Point of View

Financial Crime at the heart of Compliance transformation programs

How Financial Crime will transform your organization

July 2018

Current Trends
Our point of view
How we can help from strategy to execution
Executive Summary

In a context where regulatory pressure is stronger, fines higher and financial criminality more sophisticated, financial institutions are reassessing their financial crime framework and leading large scale projects.

A deep reorganisation of financial groups

Historically, financial groups had addressed financial crime topics in a decentralized approach preventing a holistic view of the client and his risks. In order to answer regulatory challenges and be able to capture complex multi-countries and multi-entities models, this holistic view is key. To reach this objective, financial groups are reviewing their governance and operational model around financial crime. Those transformations start with the implementation of central teams who define standardised guidelines and process that need to be rolled-out in each entity of the group through intermediary structures. A certain flexibility is required in order to allow each country to integrate regulatory constraints defined by their local regulatory if those are more restrictive than the group ones.

At the heart of digitalisation: data management, Robotics and Artificial Intelligence

The need to continuously enhance gains of agility, efficiency and productivity leads to new technologies paths in terms of financial security, with, in particular:

• The control of transactional and referential data ahead of detection systems that lead to consequent work on governance and data quality and reliability
• The implementation of machine learning to tackle alerts and data history in order to fine-tune thresholds and reduce significantly false positives and related reviews
• Numerous experiments based on advanced algorithms and unstructured data to detect new criminality schemes and evolve from static models to dynamic and predictive models for risk management
• Development of robots in order to manage recurrent tasks with low added-value

Resources at the heart of transformation

In this changing context, needs of recruitment are evolving to capture more complex profiles allying expertise in financial crime and analytical capabilities. Recruitment strategy has to take into account to the way to attract those rare profiles and to ensure their retention. Along with risk monitoring, those profiles also have to develop a Financial Crime Culture within the organization aiming at raising awareness among each resource to allow identification of any risk the earliest possible in the process, starting with the first interactions with the client.
Current Trends
Financial Crime* is at the heart of Compliance issues

- Recent Financial Crime events raised attention on new ways used by criminals to cover up the proceeds of their crimes.
- Criminals have largely sophisticated their activities, allowing them to operate through the legal economy largely.
- Disruptive technologies (bitcoin, cryptomoney,...) and innovative financial products are new channels for white collar criminals.
- The Financial Crime risk for Financial Institutions is more important than ever.

* Financial Crime in this document covers AML, Combatting the Financing of Terrorism and Sanctions Embargoes
Many Financial Institutions are in the process of assessing and monitoring their Financial Crime frameworks...

Historically, Financial Institutions have been addressing Financial Crime topics through a decentralized organization, in a best effort approach.

Indeed, their Financial Crime framework was built on separate organizational structures, each supporting a different Financial Crime topic: KYC, AML, Embargo...

In addition, each region, each business line and/or each entity has built its own Financial Crime management framework with:

- local Financial Crime processes and procedures (local scoring methods, local filtering data bases, local alert management process, ...);
- local tools to address Financial Crime, leading to a large number of tools with different functionalities and granularity levels.

With the sophistication of criminals techniques, using multiple channels across the world, this approach is now showing its limits.

The decentralized framework, currently prevailing in Financial Institutions, does not allow a global monitoring of Financial Crime nor a single view on a client and his transactions across business lines of the same Group.

Nowadays, Financial Institutions are launching Group risk assessments in order to review their Financial Crime frameworks as a whole at different levels (Governance, Process, IT & Data, etc.), highlighting areas of focus and raising awareness regarding the limits of frameworks in place.

These risk assessments are leading Financial Institutions to rethink their organization, define action plans and undertake large scale transformation projects.

Wolfsberg Group further emphasizes on the fact that risk assessments are the most important tool for the definition of an effective Financial Crime framework.

---

1 The Wolfsberg Group is an association of 13 global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.
... shedding light on the main challenges of Financial Crime risk management

**Improving operational efficiency**
- New Financial Crime techniques’ complexity is making it more difficult for Financial Institutions to build the right detection tools and thus identify meaningful and relevant alerts, while avoiding false positives.
- In parallel, guaranteeing a complete coverage of the Financial Crime related risks remains a key challenge for financial institutions.

