Empowering You with Expertise in

Anti-Money Laundering & Combat Terrorist Finance

Training by

ABM Global Compliance

Financial Service Regulatory Advisor

AML/CFT for UK

Goals

- Understand the UK's AML/CFT regulatory frameworks and legal obligations.
- Identify potential money laundering risks and recognize associated indicators.
- Develop proficiency in conducting risk-based Customer Due Diligence (CDD).
- Acquire skills in transaction monitoring and the preparation of Suspicious Activity Reports (SARs).
- Appreciate the importance of accurate record-keeping and regulatory requirements for retention.
- Explore the role of technology, in enhancing AML/CFT processes.

Summary:

The UK AML/CFT training course provides audience all they need to know about the rules and regulations, as well as the practical skills to follow them. With an emphasis on client due diligence, transaction monitoring, and reporting requirements, participants will explore the complexities of detecting and reducing money laundering concerns. The training delves into the importance of precise record-keeping and introduces participants to how technology may support anti-money laundering and counter-financing of terrorism initiatives. Participants will be well-versed in compliance procedures as we discuss the legal protections for reporters and their reporting obligations in detail. In sum, participants will leave the course with the understanding and skills necessary to help build a strong AML/CFT framework, which will protect the UK's financial system.

Module 1: Introduction to Money Laundering and Terrorist Financing

What is money laundering?

Money laundering is "the process by which the proceeds of crime are changed into assets that seem to have a legitimate origin so that they can be kept permanently or used in new criminal enterprises." (Part 7 of Proceeds of Crime Act 2002)

This process involves moving of unlawfully obtained proceeds (cash or assets) through a convoluted series of Financial Institutionsing transfers or business transactions in order to make them appear legal or genuine.

Money laundering's main objective is to conceal the real source of the funds, making them hard to track down and allowing people or organizations to profit from their illicit activity without drawing notice from financial institutions or law enforcement.

The concept behind the phrase "money laundering" is that criminals are trying to "clean" their illicit riches in order to make them seem legal. In simple words, though, it means turning black money into white money.

It lets the crooks keep control of their money and gives them a legal way to hide their source of income if they are successful. Criminals who want to avoid getting caught by the

police when they get rich quickly from doing illegal things use money laundering to help them reach their goals.

This includes drug dealers, terrorists, organized criminals, insider traders, tax evaders, and many more. These criminal groups want to get money and power by breaking the law, and then they try to join normal society, which goes against the rules of the compact.

Stages

Three primary steps are usually included in the money laundering process:

Placement:

This is the first time that "illegal money" gets injected into the economy. Physical placement may be a part of this, such as putting money into a Financial Institutions account or spending it to buy expensive things or real estate.

Typical techniques employed in placement include:

- Utilizing a strategy called "structuring" to deposit cash in smaller sums to evade discovery
- Acquiring cash items such as money orders or checks
- Distributing funds via cash-only enterprises like car washes and casinos.
- After successfully introducing illegal monies into the financial system, criminals begin the process of hiding their true identity and transferring the funds through money laundering.

Example: Sarah, a Financial Institutions teller at XYZ Financial Institutions, notices an unusual cash deposit made by a customer named John. John walks into the Financial Institutions and deposits $50,000 in cash into his personal savings account. Sarah finds this transaction to be out of the ordinary, as John typically only deposits smaller amounts.

Layering:

The second phase of money laundering is called "layering," Its goal is to hide the money as much as possible, taking it even further away from where it came from. This part of the process can often be the hardest of all.

Layering is used to weave an intricate web of financial transactions that makes it more challenging for law enforcement to identify the source of the money that is being used illegally. Once criminals get past the layering step, they can further protect themselves from discovery and get ready to re-inject their laundered funds into the legal economy.

Money launderers may do a number of things, such as wire transfers, currency exchanges, stock market trades, and using offshore accounts and "shell" businesses. These activities make it hard to figure out where the illegal money came from because

they build a web of complicated finances. Adding layers to the trail of money makes it more complicated and hard to follow.

Example: Mark, a compliance officer at ABC Financial Institutions, notices a series of transactions associated with a customer named Emily. Over the past month, Emily has engaged in several financial activities that seem unusually intricate.

- Emily sent a lot of money to an account in another country.
- She changed her money into different currencies a few times in a short period.
- Emily bought and sold stocks in the stock market quickly, but it wasn't clear why she was doing it.

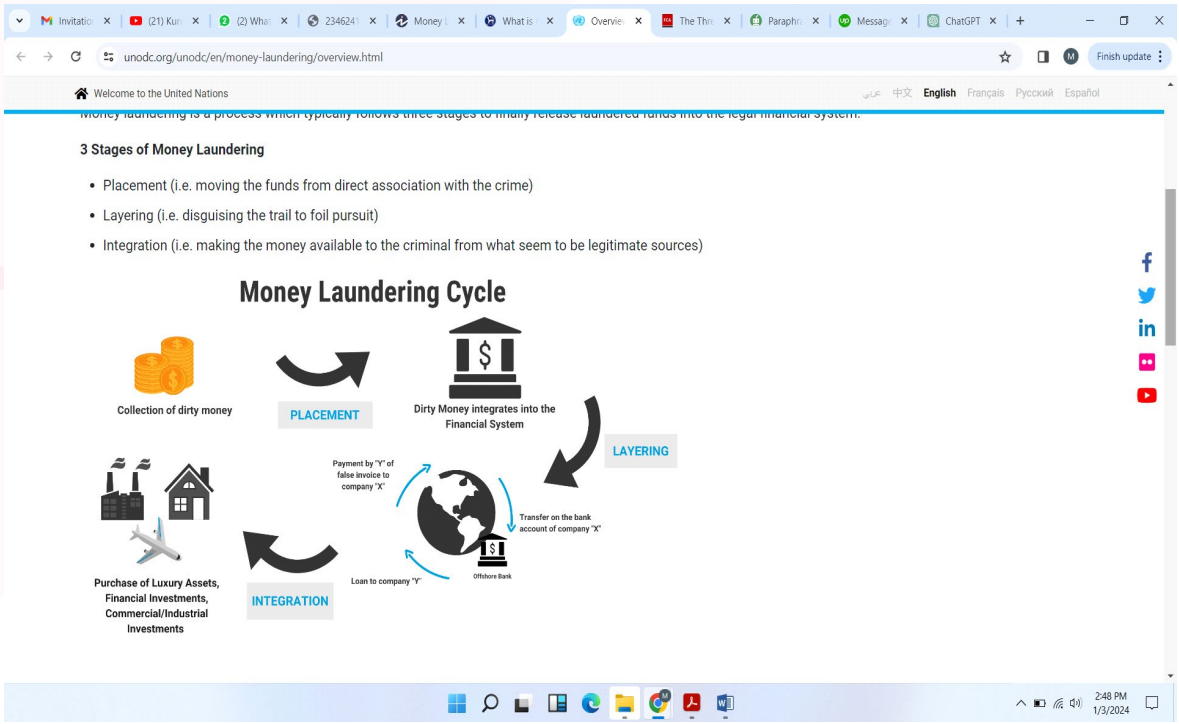
Integration:

In the last phase, the "cleaned" money is put back into the economy and makes an appearance as assets or income that is acceptable. This may entail using the money to buy companies, engage in legitimate ventures, or buy valuable properties.

Money laundering is frequently linked to a number of illegal operations, such as drug trafficking, organized crime, fraud, corruption, and tax evasion. Due to the fact that detecting and stopping these illegal acts necessitates a concerted effort, it presents serious hurdles to financial institutions and law enforcement.

Example: Sama, a diligent employee at XYZ Financial Services, notices some unusual financial activities involving a local business owner, Mike.

- Mike, the owner of a small cafÈ, suddenly acquires a high-end luxury car for personal use.
- He invests a significant portion of money into expanding his cafÈ, renovating the premises, and introducing premium menu items.
- Mike starts making substantial donations to local charities and community projects.



Module 2: What is Terrorist financing?

The act of giving money or resources to people, groups, or organizations that carry out terrorist activities is referred to as terrorist financing. This kind of funding is essential to terrorism because it allows terrorists to carry out their violent crimes, uphold their organizational structures, and continue their operations over an extended period of time. One of the most important aspects of international efforts to improve security and combat the threats posed by terrorism is the fight against terrorist financing.

According to Terrorism Act 2000, "terrorist property" includes

(a) Money or other things that are likely to be used for terrorist purposes, such as the resources of an illegal group;

(b) The money or other things that are made from committing terrorist acts; and

(c) The money or other things that are made from committing terrorist acts (Terrorism Act 2000).

Funding Sources:

- **Illegal Activities**: To raise money, terrorist groups frequently take part in extortion, drug trafficking, arms smuggling, kidnapping for ransom, and other illegal operations.

- **Individual Providers:** Financial donations from receptive parties that hold similar ideological views may reach terrorist groups. Either official or informal avenues may be used to make these contributions.

- **Charity and gifts**: Terrorist groups may use charity organizations or create their own fake charities to get gifts from people who don't know any better and think they are helping good causes.
- **Kidnapping and Ransom**: Terrorist groups may use kidnapping for ransom as a way to make money. Payments made in ransom by people, businesses, or states can help them get more money.
- **Fraud and Identity Theft**: Terrorists may commit credit card fraud, Financial Institutions fraud, or other types of financial crime in order to get money.
- **Trade-Based Financing**: Terrorist groups can get money from illegal trade activities and not paying taxes. They might take advantage of trade lines or launder money through trade.
- **Cybercrime**: Some terrorist groups may use cybercrime to commit scams or steal financial information.

Example Based on a Scenario: Funding by Kidnapping and Ransom

Characters:

Ahmed, the Terrorist Leader: the head of a terrorist organization active in a conflict-ridden area.
Elena, the financier: someone who supports the group's goals but refrains from taking part in violent actions.
Sarah was the victim: a well-known businesslady with regional experience.
Situation:

Sarah is a wealthy corporate executive who the terrorist group's leader, Ahmed, believes may be a good candidate for kidnapping. The gang successfully prepares and carries out a kidnapping operation, seizing Sarah and requesting a large ransom to free her.

Elena chooses to help the gang out financially since she supports their purpose but is unwilling to employ physical force. She moves a substantial sum of money to an offshore account under the terrorist organization's control, hiding the transaction with a string of ostensibly legal financial exchanges in several nations.

Consequently, the terrorist organization gets the extra cash from Elena as well as the ransom from the victim's family. This terrorist organization is able to finance its operations, get weapons, and continue its activities in the region because of a combination of unlawful actions (kidnapping for ransom) and financial assistance from those who sympathize with it.

> This scenario highlights the complicated nature of financial sources for terrorist organizations by demonstrating how terrorist financing can involve both criminal activity and support from individuals who hold similar ideological beliefs.

Process of Terrorist Financing:

- **Obtaining funds:** Terrorist organizations start the process by obtaining money through a variety of channels, such as illicit operations, gifts, individual support, charitable organization hiding actual cause etc.
- **Money Transfer:** After money is raised, it is frequently transferred across countries via the Financial Institutionsing system, remittances, or unofficial routes. It is possible to transfer money through middlemen to hide its source.
- **Layering:** Terrorist financiers use layering, which is similar to money laundering, to hide the source of funding. Complex financial transactions are used in this to obstruct discovery and cause confusion.
- **Integration:** The money is either incorporated into the legal economy or goes toward certain goals, such buying weapons, plotting assaults, or maintaining the terrorist group's infrastructure.

For Example

Terrorist financing

Maria: A charismatic extremist group commander. Maria is skilled in enlisting supporters for the group's extremist philosophy.

David: A businessman in his forties with strong radical beliefs. David contributes financially to "Marias group" and believes in the organization's mission.

Sophie: A proficient money launderer who works undercover. Sophie assists with the transportation of monies to fund " Marias group " activities.

- **Raising funds:** During a secret meeting, Maria uses her charismatic personality to recruit David. Due to his extremist ideas, David becomes a strong follower of ìMariaís groupî and resolves to financially contribute to their cause.
- **Fund Transfer:** David wires $200,000 to Sophie, a skilled money launderer. Sophie moves funds across borders using various financial instruments and digital currencies while remaining under the radar.
- **Layering:** Sophie conducts a number of sophisticated activities, such as currency conversion, minor investments, and money transfers across Financial Institutions accounts. This layering method is meticulously designed to conceal the source of the funding.
- **Integration:** "Mariaís groupî uses the combined finances to procure weapons, fund training camps, and assist logistics for planned strikes. Some monies are invested in what appear to be respectable firms to offer cover for illegal activity.

Difference between Money Laundering and Terrorist Financing

Goals and Purpose

Money laundering: The main goal of money laundering is to hide where illegally gained funds came from. It includes using a complicated set of financial transactions to make money that was obtained illegally look like it was earned legally.

Terrorist Financing: The main goal of terrorist financing is to give money to people or groups that are doing terrorist actions. The money can be used to plan and carry out terrorist acts, buy weapons, or keep terrorist networks going.

Source of the Money:

Money laundering is the process of hiding money that comes from illegal activities like drug dealing, corruption, fraud, or other illegal businesses.

Terrorist financing includes both legal and illegal ways of getting money to support terrorist acts, such as through donations, gifts, state sponsorship, illegal actions, and other means.

Module 3 Overview of AML/CFT

Anti-money laundering (AML):

Anti-money laundering (AML) is the umbrella term for a collection of policies, rules, and guidelines intended to stop money laundering and the transfer of unlawful cash into the official financial system.

Key Goals of AML are:

Preventing Money Laundering: Anti-Money Laundering (AML) procedures are designed to identify and discourage the methods that criminals use to conceal the source of their cash.

Improving Transparency: Anti-money laundering legislation (AML) encourages financial institutions to be aware of their clients and to report any questionable activity.

