MONEY LAUNDERING AND THE RISK IN THE RISK-BASED APPROACH: THE AUSTRALIAN CONTEXT

DORON GOLDBARSHT* AND ELIZABETH SHEEDY**

In recent years, the Australian regulator has taken enforcement action against reporting entities for failure to comply with the risk-based approach to anti-money laundering ('AML') and counterterrorism financing ('CTF'), resulting in massive penalties and other damaging repercussions. These actions have highlighted the need for reporting entities to identify and respond to the AML/CTF risks posed by their businesses even more than before. This paper aims to provide a critical analysis of how the concept of risk operates within Australia's AML/CTF regulatory framework and to suggest ways of enhancing the efficiency of compliance with the global standard. Against the backdrop of these enforcement actions and their pronounced implications, this article offers an original and interdisciplinary contribution by thoroughly exploring the subtle nuances of how risk, as a pivotal concept, orchestrates the course of AML/CTF regulatory endeavours within Australia. By meticulous analysis and well-reasoned suggestions, this article takes on the mantle of not only investigating the status quo but also envisioning pathways for augmenting compliance efficiencies in harmony with global standards. In doing so, it navigates uncharted avenues within the legal domain, casting a spotlight on the intrinsic symbiosis between risk comprehension and regulatory adeptness.

I INTRODUCTION

In 2003, the Financial Action Task Force ('FATF') explicitly introduced a risk-based approach to combat money laundering and terrorist financing.[1] The risk-

* Doron Goldbarsht, LLB LLM (HUJI) PhD (UNSW), is an Associate Professor at Macquarie Law School in New South Wales, Australia and the Director of the Financial Integrity Hub (doron.goldbarsht@mq.edu.au).

** Elizabeth Sheedy, BCom (UNSW) PhD (MQ), is a Professor in the Department of Applied Finance at Macquarie Business School, New South Wales, Australia and Advisory Board Member of the Financial Integrity Hub.

The authors wish to thank Mr Samuel Orchard for his excellent research assistance. We gratefully acknowledge the support of Arctic-Intelligence and the Financial Integrity Hub at Macquarie Law School in New South Wales, Australia for partly funding this research.

1 Anna Simonova, 'The Risk-Based Approach to Anti-Money Laundering: Problems and Solutions' (2011) 14(4) *Journal of Money Laundering Control* 346, 346.

based approach shifted the responsibility for establishing the principles and regulations that best aid in the detection and prevention of money laundering to domestic regulators.[2] Some argued that the approach was too prescriptive, restricting regulated entities from using their own initiative.[3]

Between 2007 and 2009, the FATF collaborated with industry sectors to develop high-level principles and guidance that would assist both public authorities and private companies in applying a risk-based approach.[4] Having standards and guidance in place would also facilitate international cooperation and information-sharing among institutions and regulators — a crucial strategy in combating money laundering and terrorist financing activities, which often span national borders.[5] However, despite its intention to foster common understanding and interpretation, the FATF proffered only a vague description of the risk-based approach as one that 'encompasses recognising the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks',[6] resulting in its inconsistent application between jurisdictions.[7] Despite this, the risk-based approach has been globally adopted.[8] By 2012, it was widely accepted as the most effective approach across all industries, and in institutions of all sizes and sectors, for the prevention and detection of money laundering and terrorist financing activities.[9]

Following this introductory Part I, Part II of this paper details the shift from a rule-based system to a risk-based approach in the FATF global standards for anti-money laundering ('AML'), revealing the reasons for the change and identifying the challenges inherent in the practice of effective risk management across industries.

2 Lishan Ai, John Broome and Hao Yan, 'Carrying Out a Risk-Based Approach to AML in China: Partial or Full Implementation?' (2010) 13(4) *Journal of Money Laundering Control* 394, 399.

3 Ibid 398.

4 The guidance covered the application of the risk-based approach with regard to the

> financial sector, real estate agents, accountants, trust and company service providers … dealers in precious metals and stones, casinos, legal professionals, money services businesses … and the life insurance sector.

Financial Action Task Force, *Guidance for a Risk-Based Approach: The Banking Sector* (Report, October 2014) 3 n 4 ('*The Banking Sector*'). See, eg, Financial Action Task Force, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures* (Report, June 2007) 1 [1.2] ('*Guidance on the Risk-Based Approach*').

5 *Guidance on the Risk-Based Approach* (n 4) 4.

6 Ibid 2 [1.8].

7 Simonova (n 1) 349–50.

8 Doron Goldbarsht, 'Who's the Legislator Anyway? How the FATF's Global Norms Reshape Australian Counter Terrorist Financing Laws' (2017) 45(1) *Federal Law Review* 127, 132.

9 Gary W Sutton, 'The New FATF Standards' (2012) 4(1) *George Mason Journal of International Commercial Law* 68, 75–6. For a detailed transition from rules to risks, see Doron Goldbarsht and Louis De Koker, 'Financial Crime and the Law: Identifying and Mitigating Risks' in Doron Goldbarsht and Louis De Koker (eds), *Financial Crime and the Law: Identifying and Mitigating Risks* (Springer, 2024) 1, 2–5.

Part III provides a case study of the AML risk regime in Australia, demonstrating the need to rethink the application of a risk-based approach domestically in the context of risk-oriented AML procedures. Part IV considers the potential for sector-specific content to enhance the efficiency and effectiveness of AML systems and concludes with a suggestion for an alternative approach to AML risk management.

II THE GLOBAL REGIME

The FATF is an intergovernmental organisation responsible for setting international AML and counterterrorism financing ('CTF') standards and promoting effective implementation of legal, regulatory and operational measures for combating threats to the integrity of the international financial system.[10] It was formed in 1989 by the Group of Seven industrialised nations and now comprises 37 member countries and two regional organisations. In 1990, the FATF issued 40 recommendations to combat the 'menace' of money laundering and, in 2001, it issued nine additional recommendations in response to growing terrorism concerns.[11] Together, the FATF recommendations are recognised as the global standard for AML and CTF.[12] Member countries are expected to comply with the recommendations by enacting laws and regulations to prevent money laundering and terrorist financing threats within their respective jurisdictions.[13]

The FATF encourages member countries to adopt a risk-based approach to ensure that the measures taken to 'identify, assess and understand … money laundering and terrorist financing … are commensurate with the risks identified'.[14] While the 2003 revised recommendations provided for the risk-based approach to be applied in some areas, 'the 2012 [revised] Recommendations consider[ed] the … [approach] to be an "essential foundation" of a country's AML/CTF framework' and 'an over-arching requirement applicable to all relevant FATF Recommendations'.[15] The need for members to adopt the risk-based approach was also emphasised in the FATF's updated *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*.[16]

In addition to adopting the 40 recommendations, most countries have also enacted solid legal frameworks for assessing risk and have implemented a risk-based

10 Goldbarsht (n 8) 131.

11 Ibid 131–2; Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (Report, November 2023) 7 ('*International Standards*').

12 Goldbarsht (n 8) 131–2.

13 Ibid 138–9.

14 'Recommendation 1: Assessing Risks and Applying a Risk-Based Approach', *Caribbean Financial Action Task Force* (Web Page, 2024) <www.cfatf-gafic.org/index.php/documents/fatf-40r/366-fatf-recommendation-1-assessing-risks-and-applying-a-risk-based-approach>.

15 *The Banking Sector* (n 4) 6 [13].

16 *International Standards* (n 11) 10. These standards have been regularly updated since 2012.

approach for combating money laundering and terrorist financing in their domestic legal frameworks.[17] '[A] notable example is the US Patriot Act,[18] which … [marks] a shift in money laundering policy from a rule-based approach to a risk-based approach.'[19] Under the risk-based approach, members enacting FATF-compliant legislation and their financial intelligence units ('FIUs'), such as the Australian Transaction Reports and Analysis Centre ('AUSTRAC') in Australia, need to 'identify, assess and understand the … [money laundering] risks to which they are exposed and take … measures commensurate to those risks in order to mitigate them effectively'.[20] It is believed that an effective risk-based approach is fundamental to the effective implementation of the FATF recommendations.[21] In order to gain a better understanding of the risk-based approach to AML and what it entails, one must appreciate its history and context.

A *From Rule-Based to Risk-Based*

The risk-based approach was preceded by the rule-based approach to AML/CTF, which required reporting entities to report transactions to the relevant FIUs according to fixed parameters or specified thresholds.[22] Participants were treated equally, as rigid reliance on clear and transparent rules resulted in subjects being confronted with the same 'precise norms'.[23] However, with rigidity came predictability, as criminals were able to exploit the strict regulatory parameters by manipulating their transactions to avoid detection.[24] Additionally, the formal rule-based approach could result in over-reporting, leading to high compliance costs for the private sector and reduced investigative capacity for FIUs.[25] Accordingly, the adoption of a risk-based approach was aimed at addressing these formulaic shortcomings by allowing regulated entities to target their resources towards

17 Financial Action Task Force, *Report on the State of Effectiveness and Compliance with the FATF Standards* (Report, April 2022) 15.

18 The USA PATRIOT Act is officially titled the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001: Mark Pieth and Gemma Aiolfi, *Anti-Money Laundering: Levelling the Playing Field* (Basel Institute on Governance, 2003) 27 n 84.

