KPMG

Insights on evolving AML practices

A benchmark analysis of European Banks

April 2021

Introduction

Banks in Europe continue to restructure their AML functions and lines of defense. In recent years, supervisory activities and regulatory expectations for AML have been significantly heightened.

The objective of this survey is to collect insights on a range of AML practices along with other related aspects to help understand better:

- the advancement in setting up a AML team and the challenges faced by banks;
- the core roles and responsibilities of 1LoD & 2LoD related to AML work;
- the most common practices in various aspects related to AML that have been adopted by banks.

Our survey was targeted to banks across Europe.

As a valued client of KPMG Firm, we would like to thank you for participating in this benchmark. The value of an exercise such as this is driven by the information, insights and practices that you have shared with us.

We hope that this summary pack can act as an aid both to better understand the key areas of focus for improvement as well as wider AML practices.

Timo Purkott
Partner, Financial Services
KPMG in Germany

Dr. Henning Dankenbring
Partner, KPMG ECB Office
KPMG in Germany

KPMG

Agenda

1. Executive summary

AML Benchmarking Survey – 8 things you need to know…

Banks in Europe continue to restructure their AML functions and lines of defense. In recent years, supervisory activities and regulatory expectations for Anti Money Laundering (AML) have been significantly heightened. The AML benchmarking survey is designed to gain insights on the various aspects of industry applied AML practices across the Europe. Some of the key insights from the survey are mentioned below:

1 Data quality responsibilities related to AML typically allocated to 1LoD

Many respondents confirmed that data quality responsibilities related to AML work should be allocated to 1LoD.

2 Poor data quality and bureaucratic processes as main barriers to defining clear responsibilities

Majority of respondents indicated that poor data quality and bureaucratic processes are the main barriers to clearly defining responsibilities between 1LoD and 2LoD related to AML.

3 Upto ~100% increase in AML budget investment compared to 3 years ago (i.e. CtB budget increase)

One fourth of respondents indicated upto ~100% increase in AML budget investment in order to strengthen 1LoD & 2LoD responsibilities to mitigate AML/CFT risks compared to 3 years ago.

4 More than 50% of headcount in compliance represents FCC headcount

Many respondents stated that more than 50% of headcount in compliance represents Financial Crime Compliance (FCC) headcount.

5 Investments in automated solutions or new technologies to improve overall AML framework

Almost all respondents confirmed investments in automated solutions or new technologies to improve overall AML framework.

6 For vendor solutions cost & integration issues identified as key challenges

For vendor solutions, cost consideration and integration issues with firm's in-house systems are identified as main challenges.

7 Inadequate policies, procedures and controls giving rise to bribery and corruption practices

Vast majority of respondents indicated that inadequate, policies, procedures and controls are the main factors facilitating bribery and corruption practices.

8 0% to 5% as the best estimate for conversion rate of alerts to SAR

Most of the respondents estimated 0% to 5% as the conversion rate of alerts to Suspicious Activity Reports (SARs).

Potential considerations on the basis of the survey results ….

- Review 1LoD and 2LoD roles & responsibilities related to AML
- Rethink AML budget investment
- Data & IT infrastructure supported with emerging technologies
- Evaluate adequacy of resources
- Review AML / FCC policies, procedures and processes

Note: Analysis on the basis of total responses

2. About the survey

The survey allows for insights from 47 European banks among AML / Compliance professionals representing 14 countries across Europe…

Banks are generally reliant on the Three Lines of Defense Model (3LoD) to facilitate an effective risk management system and control. Many banks have expressed interest in better understanding the typical roles and responsibilities of the 1st and 2nd LoD for AML and how they compare against their peers. In this context, KPMG designed a short survey to gain a greater understanding of the intricacies related to this topic.

Purpose of the survey…

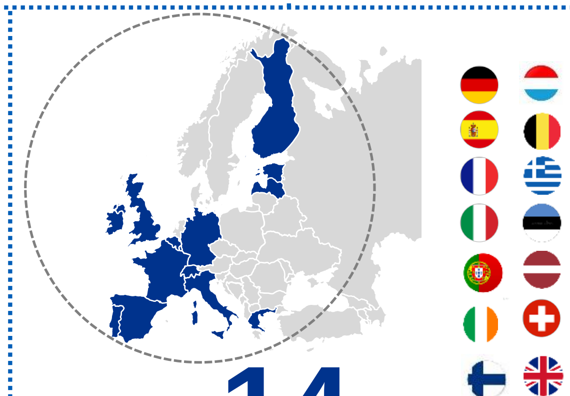
The AML benchmarking survey (“survey”) intended to collect insights on the range of practices related to roles and responsibilities of 1st and 2nd LoD regarding AML along with other key aspects of banks across Europe, in order to perform a benchmark analysis for participating banks.

Scope of the survey…

The survey is conducted between February 2021 and April 2021 among AML / Compliance/ Financial Crime executives from 47 European banks (“banks”) representing 14 countries/ regions/ jurisdictions across Europe.

47

Banks



14

countries

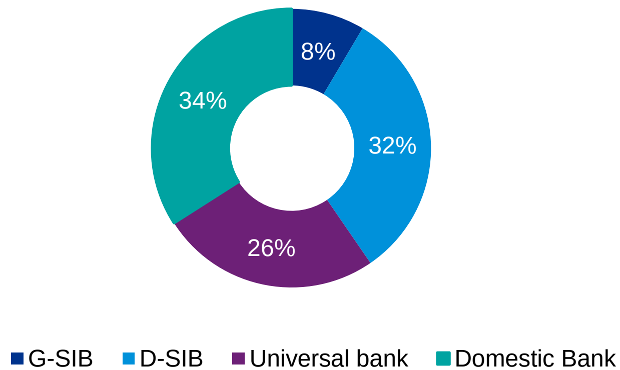
96%

of respondents are part of 2LOD

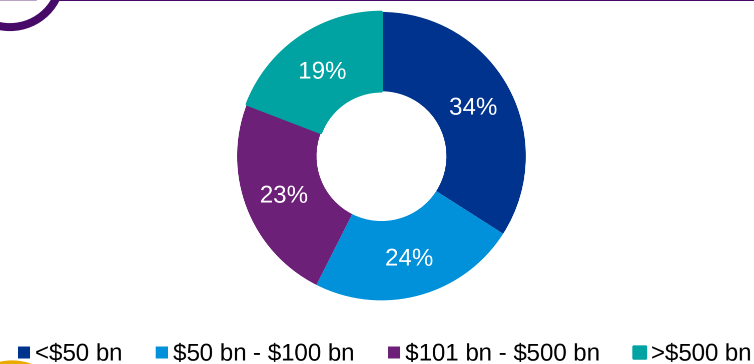
AML / Compliance professionals, who responded to the survey represent banks with varying asset sizes and overlook different types of businesses…

The respondents included a wide representation of significant banks with varying asset sizes (less than $50 billion to over $ 500 billion) covering Domestic Banks, Universal Banks, Domestic Systemically Important Banks (D-SIB) and Global Systemically Important Banks (G-SIB) across Europe.

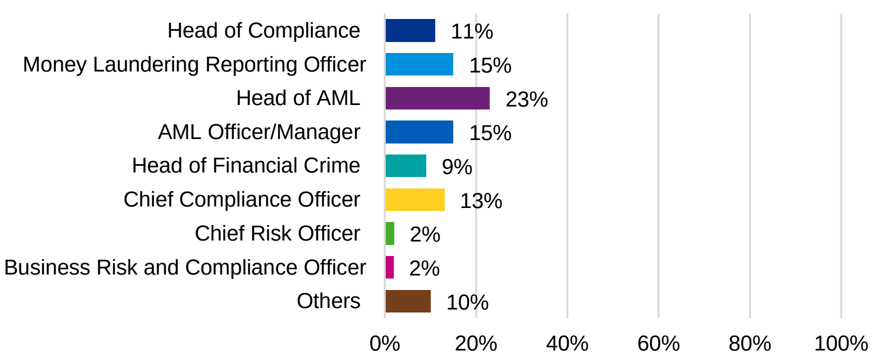
Types of banks



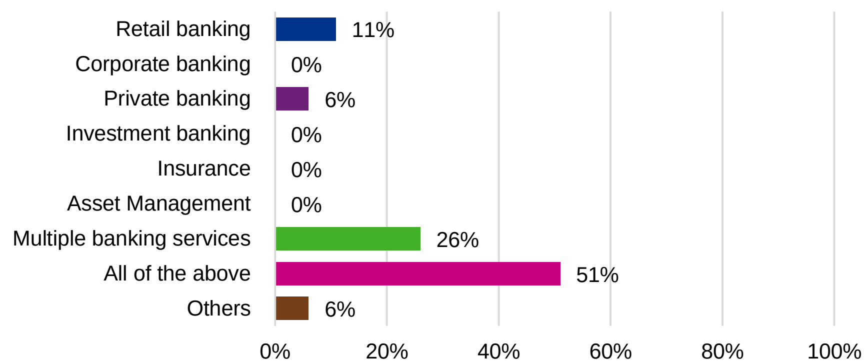
Assets size of banks



Respondents‘ profile



Types of businesses



2. About the survey

The survey covers seven topics related to AML including other key aspects...

The AML benchmarking survey ("survey") is designed to gain insights on the following industry applied AML practices and other related aspects:

1 Roles & Responsibilities of 1LOD & 2LOD

- Alignment of responsibilities between 1st and 2nd LoD
- Barriers to defining clear roles and responsibilities between 1st and 2nd LoD
- Drivers of change in responsibilities of 1st or 2nd LoD

2 AML Budget Investment

- Investment in strengthening 1LOD and 2LOD responsibilities compared to three years ago
- Areas of AML budget investment

3 Compliance Resource Allocation

- Maximum resources allocated for the work in compliance
- % of headcount of FCC in relation to the firm
- % of headcount of FCC in relation to the compliance division

4 Automation and Use of Technology

- Use of automated solutions or new technologies
- Automated solutions or new technologies developed in-house or provided by an external vendor

5 Vendor Solutions for AML

- Preferred vendor solutions/vendors used for combating AML activities
- Main challenges being faced with vendor solutions

6 Fraud and Bribery & Corruption practices

- Most effective ways of detecting fraud within your firm
- Main factors facilitating bribery and corruption practices

7 Suspicious Activity Reports Conversion Rate

- Best estimate for conversion rate of alerts to Suspicious Activity Reports (SAR)

3. Key observations & considerations

1 Roles & Responsibilities of 1LoD & 2LoD

Poor data quality is one of the main barrier to defining clear roles & responsibilities between 1LoD & 2LoD related to AML work.

Review of allocation of responsibilities between 1LoD & 2LoD

~50%

of total respondents confirmed that they are currently reviewing the allocation of responsibilities between 1LoD and 2LoD related to AML work.

Degree of cooperation between 1LoD & 2LoD

Cooperation model:

Responsibilities which should be allocated to the 1LoD…

Ensure data quality

52%

of banks* indicated that data quality responsibilities related to AML work should be allocated to 1LoD.

Perform periodic CDD/EDD

39%

of banks* mentioned that periodic CDD/EDD activities should be allocated to 1LoD.

Develop control measures

35%

of banks* mentioned development of control measures should be allocated to 1LoD.

Barriers to defining clear responsibilities**

Data quality issues	Inadequate IT infrastructure	Bureaucratic processes
50%	47%	47%

Drivers for change in responsibilities**

Regulatory pressure	Group mandate (eg:CoE)	Cost considerations
79%	45%	33%

* % of banks which are reviewing the allocation of responsibilities between 1LoD & 2LoD ** % of total respondents

Key considerations

Improve data management

Poor data quality is one of the biggest contributor that is posing challenge in defining clear responsibilities between 1LoD & 2LoD. Banks should consider to implement robust data governance framework so as to eliminate ambiguity in the responsibilities among various functions.

Enhance IT infrastructure

Implement integrated and automated AML systems for CDD/KYC, watchlist screening, transaction monitoring and reporting, so that all of these work together in a seamless fashion and thereby streamline responsibilities among various functions.

Harmonise various processes

Move away from siloed processes to more harmonized processes so as to avoid redundant activities and complicated bureaucratic system giving rise to vague roles and responsibilities.

2 AML Budget Investment

One fourth of respondents indicated upto 100% increase in AML budget investment compared to 3 years ago (i.e. CtB budget increase)

AML budget investment

~100%

One fourth of total respondents indicated around 100% increase in AML budget investment compared to 3 years ago.

Areas of AML budget investment

Systems enhancements	KYC review / updates	Regulatory/ group updates
79%	79%	70%

3 Compliance Resource Allocation

More than 50% of headcount in compliance represents Financial Crime Compliance (FCC) headcount

Areas where maximum resources are allocated

Rank	
#1	Controls
#2	Standards
#3	Advisory

FCC Headcount

Portion of FCC headcount out of overall Firm's Headcount :	Portion of FCC headcount out of overall headcount in Compliance :
Within the range of 0% to less than 10%	More than 50%

Key considerations

Review AML investments

Significant amount of money continue to be spent on enhancing systems for activities such as transaction monitoring. Senior management should consider to review whether these investments are yielding desired returns.

Regulatory change management

Regulatory action related to AML continue to gain traction. It is increasingly vital for banks to deploy integrated and automated solution which can track the regulatory changes swiftly across jurisdictions so as to reduce cost and improve compliance obligations.

Adequacy of resources

To establish effective AML program it is important for banks to employ resources where it is required the most. Banks should consider to review resourcing periodically to ensure it is right sized for organization size, complexity and risk.

4 Automation and Use of Technology

Vast majority of respondents confirmed investments in automated solutions or new technologies to improve overall AML framework.

Investment in automated solutions or new technologies *

~90%

of total respondents confirmed investment in automated solution or new technologies to improve overall AML framework.

Solutions developed in-house or provided by an external vendor **

50%

of respondents mentioned that automated solution or new technologies are provided by an external vendor with required modifications.

5 Vendor Solutions for AML

For vendor solutions, cost consideration and integration issues with firm's in-house systems are identified as main challenges.

Banks' commonly used vendor solutions/ vendors

Few examples:

sas | FICO | NICE · ACTIMIZE

Challenges faced with vendor solutions

Integration issues	Cost considerations	Lack of flexibility
62%	55%	36%

* % of total respondents

** % of respondents which are investing in automated solutions or new technologies

Key considerations

Third party management

Before partnering with a third-party entity, bank should conduct robust due diligence of the entity not only during onboarding phase, but also on a periodic basis. It is imperative that the due diligence process takes into consideration financial, reputational, operational, legal & regulatory risks.

AI & ML augmented solutions

Banks should consider to enrich the existing tools and systems deployed for combating AML risk with emerging technologies such as Artificial Intelligence (AI) & Machine Learning (ML) in order to increase the efficiency of screening systems. However, it is essential to understand that such solutions will not entirely replace "human judgement".

Management of emerging threats

When deploying new solutions, banks should establish adequate measures in order to mitigate the ever increasing threat from cyber enabled criminals. It is important, to regularly update AML detection models and systems due to rapidly changing consumer behavior as a side effect of the ongoing pandemic.

6 Fraud & ABC practices

Majority of banks confirmed that inadequate policies, procedures and controls are giving rise to bribery and corruption practices

Three effective ways of detecting fraud

1. IT controls	2. Periodic trainings	3. Data analytics
60%	57%	51%

Top factors facilitating bribery and corruption practices

Inadequate policies /procedures/ controls	Acceptable norm	Weak law enforcement
77%	40%	36%

7 SARs Conversion Rate

0% to 5% as the best estimate for conversion rate of alerts to Suspicious Activity Reports(SARs)

SAR conversion rate

Best estimate for the conversion rate of alerts to Suspicious Activity Reports:

Within the range of 0% to 5%

Key considerations

Review policies and procedures

Senior management should regularly review AML policies and procedures and ensure that these are aligned with regulatory/supervisory guidance, group standards and global and local standards.

Positive AML culture

Bank should continue to maintain positive AML culture within the firm by periodically providing trainings to employees on emerging AML risks such as AML concern stemming from ESG area, ongoing pandemic, emerging technologies, digital finance etc. This will equip them to combat AML risks effectively.

