

Anthony Quinn,  
Arctic Intelligence,  
36a Hickson Road,  
Sydney, NSW 2000.

28<sup>th</sup> January 2025

AUSTRAC - [economiccrime@ag.gov.au](mailto:economiccrime@ag.gov.au)

## **Reforming Australia's anti-money laundering and counter-terrorism financing regime**

Dear Sir/Madam,

On behalf of Arctic Intelligence, I would like to thank AUSTRAC for the opportunity to contribute to the first round of public consultation on the Exposure Draft AML/CTF Rules. This submission builds upon previous [submissions](#) made to the Attorney General's Department (AGD) but will focus on a narrower subset of the AML/CTF Rules in particular:

### **Part 4 – AML/CTF Programs**

- Division 1 – ML/TF risk assessment
- Division 2 – AML/CTF policies (*where relevant to ML/TF risk assessments*)
- Division 3 – AML/CTF compliance officers (*where relevant to ML/TF risk assessments*)
- Division 4 – AML/CTF program documentation (*where relevant to ML/TF risk assessments*)

We note AUSTRAC's comments that the AML/CTF Amendment Act is "*largely self-contained in relation to ML/TF risk assessments*" and "*AUSTRAC does not envisage making significant rules prescribing further detail*" other than adding an additional trigger for a review of the ML/TF risk assessment "*as soon as practicable*" after the governing body of the reporting entity receives the independent evaluation report containing adverse findings and apply updates to the ML/TF risk assessment which we **agree** with.

However, we **disagree** that the AML/CTF Amendment Bill alone provides enough clarity and coverage and we feel strongly that reporting entity's, would benefit from clearer and more explicit guidance from AUSTRAC in the form of AML/CTF Rules (as well as guidance) in relation to ML/TF risk assessments, which we have proposed some suggested items for AUSTRAC to consider, hopefully re-considering your position that the Bill itself contains sufficient clarity.

If you would like further clarification or information on anything contained in my submission, please do not hesitate to contact me and I welcome the opportunity to participate in any round table discussions that may be held and subsequent stages of this consultation process.

Yours sincerely,



Anthony Quinn  
Founder/CEO - Arctic Intelligence

[Anthony.Quinn@arctic-intelligence.com](mailto:Anthony.Quinn@arctic-intelligence.com)

**Submitted:** 28-Jan-2025 (via website upload)

## Part 4 – Division 1 – ML/TF risk assessments

### 1. General Comments

#### 1.1 Explicit requirement to conduct an ML/TF/PF risk assessment

We **agree** with the approach taken in the AML/CTF Amendment Bill 2024 to establish an express, rather than implied requirement that reporting entity’s must conduct an Enterprise-Wide ML/TF Risk Assessment (EWRA).

We also **agree** that ML/TF risk assessment should also explicitly include proliferation financing to bring Australian reporting entity’s into line with FATF recommendations.

For the record, we **disagree** with AGD’s decision to exclude High-Value Dealers from the scope of designated services for reasons outlined in prior [submissions](#), which was surprising given their predecessor DFAT wrote several [papers](#) on this highlighting the extent of the money laundering risks these sectors pose to Australia.

Unfortunately, this was overlooked, presumably due to decades of apathy by the Australian Government in regulating Tranche 2 sectors and suddenly realising they needed to act before the next FATF mutual evaluation and potentially these sectors became sidelined because Australia has started to reform its rules after decades of failing to act and is now running out of time. However, by excluding high-value dealer sectors like the art and antiquities market, auction houses and brokers, motorised vehicle dealers and luxury goods dealers, Australia will remain out of step with FATF standards, and despite raising this clear oversight in our two submissions to the AGD they remained entirely silent on this, then failed to include these sectors, which in our opinion is a mistake.

### 2. Explicit rules on ML/TF/PF Risk Assessments

Whilst AUSTRAC has stated that the guidance on ML/TF Risk Assessments is self-contained in the Act and “*does not intend to issue significant Rules prescribing further detail*” we **disagree** with this position and feel that reporting entity’s would benefit if AUSTRAC’s expectations were explicitly described, and we believe this would improve the overall quality of financial crime risk management across Australian reporting entity’s.

This is important given the historical context of AML/CTF compliance in Australia where we’ve seen continuous, systemic and epic compliance failures in both the Banking and Gaming sectors over the last decade (triggering Royal Commissions, Parliamentary and State Level Public Inquiries), which highlighted a clear lack of capability by many reporting entity’s in managing financial crime risks effectively, in our opinion because of a lack of care, capacity and/or capability in financial crime risk management, which these reforms have the opportunity to address.

#### 2.1 Establishing the nature, size, and complexity of the organisation in EWRA

We **agree** that the ML/TF/PF risk assessment should expressly include information pertaining to the nature, size, and complexity of its business.

