# Certified AML and Fraud Professional (CAFP) Test Content Outline

## Domain 1: Assessment (35%)

**Task 1: Establish procedures to consistently address regulatory requirements.**

**Knowledge required:**

a. Risk assessment process
   - Identification of specific risk categories
   - Analysis of specific risk categories

b. Compliance guidance and regulations for a Customer Identification Program (CIP)
   - CIP notices
   - Section 311 of the USA PATRIOT Act
   - Section 326 of the USA PATRIOT Act

c. Compliance guidance and regulations for customer due diligence (CDD)/enhanced due diligence (EDD)
   - May 2016 Financial Crimes Enforcement Network (FinCEN) Final Rule CDD/beneficial ownership and FAQs
   - Federal Financial Institutions Examination Council (FFIEC) special measures

d. Compliance guidance and regulations for customer risk rating/Know Your Customer (KYC)
   - FFIEC Appendix K
   - Customer risk factors to determine overall risk posed to the institution
   - Procedures for identifying and reporting of suspicious activity

e. Compliance guidance and regulations for politically exposed persons (PEPs)
   - FFIEC
   - FinCEN FAQs and guidance
   - Fact Sheet for Section 312 of the USA PATRIOT Act Final Regulation and Notice of Proposed Rulemaking

f. Compliance guidance and regulations for Office of Foreign Assets Control (OFAC)
   - OFAC regulations for the financial community
   - OFAC Enforcement Guidelines
   - OFAC FAQs
   - FFIEC
   - "Specially Designated Nationals" (SDN) versus sanctions
   - Reporting requirements
   - Record retention
   - Initial and ongoing screening
   - Blocking versus rejecting transactions

g. Fraud guidance and regulations (e.g., identity theft, synthetic, first-party)
   - Fair and Accurate Credit Transactions Act (FACTA) Red Flags Rule
   - FFIEC multifactor authentication
   - Fannie Mae and Freddie Mac requirements
   - SEC requirements (e.g., Ponzi, pump-and-dump, insider trading)

h. Cyber guidance
   - Executive Order 13691
   - Executive Order 51117
   - Economic Espionage Act of 1996

- FinCEN Advisories FIN-2016-A005, FIN-2016-A003, FIN-2013-A001, FIN-2012-A005, and FIN-2011-A016
- FinCEN Guidance on the Scope of Permissible Information Sharing covered by Section 314(b) Safe Harbor of the USA PATRIOT Act

**Task 2: Evaluate customer risk.**

**Knowledge required:**

a. Compliance guidance and regulations (e.g., CIP, CDD/EDD, OFAC)
   - FFIEC
   - USA PATRIOT Act Sections 312 and 326
   - U.S. Treasury Guidance for Financial Institutions
   - FFIEC Appendix J and Appendix K
b. Fraud guidance and regulations (e.g., identity theft, synthetic, first-party)
   - Identity theft (FinCEN advisory, FACTA, Federal Trade Commission [FTC], red flags)
   - New account fraud (FinCEN advisory, red flags)
   - First-party fraud (deposit, credit)

**Task 3: Evaluate risk to prevent and detect financial crimes.**

**Knowledge required:**

a. Relationship risk (e.g., beneficial ownership, account maintenance, vendor, employee, customer)
b. Geographic risk (e.g., Financial Action Task Force [FATF], State Department, OFAC, U.S. Postal Service, Organisation for Economic Co-operation and Development (OECD), high-intensity drug trafficking area [HIDTA], high-intensity financial crimes areas [HIFCA], Geographic Targeting Orders [GTO])
c. Product/service risk (e.g., channels, assessment of risk, fraud solutions)
d. Cyber risk (e.g., National Institute of Standards and Technology [NIST], SWIFT Customer Security Program [CSP] [self-attestation])
e. Transaction risk and fraud types (e.g., counterfeit, lost/stolen, altered, endorsement, account takeover [ATO], e-commerce, unauthorized, scams)

**Task 4: Monitor external sources of information (e.g., negative news, dark web, forums, social media).**

**Knowledge required:**

a. Common points of purchase (CPP)
b. Financial Services Information Sharing and Analysis Center (FS-ISAC)
c. Dark web (compromised data, evolving tactics, threats to an institution)
d. Open-source intelligence

**Task 5: Participate in internal and external information sharing to gain intelligence.**

**Knowledge required:**

a. FinCEN advisory (formal collaboration between financial crimes and information security)
b. FS-ISAC
c. InfraGard
d. Section 314(b) of the USA PATRIOT Act
e. U.S. Secret Service Electronic Crimes Task Force
f. Department of Homeland Security's Enhanced Cybersecurity Services
g. Third-party services (FICO, early warning systems [EWS], processors and payment network, roundtable information sharing, BITS)

**Task 6: Analyze an event or alert to determine the next course of action.**

**Knowledge required:**

a. Anti-money laundering (AML) and fraud scenarios/typologies

b. Brute force attacks (rainbow table)
c. Malware
d. Social engineering (e.g., business email compromise [BEC], distributed denial of service [DDoS], phishing, vishing, spoofing)
e. Network attacks (Bluejacking, Bluesnarfing, port scanning, device ID)
f. Jackpotting (hardware/software machine or terminal)
g. Identification and reporting of suspicious activity