Improving Regulatory compliance: AML rules are meant to make sure that financial institutions follow the laws and rules that apply to them. This encourages everyone to follow the rules of what is right and legal.

Ensure due diligence: One main goal is to get financial institutions to do their research on their customers, figure out the risks that come with transactions, and take steps to successfully lower those risks.

International cooperation: AML programs encourage countries and financial institutions around the world to work together and share information in order to stop money laundering and other financial crimes that happen across borders.

Minimizing reputational risks: Anti-money laundering (AML) rules help Financial Institutions lower the negative risks that come with laundering money, which builds trust in the financial system.

Encouraging the Suspicious Activities reporting: One important goal is to set up a way for suspicious activities to be found and reported quickly, so that the authorities can look into them and take the right steps.

Adaptation to Varying Threats: AML programs try to stay flexible and adaptable to new ways of moving money, new financial threats, and changes in the rules that govern them.

Keeping the world's financial system safe: Overall, the main goal of AML is to protect the world's financial system from the bad effects of money laundering, making sure it stays honest, stable, and strong against illegal activities.

6 popular elements of AML are:

- **Customer due diligence (CDD)** is the process of confirming a customer's identification and determining the nature of their business dealings.
- **Transaction monitoring** is the ongoing observation of financial transactions in order to spot odd trends or sizable transactions that might point to the laundering of money.
- **Reporting Suspicious Activity** by notifying the relevant authorities of possible money laundering operations.
- **Record-keeping** of all transactions, client data, and risk evaluations.
- **Providing education and training** to staff members so they can identify and report suspicious activity.
- **Regulatory Compliance** by keeping updates of AML rules and regulations in order to adjust to changing risks.

For Example:
Alex (Financial Institutions Compliance Officer): Alex is responsible for ensuring the Financial Institutions's compliance with Anti-Money Laundering (AML) policies.
Sarah (Financial Institutions Customer): Sarah is a regular customer who conducts typical Financial Institutionsing transactions.
John: John is a new customer attempting to deposit a large sum of cash without providing clear explanations.

Sarah, a regular customer, continues her routine transactions without any issues. However, when John, a new customer, attempts to open an account and deposit a substantial amount of cash, Alex initiates the customer due diligence (CDD) process.

John is required to provide identification, explain the source of funds, and clarify the purpose of the large deposit. This is a standard procedure to understand the legitimacy of the transaction.

Combating Terrorism Financing (CFT):

Countering financing of operations aimed at using terrorism to further political, religious, or ideological objectives is what counterterrorism (CFT) is all about.

Principal Goals of CFT are:

Disrupting Terrorism Financing: The main goal of CFT is to locate and stop the money flow that terrorist groups get.

Global Cooperation: To combat the cross-border financing of terrorists, international cooperation is essential.

Enhancing National Security: CTF programs are very important for improving national security because they stop terrorist groups from getting money to do bad things that put people's safety and well-being at risk.

Meeting the requirements of international standards: The Financial Action Task Force (FATF) and other groups work with the CTF to make sure that countries and financial institutions follow the rules and responsibilities that are set by the FATF and other groups to stop terrorists from getting money.

Intelligence sharing: One of the CTF's goals is to encourage countries to work together and share information so that they can fight cross-border funding of terrorism and make sure that everyone is working together to deal with global threats.

Resilience of the Financial System: The goal of putting in place CTF steps is to make the financial system less vulnerable to being used by terrorist groups, so it stays stable and honest.

Getting Better at Due Diligence: The CTF's main goal is to make sure that strong due diligence processes are in place to find and evaluate the risks that come with customers and transactions that may be linked to terrorist funding.

Boosting trust and safety in the public: CTF measures help keep people safe by stopping terrorist activities. This builds trust in the economy and the Financial Institutionsing system in particular.

Key Elements of CFT are:

Risk assessment is the process of determining and evaluating the hazards associated with the financing of terrorism.

Reporting any transactions or actions that give rise to suspicions of being connected to the funding of terrorism is known as suspicious activity reporting, or SAR.

Frameworks for rules and regulations: Setting up and enforcing broad legal and regulatory frameworks that make activities that help terrorists get money illegal, and making sure that both financial institutions and people follow these rules.

Due Diligence for the Customer (CDD): Putting in place strong customer due diligence procedures to make sure customers are who they say they are, figure out how risky they are, and keep an eye on deals for any strange or suspicious activity.

Enhanced Due Diligence (EDD): Using stricter due diligence procedures on customers or transactions that pose a higher risk, such as asking for more information and keeping a closer eye on them, can help lower the risks of terrorist funding.

Watching over transactions: Using high-tech monitoring systems to look for patterns in transactions that could point to possible terrorist funding activities. To do this, you need to set up alerts for activities that seem odd or pose a high risk.

Sharing of information: Getting organizations from around the worldólike Financial Institutionss, police, intelligence agencies, and regulatory bodiesóto share information and data more easily. Together, we can find and stop terrorist support better when we work together better.

Regulatory Structure:

Financial regulatory agencies and national governments usually create AML and CFT legislation.

These rules must be followed by financial institutions; failure to do so may result in legal repercussions.

For Example:
Lisa: Lisa works for a financial institution and is responsible for implementing CFT policies.
James: James is a customer whose financial transactions have raised suspicions

Lisa conducts a routine risk assessment, evaluating the hazards associated with various financial transactions. During this assessment, she identifies certain transactions by James that appear unusual. Based on the risk assessment, James becomes a high-risk customer due to the observed patterns in his transactions.

Importance of AML/CFT compliance

Compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations is vital for maintaining the integrity of financial institutions and shielding society from the damaging effects of financial crime. AML/CFT compliance is crucial for the following main reasons:

Preventing Money Laundering:
The purpose of anti-money laundering (AML) procedures is to identify and stop the illicit practice of hiding the source of money gained through illegal means and disguising it as coming from authorized sources. The integrity of the financial system is preserved by businesses and financial institutions through the prevention of money laundering.

Countering Terrorism Financing:
Finding and stopping the funding of terrorist activity is the main goal of CFT initiatives. It is crucial for both national and international security to stop the funding of terrorist groups.
Sustaining Economic Stability:

Financial institutions and markets may become unstable as a result of money laundering and terrorism financing. AML/CFT procedures make guarantee that money is utilized for authorized reasons, which contributes to the stability of financial systems.
Compliance with Laws and Regulations:

In most jurisdictions, adherence to AML/CFT legislation is legally required. Serious fines, penalties, and legal action against people or organizations are possible outcomes of non-compliance. Respecting these rules is necessary to stay out of trouble with the law.
Preserving One's Image:

Companies and financial institutions run a serious danger of having their reputations severely damaged if they are implicated in money laundering or terrorism financing. A tarnished reputation may result in a decline in trust, clientele, and commercial partnerships.
Safety of the Nation:

Measures for AML/CFT are essential to national security initiatives. The identification and disruption of terrorists' and criminal organizations' financial networks aids in the prevention of actions that could endanger national security.
International Collaboration:

Financing for terrorism and money laundering frequently cross-national boundaries. AML/CFT compliance promotes global collaboration and information exchange between nations and financial institutions, enhancing our ability to fight financial crime on a worldwide scale.
Improving the Integrity of Financial Institutions:

Financial institutions' integrity is improved by adhering to AML/CFT regulations. It draws clients who appreciate openness and responsibility by displaying a dedication to moral corporate conduct and prudent financial management.
Due diligence on the part of the customer:

AML/CFT protocols, like Know Your Customer (KYC) processes, guarantee that companies have a comprehensive grasp of their clientele. This lays the groundwork for ethical commercial dealings while also aiding in the prevention of financial crime.
Adapting to Evolving Threats:

Techniques used in financial crime are always changing. In order to keep ahead of criminal actors, AML/CFT compliance necessitates ongoing monitoring and adaptation to new and emerging threats.

Module 4 Application of AML/CFT regulations on different stages of Money Laundering

AML/CFT mitigation controls at Placement:

Financial institutions must keep an eye on transactions for any odd trends, such as a lot of little deposits that might point to structuring.

Automated algorithms have the ability to identify several minor transactions from several users as suspicious, which prompts additional research.

Example
Scenerio
Michael (Structured Depositor): Michael is a low-level operative working for an extremist group "His role is to deposit small amounts of money in various accounts to fund the group's activities while avoiding suspicion.
Sophie (AML Analyst): Sophie is a diligent Anti-Money Laundering (AML) analyst working at a financial institution.

Structured Deposits:
Michael, the operative, makes multiple small cash deposits at various branches of a Financial Institutions, each below the reporting threshold, to avoid attracting attention.
Transaction Monitoring by AI:
The AI system, constantly monitoring transactions, detects a pattern of numerous small deposits from different users in a short timeframe.
The system identifies Michael's transactions as potentially suspicious based on the structured nature of the deposits.
Alert to AML Analyst:
Sophie, the AML analyst, receives an alert from the automated system regarding the suspicious deposit pattern.
The alert prompts Sophie to conduct additional research into Michael's transactions to assess the legitimacy and identify any potential links to illicit activities.

Compliance with AML/CFT mitigation controls at Layering:

- **Transaction Monitoring and Analysis:** Under AML/CFT regulations, transactions must be continuously monitored, particularly those with high volumes or complex patterns. Reporting entities may be required to conduct enhanced due diligence on transactions that display layering characteristics, like fast money transfers between multiple accounts.

- **Know Your Customer (KYC):** Robust KYC procedures necessitate that financial institutions have a clear understanding of the beneficial owners of accounts involved in complex transactions.

Scenario

Characters:

Olivia (Layering Specialist): Olivia is a financial expert and a key operative for an international criminal organization. Her expertise lies in creating intricate financial transactions to layer and obscure the illicit origins of funds.

David (Business Owner): David is a seemingly legitimate business owner who unwittingly becomes a part of the layering process. He owns a chain of small retail stores.

Initiating Layering:

Olivia, the Layering Specialist, receives a significant amount of illicit funds generated through various criminal activities conducted by organization
She devises a plan to layer and obscure the source of these funds to make them appear legitimate.

Transaction through Legitimate Business:

Olivia approaches David, the unsuspecting business owner, and proposes a partnership or investment opportunity for his retail stores.
David, unaware of the illicit origins, agrees to engage in a seemingly legitimate financial transaction with Olivia.

Intricate Financial Transactions:

Olivia initiates a series of complex financial transactions involving the purchase and sale of goods, inter-company transfers, and investments in various industries.
These transactions are designed to create layers of complexity, making it difficult for investigators to trace the funds back to their illicit source.

Use of Shell Companies:

Olivia establishes shell companies in tax havens and engages in transactions between these entities, further complicating the financial trail.
The shell companies act as a layer to obfuscate the flow of funds and add an additional level of complexity.

Investigation by AML Detective:

Detective Smith, the AML investigator, notices unusual patterns in financial transactions related to David's retail stores.
Suspecting layering, Detective Smith initiates a comprehensive investigation into the transactions involving David and the intricate financial network established by Olivia.

Legal Action and Asset Freezing:

Based on the findings of the investigation, law enforcement takes legal action

against Olivia and her associates.
Assets involved in the layering process are frozen, disrupting the financial network

AML/CFT mitigation controls at Integration:

- **Transaction Monitoring and Reporting**: Unusual or large transactions, especially those involving cash or rapid investments in businesses, trigger transaction monitoring systems. Financial institutions are required to report such transactions to regulatory authorities.

- **Customer Due Diligence (CDD)**: Effective CDD procedures would involve verifying the legitimacy of the business and its owners before allowing substantial investments.

- **Suspicious Activity Reporting (SAR):** If a financial institution suspects that funds are being used for illicit purposes, it is required to file a Suspicious Activity Report (SAR) with the appropriate authorities.

Scenario:

Characters:

Sophie (Business Owner): Sophie is a legitimate entrepreneur who owns a technology start-up called "TechPulse Innovations."

Martin (Money Launderer): Martin is a skilled money launderer associated with an organized crime syndicate. His objective is to integrate illicit funds into seemingly legitimate businesses.

Targeting a Legitimate Business:

Martin, the money launderer, identifies "TechPulse Innovations" as a potential target for integration due to its promising growth and financial stability.
Large Cash Investment:

Martin approaches Sophie offering a substantial cash investment in TechPulse Innovations to accelerate its expansion.
This investment is part of the money laundering strategy to integrate illicit funds into the legitimate business.
Transaction Monitoring Activation:
The large cash investment triggers the transaction monitoring system at the financial institution where TechPulse Innovations holds its accounts.
Unusual patterns and the significant cash amount raise red flags in the system,

prompting further scrutiny.

Customer Due Diligence (CDD):

Detective Patel, the AML investigator, initiates a thorough Customer Due Diligence (CDD) process on TechPulse Innovations and its owner, Sophie.

The objective is to verify the legitimacy of the business and ensure that the large cash investment aligns with lawful activities.

Suspicious Activity Reporting (SAR):

Detective Patel, upon discovering inconsistencies and potential red flags during CDD, decides to file a Suspicious Activity Report (SAR) with the regulatory authorities. The SAR includes details about the large cash investment, Martin's involvement, and the need for further investigation.

Regulatory Action:

The regulatory authorities review the SAR filed by Detective Patel and initiate an investigation into TechPulse Innovations and Martin.

If the investigation uncovers illicit activities, regulatory actions such as fines, penalties, or legal consequences may be imposed.

Module 5: Legal Framework

Global context of AML/CFT standards

Standards for anti-money laundering (AML) and counter-terrorism financing (CFT) are critical components of the global effort to combat financial crime. These guidelines are designed to prevent and combat illegal financial activity such as money laundering, terrorist financing, and other types of financial crime.

Financial Action Task Force (FATF)

The Financial Action Task Force is an international organization whose mission is to prevent the financing of terrorism and money laundering. Its 37 member jurisdictions and two regional organizations collectively constitute the preponderance of significant global financial centers. Establishing global AML compliance standards and supervising their effective implementation is its primary objective. To accomplish this objective, the FATF consistently issues revised AML/CFT recommendations.