We feel AUSTRAC Rules should be provided setting out explicit expectations of the minimum information that should be documented by the reporting entity when documenting their EWRA in this regard as just stating ‘nature, size and complexity’, is wide open to interpretation.

We would like to propose at least the following information should be required to be documented:

No	Suggested Minimum Requirements for Nature, Size and Complexity Explanations
1	General information such as legal status, legal name, trading name, country, and date of incorporation
2	Description of the nature of the business including history of the company, the customers it services (and targets), the products and services offered, the channels it distributes them through (including the use of third-party intermediaries such as brokers, agents, or other intermediaries), the geographies, industries, and markets it operates in (and plans to operate in the next 12 months). Also types of activities that the business prohibits (i.e., engaging with shell companies, offering products in countries determined to be too high risk, offering products to unregulated entity’s) and how it manages

No	Suggested Minimum Requirements for Nature, Size and Complexity Explanations
3	Description on the size of the business in terms of the number of customers, number of branches/offices, number of employees and the size of business by financial metrics, revenue, profit growth etc.
4	Description on the complexity of the business including any recent or planned M&A activity, the relationship of the business to parent organisations (i.e., subsidiary of a foreign branch) and the role between the parent and subsidiaries from an ML/TF perspective.
5	Description of the Board Governance and Oversight framework including the relationship of the AML Compliance Officer to the Board, the level of skills, expertise, and qualifications of the AML Compliance Officer(s), a description of the explicit roles and responsibilities and the frequency and content of management information supplied by them to the Board in relation to ML/TF/PF matters.

By issuing more specific guidance about what is meant by ‘nature, size and complexity’, it is likely that the quality of AML/CTF Policies will improve since reporting entity’s will need to apply a deeper level of thinking when documenting this, than they otherwise might have.

## 2.2 Documenting the ML/TF risk assessment methodology

We also **agree** that reporting entity’s should be required to document the ML/TF/PF risk methodology, including the rationale behind decisions such as weighting risk groups, risk categories, risk factors and controls and any rationale for determining what risks to consider and the risk ratings that have been applied.

However, simply requesting regulated entity’s document their ML/TF/PF risk assessment methodology alone **does not go anyway near far enough** and again we feel AUSTRAC should issue explicit rules that set the expectations of the minimum information that should be provided by reporting entity’s when documenting their Enterprise-Wide ML/TF/PF Risk Assessment methodology.

We believe that AUSTRAC should issue Rules (and accompanying guidance) that clearly articulates what is expected to be documented in relation to the ML/TF/PF Risk Assessment methodology and have provided descriptive suggestions about the substance behind the methodology that we feel reporting entity’s should be including in their documentation for your consideration.

No	ML/TF/PF Risk Methodology Requirements
1	Explanation of the process that the Board and Senior Executive team undertook to determine the organisations risk appetite and risk tolerance as it pertains to ML/TF/PF risks and actions that are to be taken if the ML/TF/PF risk assessment demonstrates that residual risks are outside stated appetite and/or risk tolerance statements.
2	Explanation of the ML/TF/PF methodology the reporting entity has put in place, when and how it was developed, how long it has been in effect for and how frequently it is updated, and whether the ML/TF/PF risk assessment has been subject to external review by suitably qualified experts.
3	Explanation of the ML/TF risk assessment approach to identifying and assessing inherent risks, for example, what risk groups, risk categories, risk factors and risk indicators were considered (and why), whether all risks are weighted equally or whether there is some proportionality and what the rationale is.
4	Explanation of the ML/TF risk assessment approach to conducting control design and operational effectiveness testing, testing methods, size of testing samples, how control effectiveness was determined, and any weighting applied to key controls etc.
5	Explanation of how the ML/TF risks are aggregated across different legal entity’s, business lines, operating divisions, product lines and countries as appropriate.
6	Explanation the process for documenting enhancement opportunities to continuously improve the approach to ML/TF risk assessment.
7	Explanation of the time-based and event-based triggers that has in the past prompted a review and refresh of the ML/TF risk assessment.
8	Explanation of what process the organisation undertakes to gather qualitative (question-based) and quantitative (data-based) inputs to inform the ML/TF risk assessment process and to strike the right balance between subjective and objective approaches to ML/TF risk assessment.
9	Explanation of how the ML/TF risk assessment methodology aligns to international standards of risk management (i.e., ISO31000 or similar).
10	Explanation of how the ML/TF risk assessment inputs and outcomes are presented and discussed with the Board and Executive committee and how any follow-up actions to continuously improve this process are tracked and monitored.
11	Explanation whether the organisation is adopting RegTech to conduct enterprise-wide ML/TF risk assessments or if not to provide an explanation and justification that excel spreadsheets are fit for purpose (which they are most certainly not for organisations of a certain size or complexity)  AUSTRAC would not accept a major financial institution to perform ML/TF Transaction Monitoring using spreadsheets, to monitor clients, accounts, or transactions, but seem to remain non-committal in setting expectations for large, sophisticated reporting entity’s to discontinue the widespread use of excel spreadsheets which are not fit for purpose, which is disappointing and luddite – it’s 2025, not 2005 😞