19 Emmanuel Senanu Mekpor, Anthony Aboagye and Jonathan Welbeck, 'The Determinants of Anti-Money Laundering Compliance among the Financial Action Task Force (FATF) Member States' (2018) 26(3) *Journal of Financial Regulation and Compliance* 442, 444.

20 *The Banking Sector* (n 4) 6 [9].

21 Stuart Ross and Michelle Hannan, 'Money Laundering Regulation and Risk-Based Decision-Making' (2007) 10(1) *Journal of Money Laundering Control* 106, 106.

22 Mekpor, Aboagye and Welbeck (n 19) 444.

23 Brigitte Unger and Frans van Waarden, 'How to Dodge Drowning in Data? Rule- and Risk-Based Anti Money Laundering Policies Compared' (2009) 5(2) *Review of Law and Economics* 953, 957.

24 Ibid.

25 Ibid.

higher-risk areas specific to their geographic location, customer base and business model.[26]

Another reason for the shift away from the rule-based approach was its ineffectiveness with respect to money laundering and terrorist financing activities.[27] For example, with money laundering — in which the perpetrator's objective is to identify and exploit loopholes in the regulatory system — the very purpose of prescribing rules is defeated.[28] But, in a dynamic regulatory environment, the risk-based approach provides an avenue to link 'detection, prevention and control directly to the activities that are the focus of regulation'.[29] Under the risk-based approach, it is the responsibility of reporting entities to understand a customer's business relationship and to scrutinise transactions undertaken to ensure that they are consistent with the institution's knowledge of the customer, their business and their risk profile.[30] Thus, entities can no longer rely on established procedures for guidance on compliance with AML rules. Rather, they must 'understand how their business gives rise to risks and establish strategies and procedures for responding to those risks'.[31]

In effect, the risk-based approach transfers responsibility from regulatory institutions (which previously defined the rules and the models for rule-based and case-based systems, such as FIUs) to the entities themselves.[32] Under the risk-based approach, the reporting entity must define and specify the risks to be managed.[33] It should then implement the most appropriate strategies to address those risks.[34] Essentially, the change in the locus of regulation involves increased self-regulation from industries (comprised of reporting entities) and the 'adoption of private-sector styles of management and regulation'.[35] Reporting entities 'must now be pro-active agents in the mitigation of money laundering risk[s]'.[36] This represents a significant change in the distribution of regulatory responsibility and in the roles of the FATF, FIUs and other responsible AML agencies.[37]

26 Ibid; Lishan Ai and Jun Tang, 'Risk-Based Approach for Designing Enterprise-Wide AML Information System Solution' (2011) 18(3) *Journal of Financial Crime* 268, 271.

27 Ross and Hannan (n 21) 107.

28 Ibid.

29 Ibid 107–8.

30 See recommendation 10: *International Standards* (n 11) 14–15.

31 Ross and Hannan (n 21) 108.

32 Ibid.

33 Ibid.

34 Ibid.

35 Ibid.

36 Ibid.

37 Pieth and Aiolfi (n 18) 15.

The change from rules to risks as the focus of AML compliance represents a paradigmatic shift. The current risk-based approach has reduced the flow of reports and has also provided 'greater flexibility and sensitivity in responding to complex [money laundering issues]'.[38] The approach obliges not only banks and other financial institutions, but also designated non-financial businesses and professions ('DNFBPs') entities such as real estate agencies, legal professionals and accountants 'to document the transactions or activities they … [consider to be] *high risk* relating to their unique professions'.[39] These organisations, therefore, have an obligation to perform their own risk assessment according to their customer base, business model and geographic location, applying enhanced measures in high-risk situations and reduced measures in low-risk situations. Yet, that approach appears fundamentally inconsistent with the FATF's prescribed arbitrary characterisation of certain customers (such as politically exposed persons),[40] corporate structures (such as non-profit organisations)[41] and countries (such as Pakistan)[42] as high risk, resulting in several theoretical and practical issues for entities to consider if they wish to comply with the AML/CTF framework in their jurisdiction. Indeed, the risk-based approach is not a 'zero failure' approach and, as discussed in the following section, there may be occasions where regulators and institutions reach alternative conclusions as to the identification of money laundering risks.[43]

B *The Challenges of Risk Management*

Scholars have postulated that the main challenge associated with the risk-based approach to AML is the conceptualisation of risk and the lack of a standardised risk framework.[44] We will demonstrate that this understanding is not consistent with recent Australian experience. Rather, the challenges relate to poor risk oversight, behavioural biases and poorly designed incentives.

According to the international risk management standard, *ISO 31000: Risk Management* ('*ISO 31000*'), risk can be defined very simply as the 'effect of

38 Ross and Hannan (n 21) 107.

39 Mekpor, Aboagye and Welbeck (n 19) 444 (emphasis added). See especially recommendation 22 of the *International Standards* (n 11) 19–20. See generally Abdullahi Usman Bello and Jackie Harvey, 'From a Risk-Based to an Uncertainty-Based Approach to Anti-Money Laundering Compliance' (2016) 30(1) *Security Journal* 24, 25–6. As of June 2023, more than 200 jurisdictions have introduced new or amended regulatory regimes to cover DNFBPs, thus complying with the FATF standards. Australia is now one of only five nations — alongside China, Haiti, Madagascar and the US — that do not yet regulate DNFBPs as envisaged by the FATF: 'Consolidated Assessment Ratings', *FATF* (Web Page, 24 June 2024) <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html>.

40 See recommendation 12 of the *International Standards* (n 11) 16.

41 See recommendation 8 of ibid 13.

42 Ibid 19; Bello and Harvey (n 39) 30.

43 Firas Murrar, 'Adopting a Risk-Based Approach for Non-Profit Organisations' (2022) 25(1) *Journal of Money Laundering Control* 19, 20.

44 Bello and Harvey (n 39) 27–8.

uncertainty on objectives'.[45] Risk management can be defined as 'activities that direct and control an organisation in terms of risk, including the identification, analysis, treatment and monitoring of risk'.[46] The standard was first published in 2009 and was revised in 2018.[47] It is designed to cover all types of organisations and all types of risk,[48] including the risks associated with money laundering and terrorist financing. It includes a risk management framework, all of which suggests that AML risk management failures cannot be blamed on the lack of a risk management framework or conceptualisation of risk.

Risk governance and the risk management profession emerged in the late 20th century.[49] It can be seen as a response to an 'increasingly litigious and regulated society' and a growing understanding that humans are 'prone to … risk management [errors] … [due to] a range of biases and blind spots'.[50] Some of these biases — including overconfidence, short-termism and the availability heuristic — are seen as fundamental causes of many famous risk management catastrophes.[51] Examples range from the 1986 Space Shuttle Challenger disaster to the inadequate preparation of almost every organisation and government for a serious pandemic prior to 2020.[52]

The emergence of risk governance has seen the proliferation of numerous professional associations,[53] a flourishing consulting community, and a significant academic literature that crosses multiple disciplines, including actuarial science, accounting, finance, management and psychology. These days, it is common for listed companies to have a board subcommittee tasked with the oversight of risk.[54]

45 International Organization for Standardization, *ISO 31000: Risk Management* (Guidelines, 2018) 1 ('*ISO 31000*').

46 Elizabeth Sheedy, *Risk Governance: Biases, Blind Spots and Bonuses* (Routledge, 2021) 22.

47 Grant Purdy, 'ISO 31000:2009: Setting a New Standard for Risk Management' (2010) 30(6) *Risk Analysis* 881, 881; *ISO 31000* (n 45) 1.

48 International Organization for Standardization, *ISO 31000:2018 Risk Management: A Practical Guide* (Guide, 2021) 8.

49 G Neil Crockford, 'The Bibliography and History of Risk Management: Some Preliminary Observations' (1982) 7(2) *Geneva Papers on Risk and Insurance* 169, 174; Robert I Mehr and Bob A Hedges, *Risk Management in the Business Enterprise* (Richard D Irwin, 1963); Georges Dionne, 'Risk Management: History, Definition, and Critique' (2013) 16(2) *Risk Management and Insurance Review* 147, 149.

50 Sheedy (n 46) 4.

51 Michelle M Harner, 'Barriers to Effective Risk Management' (2010) 40(4) *Seton Hall Law Review* 1323, 1354–7; Emilios Avgouleas, 'The Global Financial Crisis, Behavioural Finance and Financial Regulation: In Search of a New Orthodoxy' (2009) 9(1) *Journal of Corporate Law Studies* 23, 33; Sheedy (n 46) 184.

52 Sheedy (n 46) 184.

53 Examples include the Institute of Risk Management, the Global Association of Risk Professionals, the Risk Management Association, the International Association of Risk and Compliance Professionals, and the Professional Risk Managers' International Association.

54 Ngoc Bich Tao and Marion Hutchinson, 'Corporate Governance and Risk Management: The Role of Risk Management and Compensation Committees' (2013) 9(1) *Journal of Contemporary Accounting and Economics* 83, 85.

Many organisations employ armies of risk professionals, reporting to a chief risk officer who sits on the most senior executive committee. In this context, the risk of money laundering or terrorist financing is but one of many risks — although it does have some particular challenges, as will be explained below. A risk professional would approach these challenges by initially assessing (a) the likelihood that the organisation could facilitate money laundering or terrorist financing and (b) the impacts of such an occurrence on the organisation.