**Ensuring global monitoring of Financial Crime**
- The evolution of Financial Crime patterns and new regulators expectations are prompting Financial Institutions to consider Financial Crime as a whole.
- Being able to perform analyses across different risk typologies, different geographies or different business lines is now fundamental for Financial Institutions.

**Managing Data complexity**
- To identify the increasingly complex crime patterns, Financial Institutions need to properly leverage growing volumes of data: their dispersion, their availability, their quality and their adequate use are a great challenge.
- Financial Institutions are also facing data privacy issues, conflicting domestic and international laws.

**Upskilling resources**
- To address regulatory constraints on Financial Crime, Financial Institutions need to reinforce their organization.
- They need to hire adequate profiles with the right competencies, be them Compliance or Analytics profiles, at each step of the Financial Crime process.
Our point of view
Compliance Management programs are under constant process of revision and optimization

Financial institutions are facing rising regulatory requirements regarding their Compliance frameworks from relevant laws and regulations - For example EU and US regulations regarding AML/CTF and Sanctions as well as UK and US regulations for Anti-Bribery and Corruption (and new French regulation: Sapin 2) were subject to various domestic amendments impacting financial institutions at a global level.

Therefore, Compliance Management programs are under constant process of revision and optimization, including the risk assessment procedures, to meet regulatory requirements and to mitigate business and regulatory risks including the risk of potential fines.

- Performance of a risk-based approach, focusing on AML/CFT Risk Assessment
- AML/CFT Risk Assessment conducted only upon quantitative data
- Conduction of a merged approach, joining the qualitative and quantitative data for Risk Assessments, for different Financial Crime risk types
- Introduction of an IT supported end-to-end workflow process, covering quantitative and qualitative assessment of different risk types
- Daily risk assessment with automatic data communication between risk assessment workflow tool and monitoring or screening tools

Past

Now

Future
Increasing regulatory pressure requires Financial Institutions to rethink their current frameworks

In order to improve the monitoring of Financial Crime activities, Financial Institutions have been leading large scale projects to reduce Financial Crime risks.

Implementation of a holistic approach through organization and processes
- In order to be able to perform cross-analysis of transactions and payments, Financial Institutions aim at having a global view of a client and his transactions.
- Therefore, they are reviewing their way of working through the implementation of new governance around Financial Crime and standardization of related processes.

Focus on Financial Crime Culture and profiles selection
- Financial Institutions are today conscious of the importance to raise awareness across the organization and to hire, train and federate the right talents required for Financial Crime risk management.
- A high level sponsorship is required to ensure adoption and sustainability of such initiative across the organization.

Review of IT Architecture and Data management
- Financial Crime monitoring requires to aggregate, at different levels of the organization, data from different sources and of different types, prompting investments in cutting-edge technology such as data lakes and data analytics.
- Data quality being a key issue to ensure reliable outputs and efficient analytics, Financial Institutions are reviewing Data Governance and leading Data quality remediation plans.


Section 2 – Our point of view

Setting the right organization is the stepping stone towards an efficient Financial Crime organization

Financial Crime Central team: a key step to be able to manage Financial Crime across the organization.

Financial Institutions need to move from a silo-based approach towards a global management of Financial Crime. They have started developing Financial Crime central teams, modelled on the government agencies.

Central teams were first designed as hubs to gather and share Financial Crime intelligence.

Recognizing the importance of having Financial Crime information centralized to perform efficient investigations, Financial Institutions have been giving a wider role to those Central teams:

• Data gathering and aggregation at Group level;
• Investigation of unusual events and suspicious transactions;
• Cross-analysis to identify suspicious behaviors and patterns;
• Suspicious Activity Report (SAR) production to competent authorities when needed;
• Regulatory watch and trends analysis;
• Raising awareness across the organization in terms of Financial Crime;
• Processes improvement / standardization.

In international large groups, a single central team will struggle to cover the whole scope of activities, and should thus leverage intermediate teams, organized by region, activity or business line. These intermediate teams will be responsible, on their scope, of the production of Financial Crime information and indicators to report them to the Group team in charge of global consolidation.

Thanks to their global approach, Financial Crime central teams provide Financial Institutions with a holistic view on Financial Crime data. Having a consolidated view allows them to easily detect sophisticated and cross-border behavior patterns and to tackle Financial Crime in a unified and efficient manner.
Section 2 – Our point of view

For this target organization to be efficient, standardization is a key success factor

For Financial Crime teams to acquire a holistic view on a client and be able to lead accelerated cross-entities investigations across various dimensions (clients, activities, geographies, types of financial crime, etc...), they need to easily share and aggregate data within the same Group.

