True Cost of AML Compliance

Singapore "Snapshot"

2019

LexisNexis® RISK SOLUTIONS

Background & Objectives

LexisNexis® Risk Solutions has conducted a global survey of its True Cost of AML Compliance study. The following report presents findings from the Singapore market along with regional APAC insights. Specific objectives included to:

- Identify the drivers and influencers impacting AML compliance (and change);
- Understand spending trends for AML compliance, including:
  - How spending is divided by cost of compliance area (e.g., sanctions, transaction monitoring, technology, KYC due diligence, etc…);
  - The human resources component of these costs, particularly numbers of FTEs for compliance and sanctions screening; and
  - The processing time component (e.g., length of time to complete customer due diligence by type of client/entity);
- Determine the business impact of the AML compliance environment, particularly with regard to new regulations and provisions;
- Identify the challenges and opportunities associated with AML compliance, including with non-bank payment providers; and
- Understand the role of technology with the above.

Methodology & Definitions

LexisNexis® Risk Solutions retained KS&R, a global market research firm, to conduct this research study.

- Data was collected by phone during March 2019 with a total of 233 completions across 4 APAC markets. **The following report details the Singapore results.**

Total	Singapore	Indonesia	Malaysia	Philippines
233 completions	70 completions	63 completions	50 completions	50 completions

- Respondents included decision makers within the financial crime function who oversee KYC remediation, sanctions monitoring and/or AML transaction monitoring. Organizations represented banks, investment firms, asset management firms, and insurance firms.
- LexisNexis® Risk Solutions was **not** identified as the sponsor of the research in order to lessen potential for brand bias.

In this report, firms are referred to in terms of their asset size. For this study, these are defined as: Small asset size – having <US$10B total assets, Mid/large asset size – having US$10B+ total assets

Key Findings

LexisNexis® RISK SOLUTIONS

Key Findings

- The true cost of AML compliance across all Singapore financial services firms is estimated to be US$3.13B. Though this spend is largely attributed to larger asset-sized firms (US$10B+), it is smaller firms (<US$10B in assets) that spend somewhat more as a percentage of assets -- the cost of AML compliance is higher among smaller firms (an average of .26%) than larger firms (an average of .06%).
- The distribution of compliance costs is similar by size of organization, with costs being fairly equally distributed across labour and technology. But given that larger firms employ over twice as many FTEs as smaller firms on average, this contributes to exponentially higher compliance costs. Labour includes not only salaries, but also benefits, taxes, and overhead.
    - Average compliance costs are spread similarly across labour-consuming activities, with just over one-quarter involving KYC, which consumes labour hours through information collection, list screening, and risk assessment.
        - Remaining costs involve transaction monitoring, investigations, and overall compliance management.
    - Use of newer technologies/services is similarly limited across smaller and larger firms.
        - Cloud-based KYC utilities are most used, followed by shared interbank compliance databases, unstructured text analysis, and in-memory processing.
        - Larger firms are more likely than smaller ones to use more advanced technologies such as artificial intelligence and unstructured audio analysis.
        - However, while a majority currently/are able to monitor digital identities (74%) and online transactions in real-time for criminal behavior (73%), nearly half (44%) are leaving themselves open to sanctions breaches by <u>not</u> currently having that monitoring capability.

Key Findings (cont.)

- Though business de-risking is among key drivers for Singapore financial firms, it ranks lower than others. With Singapore's status as both a major global financial centre and an international trade/transportation hub, the size and foreign exposure of Singapore's private banking and asset management industry, and being situated in a region where several terrorist groups operate actively and have carried out attacks in recent years, its money laundering vulnerabilities increase. This adds additional risk to financial firms and makes de-risking even more important.
  - Under half view AML compliance as negatively impacting productivity (42%) and customer acquisition (40%), but the impacts are not insignificant. Average annual hours of lost productivity are estimated to be nearly 30 per FTE and annual opportunity costs of refused accounts/customer walkouts and delayed account opening are between 2% - 4% of new account applications.
  - These things individually, but especially combined, can lead to higher long-term costs.
- The above will likely be compounded by an expected increase in alert volumes and cost increases over the course of the year.
  - A majority (70%) expect alert volumes to increase, by an average of 11%.
  - AML compliance and sanctions costs are expected to grow by an average of 10% and 9% respectively.

Key Findings (cont.)

- On top of this, non-bank payment providers are proving to be a new challenge for compliance organizations.
    - Over the past year, 1 in 5 suspicious activity reports have involved non-bank payment providers.
    - As a result, alert volumes have increased, as well as have technology and resource costs.
    - In response to the impact from these providers, a number of financial firms have created a team to evaluate emerging payment technologies, implemented more rigorous training, migrated to dynamic monitoring, or implemented FinTech/RegTech.
- Regional findings show that firms which use a mix of compliance technologies have a lower cost per FTE and are able to conduct due diligence and clear alerts faster.

Detailed Findings

Larger ($10B+ asset) sized financial firms in Singapore screen significantly more names per day, and, as such, have larger compliance operations teams.

A majority of FTEs have been employed for under 10 years and are likely to earn under US$40,000-US$60,000 a year.

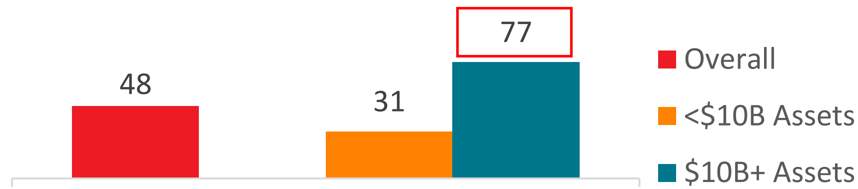
FTEs employed by larger ($10B+) firms earn a higher salary, on average, than those in smaller firms.

Q2c: Please indicate your best estimate of the number of FTE staff employed in the AML compliance operations departments.

Q3/Q4. On average, how many names are screened per day across all of the FTE analysts in your compliance/sanctions screening operations?

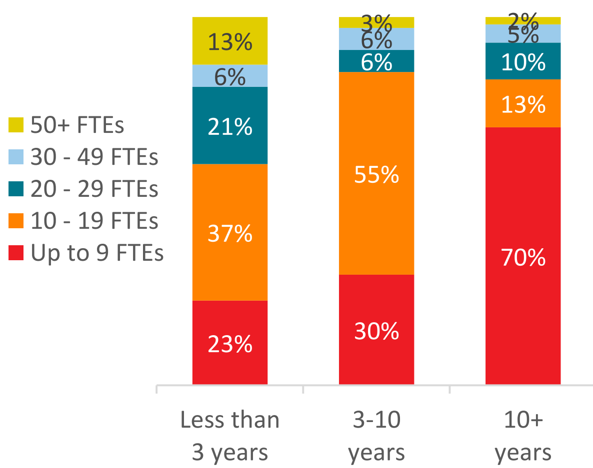
Q7: Please estimate the average annual salary of your firm's compliance personnel.

Average FTE Staff Employed in AML Compliance Operations

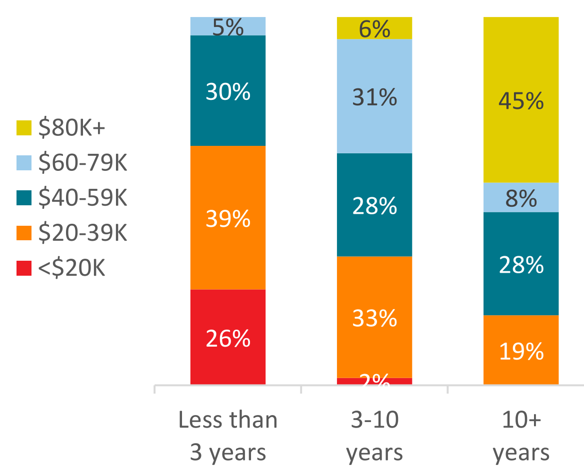


	Overall	<$10B Assets	$10B+ Assets
Mean # of Names for Compliance screening (per day)	258	213	328
Mean # of Names for Sanctions screening (per day)	213	166	289

Number of FTE Staff by Tenure



Average FTE Salary by Tenure



	Overall	<$10B Assets	$10B+ Assets
Average FTE Salary	US$57,163	US$51,269	US$66,750

LexisNexis® RISK SOLUTIONS

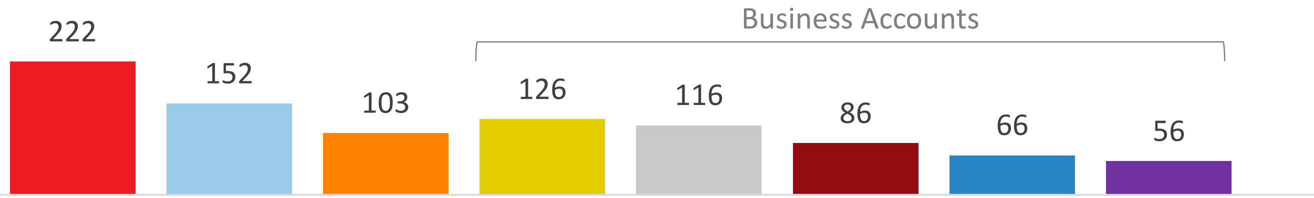
Business accounts consume more due diligence time for Singapore financial firms overall.

However, the time spent to complete due diligence is similar across organization size and type.

Regionally, those that invest in more compliance technology / services are able to complete due diligence more quickly than others (*see Regional Findings section*).

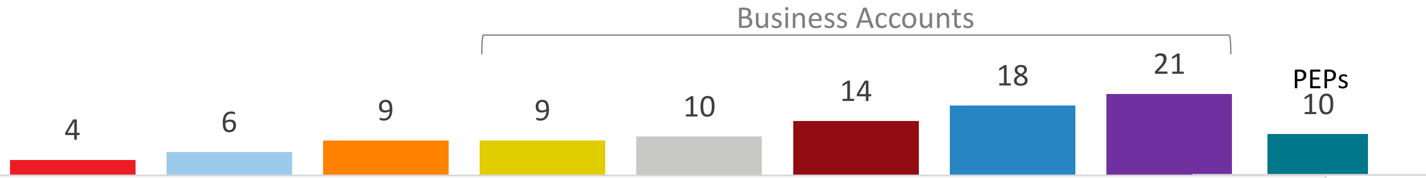
Domestic Retail | Private Banking / Wealth mgmt. | Foreign Individuals | SME | Domestic Midmarket Corporate | Domestic Large Corporate | Foreign SME | Foreign Corporate

Average New Accounts Opened Monthly



	Domestic Retail	Private Banking / Wealth mgmt.	Foreign Individuals	SME	Domestic Midmarket Corporate	Domestic Large Corporate	Foreign SME	Foreign Corporate
Mid/large ($10B+) Assets	303	239	171	195	199	156	115	101
Sm (<$10B) Assets	167	88	45	81	61	40	19	12
Banks	326	247	181	198	196	159	120	107
Investment Firms	125	69	42	76	62	41	23	16

Average Hours Required for Completing Customer Due Diligence



	Domestic Retail	Private Banking / Wealth mgmt.	Foreign Individuals	SME	Domestic Midmarket Corporate	Domestic Large Corporate	Foreign SME	Foreign Corporate	PEPs
Mid/large ($10B+) Assets	5	6	11	10	12	15	19	23	11
Sm (<$10B) Assets	4	7	8	9	9	14	18	20	9
Banks	5	6	11	10	12	17	21	23	12
Investment Firms	4	8	9	11	11	14	17	21	9

