



AML Compliance and Financial Crime Risk Assessment Technology

Hosted by: CAMLI and Arctic Intelligence

15 August 2024



Introduction to Financial Crime Risk Assessments

What do the FATF recommendations say in relation to Money Laundering and Terrorism Financing Risks?



Guidance for FATF member countries: (page 10)

- ❖ countries should take appropriate steps to identify and assess the ML/TF risks for the country, on an ongoing basis (i.e., [National Risk Assessments](#))
- ❖ once these risks are properly understood, countries will be able to [implement AML/CTF measures](#) that mitigate these risks
- ❖ the [risk-based approach](#), is central to the effective implementation of the FATF Standards and applies to financial institutions and designated non-financial businesses and professions (i.e., gaming, lawyers, accountants, real-estate & high-value goods dealers).

Guidance for regulated entities: (pages 34-35)

- ❖ FI's and DNFBPs should be required to take appropriate steps to [identify and assess](#) their money laundering and terrorist financing risks (*for customers, countries or geographic areas; and products, services, transactions or delivery channels*)
- ❖ They should [document](#) those assessments in order to be able to [demonstrate](#) their basis, [keep](#) these assessments [up to date](#) and [provide to regulators](#).

Source: FATF Recommendations '23 - <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html>

What are the sectors that are required to implement and maintain an Enterprise-Wide ML/TF Risk Assessment?

Regulated entities in over 200 FATF-member countries and over 30 industry sectors and sub-sectors* are required to maintain an EWRA[^]

Financial Institutions

- ❖ Asset Managers, Hedge Funds & Fund Managers
- ❖ Banks, Building Societies, Credit Unions & Mutuals
- ❖ Cash in Transit and Safety Deposit Box Providers
- ❖ Corporate Finance and Private Equity
- ❖ Cryptocurrency & Digital Currency Exchanges
- ❖ FinTech's
- ❖ Foreign Exchange & MSBs (Money Remitters)
- ❖ Financial Planners
- ❖ Insurance Companies
- ❖ Investment Managers
- ❖ Leasing & Hire Purchase Financing Businesses
- ❖ Non-Bank Financial Institutions
- ❖ Payment Processing Services
- ❖ Stockbrokers
- ❖ Superannuation, Retirement & Pensions

DNFSBP's (Other Sectors)

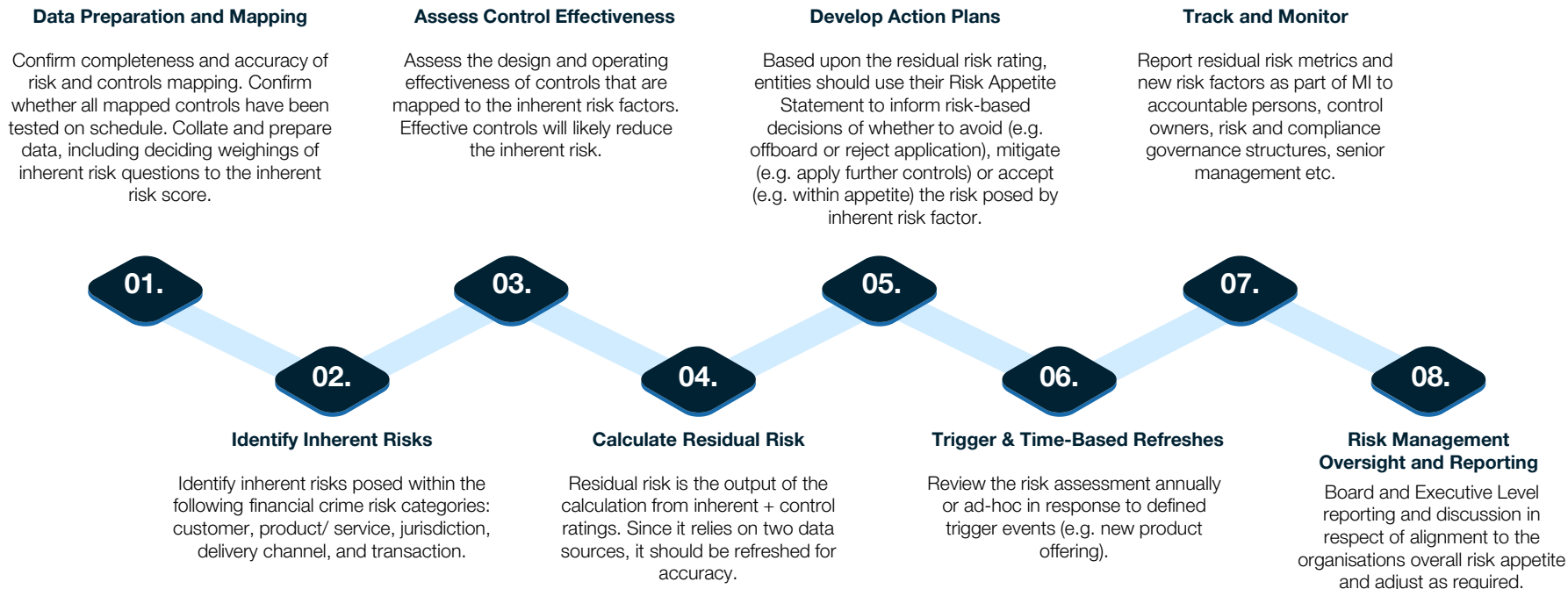
- ❖ Bookmakers & Betting Agencies
- ❖ Casinos
- ❖ Physical Gaming Venues
- ❖ Online Gambling
- ❖ Accountants & Bookkeepers
- ❖ Lawyers & Conveyancers
- ❖ Trust & Company Service Providers (TCSPs)
- ❖ Real Estate Professionals
- ❖ Antique & Fine Art Dealers
- ❖ Auctioneers & Brokers
- ❖ Bullion & Precious Stone Dealers & Jewellers
- ❖ Motorised Vehicle Dealers (Cars, Boats, Planes)
- ❖ Luxury Goods Dealers
- ❖ Pawnbrokers & Secondhand Dealers
- ❖ Other Sectors (i.e., Marijuana businesses, NGO's)

