Age of Acceleration

Staying at the forefront of change in an evolving legal landscape

August 2023

CORRS
CHAMBERS
WESTGARTH

Corrs Chambers Westgarth is Australia's leading independent law firm.

We provide exceptional legal services across the full spectrum of matters, including major transactions, projects and significant disputes, offering strategic advice on our clients' most challenging issues.

With more than 175 years of history and a talented and diverse team of over 1000 people, we pride ourselves on our client-focused approach and commitment to excellence. Our fundamental ambition is the success of our clients, and this is reflected in everything we do.

We advise on the most significant global matters and connect with the best lawyers internationally to provide our clients with the right team for every engagement. We are also at the forefront of some of the most high-profile public international law matters in our region, assisting governments and corporations with the resolution of highly complex cross-border disputes.

We are the firm of choice for many of the world's leading organisations, with our people consistently recognised for providing outstanding client service and delivering exceptional results.

Foreword

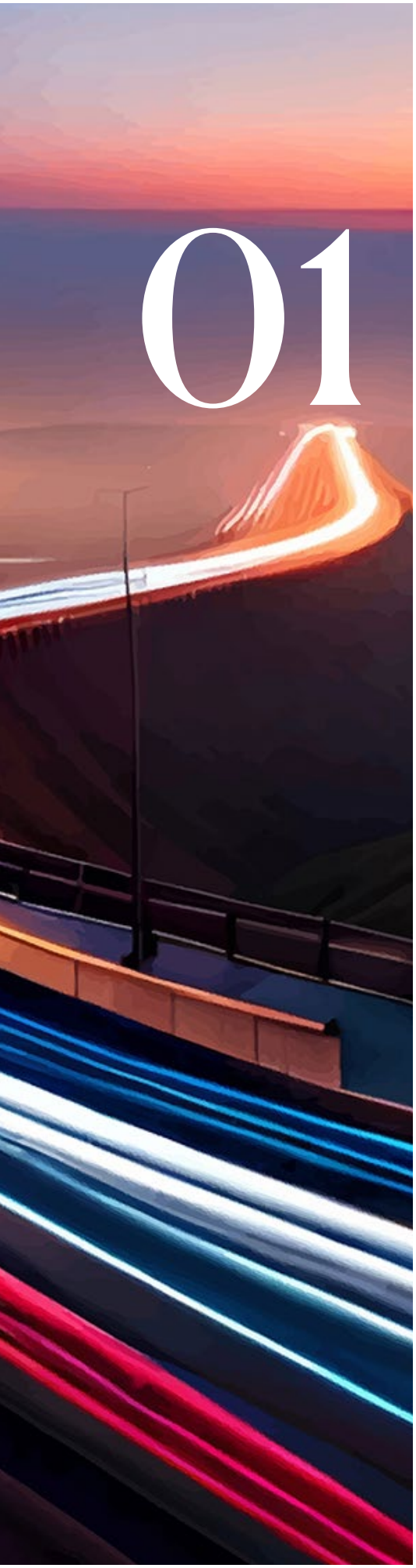
Ongoing inflationary pressures, geopolitical uncertainty, enduring supply chain challenges and a sharper focus by regulators on a variety of issues – including cyber security and whistleblowing – are contributing to ever more complexity in the Australian legal landscape.

This collection of insights provides a guide for general counsel on staying at the forefront of change, in an environment where that has never been more important.

We hope you find it helpful.

Gavin MacLaren
Senior Partner and CEO
Corrs Chambers Westgarth

Contents



01

‘Gatekeepers’ to the board: regulators’ changing expectations of general counsel

By **Mark Wilks,** Head of Commercial Litigation, **Abigail Gill**, Head of Investigations and Inquiries, **Sandy Mak**, Head of Corporate, **Andrew Lumsden**, Partner and **Katrina Sleiman**, Partner

General counsel have never been under such intense scrutiny. Regulators including the Australian Securities and Investments Commission (ASIC) are zeroing in on officers like general counsel, whom ASIC regard as ‘gatekeepers’, and seeking to hold them responsible for ensuring the prevention of corporate misconduct.

What are the regulators’ expectations of general counsel in managing and highlighting risk? And how do these dynamics impact the role and the potential liability of general counsel?

For many years, those of us interested in the area of governance and directors' duties have been watching ASIC's prosecution 'slate' waiting for the next big 'stepping stone' prosecution.

Many thought it would come out of the Crown Resorts Sydney, Melbourne and Perth casino inquiries, which identified much evidence of senior officers having overseen endemic widespread and serious non-compliance over a number of years – non-compliance that, if not strictly illegal, had caused significant reputational damage and consequent financial loss to the company (including its employees) and its shareholders. Notwithstanding this, there were no cases launched by ASIC against any officers for these missteps.