Significantly or directionally much higher than others within type of account

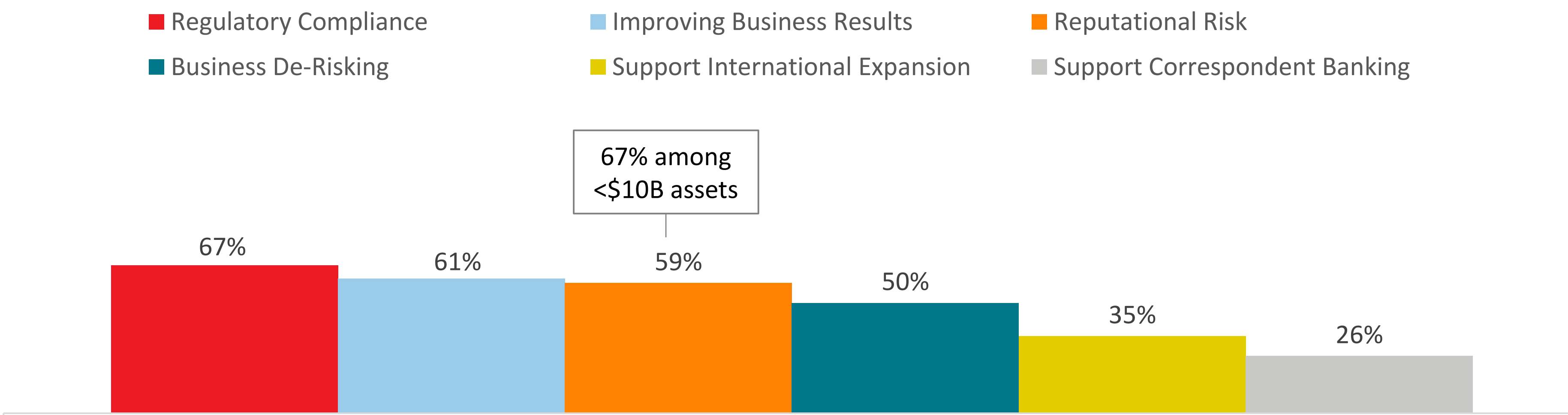
Q1: For each of the following customer types that apply to your institution, please give your best estimate of the number of new accounts opened monthly.
Q17a: What would you say is the average time required for completing customer due diligence on the following?

LexisNexis® RISK SOLUTIONS

Regulatory compliance, improving business results, and reputational risk are the top AML drivers for Singapore financial services firms.

While business de-risking is a top driver among significantly more Singapore financial institutions (50%) than US firms (28%), only just over half rank it as a top driver of AML initiative. This is somewhat surprising, given that Singapore's status as both a major global financial centre and an international trade/transportation hub makes it vulnerable to becoming a transit point for illicit funds from abroad. The size and foreign exposure of Singapore's private banking and asset management industry, in particular, increases Singapore's money laundering vulnerabilities. Additionally, Singapore is situated in a region where several terrorist groups operate actively and have carried out attacks in the last 10 years. [1]

Drivers of AML Initiatives in Respondents' Organizations (Ranked Among Top 3)



[1] https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Singapore-2016-Executive-Summary.pdf

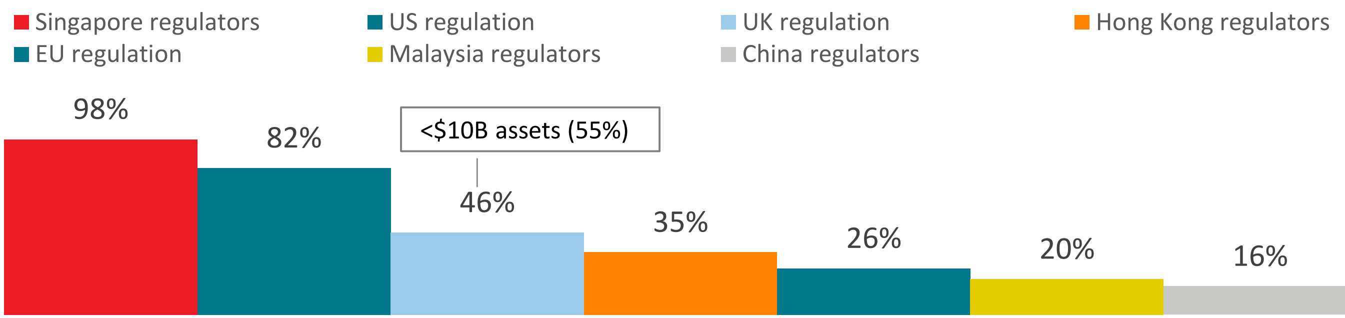
Q8: What would you say are the top drivers for AML initiatives at your firm, and their relative importance?

Not surprisingly, Singapore regulation has the most impact on financial firms. However, US regulation is also very influential.

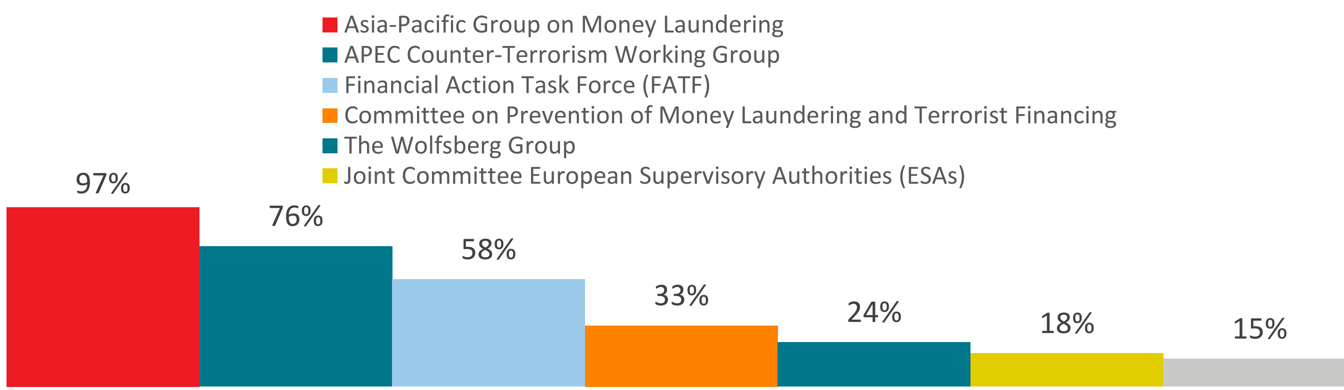
Among organizations with the greatest impact on regulatory compliance, Asia-Pacific Group on Money Laundering leads, followed by APEC Counter-Terrorism Working Group and FAFT.

FATF's 2016 assessment of Singapore noted that the financial sector has a reasonable understanding of money laundering risks and has taken steps to mitigate them. But, moderate gap are said to remain. Among FATF's recommendations for improvement are to conduct comprehensive risk assessments for all types of legal persons to identify where the risks are and develop policy to address them, as well as take steps to improve capabilities to proactively identify and investigate money laundering, especially from foreign sources.[2]

Regulators Having Greatest Impact on Regulatory Compliance (Ranked in Top 5)



Organizations Having Greatest Impact on Regulatory Compliance (Ranked in Top 5)



[2] Ibid.

Q9: Which regulator do you see as having the greatest impact (including indirect influence) on regulatory compliance change in your country/region?

Q10: Which organizations do you see as having the greatest impact (including indirect influence) on regulatory compliance change in your country/region?

LexisNexis® RISK SOLUTIONS

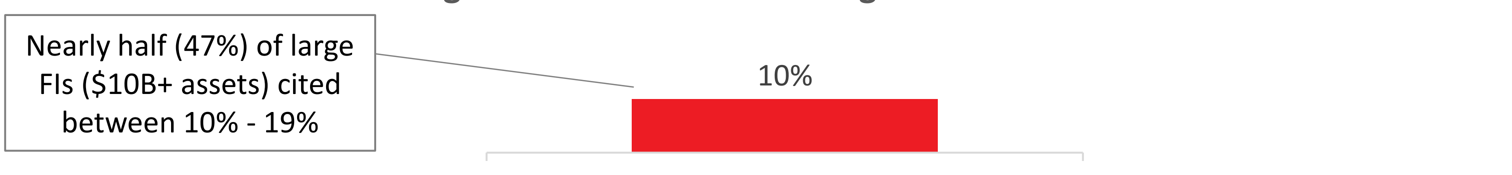
AML compliance costs have reportedly increased by ~10% during the past 24 months, though somewhat more so among larger firms.

There are expectations that AML compliance and sanctions costs will continue to rise over the coming year.

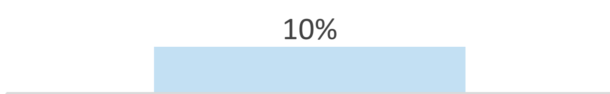
These larger firms employ more human resources and have higher screening volumes.

Across firm size, there are expectations that AML compliance and sanctions costs will rise similarly during the coming year. However, a number of firms expect to increase compliance staff in order to address challenges and risks posed by non-bank payment providers. Added labor should theoretically add much more costs to compliance operations; alternatively, investments in compliance technology can reduce the longer-term expenses, especially where there are concerns for ever-increasing alert volumes and false positives.

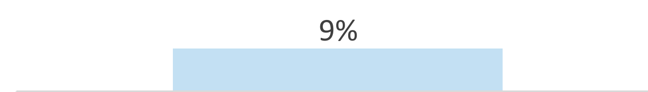
Avg. AML Cost Increase During Past 24 Months



Avg. Expected AML Compliance Cost Increase



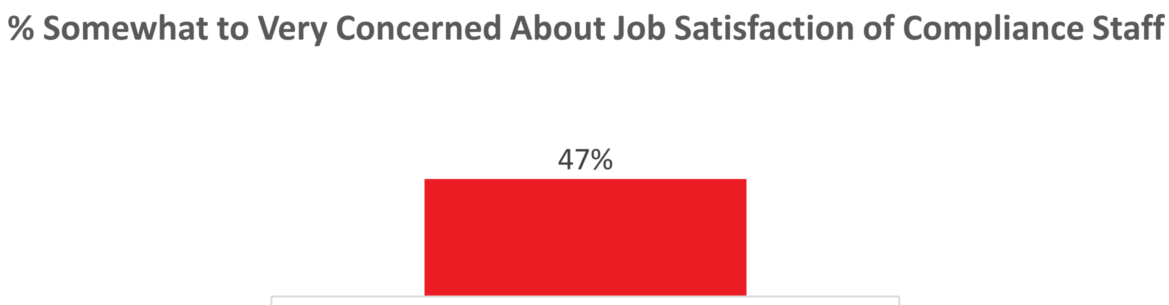
Avg. Expected AML Sanctions Cost Increase

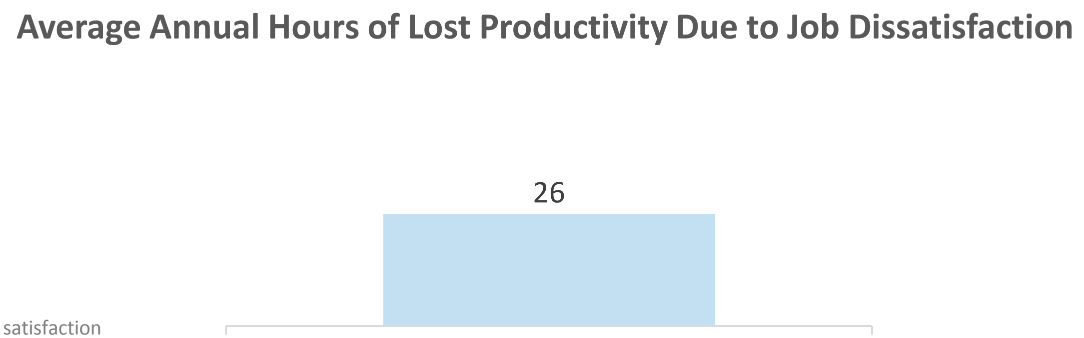


LexisNexis® RISK SOLUTIONS

Q11: Over the past 24 months, have your firm's AML compliance costs increased or decreased, and by how much? Please provide your best estimate? Q12: In 2019, do you expect your firm's overall AML compliance costs will increase or decrease, and by how much? Q13: In 2019, do you expect your firm's sanctions compliance costs will increase or decrease, and by how much?

