Certified AML and Fraud Professional (CAFP) Test Content Outline

Domain 1: Program Governance (34%)

Task 1: Establish procedures and controls to effectively address Bank Secrecy Act (BSA) / Anti-Money Laundering (AML) compliance guidance and regulatory requirements.

Knowledge required:

- Designated individual responsible for BSA/AML
- Internal Controls (e.g., Customer Identification Program [CIP]/Know Your Customer [KYC], Suspicious Activity Reporting [SAR])
- Training
- Independent testing
- Customer Due Diligence (CDD)/Enhanced Due Diligence (EDD)

Task 2: Establish procedures and controls to effectively address Office of Foreign Assets Control (OFAC) compliance guidance and regulatory requirements.

Knowledge required:

- OFAC regulations/guidelines/FAQ
- Sanctions and watchlists (e.g., SDN, CON, PLC)
- Reporting Requirements
- Initial and ongoing screening
- Blocking and rejecting transactions
- Training
- Record retention

Task 3: Establish procedures and controls to effectively address Fraud compliance guidance and regulatory requirements.

Knowledge required:

- Availability of Funds and Collection of Checks (Regulation CC)
- Electronic Funds Act (Regulation E) and error resolution process
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transactions Act (FACTA) Red Flags Rule
- UCC Article 3 and 4 – Check Liability
- Truth in Lending Act (Regulation Z)
- Training (e.g., employees)
- Education (e.g., customer, community)
- Record retention

Task 4: Understand AML, OFAC, and Fraud risk assessment processes.

Knowledge required:

- Three lines of defense
- Identification and analysis of specific risk categories (e.g., relationship risk, geographic risk [e.g., HIDTA, HIFCA], product/service risk, transaction risk, access channel risk)
- Analysis of new activities (e.g., new or modified products, services, or customers)
- Higher risk industries (e.g., marijuana-related businesses [MRBs], money services businesses [MSBs])
- Higher-risk customers (e.g., PEPs, attorneys, accountants, brokers)

Task 5: Implement the Anti-Money Laundering Act (AMLA).

Knowledge required:

- Whistleblower Protections
- Beneficial Ownership Information (BOI)
- Information sharing with foreign branches, subsidiaries, and affiliates
- AMLA Priorities

Domain 2: Detection and Investigation (40%)

Task 1: Develop strategies and models for system alert generation.

Knowledge required:

- How risk appetite and risk tolerance can influence risk models and alert generation
- How risk models are constructed (e.g., data input, data processing, assessment of outcomes)
- Use of the risk assessments to develop AML and Fraud strategies

Task 2: Identify and understand red flags and alert analysis.

Knowledge required:

- Fraud red flags and typologies (e.g., address verification, ID theft)
- Common scams (e.g., impersonation, romance, tech support)
- Money Laundering/Terrorist Financing red flags and typologies
- Customer risk rating and high-risk customer types (e.g., money service businesses, Politically Exposed Persons [PEPs])
- Alert analysis, referrals, and escalation

Task 3: Investigate the case by reviewing and determining the activity type, identifying suspects (i.e., known, unknown) and victims.

Knowledge required:

- Customer Due Diligence (e.g., internal information, handwriting, video/voice surveillance)
- Cyber indicators (e.g., IP address, user agent string, hosting provider, URL, image)
- Public records
- Open-source intelligence (e.g., negative news, social media, search engine)
- Types of law enforcement inquiries (e.g., Section 314(a) of the USA PATRIOT Act, subpoenas)

- Section 314(b) of the USA PATRIOT Act
- Recoverability (e.g., transactions, liability, IC3.gov)

Task 4: Conclude investigation with supporting documentation and SAR decisioning.

Knowledge required:

- Timeframe requirements (e.g., Regulation E, SAR filing)
- Required documents based on fraud activity type (e.g., affidavits, hold harmless)
- Supporting documentation for SAR or non-SAR decisioning (e.g., negative news, opensource intelligence, accounts activity, IP addresses)

Task 5: Determine the next course of action (e.g., account closure, reporting) in a case based on the identified risk.

Knowledge required:

- Remediation and recoverability efforts (e.g., return money, open new accounts, update third-party agencies, recover funds, charge off)
- Internal customer risk score modification (e.g., behavior, transactions, customer business)
- Internal risk assessment modification (e.g., changes in geography, product, exam results)
- When to elevate the case internally or externally (e.g., human trafficking, terrorist financing, insider abuse, institutional monetary losses)

Domain 3: Reporting (26%)

Task 1: Understand regulatory reporting and filing requirements (e.g., currency transaction reports [CTRs], suspicious activity reports [SARs], FACTA Red Flags Rule, Foreign Bank and Financial Accounts [FBAR], Designation of Exempt Person [DOEP]).

Knowledge required:

- Thresholds
- Time frames
- Record retention requirements
- Continuing activity (i.e., supplemental SAR, 90-day SAR)
- Amendments (e.g., what is it, when is it necessary)
- Backfilling (e.g., what is it, when is it necessary)
- CTR exemptions (e.g., what is it, when is it necessary)

Task 2: Respond to information requests.

Knowledge required:

- SAR confidentiality
- National Security Letters
- Subpoenas (e.g., Grand Jury Subpoenas, criminal, civil)
- Law enforcement agency requests (e.g., keep account open, account documentation, surveillance footage)
- 314(a) reporting and requirements