But then came the Star prosecution, in which ASIC commenced civil penalty proceedings in the Federal Court against 11 current and former directors and officers of The Star Entertainment Group Limited (ASX: SGR) (**Star**) (discussed in detail below). What made Star different? Maybe it was a perfect storm (at least for the 11 individuals involved) of:

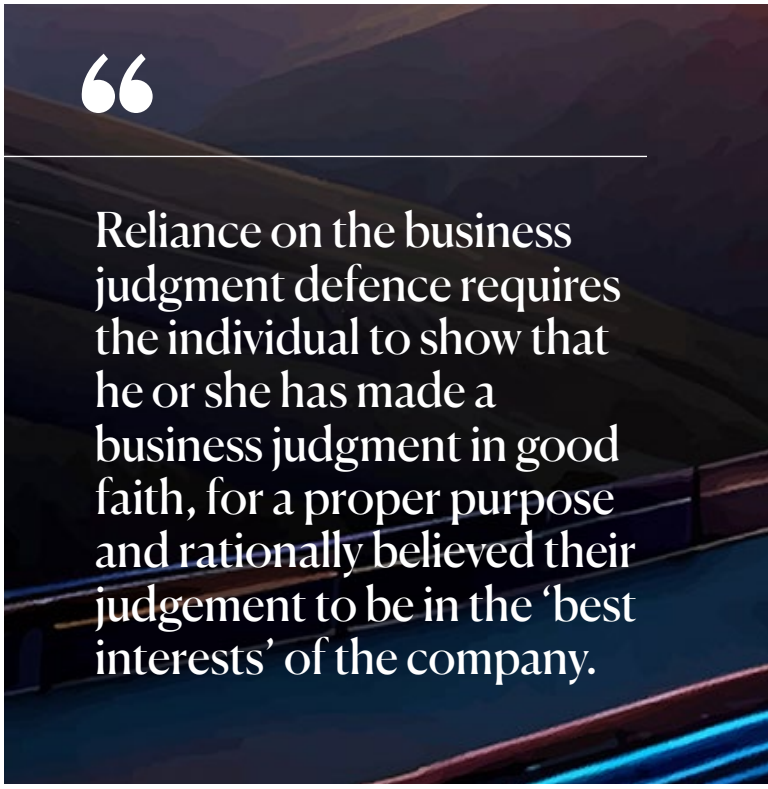
- an ASIC Commissioner with a strong belief in 'Gatekeeper Theory' and looking to test it as an enforcement thesis (below); and
- 'serious and systemic' breaches of federal law occurring over a number of years.

But maybe the biggest issue was the senior management of Star not observing what was happening at Crown and taking immediate steps to stop behaviour that ASIC thinks they knew, or ought to have known, gave rise to risks posed by gambling junket Suncity (and junkets generally) in respect of non-compliance with anti-money laundering laws. To ASIC, it seems this foreseeable risk ought to have been better managed by the defendants.

Star – the facts of the case

ASIC commenced civil penalty proceedings in the Federal Court against 11 current and former directors and officers of Star for alleged breaches of their care and diligence duties owed to the company under s 180(1) of the *Corporations Act 2001* (Cth). One of those officers was the former group General Counsel. ASIC alleges that Star's board and executives failed to give sufficient focus to the risk of money laundering and criminal associations that were inherent in the operation of a large casino with an international customer base.

This is another 'stepping stone' case brought by ASIC, and is one of very few cases ASIC has sought to bring under s 180(1) of the Corporations Act against officers who are not directors.



The Star prosecution follows the traditional mechanism for a stepping stone case. ASIC alleges that Star's officers failed to exercise the degree of care and diligence that a reasonable person would have exercised in her or his position during the relevant period to 'prevent a foreseeable risk of harm to the interests of the company'. These claims align with comments by then Chief Justice Tom Bathurst that directors and officers could be liable for conduct falling short of a strict breach of the law, which is nevertheless inappropriate or unethical, where such conduct results in significant reputational damage with consequent financial implications.

ASIC does not need to establish that Star necessarily breached the law but rather that the officers' conduct in exposing Star to a potential breach was a breach of the care and diligence obligation. In particular:

- that the General Counsel of Star should have taken all reasonable steps to ensure that Star complied with its legal obligations and protected Star from legal risks; and
- that the General Counsel failed to take reasonable steps to ensure the board of directors of Star was informed of matters that created or increased a risk that Star would breach its legal obligations.

Cassimatis[1] showed that a contravention of the law is not a necessary precondition to a breach of directors' duties and that the protections of s 180(1) extend to an obligation to protect a corporation's reputation. While ASIC has emphasised corporate reputation in the Star prosecution, it is not suggesting that this is a case solely involving an issue of reputation. The ASIC case alleges that Star was exposed to the risk it would breach the relevant anti-money laundering / counter-terrorism financing (**AML/CTF**) legislation. But ASIC is not seeking to prove breaches of that regime. In that respect the case sits better with *Vocation*,[2] in which it was clear that Vocation breached the Corporations Act (i.e. failing to make adequate disclosure). In that case, ASIC showed how, by exposing Vocation to the disclosure breach, the Chair, CFO and CEO had breached their duty of care owed in failing to 'prevent a foreseeable risk of harm to the interests of the company'.