This requires to build a common standardized framework including a common language and standardized processes, procedures and methodologies.

Within large international groups, setting up such initiative is quite a difficult exercise, due to:
• Local regulatory constraints and best practices;
• Different risk appetites;
• Language barrier;
• Compliance culture diversity;
• Activities to monitor.

In order to facilitate transfer of information, unique definitions and standard guidelines should be defined at Group level describing Group objectives to achieve and main principles to be implemented across the organization. This roll-out is quite challenging in worldwide organizations.

These Group guidelines should constitute the basic framework for any local implementation. Local entities will have the ability to add more restrictive constraints and obligations induced by local regulatory specifications and/or best practices.

Strong focus should be set on standardization of topics such as:

- Definition of the minimum set of data to be collected and implementation of a unique method for client scoring.
- Standardization of the workflow from alert generation until a potential SAR generation.
- Implementation of global central data base that should include all minimum data required at local level.
- Creation of a global scenarios repository ensuring consistency between locations.
Section 2 – Our point of view

Time being an essence in Financial Crime detection, leveraging right technologies is key to reduce risks and increase efficiency

Strong regulatory requirements and complex Financial Crime techniques on one side, and increasing volumes of data and transactions to monitor on the other, are leading Financial Institutions to **reshape their technology environment**.

**Speed** and reliability of analysis are becoming key for **proactive** and efficient Financial crime detection.

Financial Institutions now need to **store** all the **data** required, **manage** them, **consolidate** them and be able to **analyze** them for **cross-investigation** purposes.

Therefore, they need **agile** and **flexible** solutions for data storage and **Big Data** capabilities for a better detection of criminal patterns.
For the past years, Financial Institutions have been used to deal with a slowly evolving environment, that neither required high agility nor fast adaptability.

Therefore, they relied on solutions that allowed them to extract data from different sources, transform them and load them in repositories (data waterhouses - DWH), dedicated for a specific use (AML, Sanctions, etc.). These DWH allowed Financial Institutions to store structured internal data, formatted to answer specific needs.

As criminal patterns become more and more complex, regulators are prompted to strengthen their regulatory framework. In this context, Financial Institutions require more and more to access quickly an increasing volume of data, that can be structured or unstructured (voice, email, chat, etc.), and that can be issued by internal or external (e.g. negative News) sources. These data are necessary to efficiently and relevantly identify and track new criminal patterns.

To address these new stakes, new technical solutions are emerging to allow Financial Institutions to run more relevant and adaptable analyses.
...which leads to the emergence of new models, based on data lake solutions...

The new trends are pushing Financial Crime towards an integrated model requiring to handle data from different sources, format, and that can be structured or unstructured.

### Data lakes offer a more complete approach for collecting and storing Financial Crime related data

- **Implementing a data lake is equivalent to deploying a golden source** for all available Financial Crime data by drawing data from multiple sources and storing them in their native format in order to have a centralized pool of data.

- Data Lakes allow Financial Institutions to **store in a single location** all type of data related to Financial Crime including both **structured** and **unstructured** data from **internal** and **external** sources, leading them to leverage all accessible and relevant data as an asset to monitor risks and produce **new insights**.

- **It allows to break down silos among the existing information systems** by unifying the data of different units equipped with their own IT tools regarding Financial Crime, and therefore tackle all the related topics (AML, Sanctions, etc.) through the same IT setup.

### Data lakes capabilities

| Overcoming volume, velocity and variety challenges, giving the possibility to **analyze an exponentially increasing volume** of transaction data. | Ingest **structured, unstructured and semi-structured data** for broadly diversified analysis and detection of new scenarios. | Possibility to add new data sources to offer **more flexibility** to take into account new regulatory demands. | **No expensive or time-consuming modeling needed**, as the data schema does not have to be defined up front. | **Cost benefits** in storing vast amounts of data in far less space than would be required for even relatively small conventional databases. |

Data lakes are answering the new needs to **handle a higher volume of data with variable format and source**, and provide a dynamic setup allowing Financial Institutions to **adapt to evolving criminal techniques**. As the criminal pattern varies, the data lake can provide new data from different sources to build **dynamic analytics**.
...robotics and dynamic analytics

In order to optimize Financial Crime monitoring and considering the requirements to uncover the increasingly complex criminal patterns, Financial institutions are investing in:

- RPA* to automate low-value repetitive tasks such as collecting information for KYC and Due Diligences,
- Advanced Analytics capabilities using intelligent algorithms that allows to convert raw data into valuable insights.