* The list of regulated businesses varies between countries depending on the maturity of the AML/CTF laws and oversight.

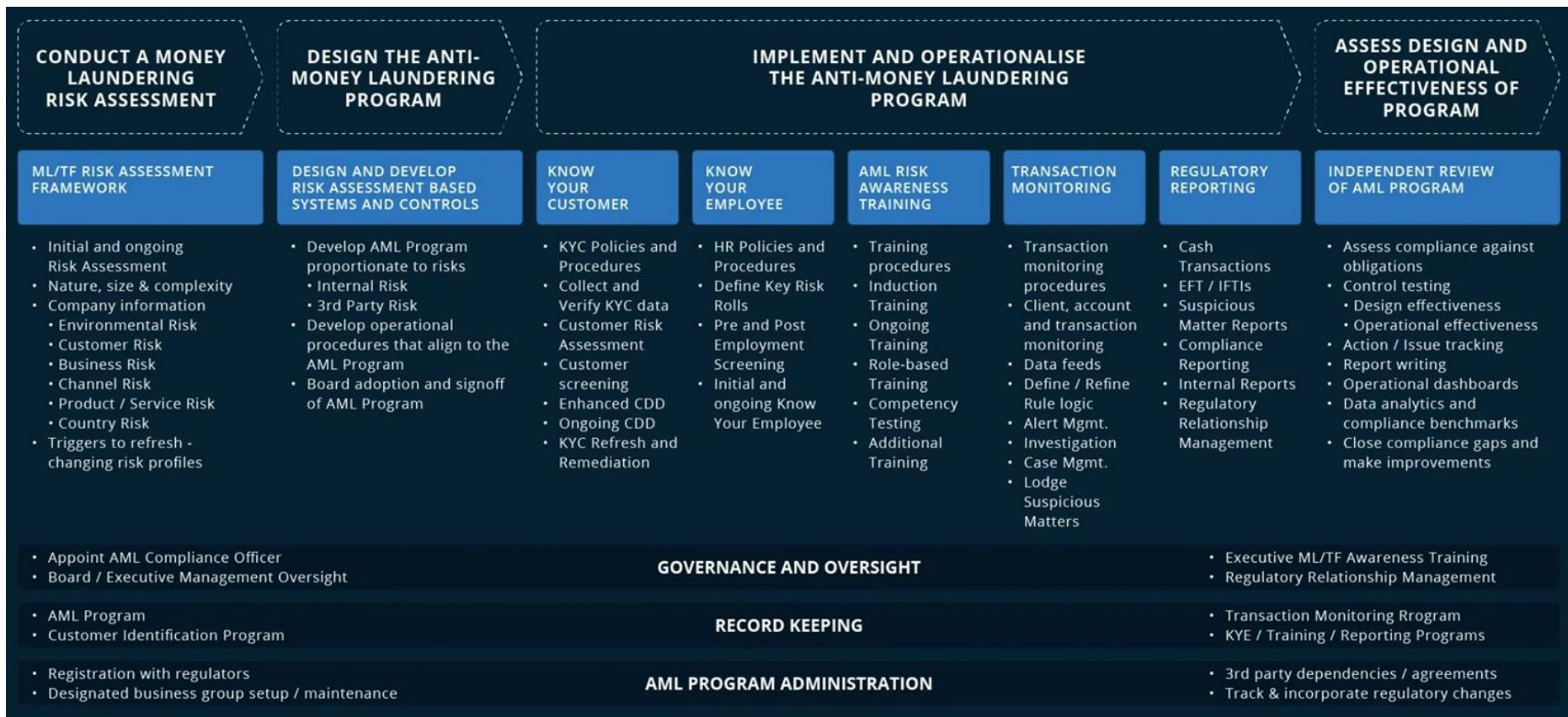
Note: Enterprise-Wide Risk Assessment (EWRA) is also often called Business Risk Assessment (BRA) in certain countries.