Robust SAR process

Banks should deploy robust framework to report suspicious transactions effectively. Implement emerging technology powered solutions to effectively detect suspicious transactions or abnormal patterns not only to reduce the number of false positives alerts, but also to augment SAR process.

Additional Information

Few points for considerations as quoted by the respondents in the survey so as to enhance the AML program

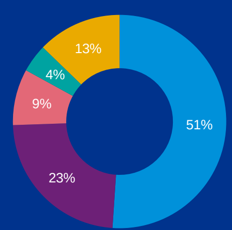
Points highlighted by respondents to improve AML framework

1. Moving away from the culture of "tendency to rely on 2LoD or compliance" for AML work
2. Adequate AML risk oversight by senior management
3. Minimize the knowledge gap related to AML between 1LoD and 2LoD
4. Controls such as KYC overdue, improper handling of alerts etc should be managed by 1LoD.
5. 2LoD to provide standards while 1LoD to implement respective procedures to comply with those standards.
6. Functions with in a AML framework should be approved by the Board.

Periodic review of AML program components

~50%

of total respondents confirmed that they update various components of existing AML program (such as CDD, EDD etc.) on a periodic basis.



Key considerations

Enhance AML risk assessment

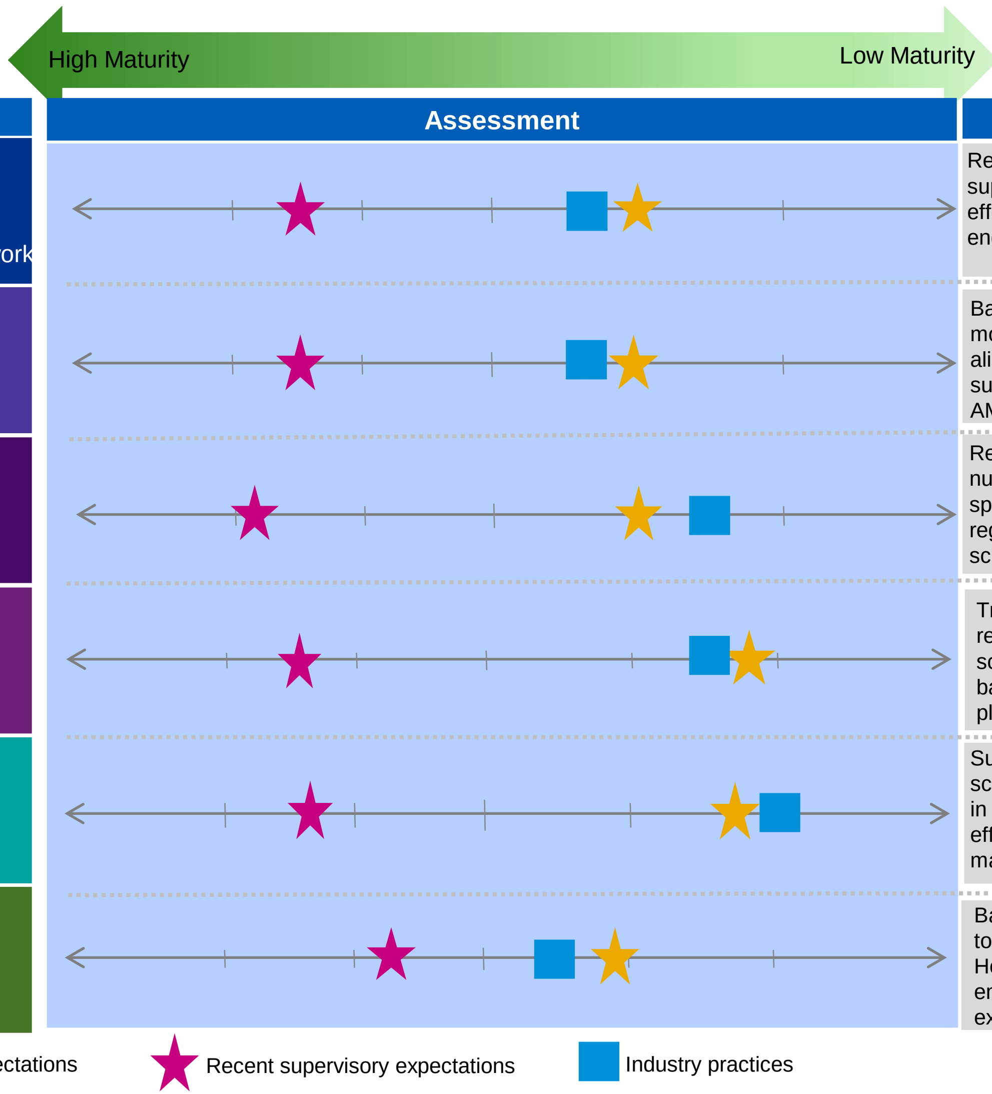
Few key points to consider:

- Establish the framework to assess the firm wide impact of AML risks and systems specifically at the product or business unit level.
- Board and senior management to define metrics which measure whether the results of an AML risk assessment exceeds bank's risk appetite.
- Banks may establish committees or internal bodies, however it is vital that the information reaches to the most senior levels within the firm to ensure they understand the AML risk profile appropriately.
- Conduct periodic coverage assessments to make sure their transaction monitoring programs monitor risks adequately.
- Increase the frequency to perform risk assessment, for instance quarterly instead of annually, due to rapidly changing situation as a result of pandemic and other emerging AML risks.
- Swiftly anticipate and include new risks and move towards forward looking processes.

4. AML program maturity assessment

4. AML program maturity assessment of select components

KPMG analysis - Maturity assessment of selected AML program components



Key components	Remarks
AML governance framework	Recent on-site inspections results disclosed by supervisors indicate banks have to put more efforts to ensure adequate senior management engagement.
Policies & procedures	Banks have policies and procedures in place but more needs to be done to ensure these are aligned with recently published regulatory & supervisory ML/TF guidelines & rapidly changing AML landscape.
CDD/EDD/KYC	Recent penalties levied by regulators on numerous institutions due to weaknesses in this space indicate banks have work to do and regulators/ supervisors will continue to heighten scrutiny in the near future.
Transaction Monitoring	Transaction monitoring is another area where regulators/supervisors have increased their scrutiny significantly. Recent scandals show that banks have to increase their efforts to put in place robust defence mechanisms.
Data Management	Supervisors have significantly heightened scrutiny on banks‘ data management capabilities in the last few years. Banks have to put more efforts to deploy robust end to end data management framework.
Training	Banks have deployed various training programs to increase employees awareness on AML risks. However, banks have to further ensure that employees are adequately trained on AML risks exacerbated by pandemic, digital finance etc.

4. AML program maturity assessment of select components

How banks can prepare and prioritize?...

Enhance data management capabilities

Deploy sound data management framework that enables seamless collection, consolidation and governance of data to meet AML requirements.

Strengthen IT infrastructure

Augment existing system capabilities with cloud computing, AI & ML in order to screen transactions not only to reduce the number of false positives alerts, but also to enhance suspicious activities detection process.

Update policies and procedures

Align policies and procedures with group standards as well as ever changing regulatory /supervisory guidelines and expectations and ensure these are regularly reviewed and approved by the senior management.

Review AML budget investment

Review AML budget investment strategy and develop AML compliance roadmap with a focus on minimizing costs, increasing efficiency and ultimately demonstrating progress towards AML sustainability.

Ensure adequacy of resources

Perform periodic assessment to ensure that teams are adequately resourced and have the requisite subject matter knowledge and experience to perform their job functions in the increasingly evolving AML landscape.

Promote positive AML culture

Maintain positive AML/CFT culture within the firm by periodically providing trainings to employees on emerging ML/TF risks stemming from ESG area, digital finance, emerging technologies and ongoing pandemic.

Few points to keep in mind while transforming AML program…

- **Prudent risk assessment** – Banks should prudently identify the risks inherent in their business, looking at products & services, customers and geography.
- **Comprehensive internal controls review –** Banks should carefully evaluate policies, procedures, and processes with respect to their ability to achieve AML compliance.
- **Independent testing –** It should be performed by internal audit function along with external parties. This should be a risk-based audit that is responsive to a bank's risk profile.
- **Dedicated AML compliance officer (MLRO)** – The compliance officer should be capable of deploying robust AML program, and ensure that the senior management be aware of the bank's compliance status.

5. Annex

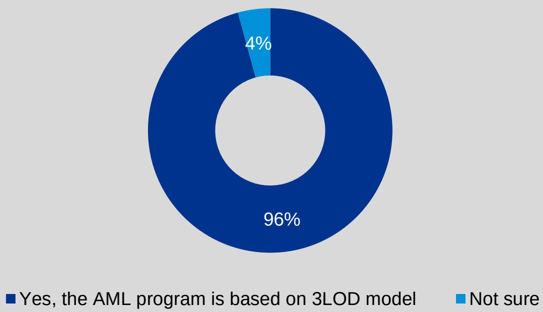
5.1 Detailed findings of the survey

5.1 Detailed findings of the survey

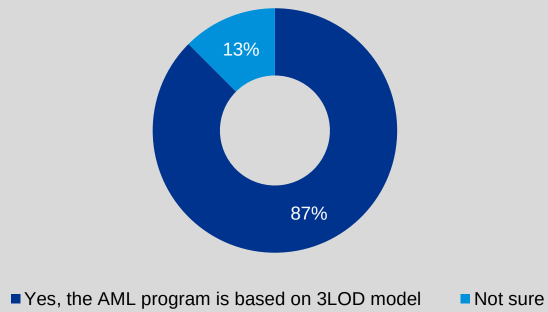
Almost all banks confirmed that their AML governance framework is based on a three lines of defense (3LOD) model…

Is the AML program in your bank based on a "three lines of defense" model?

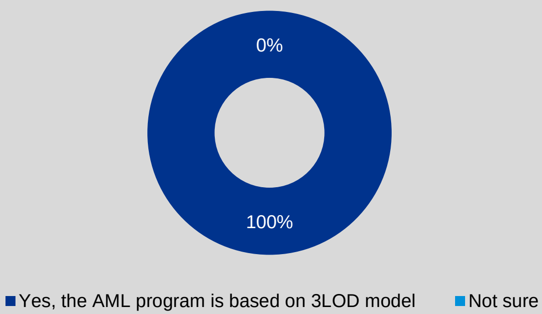
Total responses



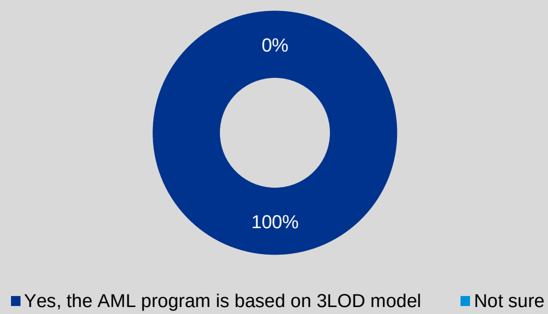
Banks with total assets <$50 bn



Banks with total assets $50 bn - $500 bn



Banks with total assets >$500 bn



KPMG Comments

- Almost all banks responded that their AML program is based on the 3LOD model
- To combat ML/TF risks effectively, it is essential to implement a strong AML/CFT governance framework such as the three lines of defense model.

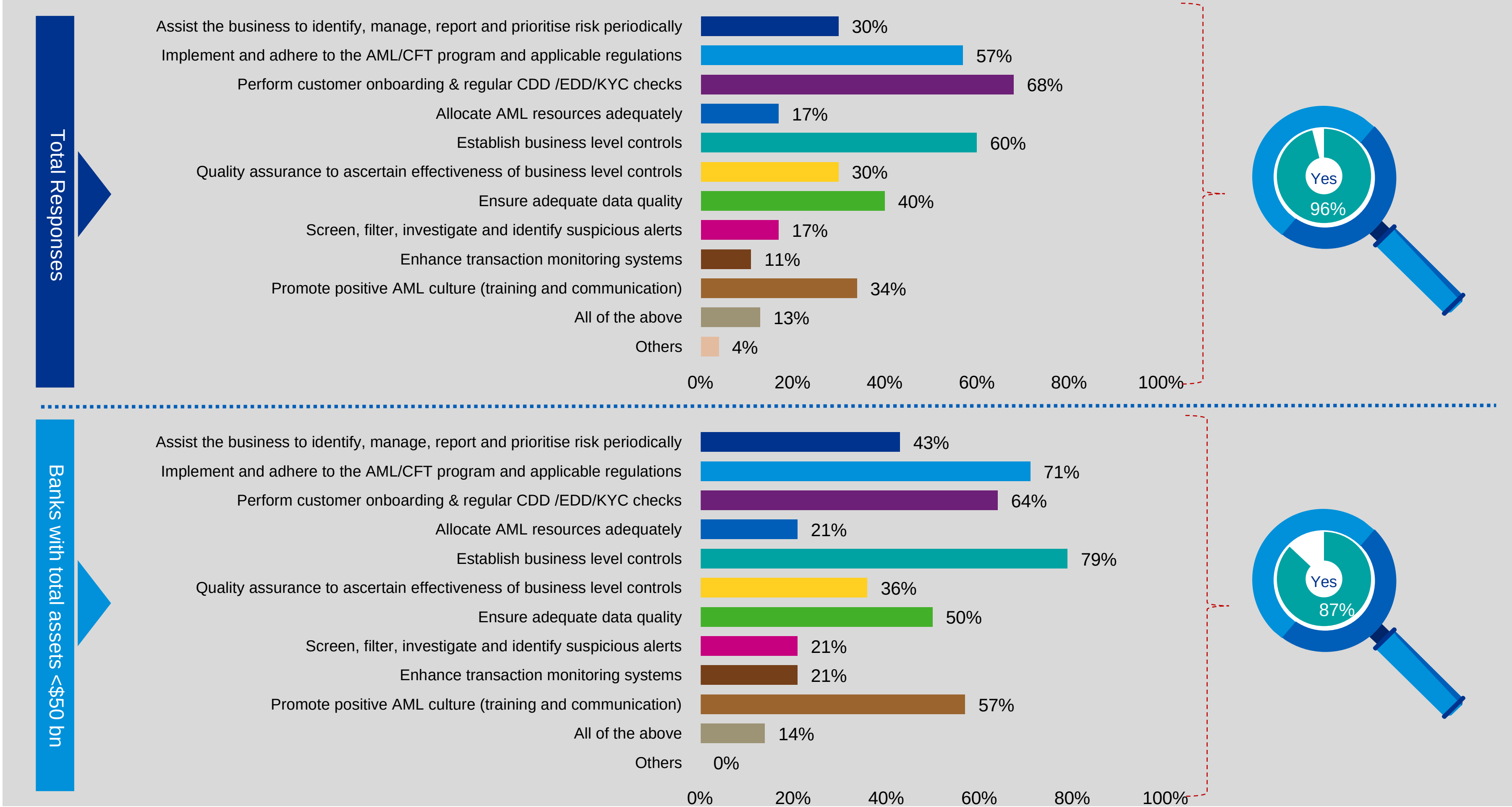
Select regulatory reference

- "The business lines, as the first line of defense (1LoD), take risks and are responsible for their operational management directly and on a permanent basis.
- The risk management function and compliance function form the second line of defense (2LoD) and facilitates the implementation of a sound risk management framework through out the firm.
- The independent internal audit function, as the third line of defense (3LoD) is in charge of the independent review of the first two lines of defense." - EBA

