AML Industry Benchmarking Report 2022

ARCTIC INTELLIGENCE

COMPLIANCE. THE SMART WAY.

ARCTIC-INTELLIGENCE.COM

Table of contents

Executive Summary

About Arctic Intelligence

Arctic Intelligence is a multi-award-winning RegTech firm specialising in software for enterprise-wide audit, compliance, and risk management related to financial crime.

Arctic Intelligence was founded in 2015 and is trusted by hundreds of large and small clients across 20+ industry sectors across the world. Our vision is to combine purpose-built technology with financial crime expertise. Our platforms help businesses identify and assess risks and build appropriate and proportionate control frameworks to mitigate and manage them.

Our goal is to uplift the capability and capacity of regulated businesses to understand the financial crime risks they are exposed to from organised criminal networks and help them strengthen their defences against these risks.

Why enterprise-wide risk assessments?

Business-wide or Enterprise-wide Risk Assessments (or EWRA) are mandatory for millions of businesses globally. However, they are still overwhelmingly conducted manually on spreadsheets.

We believe technology has a more significant role in managing enterprise-wide financial crime risks.

Why did we create this report?

Money laundering and terrorism financing laws apply to millions of businesses, across 30+ industry sectors, and in over 200 Financial Action Task Force (FATF) member countries. And yet, there is no industry standard on how businesses should apply the risk-based approach.

The risk-based approach puts the onus on regulated businesses to identify and assess financial crime risks and then implement, monitor and continuously improve the control framework to effectively mitigate and manage these risks.

Regulators provide guidance on 'what' constitutes a risk but generally leave it to regulated businesses to determine the 'how'. The how involves designing an appropriate ML/TF risk assessment methodology, determining the risks to assess, deciding what controls to implement that are appropriate and proportionate to managing the risks and testing the design and operational effectiveness of these controls.

Despite this guidance, many regulated businesses struggle with the 'how' and it is our goal at Arctic Intelligence to help businesses with designing and implementing robust enterprise-wide financial crime risk assessments.

In our second AML Industry Benchmarking Report, we unpack the key findings, observations, and recommendations based on hundreds of ML/TF risk assessments.

Executive Summary

About the AML Industry Benchmarking Report

In 2021, we released our first AML Industry Benchmarking Report. It has been downloaded by thousands of people across the financial crime ecosystem, including regulators, consultants, and organisations interested in seeing how they compare to their peers.

The 2022 AML Benchmarking Report builds on this and takes an even deeper dive into EWRAs using aggregated data from hundreds of risk assessments and hundreds of survey respondents. We hope the report's insights can help organisations better understand ML/TF risks and the effectiveness of specific controls to reduce residual risk exposures.

About the data

157 respondents from **41 countries** responded to the public survey. The top 3 being Australia, Hong Kong and the US.

181 **Risk assessments** analysed.

6 main industry sectors are represented, of which 75% are Financial Services.

6 **countries** are represented from 2021.

Hundreds of data points were assessed.

In the report, we take an in-depth look at the methodology and data sets used.

Top 3 Key Findings

1 Dramatic reduction in the **time spent** conducting ML/TF risk assessments for platform users compared to non-users across all industries. An average of **23.5 days** for users compared to non-users surveyed who reported **up to 3 months** (49%), up to 6 months (13%), with 24% unsure of how long it takes to complete.

2 **33%** of survey respondents refresh their ML/TF risk assessment **every year**, while **9%** refresh **every 2 years**.

Surprisingly, **8%** reported a refresh **every 6 months** and 33% whenever a change occurs.

3 The top 3 challenges reported from the survey were (1) Gathering risk assessment data and evidencing effectiveness **(48%)**; (2) Developing the ML/TF risk assessment methodology **(47%)**; and (3) Understanding regulatory obligations **(32%)**.

What else is covered?

We delve into the common risk assessment challenges and the role Regulatory Technology (RegTech) plays in uplifting risk management capabilities.

We look at the top-line inherent risk, control effectiveness, and residual risk ratings before deep diving into each risk group, drawing insights and observations, and wrap up with some closing thoughts.

We hope you enjoy it!

Introduction and Methodology

Following the launch of last year's inaugural AML Industry Benchmarking Report, we are proud to bring you the 2022 AML Industry Benchmark Report, which is jam-packed with fascinating facts, figures, insights and observations about the global level of maturity in conducting ML/TF risk assessments.

Having spent hours pouring over the results compiled into hundreds of different charts, graphs and statements, we have applied our observations and recommendations in the hope it helps to raise the bar on how enterprise-wide risk assessments can, and should be conducted in the future.

Whilst some regulated businesses have progressed at maturing their ML/TF risk and control frameworks, much more can be done. Overwhelmingly, EWRAs are still conducted manually, infrequently, and are often unexplainable. Manual approaches are not only inefficient but are ineffective at delivering risk assessment information in a timely and accurate manner, free from bias.

There is still a long way to go until digitised approaches to financial crime risk assessments become mainstream. We invite regulators, regulated businesses and consultants to raise their game and explore how technology can help uplift their capabilities – ultimately so you can spend far less time gathering data and far more time understanding and managing financial crime risks.

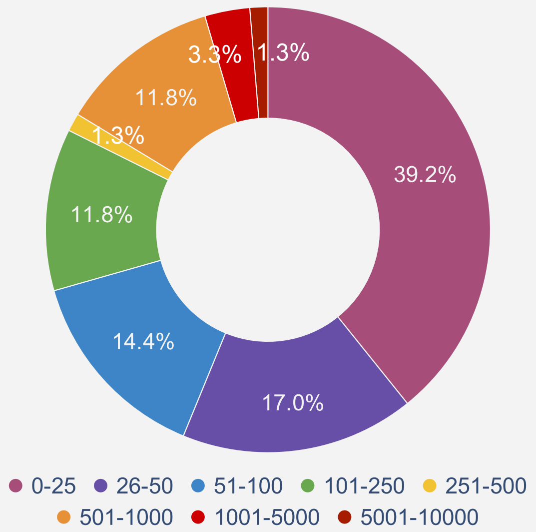
Anthony Quinn
Founder and CEO

Anthony.Quinn@arctic-intelligence.com

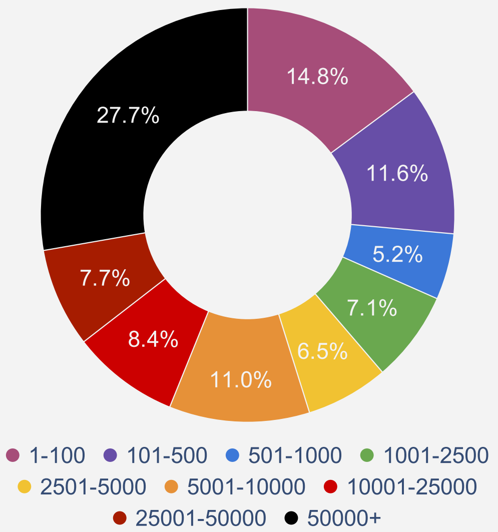
Source Data Set

These insights are based on a data set of 181 risk assessments by Arctic Intelligence customers in 2021 and survey responses from our customers and other respondents from diverse organisations, predominantly from the financial crime risk and compliance functions. The data covers multiple countries, industry sectors, and organisation sizes.

Risk assessments by number of employees



Risk assessments by number of customers



Risk assessments by country

6 countries represented.

Risk assessments by industry type

- Financial Services (75%)
- Gaming and Wagering (17%)
- Legal (5%)
- Real Estate (1%)
- Accountants and Bookkeepers (1%)
- Bullion Dealers (1%)

Risk Assessment Challenges

AML/CTF Risk Assessment Challenges

There are several challenges to identifying and assessing an organisation's risks and vulnerabilities to money laundering and terrorism financing.

Nearly half of the respondents to the survey reported struggling to develop a robust methodology and gather the right data.

Top 3 Risk Assessment Challenges*

1 **48%** Gathering risk assessment input data and evidencing effectiveness

2 **47%** Developing the risk assessment approach and methodology

3 **32%** Understanding regulatory obligations

* % based on respondent's surveys

Risk Assessment Challenges

Most surveyed organisations conduct risk assessments intermittently, which could be because the majority also reported taking many months to complete them. In contrast, our clients take an average of just 23 days with our platforms.

How long does it take to complete risk assessment?*

49% – Up to 3 months

13% – Up to 6 months

14% – Up to 12 months

24% – Unsure

How frequently do you conduct risk assessments?*

33% – Whenever there is change

31% – Once a year

15% – Unknown/Unsure

9% – Once every 2 years

8% – Every 6 months

4% – Whenever told to do so

What do you find most challenging?