ASIC alleges that the conduct of the officers exposed Star to harm by creating or increasing the risks that:

- Star group entities would fail to meet their AML/CTF obligations;
- Star's relationship with one of its lenders would be undermined;
- Star would suffer significant reputational damage; and
- Star would be exposed to investigations by state and federal regulators and to inquiries and legal proceedings resulting from those investigations.

Business judgment rule and stepping stones

For every officer who finds themselves threatened with a stepping stone prosecution, the question that inevitably arises is whether the business judgment defence (s 180(2) of the Corporations Act) will be available. Reliance on this defence requires the individual to show (among other things) that he or she has made a business judgment in good faith, for a proper purpose and rationally believed their judgement to be in the 'best interests' of the company.

Since the onus is on the officer to establish each of the different elements, it has proven quite difficult for officers to rely upon this defence. Unfortunately, the stepping stone cases (and most cases of directors' negligence) contain very few instances where the business judgment rule has aided directors or company officers to avoid liability. This is particularly so in cases where the company's contravention has involved a failure to make disclosure, on the basis that disclosure compliance is not a business judgment matter but instead a question of observing the law.[3]

1 *Australian Securities and Investments Commission v Cassimatis* (No 8) [2016] FCA 1023, 26 August 2016.

2 *Australian Securities and Investments Commission v Vocation Limited* (In Liquidation) [2019] FCA 807, 31 May 2019.

3 *Australian Securities and Investments Commission v Fortescue Metals Group Ltd* (2011) 190 FCR 364, 427 [197]; [2011] FCAFC 19 in which Keane CJ commented that disclosure compliance is not a business judgment matter but instead a question of observing the law. In Vocation the finding in Fortescue was affirmed.

> General counsel clearly play a critical role as a gatekeeper of legal risk and compliance within the organisation.

It is probably not the case that the business judgment defence can never apply to a stepping stone or compliance-based case like Star. In *Mariner*,[4] the Court clearly thought that the compliance and business aspects of the decision were inextricably linked and, accordingly, that a business judgment was made. That said, the business judgment rule defence is unlikely to feature in the Star prosecution since it is hard to suggest that Star was permitted to lawfully decide, as a matter of business judgment, that Star should assume the risk of non-compliance with its AML/CTF obligations. In those circumstances, the relevant officers may be liable as an accessory. What s 180(1) is concerned with in this context is the foreseeable risk that failure to take adequate care in relation to Star's compliance with the law would cause harm to the company.

Reliance

Some of the officers who were not responsible for the day-to-day running of Star may believe that they were entitled to rely on other senior executives charged with managing this issue. In the case of their AML/CTF compliance, they might argue that, as a technical area, the adequacy of the organisation's risk management and compliance systems and processes must be informed by advice from people with technical expertise in that area and it was reasonable for officers to rely on those people in the absence of any evidence that their expertise was lacking, or the processes implemented in reliance on their advice were not working.

That said, it is not enough to merely do as advised. Star's officers were bound to inform themselves about the AML/CTF compliance risks and make an independent assessment of the information or advice provided. In that sense, the reliance must also be 'reasonable'. A number of sources of information or advice received by the company would likely improve the likelihood of the ability of the officers to rely on the advice. Further, ASIC alleges that the defendants had information available to them that these risks were not being appropriately managed and failed to act, and therefore appear to have had compelling reasons to question any advice to the contrary.

ASIC and gatekeepers

ASIC has suggested that it can achieve its regulatory objectives by focusing on key individuals within a company and holding them to account for the "sins" of the companies that employ them or which they govern. The rationale for this theory is that the value an individual attributes to their own personal reputation is such that they

4 *Australian Securities and Investments Commission v Mariner Corporation Limited* [2015] FCA 589, 19 June 2015.

will not rationally sacrifice that reputation for a perceived corporate benefit. This places these individuals in a position to prevent corporate misconduct by withholding their validation of poor conduct, thereby mitigating corporate conduct that would expose the company (and expose the officers to a breach of duty claim).

This proposition is a variation of the approach developed in the United States,which focuses on third parties, such as external lawyers and auditors, and emphasises that a corporate gatekeeper is motivated to prevent wrongdoing because the expected liability or reputational harm (arising from failing to prevent misconduct) exceeds the gain in fees received. This model, however, fails to distinguish among gatekeepers or account for how gatekeepers with different incentives respond to legal controls.

The ASIC prosecution theory seems to suggest that investor and financial consumer trust and confidence is likely to be preserved by advancing positive and transparent gatekeeper conduct and culture. Within the group of targeted gatekeepers are company directors and senior executives, including the general counsel.