5.1 Detailed findings of the survey

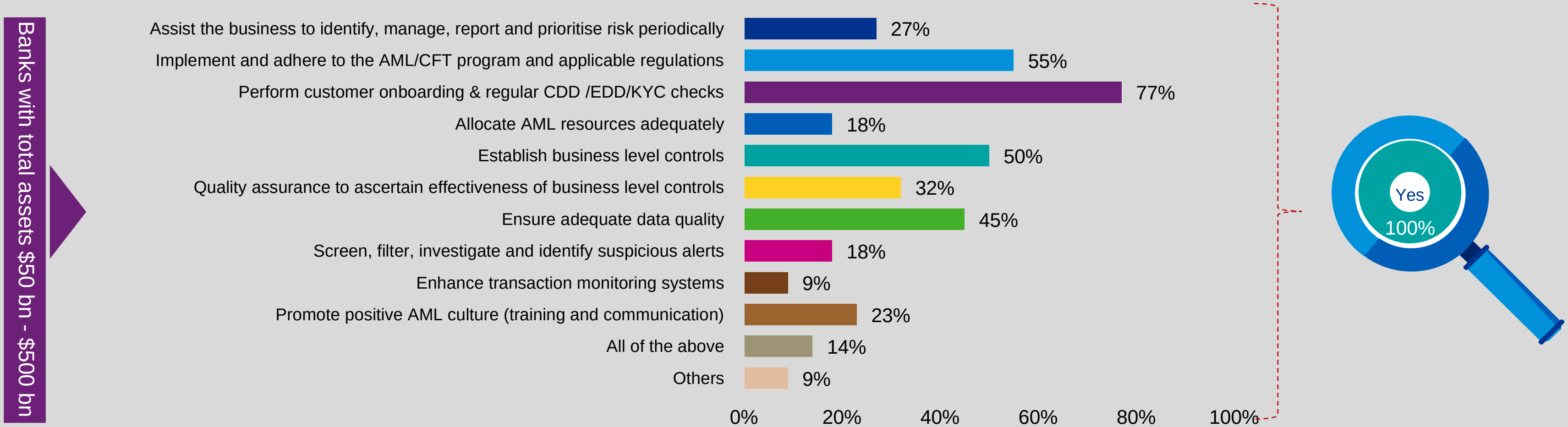
Responsibilities of 1LoD can differ from one bank to another depending on the size, complexity and AML team structure of the bank…

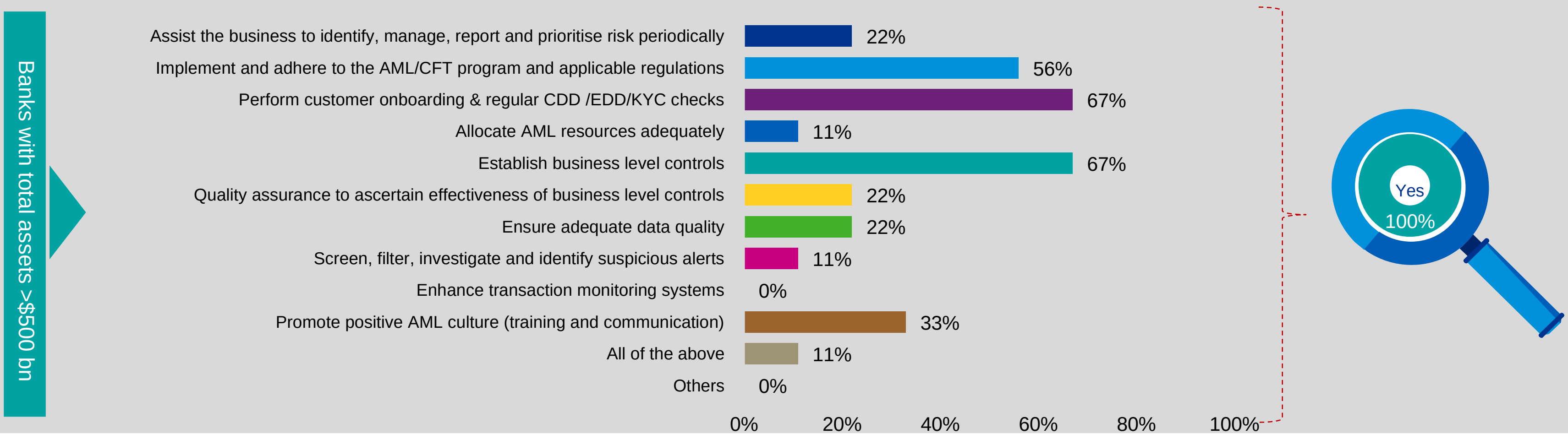
What are the specific responsibilities of the first line of defense (1LoD) in your bank?



Responsibilities of 1LoD can differ from one bank to another depending on the size, complexity and AML team structure of the bank…

What are the specific responsibilities of the first line of defense (1LoD) in your bank?

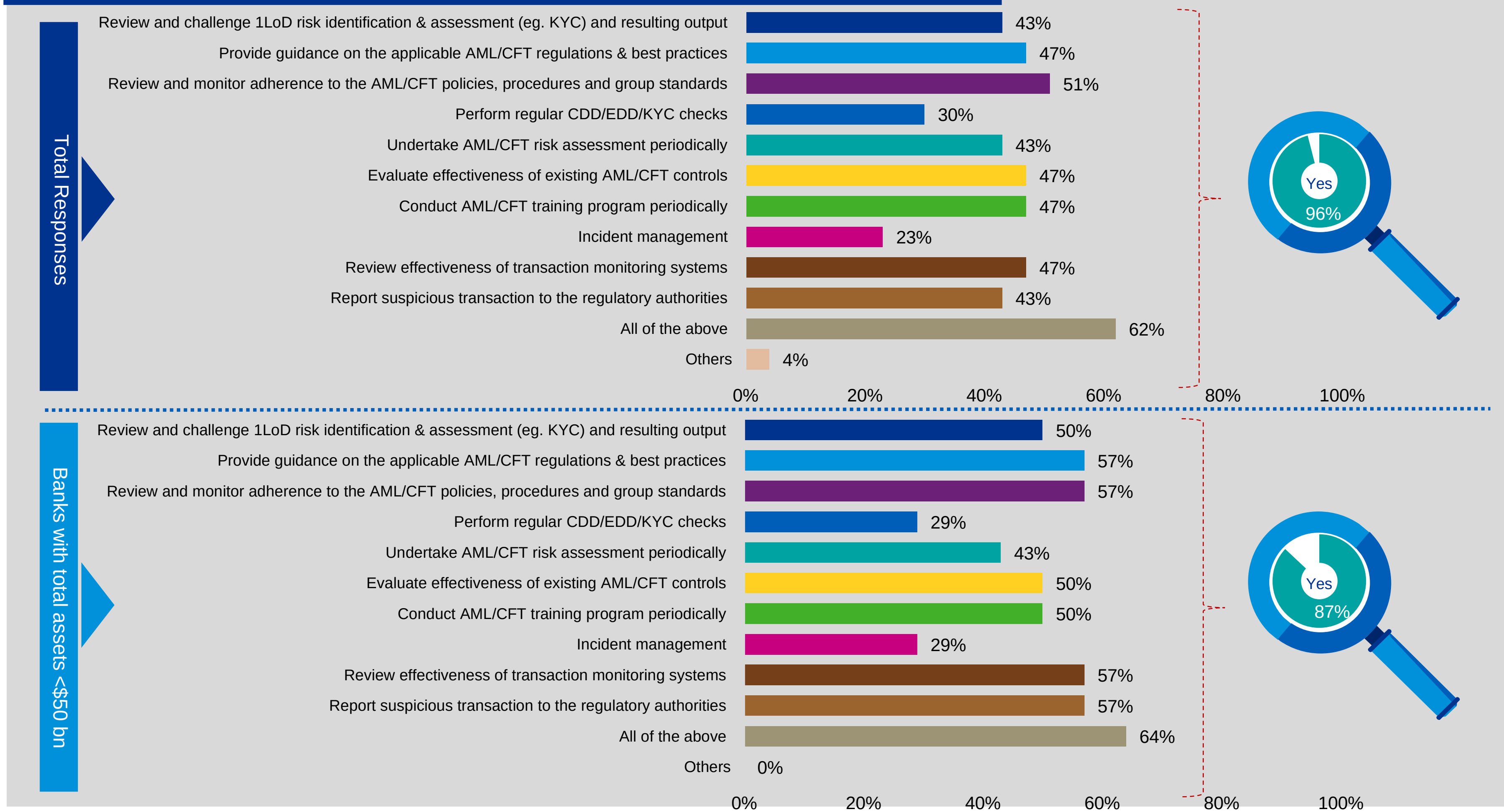




5.1 Detailed findings of the survey

Responsibilities of 2LoD can differ from one bank to another depending on the size, complexity and AML team structure of the bank…

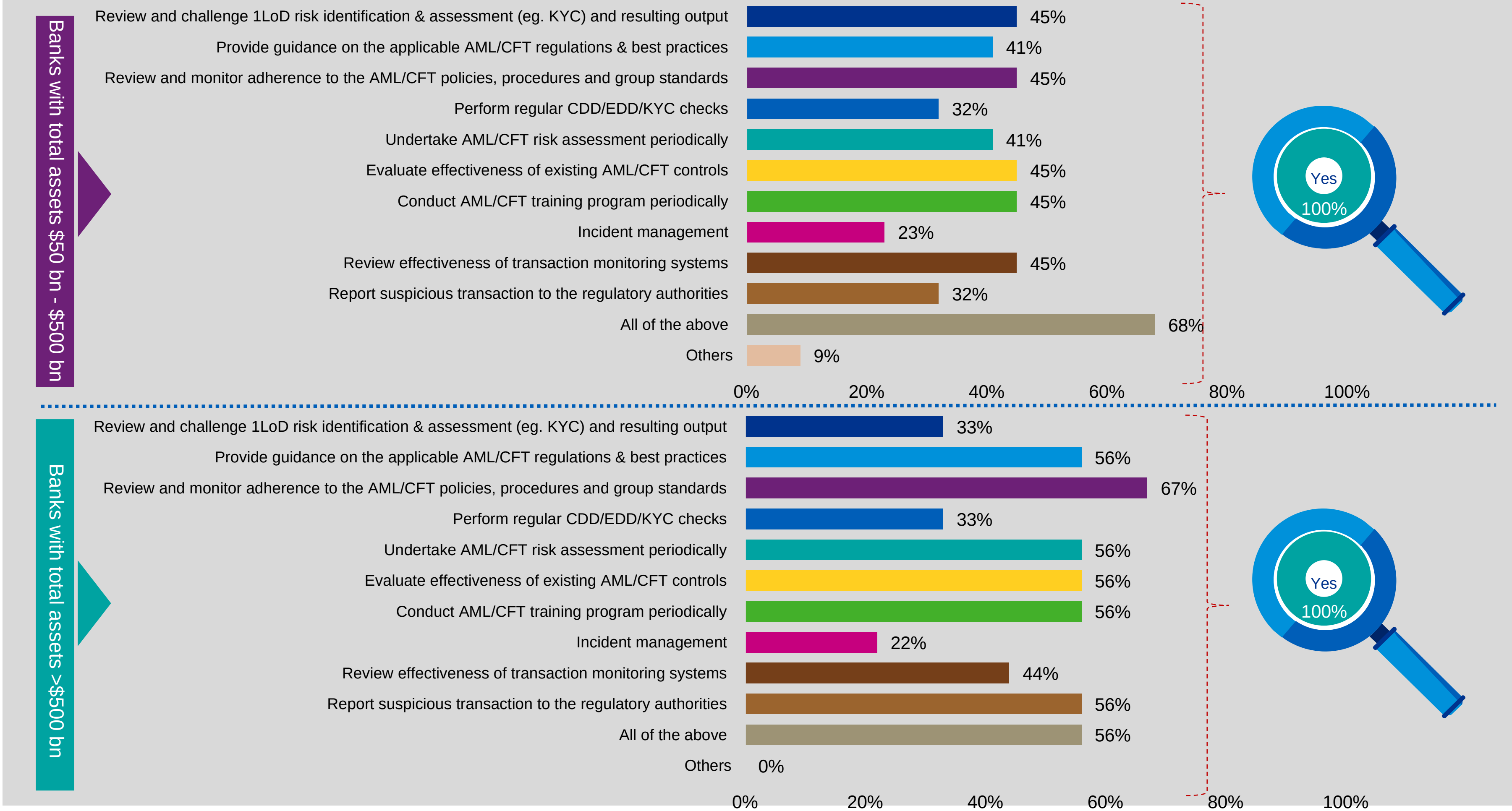
What are the specific responsibilities of the second line of defense (2LoD) in your bank?



5.1 Detailed findings of the survey

Responsibilities of 2LoD can differ from one bank to another depending on the size, complexity and AML team structure of the bank…

What are the specific responsibilities of the second line of defense (2LoD) in your bank?

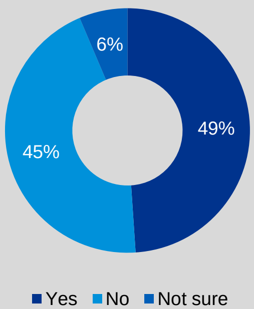


5.1 Detailed findings of the survey

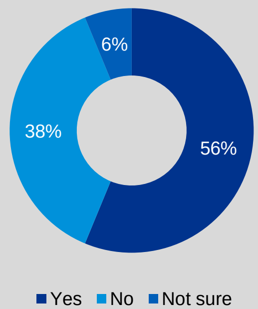
The difference in distribution of results among small, medium and large banks indicate the maturity of the AML governance framework at the large banks…

Are you currently reviewing allocation of responsibilities between 1LoD and 2LoD in your bank?

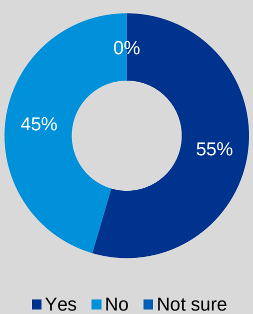
Total responses



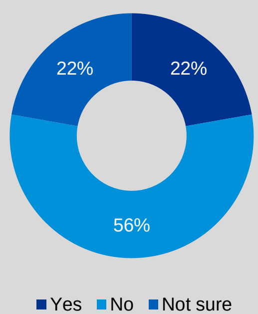
Banks with total assets <$50 bn



Banks with total assets $50 bn - $500 bn



Banks with total assets >$500 bn



KPMG Comments

Total responses

Nearly 50% of total respondents indicated that they are currently reviewing allocation of responsibilities between 1LoD & 2LoD related to AML work. The distribution of results is different for the large banks (assets size >$500 bn) when compared with the small banks and the medium banks. Several factors contribute to this difference, such as the **maturity of the AML governance framework at the large banks when compared with the small and the large banks.**

Small banks

Medium banks

More than half of the small banks and the medium banks confirmed that they are currently reviewing allocation of responsibilities between 1LoD & 2LoD related to AML work.

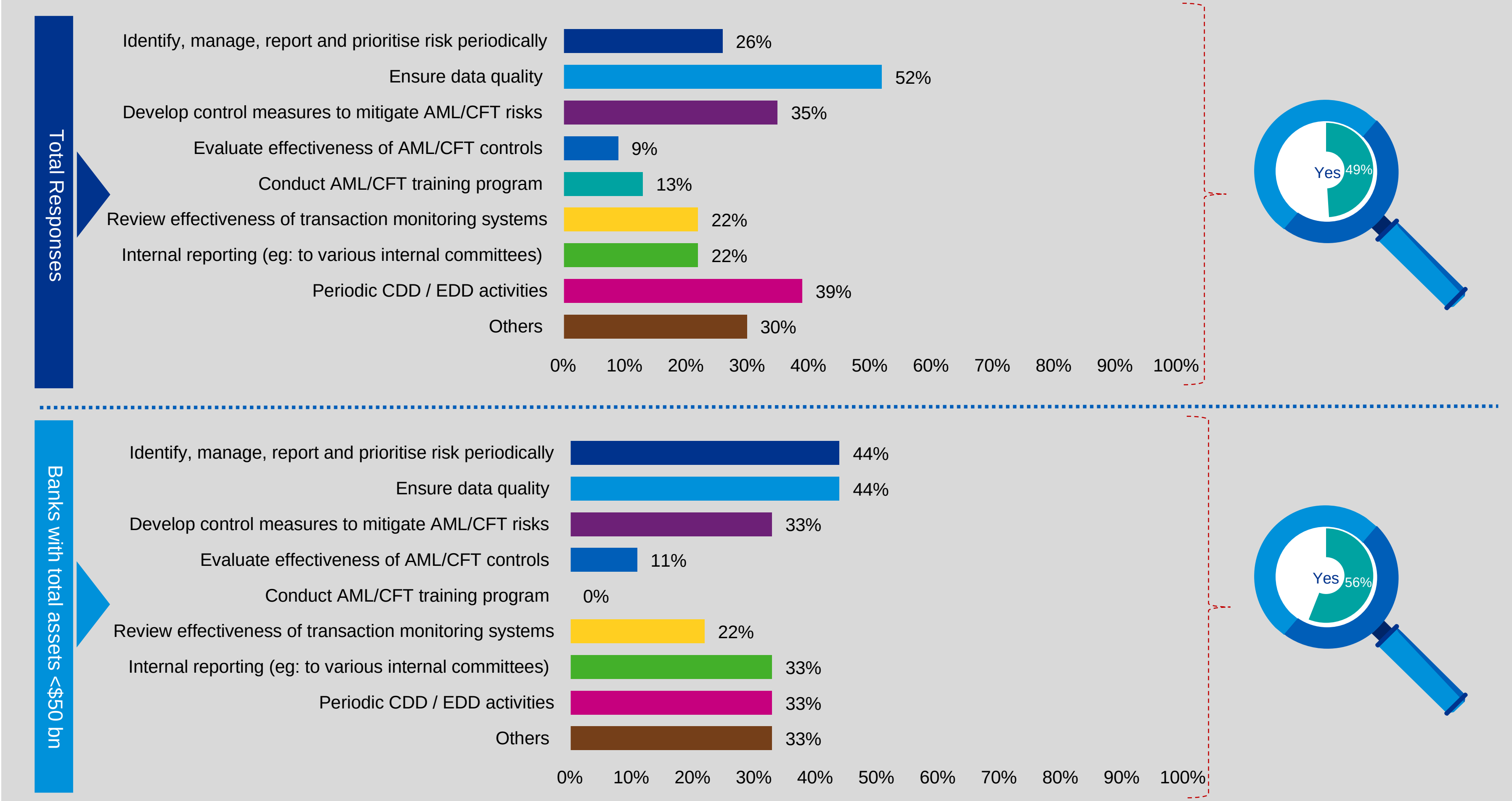
Large banks

Only few large banks confirmed that that they are currently reviewing allocation of responsibilities between 1LoD & 2LoD related to AML work.