Based on survey responses, collecting evidence, developing a methodology, and understanding regulatory risk assessments were among the most significant challenges encountered.

#	Responses	Respondents	%
1	Collecting documentation/evidence	76	48.41%
2	Developing the approach and methodology	75	47.77%
3	Understanding regulatory obligations	51	32.48%
4	Consistency in collecting and preparing results	45	28.66%
5	Preparing reporting	44	28.03%
6	Relying on internal teams to input to assessments	41	26.11%
7	Rolling out and managing the process across teams	34	21.66%
8	Approval by senior management	33	21.02%

* % based on respondent's surveys

Risk Assessment Challenges

There are many challenges faced by organisations in building an effective enterprise-wide ML/TF risk assessment.

1

Setting Board ML/TF Risk Appetite

Does your Board understand enough about ML/TF risks to set risk statement and risk tolerances?

2

Deciding what methodology to use

Is your ML/TF risk assessment methodology and framework logical, explainable and defendable?

3

Appropriateness of EWRA

Is your ML/TF risk and controls assessment appropriate and proportionate given your nature, size and complexity?

4

Objectivity vs. Subjectivity

Does your EWRA strike the right balance between question based (subjective) and data based (objective)?

5

Deciding what risks to assess

How do you decide the risk groups, risk categories, risk factors and risk indicators to assess?

6

Applying relative weightings

Are all risks and controls treated equally or can you allocate weights to higher risks and key controls?

7

Control effectiveness testing

How do you decide and assess the existence and effectiveness of control design and operational performance controls?

8

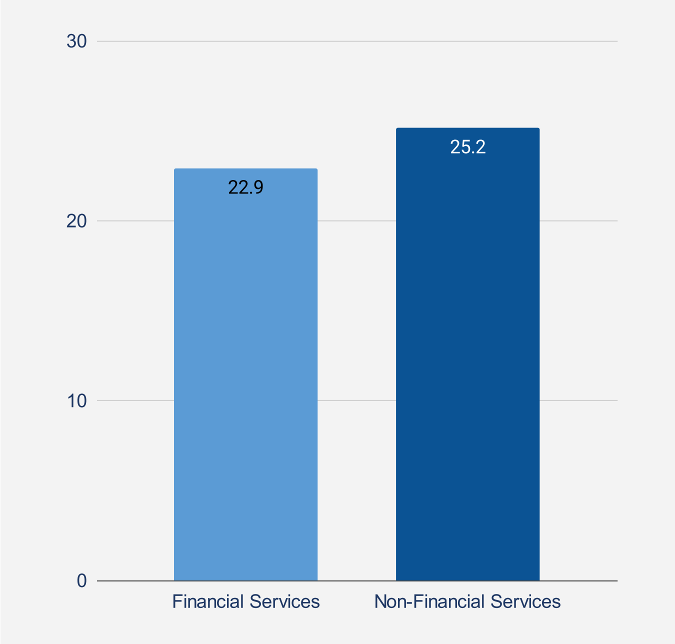
Keeping EWRA's current and compliant

How often is this done? How is it kept updated with changing threats, environments, and laws?

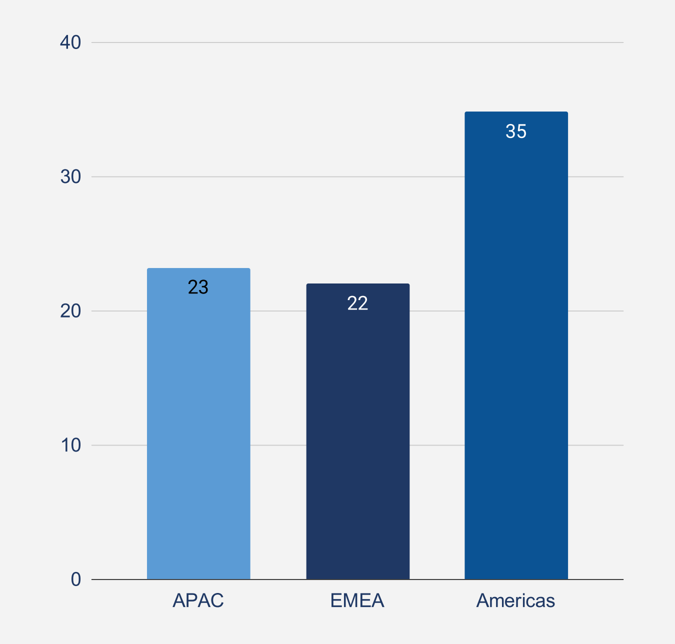
Technology Delivers Time-Savings

The time taken to design an ML/TF Risk Assessment Framework and roll-out and coordinate the process across the enterprise remains in the top 3 challenges.

Average number of days by sector



Average number of days by region



Our clients took an average of 29 days to conduct the enterprise ML/TF assessment across all industry sectors and regions.

This is in stark contrast to public survey participants that do not use technology to conduct ML/TF risk assessments who reported that the time taken to design ML/TF risk assessment frameworks and conduct these across the enterprise took considerably longer and remains a significant challenge.

As well as time savings, our clients reported numerous other benefits associated with adopting technology to conduct enterprise-wide risk assessments, which we have summarised on page 14 of this report.

Enabling Technology

Why RegTech?

Survey results have shown that the ML/TF risk assessment process can be a cumbersome and time-consuming process passing multiple versions of spreadsheets back and forth over email and then consolidating and analysing the results manually making this a challenge for many.

Respondents to the survey stated that they have either adopted or plan to adopt RegTech solutions across their business based on the features and benefits that they see will deliver significant value to their organisation. Much of the RegTech adoption reported has been in the KYC and Transaction Monitoring space, with businesses just starting to look beyond that.

Desired Features

Centralised platform for completing ML/TF risk assessments with audit trail

Reduce the time spent conducting ML/TF risk assessments

Ability to have multiple team members simultaneously completing the assessment

Ability to conduct ML/TF risk assessments easily across the enterprise

Ability to demonstrate and evidence the risk assessment and mitigating controls

Being able to explain and defend the inputs and outputs to Boards and Regulators

Ability to see real-time reporting across the enterprise at any given point in time

Peace of mind that the ML/TF risk assessment has been completed transparently

Enabling Technology

Removing the barriers to RegTech adoption

We asked our respondents whether they were looking to adopt RegTech to digitise their enterprise-wide risk assessments (EWRA) and what they need to see to build a business case and obtain approval, and the key features they are looking for in an EWRA solution.

Does your organisation have plans to digitise your risk assessment process?

Response	#	%
We have already digitised	32	20.38%
Actively looking for an EWRA solution now	19	12.10%
Actively looking for an EWRA solution in next 3-6 months	14	8.92%
Expect to adopt an EWRA solution in next 12 months	24	15.29%
Not in the foreseeable future	64	40.76%
Unknown	4	2.55%

What functionality/features would you like to see in a risk assessment solution?

Response	#	%
A solution that provides a structured, intuitive process which we did not have	70	44.59%
A solution that allows me to have oversight of the work across the organisation	65	41.40%
A solution that provides the ability to manage this process centrally	59	37.58%
A solution that provides a structured, intuitive process which we did not have	57	36.31%
Peace of mind that we have a secure process in place	53	33.76%
ROI in year 1	25	15.92%
ROI in year 3	19	12.10%

If you're not looking at RegTech for EWRA, why not?

For regulated businesses (and their risk advisers) conducting financial crime risk assessments manually using spreadsheets – ask yourselves, or your vendor/ consultant these questions.

- [ ] How is the ML/TF risk assessment methodology documented and can it be modified?
- [ ] How easy is it to add/modify my own risks and controls into the ML/TF risk methodology?
- [ ] What is the process for gathering data and generating reports across the enterprise?
- [ ] How long on average does it take to plan and execute a ML/TF risk assessment process across the enterprise?
- [ ] How do you keep track of the audit trail including why risks were assessed in a particular way?
- [ ] Does the ML/TF risk assessment apply proportionate weightings to risks and controls?
- [ ] How do you demonstrate supporting documentary evidence that justifies risk decisions?
- [ ] How do you evidence the existence and effectiveness of controls testing performed?
- [ ] Can you produce a real-time dashboard on the state of the risk assessment at any point in time?
- [ ] How easily can you standardise and repeat the risk assessment and compare the results over time?

Is it time to uplift your risk assessment approach?