ML/TF RISK ASSESSMENT HIGH-LEVEL PROCESS

An ML/TF risk assessment is an ongoing process and must be continuously reviewed



ML/TF RISK ASSESSMENTS IN THE COMPLIANCE VALUE CHAIN



WHAT ARE GOOD VS. BAD PRACTICES?

Good Practice



- » Risk assessment is a continuous process revisited frequently throughout the year
- » The firm understands the impact of financial crime on its customers
- » The firm review and updates its financial crime risk assessment where it creates new products or services
- » The firm is completing data-driven risk assessments reducing manual efforts in data gathering
- » Board are presented with the risk assessment results ensuring they are aware of strengths/ weaknesses of the financial crime framework
- » The weaknesses identified are mapped to actionable activities to reduce the risk or enhance the control environment
- » The firm bolsters insufficient in-house knowledge or resource with external expertise, for example in relation to assessing financial crime risk or monitoring compliance with standards.

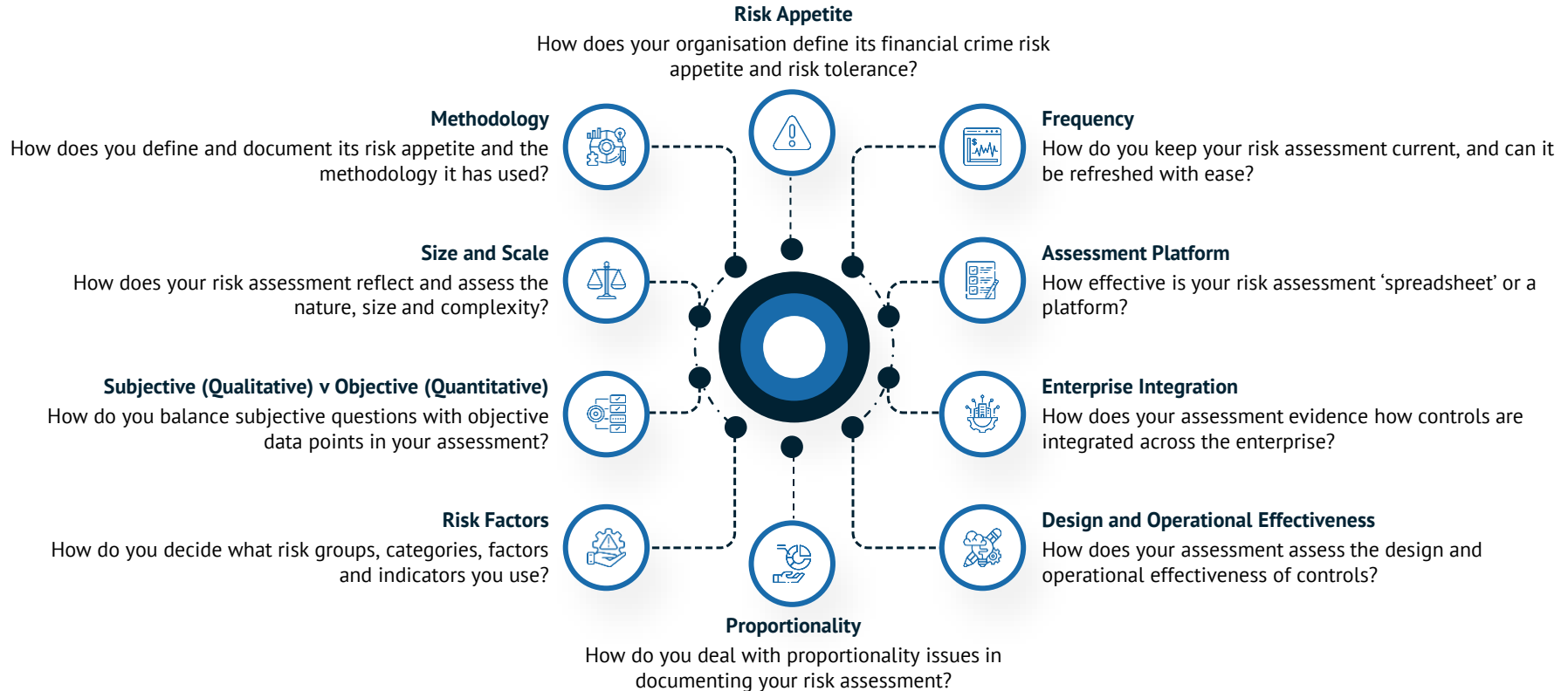
Poor Practice



- » Risk assessment is a one-off process every one or two years only to produce a report for regulatory reasons
- » The firm does not consider the impacts of financial crime on their customers
- » Lack of efforts to understand risk the firm faces and the effectiveness of the controls
- » Lack of data used to support the outcome of the inherent risk and control effectiveness
- » No consideration of external sources of information supporting the risk assessment process e.g. NRA
- » The firm makes no attempts to address the financial crime risks identified through the risk assessment process
- » Teams are under resourced leading to missing data, delays in completion and a report which does not reflect the risks.
- » Control owners are not identified or consulted with to incorporate any testing that may have been completed to assess the effectiveness on the control
- » Lack of transparency with regulators, where self identified issues are not shared, where reasonably expected to do so

RISK ASSESSMENT SUCCESS FACTORS

There are no right or wrong answers or approaches – the key is to adopt an approach that is logical, explainable, defensible and repeatable – but there are numerous things to consider and ten key questions to ask yourself





Key challenges and how to overcome them

Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 1

Defining your ML/TF risk appetite and risk tolerance

Risk Appetite

The amount of risk your organisation is willing to accept to achieve its objectives.

(In other words, the maximum amount of residual risk an organisation will accept after mitigating controls have been applied)

Vs.

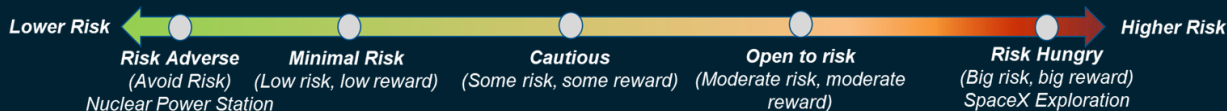
Risk Tolerance

The acceptable deviation from your organisation's risk appetite.

Zero tolerance vs. some tolerance?

Have to take some risk as cannot mitigate every single risk!

Risk adverse vs. Risk taking?





Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 2

Deciding what ML/TF risk assessment methodology to use

Key considerations include:

- ❖ Question driven (subjective) vs. data driven (objective) or a hybrid approach
- ❖ Replicating existing ML/TF risk assessment models or building from scratch
- ❖ How to assess Inherent Risks (i.e., likelihood x impact)
- ❖ How to assess Control Effectiveness (i.e., control design and performance)
- ❖ How to assess Residual Risk (i.e., logic of reducing risks)
- ❖ How to document the methodology and rationale behind the risk approach.

Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 3

Assessing the nature, size and complexity of the organisation

Risk assessments (and controls) must be **appropriate** and **proportionate** given the nature, size and complexity of the organisation – but what does this mean?

Nature of the business

- What does the business do?
- How does it make money
- What products and services are offered?
- What types of customer does it serve?
- What customer segments does it serve?
- How are customers acquired?
- What countries does it operate in?

Size of the business

- What is the size of the customer base?
- How much revenue is earned annually?
- How many staff does the business employ?
- How many customers are served?
- How many offices/branches are there?

Complexity of the business

- How many products/services are offered?
- What is the nature of products/services?
- How many and what channels are used?
- How many countries does it operate in?
- How regulated is the business?
- What is the ownership structure?
- What is the governance structure?



Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 4

Adopting a subjective (question driven), objective (data driven) or hybrid approach to assessing risk

Risk assessments that are **subjective**, rely on individuals making judgements on risks and controls, which may have bias and **objective** (data driven) approaches may miss data and subtle qualitative elements – what is best?

Subjective Approach

*Is **question-driven** and relies upon an individual's judgment of:*

- The likelihood of a risk occurring?
- The impact of a risk occurring?
- What the inherent risk of this is?
- How effective controls are at reducing risk?
- What the residual risk is?

Objective Approach

*Is **data-driven** and rely upon the organisation's data mastery:*

- What data inputs do I need?
- Is data all in one place or distributed?
- Is data standardised, clean & accurate?
- How will I extract/load/transform data?
- How will I apply risk decisioning to data?

Hybrid Approach

*Is **both** question-driven (qualitative) & data-driven (quantitative)*

- Qualitative inputs to risk combined with quantitative data inputs can often lead to a more robust outcome



Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 5

Deciding what risk groups, risk categories, risk factors and risk indicators to use

You will need to decide on the risk hierarchy and the content of your risk model...