A major impediment to risk reduction in the case of AML/CTF is that even though they have negative impact, some of the impacts are likely to be viewed as positive to the overall running of the organisation. In the case of a bank or casino, for example, transacting with criminals who wish to wash their dirty money can be very profitable in the short-term. Indeed, the process of money laundering does not, by itself, damage the commercial interests of the facilitating (either passively or consciously) organisation.[55]

The risk of harm posed to organisations is, rather, a product of the fact that facilitating money laundering is (a) harmful to the broader society and (b) prohibited and, accordingly, the accompanying reputational stigma of noncompliance. A risk professional would consider a range of negative impacts:

- **Regulatory fines** are a potential negative impact, depending on both the probability of being caught and the size of the fine. Regulators must establish a reputation on these two aspects in order to pose a credible threat. In addition to the fines themselves, firms often incur significant legal costs immediately following regulatory action.[56] The initial regulatory intervention can also lead to more intense regulatory scrutiny, which can increase the costs of the business. However, one of the problems with regulatory actions is that they are normally imposed on the organisation rather than on any individual executive or director, limiting their effectiveness due to a lack of individual accountability.
- **Stakeholder impacts** are increasingly considered by risk professionals, although organisations vary in the extent to which they consider stakeholders other than shareholders. Concern for a wider set of stakeholders is a relatively recent phenomenon associated with the corporate social responsibility ('CSR') movement.[57] Unfortunately, however, the adverse impacts of money laundering and terrorist financing are quite diffuse and are often felt by victims of crime and terrorism in other countries. The more diffuse the impact, the less likely that an organisation will take it into account. In many cases,

55 Antoinette Verhage, 'Between the Hammer and the Anvil? The Anti-Money Laundering-Complex and Its Interactions with the Compliance Industry' (2009) 52(1) *Crime, Law and Social Change* 9, 12.

56 See, eg, the $3.4 million in costs incurred in *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Crown Melbourne Ltd* (2023) 168 ACSR 420.

57 The following review of CSR focuses on the potential business justification for engaging in prosocial activities: Archie B Carroll and Kareem M Shabana, 'The Business Case for Corporate Social Responsibility: A Review of Concepts, Research and Practice' (2010) 12(1) *International Journal of Management Reviews* 85.

organisations may not fully appreciate the consequences of money laundering and terrorist financing.

- **Reputational costs** can be extremely important, but they are often not fully understood — even by professional risk managers. If it becomes known that an organisation has facilitated money laundering or terrorist financing, this can lead to a loss of customers, difficulty in recruiting and retaining talent, higher costs of debt and equity capital, increased insurance expenses and the loss of a licence to operate, to name a few.[58] Notably, all these impacts would have significant financial consequences, moderated, in part, by the size of the company and the virality of the breach.[59] These days, loss of reputation is made much easier by the prevalence of social media. Information about inadequate business practices can be leaked by employees or customers, even if regulators are ineffective. Society now tends to hold well-known businesses to a high ethical standard, with many investors eschewing organisations that are considered unethical or careless in their management of risks. Accordingly, major brands will invest heavily in risk management controls to prevent any highly publicised scandals likely to result in the forced departure of senior executives and directors, catastrophic loss in shareholder value and/or takeover by better-managed firms.

The risk management literature has highlighted many problems in the practice of risk management.[60] These problems include challenges due to the complexity of organisations, the existence of multiple risks, interactions between risks, the difficulty of quantifying risk, the relative invisibility of certain risks, the tendency for risk management to degenerate into a 'box-ticking' exercise and the propensity for risk managers and compliance officers to be ignored.[61]

At a fundamental level, firms typically fail at risk management because competing priorities prevail — especially short-term profits. In addition to the behavioural biases noted previously, remuneration structures may work against effective risk management, as the risk management function is, inherently, a cost centre and may be seen as detrimental to the economic performance of a company in times of financial uncertainty.[62] Commonly used incentive schemes are known to encourage an excessive focus by executives on short-term profits, and poor

58 Elizabeth Sheedy, Le Zhang and Kenny Chi Ho Tam, 'Incentives and Culture in Risk Compliance' (2019) 107 *Journal of Banking and Finance* 1.

59 Franco Fiordelisi, Maria-Gaia Soana and Paola Schwizer, 'The Determinants of Reputational Risk in the Banking Sector' (2013) 37(5) *Journal of Banking and Finance* 1359.

60 See, eg, René M Stulz, 'Risk-Taking and Risk Management by Banks' (2015) 27(1) *Journal of Applied Corporate Finance* 8; Anette Mikes and Robert S Kaplan, 'When One Size Doesn't Fit All: Evolving Directions in the Research and Practice of Enterprise Risk Management' (2015) 27(1) *Journal of Applied Corporate Finance* 37.

61 Elizabeth Sheedy and Dominic SB Canestrari-Soh, 'Does Executive Accountability Enhance Risk Management and Risk Culture?' (2023) 63(4) *Accounting and Finance* 4093, 4094.

62 Elizabeth Sheedy and Barbara Griffin, 'Risk Governance, Structures, Culture, and Behavior: A View from the Inside' (2018) 26(1) *Corporate Governance* 4, 5, 20.

compliance outcomes.[63] This is because good risk management practices tend to involve both higher costs and foregone revenues immediately, while the benefits of risk management are typically experienced over a much longer horizon or, in the case of a lack of regulatory action, not at all.[64] This dynamic was amply demonstrated during the global financial crisis of 2007–08. Bank CEOs with inappropriate incentives took excessive risks, in order to chase high short-term profits, with disastrous long-term consequences.[65]

Despite the existence of risk management policies and frameworks in many firms, organisational culture sometimes undermines their potency. Increasingly the literature is supporting the importance of a sound 'risk culture' for supporting effective risk management practices.[66] Indeed, an unfavourable risk culture may mean that the risk management frameworks are designed poorly, risk/compliance functions are poorly resourced, and the frameworks are therefore doomed to failure from the beginning. Risk culture is defined as the behavioural norms that either support or oppose risk management.[67] It is influenced by reward and consequence management systems, as well as the words and actions of leaders.[68]

All of these general risk management problems are potentially relevant to the case of AML/CTF risks. They are exacerbated by several factors, including the high cost of controls in this risk category, the significant profits that can be generated by taking AML/CTF risks, the diffuse nature of negative stakeholder impacts, the complexity and relative novelty of AML/CTF risks, the lack of a regulatory track record to provide a credible threat to business as usual and the use of new and emerging technologies to facilitate immediate cross-border transactions.

What about the role of directors in all this? Scholars of governance identify four fundamental board responsibilities that are crucial for risk management: formulating strategy and risk appetite, policymaking, supervising executive activities and providing accountability to shareholders and other relevant stakeholders.[69] A properly functioning board ought to provide adequate oversight, challenging the executive, as well as ensuring that risk systems and processes are established and adequately resourced. Directors have a role to play in hiring suitable senior executives and setting their remuneration. All these decisions are crucial elements in establishing a sound risk culture. The central role of the board

63 Sheedy, Zhang and Tam (n 58).

64 Sheedy and Canestrari-Soh (n 61).

65 Adam C Kolasinski and Nan Yang, 'Managerial Myopia and the Mortgage Meltdown' (2018) 128(3) *Journal of Financial Economics* 466.

66 Sheedy and Griffin (n 62).

67 Financial Stability Board, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture* (Report, 7 April 2014) 1 n 6 ('*FSB Guidance*'), quoting Institute of International Finance, *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System* (Report, December 2009) 31.

68 *FSB Guidance* (n 67).

69 Bob Tricker, *Corporate Governance: Principles, Policies and Practices* (Oxford University Press, 3rd ed, 2015) 46.

in risk governance is clearly espoused in corporate governance principles, especially those for financial institutions where risk management is most mature.[70] In the end, risk governance is unlikely to succeed without effective leadership from the board of directors.

The case studies we present in Part III(C) document a series of instances in Australia where there have been failures to effectively adopt or comply with AML/CTF risk measures. They exemplify the risk management challenges explained above.

III THE AUSTRALIAN REGIME

A *The Risk-Based Approach in Australia*

Australia, as a founding member of the FATF, follows a flexible rule- and risk-based approach to AML/CTF compliance in accordance with the FATF recommendations. The approach is reflected in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ('*AML/CTF Act*'), a complex piece of legislation. Parts 2, 3 and 3A of the Act impose rules and obligations on reporting entities to adopt specific identification procedures for their customers; to adhere to reporting requirements in relation to, for example, suspicious transactions; and to be listed on a 'Reporting Entities Roll'. However, relevantly, pt 7 requires that reporting entities have and comply with an AML/CTF program that is designed to identify, mitigate and manage the risk of money laundering and terrorism financing.[71]

The risk-based approach embodied in pt 7 of the Act was explained in the second reading speech for the Bill that became the *AML/CTF Act*:

> Consistent with the Government's commitment to reducing regulatory burdens on business, the legislative package implements a risk-based approach to regulation. Reporting entities will manage operational risks through AML/CTF programs developed in accordance with operational Rules. AUSTRAC will monitor compliance with these programs and will assess the reasonableness of the entity's risk assessment.
>
> The risk-based regulatory approach recognises that reporting entities have the experience and knowledge needed to assess and mitigate risk. It will also help mitigate compliance costs by providing industry with the tools to concentrate their resources on areas where money laundering and terrorism financing risk is higher. Industry has

70 See, eg, Basel Committee on Banking Supervision, *Corporate Governance Principles for Banks* (Guidelines, July 2015) 8; Australian Prudential Regulation Authority, *Prudential Practice Guide: CPG 220 Risk Management* (Report, April 2018) 8; Organisation for Economic Co-Operation and Development, *G20/OECD Principles of Corporate Governance* (OECD Publishing, 2015) 45; ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations* (Principles and Recommendations, February 2019) 6.