RegTech benefits are beyond doubt

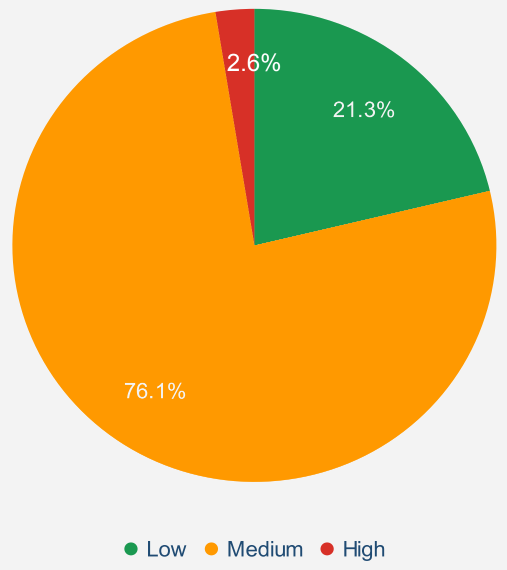
RegTech adoption delivers better risk and compliance outcomes than traditional approaches. These are some of the benefits our clients have realised.

- **Auditability** - chronological history of all your risk assessments and supporting documents in one place with a field level audit trail to explain to Boards and Regulators all risk decisions.
- **Reliability** - solutions are designed, built and maintained by industry experts, with ongoing roadmap enhancements based on continuous feedback from clients, partners and regulators.
- **Efficiency -** significantly reduces the time and effort of conducting complex risk assessments across multiple assessment units in identifying and assessing risks.
- **Standardisation** - by adopting a common approach to risk methodologies, risk models and control libraries prevents *"reinventing the wheel"* every time a risk assessment process is started.
- **Repeatability** - by adopting a platform-based approach it means risk assessments can easily be repeated allowing for time-based and assessment level benchmarking.
- **Configurability** - tailor the risk assessment methodology, content and assessment units to suit your organisations requirements and set granular role-based access permissions.
- **Explainability** - by basing risk assessments on a robust methodology, framework and process it makes it easier to explain and defend to Boards and Regulators.
- **Flexibility** - you have the option of using our expert developed content modules, importing your own or creating a hybrid of the two, allowing full flexibility and control over the platform.
- **Workflow -** easily understand the completeness of risk assessments and where risk indicators are awaiting review and approval across the enterprise, supported by action and issue tracking.
- **Enterprise-wide analytics** - reduces the time spent gathering and analysing risk assessment data by having real-time dashboards and analytics across the enterprise.
- **Support** - our team is with you every step of the way and can provide advice and support in configuring the platform and executing risk assessments and keep you up-to-date on regulatory changes.
- **Record Keeping** - is easy with all documents stored in one place providing an immutable record of the risk assessment that has taken place and any documentary evidence considered.
- **Self-sufficiency** - reduce the reliance on expensive consultants or reduce key person risk by digitising the end-to-end risk assessment process.
- **Time and cost savings** - are delivered by significantly reducing the time it takes to conduct enterprise-wide risk assessments, meaning more time is spent managing risks, not documents.

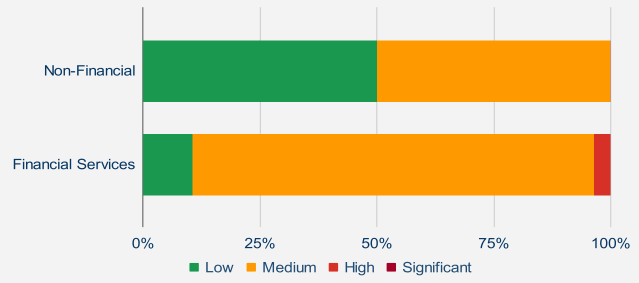
Overall ML/TF Inherent Risk

Overall ML/TF Inherent Risk means the level of risk present across the business (all risk groups) without taking into consideration the existence and effectiveness of controls to mitigate and manage this risk. Only 2.6% of risk assessments have an overall inherent risk rating of high, with over three quarters (76%) reporting medium and the rest low (21%). Regulatory guidance suggests that many industry sectors are considered higher-risk, for example, gaming. This is inconsistent with how some clients perceived their inherent risks.

Overall Inherent Risk Rating

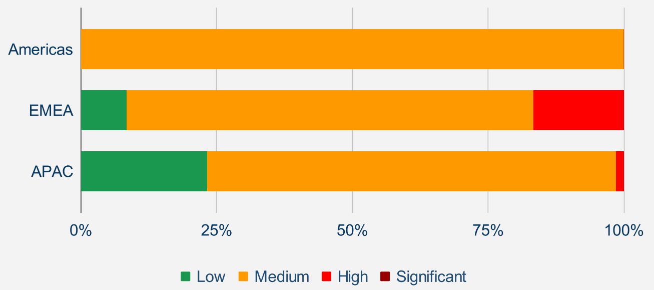


Overall Inherent Risk by Industry



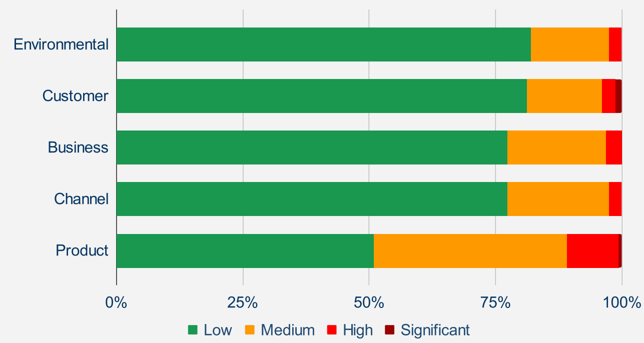
Surprisingly, no respondents outside financial services assessed their inherent risk rating to be high.

Overall Inherent Risk by Region



Only a small proportion of regions, assessed their inherent risks to be high

Overall Inherent Risk by Risk Group

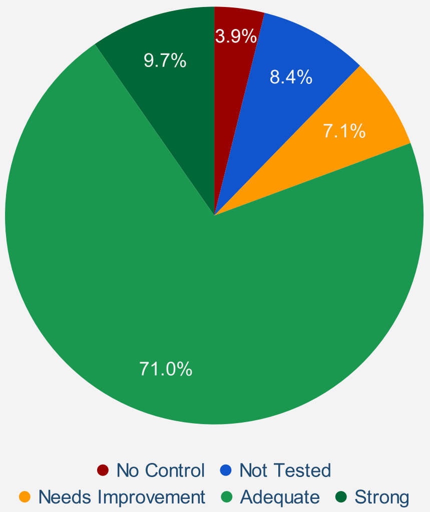


Product risk was reported to pose the most inherent risk of all the ML/TF risk groups.

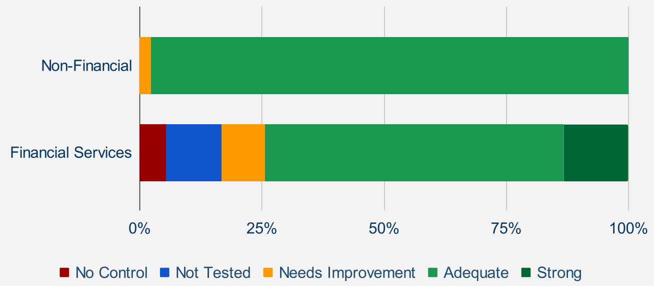
Overall Controls Effectiveness

Overall Control Effectiveness is an indicator of the existence and effectiveness of mitigating controls. Across our clients, less than 10% of controls were considered strong, with 71% being adequate. In addition, over 10% assessed that no controls existed, or if they exist, have not been tested, with the balance recognised as needing improvement.

Overall Controls Effectiveness Rating

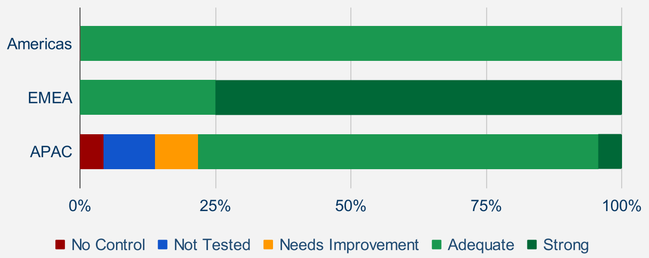


Overall Control Effectiveness Rating by Industry



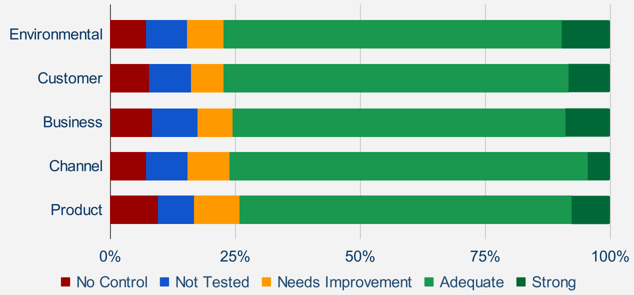
Very few assessments had strong controls, and most were rated as adequate.

