Deloitte.

ALTERNATIVE
INVESTMENTS

REGULATORY

INVESTMENT
FUNDS

RISK & ASSET
MANAGEMENT

BANKING

SUSTAINABILITY

TECHNOLOGIES
INNOVATION

AML/CTF and Due Diligence on Counterparties:
How can technology help with current market challenges?

Link'n Learn 2024/2025 – 08/01/2025

Getting Started

Here with you today

Floriane Lecoq
Senior Manager
+352 621568493
flecoq@deloitte.lu

Kevin Pericart
Manager
+352 621714383
kpericart@deloitte.lu

Agenda

1   Set the scene – Market challenges
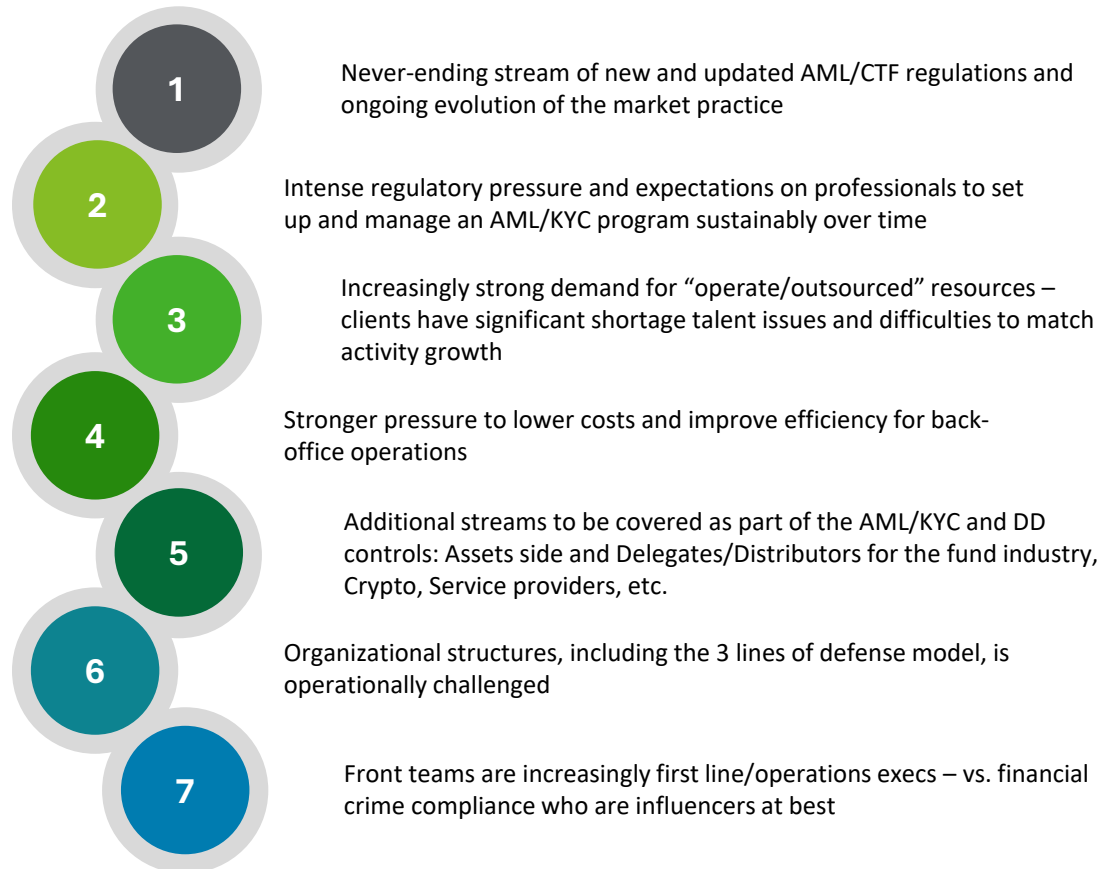
2   How can the technology help?

3   Leveraging Tech for current Hot topics

Set the scene

Market challenges on AML/CTF and Due Diligence on Counterparties
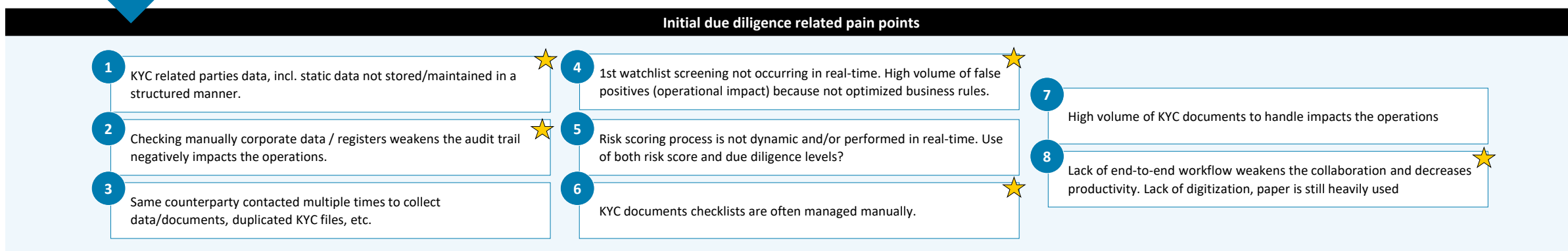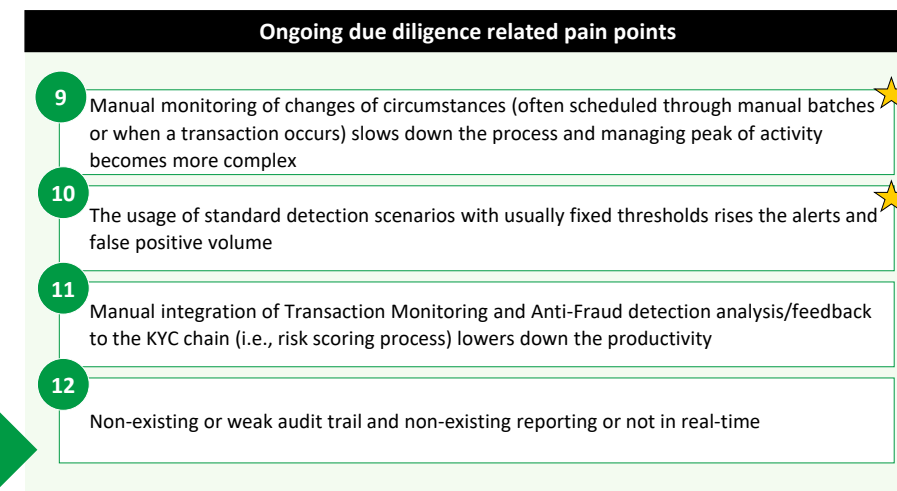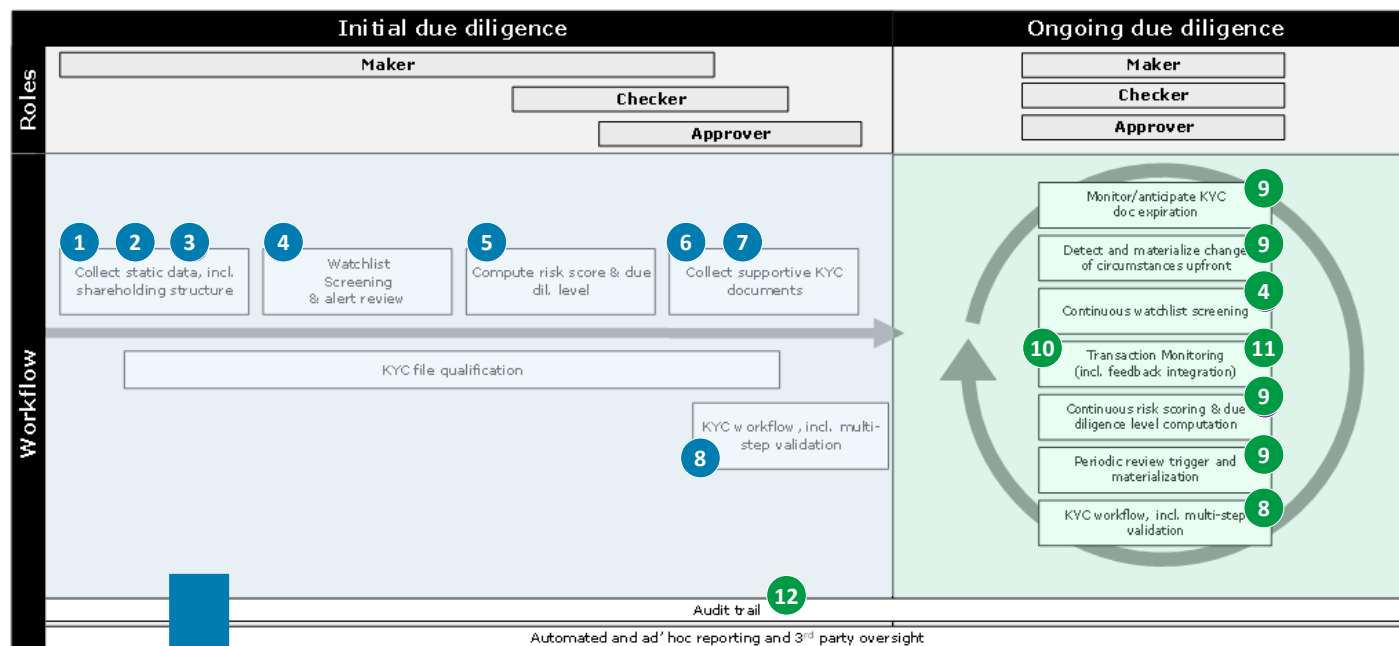
Set the scene
Current market challenges