FATF requirements must be met by member states and their financial institutions through the following means:

- ID verification procedure implementation for Know Your Customer (KYC).
- Implementing the due diligence measures recommended by the FATF.
- Maintaining accurate records regarding high-risk customers.
- Consistently monitoring accounts for indications of suspect financial activity and notifying the relevant national authority of such findings.
- Implementing stringent sanctions against individuals and affiliated entities that do not adhere to the regulations set forth by the FATF.

FATF member countries are at https://www.fatf-gafi.org/en/countries/fatf.html

The International Monetary Fund (IMF)

The International Monetary Fund (IMF) collaborates with its member nations to enhance their financial systems and regulatory frameworks, thereby exerting a substantial influence in the fight against money laundering and terrorism financing. Although the IMF lacks direct law enforcement jurisdiction, it furnishes its member nations with guidance, technical assistance, and expertise to bolster their capabilities in countering illicit financial activities.

Several major issues are included in the worldwide context of AML/CFT standards:

International Collaboration:

International institutions, such as the Financial Action Task Force (FATF), establish and promote AML/CFT standards. The Financial Action Task Force (FATF) is an intergovernmental organization that establishes global standards and encourages the adoption of legal, regulatory, and operational measures to address money laundering, terrorism financing, and other associated concerns.

Implementation at the regional and national levels:

Countries all over the world put AML/CFT rules in place at the national level, tailoring them to their legal and regulatory systems. Many countries develop regulatory agencies, rules, and regulations to ensure that these criteria are met.

Jurisdictions that refuse to cooperate:

The FATF recognizes jurisdictions that lack adequate measures to prevent money laundering and terrorism funding and labels them "non-cooperative." This categorization can have serious consequences for international financial operations involving firms in those nations.

The global context of AML/CFT standards indicates a determined effort to provide a coordinated and effective worldwide response to the issues posed by money laundering and terrorism financing.

UK AML legislation and regulatory bodies

The United Kingdom has been actively involved in preventing money laundering through a range of legal initiatives. An important legislative milestone is the enactment of the UK's Anti-Money Laundering Act (AMLA) in 2018. It is important to be aware that there may have been additional advancements or modifications after my previous update, hence it is crucial to consult the most recent sources for the most current information. Presented here is a thorough summary of the governing bodies responsible for enforcing the Anti-Money Laundering Act in the United Kingdom:

Anti-Money Laundering Act of the United Kingdom of Great Britain and Northern Ireland:

The Anti-Money Laundering Act of the United Kingdom of Great Britain and Northern Ireland is a comprehensive piece of legislation aimed to strengthen the United Kingdom's capabilities to combat money laundering and terrorism funding.

Key Authorities and Regulatory Organizations:

Financial Conduct Authority (FCA):

The FCA is the major regulatory organization in the United Kingdom that oversees financial institutions such as Financial Institutionss, investment firms, and other financial service providers.

It is critical in implementing AML legislation and ensuring financial industry compliance.

NCA (National Crime Agency):

The National Crime Agency (NCA) is the UK's principal agency for combating severe and organized crime, including money laundering. To investigate and punish money laundering charges, it collaborates closely with other law enforcement authorities and foreign partners.

The mission of the National Crime Agency is to safeguard the public against organized and severe criminal activity.

This is achieved by:

Demolishment of the most perilous organized crime syndicates that present a challenge to the United Kingdom

Guidance of the nationwide operational campaign against severe and organized crime within the United Kingdom.

HMRC (HM Revenue & Customs):

HMRC is in charge of enforcing AML requirements in specific industries, including oversight of enterprises engaged in high-value transactions.

It is in charge of compliance in fields such as estate agency, high-value dealers, and money service enterprises.

CPS (Crown Prosecution Service):

The CPS prosecutes criminal matters that have been examined by law enforcement, especially those involving money laundering.

Following the completion of investigations, it plays a part in the legal process.

Anti-Money Laundering Act 2017

This act gives the government the power to impose sanctions when necessary to fulfill international obligations, fight against terrorism, and maintain peace and security. It also helps in achieving foreign policy goals. Additionally, the act includes measures to find, investigate, and prevent money laundering, which is the process of making illegally

obtained money look legal. In simple terms, it's a law to support global efforts, tackle terrorism, and address financial wrongdoing (Sanctions and Anti-Money Laundering Act 2017).

Key Provisions of MLR 2017 are:

- Money Laundering and Terrorist Financing
- Risk assessment and controls
- Customer Due Diligence
- Reliance and Record-keeping
- Beneficial Ownership Information
- Money Laundering and Terrorist Financing: Supervision and Registration
- Transfer of Funds (Information on the Payer) Regulations
- Information and Investigation
- Enforcement
- Appeals

Fourth Money Laundering Directive (4MLD) and Fifth Money Laundering Directive (5MLD):

The UK has implemented European Union directives to strengthen its AML system. The 4MLD and 5MLD propose new measures to address rising risks and improve financial transaction transparency.

In order to detect and prevent money laundering, 5AMLD intends to increase the number of organizations required to comply with AML regulations and implement more stringent regulations.

- 5AMLD incorporates technological advancements and financial sector trends, while also furnishing a precise explanation of cryptocurrency and requirements regarding virtual currency exchanges and purses.
- The directive places emphasis on the oversight of anonymous prepaid cards and the enhancement of public accessibility to property data.

5AMLD's overarching objective is to bolster confidence and financial integrity through its efforts to combat money laundering and terrorist financing.

National Risk Assessment (NRA):

NRAs are conducted in the United Kingdom to analyze the hazards of money laundering and terrorism financing. The findings help to shape AML strategies and priorities.

Sanctions Regulations:

Individuals and businesses implicated in money laundering and other illegal actions face sanctions in the United Kingdom. The sanctions regime is part of broader anti-money laundering initiatives to combat financial crime.

Module 6: Risk Assessment

A key idea in attempts to combat the funding of terrorism (CFT) and prevent money laundering (AML) is the risk-based approach (RBA).

RBA is a crucial principle in the endeavor to combat the financing of terrorism (CFT) and deter money laundering (AML).

The Financial Action Task Force (FATF), a global organization responsible for establishing guidelines on anti-money laundering (AML) and countering the financing of terrorism (CFT), actively promotes the adoption of the risk-based approach (RBA). Below is a summary of the fundamental elements associated with the risk-based approach:

- **The Financial Action Task Force (FATF)**

  FATF is an intergovernmental organization that establishes worldwide benchmarks for addressing money laundering, terrorist financing, and other associated risks to the stability of the global financial system. The recommendations issued by FATF offer a structured approach for nations to adopt and enforce robust anti-money laundering (AML) and countering the financing of terrorism (CFT) policies.

- **Risk-Based Approach (RBA):**

  The Risk-Based Approach is a guiding philosophy that entails evaluating the risk characteristics of transactions, clients, and business relationships in order to allocate resources in a more efficient manner. Institutions customize their anti-money laundering (AML) and countering the financing of terrorism (CFT) measures according to the amount of risk associated with each specific case, rather than using a standardized method.

- **Risk Appetite:**

  Risk appetite refers to the extent to which an organization is willing to tolerate risk in order to achieve its goals. It provides guidance for determining the appropriate level of risk exposure that is deemed acceptable.

- **Inherent Risk:**

  Inherent risk denotes the degree of risk linked to a client, transaction, or business association without any mitigating procedures in place. It denotes the inherent risk that exists prior to the use of risk management techniques.

Some examples are:

Online Account Opening

Identity Fraud Risk: The utilization of fraudulent or stolen identities to create accounts is facilitated by the lack of physical verification during non-face-to-face account openings, which introduces an inherent risk of identity theft.

Remote Transactions:

Due to the possible absence of comprehensive identity verification, non-face-to-face transactions are vulnerable to inherent risks associated with unauthorized access, which may result in fraudulent or unauthorized transactions.

Digital Payments:

Vulnerabilities in the authentication processes of digital payment methods expose them to inherent risks, including unauthorized access and fraudulent activities, particularly when feeble passwords or PINs are employed.

Remote Customer Service:

The provision of customer service remotely entails inherent risks associated with social engineering attacks. In such attacks, criminals can manipulate individuals into sharing sensitive information by taking advantage of the lack of face-to-face verification.

Mobile Banking:

Device Security Concerns: Mobile banking entails inherent risks owing to potential security breaches on mobile devices, which may result in unauthorized access and expose sensitive financial data to cyber threats.

- **Residual Risk:**

Residual risk refers to the level of risk that remains after implementing risk reduction strategies. It represents the ongoing risk that remains even after implementing controls and procedures to decrease the inherent risk.

Examples are:

Credit Risk:

Economic Downturn: Despite rigorous credit risk evaluations, borrowers in financial difficulties during economic downturns increase loan default risk.

Operations Risk:

Technology Failures: After IT precautions, unforeseen technology failures, system problems, or cyberattacks may cause operational disruption.

Market Risk:

Unexpected Market Movements: Rapid fluctuations in interest rates, foreign currency rates, or commodity prices might affect the institution's portfolios notwithstanding risk management procedures.

Liquidity risk:

Sudden Withdrawals: Despite liquidity management efforts, depositors and investors may make large withdrawals, especially during financial instability, which could affect the institution's liquidity.

The Risk of Compliance and Regulation

Changes in regulations, new compliance standards, or legal interpretations may influence the institution's operations and profitability despite continued compliance efforts.

Security Risk:

Sophisticated Cyber Attacks: Advanced persistent assaults and zero-day vulnerabilities may not be detectable or avoidable even with strong cybersecurity solutions.

Interest Rate Risk:

Interest Rate fluctuations: After interest rate risk management, unexpected and significant interest rate fluctuations might affect the institution's net interest income and assets and liabilities.

Fraud Risk:

Internal Fraud: Employees or insiders may embezzle, make illicit transactions, or manipulate financial records despite internal controls.

- **Risk Matrix:**

A risk matrix is a tool utilized to evaluate and visually represent the degree of risk linked to various elements. Usually, it entails graphing the probability of an occurrence in relation to its potential consequences. This matrix facilitates the classification of hazards and their prioritization according to their importance.

Following is example of risk matrix

Inherent Risk Rating Matrix

Likelihood	Consequences					
	Ratings	1	2	3	4	5
	5	MH	H	H	H	H
	4	MH	MH	H	H	H
	3	M	M	MH	MH	H
	2	L	L	M	MH	MH
	1	L	L	L	M	MH

Residual Risk Rating Matrix

Inherent Risk	Existing Controls				
	Ratings	1	2	3	4
	H	H	H	MH	M
	MH	MH	MH	M	L
	M	M	M	M	L
	L	L	L	L	L

- **Risk Assessment:**

  Risk assessment entails the methodical identification, analysis, and evaluation of hazards linked to a certain activity or business association. It evaluates variables such as client demographics, transaction behavior, and geographical data to ascertain the degree of risk.

Main risk Factors

- Customer Risk:
- Transaction Risk:
- Agent Risks:
- Geographical Risks
- Volume of transaction
- Delivery Channel
- Product and Services

Customer Risk

Higher-risk categories of customer will include:

- **PEPs**

  John, a high-ranking government official, opens a Financial Institutions account. Due to his prominent position by holding high public office (FCA), he falls into the PEP category, posing a higher risk of potential involvement in corruption or illicit activities (Guidance on the treatment of politically exposed persons (PEPs) under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017).

- **Customer with Unusual behavior**

  Sarah, a long-time customer known for making small, routine transactions suddenly starts depositing large sums of cash without a clear explanation. The sudden change in behavior raises concerns and increases the risk associated with her transactions.

- **Customer doing on someone else behalf**

  Alex conducts financial transactions on behalf of his friend without providing a valid reason. The lack of clarity regarding the nature of the transactions increases the risk associated with Alex as a customer.

- **Customer getting instructions from Someone**

  Mary consistently receives instructions from an unidentified individual regarding fund transfers and transactions. The reliance on external instructions without proper verification raises the risk associated with Mary's account.

- **Customer Sending to High Risk Jurisdictions**

  David frequently sends large sums of money to a country known for high levels of financial crime and corruption. The destination's high-risk status increases the overall risk associated with David's transactions.

- **Non Local Customer**

  Lisa, a foreign individual, opens an account in a local Financial Institutions. Being a non-local customer, Lisa may pose a higher risk due to potential challenges in verifying her background and monitoring her financial activities from abroad.

Transaction risk

Higher-risk transactions will include:

- **Cash Intensive Business**

  "Quick Mart," a little convenience store, predominantly conducts business through cash transactions. The business carries out a substantial proportion of its sales using physical currency, rendering it vulnerable to potential illicit financial activities such as money laundering or tax evasion. Consequently, this transaction can be classified as a higher-risk transaction.

- **Transaction sending to High Risk Country**

  Mr. Smith, a client of a financial institution, frequently transfers substantial amounts of money to a country with inadequate anti-money laundering and counter-terrorism financing rules and a significant incidence of financial misconduct. This

transaction has a greater risk because it is connected to a country that lacks sufficient regulatory measures.

- **Transaction is of High value or Occasional Transaction**

ABC Corporation, a manufacturing company, unexpectedly undertakes a singular transaction of remarkably high worth that diverges from its typical business pattern. The abrupt and substantial surge in transaction value arouses suspicion and classifies it as a transaction with a greater level of risk.

- **Transaction does not make economic sense**

Ms. Johnson is an active participant in frequent purchasing and selling activities of the same asset over a short period, which leads to substantial financial losses. This form of circular and economically illogical transaction gives rise to worries regarding potential money laundering, as it deviates from customary economic conduct.