Overall Control Effectiveness by Region



Respondents from the Americas noted all controls were adequate, whilst in EMEA 30% were assessed as adequate with 70% assessed as strong. Meanwhile, in APAC only a very small percentage rated their controls as strong.

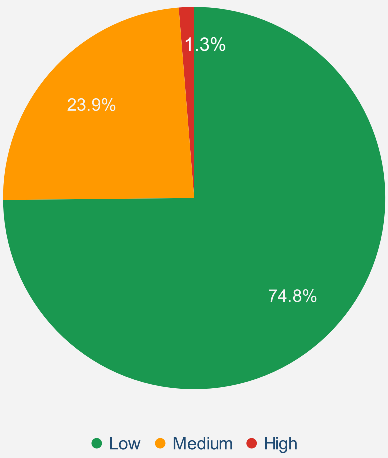
Overall Control Effectiveness by Risk Group



Overall Residual Risk

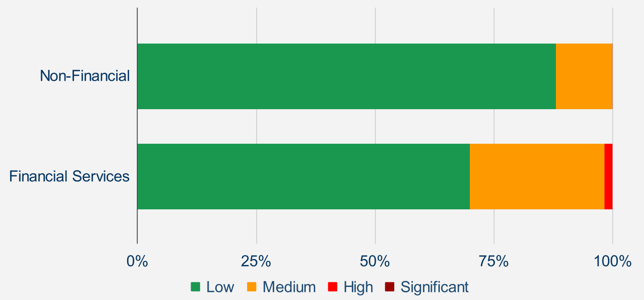
Most organisations have a low risk appetite for financial crime related incidents so it is unsurprising to see 74.8% low residual risk rating (down from 78% last year), with 23.9% medium and only 1.3% of respondents rating residual risk as high. Given the number of money laundering failures around the world, the predominance of low residual risk ratings across all industries and regions indicates the perception of mitigating controls is high.

Overall Residual Risk Rating



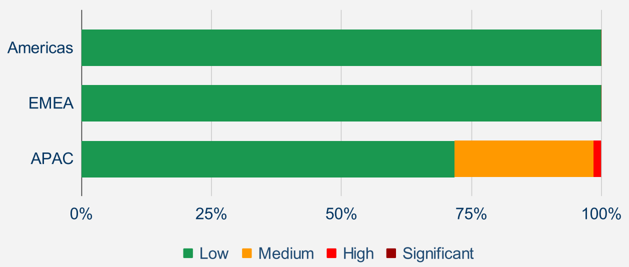
Most organisations assessed their overall residual money laundering risks to be low.

Overall Residual Risk Rating by Industry



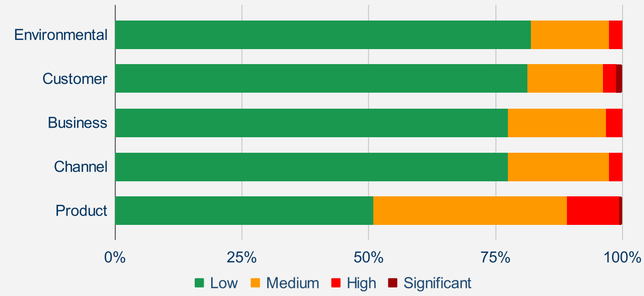
In financial services, where there is a higher report of exploitation by criminal networks, the residual risk is slightly higher than non-financial services due to mitigating controls.

Overall Residual Risk by Region



Globally, very few organisations feel they are at risk to money laundering.

Overall Residual Risk by Risk Group

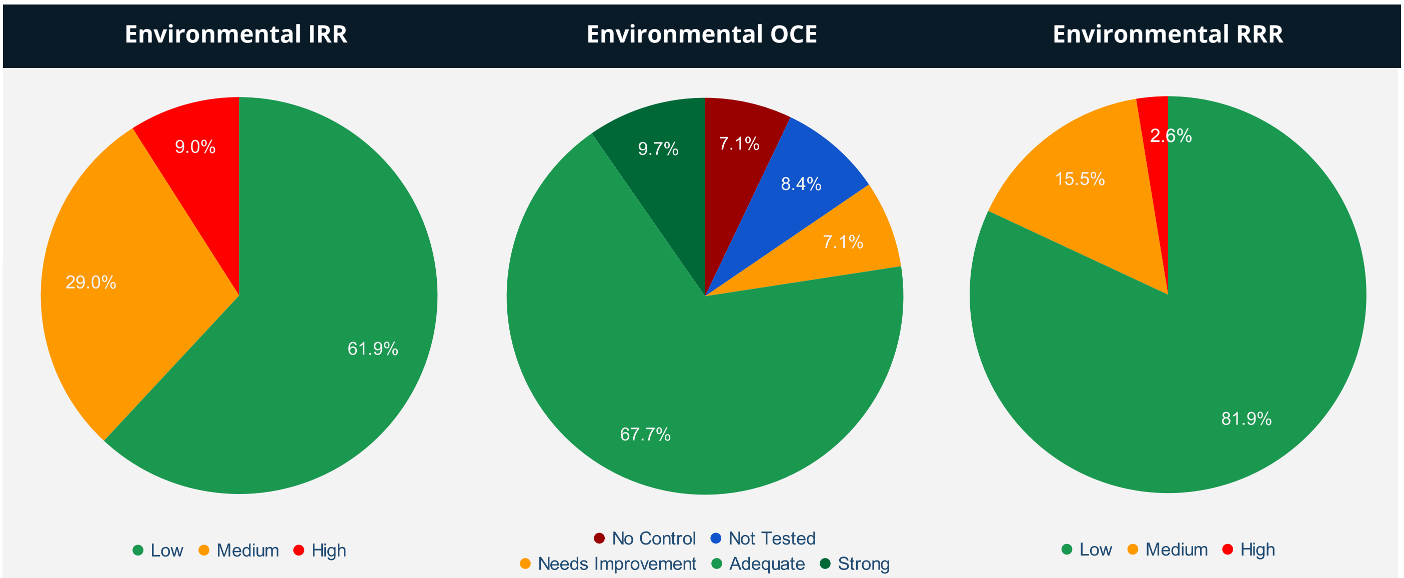


Many products are considered to pose higher risks for money laundering but very few were assessed as high risk after considering mitigating controls.

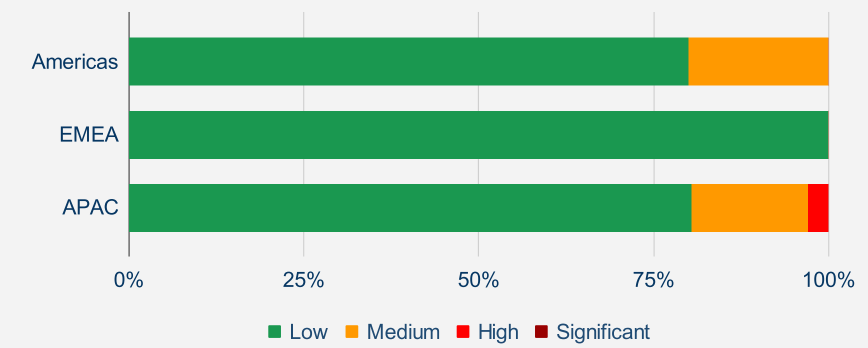
Detailed Findings by Risk Group

Environmental Risk

Environmental risk is the vulnerability to money laundering and terrorism financing risks because of the external and internal environment that businesses operate in. This section summarises the Inherent Risk Rating (IRR), Overall Control Effectiveness (OCE) and Residual Risk Rating (RRR) as it relates to Environmental risk.

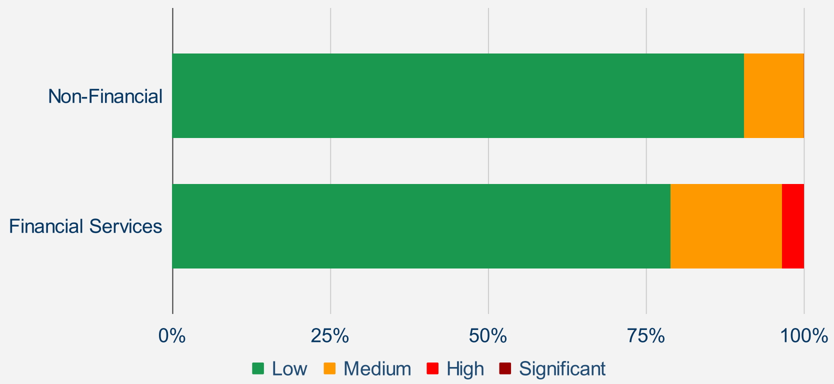


Only a small proportion assessed environmental risk to be high, with most (~80%) assessing controls as adequate or strong.



