Detailed Briefing Document: Customer Due Diligence (CDD) in Financial Compliance
Source:

1. Introduction to Due Diligence and CDD
The concept of 'due diligence' broadly refers to "action that is considered reasonable for people to be expected to take in order to keep themselves or others and their property safe." This principle applies across various contexts, from real estate inspections to comprehensive business examinations during mergers and acquisitions. In a business context, it means "the detailed examination of a company and its financial records, done before becoming involved in a business arrangement with it." Fundamentally, due diligence is a "business practice that seeks to ensure that people and organisations keep their dealings secure by understanding the facts and risks associated with the business, and with the transactions, properties or parties involved."

Customer Due Diligence (CDD) specifically applies to "enquiries made about the customers of an organisation to support a decision as to whether or not business should be undertaken or continued with these customers." For regulated firms, CDD is not merely good business practice; it is driven by stringent regulatory requirements, particularly due to their "prominent role... in controlling which people and organisations can gain and retain access to the financial system and is necessary to maintaining the integrity of the system."

2. Core Regulatory Drivers for CDD
The primary regulatory driver for CDD obligations is Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) regulations. These regulations are designed to prevent the financial system from being used by criminals to "recycle the proceeds of crime or to support terrorist activities." AML/CFT regulations extend beyond financial institutions to "designated non-financial businesses and professions (DNFBPs)" such as casinos, real estate agents, and lawyers, who are involved in handling financial flows or high-value assets.

A core element of AML/CFT regulations is the requirement for firms to "understand their customers and the nature of their customer relationships sufficiently to prevent criminals from entering the financial system and using a firm’s products and services for illegitimate purposes." This involves identifying customers through a Customer Identification Programme (CIP) and performing CDD enquiries across various aspects of the customer's activities and beneficial owners to assess associated risks.

Beyond AML/CFT, other regulatory drivers for CDD include:

- **Tax Regulations**: Such as the Common Reporting Standard (CRS), requiring financial institutions to collect specific information for reporting purposes.
- **Conduct of Business Regulations**: Like The Markets in Financial Instruments Directive (MiFID), which ensure responsible business conduct, consumer protection, and the suitability of products and services for customers. Firms must "act responsibly and to have the necessary resources and procedures in place for safeguarding the best interests of their customers."
- **Sanctions:** Firms are legally required to identify and manage direct and indirect sanctions exposure by screening customers against relevant lists.

These various CDD requirements collectively form part of a firm's Know Your Customer (KYC) framework.

3. **Key Concepts: Money Laundering, Terrorist Financing, and Proliferation Financing**
   - **Money Laundering:** "Activity undertaken to hide the true origin of criminally derived property with the intention that someone will ultimately benefit from it." Techniques include concealing identity, using legitimate businesses, creating complex corporate webs, and exploiting jurisdictions with weaker controls.
   - **Terrorist Financing:** "The act of providing financial support for terrorist activities." Unlike money laundering, funds often originate from legitimate sources, but their destination needs to be concealed.
   - **Proliferation Financing:** "The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials."

4. FATF Recommendations and CDD Obligations
The Financial Action Task Force (FATF) is the global standard-setting body for AML/CFT. Its 40 Recommendations provide the umbrella framework implemented into national laws worldwide.

FATF Recommendation 10 defines core standards for CDD measures, stipulating:

- "Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information."
- Prohibition on anonymous accounts.
- Requirement to apply CDD to all business relationships, occasional transactions above a minimum threshold, and wire transfers.
- CDD must be carried out before establishing a business relationship.
- Application of CDD to all new relationships and to existing ones on a risk-sensitive basis.
- Critically, Recommendation 10 requires firms to perform CDD using a risk-based approach.
- FATF Recommendation 11 sets out record-keeping requirements for CDD, with a minimum retention period of five years.

5. CDD from Three Angles
The source defines CDD from three key perspectives:

CDD as a set of enquiries: This involves investigating relevant elements of a customer relationship to establish a risk profile. Enquiries include:
- Identifying and verifying customer identity.
- Establishing a customer profile, including business activities and source of wealth.
- Understanding the purpose, nature, and context of the relationship, products/services used, and source of funds.
- Identifying parties with effective control (e.g., beneficial owners of corporate customers).