- **Transaction through Third party**

XYZ Company constantly employs an intermediary third party to move monies between its subsidiaries through a series of transactions. The presence of a third party gives rise to suspicion, particularly if the transactions lack a distinct economic objective or if the third party is situated in a jurisdiction with inadequate anti-money laundering and counter-terrorism financing rules.

Risk related to agents

Payment institutions in the UK have the option to onboard agents to expand their business without the necessity of opening separate branches.

Following are the possible risks associated:

The following are examples of common risk indicators that principals and agents need to be
aware of:
ï represent more than one principal or act as both an agent and a principal
ï are reluctant to provide information regarding their customerís identity to the principal
ï record unusual or suspicious customer information (many transactions attributed to a single customer or customer details that may be false or incorrect)
ï have a high number of transactions that fall just under the threshold for due diligence or reporting to the principal
ï report a high volume of business with single customer to a high-risk country
ï process a customer sending money to several destinations or the same recipient on the same day
ï have a pattern of customers in the office that doesn't support the turnover

ï have an unusually high transaction size
ï have an unusually large cash transaction
ï have a size and frequency of transactions that:
o are different from the customerís normal pattern
o have changed since the agency relationship was established
o are higher than comparable agencies
o change significantly under new management of the agency
ï have transactions that seem unnecessarily complicated, or seem to use front men or companies
ï undertake a large proportion of business with high-risk countries
ï undertake business outside normal business hours
ï have records in which fake identities repeat common fields, for example a different surname with all the other details like birth day and address the same
ï transactions too fast to be possible
ï are located geographically in a high-risk area (e.g. in another cash intensive business, or in a border area)
ï remit funds overseas in cash through couriers or parcel companies
ï former money service businesses re-registering as different cash businesses
76
April 2020
ï money service businesses not disclosing money service business activity to their bank
ï multiple money service business premises operating in very small area
ï money service businesses with bank accounts held in higher risk countries rather than the UK

Geographic risks:

High-Risk Jurisdictions:

Michelle frequently transfers funds to nations renowned for their elevated rates of financial malfeasance and corruption. The destination countries provide a larger geographical risk due to inadequate regulatory restrictions, increasing the overall risk associated with Michelle's transactions.

List of FATF high risk countries is at https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2023.html and list issued by UK for high risk jurisdictions is at https://www.lawsociety.org.uk/topics/anti-money-laundering/high-risk-third-countries-for-aml-purposes

Political instability:

James, a client residing in a region experiencing persistent political turmoil, participates in substantial financial transactions. The volatile political climate adds a further element of uncertainty, as it might potentially enable money laundering or illicit financial operations.

When there is political instability, there is often economic instability as well, which makes markets and financial institutions less stable. Devaluation of the currency, inflation, and changes in government policies can all have an effect on business deals.

Volume of Transactions:

Unusual and Occasionally Transections:

These are transactions that deviate significantly from the normal patterns or volumes associated with a particular customer or business.

Marry typically engages in small, routine transactions suddenly initiates a large, one-time transfer to an offshore account. This unusual transaction may signal potential money laundering, tax evasion, or other illicit activities.

The Smurfs:

Smurfing, which is also called structuring, is the act of hiding big transactions by breaking them up into smaller ones that are less noticeable.

Jeena intends to deposit $50,000 in cash into a bank account, which would trigger mandatory reporting requirements. To avoid detection, the Jeena breaks down the $50,000 into smaller transactions, depositing $5,000 each on ten different occasions.

Speed of Transactions:

The rate at which transactions happen, especially in high-frequency trading or systems that handle trades quickly.

Risk involved in such case is transactions that happen quickly can make mistakes, system problems, or illegal dealing more likely. Let us say that Jeena, the person who is smurfing, chooses to take out $50,000 in cash from her bank account right after depositing each $5,000. To stay even more hidden, she quickly takes out the money within minutes or hours of each payment and does this several times.

The speed of transactions becomes an important part of the plan in this case. By depositing and withdrawing money quickly and in smaller amounts, Jeena hopes to hide the total transaction and make it less likely that it will be reported as required.

Traditional transaction monitoring tools may not be able to keep up with all of these transactions happening so quickly, which can be a problem.

Risks of Transaction Monitoring:

Transection monitoring is the system and procedure in place for keeping an eye on and finding suspicious deals are working.

If the transaction monitoring tools aren't good enough, you might miss alerts for activities that could be suspicious. This can cause people to take too long or not enough action to reduce the risks that come with illegal financial dealings.

Method of delivery:

Transactions involving Third Parties:

When third parties are involved, there is a chance that there won't be direct control or transparency over the transaction, which leaves it open to abuse or illegal activity.

Example: Sarah asks her friend Jake if she can receive funds from a business transaction into his bank account, hiding the true beneficiary and purpose of the funds.

Money Transferred Across International Borders (cross-border transactions):

Cross-border transactions add another layer of complexity, with currency exchange risks, regulatory variations, and the possibility of being used by criminal actors in countries with lax financial controls.

Example: Emma's company in Country A receives payments from customers in Country B but routes the funds through an intermediary jurisdiction with lower tax regulations, minimizing tax liabilities.

Using Brokers or Agents as Intermediaries:

Using intermediaries might increase the chance of financial fraud, as well as the possibility of sensitive information being disclosed without authorization.

Example: Mike hires a broker, Alex, to facilitate a financial transaction, and Alex misuses the entrusted funds for personal gain, leading to financial losses for Mike.

Channels of Electronic Delivery (Online Transactions):

Using electronic delivery methods puts transactions at risk from identity theft, phishing, and hacking, which can lead to illegal access and financial losses.

Example: Jenny falls for a phishing scam, which means that her online banking credentials are stolen. This could lead to unauthorized activities and even financial fraud.

Cash Transactions:

Handling cash transactions entails risks associated with money laundering, theft, and the challenge of determining the source of funds.

Example: Mark sells a valuable item and receives a large amount of cash, but fails to properly document the source of the funds, raising suspicions of potential money laundering.

Mitigation strategies

The term "mitigation strategies" describes the preemptive steps and actions used to lessen or completely eradicate the possibility and impact of risks or dangers. Here are some mitigation techniques in the context of the material you gave, which focuses on the difficulties in identifying risks associated with money laundering (ML) and terrorism financing (TF):

1. Improved Customer Due Diligence (CDD): Plan: Put in place strict CDD procedures.

Explanation: To determine a customer's risk profile, thoroughly investigate their background. This entails confirming their identity, comprehending the type of transactions they are engaging in, and routinely updating their client data.

2. Automated Monitoring Systems: Use cutting-edge monitoring systems as part of your strategy.

Explanation: Utilize technology to keep an eye on consumer behavior and transactional data automatically. Automated systems have the ability to spot odd trends or dangerous activity, which prompts additional research.

3. Artificial Intelligence and Data Analytics: Strategy: Make use of AI and data analytics.

Explanation: Process massive information and spot patterns suggestive of ML/TF dangers by utilizing artificial intelligence and advanced analytics. This has the potential to improve risk assessments' efficacy.

4. Information Sharing Mechanisms: Plan: Create a safe environment for sharing information with regulatory bodies.

Justification: Work together with other financial institutions and the appropriate authorities to establish safe and efficient routes for exchanging private data with regulatory authorities. This can close information gaps and enhance the risk assessment procedure as a whole.

5. Training and Awareness Initiatives: Plan: Organize frequent training initiatives.

Justification: Inform employees about the most recent ML/TF threats, detection methods, and legal obligations. Employees with more knowledge are better able to spot and report questionable activity.

6. International Collaboration: Strategy: Promote cross-border cooperation.

Justification: Collaborate with international partners and institutions to exchange best practices, information, and perspectives. A more thorough grasp of the hazards associated with cross-border ML/TF can be obtained through collaborative initiatives.

7. Frequent Assessments and Audits: Plan: Perform both internal and external audits on a frequent basis.

Justification: Regular evaluations of internal controls and procedures aid in identifying gaps and potential areas for development. An objective assessment of the efficacy of anti-money laundering (AML) procedures can be obtained through external audits.

8. Compliance with Regulatory Standards: Plan: Make sure you follow the rules.

Justification: Stay up to date on and follow changing CFT and AML legislation. Compliance guarantees that financial institutions are carrying out their operations in accordance with the law and industry norms.

9. Whistleblower Programs: Put in place whistleblower mechanisms as part of your strategy.

Justification: Provide a private route for reporting any suspicious activity to promote the reporting of such actions. Programs for whistleblowers might serve as an extra line of protection against unethical financial activity.

10. Continuous Risk Assessment: Plan: Make use of a method to continuous risk assessment.

Justification: Be aware that hazards change with time. Establish procedures for continuous risk assessment and make necessary adjustments to mitigation plans.

When combined, these tactics help to create a thorough and proactive strategy that lessens the difficulties in detecting and managing money laundering and terrorist financing concerns in the financial industry. It's crucial to remember that successful risk reduction frequently necessitates a blend of these tactics, each one relevant to the risks and circumstances that each financial institution faces.

Module 7: Customer Due Diligence (CDD)

Application of CDD, SDD and EDD as per risk

Customer Due Diligence (CDD)

Customer Due Diligence (CDD) (under regulation 27) is a critical component of anti-money laundering (AML) and counter-terrorist financing (CTF) initiatives. CDD entails a detailed examination of a customer's identity, risk profile, and business activities in order to reduce the danger of financial crimes. The fundamental principles of CDD concentrate around gathering and confirming client information, comprehending the nature of the customer's activity, and monitoring the account for suspicious behavior.

Simplified due diligence (SDD)

Simplified due diligence (SDD) is the lowest level of customer due diligence (CDD) that a financial institution can employ. It is a brief identity verification process that can be applied

to eligible customers when the risk of money laundering or terrorist financing is deemed very ìlowî.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is a comprehensive framework comprising rules and procedures designed to address high-risk clients and significant financial transactions. Companies must follow Enhanced Due Diligence steps if they do business with any of the following people or groups:

- Politically Exposed Persons (PEPs) or people close to them, like family members, can't work for any company in a High-Risk Third Country.
- Businesses in fields where money laundering is more likely to happen, like gaming
- The ultimate beneficial owners of Shell companies
- Companies that gave money to terrorist groups were put on a watchlist.
- Private banking and business banking

Customer Due Diligence (CDD)

The following are the basic steps and example of CDD:

Example:
Ms. Emily Johnson:

Emily is a freelance graphic designer with a passion for creative projects. As a self-employed professional, she values financial stability and has decided to open a savings account with Secure Finance Ltd to manage her income and savings. Emily is cooperative and willingly provides the necessary documentation for the account-opening process.
Secure Finance Ltd:

Secure Finance Ltd is a reputable financial institution committed to providing reliable Financial Institutionsing services. With a focus on customer security and regulatory compliance, the Financial Institutions diligently follows the principles of Customer Due Diligence (CDD) to ensure the integrity of its financial transactions. The Financial Institutions's staff, including account managers and compliance officers, work together to create a secure Financial Institutionsing environment for their clients.

- **Customer Identification:**

  Obtain and verify the identification of the customer.

- Establish the customer's identity using dependable and independent documents, facts, or information.
- This usually entails validating the customer's identity, address, date of birth, and other pertinent information.

Secure Finance Ltd requests Ms. Emily Johnson to provide a valid government-issued ID, proof of address, and additional details to confirm her identity before opening a savings account.

- **Understanding the Customer's Business or Purpose:**

  Understand the nature of the customer's business and the relationship's purpose.

- Learn about the customer's history, business operations, and the desired aim of the business connection.
- This knowledge aids in determining the level of risk connected with the consumer.

Emily, a freelance graphic designer, explains to the Financial Institutions that she wants a savings account to manage her income from various clients. The Financial Institutions learns about her occupation and the purpose of the account.

- **Risk Assessment:**

  Evaluate and comprehend the customer's risk profile.

- Assess each customer's risk based on characteristics such as their business activities, geographical location, transaction patterns, and the kind of the products or services they consume.

Secure Finance assesses the risk associated with Emily's account based on her freelance occupation. The Financial Institutions considers factors such as the nature of her business, transaction patterns, and the potential for irregular income.

- **Ongoing Monitoring:**

  Continuously monitor client accounts and transactions.

- Implement systems and processes to detect and report any unexpected or suspicious activity.
- Review customer information on a regular basis and update it as needed.

The Financial Institutions employs a system to monitor Emily's account for any unusual activities, such as large transactions or inconsistent deposit patterns. This helps in promptly detecting and addressing any suspicious behavior.

- **Enhanced Due Diligence (EDD):**

  For higher-risk customers, use enhanced due diligence.

- Conduct more rigorous due diligence on customers who pose higher ML/TF risks, such as gathering additional information, completing more frequent reviews, and deploying stronger monitoring mechanisms.

Since Emily's freelance work poses a moderate risk due to fluctuating income, Secure Finance decides to conduct occasional reviews to ensure ongoing compliance. This involves periodic updates on her financial situation.

- **Screening for Politically Exposed Persons (PEP):**

  The principle is to screen for politically exposed people.

- Determine whether a customer is politically exposed, as these individuals may offer a higher risk owing to their potential involvement in corruption.
- Increase scrutiny and monitoring for PEPs.

Secure Finance checks whether Emily is a politically exposed person. Although unlikely, this step ensures that even individuals with lower-risk profiles are subject to necessary screenings.

- **Record Keeping:**

  Keep complete and accurate records.

- Keep track of customer identity information, due diligence procedures, and transaction history.
- These documents are used to demonstrate compliance with AML and CTF requirements.

The Financial Institutions maintains a record of Emily's identity documents, the due diligence process, and a transaction history. These records are kept securely and can be accessed as needed to demonstrate compliance with regulatory requirements.

- **Training and Awareness:**

  The principle is to train employees and raise awareness.

- Make certain that staff are well-versed in AML and CTF regulations, as well as the significance of CDD.
- Regular training programs aid in the maintenance of an alert and compliant workplace culture.