Environmental Risks

Assess the organisations vulnerability to:

- **Predicate Offences** – deceptive crimes, illicit trafficking, personal crimes, property crimes
- **Money Laundering** – higher risks associated with – business operations, channels, customer transactions, customers, products and services
- **Terrorism Financing** – higher customer risk and customer transaction risks
- **Financial Sanctions** – higher customer risk and customer transaction risks
- **Regulatory Compliance Risks** – governance and oversight, program alignment to risks, program non-compliance and reporting

Customer Risks

Assess the organisations vulnerability to:

- **Customer Types** – segmentation of customer base - individuals, private companies, public companies, offshore companies, trusts, partnerships including extent UBO's known.
- **Customer PEP Status** – number of customers that are foreign or domestic PEPs and categories of PEPs
- **Customer Location Risk** – *segmentation of customers by location/geography*
- **Customer Business Risk** – *segmentation of customers by industry sector/occupation*
- **Customer Source of Wealth** – segmentation of customers where this information is known, unknown or vague

Business Risks

Assess the organisations vulnerability to:

- **Business Location** – extent of business operations that are carried out overseas (and which countries and which operations)
- **Outsourcing Risk** – extent to which third parties are used to perform AML controls on your organisations behalf, the nature of outsourced controls, the extent of controls over the outsourced controls!
- **Employee Risks** – number of employees, proportion that are customer facing, proportion in key risk roles, proportion that have been background screened and extent of background screening, proportion having adverse screening results, functions performed etc.



Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 5

Deciding what risk groups, risk categories, risk factors and risk indicators to use (cont.)

How you build your ML/TF risk model framework is a critical component

Channel Risks

Assess the organisations vulnerability to:

- **Non-Face-to-Face Channels** – the extent to which customers are met face to face during on-boarding or when servicing their accounts
- **Methods of interacting with customers** – what methods are used, somewhat anonymous (e.g., internet, social media, SMS) or less anonymous (e.g., branch, post office, video conferencing, telephone etc.)
- **Use of third parties** – the extent to which third parties are used as channels (e.g., introducing brokers, sales agents, intermediaries) and the locations of any of these channels

Product & Services Risks

Assess the organisations vulnerability to:

- **Products and Services** – extent to which different products and services are offered (250+ Financial Services Products)
- **Attributes of products and services that make them more attractive to money launderers** – for example, transfer of funds into and out of accounts through multiple methods, by unrelated third-parties, using remote access methods, from/to foreign jurisdictions, value / transaction limits, allow overpayment or early repayment, acceptance of cash or cash equivalents, cooling off periods etc.
- **Extensiveness of use** – what proportion of customers use the product or service, what proportion of revenues are attributable, whether any transaction monitoring controls or suspicious matters related to different types of products etc.

Country Risks

Assess the organisations vulnerability to:

- **Methodology** – there is no universal standard for country risk and is geo-political, but there are numerous recognised sources such as Targeted Financial Sanctions (UN), FATF AML Concerns, High Risk and Other Monitored Jurisdictions, Terrorism Vulnerability (US Department), Illicit Drug Vulnerability (US International Narcotics Strategy Control Report), Corruption Vulnerability (Transparency International Corruption Perceptions Index), Financial Secrecy (Index), Kimberly Process (Conflict Diamonds etc.) and FATF Members/Observer Lists (and extent of compliance)
- **Frequency** – each of these are published at different times of the year and using different rating scales, so agreeing a process and frequency of updates (and reflection through the ML/TF risk assessment can be a challenge!)



Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 6

Deciding whether to introduce proportionality/weighting (or not) to the ML/TF risk assessment

Does the risk methodology **treat all risks equally** or is there a need to **proportionally weight risks** (and/or controls) in the risk model and/or across different assessment units across the enterprise?

Assessment Unit Weightings

Adjust weightings between assessment units? - for example:

- Business Unit 1 (Wholesale Banking), is riskier than Business Unit 2 (Retail Banking), but less risky than Business Unit 3 (Private Banking) – so can adjust the weightings between assessment units etc.

Risk Model Weightings

Adjust weightings between different levels in the risk model framework? for example:

- Risk Group
- Risk Categories
- Risk Factors
- Risk Indicators
- Risk Indicator Answers

Control Weightings

Adjust weightings between different levels in the control framework, for example:

- Control Categories are equal to each other or weighted differently to each other
- Controls may be key controls and have a stronger effect on mitigating (or not mitigating) risk



Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 7

Deciding how to assess the design and operational effectiveness of controls

Control Design

Control design refers to the process of assessing whether a control is “fit for purpose” and addresses the risk

Control Performance

Control performance refers to the process of assessing whether the control is operating effectively

Control Effectiveness

Control effectiveness refers to the process of assessing just **how** effectively a control is operating