71 *Chief Executive Officer of Australian Transaction Reports and Analysis Centre v TAB Ltd [No 3]* [2017] FCA 1296, [4] (Perram J) ('*AUSTRAC v TAB [No 3]*').

> endorsed the risk-based approach. Australia's risk-based approach is similar to that taken in the United States and the United Kingdom.[72]

It is thus evident that the Parliament placed the concept of AML/CTF programs at the heart of the regulatory scheme, with AUSTRAC responsible for monitoring compliance. In a sense, the scheme involves entrusting industry, to a degree, with the operation of the AML/CTF risk management system. The *AML/CTF Act* 'deals severely with breaches of that trust'[73] through the issuance of enforceable undertakings, infringement notices, remedial directions and pecuniary penalties, to a maximum of 20,000 penalty units for individuals and 100,000 penalty units for bodies corporate per offence.[74]

Under the *AML/CTF Act*, a reporting entity is required to demonstrate to AUSTRAC how its AML/CTF program addresses the money laundering and terrorist financing ('ML/TF') risks that its business may reasonably face.[75] The entity's risk management policies, procedures and controls must be independently reviewed on a regular basis to ensure that they properly address the specific money laundering and terrorism financing risks that it faces and that they comply with legal obligations and are working efficiently.[76] The reviews must be conducted by someone — such as an auditor, lawyer, accountant or AML/CTF consultant — who understands the business or organisation, as well as the money laundering and terrorist financing risks involved, and was not involved in developing the program.[77] They are to be submitted to senior management, recognising the difficulty for any external body, such as AUSTRAC, to continually evaluate such programs.[78] However, even though the *AML/CTF Act* defines a 'reporting entity' as a provider of 'designated service[s]',[79] entities must determine for themselves whether they provide such services,[80] by taking into account the likely level of money laundering risk posed by their business, along with its size, nature and complexity.[81]

72 Commonwealth, *Parliamentary Debates*, Senate, 29 November 2006, 96 (Richard Colbeck).

73 *AUSTRAC v TAB [No 3]* (n 74) [3] (Perram J).

74 Ibid [4], discussing *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 175(4)–(5) ('*AML/CTF Act*'). At the time of writing (June 2023), the value of a penalty unit for a Commonwealth criminal offence is $275: *Crimes Act 1914* (Cth) s 4AA(1).

75 *AML/CTF Act* (n 74) s 47.

76 'Independent Reviews', *AUSTRAC* (Web Page, 15 January 2024) <https://www.austrac.gov.au/business/core-guidance/amlctf-programs/independent-reviews>.

77 Ibid.

78 Ibid.

79 *AML/CTF Act* (n 74) s 5 (definition of 'reporting entity').

80 Ibid s 6; 'Who and What We Regulate', *AUSTRAC* (Web Page, 17 January 2024) <www.austrac.gov.au/business/new-austrac-start-here/designated-services-what-we-regulate> ('Who AUSTRAC Regulates').

81 'AML/CTF Programs', *AUSTRAC* (Web Page, 15 January 2024) <www.austrac.gov.au/business/how-comply-guidance-and-resources/amlctf-programs/amlctf-programs-overview> ('AML/CTF Programs').

In the last few years, AUSTRAC has taken enforcement action against various reporting entities that have failed to comply with AML/CTF legislation. Such enforcement action can include civil penalty orders, enforceable undertakings, infringement notices and remedial directions. A common theme across most of these actions is a failure to comply with the risk-based approach to AML/CTF regulations.[82]

B *Risk in the Australian Money Laundering and Terrorist Financing Context*

AUSTRAC requires a reporting entity's AML/CTF program to show how it addresses ML/TF risks that the business may reasonably face. It requires that businesses develop and document policies, procedures and controls to identify, mitigate and manage such risks. Entities must determine for themselves whether they provide designated services,[83] by taking into account the likely level of money laundering and terrorist financing risks posed by their business, along with its size, nature and complexity.[84]

In Australia, an ML/TF risk has the meaning provided in r 1.2.1 of the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)* (Cth):

> *ML/TF risk* means the risk that a reporting entity may reasonably face that the provision by the reporting entity of designated services might (whether inadvertently or otherwise) involve or facilitate money laundering or the financing of terrorism.

This is consistent with the definition of risk in *ISO 31000*.[85]

C *AML/CTF Programs and the Consequences of Not Complying*

An AML/CTF program is a set of policies, procedures and controls that regulated entities must implement to detect and deter money laundering and terrorist financing.[86] The program must be based on a risk assessment made by the entity that considers the entity's customers and transactions and it must be tailored to the level of risk identified.[87] Each regulated entity is required to establish and maintain the AML/CTF program, review it regularly and update it in accordance with

82 See 'Lists of Enforcement Actions Taken', *AUSTRAC* (Web Page, 19 March 2024) <https://www.austrac.gov.au/lists-enforcement-actions-taken>.

83 *AML/CTF Act* (n 74) s 6; 'Who AUSTRAC Regulates' (n 80).

84 'AML/CTF Programs' (n 81).

85 *ISO 31000* (n 45) 1 [3].

86 *AML/CTF Act* (n 74) s 81.

87 Ibid pt 7.

changes in the entity's risk profile.[88] It is worth noting, however, that these requirements are entirely consistent with *ISO 31000* and corporate governance principles relating to the management of all risks.[89]

To meet its obligations under the *AML/CTF Act*, a reporting entity can adopt and maintain a 'standard program' for individual reporting entities,[90] a 'joint program' for members of a designated business group who choose this option for their AML/CTF program,[91] or a 'special program' for holders of an Australian financial services licence, such as financial planners who arrange designated services from other reporting entities for their clients.[92] The legal framework is outlined below.

Each AML/CTF 'program is divided into Part A (general) and Part B (customer identification)'.[93] There is a statutory requirement to comply with Part A; a failure to do so may result in a civil penalty.[94] Part A provides the framework through which boards and senior management assess their money laundering and terrorist financing risks, determine their risk appetite and decide which risk-based controls they will apply to mitigate and manage the risks they choose to accept. Once a reporting entity identifies the money laundering and terrorist financing risks it reasonably faces and carries out an assessment of those risks in accordance with an appropriate risk methodology, the entity must align its Part A program to those risks.[95] In doing so, the entity must have regard to the nature, size and complexity of its business, as well as the money laundering and terrorist financing risks related to its designated services and the customers, channels and foreign jurisdictions with which it deals.[96]

In recent years, AUSTRAC has applied for six penalty orders from the Federal Court of Australia:

Table 1: Analysis of Australian AML Cases

Case	The Role of Board and Senior Management: Key Findings

88 Ibid s 81.

89 See above Part II.

90 *AML/CTF Act* (n 74) s 84.

91 Ibid s 85. A designated business group consists of two or more reporting entities that join together to share the administration of some or all of their AML/CTF obligations (such as customer due diligence and record-keeping requirements). Any member of the group can fulfil some of the obligations for the other members. However, each reporting entity remains ultimately responsible for meeting its own AML/CTF obligations: at ss 5 (definition of 'designated business group'), 35F, 36, 47, 106–8, 112–13, 116.

92 Ibid s 86.

93 Ibid s 80.

94 Ibid s 82.

95 *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)* (Cth) pt 8.1 ('*AML/CTF Rules*').

96 Ibid.

2017: Tabcorp (gambling company)	'Indeed, the Respondents admitted that their AML/CTF function was not sufficiently resourced. *Senior management should have taken steps to inform themselves of this*. And, it need hardly be said, the deficiencies in the program remained in place for three years.'[97]
2018: Commonwealth Bank of Australia ('CBA') (bank)	'*[I]nadequate oversight and challenge by the Board* and its gatekeeper committees of emerging non-financial risks'.[98]
2019: Westpac (bank)	'Westpac contravened the Act on over 23 million occasions. These contraventions are the result of systemic failures in its control environment, *indifference by senior management and inadequate oversight by the Board*. They stemmed from Westpac's failure to properly resource the AML/CTF function, to invest in appropriate IT systems and automated solutions and to remediate known compliance issues in a timely manner. They have occurred because Westpac adopted an ad hoc approach to ML/TF risk management and compliance.'[99]
2022: Crown (gambling company)	'Crown Melbourne's and Crown Perth's non-compliance with ss 81, 84 and 85 of the Act was long-standing, systemic and reflective of *wholly inadequate oversight by their Boards and senior management*.'[100]
2022: Star Entertainment (gambling and entertainment company)	'Star Sydney's and Star Qld's non-compliance with ss 81 and 85 of the Act is long-standing, systemic and reflective of *wholly inadequate oversight by Board and senior management*.'[101] 'The directors accepted that there had been cultural failings at Star Entertainment. A number of directors also agreed that the Board must accept responsibility for these failings, or was accountable for them.'[102]

97 *AUSTRAC v TAB [No 3]* (n 74) [33] (Perram J) (emphasis added).

98 Australian Prudential Regulation Authority, *Prudential Inquiry into the Commonwealth Bank of Australia* (Final Report, April 2018) 3 (emphasis added) ('*APRA Final Report*').