No	ML/TF/PF Risk Methodology Requirements
	<p>As a result of this passive approach taken by AUSTRAC, the largest six banks in Australia all still conduct EWRA's using spreadsheets, so it is unsurprising to see repeated material compliance failures, when they are using excel spreadsheets to manage their money laundering and terrorism financing risks.</p> <p>In other jurisdictions, regulators have gone the opposite way to AUSTRAC, writing to banks and others notifying them that spreadsheets are no longer acceptable – we have <a href="#">written extensively</a> on the limitations of excel, but AUSTRAC appears to be very passive and regressive in this regard.</p> <p>We believe that complex organisations (i.e. banks, credit unions, investment managers) that fail to consider adopting technology for this purpose, should be challenged by AUSTRAC since the value proposition and benefits are undeniable.</p>

### 2.3 Defining a baseline of ML/TF/PF risks that must be identified and assessed

We also **strongly support** the AGD's "baseline" for identifying and assessing ML/TF/PF risks as they relate to customer types, types of designated services, methods of delivery, and jurisdictions they deal with. AGD stated additional factors may be specified by AUSTRAC in the Rules, if required.

We believe that additional risks are required to be added to the AML Rules as a "baseline" as the current definitions are **too high level and overly simplistic** and should contain many other elements that are entirely missing and are essential to properly being able to identify and assess these risks, which we have simplified to get a far deeper understanding of financial crime risk management approaches so that Australia's ML/TF framework can mature far beyond the overly simplistic "baseline" that it has been using for the last 19-years.

We've summarised some of the risk groups and risk categories that we feel should be considered by regulated entity's, many of those such as environmental risk (internal and external), employee risk, outsourcing risk, transaction risk are just a few risk elements that do not warrant a mention and are for AUSTRAC to consider.

In our experience, many organisations struggle translating the "helicopter" view guidance to practical "ground floor" actionable steps, when designing ML/TF/PF risk frameworks.

#### Examples of ML/TF Risk Groups and Risk Categories that should be explicitly covered

Environmental Risks	Customer Risks	Business Risks
<p>Assess the organisations vulnerability to:</p> <ul style="list-style-type: none"> <li>• <b>Predicate Offences</b> – deceptive crimes, illicit trafficking, personal crimes, property crimes</li> <li>• <b>Money Laundering</b> – higher risks associated with – business operations, channels, customer transactions, customers, products and services</li> <li>• <b>Terrorism Financing</b> – higher customer risk and customer transaction risks</li> <li>• <b>Financial Sanctions</b> – higher customer risk and customer transaction risks</li> <li>• <b>Regulatory Compliance Risks</b> – governance and oversight, program alignment to risks, program non-compliance and reporting</li> </ul>	<p>Assess the organisations vulnerability to:</p> <ul style="list-style-type: none"> <li>• <b>Customer Types</b> – segmentation of customer base - individuals, private companies, public companies, offshore companies, trusts, partnerships including extent UBO's known.</li> <li>• <b>Customer PEP Status</b> – number of customers that are foreign or domestic PEPs and categories of PEPs</li> <li>• <b>Customer Location Risk</b> – <i>segmentation of customers by location/geography</i></li> <li>• <b>Customer Business Risk</b> – <i>segmentation of customers by industry sector/occupation</i></li> <li>• <b>Customer Source of Wealth</b> – segmentation of customers where this information is known, unknown or vague</li> </ul>	<p>Assess the organisations vulnerability to:</p> <ul style="list-style-type: none"> <li>• <b>Business Location</b> – extent of business operations that are carried out overseas (and which countries and which operations)</li> <li>• <b>Outsourcing Risk</b> – 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!</li> <li>• <b>Employee Risks</b> – 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.</li> </ul>

Channel Risks	Product & Services Risks	Country Risks
<p>Assess the organisations vulnerability to:</p> <ul style="list-style-type: none"> <li>• <b>Non-Face-to-Face Channels</b> – the extent to which customers are met face to face during on-boarding or when servicing their accounts</li> <li>• <b>Methods of interacting with customers</b> – what methods are used, somewhat anonymous (e.g., internet, social media, SMS) or less anonymous (e.g., branch, post office, video conferencing, telephone etc.)</li> <li>• <b>Use of third parties</b> – 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</li> </ul>	<p>Assess the organisations vulnerability to:</p> <ul style="list-style-type: none"> <li>• <b>Products and Services</b> – extent to which different products and services are offered (250+ Financial Services Products)</li> <li>• <b>Attributes of products and services that make them more attractive to money launderers</b> – 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.</li> <li>• <b>Extensiveness of use</b> – 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.</li> </ul>	<p>Assess the organisations vulnerability to:</p> <ul style="list-style-type: none"> <li>• <b>Methodology</b> – 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)</li> <li>• <b>Frequency</b> – 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!</li> </ul>

We would recommend AUSTRAC issuing more granular rules and guidance on what it expects reporting entity's to include in an effective EWRA. We would also like to suggest AUSTRAC includes other explicit risk considerations are include:

- **Sanctions** risk indicators as part of an ML/TF risk assessment
- **Transaction risk** indicators related to value and volume of transactions in EWRA's.

