C. Accountability, policies, decision rights, and processes used to manage data properly across an organization

Question 8

A fintech payment app experiences a sudden ten-fold surge in transactions during a major shopping festival. Which advantage of cloud computing best addresses this challenge?

- A. Scalability: cloud infrastructure can automatically allocate more computing power during peaks, then scale back
- B. Cost efficiency: cloud services are cheaper than building your own hardware overall
- C. Speed of innovation: developers can update the app multiple times per week

CHAPTER 4 ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES

Question 9

Artificial Intelligence (AI) is:

- A. Computer systems that perform tasks which normally require human intelligence, such as recognizing patterns, learning from experience, and making predictions
- B. Software tools that automatically write computer code without human instruction
- C. Computer systems that replicate full human consciousness and general reasoning

Question 10

What is Machine Learning (ML)?

- A. A system in which humans write every rule the computer must follow
- B. A system trained on many past labelled examples that learns which patterns tend to lead to which outcomes and applies that learning to new cases
- C. A system that uses cameras and sensors to observe physical environments and act autonomously

Question 11

What is 'hallucination' in the context of AI language models?

- A. When an AI model misreads a document because of poor image resolution
- B. When an AI model refuses to answer a question it was not trained on
- C. When an AI model generates plausible-sounding but false or unsupported information

Question 12

A digital lender uses an ML model to score loan applications. Applications scoring below 400 are automatically declined; those between 400 and 600 are sent to a human underwriter; those above 600 are automatically approved. What does this design illustrate about how AI is used in credit decisions?

- A. It shows that AI has fully replaced human judgment in the lending process
- B. It illustrates the layered approach - ML scores every application, but borderline cases are referred to humans, and policy rules govern the final outcomes
- C. It shows that ML models in lending are only used for the highest-risk applicants

CHAPTER 5 BLOCKCHAIN IN FINANCIAL SERVICES

Question 13

In a blockchain network, what are 'nodes'?

- A. The computers in the network that store the ledger, validate transactions, or both
- B. The regulatory bodies that oversee blockchain transactions
- C. The individual users who hold cryptocurrency wallets

Question 14

What is a 'digital signature' in blockchain systems?

- A. Mathematical proof that a transaction was authorized by the rightful owner of the asset, based on cryptography
- B. An electronic version of a handwritten signature used to open a bank account online
- C. A password used to log into a cryptocurrency exchange

Question 15

What is a 'smart contract'?

- A. A legally binding digital contract reviewed by lawyers and stored on a cloud server
- B. An AI system that negotiates contract terms between two financial institutions
- C. Shared code stored on the blockchain that automatically executes predefined rules when conditions are met

Question 16

A consortium of five banks wants to build a shared system for cross-border trade finance. They need all members to access the same record but want to restrict access to approved participants only. Which type of blockchain is most appropriate and why?

- A. A public blockchain like Ethereum, because transparency ensures all parties can verify the records
- B. A consortium blockchain, because it is a permissioned network governed by a group of organizations that balances shared control, governance standards, and compliance requirements among trusted institutions
- C. A private blockchain controlled by the largest bank, because centralized control reduces complexity

CHAPTER 6 CYBERSECURITY IN FINTECH

Question 17

The three foundational concepts of cybersecurity described in the CIA triad are:

- A. Cost, Integration, and Automation
- B. Cryptography, Identity, and Authentication
- C. Confidentiality, Integrity, and Availability

Question 18

'Social engineering' is used in overcoming cybersecurity safeguards by:

- A. Manipulating people through urgency, fear, or a pretence of authority so that they reveal information or bypass a security check
- B. Using social media platforms to market fintech products to new customer segments
- C. Building trust with customers through transparent communication about security practices

Question 19

How does 'multi-factor authentication' (MFA) increase security in a system?

- A. By requiring multiple employees to approve every customer transaction
- B. By requiring more than one form of verification before granting access, for example a password plus a code sent to a registered phone
- C. By verifying a customer's identity using their facial biometric data alone

Question 20

A fintech product manager wants to add a feature allowing users to instantly change their payout bank account with no additional verification. A risk officer objects. Who is correct and why?

- A. The product manager is correct - reducing friction always improves user experience and security is secondary to growth
- B. The risk officer is correct - changing payout details is a high-risk action that should require stronger authorization than a standard login because it is a primary target for account takeover fraud; friction should be added where significant loss can occur, not removed from high-risk actions
- C. Both are correct - the design should allow instant changes but display a warning message to the user

CHAPTER 7 GLOBAL COMPARISONS AND FUTURE HORIZONS

Question 21

What is 'embedded finance'?

- A. When a bank embeds its brand logo in a fintech company's app
- B. The process of physically integrating fintech servers within bank data centers
- C. The integration of financial services into non-financial platforms, such as a ride-sharing app offering drivers a loan or an e-commerce store offering buy-now-pay-later

Question 22

A fintech startup in a developing country has a potentially innovative product but operates in a regulatory grey area with no applicable license category. What option would be most appropriate for testing the product safely?

