Comparison Chart: Third AML Directive vs. Fourth AML Directive

Category	3rd AML Directive	4th AML Directive
Risk-Based Approach	Consider geography, customer, product and channel as part of the risk-based approach in establishing a compliance program.	Consider geography, customer, product and channel as part of the risk-based approach in establishing a compliance program. Include nationwide AML risk assessments conducted by individual EU Member States.
	"Third-country equivalent" (white list) AML systems to the EU permitted a "refutable presumption" of the application of simplified CDD in those jurisdictions.[1]	No white-listed jurisdictions.
	Customers that are financial institutions located in the EU/EEA, or in a third country which imposes equivalent AML requirements (see above) may be subject to Simplified Due Diligence requirements.	Financial institutions must determine the level of AML risk posed by a customer prior to applying the SDD status to such customer and provide justification for such qualification.
	CDD records must be retained for 5 years.	CDD records must be retained for 5 years. Any information relating to an "identified or identifiable natural person" must be deleted, unless provided for by national law. Further retention may only be granted if necessary for prevention, detection or investigation of money laundering or terrorist financing, with maximum retention of up to 10 years from the end of the business relationship with the affected customer.

Ownership and Management	Identify and conduct CDD on any beneficial owner that controls more than 25% of the shares or voting rights of a customer.	Identify and conduct CDD on any beneficial owner that controls more than 25% of the shares or voting rights of a customer. Information on beneficial owners must be submitted to a central register in each Member State.
	Issuance of bearer shares by companies permitted.	Issuance of bearer shares by companies is not permitted. Current bearer shareholders will be permitted a 9-month period to exchange their bearer shares for registered shares.
	Senior management = members of the Board of Directors of the financial institution.	Senior management = an officer or employee with specific knowledge of the institution's exposure to money laundering or terrorist financing risk and sufficient seniority to make decisions affecting its risk exposure.
Tax Crimes	N/A	Tax crimes (in the broadest definition permitted under individual Member States' laws) will be a predicate AML offense.

PEPs	Politically Exposed Persons (PEPs) = natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.	PEP = a natural person who is or who has been entrusted with prominent public functions and includes the following: (a) heads of State, heads of government, ministers and deputy or assistant ministers; (b) members of parliament or of similar legislative bodies; (c) members of the governing bodies of political parties; (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; (e) members of courts of auditors or of the boards of central banks; (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; (g) members of the administrative, management or supervisory bodies of State-owned enterprises; (h) directors, deputy directors and members of the board or equivalent function of an international organization. No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials.
	Transactions and/or relationships with PEPs, financial institutions must: (a) have appropriate risk-based procedures to determine	Transactions and/or relationships with PEPs, financial institutions must: (a) have in place appropriate risk management systems,

	whether the customer is a politically exposed person; (b) have senior management approval for establishing business relationships with such customers; (c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction; (d) conduct enhanced ongoing monitoring of the business relationship.	including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person; (b) apply the following measures in cases of business relationships with politically exposed persons: (i) obtain senior management approval for establishing or continuing business relationships with such persons; (ii) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons; (iii) conduct enhanced, ongoing monitoring of those business relationships.
	N/A	Where a PEP is no longer entrusted with a prominent public function, financial institutions must consider the continuing risk posed by affiliation with such PEP for at least 12 months (or longer, until the financial institution determines that the risk specific to such PEP has diminished).

Policies and Procedures	Disclosure of information should be in accordance with the rules on transfer of personal data to third countries as laid down in Directive 95/46/EC of the European Parliament. Information exchanged between financial institutions in connection with AML or CTF investigations shall be used exclusively for the purposes of the prevention of money laundering and terrorist financing.	The Fourth AML Directive "is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including Council Framework Decision." Member States shall ensure that the sharing of information within the group is allowed. Information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group. FIUs cooperate in the application of state-of-the-art technologies in accordance with their national law. Those technologies shall allow FIUs to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds.
	Where EU-based financial institutions have branches and subsidiaries located in third countries where the legislation in this area is deficient, they should, in order to avoid the application of very different standards within an institution or group of institutions, apply the Community standard or notify the competent authorities of the home Member State if this application is impossible.	Financial institutions that are part of a group must implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes. Financial institutions that have branches or majority-owned subsidiaries located in third countries where the minimum AML/CFT requirements are less strict than those of the home Member State, must have these branches and majority-owned subsidiaries located in the third country implement the requirements of the home Member State, including data protection, to the extent that

		the third country's law so allows. Where a third country's law does not permit implementation of the policies and procedures required above, financial institutions must ensure that branches and majority-owned subsidiaries in that third country apply additional measures to effectively handle the risk of money laundering or terrorist financing, and inform the competent authorities of their home Member State. If the additional measures are not sufficient, the competent authorities of the home Member State shall exercise additional supervisory actions, including requiring that the group does not establish or that it terminates business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the third country.

Penalties	Member States should ensure that appropriate administrative measures or penalties could be imposed on financial institutions in a manner that would be "effective, proportionate and dissuasive." For natural persons sanctions could be adjusted "in line with the activity carried out" by that person.	For serious, repeated and/or systematic failures in the areas of CDD, suspicious transaction reporting, record keeping and internal controls, minimum penalties may include:· public reprimand · cease and desist orders · suspension of authorization · temporary ban from managerial functions, and · maximum pecuniary sanctions of at least €5M or 10% of the total annual turnover (and at least €5M for a natural person). For non-financial institutions, penalties can amount to twice the amount of the benefit derived from the breach, or at least €1M.
Cash Payments for Merchants	Persons trading in goods must report cash payments of €15,000 or more, either as one or multiple related transactions.	Persons trading in goods must report cash payments of €10,000 or more, either as one or multiple related transactions.