General counsel clearly play a critical role as a gatekeeper of legal risk and compliance within the organisation. ASIC Commissioner Joseph Longo has observed that "[t]he general counsel is there, frankly, as a gatekeeper, as the conscience of the corporation or the company, and the trusted adviser. It's a privileged position".

The case of the general counsel as a particular officer

As long ago as 2011, the High Court recognised that the general counsel was a particular type of 'officer' and that their responsibilities within a corporation extended to various specific subjects including compliance with all relevant legal requirements and, in particular, with continuous disclosure requirements. Once it was found that their responsibilities extended to those subjects, the question became whether the general counsel undertook those responsibilities with the requisite degree of care and diligence.

In *Shafron*,[5] the High Court found that the functions performed by the General Counsel, Mr Shafron, involved him participating in making decisions that affected the whole or substantial part of the business of James Hardie. Suggestions that participation in a decision meant that the person must have a role in actually **making** the decision were rejected. The High Court distinguished the role of an external adviser who proffered advice and information in response to particular requirements of the company.

Mr Shafron's position was qualitatively different as:

> *"...what he did went well beyond his proffering advice and information to the board of the company. He played a large and active part in formulating the proposal that he and others chose to put to the board as one that should be approved. It was the board that ultimately had to decide whether to adopt the proposal but what Mr Shafron did, as a senior executive employee of the company, was properly described as his participating in the decision to adopt the separation proposal that he had helped to devise."*

The High Court confirmed that Mr Shafron breached his duty of due care and diligence as an 'officer' of the corporation and endorsed the characterisation of Mr Shafron as having a duty to protect the company 'from legal risk'. By extension (as seems to be the position ASIC has taken in the Star case) the High Court's decision in *Shafron* suggests senior in-house lawyers advising a board of directors are gatekeepers responsible for:

- promoting the public interest in corporate compliance with continuous disclosure obligations and prohibitions on misleading conduct; and
- making sure that the board of directors is properly informed of matters that created or increased a risk that would breach their legal obligations.

Arguably, compliance with the law and being a good corporate citizen are also in the corporation's interests. Indeed, had the law been complied with, many years of litigation and anger from the community may have been avoided.

Looking ahead

Throughout 2023, ASIC has said that it will have a strong focus on governance and directors' duties failures, enforcement activity targeting sustainable finance practices and disclosure of climate risks, financial scams, cyber and operational resilience, and investor harms involving crypto-assets.

We expect ASIC to continue to focus on gatekeepers such as general counsel both to improve the level of disclosure and reporting and to attempt to hold them accountable for the risk of systemic regulatory breaches. It is an opportune time indeed for all general counsel to take a step back to assess the role they play in advising their boards in this wider context, particularly where they hold executive responsibility for a number of functional portfolios and risk areas beyond legal, and to determine if there is anything more they should be doing to discharge their obligations as gatekeepers going forward.

5 *Shafron v Australian Securities and Investments Commission* [2012] HCA 18, 3 May 2012.

02

Getting incident response right in a changing cyber threat environment

By **James North,** Head of Technology, Media and Telecommunications, **Andrew Lumsden**, Partner, **Michael do Rozario**, Partner and **Michael Murdocca**, Lawyer

Rapid advances in the methods deployed by threat actors have rendered the cybersecurity landscape inherently complex and unpredictable. As cyber threats continue to evolve in their frequency, sophistication and impact, boards must be prepared to treat them as being at the same level of importance as other financial, legal and regulatory considerations.

At the centre of any cyber risk framework should be an incident response plan that is shrewd and sufficiently flexible to deal with not only present foreseeable risks but also emerging and possible ones.

Even though malicious cyber actors seek to exploit system vulnerabilities and steal valuable corporate assets, affected companies are nonetheless no longer perceived by the public, media and regulators to be mere "victims". Companies are expected to turn their minds to implementing organisational frameworks and strategies to prepare for and manage a cyber incident. From a commercial and legal perspective, it is simply no longer acceptable to relegate cybersecurity to IT departments.

Despite this, many C-suites still prioritise investing in their technical capabilities without developing a wider compliance framework. This is not based on an inadequate appreciation of the seriousness of cybersecurity – indeed, they regard it as a more significant issue than the COVID-19 pandemic, economic volatility and climate change. Rather, their reliance on an 'outdated' approach to cybersecurity management is often what leads them to fail to properly adapt to the emerging cyber threat environment, the general features of which are outlined below:

Cyber threat actors

State-sponsored actors, cybercriminals, hacktivists, cyberterrorists, thrill-seekers, insider threats

Motives for cyberattacks

Geopolitical, profit, ideology, violence, satisfaction, vindication

Exploitation methods

Malware, phishing, denial-of-service attacks, spoofing, identity-based breaches, code injection, social engineering, supply chain attacks, insider threats, DNS tunnelling, IoT based attacks

Common attack vectors

Compromised credentials, weak or stolen credentials, unpatched applications or servers, insufficient authentication, phishing emails, psychological manipulation (i.e. impersonation), vulnerability exploits, poor encryption, misconfigurations, exploitations of trust, rogue insider

Why are ransomware attacks becoming increasingly common?