- A. Launch the product immediately at full scale since the absence of rules means it is implicitly permitted
- B. Apply to a regulatory sandbox, which allows the product to be tested with real customers under regulatory supervision with certain requirements temporarily relaxed, enabling the firm to demonstrate viability and work toward full licencing
- C. Relocate the company to a country with weaker regulations to avoid the compliance challenge

CHAPTER 8 ETHICS AND GOVERNANCE

Question 23

What are the three components of competence required of a professional?

- A. Speed, Accuracy, and Cost Efficiency
- B. Regulation, Compliance, and Risk Management
- C. Knowledge, Skills, and Ethical Values

Question 24

What is 'regulatory arbitrage' in the context of cross-border transactions?

- A. When firms choose to operate from jurisdictions with weaker rules to avoid stricter oversight, exploiting gaps between national regulatory regimes
- B. When firms employ a third party from a different country to shield themselves from liability incurred in the foreign country
- C. When a firm uses technology to automatically comply with the regulations of multiple countries

Question 25

A cybersecurity engineer at a fintech company discovers repeated unusual login attempts on a critical payment system. The manager says 'nothing has happened yet, let's not cause alarm.' Applying the duty of care principle, what should the engineer do and why?

- A. Follow the manager's instructions since the manager bears all accountability for the decision
- B. Escalate and investigate the issue, because duty of care requires reporting signs of failure or risks before harm occurs
- C. Wait and monitor the situation privately without escalating, to gather more evidence first

SOLUTIONS

Question 1

C is correct. (A digital-first bank-like service with no physical branches)

Neobanks are digital-only institutions that focus on fast account opening, clear fees, and user-friendly design without maintaining physical branches.

Question 2

B is correct. (Automated Teller Machines (ATMs))

ATMs are a classic Fintech 1.0 development, enabling 24/7 access to cash without bank branch hours, well before the digital disruption era. Early ATMs were located at the bank building to access the bank's network; the advent of the internet made it possible for the bank to connect with ATMs located away from bank branches, for example in a shopping mall.

Question 3

B is correct. (When one side of a transaction has more information than the other side)

Information asymmetry creates problems like adverse selection and moral hazard. In adverse selection, the party with the informational advantage exploits it against the other party — for example, less healthy individuals are more likely to buy health insurance. Moral hazard arises when, for instance, drivers take less care if insurance fully covers any damages. Insurers manage this by requiring a deductible before the insurance payment kicks in.

Question 4

C is correct. (Using financial contracts such as options and futures to offset potential future losses)

Hedging involves using financial contracts, such as options and futures contracts, to offset potential future losses. A wheat farmer, for example, can sell a futures contract to offset price risk at harvest. The futures position gains when price falls — the farmer buys the futures contract at a lower price to close the position, and this gain offsets the loss from selling the physical crop at a lower price.

Question 5

A is correct. (It confirms only that authorisation has been granted; clearing and settlement may still be pending)

Authorisation means giving permission to proceed but does not mean the transaction is fully complete in an economic sense. Clearing and settlement happen in the background after authorisation, so the 'instant' message reflects the front-end experience, not back-end finality.

Question 6

B is correct. (Arrangements that allow customers to permit approved third parties to access certain banking data through secure interfaces)

Open banking involves arrangements that allow customers to permit approved third parties to access certain banking data, or initiate some services on their behalf, through secure interfaces — often APIs. The central idea is customer control over how their financial data is shared.

Question 7

C is correct. (Accountability, policies, decision rights, and processes used to manage data properly across an organisation)

Data governance is about accountability, policies, decision rights, and processes used to manage data properly across an organisation. It ensures data is used consistently, responsibly, and in line with business, risk, and compliance requirements.

Question 8

A is correct. (Scalability — cloud infrastructure can automatically allocate more computing power during peaks, then scale back)

A payment app that processes a small volume of transactions on a normal day may face a sudden surge during a shopping festival or a market event. Cloud infrastructure can automatically allocate more computing power during such peaks, then scale back when demand drops.

Question 9

A is correct. (Computer systems that perform tasks which normally require human intelligence)

This is the standard working definition of AI — systems that perform tasks normally requiring human intelligence, including recognising patterns, learning from experience, and making predictions.

Question 10

B is correct. (A system trained on many past labelled examples that learns and applies patterns to new cases)

Instead of a human writing every rule, the system learns from historical data and applies that learning to new cases. It became standard in fraud scoring and credit risk because both have large historical datasets with clear feedback about outcomes.