Secure Finance conducts regular workshops and seminars covering key aspects of AML and CTF regulations.
Employees are trained on the importance of Customer Due Diligence (CDD) in mitigating financial risks and preventing illicit activities.
The training program includes case studies, real-world examples, and interactive sessions to ensure staff members grasp the practical application of AML and CTF principles.

Periodic updates are provided to keep employees informed about any changes in regulations, fostering a culture of compliance and vigilance within the organization.

- **Suspicious Activity Reporting:**

  The principle is to report suspicious actions to the appropriate authorities.

- Establish methods for detecting and reporting suspicious transactions.
- For law enforcement agencies to investigate and take proper action, timely reporting is critical.

Secure Finance employs advanced monitoring systems that automatically flag transactions exhibiting unusual patterns, high values, or inconsistent behavior.
Employees are trained to recognize signs of potentially suspicious activity during routine customer interactions.
The credit union has established clear and efficient procedures for reporting such activities to the designated authorities promptly.
An anonymous reporting system is in place to encourage employees to report concerns without fear of reprisal.
Regular drills and simulations are conducted to ensure that staff is well-prepared to identify and report suspicious transactions effectively.

- **Legal and Regulatory Compliance:**

  Adhere to all applicable laws and regulations.

- Ensure that local and international AML and CTF requirements are followed.
- Keep up to current on legislative changes and adapt CDD procedures accordingly.

Secure Finance regularly reviews and updates its policies and procedures to align with the latest AML and CTF regulations.
It conducts periodic internal audits to verify compliance with established protocols and promptly addresses any identified gaps.
Staff members receive ongoing training on changes in legislation and regulations, ensuring they remain well-informed and capable of implementing necessary adjustments.
Secure Finance collaborates with regulatory bodies and industry associations to stay abreast of emerging trends and best practices in AML and CTF compliance.

Following these steps assists financial institutions in developing effective CDD systems, building a strong defense against money laundering and terrorism funding. The concepts are frequently incorporated into a broader risk-based approach, enabling firms to customize their due diligence efforts to the individual risks associated with each customer.

Simplified due diligence (SDD)

Simplified Due Diligence (SDD) (under regulation 37) is an anti-money laundering (AML) and counter-terrorist financing (CTF) approach. SDD is applied to customers or transactions that are thought to be less likely to be involved in money laundering or terrorist funding. SDD's goal is to accelerate and simplify the due diligence process for these low-risk circumstances while retaining an acceptable level of control.

Minimum checks for SDD

When compared to higher levels of due diligence, SDD requires less work to gather information. Even so, SDD still needs to address the four parts of CDD set out by the Financial Action Task Force (FATF), which is in charge of monitoring financial crime around the world. Some of these are:

- Identifying and checking the customer
- Identification and confirmation of the beneficial owner
- Knowing what the friendship is for and how it works
- Continuous watching

Scenario: A local retail store owner, Mr. Patel, approaches a Financial Institutions to open a basic business account for daily transactions.
SDD Application: Given Mr. Patel's straightforward and low-risk retail business, the Financial Institutions may apply SDD. This involves simplified customer identification procedures and reduced ongoing monitoring, as the risk associated with Mr. Patel's business is considered minimal.

The following are the main components of Simplified Due Diligence:

- **Risk-Based strategy**:
    - SDD adheres to the risk-based strategy, which entails adjusting due diligence measures to the assessed risk level of customers and transactions.

A local retail business is considered a low-risk customer due to its nature and small-scale operations.

- **Identifying Lower-Risk consumers:**
    - SDD is often used to consumers or transactions that are thought to be less likely to be involved in money laundering or terrorist funding. Certain types of consumers, such as low-value accounts or well-established and respected companies, may fall into this category.

Mr. Patelís store, a well-established and respected local retailer with a limited customer base, is identified as a lower-risk consumer.

- **Less comprehensive Customer Verification Requirements**:
    - SDD requires less comprehensive customer verification than ordinary due diligence. The level of examination used is proportionate to the lower evaluated risk.

Instead of requiring extensive documentation, the Financial Institutions may only request basic identification documents from the owner, such as a driver's license and proof of address.

- **Limited Documentation Requirements**:
    - Customers' documentation requirements under SDD are often less onerous. Customers in this category may not demand as much comprehensive information or supporting paperwork from financial institutions.

Mr. Patel may not need to provide in-depth financial statements or extensive business documentation typically required for higher-risk businesses.

- **Simplified Ongoing Monitoring:**
    - Under SDD, ongoing monitoring of transactions is simplified. While financial institutions continue to scrutinize transactions for odd or suspicious activity, the level of attention is often lower than in higher-risk cases.

Although the Financial Institutions continues to monitor Mr. Patelís transactions for any unusual activities, the level of scrutiny is proportionate to the perceived lower risk, allowing for more straightforward monitoring procedures.

- **Exemption from Enhanced Due Diligence**:
    - Customers subject to SDD may be excluded from the more onerous enhanced due diligence (EDD) requirements. This covers cases where more thorough background checks and additional safeguards are not deemed necessary due to the low risk of the customer or transaction.

Mr. Patelís store, being a low-risk retail business, may be exempt from enhanced due diligence requirements that would apply to higher-risk businesses. This exemption is based on the categorical determination of low risk.

- **Categorical Determination of Eligibility**:
    - SDD is frequently used to determine eligibility based on established groups of customers or transactions that are deemed intrinsically low risk. Certain sorts of enterprises, such as government agencies or publicly traded companies, may, for example, be automatically qualified for SDD.

The local retail business category, to which small store belongs, is automatically qualified

for Simplified Due Diligence due to its intrinsically low-risk nature.

- **Periodic Review**:
    - While SDD requires less ongoing monitoring, periodic reviews are still required. Financial institutions must ensure that the customer's or transaction's low-risk designation is maintained throughout time.

Although ongoing monitoring is simplified, the Financial Institutions performs periodic reviews to ensure that store maintains its low-risk designation over time.

- **Clearly Defined Policies and Procedures**:
    - Financial institutions must create clearly defined policies and procedures for implementing SDD. This involves describing the decreased due diligence needs and setting criteria for recognizing low-risk cases.

The Financial Institutions has established clearly defined policies outlining the reduced due diligence requirements for businesses like Mr. Patelís store. These policies specify the criteria for recognizing low-risk cases.

- **Regulatory Standards Compliance**:
    - Financial institutions must verify that their SDD processes are in accordance with applicable AML and CTF regulatory standards. Compliance is critical to preserving the financial system's integrity and meeting legal commitments.

The Financial Institutions ensures that its SDD processes adhere to applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulatory standards. Compliance is crucial to upholding the financial system's integrity and meeting legal obligations.

By implementing Simplified Due Diligence, financial institutions can more efficiently allocate resources, focusing expanded due diligence efforts on higher-risk scenarios while ensuring that adequate procedures to limit the risk of money laundering and terrorism financing remain in place.

Enhanced due diligence (EDD)

Regulation 33(1) of MLR 2017 sets out a list of circumstances in which EDD measures must be applied. EDD is a higher level of analysis and inquiry that goes above and beyond traditional customer due diligence processes. It is usually applied to customers or transactions that are thought to be more likely to be involved in money laundering, terrorism funding, or other financial crimes. EDD's goal is to obtain a better knowledge of the risks associated with certain consumers and to apply further preventive measures.

Scenario: Mr. Johnson, a high-profile government official, intends to open a significant investment account at a financial institution.

EDD Application: Recognizing Mr. Johnson as a politically exposed person (PEP), the Financial Institutions implements EDD measures. This includes gathering additional information about his financial activities, conducting more frequent reviews, and employing stringent monitoring mechanisms to mitigate the heightened risk associated with PEPs.

Here are some of the most important aspects and principles of Enhanced Due Diligence:

- **Risk-Based Approach:**
    - EDD is an essential component of anti-money laundering (AML) and counter-terrorist financing (CTF) activities. It entails assessing consumers' risk profiles and changing due diligence efforts accordingly.

Recognizing Mr. Johnson as a high-profile government official, the Financial Institutions employs EDD as part of its risk-based approach to evaluate the elevated risk associated with politically exposed persons (PEPs).

- **Identifying High-Risk clients:**
    - EDD is often used to clients who are deemed to be at higher risk. Consumers in high-risk jurisdictions, consumers with complex ownership structures, and those engaging in high-value transactions are examples of politically exposed persons (PEPs).

Mr. Johnson, being a government official, is automatically categorized as a high-risk client due to his status as a politically exposed person (PEP).

- **Thorough Customer Verification:**
    - EDD necessitates a more thorough verification of the customer's identification. This could entail getting additional documentation, running more thorough background checks, and establishing the source of funding.

EDD involves a meticulous verification process for Mr. Johnson's identification. The Financial Institutions requests additional documentation, conducts extensive background checks, and scrutinizes the source of funding for his significant investment.

- **Understanding Business Relationships:**
    - EDD places a premium on gaining a comprehensive understanding of the customer's business activities, transactions, and relationships. To assess associated risks, financial institutions must understand the purpose and nature of the business connection.

The Financial Institutions delves into a comprehensive understanding of Mr. Johnson's business activities, examining his transactions and relationships. This ensures a thorough assessment of associated risks related to his political position.

- **Tighter Transaction Monitoring:**
    - Transaction monitoring gets more stringent under EDD. Financial institutions improve their systems to detect and report any unusual or suspicious activity as soon as possible.

Transaction monitoring becomes more stringent under EDD. The Financial Institutions enhances its systems to promptly detect and report any unusual or suspicious activity related to Mr. Johnson's investment account.

- **Periodic Review and Information Updating**:
    - EDD requires more regular checks of customer information. Updating customer profiles on a regular basis guarantees that the financial institution has the most up-to-date information for risk assessment.

EDD mandates more frequent checks of Mr. Johnson's information. The Financial Institutions updates his profile regularly to ensure that the most current information is available for ongoing risk assessment.

- **Senior Management Approval**:
    - Senior management approval may be necessary in specific instances when conducting EDD. This ensures that the decision to implement increased measures comes from a higher level within the business.

Due to the elevated risk associated with politically exposed persons, senior management approval is sought before implementing EDD measures for Mr. Johnson. This ensures a higher level of oversight in decision-making.

- **Continual Monitoring:**
    - EDD is a continual process, not a one-time event. Financial institutions must remain watchful and change their risk management procedures in response to changing customer profiles and external circumstances.

EDD is an ongoing process. The Financial Institutions remains vigilant, adapting risk management procedures as needed in response to changing profiles and external circumstances related to Mr. Johnson's account.

- **Documentation and Record Keeping**:
    - In EDD, comprehensive and well-documented records are essential. Financial institutions must keep track of the additional due diligence measures they conduct, as well as the reasoning behind their decisions.

The Financial Institutions maintains comprehensive and well-documented records of the EDD conducted on Mr. Johnson. This includes details of additional due diligence measures

and the rationale behind the decisions made.

- **Training and Awareness:**
    - EDD process staff should undergo specific training. This guarantees that personnel understand the complexities of higher-risk customer assessments and can perform improved due diligence processes efficiently.

Staff involved in the EDD process undergo specific training to understand the complexities of assessing higher-risk customers. This ensures that the Financial Institutions's personnel can efficiently and effectively perform the enhanced due diligence procedures.

- **Compliance with Regulatory Requirements:**
    - In EDD, compliance with relevant laws and regulations is critical. Financial institutions must ensure that their improved due diligence activities comply with AML and CTF regulatory standards.

Throughout the EDD process, the Financial Institutions ensures strict compliance with relevant AML and CTF laws and regulations. Adherence to regulatory standards is a critical aspect of the Financial Institutions's commitment to maintaining the integrity of its operations.

Financial institutions hope to reduce the risk associated with higher-risk customers and transactions by implementing Enhanced Due Diligence, hence boosting their overall AML and CTF operations. The extent to which increased due diligence is required may differ depending on the individual risk considerations connected with each customer or transaction.

Module 8: Understanding Suspicious Activity Report (SAR) requirements

What is Suspicious Activity Report (SAR)

The SAR was introduced by the Bank Secrecy Act (BSA) of 1970 as a critical tool for overseeing and recognizing suspicious behaviors and criminal activity that are not normally emphasized in other reports, such as the currency transaction report.

The SAR report emerged in 1996 as the standardized form for reporting suspicious activity in order to combat money laundering.

SAR is a document filed by related institutions to track suspicious activities and notify regulatory bodies about them. A SAR is a disclosure made to the National Crime Agency (NCA) about known or suspected:

- Money laundering ñ under part 7 of the Proceeds of Crime Act 2002 (POCA)

    The SAR serves as a disclosure made in accordance with part 7 of POCA, aimed at addressing and preventing money laundering activities.

- Terrorist financing ñ under part 3 of the Terrorism Act 2000 (TACT)

In compliance with part 3 of TACT, the SAR is a critical tool for reporting and combating suspicious activities related to terrorist financing, ensuring national security and regulatory compliance.

Reason

When Should Suspicious Activity Be Reported?

Companies must issue SAR when one of the following occurs:

Customers engaged in large cash transactions frequently may need to report, particularly if their activities don't seem to fit with their usual pattern.

James, the owner of a small company, usually uses computers to handle transactions for his retail business. But in the last month, he has started depositing large amounts of money many times per week. Since this sudden behavior shift varies from his typical transaction patterns, questions are raised.

Unusually quick transfers of money between accounts or between different financial institutions should raise red flags and be reported.

In a short amount of time, Emily, a freelance consultant, moves money quickly between her personal, professional, and offshore bank accounts. Since these transactions seem inappropriate and mysterious, worries regarding possible money laundering are raised by their speed and frequency. Transactions deliberately structured to avoid reporting thresholds, known as structuring or smurfing, should be reported.

Transactions that noticeably depart from the regular flow of the client's business without a clear justification could be viewed as suspicious.