99 Chief Executive Officer of the Australian Transaction Reports and Analysis Centre, 'Concise Statement', Submission in *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Westpac Banking Corporation*, NSD1914/2019, 20 November 2019, 2 [4] (emphasis added).

100 Chief Executive Officer of the Australian Transaction Reports and Analysis Centre, 'Concise Statement', Submission in *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Crown Melbourne Ltd*, NSD134/2022, 1 March 2022, 3 [12] (emphasis added) ('Concise Statement in *Crown*').

101 Chief Executive Officer of the Australian Transaction Reports and Analysis Centre, 'Concise Statement', Submission in *Chief Executive Officer of The Australian Transaction Reports and Analysis Centre v The Star Pty Ltd*, NSD1025/2022, 30 November 2022, 3 [11] (emphasis added).

102 Parliament of NSW, *Review of The Star Pty Ltd*: *Inquiry under Sections 143 and 143A of the Casino Control Act 1992 (NSW)* (Report, 31 August 2022) vol 3, 211 [116].

2022: SkyCity (gambling and entertainment company)	'SCA's non-compliance with ss 81 and 84 of the Act was long-standing, systemic and reflective of *inadequate oversight* by the SCEG Board or SCA *Board and senior management*.'[103]

1 *The Case of Tabcorp*

In March 2017, the Federal Court ordered Tabcorp to pay a penalty of $45 million for its failure to maintain a robust AML/CTF program.[104] This was the first major action brought for breaches of the *AML/CTF Act*. It was found that while Tabcorp had in place an AML/CTF program, it did not fully meet the requirements of the Act.[105] In other words, it was not that Tabcorp failed to comply with their program, but rather that their program fell short.

In this matter, it was found that

> Parts A and B of the … [AML/CTF] program were not … aligned with a risk assessment that comprehensively identified and evaluated the ML/TF risk posed to Tabcorp's business, and therefore they did not … have regard to the full extent of the ML/TF risks to which Tabcorp was exposed.[106]

Tabcorp also admitted that its 'written transaction monitoring program did not include appropriate risk-based systems and controls to consistently monitor the transactions of customers'.[107] Additionally, the program did not specifically require Tabcorp to apply Enhanced Customer Due Diligence ('ECDD') to customers in each case where necessary, and it failed 'to establish sufficient controls for consistently supporting the conduct of ECDD to ensure operational execution, monitoring and internal reporting':[108]

> Tabcorp's written Part B Program did not include appropriate risk-based systems and controls that were designed to enable Tabcorp to be reasonably satisfied that the customer was who they claimed to be in that it failed to include customer identification procedures for retail customers in certain circumstances. … [T]he deficiencies in their program had, in fact, resulted in failures on their part to detect certain suspicious transactions and to submit suspicious matter reports ('SMRs') to

103 Chief Executive Officer of the Australian Transaction Reports and Analysis Centre, 'Concise Statement', Submission in *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v SkyCity Adelaide Pty Ltd*, NSD1046/2022, 7 December 2022, 3 [11] (emphasis added) ('Concise Statement in *SkyCity*').

104 *AUSTRAC v TAB [No 3]* (n 74) [53] (Perram J); Australian Transaction Reports and Analysis Centre, 'Record $45 Million Civil Penalty Ordered against Tabcorp' (Media Release, 16 March 2017) ('Tabcorp Civil Penalty').

105 *AUSTRAC v TAB [No 3]* (n 74) [24] (Perram J).

106 Ibid [31].

107 Ibid.

108 Ibid.

> AUSTRAC. The failure to lodge these SMRs can … have the effect of depriving law enforcement agencies of important intelligence.[109]

Tabcorp had admitted it had 'insufficient processes for consistent management oversight, assurance and operational execution of the AML/CTF program':[110]

> Its AML/CTF function was under-resourced, and Tabcorp's Senior Management did not regularly receive reports in relation to AML/CTF compliance. … There can be no doubt there was a serious failure in corporate governance, and the size of the penalty reflects a significant, extensive and systemic non-compliance.[111]

It was the view of AUSTRAC CEO Paul Jevtovic APM that this non-compliance arose from a 'corporate culture indifferent to meaningful AML/CTF compliance and … mitigation [of ML/TF risk] until [AUSTRAC] intervened'.[112]

Tabcorp's deficient AML/CTF program indicates not only a lack of compliance culture but also a lack of comprehensive understanding of the money laundering or terrorist financing risks faced by Tabcorp. However, it is important to note that this lack of understanding is merely a symptom of the prevailing culture. If mitigating AML/CTF risks were a priority, understanding these risks should not be overly complex.

As part of the settlement, Tabcorp invested in its AML/CTF program,[113] and agreed to establish a new financial crime risk team to assist in monitoring and updated the AML/CTF approach by Tabcorp.[114]

2 *The Case of CBA*

In June 2018, the Federal Court ordered the CBA to pay a penalty of $700 million:[115]

> In May 2012, the Bank introduced Intelligent Deposit Machines … as a new channel for providing designated services. This was part of a process to refresh the Bank's automated teller machine … 'fleet'. An Intelligence Deposit Machine ('IDM') is a type of automated teller machine ('ATM') which can accept cash and cheque deposits into accounts with the bank. The funds can be deposited using either the Bank's

109 Ibid [31]–[32].

110 Ibid [33].

111 Australian Transaction Reports and Analysis Centre, 'CEO Statement: Tabcorp Matter' (Media Release, 16 March 2017).

112 'Tabcorp Civil Penalty' (n 104).

113 Ibid.

114 Patrick Durkin, 'Tabcorp Pays $45 Million over "Dirty Money" Claims', *Australian Financial Review* (online, 16 February 2017) <https://www.afr.com/companies/games-and-wagering/tabcorp-pays-45-million-over-dirty-money-claims-20170216-guecan>.

115 *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Ltd* [2018] FCA 930, [46] (Yates J) ('*AUSTRAC v Commonwealth Bank*').

> branded card or the card of another financial institution. Unlike other ATMs, cash deposited through an IDM is automatically counted and instantly credited to the nominated beneficiary's account with the Bank. The funds are then immediately available for transfer, including internationally. In May 2012, when the Bank's first five IDMs were rolled out, cash deposits through the machines totalled $868,825 for the month. In May 2017, at a time when the Bank had rolled out 805 IDMs, cash deposits for the month totalled approximately $1.7 billion.[116]

It was found that CBA failed

> to carry out appropriate customer due diligence … to provide suspicious matter reporting in a timely manner or at all[117] … to comply with its own transaction monitoring program … to provide threshold transaction reporting to AUSTRAC in a timely manner; and … to undertake risk assessments and introduce sufficient and appropriate risk-based controls in relation to the money laundering and terrorism financing risks posed by the operation of its IDMs.
>
> …
>
> The Bank was also obliged to report that it had information concerning the provision, or prospective provision, of a designated service that may be relevant to the investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a State or Territory.[118]

CBA admitted to failing 'to undertake risk assessment[s] and introduc[ing] sufficient and appropriate risk-based controls in respect of its IDMs'.[119]

In an AUSTRAC media release, CEO Nicole Rose stated:

> It is the responsibility of financial institutions, their boards and senior management to ensure the organisation they oversee takes its AML/CTF obligations seriously, and that there is an organisational culture that supports this.[120]

3 *The Case of Westpac*

Most notably, in 2019, AUSTRAC initiated legal proceedings against Westpac over allegations that the bank had breached the *AML/CTF Act* on more than 23 million occasions, for widespread compliance failures across multiple businesses,

116 Ibid [3].

117 Ibid [4]. Section 41(2)(a) of the *AML/CTF Act* (n 74) imposes an obligation on a reporting entity to provide, within limited timeframes, a report to AUSTRAC of suspicious matters:

> The Bank was obliged to submit a suspicious matter report within three business days of forming a suspicion, on reasonable grounds, that a person to whom it commenced, or proposed, to provide a designated service was not the person he, she or it claimed to be.

AUSTRAC v Commonwealth Bank (n 115) [9] (Yates J).

118 *AUSTRAC v Commonwealth Bank* (n 115) [4], [9] (Yates J).

119 Ibid [41].

120 Australian Transaction Reports and Analysis Centre, 'CEO Statement: CBA Matter' (Media Release, 4 June 2018).

including Westpac's banking, superannuation, wealth management and insurance brands.[121] Westpac agreed to pay a penalty of $1.3 billion to settle the legal action.[122] The size of the penalty reflects the seriousness of the breaches, sending a strong message to reporting entities about the importance of compliance with a risk-based approach. At the time, it was the largest fine ever imposed in Australian corporate history.[123]

Given the magnitude of this risk management failure, the Australian Prudential Regulation Authority ('APRA') required Westpac to conduct an additional self-assessment of its culture, governance and accountability frameworks and practices.[124] The resultant report, published in June 2020, identified serious shortcomings including an 'immature and reactive risk culture in non-financial risk management' and a need to refocus board and executive oversight.[125]

4 *The Case of Crown*

On 1 March 2022, AUSTRAC had applied for civil penalty orders against Crown Melbourne and Crown Perth for their failure to adopt an AML/CTF program that met the legal requirements. AUSTRAC alleged the following:

> In the face of known and serious ML/TF risks, the Board and senior management of Crown Melbourne and Crown Perth failed to set any ML/TF risk appetite through the Standard Part A Programs. They failed to adopt and maintain controls to ensure that designated services were provided within an appropriate risk appetite. They failed to adopt controls to mitigate and manage the full range of ML/TF risks across all designated services — both gaming and financial.[126]

The evidence submitted established numerous corporate failings, including 'that [the] Crown's risk management and corporate governance structures were compromised', that 'Crown's directors were not informed of very significant matters of which they should have been informed', and that Crown realised there was a risk 'of exploitation by criminals utilising Crown's bank accounts for money

121 *Chief Executive Officer of Australian Transaction Reports and Analysis Centre v Westpac Banking Corporation* (2020) 148 ACSR 247, 255 [55] (Beach J). The bank suffered other repercussions, including severe reputational damage and the consequent loss of shareholder value: in the year following the AUSTRAC statement of claim in November 2019, the bank lost around 27% of its shareholder value (beyond what can be explained by other market factors), equivalent to nearly $16 billion — more than 12 times the fine amount. The Cumulative Abnormal Return analysis conducted in our research paper is available with the authors who would be happy to share upon request.