### Analytics enhance the ability to better respond to regulatory constraints and requirements

- Analytic tools are essential to take advantage of the opportunities that present the implementation of a data lake.

  The advantage of these tools is that it starts to **allow a more joined-up approach between business analytics and the operational processes**. It is helping Financial Institutions in selecting the relevant data out of the huge amount of available data that need a specific attention.

- The **combined approach between data lake and analytics is allowing institutions to rapidly respond to regulatory requirements**. It offers a way to accurately respond to their issues regarding Financial Crime, encompassing optimization of detections, enhancing their monitoring systems, refining scenarios, improving alert assessment and strengthening KYC capabilities.

  ✓ For example, plugging an analytics tool to a data lake provides the ability to combine multiple data sources and types and offers significant advantages for reducing false positive levels in identifying suspect AML cases.

---

**Combining robotics, data lake and analytics, a new approach to address the growing complexity of Financial Crime**

<table>
<thead>
<tr>
<th>Function</th>
<th>Extraction</th>
<th>Storage</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability</td>
<td>ELT-based setup</td>
<td>A data lake to store all type of data</td>
<td>From descriptive to prescriptive analytics</td>
</tr>
</tbody>
</table>

- **Extract Load Transform (ELT) based setup** which consists in extracting raw data and loading them directly in a repository, irrespectively of the format or source.
- **Data extracted this way can be internal or external, structured or unstructured.**
- **Data of various sources and in various format are stored in a data lake**, which constitutes a **global pool of all type of data** that can be relevant to Financial Crime analysis.
- **This flexible storage** is a convenient **answer to increasing regulatory requirements**, and allows to constitute a **common dataset** for all Financial Crime related uses, giving an encompassing picture of the events and trends that can be useful to detect criminal patterns.

- **Dynamic analytics tools**, plugged to the data lake, allow to produce meaningful analyses based on any data stored in the repository.
- **These tools can therefore leverage a variety of statistical, data mining techniques** to study recent and historical data, thereby allowing to forecast what crime scheme might be used in the future, adding a **prescriptive layer to the analytics**.

---

* Robotics Process Automation
Future of financial crime analytics

Next generation technology is agile and flexible, allowing compliance professionals to employ analytics in many new areas.

Capabilities of next generation financial crime analytics

1. Unstructured data analysis
2. Predictive models
3. Champion/Challenger models
4. Real-time event integration

Financial crime analytics are moving to a more dynamic model. They are data-driven, iterative and interactive in nature, providing feedback that is actionable and useful.

Moving forward, financial crime leaders employ dynamic reports allowing them to view data across multiple dimensions. These dynamic reports and the aggregation of data will allow financial crimes professionals to measure more accurately and appropriately the effectiveness of their surveillance programs.

Additionally, financial crime professionals gain the ability to mine for root causes and obtain critical insight.

Built relatively easily despite their advanced capabilities, the next wave of data analytics programs can provide a holistic – yet intuitive – view of risks across businesses and geographies.

Leading practices

<table>
<thead>
<tr>
<th>Dashboards</th>
<th>Segmentation</th>
<th>Scenario Typology</th>
<th>Thresholds</th>
<th>Risk Scoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Dashboards to track financial crime risk KPIs</td>
<td>• Segmentation cluster tests</td>
<td>• Scenario library for parallel run or independent testing</td>
<td>• Statistics and metrics dashboards</td>
<td>• Statistical models to predict risk of alerts or cases</td>
</tr>
<tr>
<td>• Heat maps to identify higher risk areas</td>
<td>• Segmentation Dashboards with KPIs to monitor model metrics</td>
<td>• What-if and scenario analytics for hypothesis testing</td>
<td>• Outlier dashboards</td>
<td></td>
</tr>
</tbody>
</table>
Section 2 – Our point of view

...relies on a standardized Data Quality Framework

Set up a Data Quality Framework to bring together a standardized approach to measuring data quality using rules and dimensions

Data Quality Dimensions

Completeness
Is any key information missing or are there null values?