### 2.3.1 Benefits of a standardised baseline approach for AUSTRAC

We would also recommend that AUSTRAC consider developing “industry baseline risk models”, expanding the excellent “sectoral risk assessment guidance papers” it has issued outlining the minimum risk groups, risk categories, risk factors and risk indicators that they expect reporting entity's in particular industry sectors to adopt. We also feel AUSTRAC would benefit themselves from digitising their approach to oversight of ML/TF/PF Risk Assessments by adopting RegTech themselves and encouraging (or mandating) the use of technology as this would undoubtedly lead to more effective regulation (as opposed to manual oversight, which is simply ineffective given the sheer volume of reporting entity's).

We have documented how RegTech can deliver significant value to AUSTRAC and Australia's fight against financial crime in a short [video](#) and [value proposition](#), which Arctic is discussing with several AML supervisors in different jurisdictions globally. It only takes one brave soul and an open mind to try new things and would open up a world of possibilities.

Without AUSTRAC's adoption of RegTech supporting a baseline approach we feel it will be almost impossible for AUSTRAC to effectively oversee 100,000+ different EWRA methodologies and would be remiss not to at least consider how technology solutions could facilitate and enable AUSTRAC in conducting comparative benchmarking of ML/TF risk management capabilities in real-time.

We would be open to exploring this with AUSTRAC and the FinTel Alliance (most of whom are using excel spreadsheets to conduct EWRA's).

## 3. Triggers for ML/TF risk assessment refreshes

### 3.1 Time-based triggers

We **disagree** with the minimum requirement for reporting entity's to have independent evaluations, including ML/TF/PF Risk Assessments every 3-years, when in most jurisdictions a mandatory expectation is that this should be conducted annually as recommended by the Financial Action Task Force (FATF).



AGD (which initially proposed every 4-years) indicated that this applies to “current and new reporting entity’s”, meaning the reporting entity’s that have been conducting ML/TF/PF risk assessments “at least annually” as per international standards could conceivably decide to revert to a three-year review instead.

We know from first-hand experience that at least 3 of the largest Australian banks are conducting EWRA’s every 2-years, not annually. We also have experienced another major banking client of ours that has a fair share of troubles and in their wisdom decided to move from an annual EWRA to one every 2-years and simultaneously move back to excel spreadsheets, regardless of whether they are fit for purpose or not, which they largely are not. We believe this is a direct result of a lack of prescription about expected frequency of ML/TF/PF risk assessments and a non-committal approach to challenging the effectiveness of using excel to conduct risk assessments by these reporting entity’s.

Obviously, a lot can happen in 2 to 3 years and reviewing the ML/TF/PF risk assessment (which includes the design and operational effectiveness of mitigating controls) so infrequently is likely to mean that these risks remain unassessed or unmitigated until it is far too late, and the damage is done. It is also obvious that looking at the enforceable undertakings that in many cases these boiled down to regulated entity’s having an insufficient understanding of their financial crime risks and controls.

In other regulatory jurisdictions, such as the UK, the Financial Conduct Authority (FCA), which is AUSTRAC’s equivalent has frequently issued “Dear CEO” letters highlighting the common failings related to Business-Wide Risk Assessments (BWRAs), which we have summarised below.

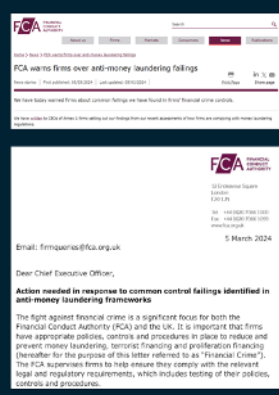
**Regulators have consistently found that the quality and substance of business-wide ML/TF risk assessments are falling far short of their expectations**

*Regulators like the UK’s Financial Conduct Authority (FCA) issue warnings in the form of “Dear CEO” letters, notifying businesses of common failings in AML frameworks and actions they need to take*

**Common failings related to business-wide ML/TF Risk Assessments (BWRA):**

- ✓ Completely absent despite the legal requirement to conduct BWRAs
- ✓ Failure to document in writing the steps taken to identify and assess ML/TF and PF risks
- ✓ Failure to understand the ML/TF and PF risks that businesses are exposed to
- ✓ Failure to design and implement appropriate controls to mitigate those risks
- ✓ Poor quality BWRAs lacking sufficient detail and methodology used is often unclear
- ✓ Failure to clearly articulate relevant mitigating measures in place to counteract risk
- ✓ Failure to determine the effectiveness of controls to mitigate ML/TF and PF risks
- ✓ Failure to establish the residual risks that the business remains exposed to
- ✓ Lack of appropriate oversight from senior management
- ✓ Absence of a clear audit trail for financial crime related decision-making.