Sarah runs a small bakery with a reputation for reliable and consistent sales. All of a sudden, she begins to receive sizable wire transfers that are identified as business payments but don't match her bakery's revenue trends. This peculiar behavior gives rise to possible criminal activity suspicions.

Customers using multiple accounts for seemingly unrelated transactions or for transactions that individually fall below reporting thresholds could be engaging in suspicious activity.

David, an individual with a history of questionable financial activities, uses multiple bank accounts to conduct transactions. He makes small deposits and withdrawals across these accounts, attempting to keep each transaction below the reporting threshold to evade detection.

A sudden and unexplained change in a customer's transaction patterns or behavior, such as a shift in the type or frequency of transactions, may raise suspicion.

Olivia, a long-time customer with a stable financial history, suddenly begins engaging in high-risk cryptocurrency transactions. This sudden change in transaction patterns, without a clear explanation, prompts the financial institution to investigate further.

Transactions involving high-risk products or services, such as those with a higher potential for money laundering, should be carefully monitored and reported if deemed suspicious.

Ethan, who has primarily engaged in domestic transactions, starts participating in transactions related to high-risk products like precious metals or cryptocurrency. This shift in behavior raises concerns about potential involvement in money laundering or other illicit activities.

Transactions involving shell companies or entities with no apparent business purpose may be indicative of attempts to conceal the true nature of the transactions.

Sophia sets up a shell company with no legitimate business activities. She uses this company to receive funds and make transactions, creating a complex structure that obscures the true nature of the transactions. This behavior raises suspicions about potential attempts to conceal illicit activities.

Transactions involving politically exposed persons, where there is a risk of corruption or bribery, may be considered high-risk and subject to reporting.

Marcus, a known government official, engages in financial transactions that seem unrelated to his official duties. This involvement raises concerns about the potential for corruption or bribery, given his status as a politically exposed person.

Customers who refuse to provide necessary information or provide false or misleading information during due diligence processes may be engaging in suspicious behavior.

Chloe, a new customer, refuses to provide required information during the due diligence process. This refusal creates uncertainty about the legitimacy of her financial activities, prompting the financial institution to view her transactions with heightened scrutiny.

Payments to third parties without a clear business rationale or legitimate purpose may raise suspicion and trigger reporting requirements.

Ryan regularly makes substantial payments to third-party entities with no apparent business relationship. The lack of a clear business rationale for these payments raises suspicions about potential involvement in money laundering or other financial crimes.

UK SAR reporting

SARs, are essential tools in the fight against financial crime in the UK, including money laundering and the funding of terrorism. When they have knowledge or suspicion of such actions, financial institutions and specific designated non-financial firms and professions are obligated to submit Suspensions and Reports (SARs) to the National Crime Agency (NCA).

When do the SAR should be submitted?

As soon as information is ëknownî or ësuspectedî that a person is engaged in money laundering

or dealing in criminal property, SAR must be submitted immediately.

Failure to Share Money Laundering Information:

Not telling authorities about money laundering, even when you know or suspect it, can lead to "failure to disclose" offenses. The duty to report arises when you become aware of such information through a disclosure made under specific sections of the Proceeds of Crime Act 2002 (POCA). These sections are:

Regulated Sector:

When individuals in the regulated sector possess knowledge or suspicion of money laundering, failure to disclose such information can result in offenses. The obligation to report arises under Section 330 of the Proceeds of Crime Act 2002 (POCA).

Non-Regulated Sector:

Similarly, individuals in the non-regulated sector must be aware of their obligation to disclose information related to money laundering. Failure to do so, despite having knowledge or suspicion, can lead to offenses under Sections 337 or 338 of POCA.

Tipping off

Tipping off, as defined by the Proceeds of Crime Act 2002, constitutes an offense in two scenarios:

- When a Suspicious Activity Report (SAR) has been filed, and its disclosure in a manner that could harm any subsequent investigation occurs.
- In situations where there is an ongoing or planned investigation into money laundering, and disclosing information likely to hinder that investigation takes place.

It's important to note that internal discussions within the organization do not qualify as tipping off.

Example:
Alex, a compliance officer at a financial institution, submits a Suspicious Activity Report (SAR) regarding a series of large transactions by a customer, indicating potential money laundering. The SAR includes details of the transactions and the customer involved.

However, contrary to legal obligations, Alex, concerned about potential consequences for the institution, discloses the specifics of the SAR to a colleague who is not part of the internal investigation team. This disclosure is made in a manner that could reach individuals outside the organization.

Offense:
Alex's action constitutes tipping off. By revealing the SAR details outside of the authorized channels, particularly to someone not involved in the investigation, there is a risk of prejudicing any subsequent inquiry or compromising the ongoing or contemplated money laundering investigation.

It's crucial for individuals in positions dealing with SARs to strictly adhere to confidentiality requirements and avoid any actions that might compromise the integrity of investigations.

Identification of suspicious activities:

Employees are trained to recognize unusual behavior that may indicate money laundering or terrorist financing e.g. by Transaction monitoring, CDD, Geographical risks, Unexplained source of wealth etc.

Other methods include:

Transaction Monitoring Systems:

Machine learning algorithms are used by advanced transaction monitoring tools to find patterns and outliers in real time. These systems can change and learn from new information, which makes them better at finding activities that seem fishy.

Data Analytics and Pattern Recognition:

Data analytics tools are used to look at big sets of data and find trends that might not be obvious if the data were looked at by hand. Finding complicated webs of transactions or connections is part of this.

Artificial Intelligence (AI) and Machine Learning (ML):

AI and ML technologies can keep getting better at spotting new patterns and trends that are linked to money laundering or funding terrorism. These methods can change to keep up with criminals' new tricks.

Risk-Based Approach:

A risk-based method is used by businesses, which look at the risk that comes with each customer and transaction. This means giving risk scores based on different factors and putting more resources into areas with bigger risks.

Regulatory Compliance Software:

Utilization of special software that helps make sure they follow changing AML and CTF rules. This program can help automate compliance tasks and keep up with changes to regulations.

How to Report Suspicious Activity (SAR)

Internal Reporting:

Recognizing Suspicious Activity

Employees are trained to spot clues of suspicious activity, especially those in positions involving risk management, compliance, or financial transactions.

Providing information to the Money Laundering Reporting Officer (MLRO):

The organization's Money Laundering Reporting Officer is notified of the detected suspicious behavior and the conclusions of the internal review (MLRO). The designated person in charge of managing AML and SAR-related operations inside the company is known as the MLRO.

Internal filing of a Suspicious Activity Report (SAR) to the Money Laundering Reporting Officer (MLRO)

Internal filing SAR to the Money Laundering Reporting Officer (MLRO) is a critical process within an organization's AML framework. Here's an overview of the steps involved:

Initial Assessment:

Upon detecting suspicious activity, the employ conducts an initial assessment to determine the validity and significance of the suspicion.

Gathering Information:

The employ gathers comprehensive information related to the suspicious activity, including transaction details, customer profiles, and any other relevant data.

Documentation:

All relevant information and findings are documented thoroughly. This documentation serves as a record of the MLRO's analysis and decision-making process.

Internal Reporting:

The employ prepares an internal report outlining the suspicious activity and the reasons for suspicion. This report is often submitted to the MLRO or a designated committee within the organization for further review.

Decision-Making:

Based on the MLRO assessment of the internal report which he has received from the employ, a decision is made on whether to proceed with filing a formal SAR with the relevant external authorities.

SAR Submission:

If the decision is to proceed, the MLRO prepares and submits the SAR to the NCA. The SAR includes all relevant details and supporting documentation.

Communication with Authorities:

The MLRO may engage in further communication with the authorities, providing additional information or cooperating with any follow-up inquiries.

Record-Keeping:

Maintain detailed records of the internal reporting process, including the initial detection, assessment, decision-making, and SAR submission. These records are crucial for audit trails and compliance purposes. If SAR is not made to NCA, MLRO need to document the valid justification of not reporting to the NCA.

How to submit a SAR to NCA?

To file a Suspicious Activity Report (SAR), utilize the NCA's online submission platform available on their website. Note that the existing SAR Online Portal is scheduled for replacement by the new SAR Portal, and updates on this transition will be communicated on the site.

Follow these steps to submit a SAR online:

ï Visit the NCA website and access the SAR submission portal.

ï Complete the required fields with relevant information about the suspicious activity, individuals involved, and any supporting documentation.

ï Upon successful submission, you will receive a confirmation email.

ï The NCA aims to process your report within approximately five to seven working days.

It's important to stay informed about any updates regarding the transition to the new SAR Portal, as the NCA may provide additional guidance or features.

Alternatively, if electronic submission is not feasible, the option to submit other types of SARs via post or fax is available.

For those specifically seeking a defense against money laundering (DAML), the NCA strongly recommends electronic submission. This ensures a streamlined process and facilitates more efficient communication for cases related to defense against money laundering.

Always check the NCA website for the latest information and updates related to SAR submission methods and platforms.

Basic Structure of a SAR to NCA:

When filling out a Suspicious Activity Report (SAR), it's important to include as much information as possible in various fields. Here's a step-by-step guide:

Customer Due Diligence (CDD): Include all available CDD information. Dates of birth are crucial for accurate identification.

Reason for Suspicion:

- Clearly explain why you're suspicious in simple English.
- Keep it concise, under 8,000 characters.
- Avoid acronyms and jargon.
- Use proper punctuation.

Additional Information:

- Populate all fields with relevant data, using 'UNKNOWN' if information is unavailable.
- Break down text into readable paragraphs.
- Provide a chronological sequence of events.

SAR Glossary Code:

- Start with a SAR glossary code.
- Briefly summarize suspicions.
- Add any useful information.
- Conclude with intended actions (e.g., exit relationship).

Examples of Text:

Use provided examples like "XXPROPXX" for property-related suspicions.

Individuals and Entities:

- Include identifying details like names, dates of birth, and addresses.
- Use 'UNKNOWN' where needed.
- For businesses, provide details like addresses and beneficial ownership.

Financial Transactions:

- If suspicion involves transactions, explain why they're suspicious.
- Include financial details and summarize cash amounts.

- Specify transaction types (e.g., online payment, cash).

Source Type Field:

Accurately classify your source type when submitting the SAR.

Previous SAR Reference:

If the subject was previously reported, include up to three SAR reference numbers.

Alerts and Keywords:

If an NCA Alert prompted the SAR, include the provided keyword.

No Attachments:

Do not send attachments with the SAR. Include all relevant information in the report.

Court Orders and Inquiries:

If served with a court order, review your activities related to the subject and file a SAR if needed.

By following these steps, you contribute to a clear, comprehensive, and effective SAR, aiding in the detection and prevention of illicit activities.

Defence against money laundering (DAML)

The DAML stands for defence against money laundering and refers to "appropriate consent" granted by the NCA to a firm, allowing it to engage in activities otherwise prohibited by the principal money laundering offenses under the Proceeds of Crime Act 2002 (POCA). To efficiently process your DAML, when submitting a Suspicious Activity Report (SAR), you need to explicitly express your intention to seek 'consent.'

A DAML serves to protect against committing principal money laundering offenses but does not provide immunity from tipping off offenses, civil liability claims, or other criminal acts, such as those under the Money Laundering Regulations 2017, Bribery Act 2010, or Fraud Act 2006.

Exemptions

- Exemptions under section 339A of POCA, effective from January 5, 2023, increased the threshold amount from £250 to £1,000. However, this exemption doesn't apply to actions like returning funds when terminating a customer relationship.

- An exemption under section 182 allows paying away funds under £1,000 when exiting a customer relationship, where suspicion of money laundering or criminal property exists.

- Under section 183, there is an exemption for mixed-property transactions, allowing reporters to ring-fence funds believed to be criminal property and transact with non-ring-fenced funds. Legal advice may be sought regarding responsibilities under this change to POCA 2002.

Making a DAML SAR

When making a DAML SAR, ensure you tick the consent box, use the appropriate glossary code, clearly identify the 'criminal property,' state reasons for suspicion, describe prohibited acts, and identify the involved parties.

After youíve made a DAML SAR

After submitting a DAML SAR, the NCA has seven working days to decide, starting the next working day after submission. If granted, you are not obliged to carry out the specified activities, and if refused, a 31-day moratorium begins, during which evidence is gathered for potential further action.

What Happens After You File a Suspicious Activity Report?

After the SAR is sent to the NCA through the dedicated channels specified by the UK Financial Intelligence Unit (UKFIU), following are the steps:

Law Enforcement Review:

The NCA reviews the SAR and assesses the information provided. This involves analyzing the nature of the suspicious activity and its potential connection to financial crime.

Investigation Initiation:

If deemed necessary, the NCA initiates an investigation into the reported suspicious activity. This may involve collaboration with other law enforcement agencies.

Information Gathering:

Law enforcement gathers additional information related to the reported activity. This may include conducting interviews, obtaining financial records, and seeking other relevant evidence.

Analysis and Decision:

Based on the findings, law enforcement conducts a detailed analysis to determine the legitimacy of the reported activity and whether it constitutes criminal behavior.

Communication with Reporting Institution:

The NCA may communicate with the reporting financial institution for additional details or clarification during the investigative process.

Further Action:

Depending on the outcome of the investigation, law enforcement may take further legal action, such as making arrests, freezing assets, or prosecuting individuals involved in illicit activities.

GDPR

What is GDPR?

GDPR stands for "General Data Protection Regulation,"

It is a set of rules about privacy and data security in the European Union since May 2018. These rules are like a guide for the organizations to handle the personal information of the people. On the other hand, it gives people more control over their own data.

It's basically about respecting people's privacy and keeping things transparent.

People, called "***data subjects,*** "have rights like checking, changing, or deleting their data. They also have the right to know how their data is used. Businesses have to follow these rules and be clear and lawful when dealing with personal data.