This trend was consistent across organisations in each region that see limited residual risk in their internal or external operating environments.

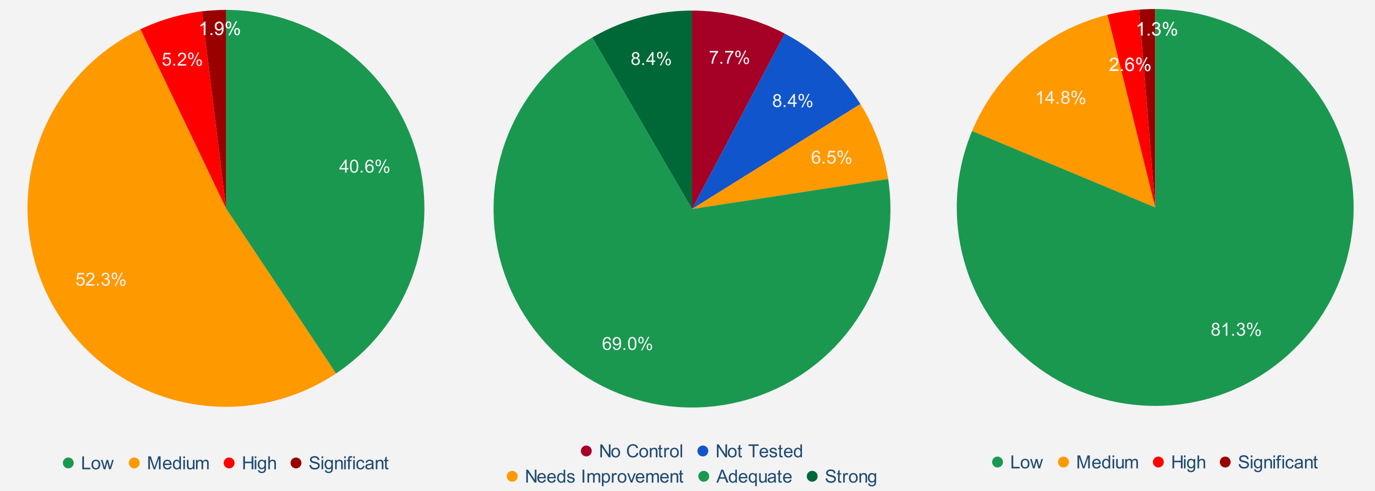
This theme continued regardless of industry sector.



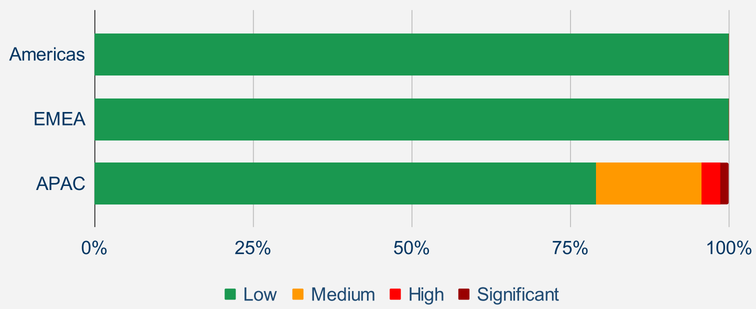
Customer Risk

Customer risk is the risk that customers may be laundering money or funding terrorism. Risks include customers who are located in higher risk countries, are engaged in higher ML/TF risk businesses or occupations, or where customers are Politically Exposed Persons (PEP), or operate higher risk legal structures.

Customer IRR	Customer OCE	Customer RRR

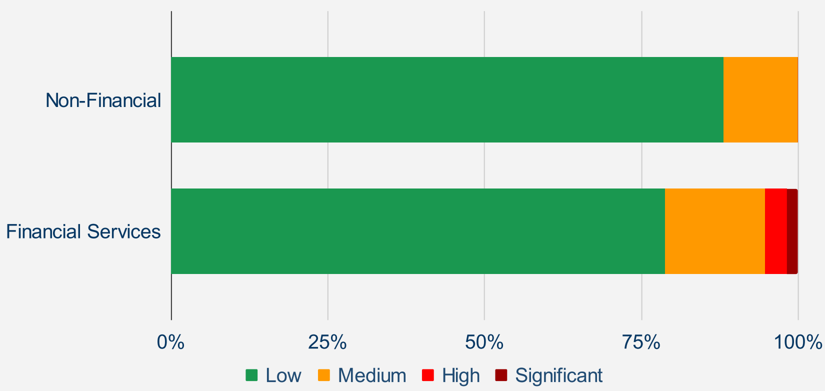


Only a very small proportion (7.1%) of customers were assessed as being high risk, with most reporting controls as strong or adequate.



The residual customer risk was predominantly low as a result of adequate controls across all regions.

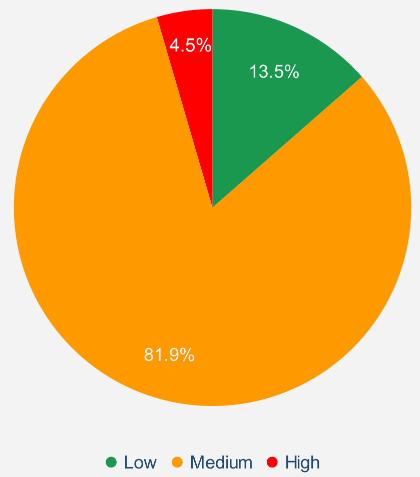
A small proportion of assessments in Financial Services had a high customer residual risk, with none in the Non-Financial Services industries.

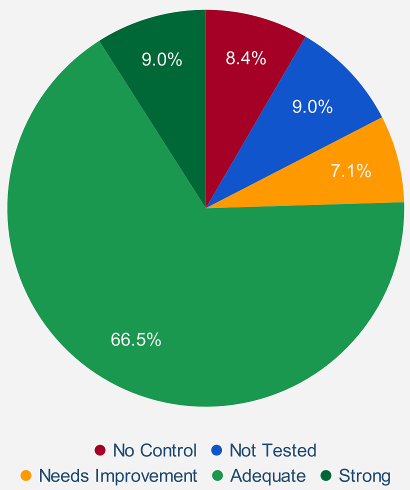


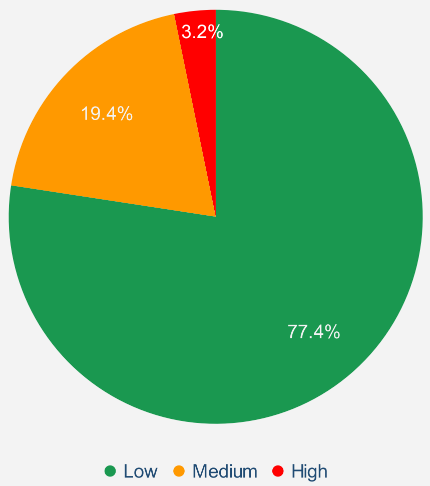
Business Risk

Business risk is the risk resulting from an organisations, business operations and includes higher risks posed by operating in higher risk countries or locations, outsourcing ML/TF controls to third parties or the risks that internal employees face based on the roles and functions they perform.

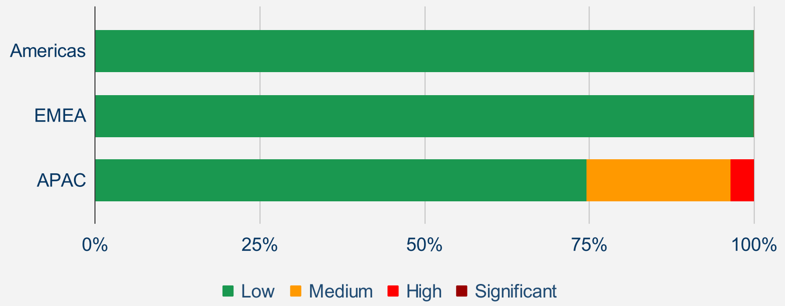
Business IRR	Business OCE	Business RRR





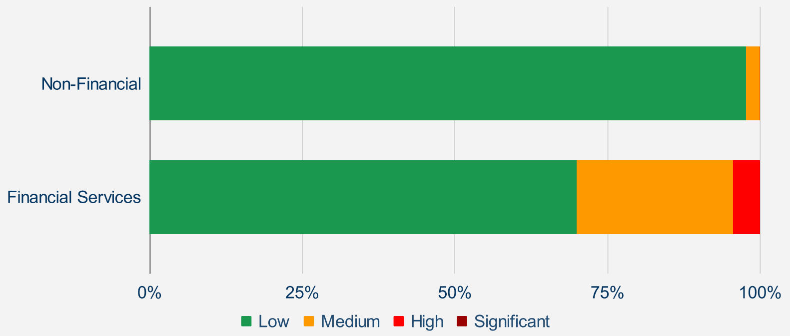


Most assessed their inherent business risk as medium. With a majority rating their controls as adequate, the resulting residual business was low for 77% of assessments, with 19% medium, and 3% high.