5.1 Detailed findings of the survey

Many respondents confirmed that data quality responsibilities related to AML work should be allocated to 1LoD.

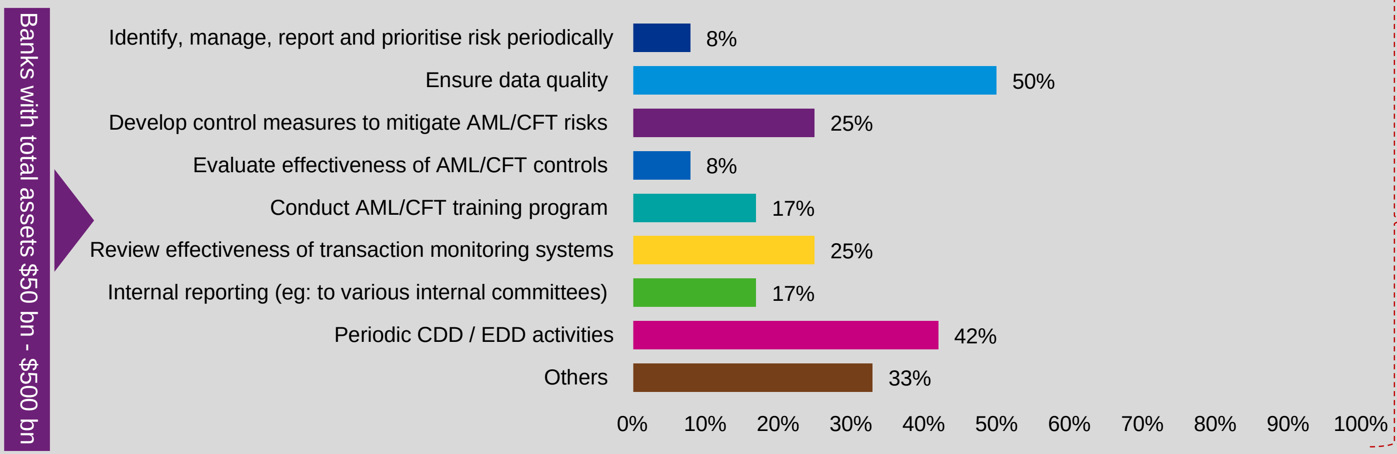
If yes, are there responsibilities which should be reallocated to the first line of defense (1LoD) in your bank?

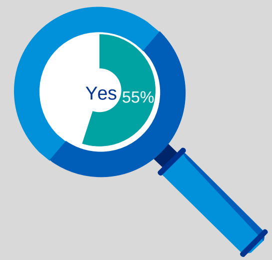


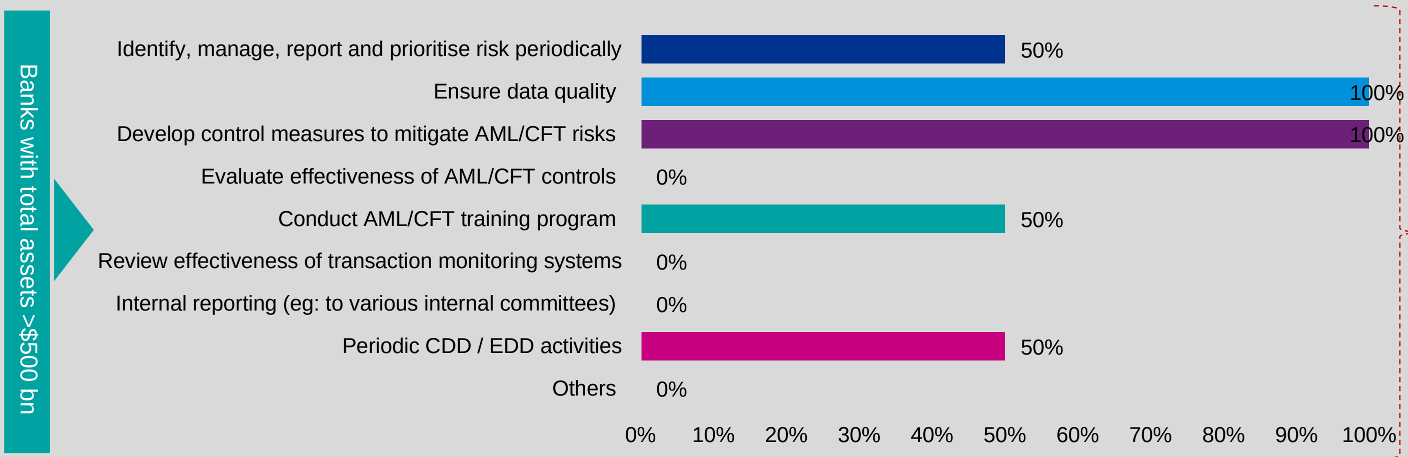
5.1 Detailed findings of the survey

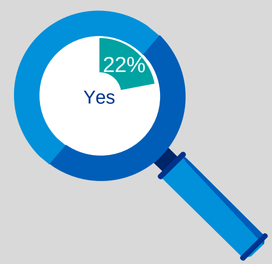
Many respondents confirmed that data quality responsibilities related to AML work should be allocated to 1LoD.

If yes, are there responsibilities which should be reallocated to the first line of defense (1LoD) in your bank?



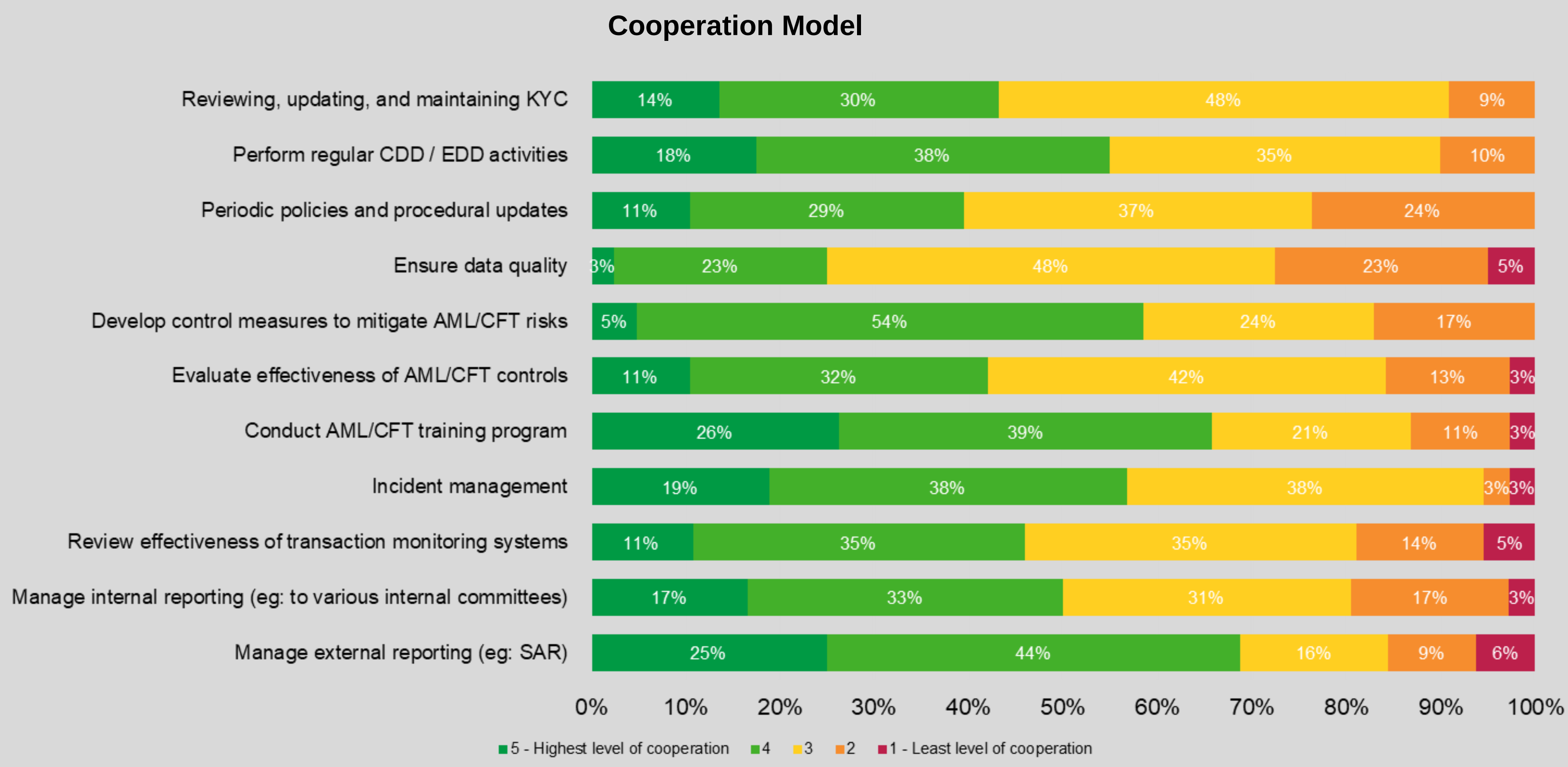






High level of cooperation between 1LoD & 2LoD in conducting AML trainings whereas low level of cooperation when comes to ensuring data quality…

To which degree there is a "cooperation model" between the first line of defense and the second line of defense in your bank regarding the given areas below;

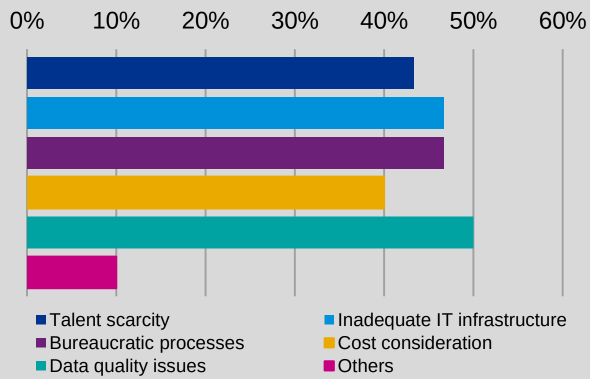


Note: Analysis on the basis of responses received

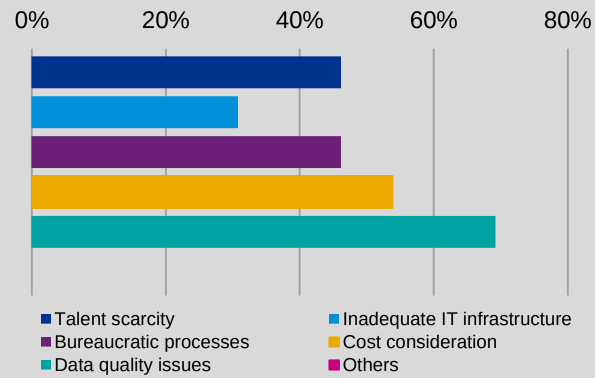
Total respondents indicated data quality issues as one of the main barrier to defining clear roles & responsibilities between 1LoD & 2LoD …

What are the biggest barriers to defining clear roles and responsibilities between first line of defense and second line of defense in your bank?

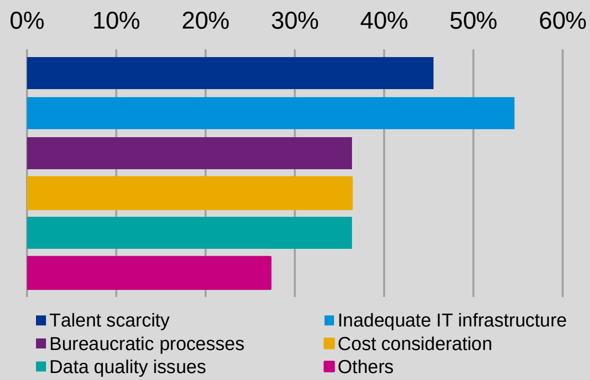
Total responses



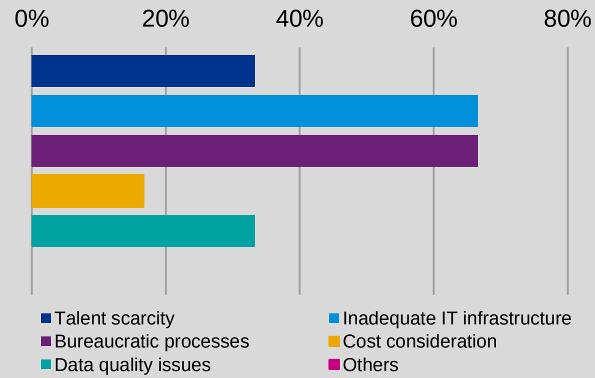
Banks with total assets <$50 bn



Banks with total assets $50 bn - $500 bn



Banks with total assets >$500 bn



Note: Analysis on the basis of responses received

KPMG Comments

Total responses

Around 50% of respondents indicated that poor data quality, bureaucratic processes and inadequate IT infrastructure are the main barriers to clearly defining roles and responsibilities between 1LoD & 2LoD.

Small banks

For the small banks, data quality issues is one of the main barrier to clearly defining roles and responsibilities between 1LoD & 2LoD.

Medium banks

For the medium banks, inadequate IT structure is one of the main barrier to clearly defining roles and responsibilities between 1LoD & 2LoD. Other barriers include AML culture i.e. tendency to rely only on 2LoD/compliance for AML work.

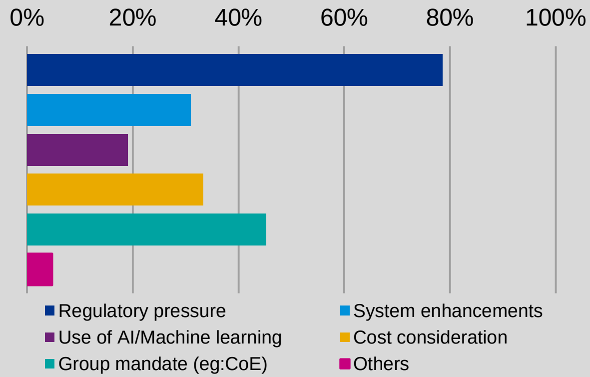
Large banks

For the large banks, inadequate IT structure and bureaucratic processes are the main barriers to clearly defining roles and responsibilities between 1LoD & 2LoD.