122 Ibid 248 [1].

123 Peter Ryan, Michael Janda and Matthew Doran, 'Westpac Settles AUSTRAC Money Laundering Case with $1.3 Billion Fine', *ABC News* (online, 24 September 2020) <www.abc.net.au/news/2020-09-24/westpac-settles-austrac-money-laundering-case/12696438>.

124 Westpac Group, *Reassessment of the Culture, Governance and Accountability Remediation Plan* (Report, June 2020) 4.

125 Ibid 6, 7.

126 'Concise Statement in *Crown*' (n 100) 5 [21].

laundering purposes which was not properly appreciated or prevented'.[127] In fact, the Chair of the Crown, Ms Coonan, acknowledged that the Board was not always receiving 'all … the information and inputs it required', and that the 'Crown's systems, processes and structures in place in relation to risk and compliance "require[d] further enhancement"'.[128] She made these comments in respect of the Crown's AML/CTF capability — noting the need for 'increased training[,] automation, resourcing and reporting'.[129] Nevertheless, Ms Coonan agreed that 'it is unsatisfactory for boards of Australian publicly listed companies to simply say they were not informed of important matters' and 'boards of listed companies have an obligation to constructively challenge management and ask the hard questions'.[130]

Interestingly, in the 2021 Crown Casino Inquiry, when questions were asked about possible money laundering activity in the Crown, AUSTRAC found that Crown executives resorted to a high-level response that its AML/CTF policy had been judged effective by its retained expert, and there was clearly a disconnect between AML/CTF oversight at Crown and senior management of the company.[131] During the public hearings, it was unveiled that Crown had 'totally inadequate' understandings of AML/CTF matters considered essential to their operation.[132] It seems the undertaking of a risk-based approach was deemed a delegable task, rather than a vital requirement which necessitated collaboration between various stakeholders for the purposes of sharing insights on business operations and ML/TF risks.

5 *The Case of Star Entities*

On 30 November 2022, AUSTRAC commenced proceedings in the Federal Court against The Star Pty Ltd and The Star Entertainment Qld Ltd ('the Star entities') following an investigation that 'identified a multitude of issues including poor governance', risk management failure, and failure 'to have and maintain a compliant AML/CTF program':[133]

> Once a reporting entity identifies and assesses its inherent ML/TF risks and the Board determines ML/TF risk appetite, the reporting entity must ensure that its Part A program includes appropriate risk-based systems and controls to mitigate and manage residual risks within appetite.

127 Independent Liquor and Gaming Authority, Parliament of New South Wales, *Inquiry under Section 143 of the Casino Control Act 1992 (NSW)* (Report, 1 February 2021) vol 2, 347 ('*ILGA Report*').

128 Ibid 350.

129 Ibid 352.

130 Ibid 350.

131 *ILGA Report* (n 127) 629 [69].

132 Ibid 538.

133 Australian Transaction Reports and Analysis Centre, 'AUSTRAC Commences Proceedings in the Federal Court against Star Entertainment Group Entities' (Media Release, 30 November 2022).

> These systems and controls must be aligned with, and proportionate to, the ML/TF risks reasonably faced by the reporting entity with respect to designated services.
>
> In the absence of appropriate ML/TF risk assessments, Star Sydney's and Star Qld's Joint Part A Programs were incapable by design of including appropriate risk-based systems and controls to mitigate and manage the ML/TF risks.[134]

AUSTRAC found that

> [t]he Joint Part A Programs had few preventative controls designed to enable Star Sydney and Star Qld to mitigate and manage its ML/TF risks in respect of these designated services. The Part A controls were predominantly detective and limited to staff observation and surveillance for unusual activity that may require SMR reporting to AUSTRAC. The Part A controls were predominantly focussed on gaming services. Higher risk financial services, that permitted money to be moved into and out of the casinos, including across international borders, were not subject to appropriate risk-based controls.[135]

Furthermore:

> Star Sydney and Star Qld each failed to include an appropriate risk-based transaction monitoring program in their Joint Part A Programs to monitor the transactions of their customers and to identify suspicious matters, as required by … the [*AML/CTF Act*].[136]

The Star entities also failed to 'include appropriate systems, controls and procedures to apply appropriate risk-based ECDD to [high-risk] customers', 'foreign politically exposed persons' and customers who were 'the subject of a suspicion … for the purposes of s 41 of the Act':[137]

> Star Sydney's and Star Qld's Joint Part A Programs did not include appropriate systems and controls designed to ensure compliance with their obligation to report SMRs, TTRs [threshold transaction reports] and IFTIs [international funds transfer instructions] to AUSTRAC.[138]

Moreover, it is alleged that

> the Joint Part B Programs did not include appropriate risk-based systems and controls that were designed to enable Star Sydney and Star Qld to be reasonably satisfied,

134 Chief Executive Officer of the Australian Transaction Reports and Analysis Centre, 'Concise Statement', Submission in *Chief Executive Officer of The Australian Transaction Reports and Analysis Centre v The Star Pty Limited*, NSD1025/2022, 30 November 2022, 6 [25]–[27] ('Concise Statement in *The Star*').

135 Ibid 6–7 [29].

136 Ibid 7 [30]. See also *AML/CTF Rules* (n 95) ch 15, r 9.1.3; *AML/CTF Act* (n 74) s 85(2)(c).

137 'Concise Statement in *The Star*' (n 134) 7 [31].

138 Ibid 8 [33]; *AML/CTF Act* (n 74) ss 41, 43, 45, as required by r 9.9.1(2) of the *AML/CTF Rules* (n 95) and s 85(2)(c) of the *AML/CTF Act* (n 74).

> where the customer was an individual, that the customer was the individual they claimed to be …[139]

The Star casinos 'failed to carry out appropriate due diligence on their customers, with a view to identifying, mitigating and managing known ML/TF risks on 1,514 occasions contrary to … the [*AML/CTF Act*]'.[140]

Overall, the 'Board and senior management failed to adopt and maintain Programs to control those ML/TF risks appropriately'.[141] It is alleged the Star casinos

> chose to … [prioritise] their customers' desire for privacy over AML/CTF compliance, including in cases where … [the casinos] were aware customers had raised red flags.
>
> …
>
> The [Star] casinos accordingly facilitated the provision of designated services in the billions of dollars in the absence of appropriate ML/TF controls.[142]

By failing to comply with the Act, the Star entities avoided allocating appropriate resources to compliance — including 'IT, staffing and the development of AML/CTF controls'.[143]

6 *The Case of SkyCity*

On 7 December 2022, AUSTRAC applied for civil penalty orders against SkyCity Adelaide Pty Ltd 'for alleged serious and systemic non-compliance' with Australia's AML/CTF laws.[144] SkyCity was targeted for, among other issues, its failure to develop and maintain a compliant AML/CTF program, placing it at risk of criminal exploitation.[145] In a media release on the same day, AUSTRAC's Deputy CEO emphasised that the 'requirement for regulated entities to have appropriate AML/CTF controls and systems in place is not optional and should be taken seriously by all businesses regulated by AUSTRAC'.[146]

It was alleged that SkyCity contravened the *AML/CTF Act* because Part A of its AML/CTF program 'was not a program that … had the primary purpose of identifying, mitigating and managing the risk that … [SkyCity] may reasonably face' and because SkyCity did not provide 'an appropriate risk methodology that

139 'Concise Statement in *The Star*' (n 134) 9–10 [39].

140 Ibid 10 [42].

141 Ibid 13 [59].

142 Ibid 15 [63], 13 [59].

143 Ibid 16 [67].

144 Australian Transaction Reports and Analysis Centre, 'AUSTRAC Commences Federal Court Proceedings against SkyCity Adelaide' (Media Release, 7 December 2022) ('SkyCity Media Release').

145 'Concise Statement in *SkyCity*' (n 103) 5 [23]–[25].