Lower barriers to entry, more advanced techniques, recognition of its scalability, goal to place pressure on organisational resources, increased data leaks

Key sectors targeted

Healthcare, finance, insurance, accounting, legal, management, recruitment

Consequences

Financial, reputational, operational, litigation and regulatory responses

The rising need for cyber-aware directors

Directors must ensure that in responding to these threats they discharge their duties with care and diligence and in good faith in the best interests of the corporation.

When a court looks to consider whether directors have failed in their duties in relation to a cyber incident, it would likely give substantial weight to the steps directors took and their preparedness. The directors will need to exercise a degree of care and diligence that a reasonable person would have exercised in her or his position to 'prevent a foreseeable risk of harm to the interests of the company'.

This may involve an evaluation of the extent to which the directors have:

- upheld cybersecurity best practices;
- reasonably informed themselves of risks (they cannot merely 'do as advised' by cybersecurity experts);
- addressed vulnerabilities (including through proper communication with shareholders); and
- implemented frameworks to both address foreseeable risks and respond to them.

> From a commercial and legal perspective, it is simply no longer acceptable to relegate cybersecurity to IT departments.

In order to avoid a claim that the directors have breached their duties under s 180 and 181 of the *Corporations Act 2001* (Cth), they will need to establish that they took reasonable steps to ensure that their company properly managed the foreseeable risks to the company from a cyber incident. What is foreseeable will be framed by a wide examination of the general circumstances in which the company operates and the general and specific obligations on the directors.

One relevant consideration will be the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*, which recommends that a company's risk management framework deals with the 'emerging risk' of cybersecurity and is reviewed at least annually so that it is appropriate and has proper regard for risks. Recent cases, such as *ASIC v RI Advice Group* [2022] FCA 496, recognise that cybersecurity risks can be materially addressed through adequate cybersecurity systems, documentation and controls. They also point to an increasing willingness by judges to impose fines and order the implementation of special cyber resilience measures where appropriate.

Amidst this changing environment, the Commonwealth Government is seeking new ways to make it obvious that cybersecurity is part of a director's responsibility. For example, it is presently considering (in its *2023-2030 Australian Cyber Security Strategy Discussion Paper*) introducing specific obligations for directors to address cybersecurity risks and consequences. Further, the Australian Computer Society has suggested imposing criminal penalties on directors who knowingly and wilfully breach privacy laws. Regardless of whether either of these measures are introduced, they point to rising expectations for directors to consider cybersecurity.

The incident response plan

A central component of any organisational response to cybersecurity should be a comprehensive and accessible incident response plan that clearly sets out:

- the roles and responsibilities of different persons and bodies (i.e. the incident response and crisis response teams, lawyers and advisers);
- the steps and processes those persons and bodies should follow;
- how impact assessments should be facilitated;
- how critical business functions should be preserved;
- escalation and reporting mechanisms (including to the board and external bodies such as the Office of the Australian Information Commissioner (**OAIC**));
- general timeframes within which decisions should be made and by whom;
- alternative approaches to making decisions where cyberattacks occur during inconvenient times or require quick responses;
- how external service providers should be engaged with and their function in the context of the broader incident response;
- how and when persons activating the incident response plan should refer to other documents such as technical process guides, asset management frameworks and business continuity plans;
- communication procedures both internally and externally; and
- post-incident actions.

Carving a pathway to effective communication and decision-making

Without an incident response plan to refer to, it may be tempting for directors to be reactive in the face of an actual or suspected cyber crisis either by instructing their communications teams to withhold information or to 'spin' the situation by publishing 'good news' stories. This could contravene certain obligations, for example:

- a cyberattack which reduces or limits the ability for an organisation to function will have material share price implications and thus must be disclosed to the ASX under Listing Rule 3.1;
- an organisation may contravene client engagement agreements or their conduct may amount to misleading or deceptive conduct where they fail to sufficiently disclose information to customers; and
- an organisation must notify individuals and the OAIC Commissioner about 'eligible data breaches' that are likely to cause serious harm.

An incident response plan would also create mechanisms for directors to address ransomware attacks, which often require quick and measured responses, including in circumstances where convening a timely board meeting is not feasible.

Organisations face complex considerations in the face of such an attack – on the one hand, the Government advises them not to make ransom payments, and, if they are made, prosecutors may interpret them as either 'instruments of crime' under the *Criminal Code 1995* (Cth) or in breach of other criminal law provisions. These include anti-money laundering, counterterrorism and sanctions laws, such as under the *Autonomous Sanctions Act 2011* (Cth), *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (Cth) and *Charter of the United Nations Act 1945* (Cth). However, the extent to which making ransomware payments could fall within the scope of these criminal law provisions is presently a legal 'grey area' and the courts have provided limited commentary on the application of potential defences in a ransomware context.