The screenshot shows the Arctic Intelligence Controls Assessment interface. The top navigation bar includes 'ARCTIC INTELLIGENCE', 'HOME', 'APP SETUP', and 'ARCTIC-DEMO-ACCOUNT'. The main header shows 'Context', 'Workflow', 'Risk Analysis', 'Controls Assessment', and 'Report'. The current view is 'Controls Assessment' for 'E-Commerce Risk Assessment - Business Division 2'. The interface includes a 'Controls Summary' and 'Controls Questionnaire' tab. The 'Controls Questionnaire' tab shows a table of controls with columns for Type, Key, Weight, Design?, Performance?, Effectiveness?, and Actions. The table lists one control: 'AML Refresher Training' with a weight of 20.00% and a status of 'Good'. The interface also includes a 'Comments' section and a 'Control Test Results' section. The bottom of the interface has a 'Complete' button and 'BACK', 'SUBMIT', and 'NEXT' buttons.

Type	Key	Weight	Design?	Performance?	Effectiveness?	Actions
AML Refresher Training	Preventative	20.00%	Good	Fair	Needs Improvement	



Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 8

Assessing how all ML/TF risks link together across the enterprise

Many larger organisations have multiple assessment units, multiple risk domains, with **hundreds of risk indicators**, rolling up to risk factors, risk categories and risk groups – which can make reporting very complicated..!



Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 9

Deciding what “system” to use – is your business still using spreadsheets to conduct ML/TF risk assessments?

Spreadsheets are still (too) widely used – but they have many [limitations](#) compared to system-based approaches – here are just a few...

Spreadsheet based approaches

- ✓ **Cost effective** – spreadsheets are free (*but you'll pay in other ways!*)
- ✗ **No/Limited Audit Trail** – No field level validation or date/time stamping
- ✗ **Spreadsheets break and are error prone** – no testing to validate logic
- ✗ **No live saving** – if your file is corrupted you will lose work
- ✗ **No version controls** – how do you ensure the assessment is the latest?
- ✗ **No user access controls** – very limited password protection only
- ✗ **No uploading documents** – cannot upload evidence (e.g. control tests)
- ✗ **Excel has only basic graphics** – need to plug-in to reporting tools
- ✗ **Less efficient** – sending/receiving across the organisation is slow
- ✗ **No report writing** – results need to be written up separately
- ✗ **No guidance notes** – no tooltips, help centres or other support
- ✗ **Hard to maintain** – no “push through” of changes or audit trail of these

System based approaches

- ✗ **Some cost involved** – but very modest compared to the benefits
- ✓ **Full audit trail** – field level comments, track reviewers/approvers real-time
- ✓ **Full testing** – systems are subject to rigorous UAT, Regression & PVT
- ✓ **Cloud-based** – 99.98% uptime and fully-backed up forever
- ✓ **Full version control** – ensures full change control on content/versions
- ✓ **Full user access controls** – set permissions to system access/functions
- ✓ **Full upload** – upload risks, controls & control testing evidence/findings
- ✓ **In-built analytics** – real-time analytics across multiple assessment units
- ✓ **Highly efficient** – hundreds of users can interact on the platform real-time
- ✓ **Full report writing** – auto generated reports and add commentary easily
- ✓ **Fully supported** – tooltips, help centre, video tutorials, in-app support
- ✓ **Easy to maintain** – update/push through content and functional changes





Top 10 Enterprise-Wide ML/TF Risk Assessment Challenges and key considerations to think about

Challenge 10

Deciding when and how to maintain the ML/TF risk assessment and keep it current

Things are changing all the time – how do you keep things current?

- ❖ **Regulatory compliance alerts** – rules, regs, guides and typologies
- ❖ **Regulatory focus areas** – industry / behaviour focussed
- ❖ **Country risks** – 240+ countries/territories and multiple sources
- ❖ **Business risks** - customer, product, channel, geography mix, reliance/relationships with third parties, employee risks etc.





About Arctic Intelligence



We are a global RegTech firm specialising in audit, risk and compliance software related to financial crime compliance and risk management.

Why Arctic?

Arctic is an acronym and stands for Audit, Risk and Compliance, Technology, Innovation Company.

Our Platforms



Enterprise-wide money laundering and terrorism financing risk assessment and AML policy platform designed for small and medium sized businesses, tailored to over 30 industry sectors and 60 countries.

14-day free trial available – click [here](#)

RISK ASSESSMENT

Fully configurable financial crime risk assessment platform designed for larger enterprises that want to tailor their own risk and control models, digitize their approach and conduct data driven risk assessments across their organisation.



Arctic Intelligence was founded in 2015 and has helped hundreds of companies in over 20 industry sectors and 20 countries improve their financial crime risk assessments.