146 'SkyCity Media Release' (n 144).

was capable of identifying and assessing the ML/TF risks of its designated services, as required by ss 84(2)(a) and (c)' of the *AML/CTF Act*.[147]

Noting that casinos operate in dynamic ML/TF risk environments, AUSTRAC found that at no time did SkyCity's Part A Programs 'include appropriate risk-based systems and controls to identify significant changes in ML/TF risks and to recognise such changes for the purposes of the Part A and Part B Programs'.[148]

AUSTRAC alleged that:

> [i]n the face of known and serious ML/TF risks, the … Board and senior management failed to set the ML/TF risk appetite through the Part A Programs. They failed to adopt and maintain controls to ensure that designated services were provided within an appropriate ML/TF risk appetite.[149]

They also 'failed to adopt controls to mitigate and manage the full range of ML/TF risks across all designated services — both gambling and financial'.[150] Without appropriate risk-based controls and assessments,

> [t]hese failures in oversight resulted in serious and systemic non-compliance with the Act over many years. These failures [ultimately] allowed high risk customers to move money in non-transparent ways with minimal due diligence on ML/TF risks.[151]

7 *Overview: Considering the Cases*

The risk-based approach to AML/CTF is a cornerstone of the *AML/CTF Act* and, on the face of it, the underlying cause of most breaches of law. However, through a review of the Federal Court's recent civil penalty orders, it is abundantly clear that failures of leadership played a crucial role in all six of the AML cases examined. This is consistent with our understanding of risk governance more generally, and risk-based approached management failures across all risk types.

The CBA case is particularly interesting because the AML scandal was one of multiple scandals that emerged at the bank in the 2010s, leading ultimately to a far-reaching prudential inquiry by the APRA, suggesting that AML deficiencies typically occur amidst a culture of dereliction of one's corporate regulatory

147 Chief Executive Officer of the Australian Transaction Reports and Analysis Centre, 'Originating Application', Submission in *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v SkyCity Adelaide Pty Ltd*, NSD1046/2022, 7 December 2022, 2 [1].

148 'Concise Statement in *SkyCity*' (n 103) 2 [18]. Once a reporting entity identifies the ML/TF risks it reasonably faces and carries out an assessment of those risks in accordance with an appropriate ML/TF risk methodology, the reporting entity must align its Part A program to those risks as assessed. In aligning a Part A program to the ML/TF risks reasonably faced, a reporting entity must have regard to the nature, size and complexity of its business, and the ML/TF risks related to their designated services, customers, channels and the foreign jurisdictions with which they deal: see *AML/CTF Rules* (n 95) rr 8.1.4, 8.1.5(3)–(4).

149 'Concise Statement in *SkyCity*' (n 103) 5 [22].

150 Ibid.

151 Ibid 5 [25].

responsibilities. APRA's final report from the inquiry thoroughly documents the governance, accountability and cultural problems that caused the risk management failures.[152] The board of directors must take ultimate responsibility for these matters.

AML and other risk management failures generally occur because the organisational culture focuses on priorities apart from risk management. Overconfidence, short-termism and remuneration systems are all barriers to establishing a sound risk culture. As a consequence, risk management systems and functions are under-resourced, poor compliance and risk management behaviour is rarely sanctioned and red flags are ignored. In such an environment, non-compliance with risk-based approaches is almost inevitable. Ultimately the 'risk' in the risk-based approach is that risk governance is difficult to do well, especially in the absence of an effective board of directors and senior management.

Furthermore, these cases highlight that despite the mandate of taking a risk-based approach to AML/CTF, it is necessary for regulated entities to develop and embed a sound risk culture across all levels of staff, including senior executives and Boards who may not understand or appreciate the significance of the consequences of non-compliance. Without a sound risk culture, it is evidently convenient and simple for senior management to accept the recommendations of other staff without making further enquiries about the robustness of the company's AML/CTF program — despite, ironically — having the deepest understanding of how the business operates.

One of the primary concerns about the risk-based approach, as highlighted through the aforementioned case studies, is that there is potential for misjudgement and underestimation of risk in the absence of a strongly embedded risk culture.

There are evidently risks to the risk-based approach. The ability to develop adequate risk-based AML programs has an impact on the exposure of regulated entities to penalties. It is worth noting that civil penalties can have severe reputational and financial consequences for reporting entities that fail to comply with the AML/CTF laws and regulations.

IV RECOMMENDATIONS

The interpretive notes to the FATF's Recommendation 1 state:

> The risk-based approach … is an effective way to combat money laundering and terrorist financing. In determining how the [approach] should be implemented in a [particular] sector, countries should consider the capacity and [AML/CTF] experience of [that] … sector. Countries should understand that the discretion afforded, and [the] responsibility imposed on, financial institutions and [DNFBPs] by the [risk-based approach] is more appropriate in sectors with greater AML/CTF capacity and experience. This should not exempt financial institutions and DNFBPs from the

152 See generally *APRA Final Report* (n 98).

> requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs [can] ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified … [This will] enable them to make decisions on how to allocate their own resources in the most effective way [possible].[153]

It is also suggested to consider the following to improve compliance and mitigate money laundering and terrorist financing risks.

A *Sector-Specific in Australia*

The *AML/CTF Act* does not discuss how the risk-based approach should be implemented in a specific sector. Notably, AUSTRAC's industry-specific guidance for AML/CTF programs comprises regulatory guides and financial crime guides on various topics, guidance videos and sector-wide risk assessments.[154] Taking the banking sector as an example, AUSTRAC has published financial crime guides on numerous topics;[155] however, there is no single complete and comprehensive guide.

A lack of consensus on a standardised definition of risk has resulted in challenges. Specifically, employees occupying risk and compliance roles often lack adequate training, and employers may not allocate sufficient resources towards tailored education for their staff. Consequently, there exists a notable absence of a shared understanding among various stakeholders regarding the nuanced meanings attributed to different types of risks. A problem that is exacerbated in the cross-border context is that '[i]nstitutions within the same country and [even] individuals within the same institution[s] [might] use different risk languages in the sense that they mean different things even when they use the same words'.[156] An analysis of conceptualisations of risk in financial institutions and legal departments operating within a similar risk-controlling environment demonstrates a firm understanding of the positive relationship between risk and return.[157] The problem lies in identifying suspicious transactions without creating a glut of false positives. Organisations are given little feedback about which transactions prove to be problematic, meaning that they are unable to refine their models, and leading to a lack of independent accurate data amenable to quantitative analysis. Whilst

153 *International Standards* (n 11) 31.

154 'Your Industry', *Australian Transaction Reports and Analysis Centre* (Web Page, 26 June 2023) <https://www.austrac.gov.au/business/your-industry>; Australian Transaction Reports and Analysis Centre, *Key Findings Overview: Australian Banking Sector Money Laundering and Terrorism Financing Risk Assessment*s (Report, 2021).

155 See, eg, Australian Transaction Reports and Analysis Centre, *Preventing the Criminal Abuse of Digital Currencies* (Financial Crime Guide, April 2022); Australian Transaction Reports and Analysis Centre, *Preventing Trade-Based Money Laundering in Australia* (Financial Crime Guide, October 2022); Australian Transaction Reports and Analysis Centre, 'Combating the Sexual Exploitation of Children for Financial Gain' (Financial Crime Guide, December 2022).

156 Simonova (n 1) 349–50.

157 Bello and Harvey (n 39) 28.

researchers have presented various models and methodologies of estimating money laundering risks and identifying abnormal transaction behaviour capable of reducing the number of false positives,[158] significant limitations exist globally in regard to a lack of sector-specific data availability which could benefit from the publication of confirmed cases of money laundering activity.

While the FATF has promulgated a regime whereby higher levels of 'suspicion' correlate with higher levels of risk, the recommendations and accompanying guidance fall short of providing a standardised framework for accurately and consistently identifying a transaction or customer as suspicious. Indeed, as recognised by Mitsilegas, criminal activities are virtually indistinguishable from legitimate financial transactions.[159] Accordingly, the lack of clear criteria to distinguish between high and low risk inhibits the effective implementation of a risk-based approach in AML regulation.

B *Standardisation of Risk*

While it is not within the scope of this paper to propose methods of risk standardisation, organisations are in dire need of guidance on the indicators that might be suggestive of criminal responsibility. The use of risk-based regulation involves some risks for both regulators and regulated entities. Allowing some discretion to the subjects being regulated poses the risk of inadequate or inconsistent detection, assessment and reporting, leading to insufficient, irrelevant or excessive information for FIUs — such as AUSTRAC in Australia.[160] The absence of clear rules may result in legal uncertainty. Similar businesses may adopt varying reporting strategies, leading to ambiguous outcomes. While risk-based regulation is intended to reduce administrative burdens and enhance effectiveness, it may also incentivise businesses to over-report suspicious activities to avoid sanctions, thereby flooding government agencies with excessive data that fails to pinpoint potential money laundering activities.[161] We suggest incorporating some degree of standardisation across each regulated industry.[162]

158 See Doron Goldbarsht, 'Leveraging AI to Mitigate Money Laundering Risks in the Banking System' in Zofia Bednarz and Monika Zalnieriute (eds), *Money, Power, and AI: Automated Banks and Automated States* (Cambridge University Press, 2023) 51, 57, 69; Joras Ferwerda and Edward R Kleemans, 'Estimating Money Laundering Risks: An Application to Business Sectors in the Netherlands' (2019) 25(1) *European Journal on Criminal Policy and Research* 45; José-de-Jesús Rocha-Salazar, María-Jesús Segovia-Vargas and María-del-Mar Camacho-Miñano, 'Money Laundering and Terrorism Financing Detection Using Neural Networks and an Abnormality Indicator' (2021) 169 *Expert Systems with Applications* 1.

159 Valsamis Mitsilegas, 'Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance versus Fundamental Legal Principles' (PhD Thesis, University of Edinburgh, 2000) 56.