An organisation may also be persuaded to give weight to ethical concerns (i.e. threats to life), reputational risks, the likelihood of negotiating lower payment thresholds and other factors such as consequences of data being sold or lost. Given the complexity involved in responding to these attacks, if a threat actor seeks to extort an organisation the last thing their crisis team wants to worry about is under what circumstances they should consult the CEO or the documents they should refer to when making decisions.

Further, the ASX has said that companies can use brief trading halts pursuant to Listing Rule 17.1 to avoid false reporting and obtain information that investors need. An incident response plan would enable companies to be prepared to gather relevant documentation and thereby avoid any allegations of having avoided making timely disclosures of a material cybersecurity incident.

Consequences of a poor incident response plan

Apart from facing obvious financial and operational strains, organisations that do not have adequate incident response plans and are later subject to a data breach may find themselves at the centre of disputes or investigations, such as:

- shareholder class actions (alleging breaches of continuous disclosure requirements or misleading or deceptive conduct);
- court proceedings for consumer class actions (alleging the company or its officers failed to secure personal information or properly respond to security breaches) and, additionally, OAIC representative actions;
- Australian Securities and Investments Commission (**ASIC**) and Australian Competition and Consumer Commission (**ACCC**)-led prosecutions;[1] and
- OAIC-led investigations (the regulator recently received increased funding), including in relation to responding to serious or repeated interferences with privacy. These now attract maximum penalties of A$2.5 million for an individual and, for a body corporate, the greater of either A$50 million, three times the value of the benefits obtained due to the contravention, or 30% of the body corporate's adjusted turnover during the breach turnover period.

The Commonwealth Government has indicated in its *Privacy Act Review Report* that it will only make it easier for individuals affected by data breaches to seek recompense and is placing pressure on companies to cover the costs of compromised personal information such as identity documentation.

One thing is clear: boards must ensure they are agile and prepared for cyberattacks. Effective incident response plans will be very important in guiding any organisational ship through the murky waters of evolving cyber threats and regulatory abrasiveness.

1 Both ASIC and the ACCC have recently demonstrated they have the 'teeth' to engage with cyber issues. ASIC may, for instance, bring stepping stones actions in serious cases where a director both (a) fails to exercise the degree of care and diligence that a reasonable person would have exercised in their position, and (b) causes the organisation to contravene the law where it was reasonably foreseeable that their actions would bring harm to the interests of the organisation.

03

The future of biodiversity risk assessment for corporations

By **Dr Louise Camenzuli,** Head of Environment and Planning, **Adam Stapledon**, Head of Banking and Finance, **Alison Morris**, Special Counsel and **Samantha Yeung**, Senior Associate

Biodiversity and climate change are now fundamental aspects of a corporation's risk assessment and strategic planning.

A number of upcoming regulatory changes and legal developments are driving the future of biodiversity regulation and sustainable financing in the Australian corporate space. What strategies can directors adopt now to stay ahead of the game?

Mandatory climate-related disclosures

The Taskforce on Climate-related Financial Disclosures (**TCFD**) was established to develop global recommendations on the types of financial information which should be disclosed by a corporation to allow investors, lenders and insurance underwriters to properly assess and price risks relating to climate change.

Climate-related disclosures are increasingly becoming part of 'business as usual' reporting. In this regard, the International Sustainability Standards Board (**ISSB**) is developing a global baseline of sustainability disclosures which builds on the climate disclosure themes developed by the TFCD. In late June 2023, the ISSB released its inaugural global sustainability disclosure standards. It is expected that these will be implemented in jurisdictions globally and become the globally accepted benchmark for the minimum standard of disclosures expected by corporations worldwide.

Since the emergence of the TCFD framework, the percentage of international and Australian companies making climate-related disclosures has steadily increased.[1] The disclosures not only require companies to make an assessment of their own climate-related risks (and create policies to mitigate that risk), but are an increasing requirement of investors who consider the risks of climate change in making financial decisions. To date, however, climate-related disclosure has been voluntary in Australia.

That said, the move towards implementing a mandatory climate-related disclosures framework in Australia is in motion. In December 2022, the Australian Treasury released a consultation paper seeking views on the design and implementation of internationally aligned mandatory requirements for climate-related disclosure.[2] The discussion is not on whether mandatory reporting is required, but what form that reporting should take and the extent to which the global baseline set by the ISSB will be adopted in Australia. The submissions on the consultation are currently being reviewed to inform a specific design proposal which will be the subject of further consultation in 2023. Large businesses should expect mandatory climate-related disclosures in the future.

Mandatory nature-related disclosures

The Taskforce on Nature-related Financial Disclosures (**TNFD**) is similar to the TCFD and aims to provide clear, structured guidance to organisations to report on nature-related risks.

The TNFD aims to navigate global finance away from harmful impacts on nature and toward more nature positive impacts. While the TNFD framework is still in the design phase, like with the TCFD, we expect that reporting on nature loss and nature risk will become mandatory in the next few years. The final framework is set for release in September 2023.