PART 2 General processing

Lawfulness of processing

The GDPR says it's fine to use personal information if it's necessary for important public tasks or the controller's official duties. This covers stuff like making sure justice is done, Parliament doing its job, following laws, government responsibilities, or supporting democracy. Basically, the law says it's okay to use personal data for these crucial things.

Special categories of personal data

The law provides guidelines on dealing with special personal data and information about criminal activities.

Despite a general prohibition, there are certain situations where it's allowed to use this data.

These exceptions involve things like work information, public interest, health care, public health, and specific activities such as archiving or research.

In simpler terms, the law outlines when and how special personal data and details about crimes can be used, considering factors like work, public well-being, and specific activities.

Rights of the Subject (Customer)

Overview and Scope:

Depending on the outcome of the investigation, law enforcement may take further legal action, such as making arrests, freezing assets, or prosecuting individuals involved in illicit activities.

GDPR

What is GDPR?

GDPR stands for "General Data Protection Regulation,"

It is a set of rules about privacy and data security in the European Union since May 2018. These rules are like a guide for the organizations to handle the personal information of the people. On the other hand, it gives people more control over their own data.

It's basically about respecting people's privacy and keeping things transparent.

People, called "***data subjects,*** "have rights like checking, changing, or deleting their data. They also have the right to know how their data is used. Businesses have to follow these rules and be clear and lawful when dealing with personal data.

PART 2 General processing

Lawfulness of processing

The GDPR says it's fine to use personal information if it's necessary for important public tasks or the controller's official duties. This covers stuff like making sure justice is done, Parliament doing its job, following laws, government responsibilities, or supporting democracy. Basically, the law says it's okay to use personal data for these crucial things.

Special categories of personal data

The law provides guidelines on dealing with special personal data and information about criminal activities.

Despite a general prohibition, there are certain situations where it's allowed to use this data.

These exceptions involve things like work information, public interest, health care, public health, and specific activities such as archiving or research.

In simpler terms, the law outlines when and how special personal data and details about crimes can be used, considering factors like work, public well-being, and specific activities.

Rights of the Subject (Customer)

Overview and Scope:

Depending on the outcome of the investigation, law enforcement may take further legal action, such as making arrests, freezing assets, or prosecuting individuals involved in illicit activities.

GDPR

What is GDPR?

GDPR stands for "General Data Protection Regulation,"

It is a set of rules about privacy and data security in the European Union since May 2018. These rules are like a guide for the organizations to handle the personal information of the people. On the other hand, it gives people more control over their own data.

It's basically about respecting people's privacy and keeping things transparent.

People, called "***data subjects,*** "have rights like checking, changing, or deleting their data. They also have the right to know how their data is used. Businesses have to follow these rules and be clear and lawful when dealing with personal data.

PART 2 General processing

Lawfulness of processing

The GDPR says it's fine to use personal information if it's necessary for important public tasks or the controller's official duties. This covers stuff like making sure justice is done, Parliament doing its job, following laws, government responsibilities, or supporting democracy. Basically, the law says it's okay to use personal data for these crucial things.

Special categories of personal data

The law provides guidelines on dealing with special personal data and information about criminal activities.

Despite a general prohibition, there are certain situations where it's allowed to use this data.

These exceptions involve things like work information, public interest, health care, public health, and specific activities such as archiving or research.

In simpler terms, the law outlines when and how special personal data and details about crimes can be used, considering factors like work, public well-being, and specific activities.

Rights of the Subject (Customer)

Overview and Scope:

The GDPR grants individuals several rights regarding their personal data. Individuals have the right to know how their personal data is being used by organizations. This includes understanding the purposes for which their data is processed, the categories of data being processed, who it's shared with, and how long it will be retained etc.

Controller's General Duties:

Controllers are the entities or organizations that determine the purposes and means of processing personal data.

They have the responsibility to provide individuals with information that is easy to understand and readily available.

This information should cover various aspects of data processing, including the purposes of processing, the categories of personal data involved, the recipients or categories of recipients to whom the data may be disclosed, and any transfers of data to third countries or international organizations.

Right of Access by the Data Subject (Customer):

- This means that individuals have the right to request and obtain a copy of their personal data held by organizations or controllers.
- It allows individuals to know what personal data is being processed about them and how it's being used.
- Individuals can check if the processing of their personal data is being done lawfully, according to data protection regulations like the GDPR.

In simpler terms, this right enables people to see what information organizations have about them and confirm if it's being handled properly and legally.

Let's say Sarah is a customer of a financial Institution, and she wants to know what personal data the financial Institution holds about her. She exercises her right of access by submitting a request to the financial Institution asking for a copy of her personal data.

The financial Institution acknowledges Sarah's request and provides her with a document containing details such as her account information, transaction history, loan or mortgage details, and any other personal data the financial Institution holds about her.

Sarah reviews the information provided by the **bank** to ensure its accuracy and completeness. She checks if the financial Institution is processing her personal data lawfully and if there are any discrepancies or concerns.

Right to Rectification:

- This right allows individuals to request corrections to any personal data that is incorrect or incomplete.
- It ensures that the information held about individuals is accurate and reflects their current situation.
- Data subjects can request changes to their personal data by contacting the organization or controller responsible for handling their information.

John, a bank customer, notices that his address listed on his bank account statement is incorrect. He recently moved to a new apartment, and he wants to ensure that his address is updated accurately in the bank's records. Here's how John might exercise his right to rectification:

- John logs into his online banking account and navigates to the "Account Settings" or "Profile Information" section.
- He notices that his old address is still listed as the primary address on file. John realizes that this information needs to be updated to reflect his current address.
- John finds an option to update his address and clicks on it. He enters his new address details, including the street name, apartment number, city, and postal code.
- After submitting the updated information, John receives a confirmation message indicating that his request for address change has been received.
- The bank processes John's request and updates his address in their system. They send him a notification confirming the successful update of his personal data.
- John reviews his next bank statement and verifies that his new address is accurately reflected on the document.

Right to Erasure or Restriction of Processing:

- This right allows individuals to request the deletion or removal of their personal data from an organization's records.
- Individuals can also request the restriction of processing of their personal data under certain circumstances, which means the organization can continue to store the data but cannot use it for processing purposes.
- This provides individuals with control over their information, allowing them to decide when and how their personal data is used by organizations.

John, a bank customer, decides to close his savings account. He contacts the bank and requests that they delete his account information from their records. The bank promptly

removes John's account details, ensuring that his personal data is no longer stored in their system. In this case, John exercised his right to erasure by requesting the deletion of his personal data (his account information) from the bank's records.

Right to object to processing

People can ask companies to stop using their personal data if they believe it's causing problems. Companies might ask for more details to confirm the request. Within 21 days, the company must reply, agreeing or explaining why they can't fully agree. If not happy with the response, people can ask a court to make the company comply. Courts can handle these requests.

Let's say you don't want a company to use your personal information anymore, like your email address. You tell them to stop using it, but they ask for more details to be sure it's really you. After you give them the extra information, they have three weeks to either stop using your email or explain why they can't. If you're still not happy, you can ask a court to make them stop.

Right to information

The right to information includes:

Knowing the identity and contact details of the company.

Understanding the reasons for using your data and the legal basis for it.

Being informed about the types of data being processed.

Knowing who else might have access to your data.

Understanding how to file a complaint if you're dissatisfied.

Knowing how to exercise your rights under these regulations.

Any other important details about how your data is being used.

Imagine you're signing up for a new app:

They should tell you who they are and why they're using your info.
They'll explain what kind of info they'll use and who else might see it.
You'll learn how to complain if you're not happy and how to use your rights.
They can put this info in their app or website where everyone can find it.

Right to information about decision-making

If a company uses your data to make decisions about you, you have the right to know why. Just ask, and they should tell you. They have to do it quickly.

If a financial institution uses an automated system to decide whether to approve your loan application, you can ask the bank to explain why they made that decision. They have to tell you promptly.

Right to intervene in automated decision-making

When a company makes a big decision about you using only computer data, they have to inform you, unless it's based on your consent or involves a contract. If the decision has legal implications for you, they must notify you promptly. Within a month, you can ask them to review or make a new decision. They must consider your request and respond within that same month. This right ensures that decisions impacting you aren't solely determined by automated systems, protecting against potential biases or errors.

Right Not to be Subject to Automated Decision-Making:

- This right allows individuals to avoid decisions that are made solely by automated systems without any human intervention.
- It safeguards individuals from potentially negative impacts that could arise from automated decisions, such as biases or errors in the algorithms used.

Sarah applies for a loan from a bank. Instead of her application being reviewed by a human loan officer, the bank's system automatically assesses her application using an algorithm. Sarah exercises her right not to be subject to automated decision-making by requesting that her loan application be reviewed by a human instead. As a result, the bank assigns a loan officer to manually review Sarah's application, ensuring that her application receives fair and personalized consideration.

Part 3: Six Principles of Law enforcement and Intelligence services processing

First data security principle:

The first data security principle states that the processing of information must be legal and fair.

Legal Processing means that:

Get permission from the person whose data it is.

Use it for a job that a law enforcement and intelligence services authority is carrying out.

There is one other situation called *¡Sensitive Processingî*

Sensitive processing, which involves sharing some personal information, is allowed with the data subject's permission and a suitable policy document, or if strictly necessary.

Sensitive processing includes data

- Where someone comes from
- Thoughts and views
- Health information
- Genetic or biometric data
- Some personal details

Example:

Legal Processing:
Let's say there's a missing person case, and the police need to gather information to locate the individual. They may need access to the missing person's phone records to track their last known location. However, accessing someone's phone records involves personal data, so they must follow legal procedures.

Sensitive Processing:
Sensitive processing could also include asking someone where they come from or what their thoughts and views are. For example, if a survey asks people about their political beliefs or their ethnicity, this would be considered sensitive processing, and it can only be done if people give their permission or if it's strictly necessary for a specific purpose.

Second data security principle:

The second data security principle says that:

- Any personal information gathered by law enforcement and intelligence services must be used for a clear, authorized reason
- And it should not be changed in a way that goes against that reason.

However there exists some exceptions such as the data can be used for another law enforcement and intelligence services purpose if it is legal, necessary, and fair to do so. Processing for a non-law enforcement reason, on the other hand, needs clear legal permission.

Let's say a police department collects personal information about a suspect during an investigation into a robbery:

Clear, Authorized Reason:

The police can use the gathered information to investigate the robbery, such as analyzing the suspect's phone records and financial transactions related to the crime.
No Unauthorized Changes:

They cannot use this information to investigate unrelated crimes or share it with third parties for marketing purposes.
Exceptions:

However, if during the robbery investigation, they discover evidence of another serious crime, like terrorism, they can use the gathered data for that additional law enforcement purpose.

If they want to use the data for non-law enforcement reasons, such as marketing, they need clear legal permission from the individuals involved.

Third data security principle:

The third data protection principle emphasizes that

- When using personal information, only the necessary and relevant data should be usedónothing more.

- In simpler terms, only the information directly needed for the task at hand should be collected and used, avoiding unnecessary or excessive details.
  For Example:

Let's say the police are investigating a case of a stolen bicycle:

Only Necessary and Relevant Data:

The police would focus on collecting information directly related to the theft, such as the description of the stolen bike, the time and location of the theft, and any eyewitness accounts.
Avoid Unnecessary Details:

They wouldn't need to gather information about the bicycle owner's medical history, employment records, or personal relationships, as these details are not relevant to solving the theft case.

Fourth data security principle:

The fourth data security principle for says that:

- Personal data must be correct and kept up to date, and mistakes should be quickly erased or fixed. It stresses the difference between facts and personal opinions.

  Imagine a police department maintains a database of individuals involved in a criminal investigation:

  The police ensure that the personal data of suspects, prisoners, victims, and witnesses are accurate and regularly updated. For instance, if a suspect changes their address or phone number, this information is promptly updated in the database.

- There should be clear differences between types of data subjects, such as suspects, prisoners, possible victims, and witnesses.

  The database categorizes individuals based on their roles in the investigation, such as suspects, prisoners, victims, and witnesses. This helps in managing and organizing the data effectively.

- Measures must be taken to stop the transmission of wrong or out-of-date information, making sure that it is checked before being shared, including all necessary information, and letting receivers know if mistakes are found after the transmission.

  Before sharing any information from the database with other law enforcement agencies or relevant parties, the police double-check the accuracy of the data. If any mistakes are discovered after transmission, they promptly inform the recipients and rectify the errors.

Fifth data security principle:

The fifth data protection principle says that:

- Any personal information that is processed for law enforcement and intelligence services purposes should only be kept for as long as it is needed for that reason.

  A police department maintains records of individuals involved in past criminal investigations:

  According to the fifth principle, personal information gathered for law enforcement purposes should only be kept for as long as it's necessary for those reasons. For instance, if a suspect is acquitted of a crime, their personal information should not be retained indefinitely but should be deleted after a certain period.

- At regular intervals, the need to keep personal information for law enforcement and intelligence services reasons must be checked to make sure it's still pertinent.

The police conduct regular reviews to assess the continued need for retaining personal information. For example, if a case is closed, and there are no pending legal proceedings or investigative needs associated with a particular individual, their personal information should be reviewed and deleted if it's no longer relevant.

Sixth data security principle:

The sixth data protection principle says that:

Keeping Data Safe:

When law enforcement and intelligence services use personal data, it must be handled in a way that ensures its safety. This involves using the right technical or organizational measures to protect the data from unauthorized use or any accidental loss, destruction, or damage.

Consider a law enforcement agency that stores personal data of individuals involved in ongoing investigations: The agency implements strict access controls to ensure that only authorized personnel can access the stored data. This may involve using password protection, encryption, or biometric authentication to prevent unauthorized access.