Financial Crime Domains

- » AML/CTF and Sanctions
- » Proliferation Financing
- » Bribery and Corruption
- » Fraud
- » Human Trafficking / Modern Slavery
- » Anti-Facilitation of Tax Evasion
- » Correspondent Banking

Other Risk Domains

- » Enterprise Risk Management
- » ESG

Awards & Accomplishments

RegTech Analyst

Top 100 RegTech firms 2021 & 2022

CRC Outlook

Top 10 Risk Management Providers 2022

A-Team Innovation

Most Innovative Data privacy by design 2021

RegTech/Fintech Awards

Rising Star – RiskTech 100, 2022
Finalist – Excellence in RegTech 2021 (Finnies)
Winner – RegTech Startup of the Year 2019
Winner – RegTech of the Year 2020 (RTA)
Winner – RegTech Exporter of the Year 2020
Award for Excellence - Regulation Asia 2021

NTA Awards

Shortlisted – National Technology Awards 2021

Planet Compliance

RegTech Top 100 (#8)

Deloitte Technology Fast 50

Top 50 firms 2019

ACCREDITATIONS

ISO 27001 INFO SEC



SECURELY HOSTED BY



SOME OF THE COMPANIES WE'VE HELPED



AMERICAS



EMEA









































APAC



COUNTRIES WE SERVE

Our AML Accelerate Platform has localised AML/CTF content aligned to laws in 60+ countries (so far)

 Australia	 Canada	 Ireland	 South Africa	 Barbados	 European Union
 New Zealand	 United Kingdom	 Brunei	 Hong Kong	 Singapore	 United States
 Germany	 France	 Italy	 UAE	 Qatar	 Denmark
 Norway	 Finland	 Sweden	 Indonesia	 Malaysia	 Philippines
 Cambodia	 Thailand	 Vietnam	 India	 Sri Lanka	 Bahamas
 Cyprus	 BVI	 Jamaica	 Trinidad	 Gibraltar	 Guernsey
 Jersey	 Malta				

We're partnering with local AML experts deliver content for even more countries – watch this space!

EMEA	APAC	AMERICAS
<ul style="list-style-type: none"> » Kenya » Mauritius » Namibia » Tanzania » Israel » Greece » Uganda » Jordan » Kuwait » Oman » Saudi Arabia » Seychelles 	<ul style="list-style-type: none"> » No more planned 	<ul style="list-style-type: none"> » Cayman Islands » Mexico » Argentina » Colombia » Brazil





INDUSTRIES WE SUPPORT

Regulated businesses in over 200 FATF-member countries and over 30 industry sectors and sub-sectors* are required to maintain an EWRA[^]

Financial Institutions

- » Asset Managers, Hedge Funds & Fund Managers
- » Banks, Building Societies, Credit Unions & Mutuals
- » Cash in Transit and Safety Deposit Box Providers
- » Corporate Finance and Private Equity
- » Cryptocurrency & Digital Currency Exchanges
- » FinTech's
- » Foreign Exchange & MSBs (Money Remitters)
- » Financial Planners
- » Insurance Companies
- » Investment Managers
- » Leasing & Hire Purchase Financing Businesses
- » Non-Bank Financial Institutions
- » Payment Processing Services
- » Stockbrokers
- » Superannuation, Retirement & Pensions

DNFSBP's (Other Sectors)

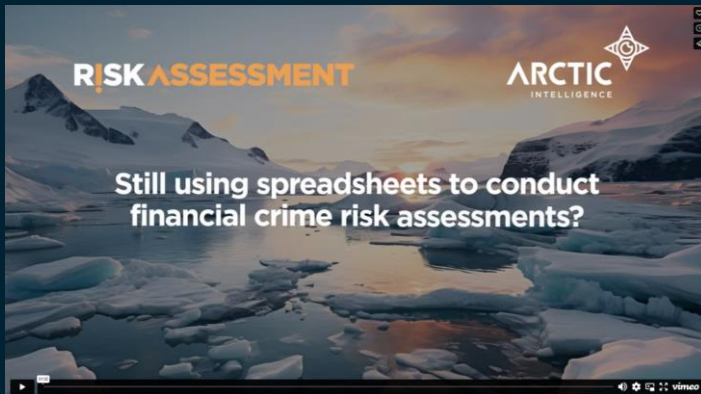
- » Bookmakers & Betting Agencies
- » Casinos
- » Physical Gaming Venues
- » Online Gambling
- » Accountants & Bookkeepers
- » Lawyers & Conveyancers
- » Trust & Company Service Providers (TCSPs)
- » Real Estate Professionals
- » Antique & Fine Art Dealers
- » Auctioneers & Brokers
- » Bullion & Precious Stone Dealers & Jewellers
- » Motorised Vehicle Dealers (Cars, Boats, Planes)
- » Luxury Goods Dealers
- » Pawnbrokers & Secondhand Dealers
- » Other Sectors (i.e., Marijuana businesses, NGO's)

* The regulated businesses vary between countries depending on the maturity of the AML/CTF laws and oversight.