Source: [https://www.fca.org.uk/publication/correspondence/dear\\_ceo\\_letter\\_action\\_response\\_common\\_control\\_failings\\_anti\\_money\\_laundering\\_frameworks.pdf](https://www.fca.org.uk/publication/correspondence/dear_ceo_letter_action_response_common_control_failings_anti_money_laundering_frameworks.pdf)



Perhaps AUSTRAC could consider issuing a “G ’Day CEO” letter? That would be fun 😊

### A lot can happen in 3 years...

The pace of change in a 3-year period for most businesses is immense – for example in the external operating environment in the last 3 years we have had a global pandemic (driving up operational risks as people work from home, a seismic shift towards digital payments and a massive rise in frauds and scams), global macro-economic slowdowns (and benefits fraud, tax evasion), massive tax evasion scandals including Australian businesses and individuals, a decline in international instability with Russia’s war on Ukraine, Israel/Palestine conflict and other international posturing.

Further in relation to the internal operating environment, organisations would also go through material changes including (but not limited to) mergers and acquisitions (already highly present in the credit union / mutual banking sector in Australia), launching new products and services, acquiring new customer types, launching into new industry segments or countries, or deploying and sunsetting new technology systems etc. so the pace of change is much faster than every 3 years and reviews of ML/TF/PF risk assessments should be conducted annually and reviewed at least every 2 years.

How can AUSTRAC reasonably expect to enforce Board oversight function if Boards are only reviewing their ML/TF/PF risks, controls and mitigating plans every 3-years, when they are likely to be either out of date or should have been actioned years prior?

### 3.2 Event Based Triggers

We also **strongly support** the requirement that reporting entity's must keep their risk assessment up to date based on "triggers" that could include "changes to a businesses' risk profile or the adoption of new technologies to manage certain AML/CTF obligations.

We recommend that AUSTRAC could develop rules clearly defining the types of "triggers" that should prompt a review of the ML/TF/PF risk assessment and have provided suggestions below:

External Events		Internal Events
Regulatory Events	Other Events	
Enforcement activity targeted at certain sectors or activities - is the same activity present?	Changes in the geo-political landscape making a country at higher risk than before.	External (or internal) independent review highlighting deficiencies in the ML/TF risk assessment.
Changes in AML/CTF regulations or rules - how do they impact your organisation?	Changes in various published country risk rankings (i.e., transparency international).	Review of ML/TF risk assessment prior to annual compliance reports being filed with the regulator.
Changes in guidance and risk typologies - has your ML/TF risk assessment considered this?	Increased media scrutiny on certain companies, industries, or activities.	Organisation is launching or has launched new products services, which pose new ML/TF risks.
Consultation papers about proposed regulatory changes - what would be the impact on your business if these laws are enacted?	Changes in the threat landscape as criminals find more innovative ways to launder criminal proceeds.	Organisation is targeting new customer segments, expanding into new geographic markets, or generally changing its business.
International guidance issued by the FATF, the Wolfsberg Group, the Egmont Group highlighting trends and risk-related guidance.	Emerging technologies that could pose new threats to your organisation, such as criminal use of Artificial Intelligence.	Merger and acquisitions activity (i.e., divestments, acquisitions) bringing together businesses with different risks and approaches.
Publishing of National Risk Assessments highlighting threats at national, industry, product, or activity level.	Collaboration through public and private partnerships could present opportunities to update ML/TF risks and controls.	Change in Board and/or Senior Management, with a greater focus on risk appetite and management.
Release of federal, state, or local crime statistics that are relevant to your industry and operations.	Investigations by journalists or law enforcement into organised criminal activity that is related to your organisation's operations.	Appointment of a new AML/CTF Compliance Officer/MLRO looking to make changes to the ML/TF risk assessment and AML Program.
Criminal or civil prosecutions or other enforcement action (i.e., enforceable undertaking, regulator appointed independent auditors).	Class actions being filed against organisations for failing to manage or disclose risks.	Appointment of risk, compliance, or legal advisors with experience in conducting and updating ML/TF risk assessments.

## Part 4 – Division 2 – AML/CTF policies

### 1. General Comments

#### 1.1 Reporting entities must develop and maintain AML/CTF policies

26F(3) of the Act requires reporting entity’s to review and update AML/CTF policies (1) in response to a review of the ML/TF risk assessment (c)(i) and (2) circumstances specified in the AML/CTF Rules.