Nearly half (47%) indicated concern about compliance staff job satisfaction.





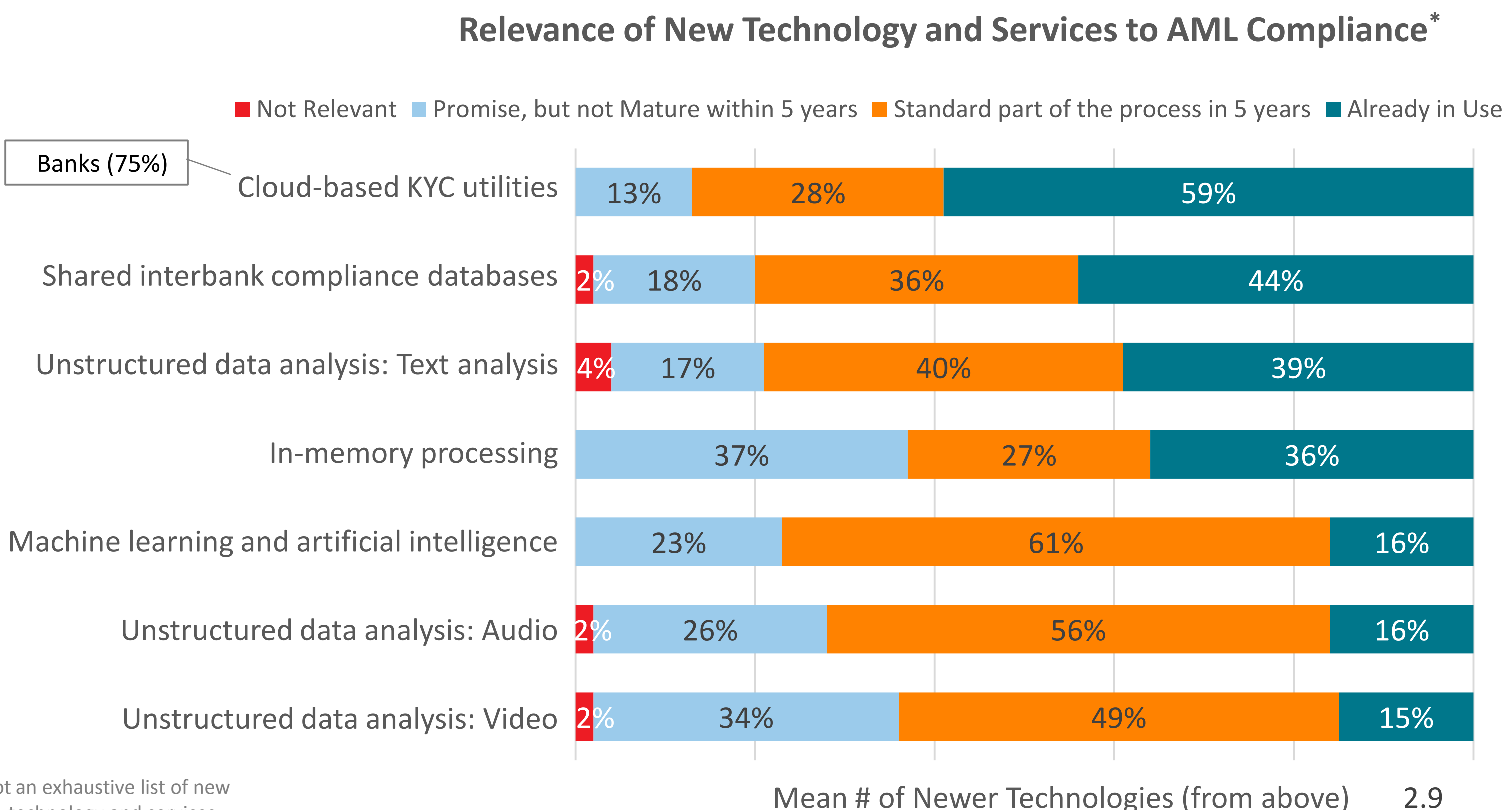
Q14: How concerned are you with job satisfaction in your compliance department?

Q15: What would you say is the annual loss in AML compliance productivity due to job satisfaction issues, expressed in average hours of lost productivity per FTE analyst?

Cloud-based KYC utilities are currently most used with regard to AML compliance, particularly among banks.

Though somewhat limited, use of shared interbank compliance databases, unstructured text analysis, and in-memory processing are next most common. Regionally, findings show that large firms, which have more AML compliance staff and higher total assets, use more of these technologies / services than others (4 or more) (*see Regional Findings section*).

Artificial intelligence and unstructured audio and video analyses are expected to become a standard part of the process in 5 years.



% Already in Use

	Small (<$10B)	Mid/Large ($10B+)
Cloud-based KYC utilities	57%	62%
Shared interbank compliance databases	43%	45%
Unstructured data analysis: Text analysis	41%	34%
In-memory processing	37%	34%
Machine learning and artificial intelligence	13%	22%
Unstructured data analysis: Audio	12%	22%
Unstructured data analysis: Video	15%	14%
Mean # of Newer Technologies	2.9	2.7

* Not an exhaustive list of new AML technology and services

Significantly or directionally much higher than other segments within technology

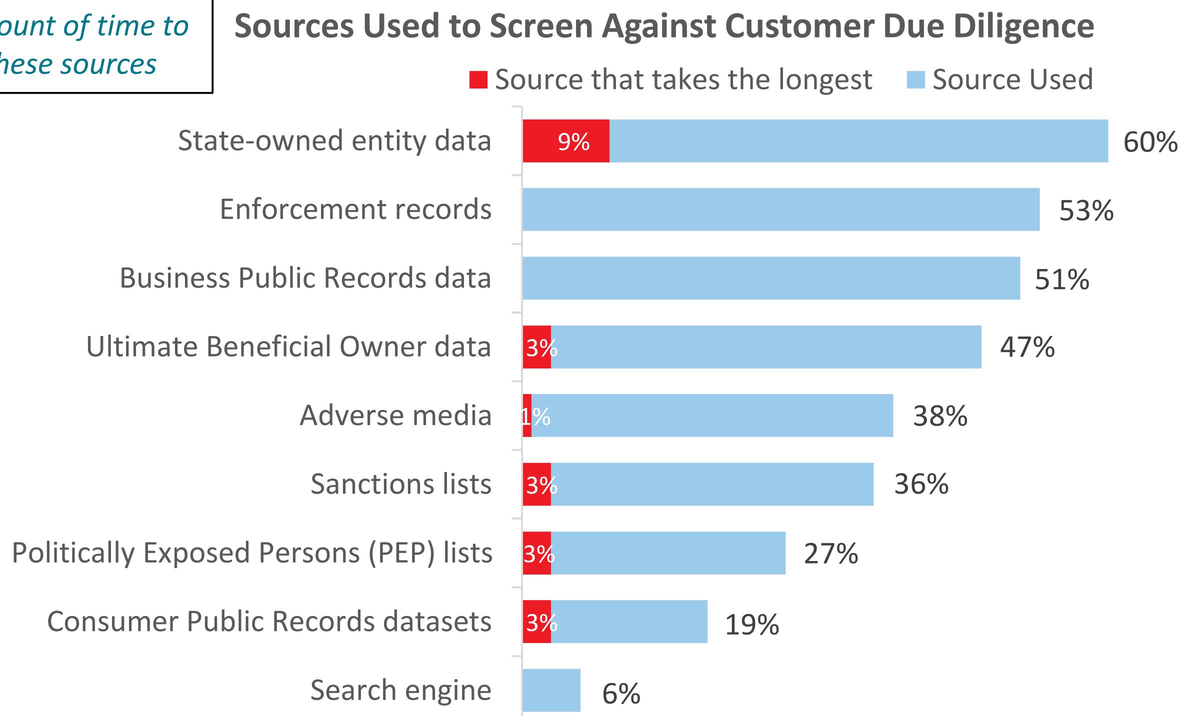
Q16: Over the next 5 years, to what degree do you think each of the following new technologies and services will be relevant to AML compliance?

Various sources are used to screen for customer due diligence, with state-owned entity data, enforcement records, business public records, and ultimate beneficial owner data among the most used.

Firms with $10B+ in assets are more likely to use consumer public records databases and search engines than others.

Given Singapore's position as a major global financial centre and an international trade/transportation hub and financial firms concern with reputational risk, use of adverse media, sanctions lists, PEP lists, etc. for due diligence screening is limited. This leaves firms open to additional risks.

84% indicate that takes a similar amount of time to screen these sources



	Small (<$10B)	Mid/Large ($10B+)
State-owned entity data	56%	66%
Enforcement records	51%	57%
Business Public Records data	56%	44%
Ultimate Beneficial Owner data	40%	$\boxed{59\%}$
Adverse media	36%	42%
Sanctions lists	39%	30%
Politically Exposed Persons (PEP) lists	31%	20%
Consumer Public Records datasets	12%	$\boxed{29\%}$
Search engine	0%	$\boxed{17\%}$

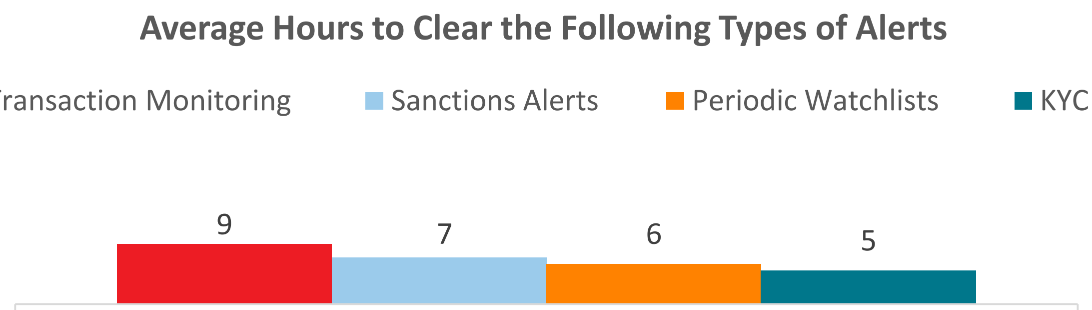
□ Significantly or directionally much higher than other segments within technology

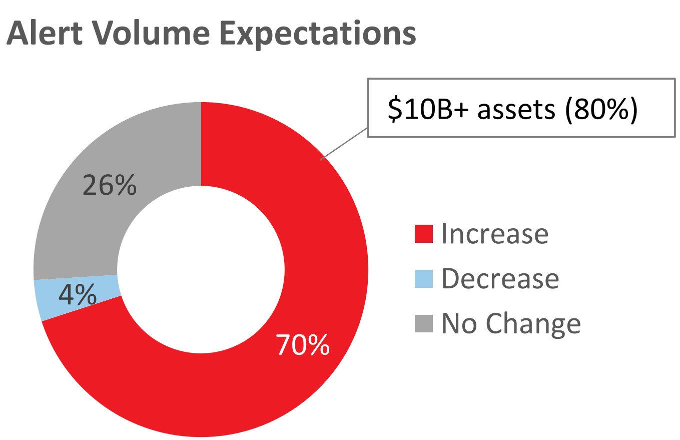
Q17b. Which sources are you using to screen against for customer due diligence?
Q17c: Which source(s) take the longest time to screen against?