160 Unger and van Waarden (n 23) 960.

161 Ibid 226–7. It is possible that this problem may be alleviated to some extent through advances in artificial intelligence, but this is not a solution in itself: see generally Doron Goldbarsht, 'Artificial Intelligence and Financial Integrity: The Case of Anti-Money Laundering' (2022) 33(1) *Journal of Banking and Finance Law and Practice* 21.

162 Unger and van Waarden (n 23) 960.

Having standards and guidance in the risk-based approach for AML facilitates international cooperation and information-sharing among institutions and regulators in several ways:

- **Common language:** standards provide a common language and framework for AML efforts, enabling institutions and regulators to communicate effectively and efficiently across different jurisdictions.[163]
- **Consistent approach:** standards ensure that institutions and regulators adopt a consistent approach in identifying, assessing and mitigating the risks of money laundering and terrorist financing activities, regardless of their location or industry.
- **Mutual recognition:** institutions and regulators in different jurisdictions are more likely to recognise and accept each other's AML efforts if they are based on common standards. This mutual recognition promotes international cooperation and reduces duplication of efforts.
- **Information-sharing:** standards provide a basis for sharing information and best practices among institutions and regulators. This information sharing can help identify and disrupt criminal networks and activities, assisting in the investigation and prosecution of money laundering and terrorist financing offences.
- **Capacity-building:** standards can assist institutions and regulators in developing their AML capacities and capabilities, particularly in countries where AML frameworks may be less developed. This capacity-building can improve the effectiveness of AML efforts and promote greater international cooperation in combating money laundering and terrorist financing activities.

Thus, standardisation in the risk-based approach to AML can play a crucial role in combating money laundering and terrorist financing activities both domestically and transnationally.

Accordingly, there appears scope for amendment to be made to the *AML/CTF Act* to incorporate an industry-wide standard definition of risk alongside publication of a series of comprehensive industry-specific guides by AUSTRAC defining certain common terms, addressing how such concepts ought to be applied by individual stakeholders (eg providing comprehensive guidance as to the application of 'risk' across the real estate industry), and identifying specific high-risk products, services and circumstances which ought to be treated with enhanced precaution. The inclusion of sector-specific information, such as the proportion of false-positive or false-negative SMRs received by AUSTRAC in relation to specific circumstances, would allow institutions to update their risk-assessments in response to accurate data, obviating a limitation identified above. Such guidance, whilst non-

163 For a variety of reasons, *ISO 31000* (n 45) is not a suitable risk management standard for all entities. First, it is a general standard that can be applied to any organisation or industry, while some organisations may prefer to use industry-specific standards or frameworks that meet their specific needs. Second, implementing *ISO 31000* can require significant time, effort and resources that may be beyond the reach of some organisations, leading them to adopt simpler risk management approaches. Third, some organisations have well-established risk management practices that are effective for their needs and may not see the need to adopt a new standard. Finally, some organisations may find *ISO 31000* too complex or difficult to implement.

prescriptive, would provide a mechanism by which a sector-wide common understanding of the application of the risk-based approach is facilitated, whilst continuing to oblige individual institutions to determine their own AML/CTF program in accordance with their specific risk profile.

C *Shift in Directors' and Senior Management's Liability*

Directors must exercise and discharge their powers in relation to a corporation with a degree of care, skill and diligence. Section 180(1) of the *Corporations Act 2001* (Cth) provides for this duty by asserting that such care and diligence exercised in accordance with the powers of a director is to be tempered by the expectations of a *reasonable person* if they were a director or officer of the corporation and sustained equivalent responsibilities.[164] At common law, the duty of care, skill and diligence is comparably similar to that expressed in the equivalent statutory provision of s 180(1), where the common law provides guidance to the practical application of the duty in connection with the exercise of director powers. Notably, *AWA Ltd v Daniels* and cases following both in the appellate jurisdiction of the courts and in recent case law have laid the foundational requirement that the s 180 duty is objective and requires directors to 'take reasonable steps to place themselves in a position to guide and monitor the … company'.[165]

In order to bolster financial integrity and address illicit financial practices, it is imperative for regulatory entities to contemplate the augmentation of directors' obligations in ensuring the efficacy of AML/CTF measures within their respective organisations. Legislative reform, including through the introduction of the Banking Executive Accountability Regime,[166] has the potential to expose influential senior directors and executives to civil penalties, disqualification and the loss of deferred remuneration. There has also been a dramatic rise in the indirect consequences of enforcement action, including significant director accountability in order to placate shareholder activism — for example, the resignation of Star Entertainment Group CEO Matt Bekier in March 2022, after the launch of an investigation by AUSTRAC in June 2021; the resignation of the Crown Resorts CEO Ken Barton and several other company directors in February 2021, amid an AUSTRAC investigation; and the stepping down of Commonwealth Bank CEO Ian Narev in July 2018, and Westpac CEO Brian Hartzer in November 2019, in

164 *Corporations Act 2001* (Cth) s 180(1)(a)–(b). In *Vines v Australian Securities and Investments Commission* (2007) 73 NSWLR 451, 461 [72] (Spigelman CJ) (emphasis omitted), the New South Wales Court of Appeal upheld the first instance findings of Austin J, quoting *Australian Securities and Investments Commission v Vines* (2005) 55 ACSR 617, 860 [1075]:

> The … standard [of a reasonable person] set by [the legislation] establishes an inquiry as to the … care and diligence that a reasonable person 'would exercise', not what the reasonable person might do … similar in concept to the standard that applies to professional negligence cases.

165 (1992) 7 ACSR 759, 864 (Rogers CJ); *Vrisakis v Australian Securities Commission* (1993) 9 WAR 395, 451 (Ipp J); *Daniels v Anderson* (1995) 37 NSWLR 438, 501 (Clarke and Sheller JJA); *Termite Resources NL (in liq) v Meadows [No 2]* (2019) 370 ALR 191, 226 [101] (White J).

166 *Treasury Laws Amendment (Banking Executive Accountability and Related Measures) Act 2018* (Cth).

response to the commencement of civil penalty proceedings by AUSTRAC. Amending the regulatory framework to transition directors' responsibilities from a mere duty of care to a more robust duty of oversight[167] may effectively mitigate the risks associated with non-compliance and uphold the integrity of the legal regime.[168] This can be achieved by imposing potential consequences for directors who fail to meet their AML/CTF obligations, encompassing civil and criminal penalties, reputational harm and personal liability.

The rationale behind this approach lies in the recognition that directors, as key decision-makers within organisations, play a pivotal role in shaping and maintaining effective AML/CTF systems. By holding them accountable for the oversight and monitoring of these systems, governments and regulatory bodies can incentivise directors to actively engage in the risk assessment, due diligence and implementation of appropriate controls to detect and prevent money laundering and terrorist financing activities. This shift in responsibilities serves as a proactive measure to strengthen the overall compliance posture and foster a culture of heightened awareness and diligence. The imposition of civil and criminal penalties, along with the potential for reputational damage and personal liability, serves as a deterrent for directors who may otherwise neglect or disregard their AML/CTF obligations. This approach might help to mitigate the risk of *inadequate oversight by the board*.

V CONCLUSION

The shift from a rule-based approach to a risk-based approach means that the determination of suspicious behaviour is no longer the sole responsibility of the government. Instead, many different actors in the financial services sector play a role. This results in a range of differing definitions and concepts of 'risk' and 'suspicious transactions', increasing uncertainty for all parties involved. This uncertainty may encourage entities to err on the side of caution by over-reporting transactions that may seem suspicious. While some degree of standardisation within the risk discourse may be beneficial in providing clarity on the meaning and interpretation of risk across various industries, this must be approached with caution to ensure that entities do not revert to rule-based regulation.

This paper has examined how the concept of risk operates within Australia's AML/CTF regulatory framework. While demonstrating global compliance with

167 However, it is important to recognise that shifting liabilities and imposing increased responsibilities on directors in relation to AML/CTF measures may also give rise to certain challenges and risks. These challenges encompass a range of potential negative outcomes, including increased economic and social costs, a heightened risk of stifling innovation and impeding economic growth, inefficient allocation of resources, negative impacts on customer relationships and potential hindrance to international competitiveness: see Christina Parajon Skinner, 'Executive Liability for Anti-Money-Laundering Controls' (2016) 116(1) *Columbia Law Review* 1, 6–13; Muhammad Saleem Korejo, Ramalinggam Rajamanickam and Muhamad Helmi Md Said, 'Financial Institutions and Anti-Money Laundering Violations: Who Is to Bear the Burden of Liability?' (2022) 25(3) *Journal of Money Laundering Control* 671.

168 Korejo, Rajamanickam and Said (n 167) 677.

the international regime promulgated by the FATF, the paper has illustrated the limitations inherent in placing responsibility for conceptualising risk with individual entities, as a lack of uniformity has resulted in inconsistency. Indeed, in light of the several case studies identified above, it is clear that Australia must rethink the application of a risk-based approach in the context of risk-oriented AML procedures. Clearly, multiple failures of leadership amongst several high-risk industries underscores a culture of neglect towards AML/CTF across the Australian corporate ecosystem and illustrates the consequences of a lack of a standardised definition of risk. Despite stopping short of proposing a method of risk standardisation across industries, the paper has illustrated the risks of failing to do so and has provided a framework for future research to investigate methods of improving compliance with the risk in the FATF's risk-based approach.