Question 11

C is correct. (When an AI model generates plausible-sounding but false or unsupported information)

Hallucination occurs partly from the model trying to provide an answer as fulfilment of a given task. In a financial context, a model that confidently states the wrong fee schedule or gives incorrect regulatory guidance creates real compliance and reputational risk.

Question 12

B is correct. (It illustrates the layered approach — ML scores every application, with humans reviewing borderline cases)

Fintech lenders rarely let a model make unlimited decisions alone. Models typically operate within policy rules, approval limits, and human review thresholds. Applications in a borderline range are referred to a human underwriter rather than being automatically approved or declined.

Question 13

A is correct. (The computers in the network that store the ledger, validate transactions, or both)

Nodes help the system check and maintain the record collectively rather than through one central operator. This is the key feature of the distributed nature of blockchain.

Question 14

A is correct. (Mathematical proof that a transaction was authorised by the rightful owner, based on cryptography)

A digital signature is mathematical proof that the instruction came from the rightful owner of the asset, similar to a handwritten signature but based on cryptography. It is used at the authorisation step of a blockchain transaction to verify who is allowed to initiate an action.

Question 15

C is correct. (Shared code stored on the blockchain that automatically executes predefined rules when conditions are met)

A smart contract uses code stored on the blockchain that executes predefined rules automatically. An analogy is a vending machine: put in the right input (dollar amount) and the machine produces the programmed output without anyone needing to authorise each transaction manually. An important limitation is that if the code is flawed, the outcome will also be flawed.

Question 16

B is correct. (A consortium blockchain — a permissioned network governed by a group of trusted institutions)

As the name suggests, the blockchain is organised and governed by a group of organisations rather than a single institution. This structure supports collaboration while maintaining governance and compliance — exactly the requirement described. A private blockchain controlled by one bank would not satisfy the multi-party trust requirement.

Question 17

C is correct. (Confidentiality, Integrity, and Availability)

The CIA triad is a classic and useful way to remember the foundations of cybersecurity: Confidentiality (keeping information private), Integrity (keeping records correct), and Availability (keeping the service running when needed).

Question 18

A is correct. (Manipulating people through urgency, fear, or a pretence of authority)

Infiltrating a system is often difficult given the layers of identity authentication, so social engineering may be easier. It does not require any technical skill — a well-crafted phone call or message can be more effective than sophisticated computer code. The Coinbase 2025 incident illustrates this.

Question 19

B is correct. (By requiring more than one form of verification before granting access)

This is the description of multi-factor authentication. It is one of the key controls in the defence in depth approach and is used as a key practice for protecting accounts and reducing account takeover risk.

Question 20

B is correct. (The risk officer is correct — friction should be added where significant loss can occur)

The best fintech products do not add friction everywhere. Adding friction is like applying brakes — it slows things down by imposing more requirements where it matters. Viewing your account balance should be easy. Adding a new payment destination, resetting your account password, or sending a large transfer should involve additional verification steps. Changing payout bank account details is a classic money-redirection fraud target that requires stronger authorisation precisely because it is where criminals direct stolen funds.

Question 21

C is correct. (The integration of financial services into non-financial platforms)

Integrating finance into non-financial platforms provides convenience to the customer and expands the scope of financial services. Examples include a ride-sharing app offering drivers loans, an e-commerce store offering BNPL instalments, and accounting software offering small business loans based on existing revenue data. This connects to the broader open banking trend.

Question 22

B is correct. (Apply to a regulatory sandbox)

Regulatory sandboxes provide a controlled environment for testing with real customers when full regulatory requirements may not yet fit the new model. An example is the MAS Singapore sandbox: a blockchain-based payment startup could run a pilot with a few hundred customers, transfer small amounts, and work toward full licensing through the sandbox process. Option C describes regulatory arbitrage, which may be harmful.

Question 23

C is correct. (Knowledge, Skills, and Ethical Values)

The three components of competence are: (a) Knowledge — gained through study and continuing education; (b) Skills — developed through practice and applying knowledge in real situations; and (c) Ethical Values — which guide how knowledge and skills are used. Without ethical values, a person may be technically capable but can produce harmful outcomes.

Question 24

A is correct. (When firms choose to operate from jurisdictions with weaker rules to avoid stricter oversight)

In cross-border transactions, enforcement is usually limited to the authority's jurisdiction. The governing law often depends on domicile — where an entity is legally established. Firms face trade-offs as different domiciles offer different legal environments and tax regimes. This allows firms to arbitrage by choosing the domicile that minimises regulatory burden.

Question 25

B is correct. (Escalate and investigate the issue)

The duty of care principle includes 'a duty to report signs of failure or risks that may cause harm' as a preventive approach. If a cybersecurity engineer notices repeated unusual login attempts on a critical system, the duty of care requires escalation and investigation. The issue should not be ignored because it is inconvenient or because nothing has happened yet. Waiting for harm to occur before acting violates the duty of care's preventive dimension.