The Act also defines that reporting entity’s must review AML/CTF policies based on the frequency defined in the Rules or at least every 3 years. Again, for the reasons described above we **disagree** that for most businesses reviewing AML/CTF policies every 3-years is sufficient.

## Part 4 – Division 3 – AML/CTF compliance officers

### 1. General Comments

We **agree** with AUSTRAC’s annual requirement for a governing body to be presented with a summary of whether the AML/CTF Program complies with both internal policies and external laws and rules, as well as an assessment of whether the reporting entity is appropriately managing its ML/TF/PF risk effectively.

In our opinion, this latter requirement to assess and report on the effectiveness of the ML/TF/PF risk management should, under most circumstances require a reporting entity to establish a regular assessment of the internal and external threat environments, assess the design and operational effectiveness of those controls, track action plans, particularly where residual risks remain outside of governing body appetite and frequent reporting in relation to changes in methodology, scope, approach, weightings and so forth, immediately prior to the annualised reporting requirement be able to provide an accurate representation.

If AUSTRAC shares this opinion, then an explicit rule for reporting entity’s to undertake an ML/TF/PF risk assessment on an annualised basis, in the prior quarter to the governing body report would clearly be a robust way for AUSTRAC and the governing body to know that the information that is being presented in regards the ML/TF/PF risk assessment is recent, reliable and a fair reflection of whether the reporting entity is in fact managing its ML/TF/PF risk appropriately. If this is not done in advance of this, what may be presented could be baseless and outdated.

Board directors and governing body members have a fiduciary and legal responsibility to ensure their organisation’s ML/TF/PF policies comply with internal policies and external laws and that enterprise-wide money laundering risk assessments effectively identify and mitigate risks.

However, in many cases Executive and Non-Executive Directors lack the appropriate skills, knowledge and practical experience to comprehend and genuinely understand ML/TF/PF risks or even lack the capacity and capability to ask intelligent and informed questions of the AML/CTF compliance officer. For example, the governing body may be presented with management’s view of the organisations ML/TF/PF risk profile but may fail to ask or understand the intricacies of the methodology that was applied and whether that is in fact, sound, logical and reasonable or even determine that the qualitative and quantitative data inputs were current, reliable and accurate, which is problematic for any governing body oversight.

It is recommended that AUSTRAC clearly defines in the rules what “*take reasonable steps*” actually means so there can be no doubt about what AUSTRAC expects. We’ve made suggestions below:

No	Actions governing body’s should be required to undertake to take to evidence they’ve taken ‘reasonable steps’
1	Governing body’s must be able to evidence that they have a clear understanding of the scope and objectives of the ML/TF/PF risk assessment to ensure that all relevant areas, including customers, products, channels, geographies, and transactions are assessed and further understand the origin and accuracy of quantitative data inputs that have been used as inputs to the ML/TF risk assessment.



No	Actions governing body's should be required to undertake to take to evidence they've taken 'reasonable steps'
2	Governing body's must critically review and scrutinise the inputs and outputs of the organisation's ML/TF/PF risk assessment and satisfy themselves that the risk assessment results are in alignment with the organisation's risk appetite statement. Governing body's should formally document and approve a risk appetite statement, specifically relevant to financial crime risk appetite.
3	<p>Governing body's must critically challenge management by asking probing and informed questions about the following:</p> <ul style="list-style-type: none"> <li>(a) <b>Risk assessment methodology including:</b> (i) the risk indicators that were included / excluded from the scope of the risk assessment (potentially due to missing or unreliable data) (ii) whether any proportionality has been applied for example to risk groups, risk categories, risk factors, risk indicators, control categories, controls or weighting between assessment units) (iii) the rationale behind the methodology (i.e., weighting decision rationale, qualitative vs. quantitative approaches) (iv) the approach taken and the results derived from the control design and operational performance testing to test the effectiveness of controls (v) the limitations or issues encountered in designing, executing and maintaining the risk assessment (vi) the internal and/or external resources (i.e., time and effort) spent on the risk assessment and the (vii) actions identified with owners and target completion dates for any identified deficiencies or areas for improvement</li> <li>(b) <b>Whether the approach to risk assessments is appropriate and fit for purpose,</b> given the nature, size and complexity for the organisation (<i>here we are implying that excel-based risk assessments performed every 2-3 years with limited documentation and audit trail should not be considered fit for purpose for a large multi-national, billion-dollar revenue business</i>).</li> <li>(c) <b>Whether the risk assessment is timely enough</b> given the volume of internal and external changes that would influence the ML/TF/PF risk assessment</li> <li>(d) <b>Whether the level of control design and operational effectiveness testing has been sufficient and</b> whether any mitigating strategies are appropriate to adequately manage the risk</li> <li>(e) <b>Whether the implementation of risk mitigation measures has been completed in a timely enough manner</b> to mitigate the risks</li> <li>(f) <b>Reviewing records related to risk assessments</b> including board discussions, management meeting minutes related to the preparation of the risk assessment and any decisions made</li> </ul>

Further the Act, requires reporting entity's to "take reasonable steps" to ensure they are:

- (i) Appropriately identifying, assessing, managing and mitigating the risks of money laundering, financing of terrorism and proliferation financing that the reporting entity may reasonably face in providing its designated services; and
- (ii) Is otherwise complying with its AML/CTF policies, the Act, the regulations and the AML/CTF Rules.