1 Never-ending stream of new and updated AML/CTF regulations and ongoing evolution of the market practice

2 Intense regulatory pressure and expectations on professionals to set up and manage an AML/KYC program sustainably over time

3 Increasingly strong demand for "operate/outsourced" resources – clients have significant shortage talent issues and difficulties to match activity growth

4 Stronger pressure to lower costs and improve efficiency for back-office operations

5 Additional streams to be covered as part of the AML/KYC and DD controls: Assets side and Delegates/Distributors for the fund industry, Crypto, Service providers, etc.

6 Organizational structures, including the 3 lines of defense model, is operationally challenged

7 Front teams are increasingly first line/operations execs – vs. financial crime compliance who are influencers at best

Need for increased **operational efficiency**
- Compliance cost increase
- Onboarding time
- Evolving regulatory environment
- Availability of suitable resources

Reaching sustainable compliance is more than ever an objective for the industry

Need for increased **risk management**
- Regulatory pressure
- Controls and sanctions
- Financial and regulatory risk
- Reputational damage

Set the scene
Usual KYC pain points observed on the market

Initial due diligence | **Ongoing due diligence**

Roles: Maker / Checker / Approver (Initial due diligence)
Roles: Maker / Checker / Approver (Ongoing due diligence)

Workflow (Initial due diligence):
1 2 3 Collect static data, incl. shareholding structure
4 Watchlist Screening & alert review
5 Compute risk score & due dil. level
6 7 Collect supportive KYC documents
KYC file qualification
KYC workflow, incl. multi-step validation 8

Workflow (Ongoing due diligence):
9 Monitor/anticipate KYC doc expiration
9 Detect and materialize change of circumstances upfront
4 Continuous watchlist screening
10 Transaction Monitoring (incl. feedback integration) 11
9 Continuous risk scoring & due diligence level computation
9 Periodic review trigger and materialization
8 KYC workflow, incl. multi-step validation