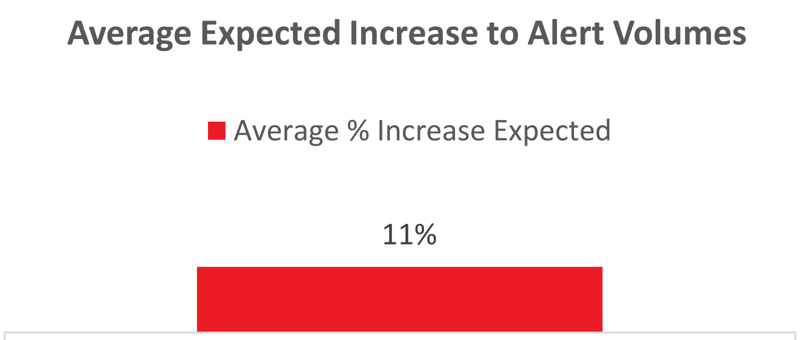
The average time required to clear various alerts in Singapore financial firms is reported to be between an average of 5 – 9 hours.

Alert volumes are largely expected to increase in 2019, especially among firms with $10B+ in assets, by an average of 11%.

Regionally, those that use more compliance technology/services are able to clear alerts much faster than others (see *Regional Findings section*).





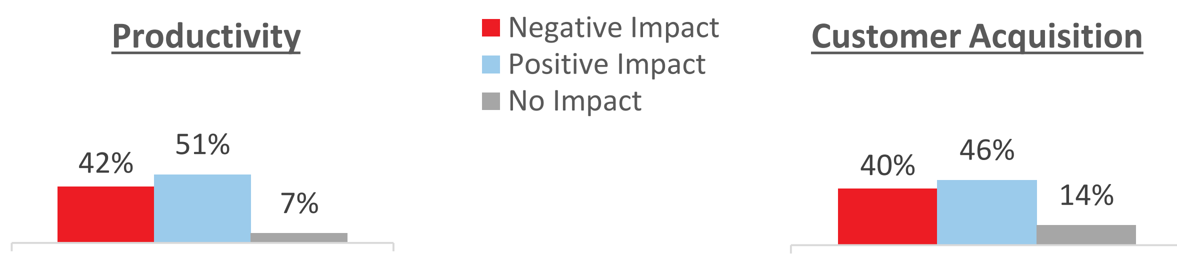


Q18: What is the average time required for an analyst to clear each of the following alert types?
Q19a: Do you expect alert volumes to increase or decrease in 2019?
Q19b. Percent you expect alert volumes to increase in 2019?

Under half of firms report that AML compliance processes have a negative impact on productivity and customer acquisition efforts.

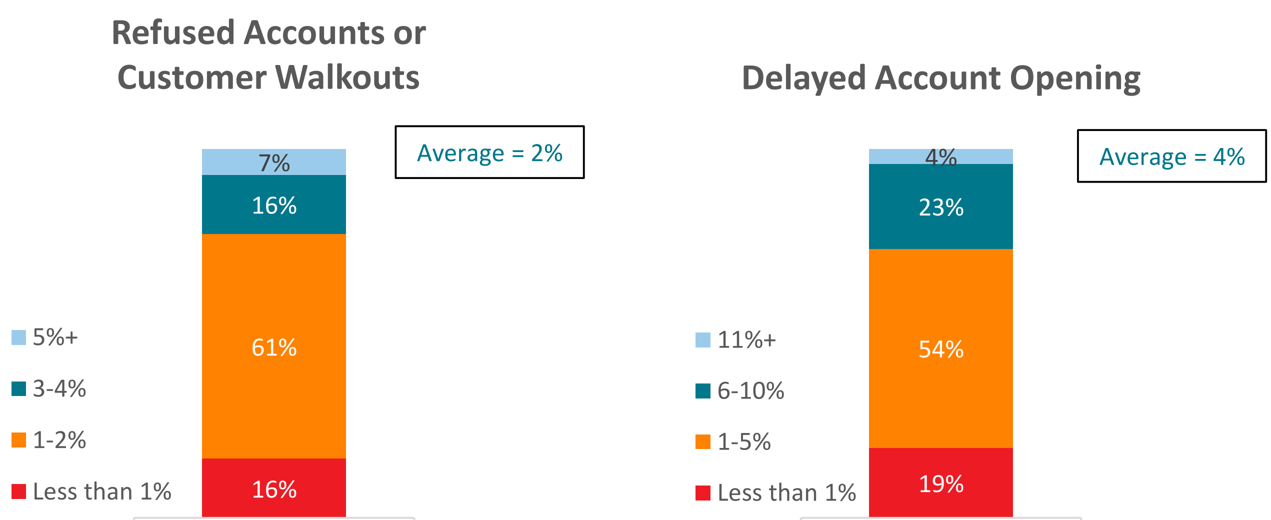
The impacts are not insignificant, however, with average annual hours of lost productivity per FTE analyst equivalent to nearly 4 days (based on 8-hour work day). And an average of 2% of accounts are lost per year, while another ~4% of new account openings are delayed.

AML Compliance Impact on . . .



Annual average hours of lost productivity per FTE = 29.5

Estimated Annual Opportunity Cost of...



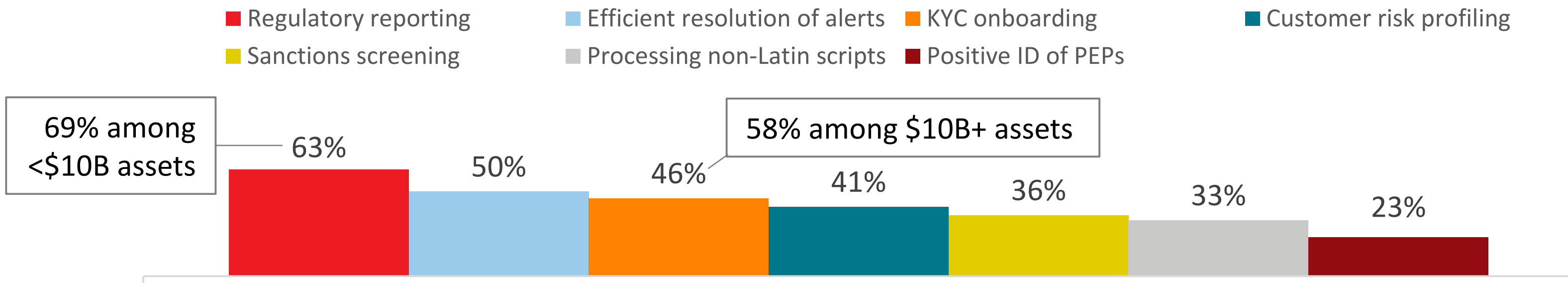
Q20a/22: What kind of impact does the AML compliance process have on LoB productivity/ customer acquisition? Q21: What is your best estimate of the annual loss in LoB productivity due to AML compliance at your firm? Q24a/23a: What do you estimate is the annual opportunity cost of refused accounts or customer walkouts/delayed account opening due to AML compliance, as a percentage of new account applications?

Regulatory reporting, efficient resolution of alerts, and KYC onboarding are key challenges for Singapore financial firms.

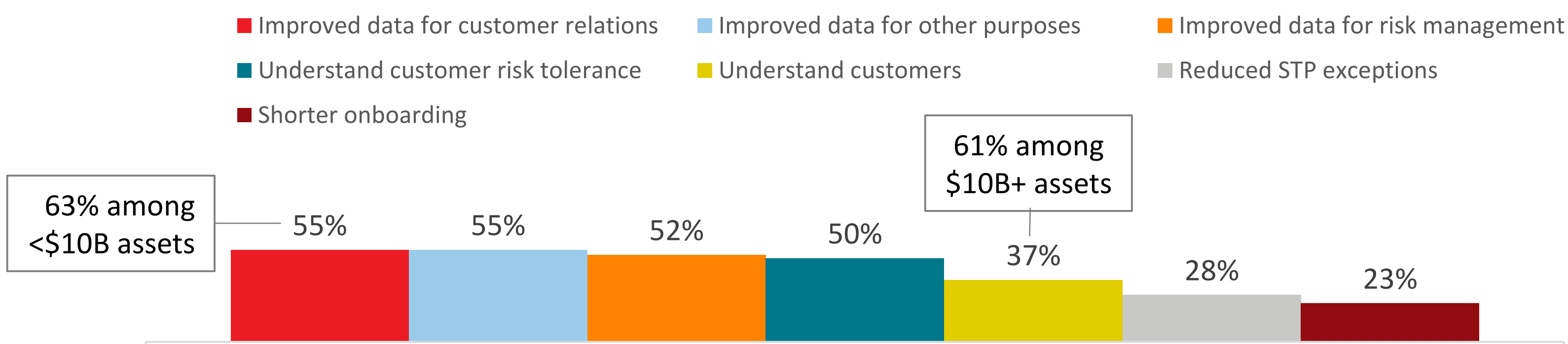
Regulatory reporting is a particular challenge for smaller firms, while KYC onboarding is for larger firms.

However, improved data for customer relations/other purposes/risk management and for understanding customer risk tolerance are perceived as key benefits of the process.

Key Challenges for Compliance Screening Operations (% Ranked Among Top 3)



Benefits from AML Compliance (% Ranked Among Top 3)



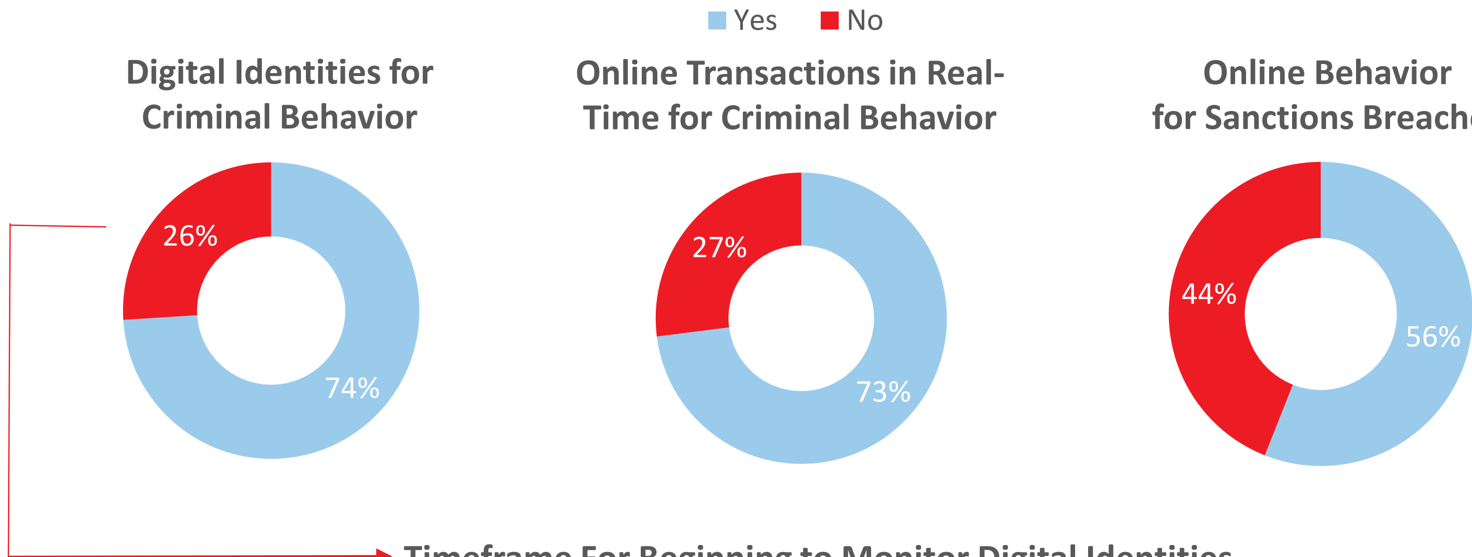
Q25: What areas in your compliance screening operations face the largest challenges under compliance change?