Without providing clarity on what "take reasonable steps" actually means is very subjective and could be taken to mean very different things – what's reasonable to one, is completely inadequate for another, so AUSTRAC should provide clarity in the Rules about what it considers to be reasonable in regard to the above obligations. Again, we've made suggestions below:

No	Actions reporting entity's should undertake to take to evidence they've taken 'reasonable steps'
1	Reporting entity's must develop and maintain a comprehensive ML/TF/PF risk assessment framework by establishing a structured approach to identifying, assessing, and documenting ML, TF, and PF risks associated with the entity's designated services. This should involve taking actions such as (i) conducting periodic and documented ML/TF/PF risk assessments considering factors such as internal (i.e., operational, employee, outsourcing) and external (i.e., external threat landscape) facing risks, customer risks, product and services risk, delivery channel risk, transaction risk and geographic exposure (ii) conduct data analytics to identify high-risk areas by analysing transaction patterns, customer behaviours in respect of products and channels, as well as industry trends and (iii) update the risk assessment regularly to reflect changes in the regulatory environment, emerging threats, or the entity's business model. Reporting entity's must be able to evidence that they are maintaining risk assessment reports, methodology documents including the rationale for risk rating weightings and other settings, and records of risk classification for customers, products and services, channels and countries etc.
2	Reporting entity's must design, implement and maintain ML/TF/PF risk-based policies and procedures by developing and enforcing policies, controls, and procedures tailored to the reporting entity's specific risk profile. This should involve taking actions such as (i) establishing frequent (i.e., at least quarterly) meetings to determine whether any triggers have occurred that would require the risk assessment and/or policies to be updated (ii) providing management reporting on the design and operational effectiveness testing results, deficiencies / improvements identified and actions to be taken to strengthen the control framework
3	Reporting entity's should maintain a mapping document that measures the levels of compliance against specific obligations as defined in the Act and Rules, with an assessment against each (i.e., fully compliant, partially compliant, non-compliant) and document any action plans where compliance deficiencies have been identified and provide regular updates to the governing body that demonstrates that the reporting entity is and remains in compliance with its regulatory AML/CTF obligations.

## 2. Other Comments

We **agree** with the requirement for every reporting entity to appoint a 'fit and proper' person as the AML/CTF Compliance Officer, that is employed or *otherwise engaged*, by the reporting entity at the management level and has sufficient authority, independence and access to resources and information to be able to perform the function.

Given the volume of reporting entities (estimated to be an additional 90,000, on top of ~17,500 currently regulated entities) and the industry distribution, particularly in the accounting and legal professions being heavily skewed towards micro-businesses that are sole traders or employ 1-5 practitioners, many "managed service providers" are now looking to offer a full-service compliance outsource model, which will include acting as the AML/CTF Compliance Officer.

In this regard, we would recommend AUSTRAC defines in the Rules the expectations where reporting entity's are outsourcing this function to managed service operators defining guard-rails around this, such as limiting the number of reporting entity's a managed service operator could act as the AML/CTF Compliance Officer for. For example, if one individual employed by a managed service operator is allowed to act as the AML/CTF Compliance Officer for say more than 10 different reporting entities, are they really going to be capable of performing the role effectively?

Also, it is debatable whether an outsourced managed service provider would be able to maintain "sufficient authority" within an organisation or have "access to resources and information" to perform the expected functions (i.e., oversee and co-ordinate day-to-day compliance and operational effectiveness and compliance, communicate with AUSTRAC etc.) effectively, so it would be good to see some Rules and/or Guidelines provided on this.

Further in terms of the currently stated considerations when appointing an AML/CTF Compliance Officer whether the person "*has the competence, character, diligence, honesty, integrity and judgement to properly perform the duties of the role*", we would recommend this definition be expanded to include **capability**, meaning the **skills, knowledge, previous experience**, to perform the role. A person may have the other attributes described but remain totally unqualified to perform the role and skills, knowledge and experience are equally important considerations when appointing and AML/CTF Compliance Officer and should also be included.