12 Audit trail
Automated and ad' hoc reporting and 3rd party oversight

Ongoing due diligence related pain points

9 Manual monitoring of changes of circumstances (often scheduled through manual batches or when a transaction occurs) slows down the process and managing peak of activity becomes more complex ⭐

10 The usage of standard detection scenarios with usually fixed thresholds rises the alerts and false positive volume ⭐

11 Manual integration of Transaction Monitoring and Anti-Fraud detection analysis/feedback to the KYC chain (i.e., risk scoring process) lowers down the productivity

12 Non-existing or weak audit trail and non-existing reporting or not in real-time

Initial due diligence related pain points

1 KYC related parties data, incl. static data not stored/maintained in a structured manner. ⭐

2 Checking manually corporate data / registers weakens the audit trail negatively impacts the operations. ⭐

3 Same counterparty contacted multiple times to collect data/documents, duplicated KYC files, etc.

4 1st watchlist screening not occurring in real-time. High volume of false positives (operational impact) because not optimized business rules. ⭐

5 Risk scoring process is not dynamic and/or performed in real-time. Use of both risk score and due diligence levels?

6 KYC documents checklists are often managed manually. ⭐

7 High volume of KYC documents to handle impacts the operations

8 Lack of end-to-end workflow weakens the collaboration and decreases productivity. Lack of digitization, paper is still heavily used ⭐

Set the scene
Need for digitization of AML/KYC processes

« Classical » solutions

- Interact with many different systems
- Several manual workflows
- Heavy operational impact
  (no re-use of existing KYC components, local folders/files, hard-copy of documents, etc.)
- No synergy cost/efficiency

1	Collect data
2	Collect documents
3	Compute risk scoring & due diligence level
4	Document qualification
5 **6** **7**	Name screening system (with dedicated watchlist feed)
8	KYC file approval
9	Reporting system

New all-in-one solutions

- All-in-one solution
- Automatic workflows
- Potential AI/GenAI support components
- Reduce operational impact
- Synergy cost/efficiency

1
- Data collection
- Document collection & review
- Risk scoring system
- AI/GenAI support components
- Built-in name screening engine
- KYC file approval
- Audit trail & reporting system
- Quick implementation & integration of the solution

How can the technology help?

Technology applied for AML/CTF and Due Diligence on Counterparties

How can the technology help?
Challenges related to the access of private KYC Data – Counterparty onboarding (1/2)

Counterparty onboarding & periodic review

- Challenges to deliver a seamless digital onboarding experience to counterparties
- Numerous, redundant outreach and inefficiencies in data collection
- Need for extensive coordination and collaboration across various business and functional groups

Counterparty

- "I want to avoid redundant touchpoints and manual handoffs because they are frustrating and delay operations"

Front office

- "I need real-time access to status of onboarding workflow"

Compliance

- "I need to create holistic view of counterparties for appropriate risk ratings"

The case for onboarding portal

- Reduce onboarding time
- Embedded regulatory checks to verify plausibility of the information and ensure the right questions are asked
- Avoid unnecessary back-and-forth between business and compliance department
- Leverage all the retrieved information to ensure data consistency through the entire onboarding process
- Allow real-time detailed analytics & reporting

How can the technology help?
Challenges related to the access of private KYC Data – Counterparty onboarding (2/2)

KEY FACTORS OF SUCCESS

Keep counterparty experience at the hear of the initiative

Only tech by itself is not a solution

Efficient integration with existing ecosystem

Requirements rationalization

FEATURES TO CONSIDER

Smart & automated workflow

Questionnaire build and review

Seamless experience across devices

Active monitoring (status, KPIs/statistics, reminders)