- Performing CDD on a continuous basis to ensure consistency with the customer's profile. CDD measures apply to all customers, private persons, and legal entities, with greater depth generally required for legal entities.

CDD as a risk-assessment process: CDD enquiries support the detection of risk factors, leading to a "customer risk profile." Identified risk factors can include:

- Presence of Politically Exposed Persons (PEPs).
- Higher-risk business activities (e.g., correspondent banking).
- Involvement of higher-risk countries.
- Sanctions exposure.
- Inconsistencies between product use and business activity. The outcome is often a financial crime risk rating, determining the level of scrutiny and depth of due diligence applied.

CDD as a business process: A core outcome is to determine if a firm can "take on a customer's business on the basis of its understanding of the risks posed by that customer relationship." This makes CDD "a key part of a firm's customer acceptance policy." The outcomes are:

- Establishing customer identity.
- Confirming relationship acceptability.
- Creating a structured set of CDD records (KYC files). CDD is a significant operational cost for regulated firms, leading to an increasing focus on efficiency. It also has a "strong customer service dimension which constitutes an important competitive factor for firms," as it is often the first interaction a customer has with a firm.

6. Importance of CDD for Regulated Firms

Effective CDD is critical for several reasons:

Foundation of an Effective AML/CFT Framework: CDD prevents illegitimate use of products/services by ensuring firms "know with whom it is dealing," guard against fraud, understand beneficial ownership, assess legitimacy of business activities and funds, and effectively perform other AML/CFT activities (sanctions screening, PEP identification, suspicious activity detection, law enforcement cooperation). It enables a risk-based approach to prevention.

Providing Suitable Products and Services: A solid understanding of customer circumstances ensures "suitability" of offerings, enshrined in Conduct of Business regulations like MiFID. This guards against "mis-selling," which carries "heavy penalties for firms owing to the threat it presents to consumers and to general confidence in the financial system."

Demonstrating Compliance: Creation and retention of CDD records (KYC files) are essential for responding to internal audits, regulatory examinations ("regulator readiness"), and law enforcement investigations.

Protecting the Firm and its Reputation: Beyond legal requirements, firms have a "moral and social responsibility to contribute to the fight against financial crime." Failures can lead to "severe impacts on a firm's reputation," including "loss of business to competition," "shareholder discontent," and significant "remedial efforts of legacy issues."

7. Consequences of CDD Failures (Case Studies)
The source highlights the severe penalties and reputational damage resulting from CDD control deficiencies:

- **NatWest:** Fined £264.8 million for AML control deficiencies. Failures included ignoring "red flags" and suspicious deposits, not scrutinising transactions significantly departing from expected activity, and lack of ongoing risk-sensitive monitoring. The sentencing judge stated, "without the Bank – and without the Bank's failures – the money could not be effectively laundered."
- **Capital One Financial Association (US):** Penalised by FinCEN for "wilful and negligent violations of the Bank Secrecy Act."
- **Crown Melbourne and Crown Perth Casino (Australia):** Ordered to pay AUS$450 million for breaching AML/CTF Act. Failings included inappropriate risk assessments, inadequate systems and controls, lack of Board oversight, deficient transaction monitoring, and insufficient enhanced CDD for higher-risk customers.
- These cases underscore "the fundamental need for a robust CDD/KYC process that is capable of identifying potential risk factors."

8. Overview of Key Terms in the Customer Lifecycle and Compliance
The source clarifies several often-interchangeable terms:

Customer Lifecycle: Designates the various stages of a customer relationship:
- Onboarding: Initial acceptance of a new customer.
- Offerings: Adding new products/services.
- Monitoring: Continuous oversight, including transaction monitoring.
- Reviews: Periodic or event-driven assessments.
- Offboarding: Termination of the customer relationship.