Q26: Which of the following do you see as benefits to the business brought by AML compliance change?

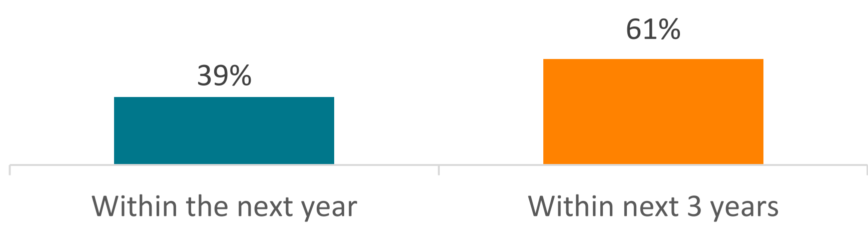
A majority of Singapore financial firms are currently monitoring digital identities for criminal behavior and are able to monitor online transactions in real-time.

Fewer are able to monitor online behavior for sanctions breaches.

% Currently Monitoring/Able to Monitor…



Timeframe For Beginning to Monitor Digital Identities



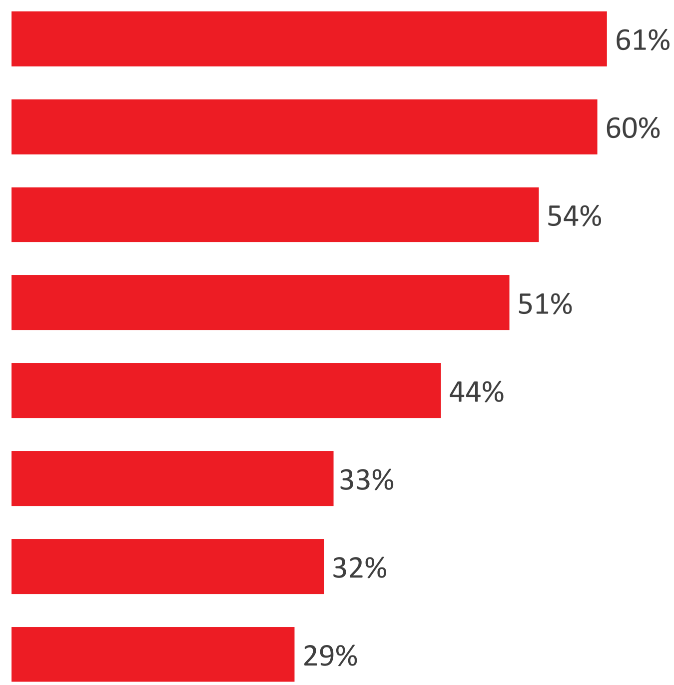
Q32a: Are you currently monitoring/able to monitor…

Q32b: Which of the following timeframes best describes when you will start to monitor digital identities for criminal behavior?

Common impacts of non-bank payment providers on compliance operations include increased cost of tech investments, alert volumes, resource costs, and risk of conducting correspondent banking.

Firms with assets of $10B+ are also likely to experience increased risk of compliance violations and risks than others.

Impacts of Non-Bank Payment Providers/Systems on Organization's AML Compliance Processes



Impacts of Non-Bank Payment Providers/Systems on Organization's AML Compliance Processes	Total	Small (<$10B)	Mid/Large ($10B+)
Increased cost of technology investments	61%	63%	58%
Increased alert volumes	60%	65%	52%
Increased cost of resources	54%	47%	66%
Increased risk of conducting correspondent banking	51%	43%	64%
Increased stress on compliance teams	44%	45%	42%
Increased risk of compliance violations and risks	33%	26%	45%
Increased false positives/wasted resource time	32%	33%	30%
Decreased productivity of compliance teams	29%	28%	31%

Significantly or directionally much higher than other segments within technology

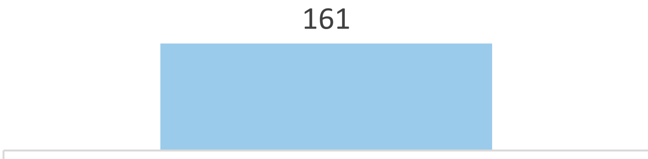
Q37. Which of the following, if any, have been the impacts of non-bank payment service providers and systems on your organization's AML compliance processes?

LexisNexis® RISK SOLUTIONS

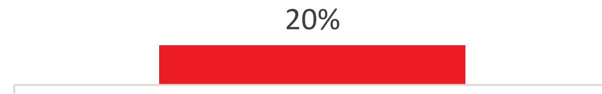
1 in 5 of the SARs reported annually involve non-bank payment providers.

Non-bank payment providers created challenges for AML compliance over the past year, as well as caused compliance organizations to change their screening operations to at least some degree.

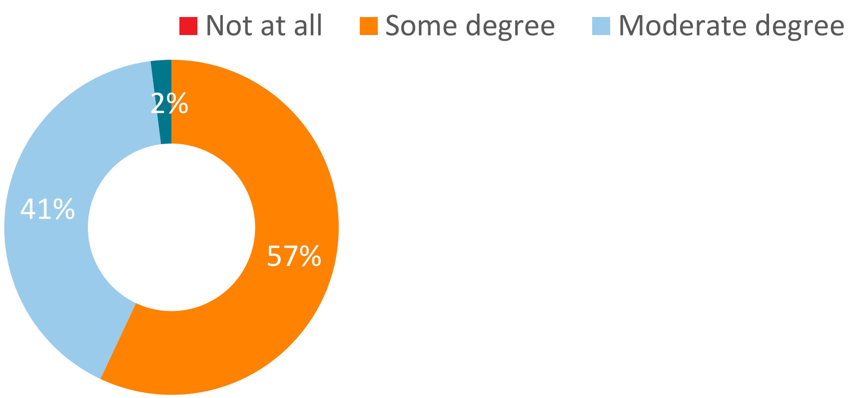
Average Submitted SARs Reports Annually



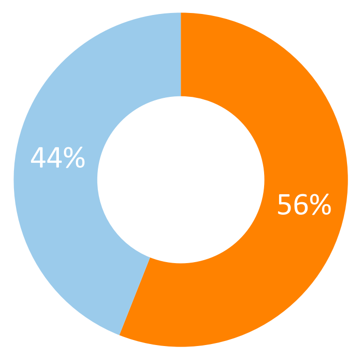
% Suspicious Activity Reports (SARs) That Involve Non-Bank Payment Provider Transactions



Degree That Non-Bank Payment Providers/Systems Created Challenges for AML Compliance Over Past Year



Degree That Rise in Transactions Through Non-Bank Payment Providers/Systems Caused AML Compliance Organization to Change its Screening Operations in Past Year

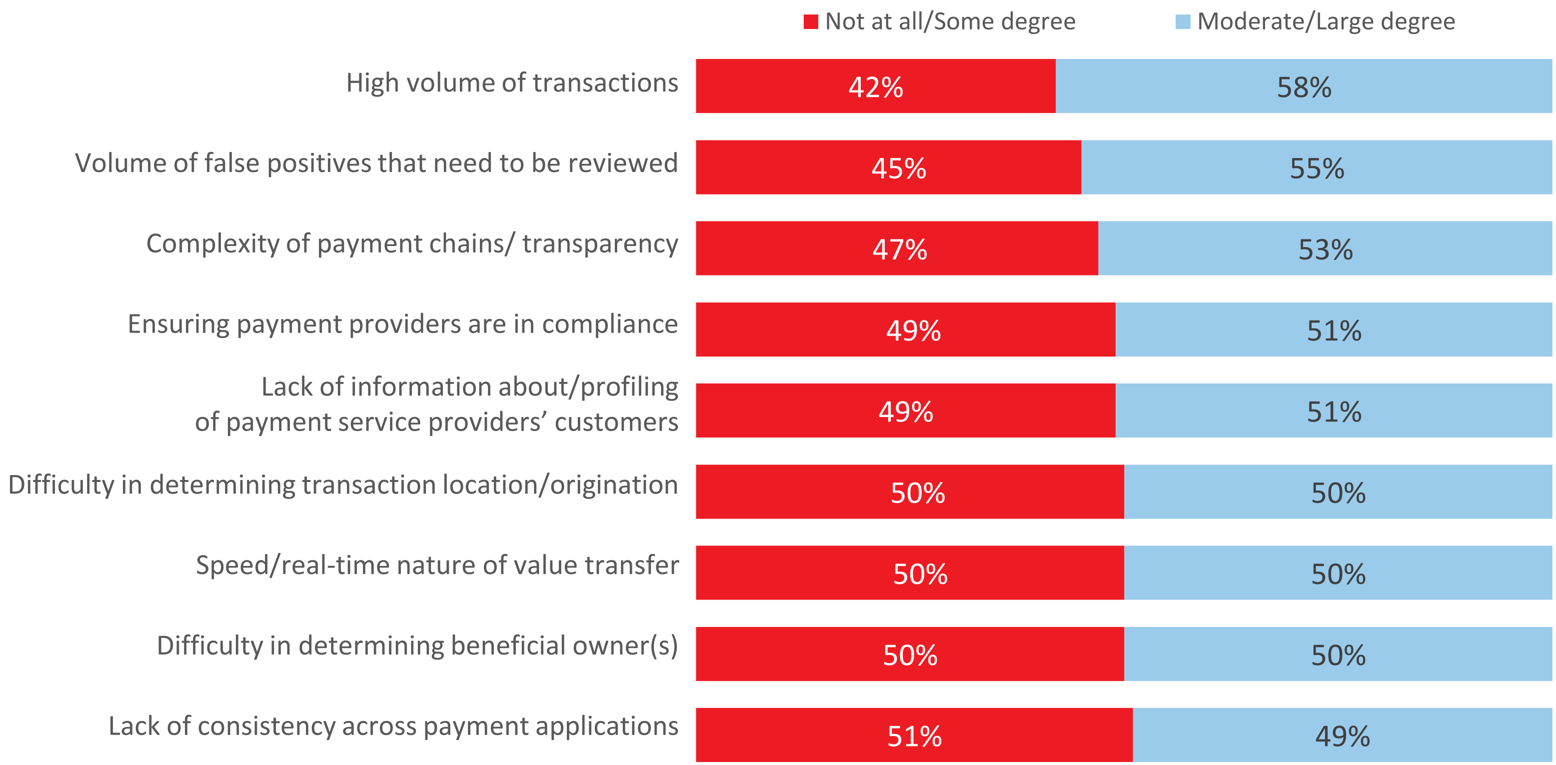


Q5n. In the past year, what is the approximate # of SARs that have been submitted by your AML Compliance operation? Q34: Approximately what % of the SARs submitted involved transactions made through non-bank payment providers? Q35: To what degree have non-bank payment service providers created challenges to your AML compliance processes **during the past year**? Q36: To what degree has the rise in the # of transactions made through non-bank payment providers caused your AML compliance organization to change its screening processes **over the past year**?

Various challenges emerge as the result of screening non-bank transactions.

Those in firms with assets of $10B+ are more likely than others to be challenged by the volume of false positives that need to be reviewed, ensuring payment providers are in compliance, and a lack of information about/profiling of payment providers' customers.