Validity
Do values adhere to defined business rules, accepted values and accepted formats?

Accuracy
Is the data accurate when compared to the source or original content?

Consistency
Is the data value consistent with required formats or definition criteria?

Integrity
Do broken links exist between data that should be related?

Timeliness
Is the information update frequency adequate to meet the business requirements?

Examples of Transaction Monitoring Data Quality challenges

- Lack of aggregation of customer names from disparate sources for monitoring
- Null or Blank values within attributes or numeric type field populated with alphanumeric or character values
- Customer addresses truncated
- Last name has more than one name populated or attributes such as Date, Postal are stored in the invalid format
- Lack of data governance or consistent monitoring of data quality issues through dashboards/KPIs
- Incorrect or inconsistent data dictionaries result in misclassified products and account types

A data quality assessment allows intuitive data profiling and visual interrogation
Section 2 – Our point of view

...Meaning an efficient Data Management framework

To ensure the added value of technology regarding Financial Crime, it is essential to use the correct data in entry of related monitoring tools. This requires the establishment of a data management strategy around a set of four relevant items.

**Establishing a Data Governance** is a key component of Financial Crime data management, as it defines proper ownership within the compliance organization for each data type related to Financial Crime and the way of using those Data.

As data is now at the center of the Financial Crime framework, it is key to make sure that the data are mastered and properly monitored through a **robust data governance**.

Knowing the definition of each data in upstream systems and identifying the right data and its golden source to link it to the right scenarios allows Financial Institutions to secure and to strengthen their Financial Crime monitoring processes and to make related analyses more relevant and more reliable. By establishing a new model based on a data lake and analytics, Financial Institutions could really take advantage of the variety of the available data over numerous of internal and external sources that they can access.

Financial Institutions must define **best practices** and **principles** in order to ensure continuous **data quality assessment** and **improvement**.

Behind the curtains of the data framework, setting the right people at the right place is the key towards efficient data management, and more globally, towards an effective Financial Crime setup.
People are one of the key success factors for an optimal Financial Crime organization...

While processes and systems are important to fight Financial Crime, people are at the heart of such frameworks. Having the right people at the right place is the challenge of every organization.

High skilled Compliance profiles to address more analytical tasks...

The profile required to fight Financial Crime has been evolving in the past years, from individuals specialized by silo (KYC, AML or Sanctions & Embargoes) and doing basic analysis towards Financial Crime experts having cross-silo skills.

Compliance officers working on Financial Crime risks should be able to:
- **Build a case** based on KYC, AML and embargo inputs;
- **Interact with other stakeholders** to enrich their knowledge on the client, his related parties and his transactions;
- **Master new technologies and data analytics** that are key for cross-analysis and for continuous optimization of the framework.

The ability of Financial Institutions to find these rare profiles will be crucial in the enforcement of an efficient Financial Crime management.

With RPA and automation of some tasks, it is necessary to manage a continuously evolving organization and required competencies. Organization should therefore rethink their strategy of recruitment and training to answer these transformations.

... spreading a Financial Crime Culture across all organization layers

Fighting Financial Crime is a matter not limited to Compliance.

Fighting Financial Crime is the responsibility of each individual across the organization.

From the Relationship Manager to the Compliance Manager through the trader booking a deal, every employee of the Financial Institutions is accountable for being vigilant to crimes that could be perpetrated and making sure that any alert is properly escalated.

It is crucial that Financial Institutions maintain awareness around fighting Financial Crime across their organizations to ensure that individuals are conscious of such risks and aware of new criminals schemes.
...an organization where Financial Crime culture should prevail

To make sure that individuals are adequately equipped to fight against Financial Crime, Financial Institutions must offer **long-term career paths** and **properly formalized training packages** that are:

- **Adapted to each role within the organization**: each individual should have a training tailored to his role with concrete examples;

- **All encompassing**: they should cover all types of risks and criminal behaviors, as well as all elements required to master the job (roles and responsibilities, governance, processes, tools, etc.);

- **Technology oriented**: in a context of increasing importance of tools and data within Financial Crime, it is key that training packages provide Financial Institutions’ employees with all the material to understand and master the technology they will have to use;

- **Up-to-date**: training should be regularly updated and should take into account the newest regulatory requirements, as well as the latest innovations in terms of Financial Crime techniques and behaviors.