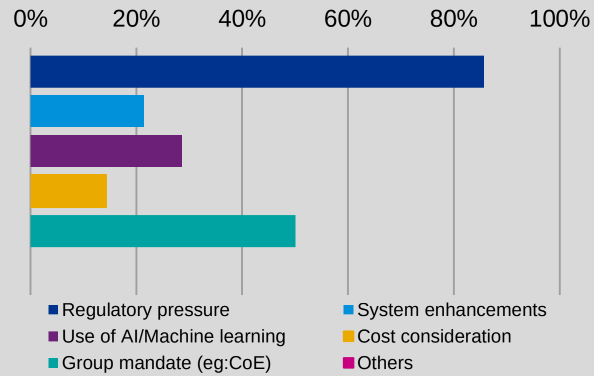
Regulatory pressure as one of the main driver for change in responsibilities of 1LoD or 2LoD…

What is driving the change in responsibilities of first line of defense or second line of defense in your bank?

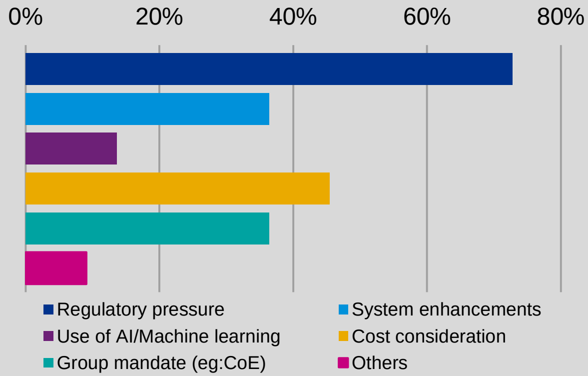
Total responses



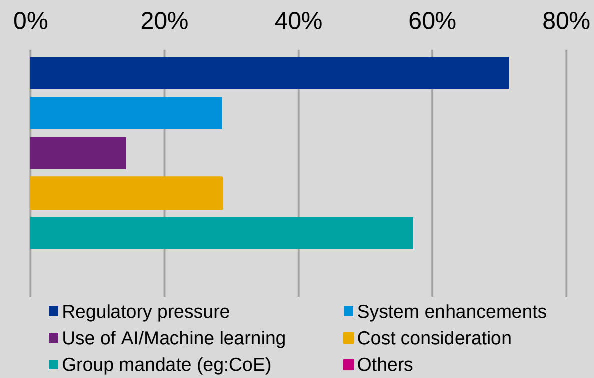
Banks with total assets <$50 bn



Banks with total assets $50 bn - $500 bn



Banks with total assets >$500 bn



Note: Analysis on the basis of responses received

KPMG Comments

Total responses

Majority of respondents indicated that regulatory pressure, senior management or group mandate (eg:CoE) and cost considerations are the main drivers for change in responsibilities of 1LoD or 2LoD.

Small banks

For the small banks, other than regulatory pressure and group mandate it is interesting to note that use of AI/ ML also acting as a driver for change in responsibilities of 1LoD or 2LoD.

Medium banks

For the medium banks, other than regulatory pressure and cost considerations it is interesting to note that system enhancements & group mandates (e.g.: CoE) are also acting as drivers for change in responsibilities of 1LoD or 2LoD.

Large banks

For the large banks, the distributions of results is very similar to the results of total responses.

Within the 1LoD the AML team typically is a part of first line controls/ oversight team…

Where in the first line of defense does the AML team sit?

KPMG Comments

Total responses | Small banks | Medium banks | Large banks

The distribution of results is almost similar for all the types of banks i.e. small, medium and large.

Majority of respondents indicated that within the 1LoD the AML team typically is a part of first line controls/ oversight team.

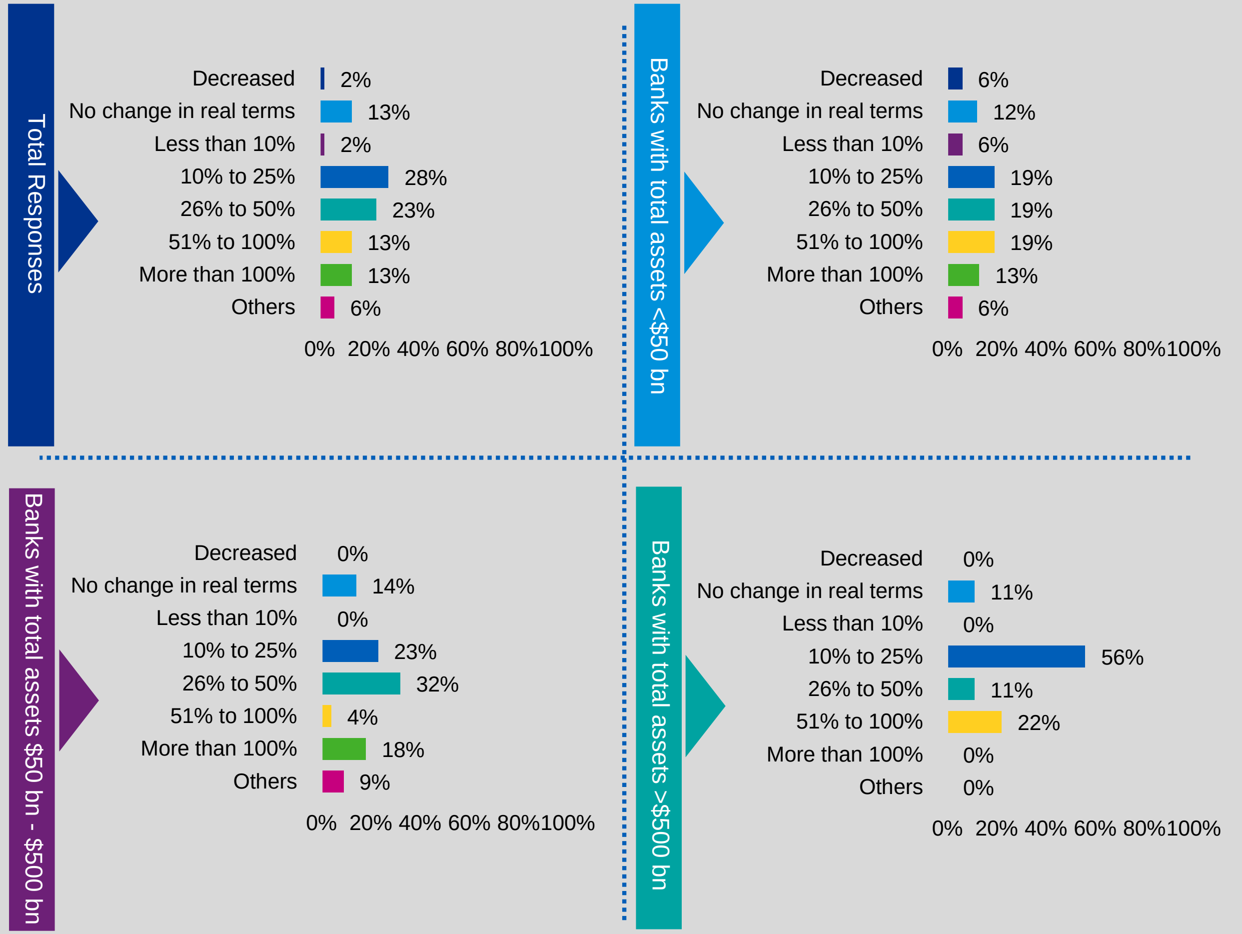
Few of the banks indicated that within the 1LoD the AML team is part of both the first line controls/ oversight team as well as the operational center of excellence.

Other examples as indicated by the respondents include – the AML team as part of centralized KYC Teams within the 1st Line of Defense.

5.1 Detailed findings of the survey

One fourth of respondents indicated upto ~100% increase in AML budget investment compared to three years ago…

How much has total investment in strengthening 1LOD and 2LOD responsibilities to mitigate AML/CFT risks increased compared to three years ago?



KPMG Comments

Total responses

Around 80% percent of survey respondents reported increases in their total investment in AML activity, with 26 percent of respondents indicating upto ~100% increases in AML investment compared to 3 years ago.

Small banks / Medium banks

The small banks and the medium banks have confirmed the most significant increase in AML investment.

13% of the small banks and 18% of the medium banks have confirmed more than 100% increases in AML investment compared to 3 years ago.

Large banks

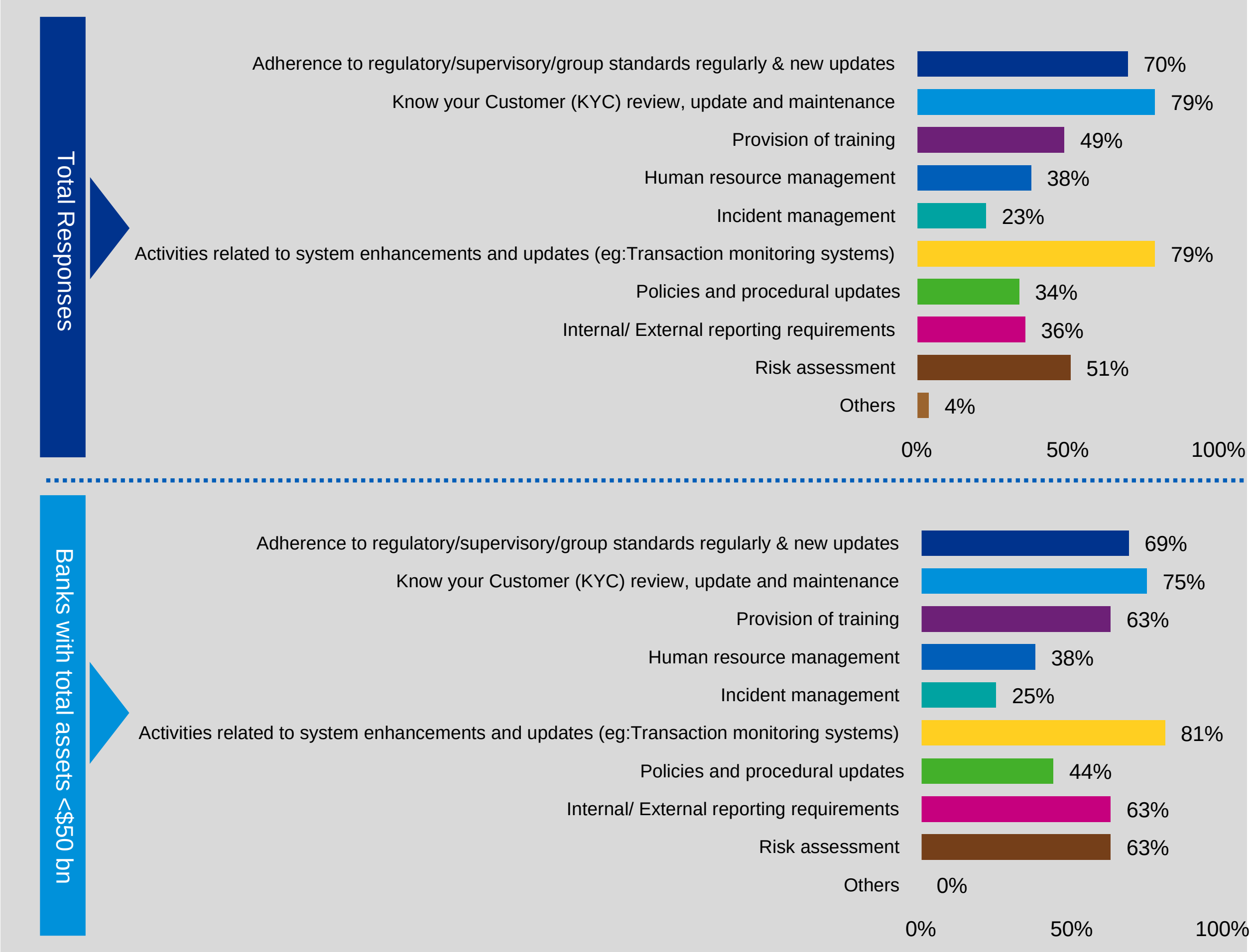
More than 50% of the large banks confirmed 10% to 25% increases in AML investment compared to 3 years ago.

From the above, it can be construed that AML program at the large banks is more matured than the AML program deployed at the small and the medium banks.

5.1 Detailed findings of the survey

Main areas of AML budget investment include system enhancements, KYC review/ update and adherence to regulatory / supervisory /group standards…

What are the areas of AML budget investment for your bank?



KPMG Comments

Total responses

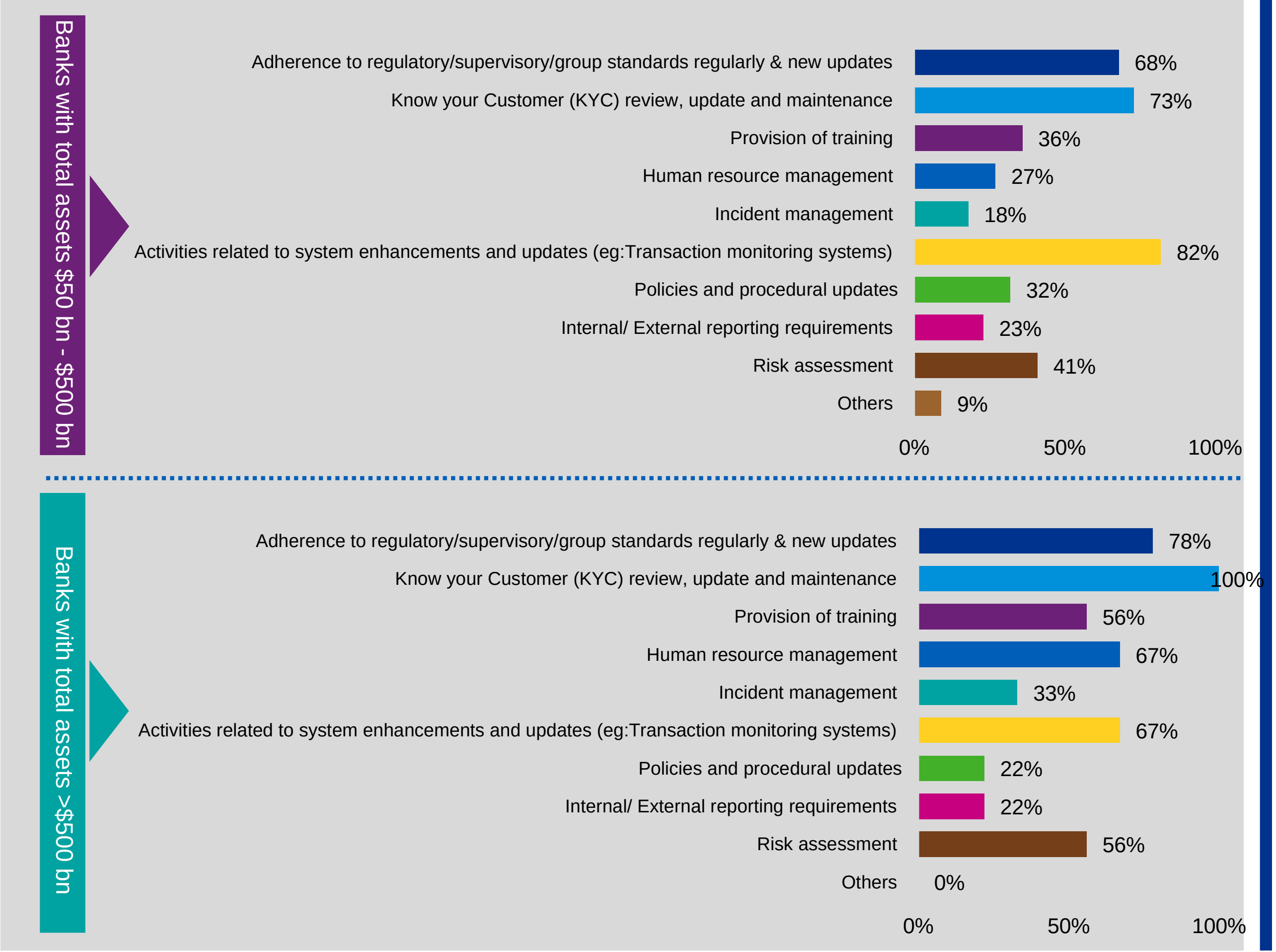
The three main areas of AML investment mentioned by the respondents include: System enhancements, KYC review/ update and adherence to regulatory / supervisory /group standards. The distribution of results is almost similar for the small and the medium banks. However, the results differs slightly **for the large banks, which confirm a large sum of money being invested for KYC review/updates instead of system enhancements.**

Small banks

For the small banks, a large sum of money is being invested in activities related to system enhancements and updates such as Transaction monitoring systems, followed by KYC review, update and maintenance and adherence to regulatory/supervisory/group standards on a ongoing basis and new updates.