Appropriate Security Measures:

"Appropriate security" means employing the right methods to keep the data secure. This includes preventing unauthorized access or use of the information and taking measures to avoid accidental mishaps, such as data loss or damage.

The agency establishs protocols to ensure that personal data is only accessed for legitimate law enforcement purposes. For instance, personnel may be required to provide justifications for accessing specific data, and audit logs may be maintained to track all accesses. The agency regularly backs up the stored data to prevent loss in case of hardware failures or other unforeseen incidents. Additionally, they implement measures such as firewalls, antivirus software, and data encryption to safeguard against cyber threats and accidental data breaches.

CHAPTER 4 Controller and processor

General obligations of Controller

This chapter lays out the rules for controllers and processors dealing with personal data for law enforcement purposes.

Every controller must employ appropriate technical and organizational methods to ensure that personal data processing complies with the rules. If deemed suitable for the processing, controllers should also have data protection policies in place. These methods must be regularly reviewed and updated as necessary.

Joint controllers

When two or more authorities work together to decide how personal data should be used, they become joint controllers. These joint controllers must work transparently to figure out who's responsible for following the rules. They need to make an agreement unless their responsibilities are already set by law. This agreement should specify which controller will be the main contact for individuals about their data.

John works at financial institution A, and Sarah works at B. They're collaborating on a new financial service that requires sharing customer data between their financial institutions. John and Sarah become joint controllers. They sit down together and agree that financial institution A will handle data protection responsibilities. They make sure to inform their customers about this arrangement. For example, if they're launching a joint service, they'll let customers know that they can contact financial institution A if they have any questions or concerns about their personal data.

Processors

Processor is the person hired by a controller to handle personal data on their behalf.

The processor can't involve another processor (sub-processor) without the controller's written permission.

The controller and processor must have a written contract that covers:

a) What data will be processed and for how long,

b) Why the data is being processed,

c) What kind of data and who it's about,

d) The responsibilities and rights of both parties.

The contract must state that the processor can only transfer data to another country if the controller says so.

In a financial institution, Sarah (the Controller) hires Mark (the Processor) to handle customer data for a new financial institution app. They sign a contract stating:

What data (customer account info) will be used and why (to manage transactions).
Mark must keep data confidential, follow Sarah's instructions, and help with data protection.
When the app ends, Mark returns or deletes the data as Sarah says.
Mark can't involve others without Sarah's permission.
Mark can only transfer data abroad if Sarah agrees.

Obligations relating to security: Security of processing

Each controller and processor must use suitable technical and organizational methods to ensure that personal data is secure. For automated processing, they should assess risks and put measures in place to:

- Stop unauthorized access or tampering with systems.
- Keep a record of all processing activities.
- Ensure systems work properly and can be restored if they stop working.
- Prevent data corruption if systems malfunction.

In a financial institution, Sarah (the Manager) and Mark (the IT Specialist) ensure customer data security:

They use strong security software to block unauthorized access.
Mark keeps a log of all data activities for tracking.
Regular system checks are done to ensure proper functioning.
Backup systems are set up to prevent data loss during malfunctions.

Obligations relating to personal data breaches

Notification of a personal data breach to the Commissioner

If a controller discovers a personal data breach, they must tell the Commissioner about it:

- As soon as possible, and ideally within 72 hours.
- Unless the breach is unlikely to harm individuals' rights and freedoms.
- If they can't notify within 72 hours, they must explain why.

The notification must include:

What data was breached, how many people are affected, and what kind of data it is.

Communication of a personal data breach to the data subject

When a personal data breach is likely to harm individuals' rights and freedoms, the controller must tell the data subjects about the breach quickly.

The notification must include:

- What happened in the breach.
- Contact details for more information.
- Possible consequences of the breach.
- Actions being taken to fix it.

The duty to inform doesn't apply if:

- The controller already had good protection measures in place.
- They've taken steps to reduce the risk.
- Informing would be too hard.

For instance, if the data was encrypted, making it unreadable to unauthorized people.

Data protection officers

Designation of a data protection officer

The controller must appoint a data protection officer, except if the controller is a court or judicial authority.

When choosing a data protection officer, the controller should consider their expertise in data protection law.

It's possible for one person to be appointed as the data protection officer for multiple controllers, depending on their organizational structure and size.

The controller must make the contact details of the data protection officer public and inform the Commissioner about them.

Position of data protection officer

The controller must make sure that the data protection officer is involved in all matters concerning personal data protection and has the resources and access needed to do their job effectively.

The data protection officer should not receive instructions on how to perform their duties, should avoid conflicts of interest, and cannot be punished for doing their job.

Data subjects can contact the data protection officer regarding their personal data or rights under this Part. The data protection officer reports to the top management of the controller.

Tasks of data protection officer

The controller must assign the data protection officer the following tasks:

- Informing and advising the controller, processors, and employees about their obligations
- Providing advice on data protection impact assessments and ensuring compliance.
- Cooperating with the Commissioner.
- Acting as the point of contact for the Commissioner regarding processing issues and consultations.
- Monitoring compliance with the controller's data protection policies.
- In relation to the policies mentioned above, the data protection officer's tasks include assigning responsibilities, raising awareness, training staff, and conducting audits as needed.
- When performing these tasks, the data protection officer must consider the risks associated with processing operations.

CHAPTER 5 Transfers of personal data to third countries etc

General principles for transfers of personal data

General Prohibition: Controllers cannot transfer personal data unless certain conditions are met.

Conditions for Transfer:

Condition 1: Transfer is necessary for law enforcement purposes.

Condition 2: Transfer is based on one of the following:

- An adequacy decision.
- Appropriate safeguards.
- Special circumstances.

Condition 3: The intended recipient is a relevant authority in a third country or an international organization.

Authorization Requirement: If the personal data was originally received from a member State other than the United Kingdom, authorization from that member State is required unless:

- The transfer is necessary to prevent an immediate and serious threat to public security or essential interests, and authorization cannot be obtained in time.
- If transfer occurs without authorization, the relevant authority in the member State must be promptly informed.No Transfer Without Permission:
- You can't send personal data to another country or international organization without permission.

Conditions for Permission:

Need for Law Enforcement: You can transfer data if it's necessary for law enforcement.

Approval Required: If you got the data from another EU country, you need their approval, unless it's urgent to prevent a big problem.

Exceptions:

Urgent Threats: If there's an immediate and serious threat to public security or a country's essential interests, and you can't get permission in time, you can still transfer data.

Inform if No Permission: If you transfer data without permission, you need to tell the authority who would've given permission.

Transfers on the basis of special circumstances

Necessary Transfers: Personal data can be transferred to another country or organization in special situations when it's necessary:

- to protect someone's life or health,
- to safeguard the legitimate interests of the person the data is about,
- to prevent a serious threat to public security,
- for specific law enforcement purposes, or
- for a legal reason.

Exceptions: However, transfers for law enforcement purposes or legal reasons don't apply if the controller decides that the rights of the person whose data is being transferred are more important than the public interest.

Documentation Requirements:

- Every transfer must be recorded.
- The records should be shared with the data protection authority upon request.
- Details like when the transfer happened, who received the data, why it was transferred, and what kind of data was transferred must be included.

Legal Purposes Defined: Transfers for a legal reason could be:

- Needed for ongoing or future legal proceedings related to law enforcement.

- Required for seeking legal advice concerning law enforcement matters.
- Necessary for establishing, exercising, or defending legal rights concerning law enforcement purposes.

Transfers to particular recipients

Transfers of personal data to persons other than relevant authorities

It there is a need to the transfers of personal data to individuals or entities other than relevant authorities there are four extra conditions for these transfers.

Condition 1: The transfer must be absolutely necessary for a specific task required by law for law enforcement purposes.

Condition 2: The controller (the person or organization transferring the data) must ensure that no fundamental rights or freedoms of the person whose data is being transferred override the public interest in the transfer.

Condition 3: The controller believes that transferring the data to a relevant authority in another country wouldn't work well or would be inappropriate. For example, if it couldn't be done in time to serve its purpose.

Condition 4: The controller must tell the recipient exactly why the data is being transferred and how it can be used.

Informing Relevant Authorities: The controller must quickly tell a relevant authority in the other country about the transfer unless it's not possible or appropriate.

Documentation and Reporting:

- The controller must keep records of these transfers.
- They also need to inform the data protection authority about the transfer.

Subsequent transfers

Condition of Transfer: When personal data is transferred according to certain rules, the original controller must insist that it's not passed on to another country or organization without their or another competent authority's permission.

Permission for Further Transfer: Another authority can only allow this further transfer if it's needed for law enforcement purposes.

Considerations for Permission: When deciding on this permission, the authority must think about:

- How serious the situation is that's prompting the request.
- The original reason why the data was transferred.

- The data protection standards in the country or organization where the data will be sent.

Authorization from Member States: If the data was initially received from another EU country, that country must also approve the further transfer unless it's urgently needed to prevent a serious threat.

Exception: If there's an urgent threat to public security or a country's essential interests and permission can't be obtained quickly, authorization isn't needed initially.

Informing Member State Authority: If a transfer happens without the required authorization, the authority in the original EU country must be informed promptly.

Enforcement

The enforcement of the General Data Protection Regulation (GDPR) is crucial for ensuring the protection of individuals' personal data. Here's an overview of the enforcement mechanisms.

Information Notices

Authorities have the right to request information from organizations (data controllers and processors) regarding their data processing activities.

If false information is provided in response to these notices, penalties can be imposed.

Assessment Notices:

These notices are issued by authorities to assess whether organizations are complying with the GDPR regulations.

There are restrictions on how and when these assessment notices can be used to ensure they are not abused by authorities.

Enforcement Notices:

Authorities can issue enforcement notices to organizations that are not complying with GDPR requirements.

These notices typically require organizations to take specific actions, such as rectifying or deleting personal data that is being processed unlawfully.

Powers of Entry and Inspection:

Authorities have the power to enter premises and inspect records to ensure compliance with GDPR regulations.

This allows them to verify whether organizations are handling personal data appropriately.

Penalties:

Fines are imposed on organizations that breach GDPR rules, with maximum penalty amounts and fixed penalties set.

Guidance is provided to ensure consistent application of penalties and enforcement actions across different cases.

Appeals and Complaints:

Individuals have the right to appeal against enforcement actions taken by authorities if they believe there has been an error or unfair treatment.

Additionally, individuals can file complaints about data protection breaches, and there are procedures in place to investigate and address these complaints.

Court Remedies:

Courts can issue orders requiring organizations to comply with GDPR regulations and provide compensation to individuals affected by data breaches.

Specific penalties for breaking data protection laws are outlined, providing clarity on the consequences of non-compliance.

CHAPTER 3 Other general processing

Exemptions

There are exceptions to the General Data Protection Regulation (GDPR) in the Data Protection Act 2018. These are for situations where the normal GDPR rules might not apply. What these exemptions mean and some examples of them are given below:

Manual Unstructured Data Held by FOI Public Authorities:

This exemption specifically applies to personal information that is stored in manual (non-digital) form by public authorities subject to Freedom of Information (FOI) regulations.

If this data is not organized in a structured manner, meaning it's not neatly arranged or categorized, then there are exceptions to the usual rule of making such information available under FOI regulations.

In simpler terms, if a public organization has certain personal data in paper files and it's not well-organized, they might not have to share it under FOI regulations.

For Example:

Imagine a government office keeping paper records of citizen complaints in a big box without any particular order. If they're doing this and it's part of their Freedom of Information (FOI) responsibilities, they might not have to share those specific files if someone requests them. This is because the data isn't neatly organized, and there are exceptions in FOI rules for such situations.

Manual Unstructured Data Used in Longstanding Historical Research:

This exemption applies to personal data kept manually and in an unorganized manner for the purpose of longstanding historical research. In simpler terms, if certain information is in paper files and not well-organized, but it's being used for long-term historical research, there are exceptions to the usual rules about sharing this data.

For example: Imagine a museum storing old letters and documents about people from the past in a box without sorting them. If they're doing this for long-term historical research, there are exceptions to the usual rules about how they have to share that information. Which means that for certain kinds of historical study, flexibility is allowed to ensure that the valuable historical data is preserved and used appropriately. This helps balance the need for privacy with the importance of historical research.

National Security and Defense Exemption:

This exemption gives some flexibility when handling personal data related to national security and defense matters. In other words, there are special rules that allow certain freedom in how this kind of sensitive information is processed to ensure the safety and security of the nation.

For Example:

Consider a military organization maintaining records of personnel assignments, security clearances, and operational details. If these records contain personal data and are crucial for national security, the National Security and Defense Exemption allows the organization flexibility in processing this information without strict adherence to certain data protection rules, ensuring the safety and defense of the country.

National Security Certificate:

This section permits the issuance of a certificate to protect specific data processing activities concerning national security. In simpler terms, it allows authorities to provide official certification to safeguard certain information processing related to keeping the nation secure.

For Example:

Imagine a scenario where the government needs to process sensitive information for national security reasons. This section allows them to issue a special certificate, like an official document, stating that the data processing activities they're doing are necessary for national security. It's a way to officially authorize and safeguard these activities to ensure the country's safety.

National Security and Defence:

This exemption provides the flexibility to adjust certain rules in the GDPR related to handling sensitive personal data and security measures when it comes to national security and defense.

These adjustments are made to address special situations, aiming to find a balance between protecting personal data and meeting the requirements of national security, historical research, and Freedom of Information regulations. In simpler terms, it allows some changes in data protection rules to ensure both privacy and the important needs of national security and related areas are met.

For Example:

This exemption provides the flexibility to adjust certain rules in the GDPR related to handling sensitive personal data and security measures when it comes to national security and defense. These adjustments are made to address special situations, aiming to find a balance between protecting personal data and meeting the requirements of national security, historical research, and Freedom of Information regulations. In simpler terms, it allows some changes in data protection rules to ensure both privacy and the important needs of national security and related areas are met.

Thank You