Less than 4% of APAC reported business residual risk to be high and in EMEA and North America no organisations reported this risk to be high.

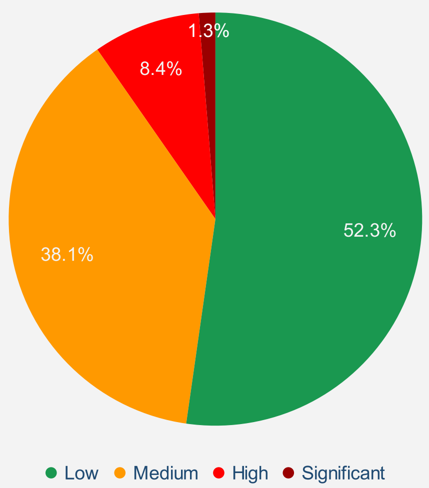
In Financial Services, 70% assessed their overall business residual risk to be low, with 26% medium and 4% high.
In Non-Financial Services, which include Gaming and designated non-financial services, none assessed their overall business residual risk as high, with 98% as low and 2% as medium.



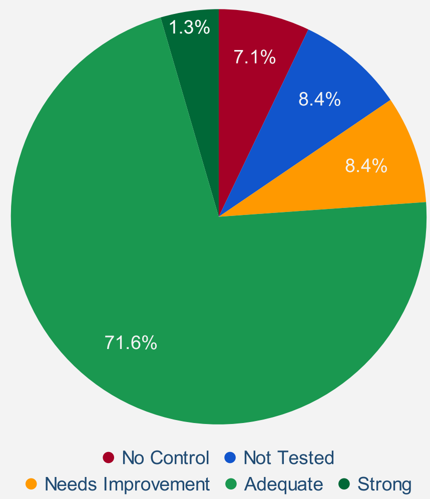
Channel Risk

Channel risk relates to the way in which customers access or buy products and services which could increase the ML/TF risk profile; for example, organisations that engage customers via non-face-to-face channels (e.g., digitally on-boarded) rather than face-to-face channels (e.g., via a branch), may pose significantly higher risks, such as identity theft and account takeover.

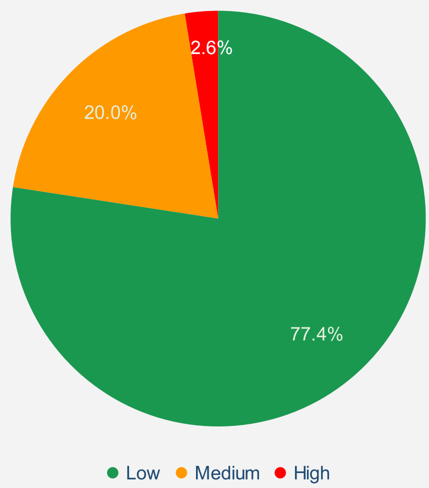
Channel IRR



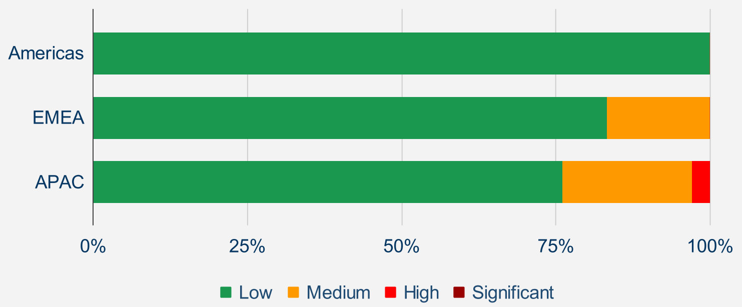
Channel OCE



Channel RRR



Less than 10% assess their overall Channel IRR to be high or significant. With almost 75% assessing their controls as adequate. As a result, 2.6% rated their overall residual channel risk rating as high, with 20% assessed as medium and 77.4% as low.

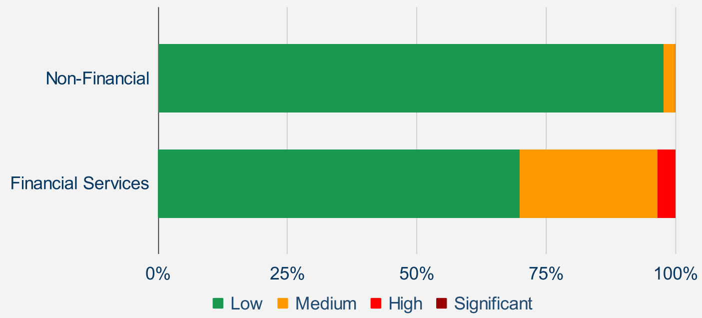


In APAC, 76% assessed their overall channel residual risk rating to be low, with 21% medium and 3% high.

In the Americas, 100% assessed their overall business residual risk rating to be low, whereas in EMEA 83.3% was low and 16.7% medium.

In Financial Services, 70% assessed their channel residual risk to be low, with 26% medium and 4% low.

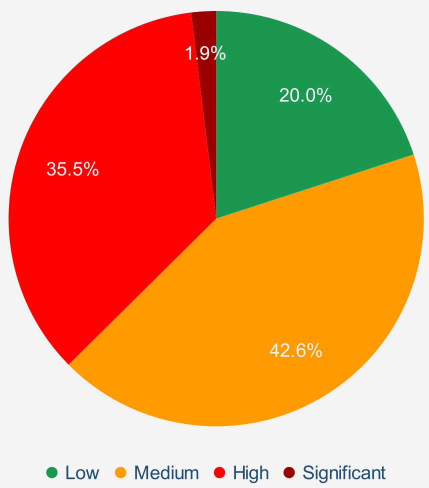
In Non-Financial services industries, none assessed their channel residual risk as high, with 98% as low and 2% medium.

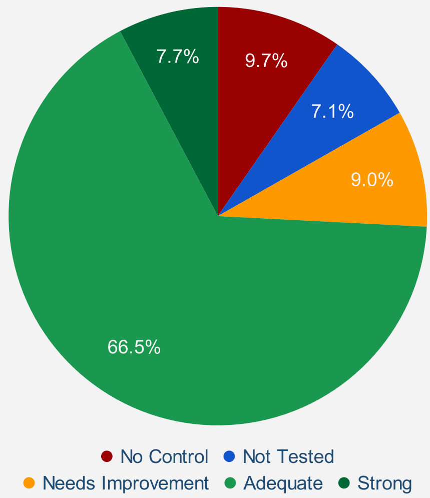


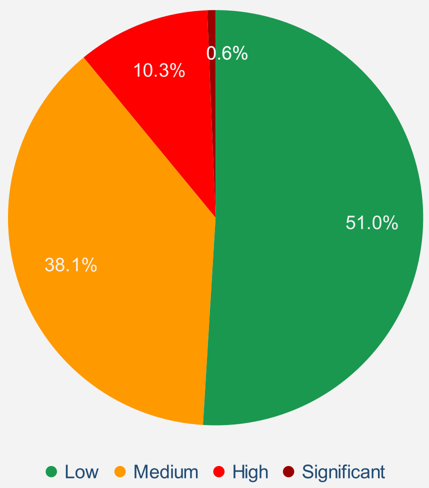
Product and Services Risk

Product and Services risk is the risk that particular product features and attributes may increase the risk of being more attractive to money launderers, such as the flexibility a product may have to deposit or withdraw funds in cash, or send or receive payments to or from unrelated parties.