Digital document management

How can the technology help?
AI/GenAI layers for AML/KYC use cases

Relevant layers for AML/KYC use cases

TECH LAYERS

	WHAT IS IT?
AI SERVICES	**AI Services** | *Advise – Implement – Operate services to enable Generative AI solutions for clients*
GENERATIVE AI APPLICATIONS	**Interface for LLMs** | *wide variety of applications developed for specific Generative AI modalities (e.g., speech, text, code, audio, video etc.)*
LARGE LANGUAGE MODELS	**Publicly Available LLMs** | *large models available via APIs without access to the model itself*
	Open-Source LLMs | *model details are publicly available to use, modify, and commercially distribute*
	Private LLMs | *purpose-built/use case-oriented/tuned version of open source or public models in private cloud/servers. Usually, small to medium sized LLMs*
AI HARDWARE & SOFTWARE INFRASTRUCTURE	**DGX Cluster** | *high-performance computing*
	InfiniBand Networking | *high-speed, low-latency networking protocol*
	CUDA Software | *software to manage workloads across GPUs*
	A100 + H100 GPUs | *GPUs required to run AI models*

How can the technology help?
The case for the usage of AI & GenAI in onboarding and ongoing monitoring

Identified use cases for AI and GenAI

No identified use cases for AI/GenAI

Initial due diligence

Ongoing Monitoring

A. Customer Identification	B. CDD and EDD Review	C. Quality Control and Approvals	D. Periodic Review	E. Monitoring and Screening
Customer Data Collection	Customer Documentation Review	Customer Identification Completion	Renewal Cycles Review	Trigger Event Review
Customer Documentation Verification	Customer Screening & Disposition	Disposition Confirmation	Customer Information Refresh	Escalation for Further Investigation If Needed
Missing Documentation/Information Identification	Entity Resolution/Network Analysis	Feedback to Analysts for Errors	Escalation for Further Investigation If Needed	Transaction Monitoring improved capabilities and alert analysis
Customer Outreach for RFIs	Initial Disposition and Documentation	KYC Record Approval		Sanctions screening improved capabilities and alert analysis
Customer Risk Rating	KYC Profile Finalization			
Sanctions screening improved capabilities and alert analysis	High Risk Relationship Memo			

Generative AI/Emerging tech is being widely tested in industry, and can act as a springboard to bend the longer-term AML cost-curve

How can the technology help?
Considerations and limitations for AI adoption

- What are the Model Performance and Stability Ongoing Monitoring considerations for AI models post-production deployments?
- What is the required model retraining frequency to keep current to rapidly changing market events/customer behaviors?
- What are the concerns around output accuracy, reliability, and model "hallucinations", especially for GenAI?
- Can GenAI/LLMs models, (e.g., open-sourced), be run locally, behind an organization's firewalls, to process confidential information?
- Which data formatting required to extract most value of the models?

Managing & Deploying Models

Domain and infrastructure

- What are the infrastructure requirements ?
- Can Foundational/General purposed models be adapted for AML-specific tasks?
- Which level of fine-tuning/specialized deployment would be required for AML-specific tasks?
- What roles are required for successful execution?
  - Subject matter experts
  - Data/software engineers
  - Data scientists/Machine learning engineers
  - Testers

Regulatory & privacy

- How open are regulators to reliance on highly performant but less explainable complex models?
- How can intellectual property and sensitive data be protected when interacting with AI Models?
- What is the regulatory standing on adoption of GenAI for AML use cases?
- What would be the regulator's limits for the deployment of AI/GenAI on AML use cases?

Leveraging Tech for current Hot topics

How can technology help to handle current hot topics?

Hot topics: Due Diligence on Assets for the Fund industry
Due diligence on assets

Assets classification and required level of due diligence

- <u>Listed Assets on regulated markets</u>: Assets that are listed on a securities exchange/traded on regulated markets. They are considered as having a **lower risk** as being less exposed to money laundering and terrorist financing risks due to existing market disclosures and controls. Professionals are hence only expected to carry out **sanction screening** (including Proliferation Financing) at the time of the first transaction, on an ongoing basis and at the sale (market practice).