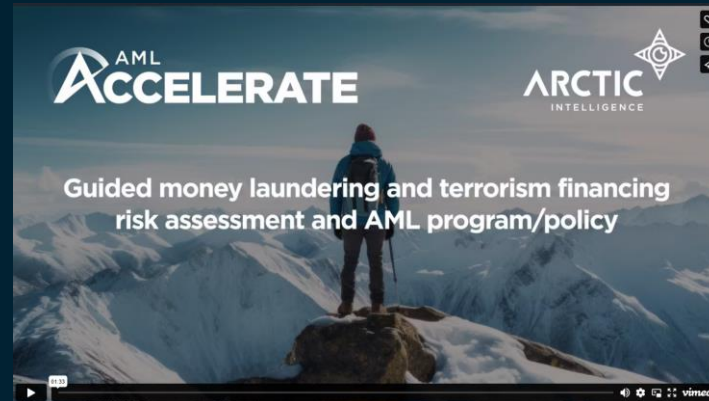
[^] Enterprise-Wide Risk Assessment (EWRA) is referred to differently in different countries, for example, Business Risk Assessment (BRA) in the UK, Financial Crime Risk Assessment (FCRA) in the Middle East/Africa and BSA/AML and OFAC Risk Assessment in the United States.

Learn more > arctic-intelligence.com/impacted-sectors

LEARN MORE ABOUT OUR MULTI-AWARD-WINNING PLATFORMS



<https://vimeo.com/866630006>



<https://vimeo.com/876792055>



<https://vimeo.com/866629090>

Download our value propositions

Risk Assessment Platform

Risk Assessment Platform for Supervisors

AML Accelerate Platform

Partner with Arctic



info@arctic-intelligence.com



Level 4, 11 York Street, Sydney,
NSW 2000 Australia



www.arctic-intelligence.com



Australia - +61 (0) 2 8001 6433
Hong Kong - +852 (0) 8197 4022
New Zealand - +64 (0) 9889 3324
USA - +1 646 475 3718
UK - +44 (0)208 157 0122
Singapore - +65 6817 8650
Canada - +1 613 518 8002



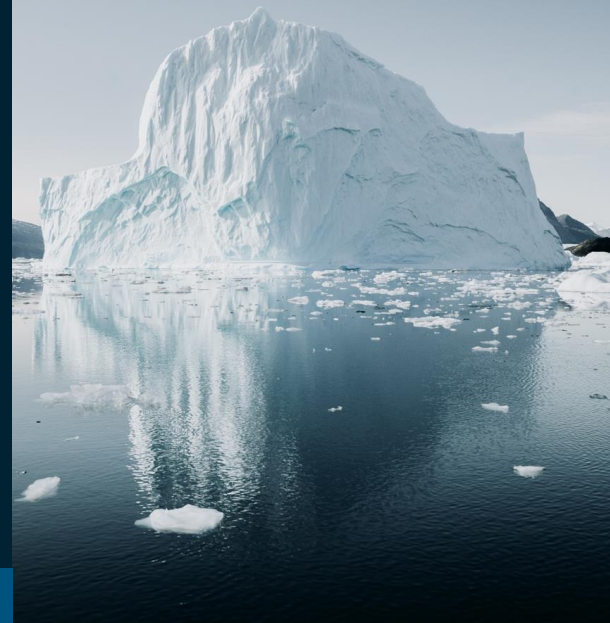
[Arctic Intelligence](#)



Anthony Quinn
Founder/CEO

Anthony.Quinn@arctic-intelligence.com
+61(0)431 157006

 Request a demo



DISCLAIMER

Copyright © 2024 Financial Crimes Consulting Pty Ltd (Trading as Arctic Intelligence) | ACN: 149 878 875. All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except as permitted by copyright law.

The information in this presentation and website is for general informational purposes only. Arctic Intelligence makes no representation or warranty, express or implied. Your use of the presentation and website is solely at your own risk. This presentation may contain links to third party content, which we do not warrant, endorse, or assume liability for. Arctic Intelligence makes no representation and assumes no responsibility for the accuracy of information contained on, or available through, this presentation and website, or its suitability for any purpose, and such information is subject to change without notice. You are encouraged to confirm any information obtained from or through this presentation and website with other sources and review all information independently. Arctic Intelligence does not recommend or endorse any specific products, processes, opinions, or other information that may be mentioned in this presentation and website.