Degree Following Have Been Challenging to AML Compliance Operations When Screening Non-Bank Transactions



% Moderate/ Large Degree

	Small (<$10B)	Mid/Large ($10B+)
High volume of transactions	56%	62%
Volume of false positives that need to be reviewed	46%	69%
Complexity of payment chains/ transparency	50%	58%
Ensuring payment providers are in compliance	39%	73%
Lack of information about/profiling of payment service providers' customers	41%	67%
Difficulty in determining transaction location/origination	44%	59%
Speed/real-time nature of value transfer	53%	45%
Difficulty in determining beneficial owner(s)	48%	54%
Lack of consistency across payment applications	43%	58%

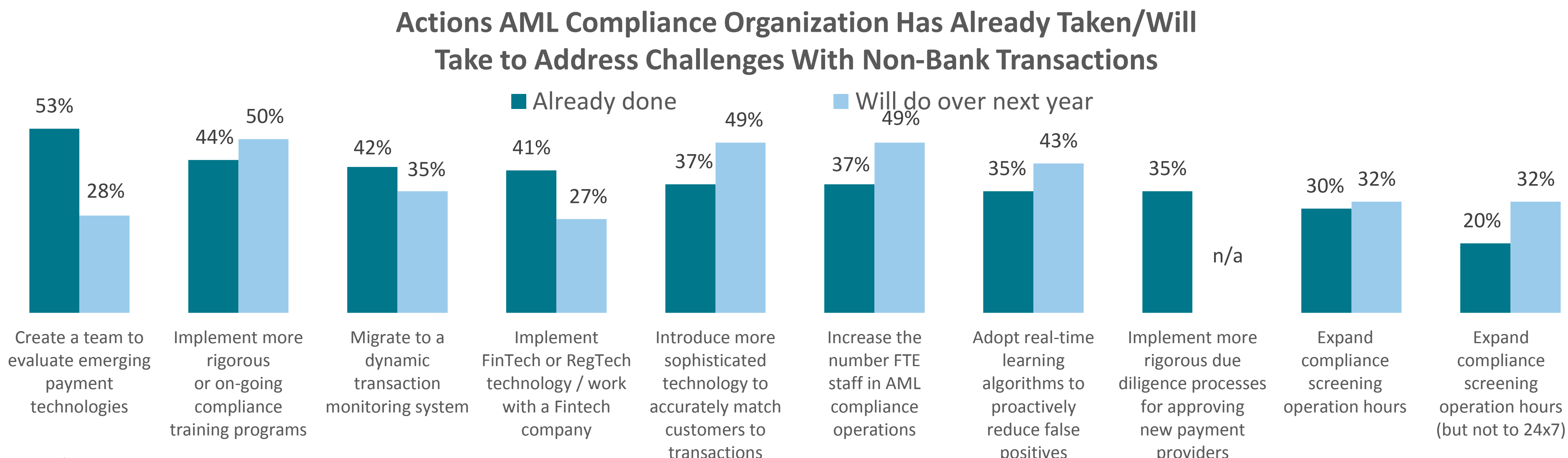
Significantly or directionally much higher than other segments within technology

Q38: Over the past year, to what degree have the following been challenging to your AML compliance operations when screening transactions made through non-bank payment providers?

In response to these challenges, a number of firms have created a team to evaluate emerging payment technologies, implemented more rigorous training, migrated to dynamic monitoring, or implemented FinTech/RegTech.

Only some of those citing increased alert volumes as a non-bank payment provider impact have implemented technology to address false positives (37%), which increase as alert volumes rise.

And, those who have migrated to dynamic monitoring or added FinTech/RegTech technology are as likely as others to also plan on increasing compliance staff (44%/41%), even though compliance technologies could lessen that need and the cost associated with human resources.



Q39a/40: Which of the following has your AML compliance organization already done/will do over next year to address challenges with transactions from non-bank payment providers?

Q39b: What steps has your AML compliance org taken to implement more rigorous due diligence processes for approving new payment providers?

Steps Taken	
Governance procedures & documentation to confirm PSP compliance	*65%*
Require more transparency about PSP transactions	*65%*
Require more PSP customer profiling information	*64%*
Require more transparency of PSP products/services offered	*49%*

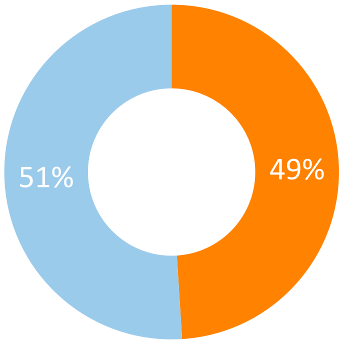
LexisNexis® RISK SOLUTIONS

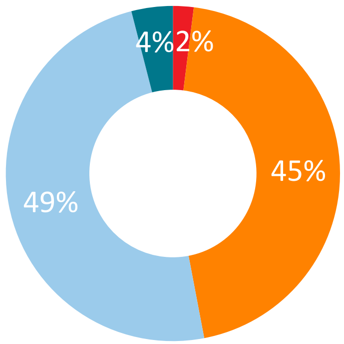
Non-bank payment providers are expected to continue creating challenges for AML compliance, in turn causing at least some changes be made to screening operations over the next year.

Degree That Non-Bank Payment Providers/Systems Are Expected to Create Challenges for AML Compliance Over Next Year

Degree That Rise in Transactions Through Non-Bank Payment Providers/Systems Are Expected to Cause AML Compliance Organization to Change its Screening Operations in Next Year

Not at all | Some degree | Moderate degree | Large degree





Q41: To what degree have non-bank payment service providers and systems created/create challenges to your organization's AML compliance processes/operations **over the next year**?

Q42: To what degree has the rise in the number of transactions made through non-bank payment service providers and systems caused/will cause your AML compliance organization to change its screening operations/processes **over the next year**?

LexisNexis® RISK SOLUTIONS

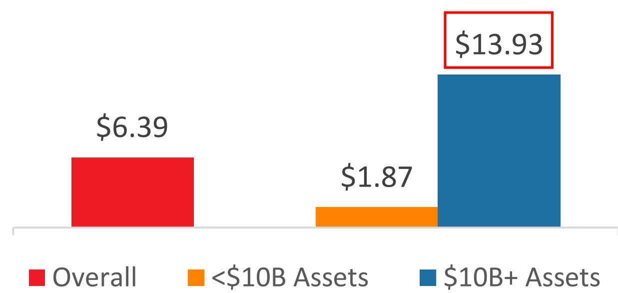
The average annual spend for AML compliance among Singapore financial firms is US$6.39M; it is even higher for firms with $10B+ in assets (US$13.93M).

This spend is split relatively closely between labour and technology.

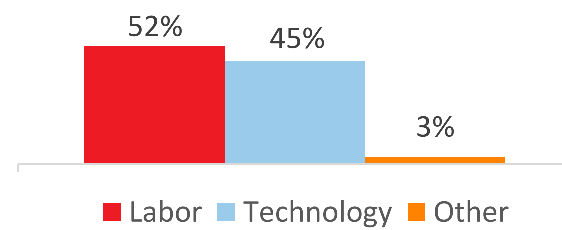
KYC makes up a good share of costs, involving collection of information, screening, analytics and risk assessment, but so too do transaction monitoring, investigations, and compliance management.

Regional findings show that the cost per FTE is lower among firms using more compliance technology / services (*see Regional Findings section*).

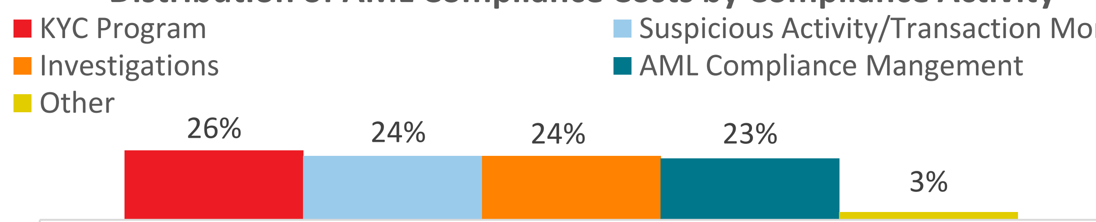
Average of AML Compliance Operations*
(Annual Cost USD in Millions)



Distribution of AML Compliance Costs



Distribution of AML Compliance Costs by Compliance Activity



Q5: Please give your best estimate of the total annual cost of your AML compliance operations in USD.

Q5b: Roughly, what % of this would you say is related to labor/resources, technology/solutions/systems?

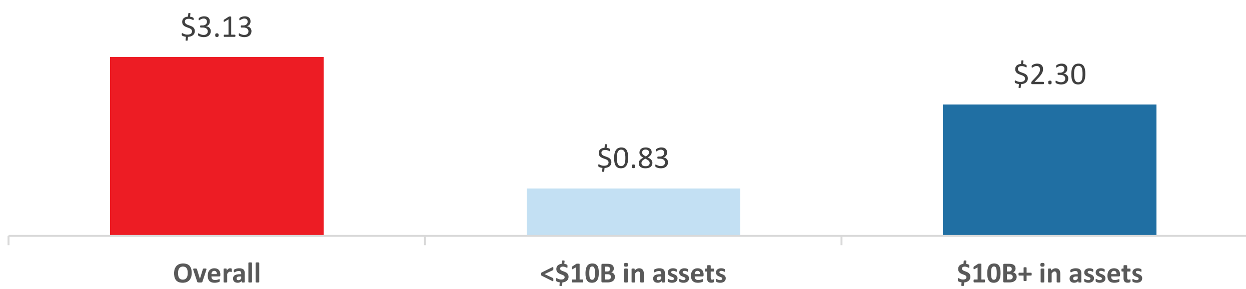
Q6: Please give your best estimate of the % that is spent on each of the following areas…

* Compliance technology, data and services can be shared across different operational and business units, making it difficult for a decision maker to know the full cost of compliance across the organization. Reported spend by survey respondents is based on a very detailed description involving labor, technology and other activities, though theses are estimates which could involve some level of variance.

With a true cost of compliance across Singapore financial firms of US$3.13B*, those with more total assets represent a significantly larger share of spend. However, smaller firms get hit harder.

But while any one/individual $10B+ asset firm spends more per year on AML compliance, there are certain basic overhead investments required for compliance operations regardless of scale. As a result, the actual cost of compliance represents a larger portion of smaller firms' assets (an average of .26% of total assets compared to an average of .06% for larger firms).