Creating an **Excellence Center** is a cornerstone in an efficient Financial Crime framework. It requires to identify **Champions** and **Ambassadors** to spread the Financial Crime **culture**, principles and best practices across the organization.

It is also strongly recommended to provide key individuals who are involved on a daily basis with clients with **Decision Support tools** that will allow them to analyze any suspicious behavior and know when it is relevant to escalate it as Financial Crime risk.
How we can help from strategy through execution
Section 3 – How we can help from strategy through execution

Our clients say ...

I want to **assess my Financial Crime framework** in an accurate manner and **compare it to the market standards**.

I need to find ways to make my Financial Crime **processes and organization more efficient**.

I want to **implement a technology** that helps me **address the new issues** related to Financial Crime.

I need to be able do **manage my data efficiently** to be **relevant** in my Financial Crime analyses and my alerts handling.

I want to **raise awareness** and **enforce a corporate culture** across my organization around Financial Crime.
Section 3 – How we can help from strategy through execution

**How Can PwC Help you**

PwC helps clients on all Financial Crime areas from strategy through execution, leading to cover the overall scope of such kind of program. We have founded our offer around eight workstreams based on the numerous models we have developed with our clients over the years.

**Strategy**
- Assess your company profile and maturity level in term of compliance around Financial Crime.
- Identify your gaps regarding the major issues of Financial Crime.
- Define target and develop your roadmap.

**Execution**
- Formulate deployment approach.
- Deploy all or part of our Financial Crime workstreams depending on your company profile.
- Test and measure results.
- Enforce continuous improvement.

Achieve sustainable and measurable results in the fight against Financial Crime
Section 3 – How we can help from strategy through execution

Our relevant Financial Crime workstreams

1. Risk assessment

- Guarantee the Financial Crime related risks coverage.
- Develop risk assessments that are relevant, all-encompassing and that provide all the information and tools required to improve the Financial Crime setup.
- Have the ability to retrieve relevant data.

2. Scenarios definition

- Identify AML/CFT risks to be covered in view of your customers, products and activities.
- Define adequate scenarios and implement them over the organization.
- Assess and optimize current scenarios.
- Identify and map all relevant data and associated sources which would ultimately be feeding the target group monitoring tool.

Your challenges

- We define the scoring method and develop the associated grid.
- We support you in leading the interviews to perform the risk assessment.
- We offer the right capabilities to analyze the results of the risk assessment and to provide you with a relevant view of the data.
- We define action plans aiming at leveraging the risk assessment to improve the overall efficiency of the Financial Crime framework, as well as the coverage of the related risks.
- We provide you with some insight to enhance your risk assessment process.

How we can help

- We can help you identify the risks to be covered based on the analysis of your environment and regulations in force.
- We have significant experience developing and enhancing existing AML screening and monitoring programs. By using methodologies and procedures that have proven consistent with regulatory expectations, we can assist you from the design of scenarios to the identification of data and related sources.
- We have developed a set of proven repositories, tools and enablers to accelerate deliveries of such projects.
Section 3 – How we can help from strategy through execution

**Our relevant Financial Crime workstreams**

### 3. KYC optimization-Automation

- Define or review target KYC processes in order to make them more consistent, scalable and cost effective.
- Help KYC/onboarding teams save time and be more efficient.
- Facilitate and optimize the gathering and management of KYC data.
- Provide data that are accurate and help establishing relevant analyses.

**Your challenges**
- PwC has developed a strong experience in designing and reviewing KYC processes.
- We can help you automate basic consistency rules, notably through the identification of internal and external sources for KYC consistency process.
- We can assist you in the definition/review of clients scoring methodology.
- We can help you leverage technology, notably through the development of data lakes for aggregating and processing KYC data or the implementation of workflow solutions.

**How we can help**
- Switch from traditional silo-based organization and move towards a more integrated Financial Crime framework.
- Streamline the operational activities related to Financial Crime in order to identify potential correlation.
- Have a global and deeper analysis and monitoring of your customers and their related behaviors.
- Establish a proper control approach in order to better manage risks related to Financial Crime.