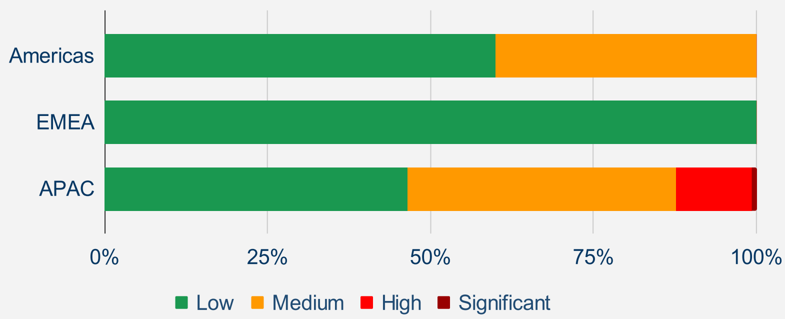
Product IRR	Product OCE	Product RRR





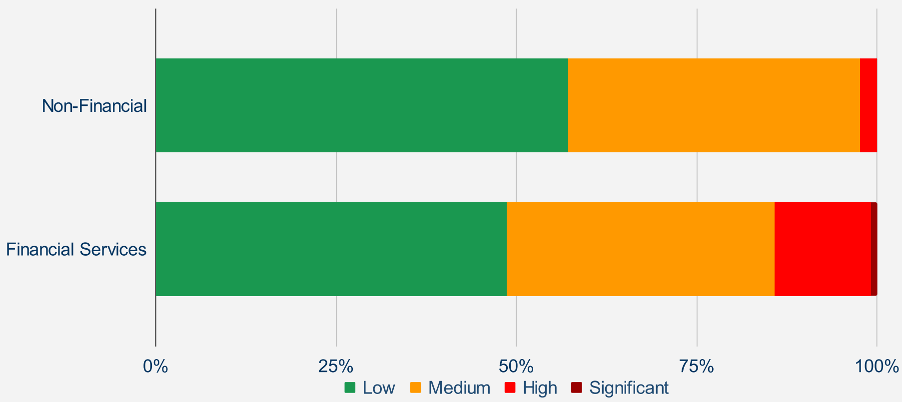


The majority of assessments had a product inherent risk rating of high or medium, as expected. Those risks were mitigated by the dominance of adequate controls, resulting in a product residual risk of low or medium for 89% of assessments.



In APAC, around 12% of products and services had a residual risk rating of High or Significant compared to Americas and EMEA where products and services were either rated Low or Medium.

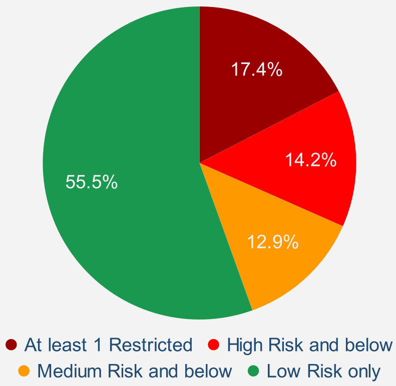
In Financial Services, nearly 15% assessed product residual risk to be high compared to just 2% in Non-Financial Services industries.



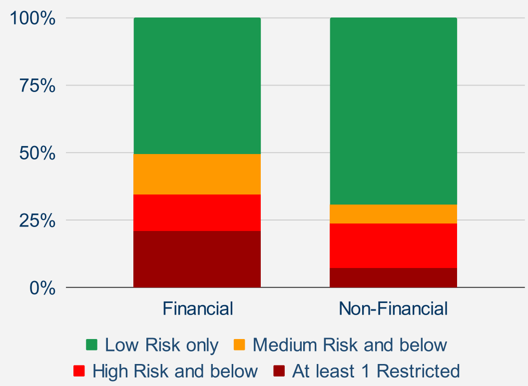
Country Risk

Country risk is the risk that organisations are exposed to through the location of their business operations, reliance on third-party intermediaries, and servicing customers in higher-risk countries, which may significantly increase the risk exposure that an organisation faces.

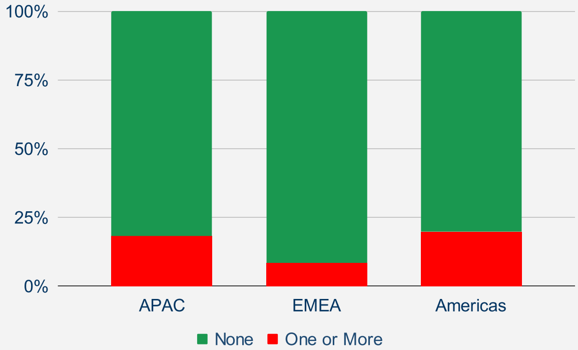
Country Risk Ratings in Programs



Country Risk Ratings by Industry

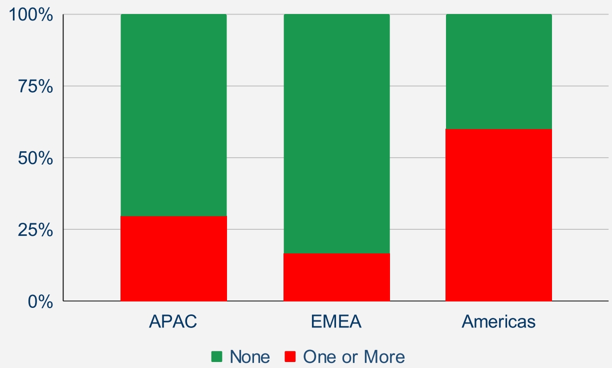


Nearly 20% of risk assessments indicate exposure to at least one restricted (sanctioned country), the majority of those in Financial Services. Only 50% of assessments in Financial Services are exposed to only low risk countries, compared to 70% of assessments in Non-Financial Services industries.



Nearly a quarter of APAC and Americas risk assessments reported having exposure to one or more restricted countries, compared to EMEA with 9%.

More than 25% in APAC and over 50% in the Americas reported dealing with one or more high risk countries compared to EMEA which is 20%. This shows that a significant portion of companies are willing to be exposed to high risk countries.

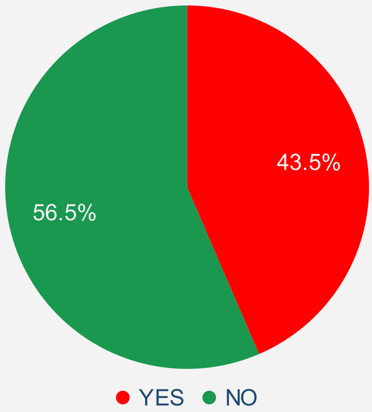


Other Insights

Other Insights from Assessments

We have pulled out some of the other interesting data and drawn insights and observations.

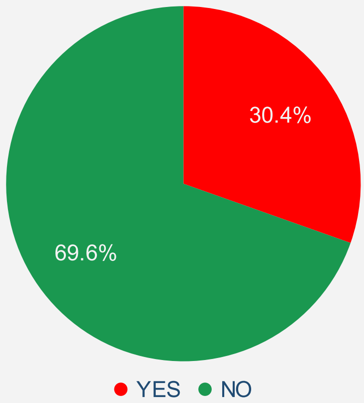
Do you outsource controls?



Less than 50% of companies outsourced their ML/ TF controls to third parties; the top 3 being:

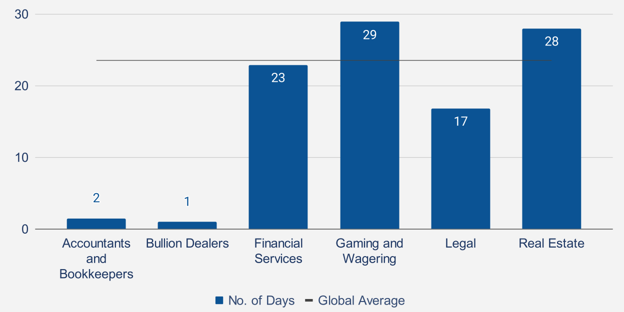
1. **22.7%** Customer Screening
2. **22%** Customer Due Diligence
3. **9.5%** Enhanced Customer Due Diligence

Do you use third party channels?



Over 30% reported they use third-party intermediaries (e.g., introducing brokers) when engaging with their customers, which introduces operational risks related to the reliance on third parties to onboard customers to the same standards.

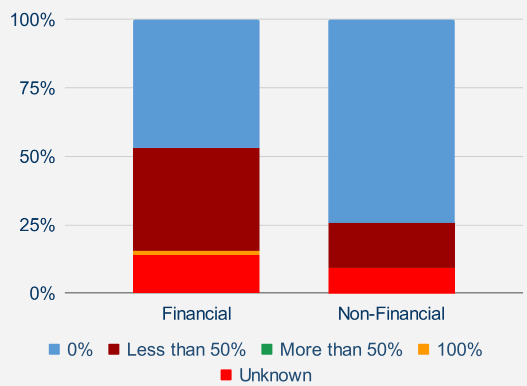
Time taken to complete the assessment



On average, across different industry sectors, the time taken to complete the ML/TF risk assessment was 23.5 days. This is substantially less time than public survey respondents who reported:

Time Taken	#	%
Up to 3 months	75	49.02%
Up to 6 months	20	13.07%
Up to 12 months	22	14.38%

Percentage customers that are high risk individuals



Almost half of financial services ML/TF risk assessments noted that none of their individual customers are high risk, compared to 75% of risk assessments from other industries.