- <u>Unlisted Assets and/or Assets posing higher ML/TF risks</u>: Assets that are not listed on a securities exchange/traded on regulated markets and/or posing higher ML/TF risks. They are considered as having a **higher risk** compared to listed assets leading to a **higher degree of scrutiny and level of due diligence. In addition to watchlist screening, a look-through approach together a deeper due diligence will be required (on a risk-based approach).

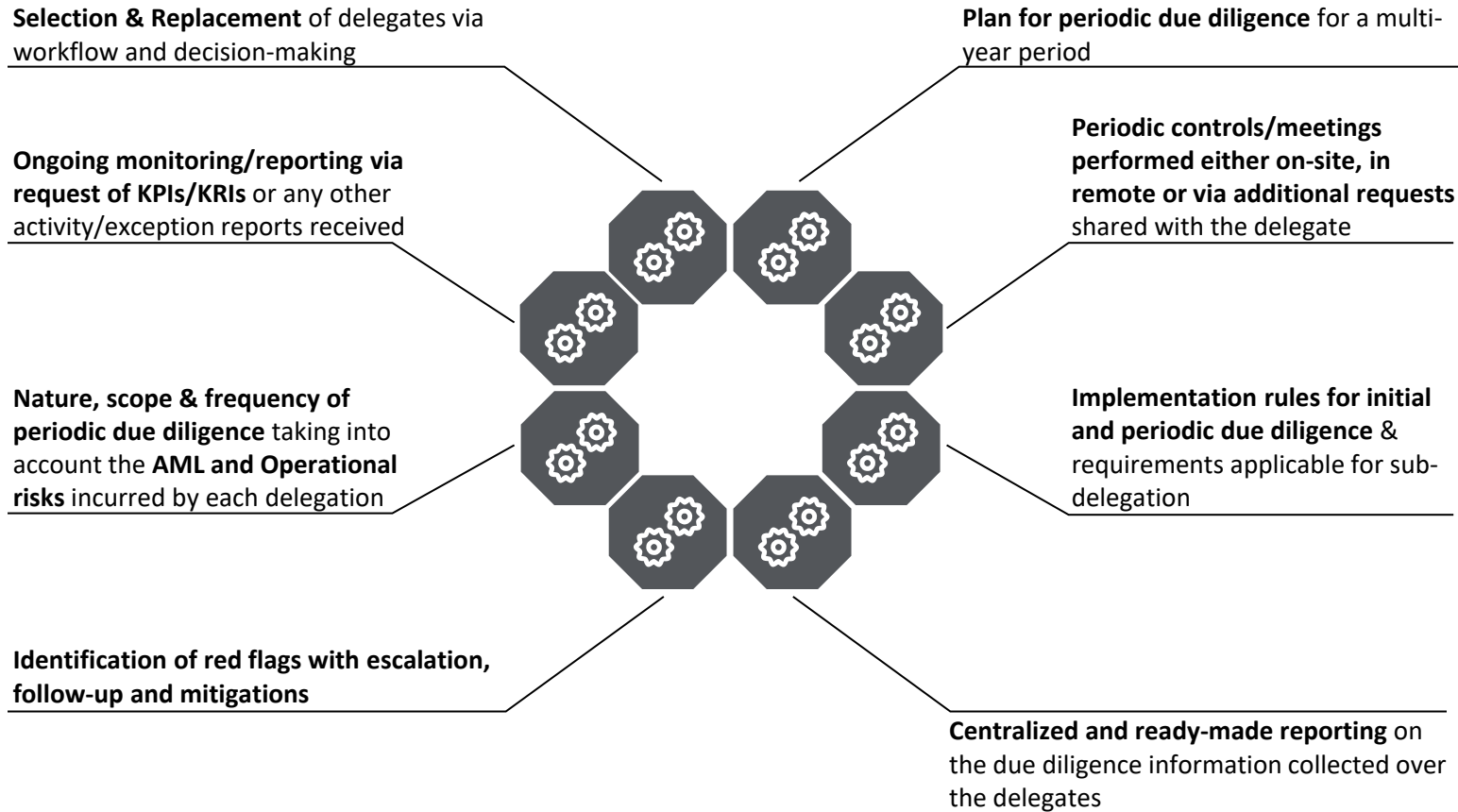|	Screening – Initial and ongoing (Targeted Financial Sanctions (TFS), adverse media)	Look-through (identification and due diligence on shareholding structure and related parties to the transaction)	Risk scoring	Corroboration using KYC document
Listed assets on regulated markets	Issuing company name/attributes AND/OR Securities identifiers (ISIN, CUSIP, SEDOL, FIGI, etc.) for sanctions only.	No	*Light*	No
Unlisted assets and/or assets posing higher ML/TF risks	*Investment:* Portfolio company and associated structure Seller and associated structure Co-investors Transaction intermediaries *Divestment:* Buyer and associated structure Transaction intermediaries	Yes	*Thorough* e.g., Counterparty type (e.g., Privately held company), country of incorporation, country of business, activity sector of the asset (e.g., oil and gas, shipping), tax risks (e.g., tax country, FATCA/CRS participating)	Yes (according to risk-based approach)