Sustainable financing

The Commonwealth Government announced in April 2023 that, in partnership with the Australian Sustainable Finance Institute, it will co-fund the initial development phase of an Australian Sustainable Finance Taxonomy (**ASFT**).

Sustainable finance taxonomies are classification systems, including a set of common definitions, which are used to define sustainable investments. The ASFT project builds on work done on equivalent sustainable finance taxonomies internationally, including in the European Union. Once established, it is expected that the ASFT will assist companies by:

- helping them to determine which of their existing economic activities and investments can be considered 'sustainable' within an Australian climate, environmental and social context;
- providing more certainty around how existing economic activities and investments will subsequently need to transition to continue to be classified as sustainable;
- increasing the integrity of so-called 'green investments'; and
- providing clarity around opportunities to create sustainable assets and to target particular sustainability objectives as part of standard operating practice.

The ASFT will also make it easier for investors to compare sustainability claims between investment products and portfolios. The ability to refer to a widely accepted common classification system may also assist companies and directors better to manage the risk that regulators, competitors or the general public characterise marketing or business activities directly or indirectly linked to sustainability objectives as greenwashing.

1 ACSI, Taskforce on Climate-related Financial Disclosures Annual Report, 'Promises, pathways & performance – climate change disclosure in the ASX200', 25 July 2022.

2 Australian Treasury, 'Climate-related financial disclosure – consultation paper', December 2022.

Increased risk of climate and biodiversity litigation

The other side of increased regulation of climate and nature-related disclosures is the increased threat of litigation. Corporations need to be cautious when reporting on climate and nature-related disclosures not to make misleading 'greenwashing' disclosures which amount to misleading or deceptive conduct.

Climate and biodiversity litigation is also developing outside of consumer law. We have seen administrative law challenges to planning approvals on climate grounds, including on the basis that a decision-maker failed to consider impacts of a proposed development on scope three greenhouse gas emissions, and on the grounds that an application for a proposed coal mine should be refused given the mine's contribution to climate change.[3]

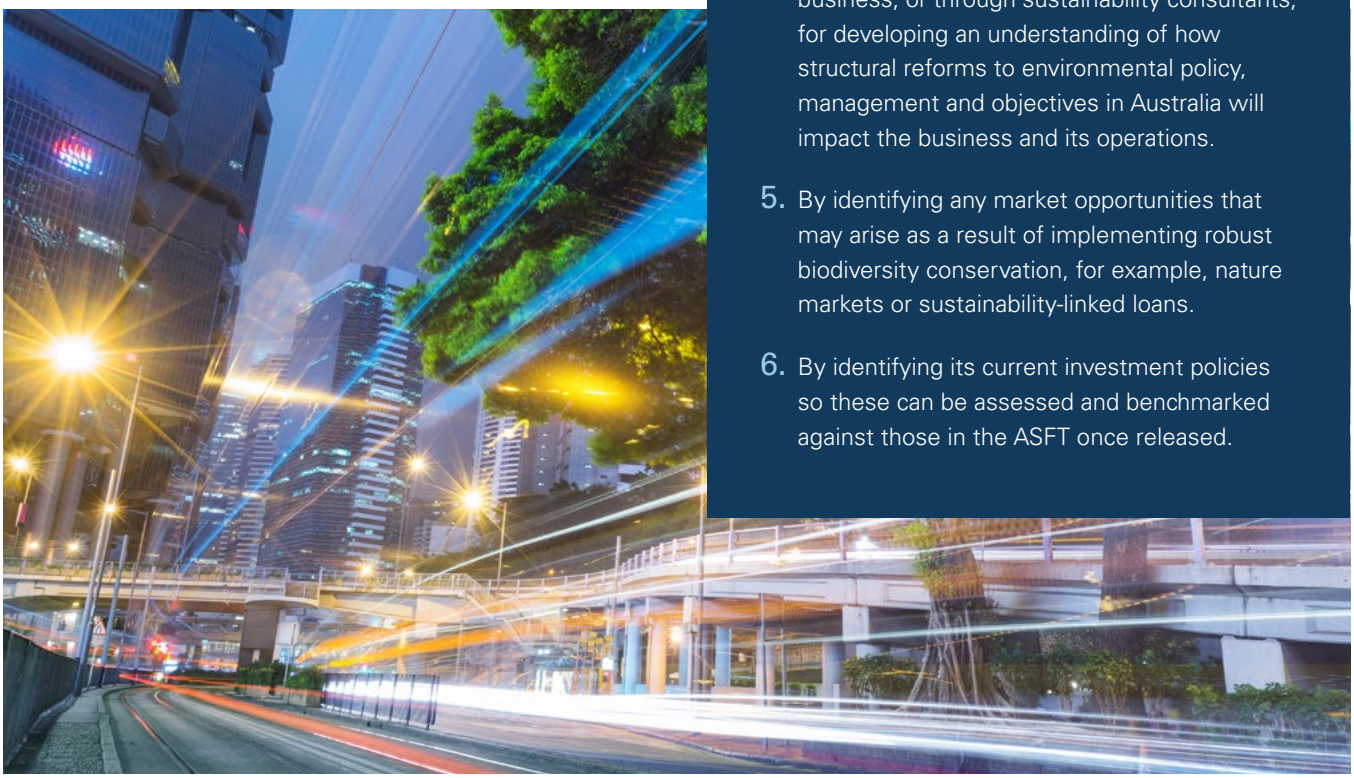
Another form of climate change litigation, not yet seen in Australia, arises in shareholder class actions, where shareholders seek to recover their losses from directors, auditors and advisers who have not adequately confronted climate change risks. Shareholder class action climate change litigation has been seen in the UK. While there are some differences between the UK and Australia, Australian law enables shareholders to bring actions on behalf of the company on similar allegations, namely via a 'derivative action' available under Part 2F.1A of the *Corporations Act 2001* (Cth).