**Task 7: Develop rules and strategies for system alert generation.**

**Knowledge required:**

a. AML and fraud false-positive rates
b. AML and fraud detection rates
c. Control and client impact/customer experience rule
d. Champion challenger/estimators
e. Anomaly detection (AML, cyber, fraud)
f. Model validation
g. Risk appetite

## Domain 2: Investigations (30%)

**Task 1: Review an activity claim/type in a confirmed case.**

**Knowledge required:**

a. AML and fraud scenarios/typologies
b. Cyber-enabled financial crimes typologies
c. AML/terrorist financing typologies

**Task 2: Identify suspects (known or unknown) and victims in a confirmed case.**

**Knowledge required:**

a. KYC (e.g., internal information, Sections 314(a) and 314(b) of the USA PATRIOT Act)
b. Public records
c. OFAC
d. Open-source intelligence
e. Interviewing tactics (e.g., elicitation technique)
f. Types of law enforcement inquiries (e.g., Section 314(a) of the USA PATRIOT Act, subpoenas)

**Task 3: Determine suspicious activity type and priority level in a confirmed case.**

**Knowledge required:**

a. Thresholds (e.g., monetary, law enforcement interest, case types)
b. Recoverability (i.e., transactions and liability)
c. Types of suspicious activity listed on the suspicious activity report (SAR) form, including “other”
d. AML and fraud scenarios/typologies

**Task 4: Conduct research by using internal and external sources of intelligence.**

**Knowledge required:**

a. Internal sources of intelligence
    - Handwriting comparison
    - Video surveillance
    - Telephony (e.g., voice, automated number identification [ANI], device)
    - Cyber Indicators (e.g., IP address, user agent string, hosting provider, URL, image)

- Account relationship/transaction information (e.g., statements, internal communication, account opening documents)

b. External sources of intelligence
   - Open-source intelligence (e.g., social media)
   - Negative news
   - Screening (e.g., OFAC, external lists)
   - Section 314(b) of the USA PATRIOT Act

**Task 5: Build the case file, including supporting documentation.**

**Knowledge required:**

a. How to pull public records
b. How to analyze account relationship/transaction information (e.g., statements, internal communication, account opening documents)
c. Time frame requirements (e.g., Regulation E, SAR filing)
d. Required documents based on activity type
e. Documentation to support SAR and non-SAR decisioning

**Task 6: Determine the next course of action (e.g., account closure, reporting) in a confirmed case based on the identified risk.**

**Knowledge required:**

a. Section 314(b) of the USA PATRIOT Act
b. SAR confidentiality
c. Customer risk score modification
d. Financial institution risk appetite
e. When to elevate the case internally or externally

## Domain 3: Reporting (17%)

**Task 1: Identify appropriate regulatory reporting requirements and file (or assist with filing) initial and ongoing reports (e.g., currency transaction reports [CTRs], SARs, FACTA Red Flags Rule, Report of Foreign Bank and Financial Accounts [FBAR], Bank Secrecy Act Designation of Exempt Person [DOEP]).**

**Knowledge required:**

a. Thresholds
b. Time frames
c. FinCEN e-filing
d. Appropriate audience for reporting
e. Record retention requirements
f. Follow-up reporting
g. Amendments
h. Backfiling
i. Exemptions
j. Section 314(a) of the USA PATRIOT Act
k. Section 314(b) of the USA PATRIOT Act
l. How to report OFAC blocked or rejected customers to the U.S. Treasury

**Task 2: File or assist with filing non-regulatory required reports (e.g., card networks, government-sponsored enterprises [GSEs], credit reporting agencies [CRAs]).**

**Knowledge required:**

a. What to submit to internal or external information sharing partners (indicators of compromise [IOCs])
b. How to submit documentation regarding card fraud loss

**Task 3: Respond to law enforcement requests.**

**Knowledge required:**

a. When a subpoena is required
b. Parameters of Section 314(a) of the USA PATRIOT Act

## Domain 4: Remediation (18%)

**Task 1: Establish and update controls (e.g., update procedures, tune rules, policy changes).**

**Knowledge required:**

a. How to identify procedural gaps
b. How to update procedures to address gaps
c. How to find guidance and regulatory updates

**Task 2: Manage relationships with customers and intermediaries (e.g., retention or termination).**

**Knowledge required:**

a. OFAC
b. Higher risk industries (e.g., marijuana-related businesses [MRBs], money services businesses [MSBs], correspondent banking/SWIFT CSP)

**Task 3: Engage in entity and/or victim remediation (e.g., return money, open new accounts, update third-party agencies, recover funds, charge off).**

**Knowledge required:**

a. Availability of Funds and Collection of Checks (Regulation CC)
b. Electronic Funds Act (Regulation E) and error resolution process
c. Fair Credit Reporting Act (FCRA)
d. FACTA ID theft remediation
e. Hold harmless agreement

**Task 4: Educate and train customers, employees, and third parties.**

**Knowledge required:**

a. Training pillar of Bank Secrecy Act (BSA)
b. Notice to Customers: A CTR Reference Guide
c. Identity theft red flags
d. Emerging typologies