Not concerned by the CSSF FAQ

Hot topics: Due Diligence on Delegates/Distributors for the Fund industry
Overview of marketing related risks

Distribution Contracts Management
Continuous evolution of the relationship from starting the engagement to termination or renewal with updates of the contract

Product Governance
Ensuring financial products, through their entire life cycle, are eligible and suitable for their target market (e.g. Avoiding mis-selling), control of distributor's remuneration

Registration Requirements
Financial products cross-border passporting and marketing authorizations hurdles (e.g. marketing an alternative investment fund to retail investors in Belgium)

Monitoring & oversight of distributors
Monitoring Framework building, draft and reviews of procedures, initial & periodic due diligence, KPIs reporting

Compliance of marketing communication
Consistent reviews of commercial materials (e.g. factsheets), website content against local marketing rules where a financial product is distributed

AML/CFT
Performing AML/CFT Distributors risk assessments, KYC checklist remediation

Areas of interest for due diligence matters

Hot topics: Due Diligence on Delegates/Distributors for the Fund industry
Due diligence on Delegates/Distributors

Selection & Replacement of delegates via workflow and decision-making

Ongoing monitoring/reporting via request of KPIs/KRIs or any other activity/exception reports received

Nature, scope & frequency of periodic due diligence taking into account the **AML and Operational risks** incurred by each delegation

Identification of red flags with escalation, follow-up and mitigations

Plan for periodic due diligence for a multi-year period

Periodic controls/meetings performed either on-site, in remote or via additional requests shared with the delegate

Implementation rules for initial and periodic due diligence & requirements applicable for sub-delegation

Centralized and ready-made reporting on the due diligence information collected over the delegates

ATTENTION POINTS

❖ Delegation performed internally within the same group as the IFM is not an exception for not performing due diligence measures.

❖ Data protection, IT Management/Coverage of cyber risks and Business/IT resilience are gaining tractions and have to be ensured.

❖ The due diligence is not a one-off exercise, and delegated activities shall remain in compliance with applicable legal & regulatory provisions.

❖ Initial and periodic due diligence assessment shall result in a final report including the results of the analysis, the escalation measures taken and the conclusion reached. It shall be validated, dated and signed by all bodies of the IFM empowered to approve or refuse the delegation.

❖ Initial and periodic due diligence assessment shall be tracked, documented and properly stored as they must be made available to the CSSF upon request and sent without delay.

Next Link'n Learn webinar

Date: 22/01/2025

Topic: Sustainability|
SFDR Reporting: state of play and key learning points

Deloitte.