Main areas of AML budget investment include system enhancements, KYC review/ update and adherence to regulatory / supervisory /group standards…

What are the areas of AML budget investment for your bank?



KPMG Comments

Medium banks

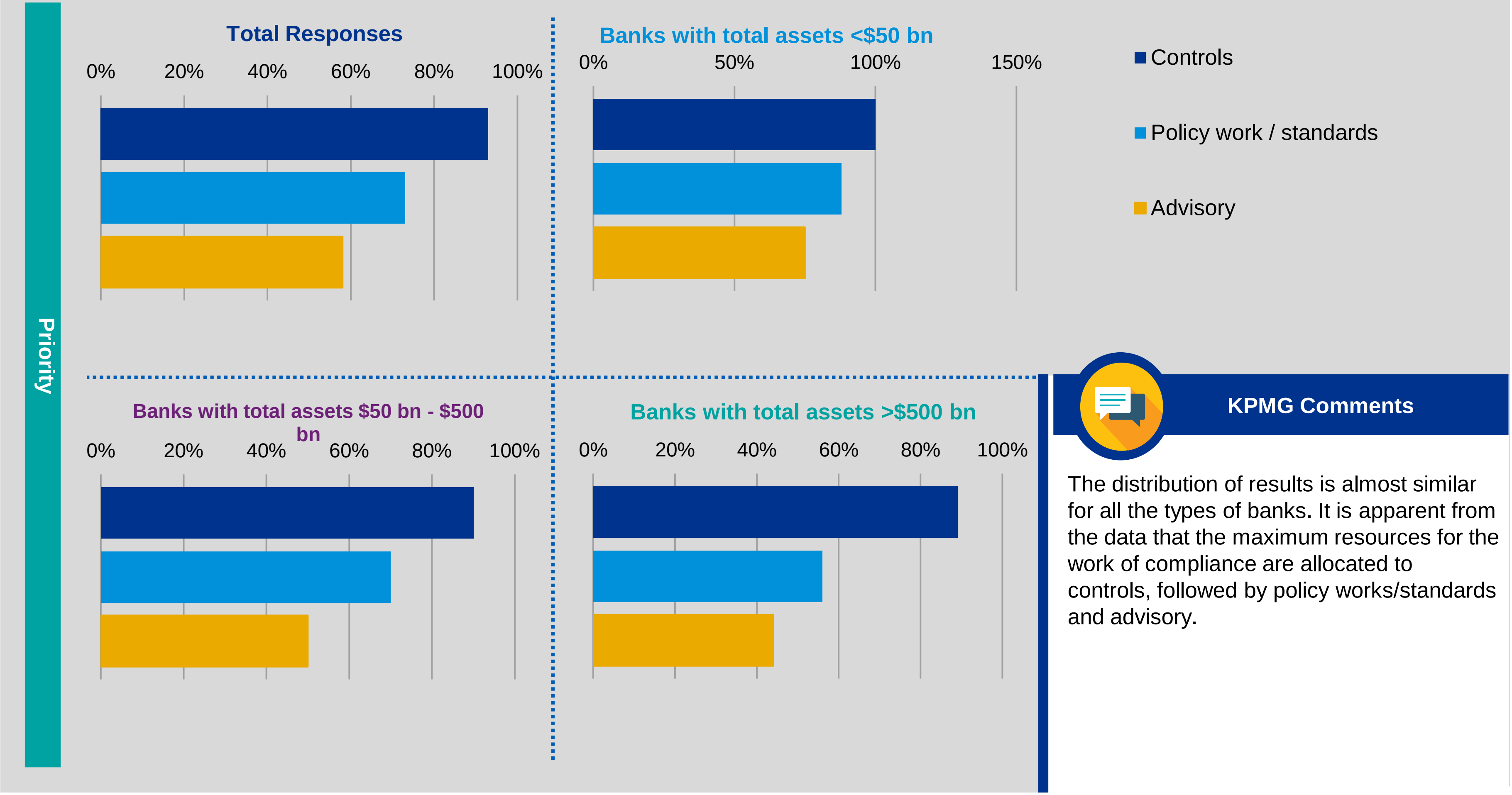
For the medium banks, the distribution of results is almost similar to the small banks i.e. a large sum of money is being invested in activities related to system enhancements and updates such as Transaction monitoring systems, followed by KYC review, update and maintenance and adherence to regulatory /supervisory/group standards on a ongoing basis and new updates.

Large banks

For the large banks, the main area of investment is related to KYC review, update and maintenance followed by activities related to adherence to regulatory /supervisory/ group standards on a ongoing basis and new updates. The investment in enhancing systems is slightly less, when compared with the small banks and the medium banks.

For the work in compliance the maximum resources are allocated to controls, followed by policy work/standards and advisory…

In which area the maximum resources are allocated for the work in compliance for your bank (areas to be listed in the order of priority)?

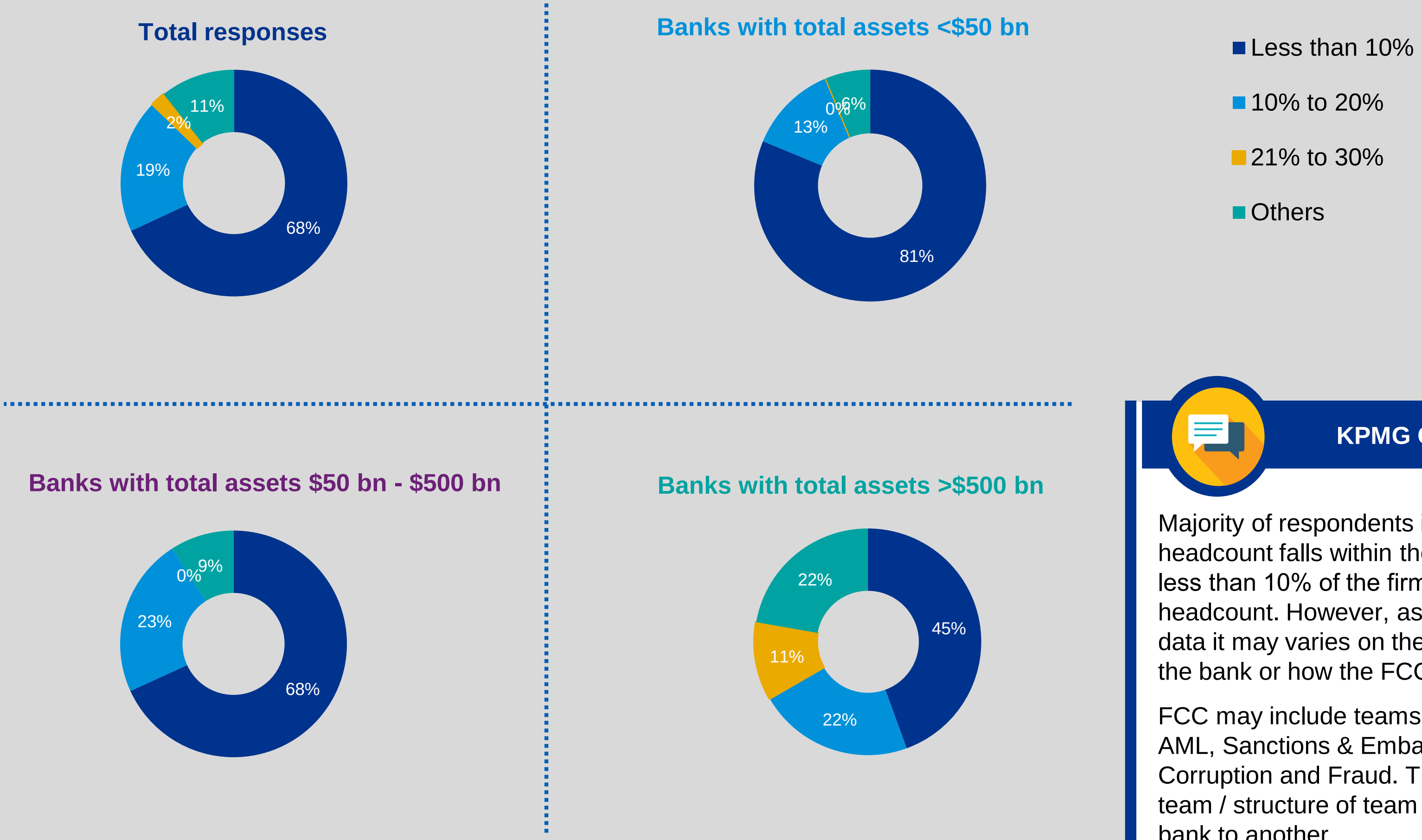


KPMG Comments

The distribution of results is almost similar for all the types of banks. It is apparent from the data that the maximum resources for the work of compliance are allocated to controls, followed by policy works/standards and advisory.

FCC headcount falls within the range of 0% to less than 10% of the firm's overall headcount…

What is the percentage of headcount of Financial Crime Compliance in relation to the bank? (Portion of the FCC headcount out of firm's overall headcount)



KPMG Comments

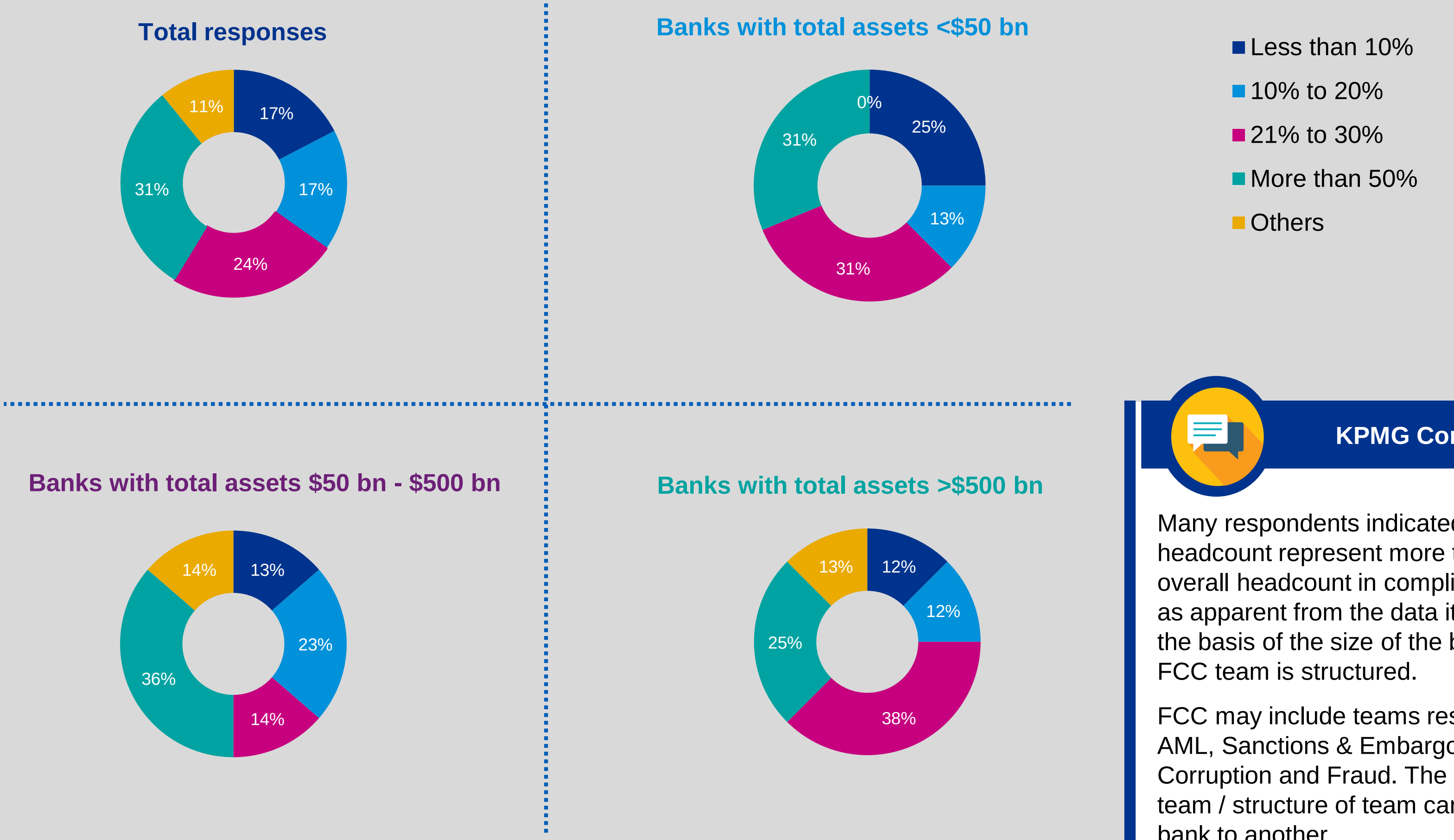
Majority of respondents indicated that FCC headcount falls within the range of 0% to less than 10% of the firm's overall headcount. However, as apparent from the data it may varies on the basis of the size of the bank or how the FCC team is structured.

FCC may include teams responsible for AML, Sanctions & Embargoes, Bribery & Corruption and Fraud. The composition of team / structure of team can differ from one bank to another.

5.1 Detailed findings of the survey

Many banks confirmed more than 50% of overall headcount in compliance represent FCC

What is the percentage of headcount of Financial Crime Compliance in relation to the compliance? (Portion of FCC headcount out of overall headcount in Compliance)



KPMG Comments

Many respondents indicated that FCC headcount represent more than 50% of the overall headcount in compliance. However, as apparent from the data it may varies on the basis of the size of the bank or how the FCC team is structured.

FCC may include teams responsible for AML, Sanctions & Embargoes, Bribery & Corruption and Fraud. The composition of team / structure of team can differ from one bank to another.

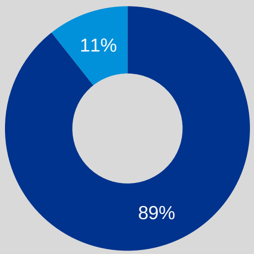
5.1 Detailed findings of the survey

Vast majority of respondents confirmed investments in automated solutions or new technologies to improve overall AML framework.

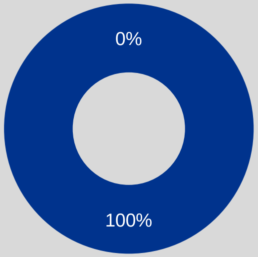
Is your bank investing in automated solutions or new technologies to improve overall AML framework?