CDD (Customer Due Diligence): "The process by which firms make risk-based enquiries and perform risk assessments to identify their customers and determine the acceptability of business relationships in line with their risk appetite and regulatory obligations." It is the universally used term in regulatory texts.
I**D&V (Identification and Verification):** "The process of collecting information about the customer relationship and verifying that this information is true and correct by using independent documentary evidence." It is a key component of CDD.
CIP (Customer Identification Program): A term specific to the USA PATRIOT Act, focusing on minimum standards for customer identification when opening an account. It is a "subset of CDD."
KYC (Know Your Customer): While often used interchangeably with CDD, for the purpose of this course, "KYC is the universe of activities and processes designed to meet a firm's regulatory obligations of customer identification, classification and due diligence across applicable regulations including financial crime, conduct of business and tax." It encompasses operational disciplines, IT systems, policies, quality assurance, and governance.
Onboarding: The "complete set of activities required to start trading with a customer," extending beyond just KYC to include credit risk assessment, legal activities (e.g., master agreements), and post-trade requirements (account setup, settlement instructions).
Offboarding: The process for exiting a customer relationship, requiring firms to meet all legal, regulatory, and commercial obligations. Steps include identifying all accounts,

communicating with the customer, closing accounts, managing outstanding transactions, ensuring no new business, and updating CDD records.

9. International Perspective on CDD Regulation

FATF Recommendations are implemented into national laws and transposed into regulatory norms by individual regulators globally.

European Union (EU):

- **European Money-Laundering Directive (EMLD):** The central piece of EU AML/CFT legislation, adopted first in 1990.
- **4MLD (2015):** Institutionalised the risk-based approach, extended PEP definition to domestic PEPs, removed blanket simplified due diligence, required CDD on branches in high-risk countries, and mandated national beneficial ownership registries.
- **5MLD (2018):** Defined cryptocurrency as "virtual assets" subject to AML/CFT, enhanced Financial Intelligence Unit (FIU) powers, limited pre-paid card use, improved safeguards for transactions with high-risk third countries, and mandated centralised bank/payment account registers.
- **6MLD (2018):** Stronger focus on money laundering scope (22 predicate offences), extended liability to businesses, and provided wider grounds for prosecution for failure to prevent money laundering.

United States:

- Bank Secrecy Act (BSA) & Patriot Act (2001): Core AML legislation.
- FinCEN: Financial Crimes Enforcement Network, an arm of the US Treasury Department, serving as the national FIU and federal regulator.
- Emphasis: Historically, strong emphasis on transaction monitoring and less on CDD enquiries, which were largely confined to customer identification. Since 9/11, increased emphasis on sanctions screening and Enhanced Due Diligence (EDD) for foreign correspondent banking.
- CDD as the "Fifth Pillar": FinCEN's revision of CDD requirements established it as a "fifth pillar" to AML programs, focusing on beneficial ownership and the purpose/nature of the relationship, supplementing existing BSA requirements.

The United Arab Emirates (UAE):

- Federal Decree-Law No. (20) Of 2018 & Cabinet Decision No. (10) of 2019: Main legislation criminalising money laundering and terrorist financing, requiring financial institutions and DNFBPs to identify/mitigate risks, perform CDD, and deal with PEPs and high-risk customers.
- Supervisory Authority: Central Bank is the principal authority; Dubai Financial Services Authority (DFSA) regulates the Dubai International Financial Centre (DIFC).

Asia-Pacific (APAC):

Singapore:Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) & Terrorism (Suppression of Financing) Act (TSOFA): Primary legislation. Monetary Authority Singapore (MAS): Main regulatory authority for financial institutions, developing policy, guidance, and regulations, and assessing/enforcing AML/CFT measures.
Malaysia:Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA): Primary legislation, including sanctions measures.

Hong Kong: Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO): Primary legislation.

- Hong Kong Monetary Authority (HKMA): Supervises compliance.
- Risk-Based Approach: Key steps include verifying legal entity existence, understanding risks, senior management oversight, good record-keeping, and effective compliance testing.

Australia: Australian Transaction Reports and Analysis Centre (AUSTRAC): Regulator and FIU.

- Anti-Money Laundering and Counter-Terrorist Financing Act 2006 (as amended 2018): Outlines obligations for KYC, transaction monitoring, and CDD, requiring consideration of broader risks, collection/verification of identification information for customers/owners/controllers, and continuous CDD/monitoring.

In summary, CDD is not merely a regulatory burden but a fundamental component of financial integrity, risk management, and responsible business conduct, with global standards set by FATF and tailored by national legislations.