- PwC provides benchmark and competitive intelligence through a center of excellence in the broad area of Financial Crime.
- We help designing Target Operating Models (TOM), from organization to processes, through procedures and governance.
- We perform gap analyses to evaluate your current Financial Crime framework as compared with the previously defined target.
- We assist you throughout your transformation by defining action plans, roadmaps and supporting you in the implementation project.
- We help you optimizing your processes, while taking into account local specificities and recent regulations.

### 4. Transformation
Section 3 – How we can help from strategy through execution

Our relevant Financial Crime workstreams

5. Data Lake Implementation

- Have a centralized and global view of data related to the client, his accounts, his transactions, his operations and his alerts.
- Break down silos in accessing to the aforementioned type of data in order to set up a golden source of data linked to Financial Crime.
- Have optimal and integrated data analysis framework.
- Enhance your capability to manage and monitor a huge volume of daily transactions data.
- Seek for the most agile IT infrastructure in order to be able to rapidly and better address regulators demands.

Your challenges

- We offer in class methodology to tackle complex issues around data aggregation, centralization and processing, notably in the context of a data lake based architecture.
- We combine our data science skills and your overall Financial Crime data to provide the expected outcomes in terms of monitoring and analytics.
- We share our experience feedback and expertise with you regarding data lake related practices within Financial Institutions, especially in the field of Financial Crime.

How we can help

6. Data Governance

- Master your data related to Financial Crime and have a good knowledge of them and the way they are used in order to cover underlying risks.
- Deal with data quality matter to ensure reliable analysis and monitoring of Financial Crime.
- Get the right data to reduce the increasing volume a false positives for better quality of analysis.
- Establish proper policies, standards and rules to control your data linked to Financial Crime.

- We assist you in establishing relevant approach regarding data screening, clearing, reconciliation and mapping, allowing you to enhance data quality and data mapping.
- PwC has developed a set of four recommendations that allow Financial Institutions to deal with data governance challenges:
  - Data ownership and stewardship;
  - Data architecture;
  - Metadata management;
  - Data delivery.
Section 3 – How we can help from strategy through execution

Our relevant Financial Crime workstreams

7. Choice of IT solution

- Define criteria to select the most adequate IT solution in order to support your Financial Crime activities.
- Assess IT solutions to ensure that they are fit for purpose and meet your requirements regarding Financial Crime.
- Ensure that target IT solution offers out of the box scenarios while being able to implement new additional and yet unknown scenarios.
- Get the most valuable IT solution that helps to process all your Financial Crime data and that can support you in your reporting and analytics tasks.

8. Awareness and Change Management

- Foster a corporate culture and behaviors, sensitive to Financial Crime risks.
- Develop new skills within the compliance function in order to be able to adapt to the upcoming organization, processes, analytics and technology around Financial Crime.
- Set up an adequate and evolving training package in order to keep up skills with the evolving and changing face of Financial Crime.

Your challenges

- We leverage our technology skills and Financial Crime expertise coupled with your industry deep knowledge to assist you in determining the best IT solution you can invest in.
- As well, PwC can assist you in the implementation of in-house solutions thanks to our system development life cycle (SDLC) framework and capabilities.
- We already deliver apps and analytics tools by leveraging benchmark and innovation.
- We merge our business capabilities, technology capabilities and analytics approaches to assist you from design stage to deployment.

How we can help

- We help identifying a resources segmentation depending on their involvement in the Financial Crime framework.
- We support you in the definition of relevant training curriculum and communication plans, based on this segmentation.
- We assist you in preparing the required training material, adapted to your needs and your specific environment: e-learning sessions, adequate slide decks, definition of the training session format, etc.
- We help you run the training programs, both in terms of coordination and animation of the training sessions.
- We support you with change management capabilities during transformation projects aiming at implementing a new organization, a new process and/or a new tool.
Your contacts

Rami Feghali
Partner, PwC France
FS Risk & Regulation lead
+33 (0) 6 10 02 56 74
rami.feghali@pwc.com

Jean Barrère
Partner, PwC France
+33 (0) 6 45 87 34 73
jean.barrere@pwc.com

Sébastien d’Aligny
Partner, PwC France
Financial Crime lead
+33 (0) 6 21 43 65 48
sebastien.daligny@pwc.com

Marielle Fernainé
Senior Manager, PwC France
+33 (0) 6 83 22 76 36
marielle.fernaine@pwc.com