Surprisingly, nearly 20% of financial service respondents did not know if they dealt with high risk individual customers.

What trends do we expect to see in the future?

We highlight emerging trends that are expected to become increasingly important for enterprise-wide risk assessments.

Rise in personal accountability regimes

Regulators have increased their expectations of Boards and Senior Executives in providing appropriate oversight of the enterprise-wide ML/TF risk assessments by introducing personal accountability regimes where Executives can be subject to civil and criminal penalties.

It is increasingly important that Executives play a meaningful role in ensuring enterprise-wide ML/TF risk assessments are conducted in a timely manner, are based on a sound and logical methodology and present the key findings, observations and recommendations to mitigate and manage ML/TF risks in line with the organisations risk appetite.

Executives must ensure appropriate oversight of action plans to address risk and compliance gaps to meet stakeholder expectations.

Rise of RegTech solutions for EWRA

There has been an emergence of RegTech solutions to address the challenges of enterprise-wide ML/TF risk assessments and currently only a small proportion of regulated entities have adopted technology platforms to conduct this cornerstone regulatory requirement.

As regulated businesses start to adopt purpose-built platforms and realise the numerous benefits, such as, audit trail, workflow and enterprise reporting - Boards and Regulators are increasingly going to be challenging their risk and compliance teams to progress beyond spreadsheets and maturing to platform-driven approaches.

Increase in regulatory expectations

Regulators haven also started to become active in providing clear feedback to regulated entities of the common failings that they see in relation to conducting enterprise-wide ML/TF risk assessments - feedback they expect to be taken onboard to increase the quality and frequency of enterprise-wide ML/TF risk assessments.

The common areas for improvement highlighted by regulators includes - failing to consider relevant risk factors; lack of clarity in the methodology, inconsistencies between customer risk assessments and EWRAs; errors and inaccuracy and lack of timeliness in reviewing and updating the EWRA.

In future, regulated entities will be expected to incorporate this feedback into their enterprise-wide ML/TF risk assessment.

Move towards real-time, data-driven

Organisations that have more mature approaches to enterprise-wide ML/TF risk assessments are increasingly looking to make these more objective and data driven, rather than subjective, or a hybrid of the two approaches.

Moving toward more frequent data-driven assessments reduces the time it takes to complete them, allowing more time to focus on analysing and managing the risks.

We anticipate that regulators will expect more frequent assessments using quantifiable data.

Closing Remarks

The 2022 AML Industry Benchmarking Report has been compiled from over one hundred and eighty ML/TF risk assessments conducted in 2021, taken from a cross-section of countries and industry sectors and supplemented by over 150 respondents from our public survey. Whilst we recognise this represents a tiny section of the overall number of regulated businesses required to complete ML/TF risk assessments, there are many interesting insights and observations that can be drawn upon and some of these may resonate with your business.

The report highlights how respondents are conducting inherent risk assessments of money laundering and terrorism financing risks, how they are assessing the existence and effectiveness of controls, what their overall residual risks are and ultimately, how well controls are designed, implemented and maintained to support the mitigation and management of these risk exposures.

Further, the report highlights that there are many challenges and obstacles that regulated businesses must overcome to manage this mandatory regulatory requirement. Some of the major challenges reported range from gathering data inputs and applying these in the ML/TF risk assessment; designing, building and maintaining a sound and robust ML/TF risk assessment methodology that is logical, defendable and explainable to the Board and Regulators and the amount of time taken to complete the ML/TF risk assessment (largely due to highly manual processes gathering, analysing, recording and reporting), meaning that the risk assessment may not even be relevant by the time it is presented to the Board for signoff.

As well as clear time-savings and efficiencies, our respondents show that regulated businesses are seeing the many other benefits of technology, such as audibility, configurability, self-sufficiency, repeatability, reliability, record-keeping, real-time reporting, and dashboard analysis. An increasing number of regulated businesses report they are looking to transition from manual spreadsheet-based approaches to digitised risk assessments with a view to increasing quality and efficiency, and generally raising the bar on what Boards and Regulators should expect to see.

Arctic Intelligence

Arctic Intelligence is a multi-award winning, RegTech firm that specialises in audit, risk and compliance software related to financial crime compliance and risk management.

Our Credentials

Arctic Intelligence continues to be recognised for our innovative approach to enterprise-wide financial crime risk assessments.

Our clients and what they say about us

Here are a few of our clients in the Financial Services sector.

APAC	EMEA	AMERICAS
BOQ	Bank of India	FirstOntario Credit Union
Suncorp	African Bank	1st Choice Savings and Credit Union Ltd
credit unionsa	Arbuthnot Latham	Vermilion Credit Union
BIBD	Paragon Group	abcu Credit Union
Beyond Bank Australia	Ford Credit	Vision Credit Union
Qudos Bank	Jupiter	bow valley credit union
Bell Potter	unionbank	Lakeland Credit Union
imb bank	Skipton Building Society	Prospera Credit Union
people's choice credit union	Hermes Investment Management	
me		
regional australia bank		
Newcastle Permanent		
Defence Bank		
QBANK		
Heritage Bank		
TAL		

Our Solutions

Arctic Intelligence has developed three leading cloud-based software solutions that leverage technology to re-engineer the way in which major financial institutions and other regulated businesses manage their financial crime risks.

AML Accelerate Platform

AML Accelerate is a cloud- based guided risk assessment solution for assessing money laundering and terrorism financing risks and developing AML/CTF Programs/Policies.

AML Accelerate has been tailored to over 30 different financial and non-financial services industries, as well as over 30 different countries.

This platform has been designed by experts to support regulated entities of all sizes, sectors and geographies in understanding ML/TF risk and demonstrating compliance.

Play Video Demo

Solution Overview

Download Brochure

Risk Assessment Platform

The Risk Assessment Platform is a cloud-based highly flexible and configurable enterprise-wide risk and control assessment solution.

The platform can be used by smaller reporting entities out-of- the-box with standard risk and control libraries for various financial crime risks or can be configured by larger organisations to suit any enterprise risk management framework and methodology.

The platform contains in-built workflows, audit trail and real- time enterprise analytics and insights

Play Video Demo

Solution Overview

Download Brochure

Health Check Platform

The Health Check Platform is a cloud-based platform designed to help regulated businesses (and their professional advisers) to assess the design and operational effectiveness of compliance programs, by mapping policies/ procedures to compliance obligations; performing control testing; documenting key observations / recommendations in reports and using data analytics to derive actionable business intelligence on compliance data.

There are two Health Check Platform modules - AML Health Check and Anti-Bribery Health Check.

Play Video Demo

Solution Overview

Download Brochure

Our Risk Assessment Platform contain various financial crime risk models and control libraries for a range of risk disciplines including; money laundering and terrorism financing, anti-bribery and corruption, sanctions, fraud, modern slavery, human trafficking, correspondent banking and wildlife trafficking.

Request Demo

Acknowledgements

There are countless people that we would like to thank and for whom not only this report but our whole business would not be possible so we would like to acknowledge each of your contributions.

Firstly, to the team at Arctic Intelligence (past and present), you are all brilliant individuals and have shown incredible tenacity, dedication and determination and I would like to genuinely thank you for being the best team a founder could hope for and coming on this roller-coaster of a journey.

Secondly, to our clients, who did their own risk assessment on Arctic and decided to take the plunge and work with us, help us grow as people, as a business and improve our solutions – we thank you for your commitment and support.

Thirdly, to our partners, new and emerging, who share our vision, passion and belief that there must be a better way to conduct financial crime risk assessments and who are embracing new ways of working – we thank you, and I am sure your clients will thank you too!

Finally, we would like to thank all the supporters behind the scenes who have shown amazing resilience and unwavering support to our whole team – each of us has many friends, families and supporters who help us all as individuals to continue to show up 110%, giving us the drive and determination to achieve our vision, we couldn't do this without you!

Thanks

Anthony Quinn
and the Arctic Intelligence Team

Special thanks to some of our partners who have agreed to help us share this report.

COMPLIANCE. THE SMART WAY.

info@arctic-intelligence.com

www.arctic-intelligence.com

Level 4, 11-17 York Street, Sydney, NSW 2000 Australia.

Australia	+61 (0) 2 8001 6433
Hong Kong	+852 (0) 8197 4022
New Zealand	+64 (0) 9889 3324
Singapore	+65 6817 8650
United Kingdom	+44 20 8157 0122
United States	+1 646 475 3718
Canada	+1 613 5188002