■ Yes ■ No

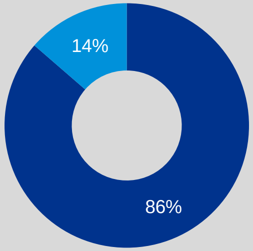
Total responses



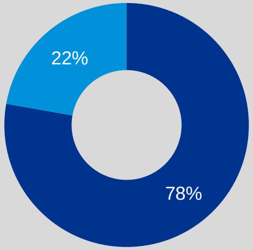
Banks with total assets <$50 bn



Banks with total assets $50 bn - $500 bn



Banks with total assets >$500 bn



KPMG Comments

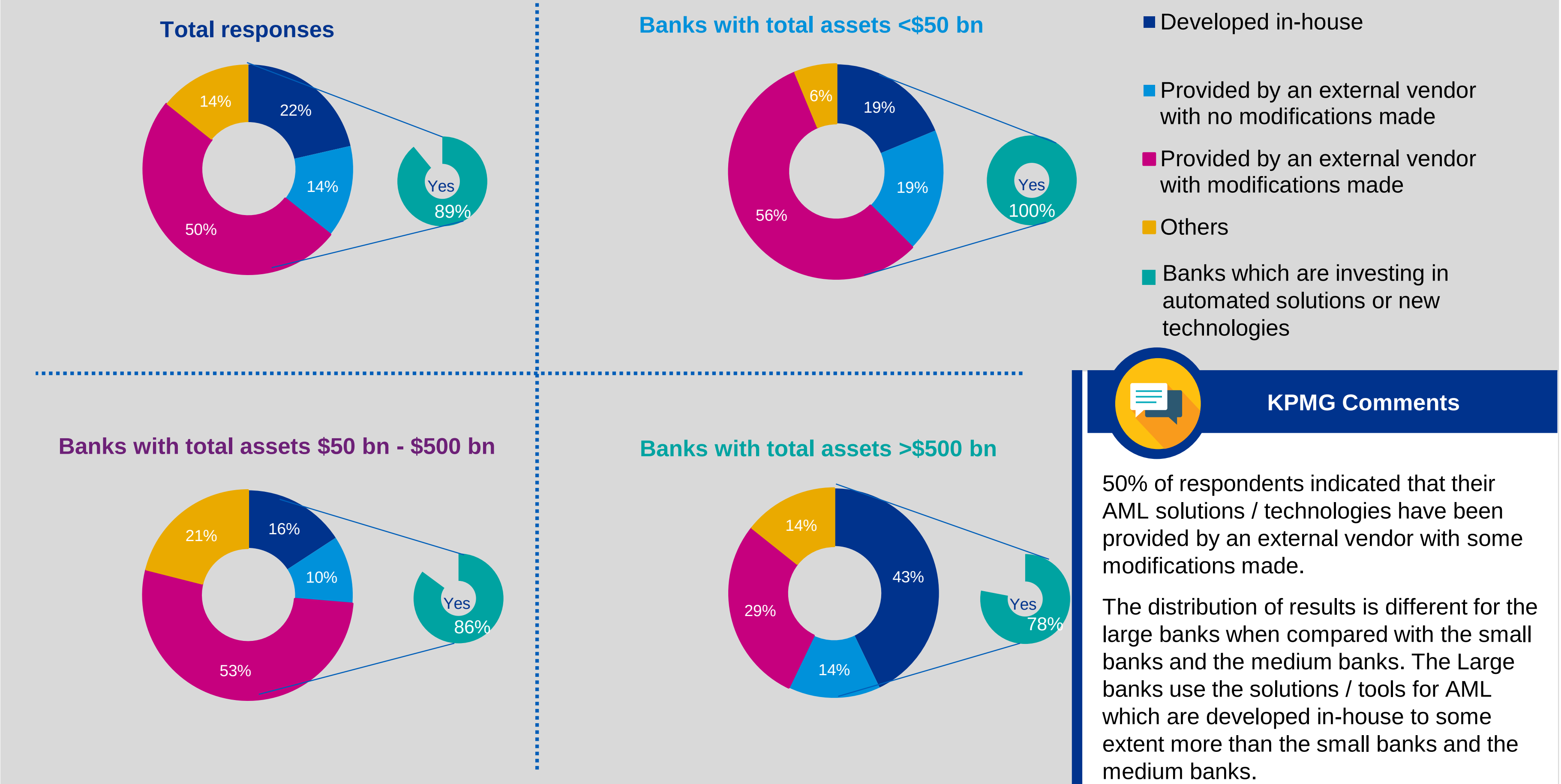
A vast majority of banks confirmed that they are investing in automated solutions or new technologies to improve overall AML framework.

The small banks and the medium banks seem to be more inclined towards making an investment in automated solutions or new technologies potentially due to less sophisticated AML framework relative to the large banks.

5.1 Detailed findings of the survey

50% of total respondents indicated the use of an external vendor AML solutions/technology with some modifications made…

If yes, are these automated solutions or new technologies developed in-house or provided by an external vendor?



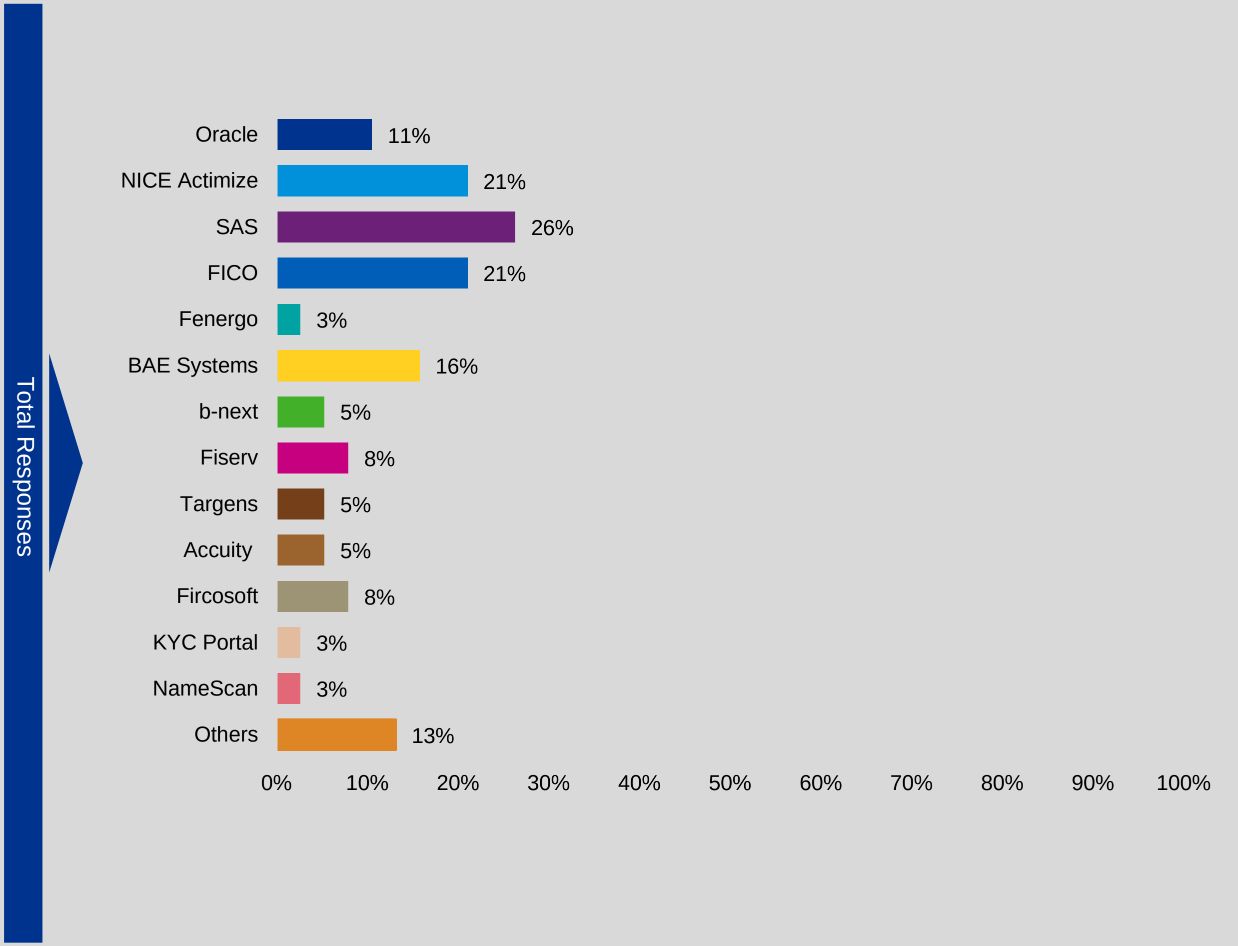
KPMG Comments

50% of respondents indicated that their AML solutions / technologies have been provided by an external vendor with some modifications made.

The distribution of results is different for the large banks when compared with the small banks and the medium banks. The Large banks use the solutions / tools for AML which are developed in-house to some extent more than the small banks and the medium banks.

SAS, FICO and NICE Actimize are the most common vendors/vendor solutions used for combating AML activities by banks…

What are your bank's preferred vendor solutions/vendors used for combating AML activities?



KPMG Comments

Most of the respondents prefer a wide range of vendors/vendor solutions for AML.

SAS, FICO and Nice Actimize are the most commonly used vendors/ vendor solutions for AML.

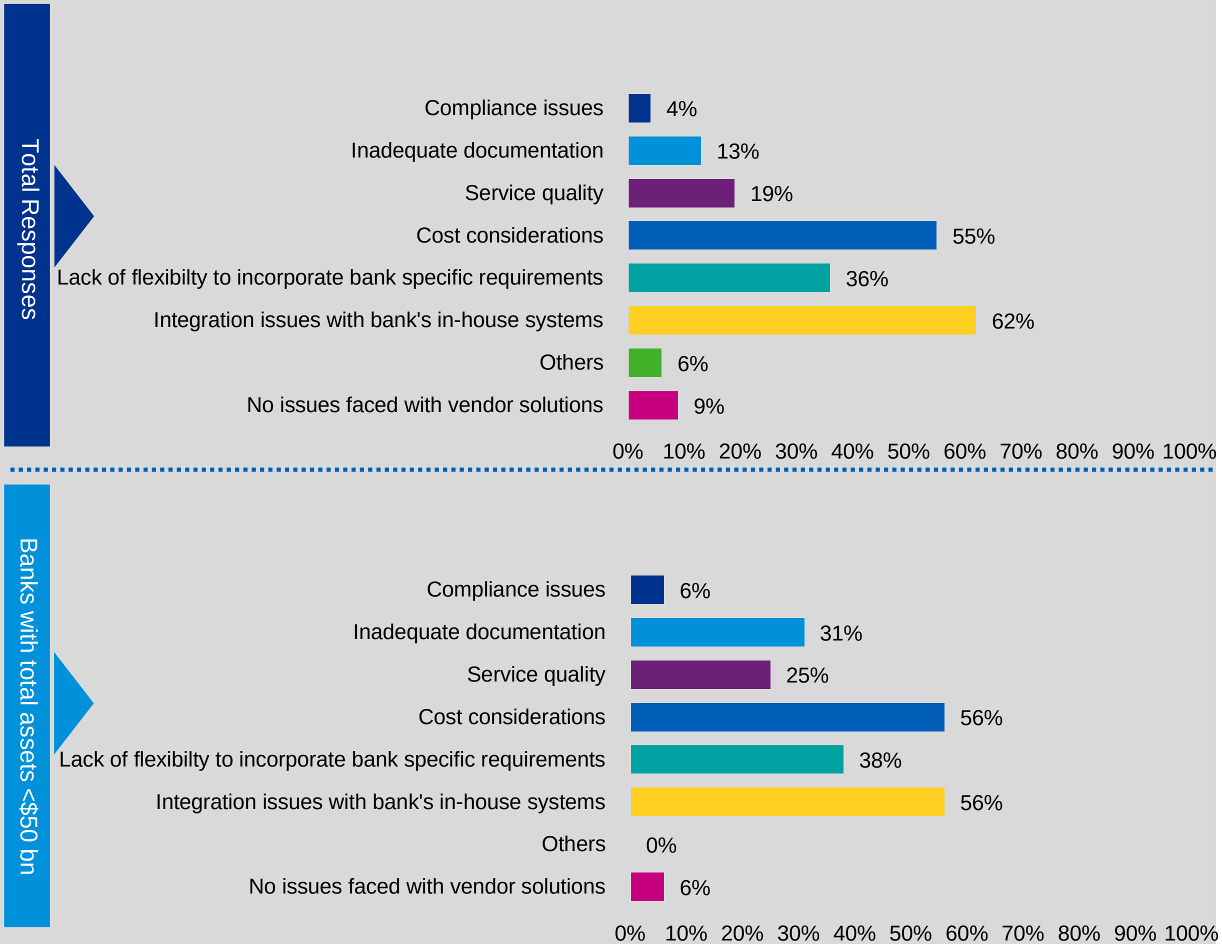
BAE systems is another common vendor used by some of the banks specifically large banks.

Few of the other respondents indicated they also use the following vendors/vendor solutions:

– SIOPEIA,
– Factiva - Dow Jones,
– GIANOS (OASI) ,
– SWIFT (Sanctions Screening, Compliance Analytics, Correspondent Monitoring),
– AIA (Spanish vendor);
– Pythagoras
– LexisNexis and
– Salv

For vendor solutions, integration issues with firm's in-house systems and cost consideration are cited as main challenges.

What are the major challenges being faced with vendor solutions?



KPMG Comments

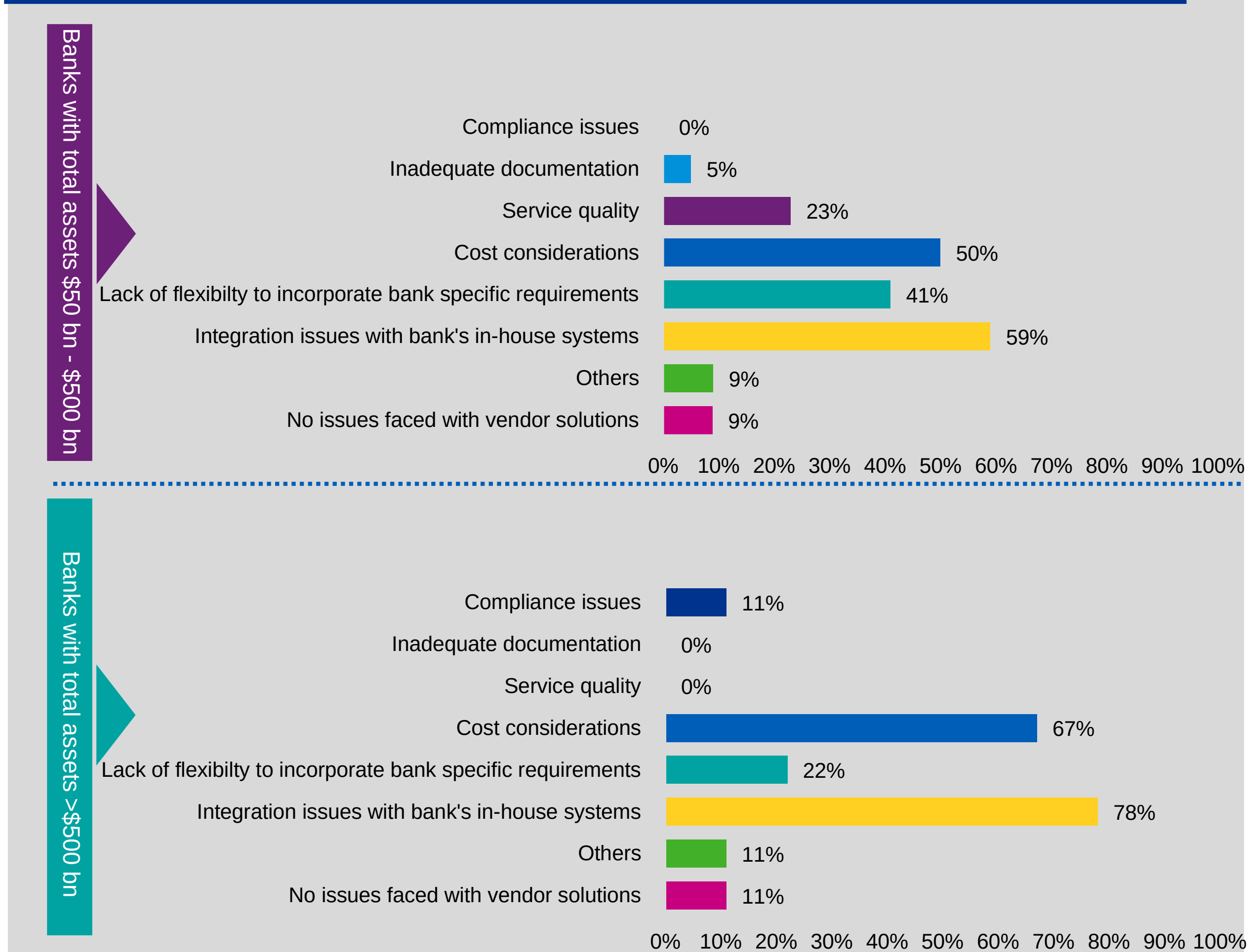
The distribution of results is almost similar for all the types of banks.

It is apparent from the data that cost considerations and integration issues with firm‘s in-house systems are the main challenges, which banks face with vendor solutions.

Some of the banks have also indicated lack of flexibility to incorporate bank specific requirements as another challenge faced by banks, when deploying vendor solutions for AML

For vendor solutions, integration issues with firm's in-house systems and cost consideration are cited as main challenges.

What are the major challenges being faced with vendor solutions?