We also agree with AUSTRAC's ability to require a reporting entity to undertake an ML/TF/PF risk assessment and agree with all of the circumstances. However, given AUSTRAC resources determining whether a particular reporting entity has an adequate ML/TF/PF risk assessment in place on an individualised basis will require far more resource than AUSTRAC has available, but if AUSTRAC were open to looking at standardisation and adoption of enabling technology as described earlier, then they could easily benchmark ML/TF/PF risk assessment outcomes far more easily than the 'knock on the door' approach.

It may also be worth noting that the risk assessment requirements specify proliferation financing must be included, yet many of the abbreviations across the Rules use only ML/TF only and would be better if PF were added as a clear reminder that it is expected to be included.

## Part 4 – Division 4 – AML/CTF program documentation

We agree with the time period for AML/CTF program documentation as drafted and no further comments other than those already provided.

### Additional considerations for AUSTRAC

Often when there are material AML/CTF compliance failures these frequently relate to issues that have remained undetected or unaddressed for years (or even decades) because of independent reviews either not having been completed in a timely manner (if at all) or by independent reviewers not being sufficiently skilled or thorough in their reviews, particularly in the areas of control effectiveness testing.

We **disagree** with 26, 4(f)(ii) in the Act that requires independent evaluations of the reporting entity’s AML/CTF program at least once every 3 years, which we feel is far too long a period and suggested to AGD in our previous submission that this should be at least every 2-years.

However, 26, 4(f)(i) states that the frequency of independent evaluations must be appropriate to the “nature, size and complexity of the reporting entity’s business”, which in itself is vague for the reasons provided earlier in this submission and provides no clarity on what is appropriate and we feel AUSTRAC should prescribe in the Rules their expectations of when a business of a certain nature, size and/or complexity warrants an independent review more frequently than every three years, to avoid large, complex businesses in higher risk sectors deciding that they will default to the 3-year cycle, when either annually or every two years is more appropriate.

We would like to suggest that AUSTRAC define some parameters around this, for example:

Frequency of independent evaluation	Nature	Size	Complexity
1-Year Cycle	High-risk industry sectors (AUSTRAC to define) – crypto, casinos, online gaming	>\$100m in revenue; or >10,000 employees; or >100,000 customers; or >100,000 accounts; or > 10 designated services >25 branches/offices >10 legal entities in group	>75% of revenue from overseas markets; or  Prior to or within 6-months after any M&A activity
2-Year Cycle	Medium-risk industry sectors (AUSTRAC to define)	>\$50m in revenue; or >5,000 employees; or >50,000 customers; or >50,000 accounts; or > 5 designated services >15 branches/offices >5 legal entities in group	>50% of revenue from overseas markets; or  Prior to or within 6-months after any M&A activity

The above is illustrative, to get the point across, and of course the ‘criteria’ can be debated, but the point is there should be some criteria defined that is more prescriptive otherwise AUSTRAC can expect that 3-years independent evaluations will immediately become the industry default, if it is left entirely to the discretion of the reporting entity to decide when independent evaluations should be conducted.

We would also recommend that AUSTRAC’s website is also updated since it states “*you must decide on how often reviews are done. How you decide depends on the size of your business, what kind of business you have, how complex your business is and your level of ML/TF risk*”. **This simply does not go far enough.**

We have met many businesses that have never had an independent review of their AML/CTF Program since the laws were enacted in 2006 (19 years ago), so this risk-based approach to independent reviews is not driving the right behaviours or outcomes needed for the 17,500 businesses regulated by AUSTRAC a problem that will be exacerbated with Tranche 2.

Further, we believe AUSTRAC should provide explicit rules on who is qualified to undertake an independent evaluation. We often hear about unqualified persons conducting superficial independent reviews, giving regulated businesses a false sense of comfort, and often failing to perform control testing at all, which in our opinion does not even constitute an independent review.

Several years back, AUSTRAC established an Approved Persons list for practitioners that had demonstrated their skills, qualifications and/or experience in AML/CTF, much like the Skilled Person panels that exist in the UK and administered by the Financial Conduct Authority. In Australia, this process and concept was dropped, and it was not clear why, but seems like a sensible thing to consider reinstating.

## **Closing Remarks**

We appreciate the opportunity to comment as part of the first round of consultation feedback and we hope that you find the comments constructive and hope that some of these suggestions will be carefully considered and hopefully adopted as we do feel some further rules and guidance are required in relation to the ML/TF/PF Risk Assessment process, beyond what's contained in the AML/CTF Amendment Bill.

We would welcome the opportunity to discuss any of the suggestions provided in any public or private forum that AUSTRAC holds in relation to the consultation process.

Finally, we appreciate that AUSTRAC may not agree with some or all of this feedback and that not all suggestions can or will be actioned but we appreciate you taking the time to consider them and we commend AUSTRAC for its many stakeholder initiatives and its progressive approach to AML/CTF regulation and we look forward to supporting these common goals to help reporting entities to fight financial crime in Australia.