True Cost of Compliance Across Singapore Financial Firms
(USD in Billions)



AML Costs as a % of Total Assets	0.18%	0.26%	0.06%

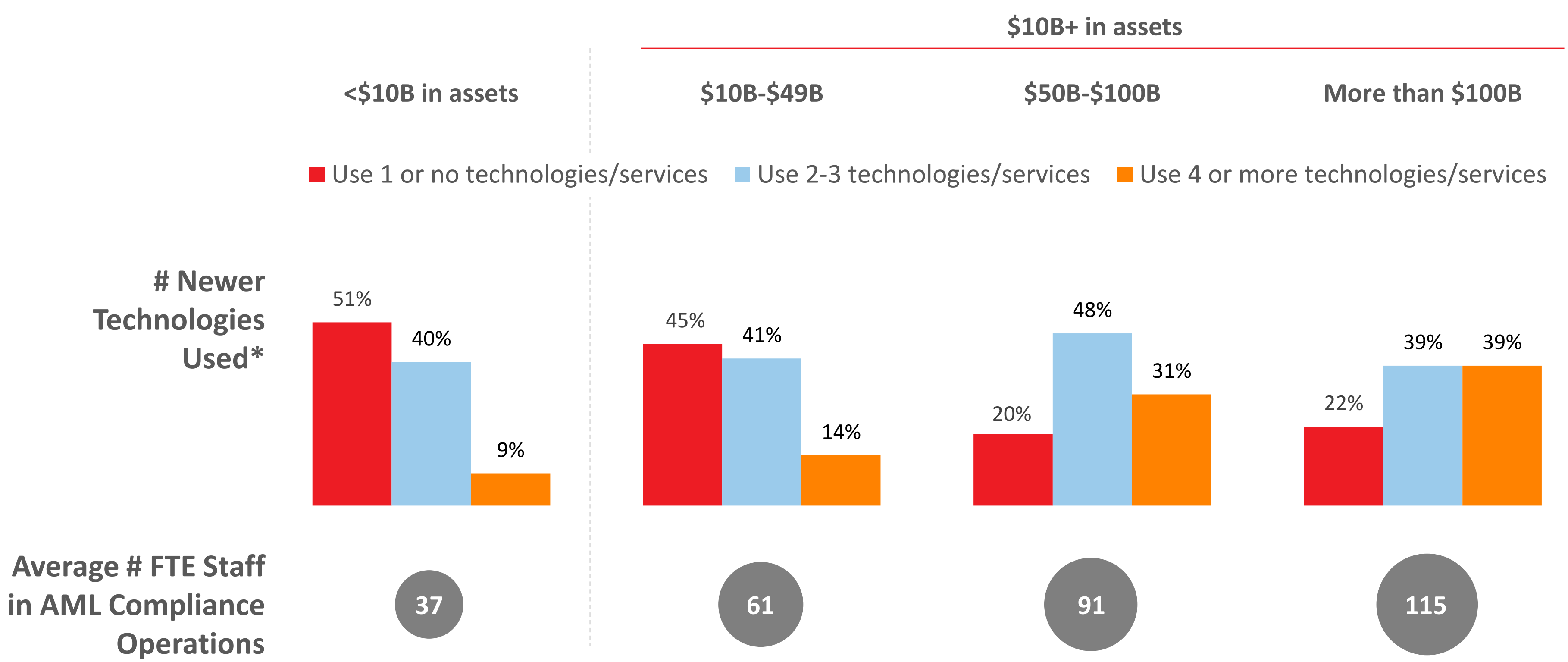
Q5: Please give your best estimate of the total annual cost of your AML compliance operations in USD. This includes resources/labour, systems/solutions/data and other governance activities for all aspects of compliance such as customer due diligence, sanctions screening, transaction monitoring, investigations, reporting, analytics/risk assessment, auditing, training, etc… Q5aa: Roughly, what percentage would you say this spend is of your institution's total assets under management?

* Total annual cost of compliance across firms within the market is extrapolated by multiplying the total number of financial services firms for an asset tier by the average reported AML compliance spend for that tier; the total is the sum of total spend across each asset tier. Since different asset tiers report different AML compliance spend levels, using this "bottoms-up" approach provides a more accurate estimate in order to account for these differences, compared to a more simpler approach of multiplying the overall average by the overall number of firms.

Regional Findings – Technology Usage

Across the APAC countries studied, there is a relationship between size of firm/number of FTEs and the number of newer compliance technologies/services used.

Firms with more assets under management have larger compliance operations teams and use more technologies/services on average than smaller firms.



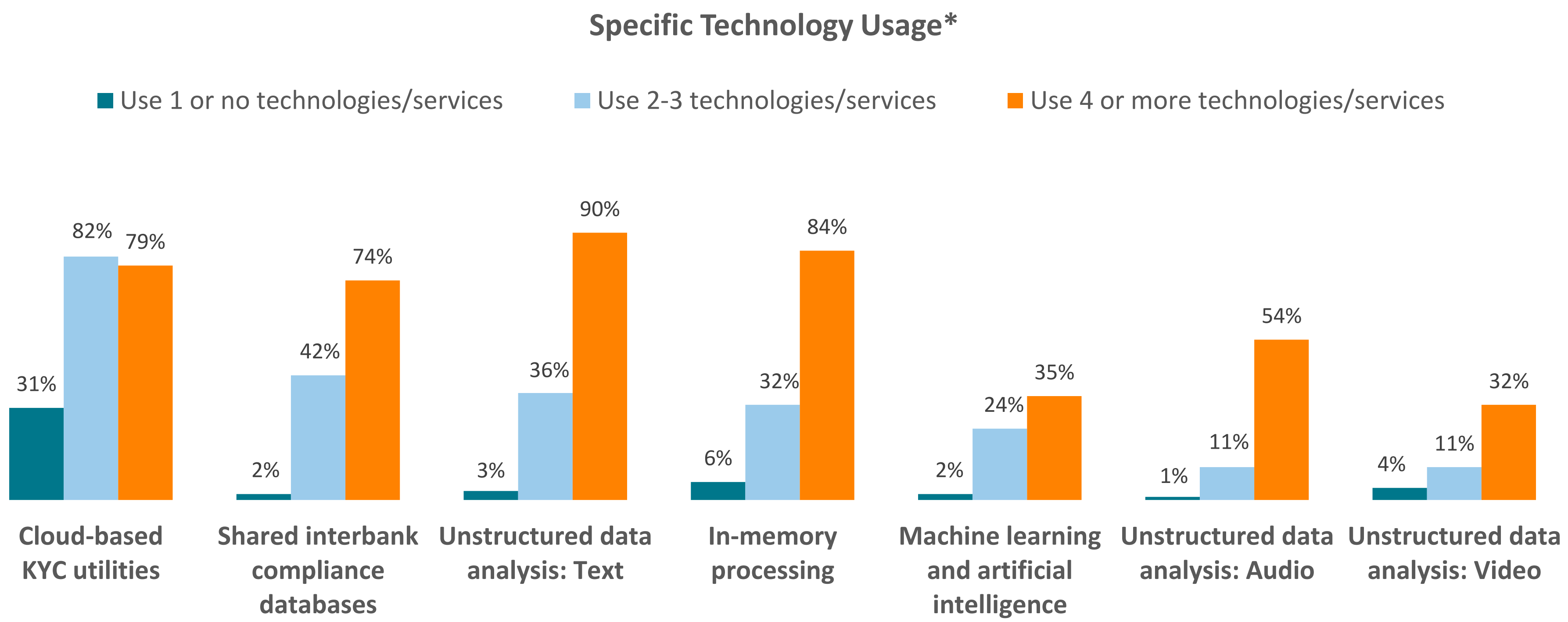
* Includes only those new technologies tested in this research

Q2c: Please indicate your best estimate of the number of FTE staff employed in the AML compliance operations departments. Q16: Over the next 5 years, to what degree do you think each of the following new technologies and services will be relevant to AML compliance?

LexisNexis® RISK SOLUTIONS

Firms using 4 or more technologies/services tend to use various combinations, with unstructured text analysis, in-memory processing, cloud-based KYC utilities, and shared interbank compliance databases being most common.

Cloud-based KYC utilities are also commonly used among those using 2-3 technologies/services; usage of any one technology is limited among those using fewer.



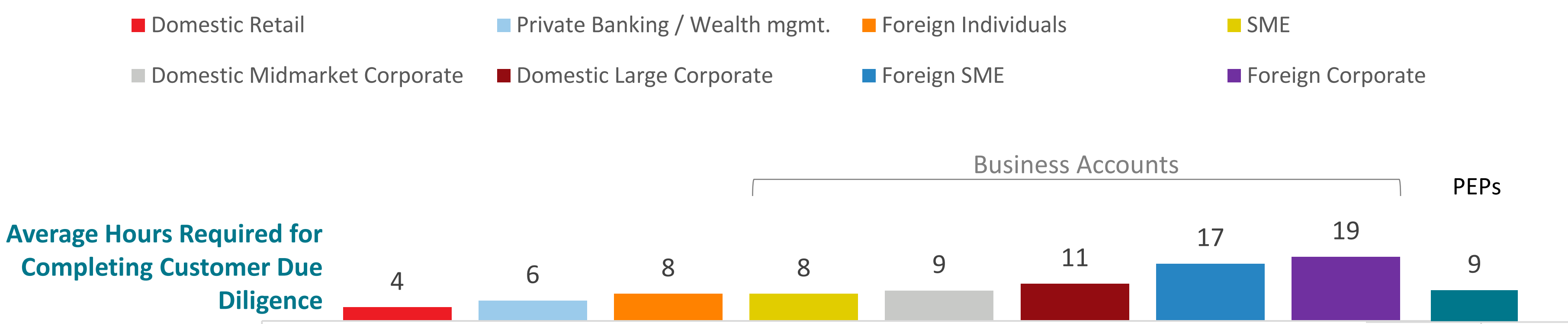
LexisNexis® RISK SOLUTIONS

* Includes only those new technologies tested in this research

Q16: Over the next 5 years, to what degree do you think each of the following new technologies and services will be relevant to AML compliance?

Regional Findings

The use of these 4 or more technologies/services allows APAC financial services firms realize some time efficiencies when conducting due diligence for new accounts.



Use 1 or no technologies/services	4	6	8	9	10	13	20	22	9
Use 2-3 technologies/services	4	5	8	7	8	9	15	18	8
Use 4 or more technologies/services	3	5	7	7	7	8	12	13	7

LexisNexis® RISK SOLUTIONS

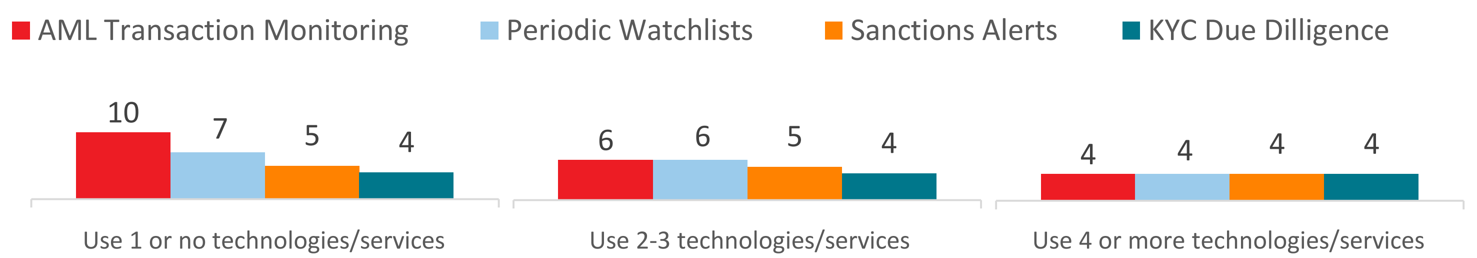
Q17a: What would you say is the average time required for completing customer due diligence on the following?

Those using more compliance technology/services are also able to clear alerts faster than others.

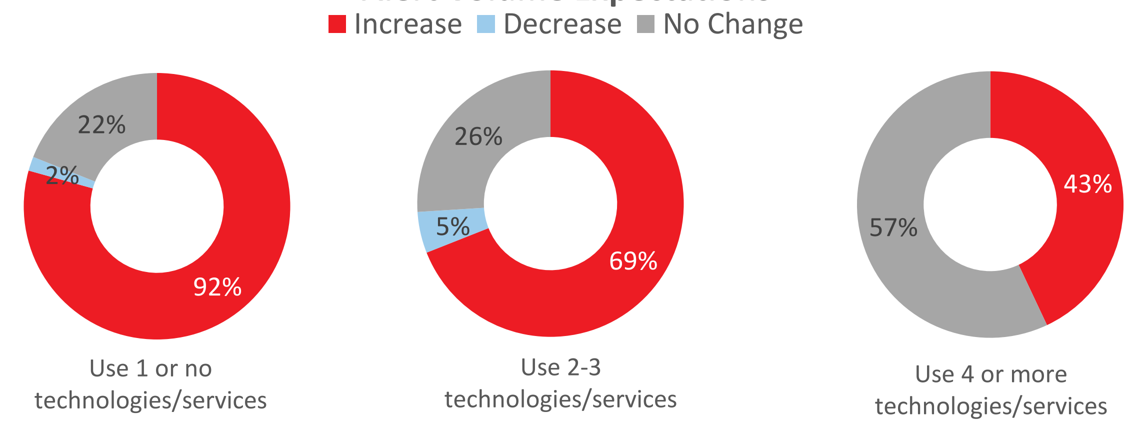
Regional Findings

Interestingly, those which use few or no technologies/services are significantly more likely to expect an increase in alert volumes in 2019, which suggests that they will be less prepared and efficient to handle this if that occurs.