KPMG Comments

The distribution of results is almost similar for all the types of banks.

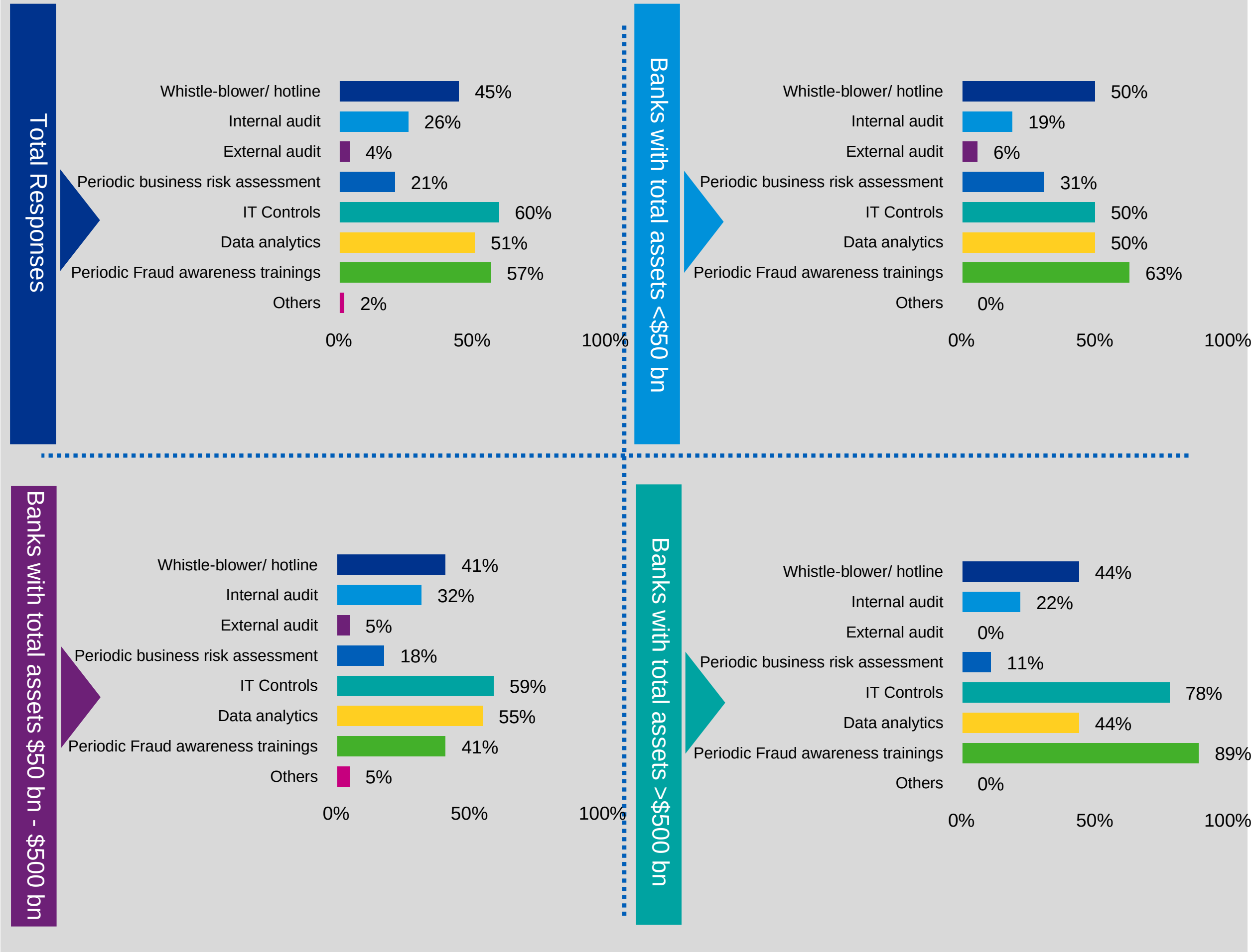
It is apparent from the data that cost considerations and integration issues with firm‘s in-house systems are the main challenges, which banks face with vendor solutions.

Some of the banks have also indicated lack of flexibility to incorporate bank specific requirements as another challenge faced by banks, when deploying vendor solutions for AML

5.1 Detailed findings of the survey

Most of the respondents indicated IT controls, periodic trainings and data analytics are the three most effective ways of detecting fraud…

In your view, what are the three most effective ways of detecting fraud within your bank?



KPMG Comments

The distribution of results is almost similar for all the types of banks.

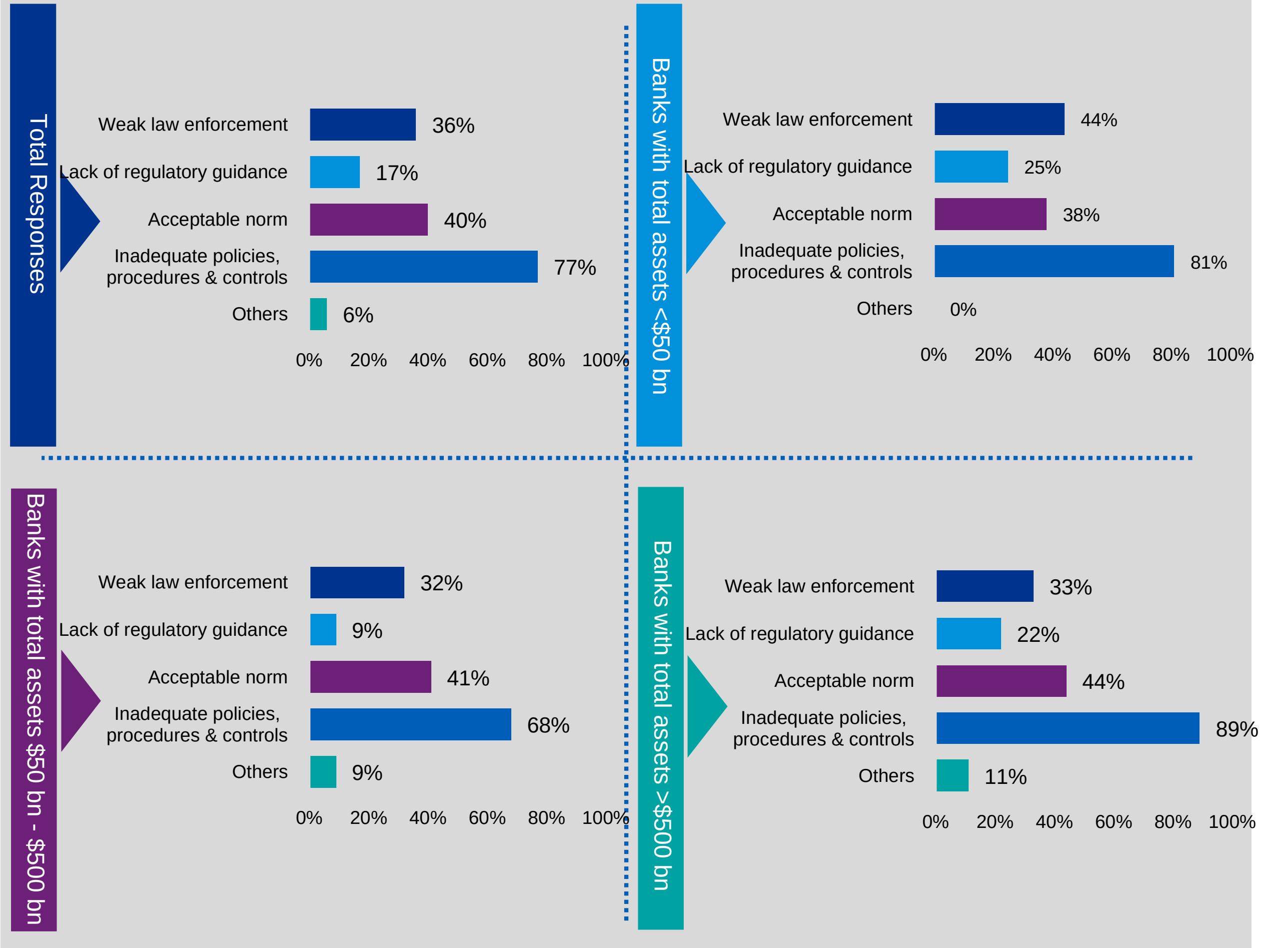
Majority of respondents indicated that IT controls, periodic fraud awareness trainings, and data analytics are the three most effective ways of detecting fraud.

Many banks also mentioned that whistle-blower/hotline is another effective way of detecting fraud.

With the rapidly changing financial industry landscape, banks should consider to periodically provide trainings to employees on emerging risks such as AML concerns stemming from ESG area, ongoing pandemic, emerging technologies, digital finance etc. This will equip them to mitigate instances of fraud faced by banks.

Majority of banks confirmed that inadequate policies, procedures and controls are giving rise to bribery and corruption practices

In your view, what are the main factors facilitating bribery and corruption practices?



KPMG Comments

Many respondents indicated that inadequate policies, procedures and controls are giving rise to bribery and corruption practices.

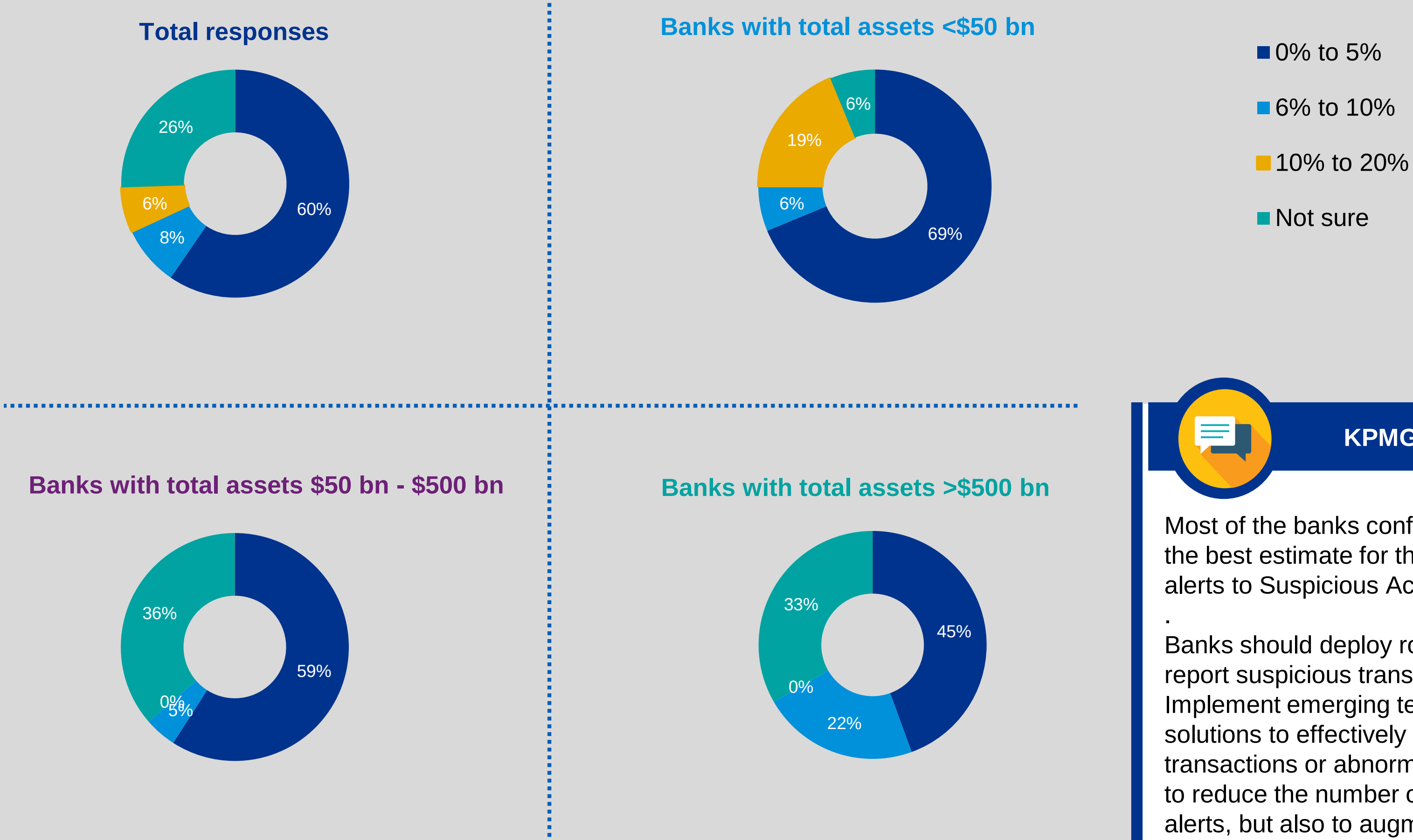
Senior management should regularly review policies and procedures and ensure that these are aligned with regulatory /supervisory guidance, group standards and global and local standards.

In order to determine the effectiveness of controls, 2LoD should consider to perform spot checks on the controls established to circumvent bribery and corruption practices.

5.1 Detailed findings of the survey

Majority of respondents indicated 0% to 5% as the best estimate for the conversion rate of alerts to Suspicious Activity Reports (SARs)

For your bank, what is the best estimate for the conversion rate of alerts to Suspicious Activity Reports (SARs)?



KPMG Comments

Most of the banks confirmed 0% to 5% as the best estimate for the conversion rate of alerts to Suspicious Activity Reports (SARs)
.
Banks should deploy robust framework to report suspicious transactions effectively. Implement emerging technology powered solutions to effectively detect suspicious transactions or abnormal patterns not only to reduce the number of false positives alerts, but also to augment SAR process.
.

5.2 Evolving EU AML/CFT regime

Evolving EU AML/CFT Regime…

	Prudential Framework		AML/CFT Framework		
Main Goal	**Prudential Supervisor** Ensure the safety and soundness of credit institutions to protect depositors' money and maintain financial stability	Exchange of Information & Cooperation	**AML/CFT Supervisor** Verify that banks have adequate internal AML/CFT procedures in place; ensure compliance through administrative sanctions and corrective measures, etc.	**Financial Intelligence Unit (FIU)** Collect and analyse suspicious transaction reports (STRs) and inform law enforcement authorities	**Law enforcement authorities (LEAs)** Investigate and prosecute ML/TF, other crimes and tax offences. **Courts** can impose criminal sanctions on natural persons and in some cases also on legal entities
Legislation	– CRR – CRD – SSM Regulation		– AMLD	– AMLD	– EU directives on combatting ML/TF through the use of criminal law – National criminal law

Key measures to enhance AML/CFT framework

2020

- Deadline for transposition of the 5AMLD
- EBA First report published
- EBA launched consultation on revised ML/TF risks factors guidelines
- EU AML Action Plan
- Updated list of high-risk third countries
- Updated list of high-risk third countries
- Refined methodology for the identification of high risk third countries
- Delegated acts
- Country specific recommendations/ European Semester on AML/CFT
- Transfer of technical management of FIU.net to the Commission
- Establishment of the Economic and Financial Crimes Commission - EFECC

2021

Criminal law enforcement and information sharing:
- Guidance on PPPs and possible EDPB opinion on data protection;
- Monitor implementation of directives on criminal law;
- Options to enhance domestic and cross-border information exchange

EBA published final guidelines on ML/TF risks factors

EU AML/CFT single rule book

Legislative proposal:
- Identifying areas to be turned in a regulation alongside an amended directive
- Setting out new areas to be regulated at EU level
- Identifying amendments necessary in respect of other existing legislation

Ongoing Measures

- Work on interconnecting the beneficial ownership registers
- Study assessing the effective application of the 4AMLD
- Third Supranational Risk Assessment
- Country specific recommendations/ European Semester on AML/CFT
- Infringements against some Member States
- Current EBA work

Source: ECB; AME AML Europe

Your Contacts for the AML Survey

Timo Purkott

Partner,
Financial Services

T +49 69 9587 1533
M +49 174 340 7416
tpurkott@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
The SQUAIRE/Am Flughafen
60549 Frankfurt am Main

Girija Chandrawat

Senior Manager
Financial Services

T +49 69 9587 1212
M +49 151 14395317
gchandrawat@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
The SQUAIRE/Am Flughafen
60549 Frankfurt am Main

KPMG Member Firm Contacts