Average Hours to Clear the Following Types of Alerts



Alert Volume Expectations



Q18: What is the average time required for an analyst to clear each of the following alert types?
Q19a: Do you expect alert volumes to increase or decrease in 2019?
Q19b. Percent you expect alert volumes to increase in 2019?

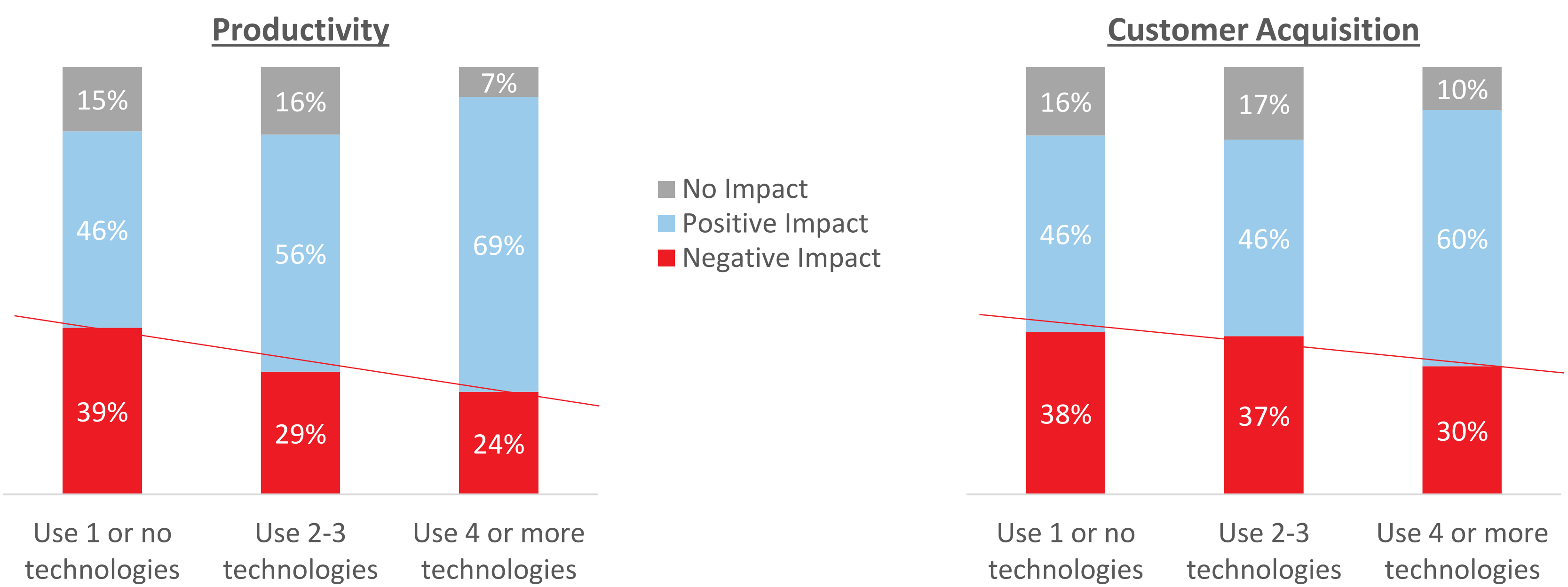
LexisNexis® RISK SOLUTIONS

Relatedly, those firms using more technologies/services are less likely to feel negative impacts of AML compliance on productivity and customer acquisition.

Regional Findings

And even those firms experiencing lost productivity lose fewer hours than those using fewer technologies/services.

AML Compliance Impact on . . .



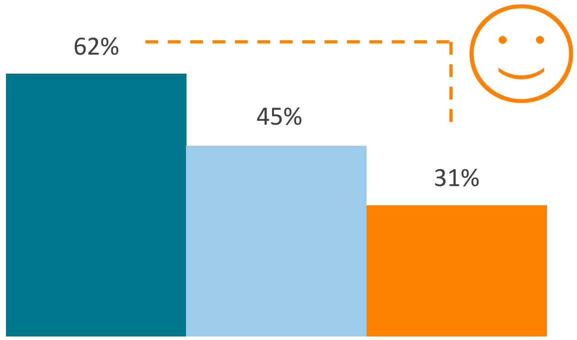
29	25	17	*Annual average hours of lost productivity per FTE*

LexisNexis® RISK SOLUTIONS

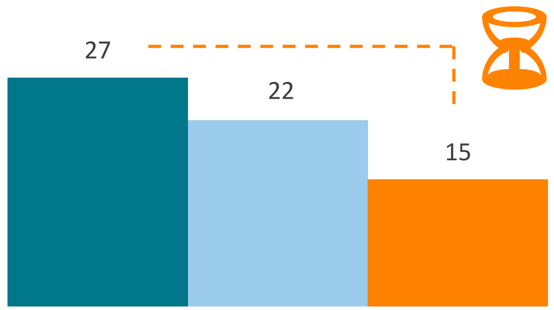
Q20a/22: What kind of impact does the AML compliance process have on LoB productivity/customer acquisition? Q21: What is your best estimate of the annual loss in LoB productivity due to AML compliance at your firm?

Being that FTEs are working more efficiently, there is less concern about job dissatisfaction and fewer hours of lost productivity related to this in firms using 4 or more technologies/services.

% Somewhat to Very Concerned About Job Satisfaction of Compliance Staff



Average Annual Hours of Lost Productivity Due to Job Dissatisfaction



■ Use 1 or no technologies/services ■ Use 2-3 technologies/services ■ Use 4 or more technologies/services

LexisNexis® RISK SOLUTIONS

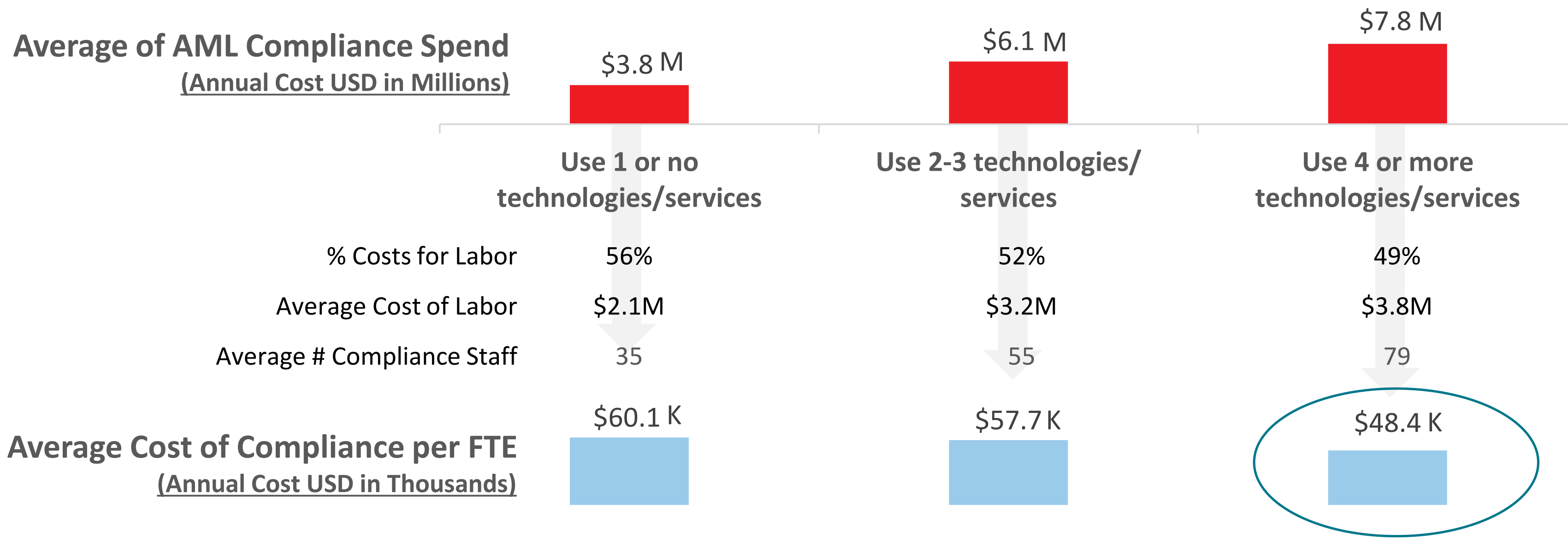
Q14: How concerned are you with job satisfaction in your compliance department?

Q15: What would you say is the annual loss in AML compliance productivity due to job satisfaction issues, expressed in average hours of lost productivity per FTE analyst?

Regional Findings

Though APAC firms that are using more compliance technologies/services have larger initial outlays related to such technology, this can be viewed as an investment to manage longer-term AML compliance costs.

By adding more technology as compliance workforces grow, financial firms are actually decreasing the labor-related cost of compliance per FTE, as well as the opportunity costs associated with onboarding friction and lost business. Keeping FTE costs lower is essential to profitability, since labor tends to account for significant increased expenses year-over-year.



Q2c: Please indicate your best estimate of the number of FTE staff employed in the AML compliance operations departments. Q5: Please give your best estimate of the total annual cost of your AML compliance operations in USD. This includes resources/labour, systems/solutions/data and other governance activities for all aspects of compliance such as customer due diligence, sanctions screening, transaction monitoring, investigations, reporting, analytics/risk assessment, auditing, training, etc… Q5b: Roughly, what % of this would you say is related to labor/resources, technology/solutions/systems?

LexisNexis® RISK SOLUTIONS

* Includes only those new technologies tested in this research

Implications

Implications

- Technology plays an important role in effectively managing the impact of AML compliance on the business.
  - It's not just about managing the direct costs, but also the indirect and opportunity costs that can be harder to measure.
  - And, these opportunity costs are not just about lost prospects and future revenues associated with friction and delays at onboarding. Missing a holistic view with KYC adds the risk of letting "bad actors" in the door, thereby incurring hefty fines and reputational damage.
  - Having accurate data and highly capable solutions generates a degree of utility for not just compliance, but other functional areas as well. This includes business development and marketing; knowing more about customers can help inform the right products and services to position with customers.

- As compliance regulations grow in complexity and translate into more alert volumes, it will become increasingly difficult for APAC financial firms to keep pace, manage false positives, and avoid non-compliance issues. A common reaction can be to add more human resources. However, this is not a profitable long-term solution.
  - The cost of human resources almost always trends upward. At some point, firms will reach a point of diminishing returns.
  - The rise in human resource costs can rise sharply where financial firms feel the need for more skilled resources to address more complex compliance decisions. More demand increases salary demands, especially if there is a limited universe of skilled resources that firms are fighting for.
  - Further, without the support of expanded data sources, bad data can lead to bad decisions regardless of the number of human resources applied to a case.

Implications (cont.)

- It is understood that financial executives, who face personal liability for non-compliance, can be wary of foregoing human input with these decisions. But technology does not need to replace human involvement; it can augment it to improve compliance processes and reduce the need for bringing on more resources (while keeping those you have) – thus “future proofing” against significant cost increases over the long term.
  - Using solutions to help compliance teams analyze existing data, have access to other external information, and make decisions from a more holistic view of the customer can reduce onboarding times, decrease remediation costs, lessen processing times, increase throughput (without hiring more people) and create a more effective means of preventing financial crime over the long term.

LexisNexis®
RISK SOLUTIONS