Strategies for directors

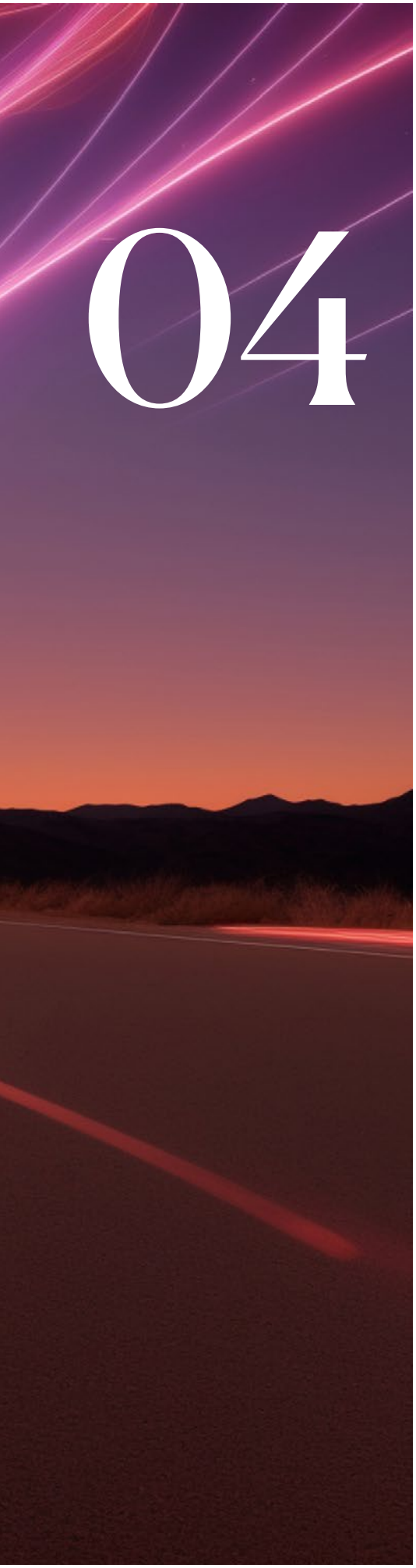
In this quickly changing corporate environment, there are clear financial and reputational benefits for corporations that can respond proactively. Businesses can benefit by protecting and enhancing their social capital and reputation and avoid shocks associated with the introduction of mandatory reporting and litigation.

We have identified the following ways in which directors can protect and propel their companies forward economically, socially and sustainably in light of the upcoming changes:

1. By carrying out risk assessment of nature and climate-related impacts and dependencies within the business. The implementation of mandatory nature and climate-related disclosures is impending, with introductory action set to assist business to prepare and implement systems which can manage any future financial risk disclosure requirements.
2. By implementing or improving environmental, social and governance metrics and sustainable practices into credit and risk analysis.
3. By increasing accessibility of debt financing.
4. By assigning responsibility within the business, or through sustainability consultants, for developing an understanding of how structural reforms to environmental policy, management and objectives in Australia will impact the business and its operations.
5. By identifying any market opportunities that may arise as a result of implementing robust biodiversity conservation, for example, nature markets or sustainability-linked loans.
6. By identifying its current investment policies so these can be assessed and benchmarked against those in the ASFT once released.



3 See *Australian Conservation Foundation Inc v Minister for the Environment* [2017] FCAFC 134, Mullaley Gas and Pipeline Accord Inc v Santos NSW (Eastern) Pty Ltd [2021] NSWLEC 110 and *Gloucester Resources Limited v Minister for Planning* [2019] NSWLEC 7.



04

ESG and the successful delivery of major projects: key considerations for project proponents

By **Andrew Stephenson**, Head of Projects, **Dr Phoebe Wynn-Pope**, Head of Responsible Business and ESG and **Dr Louise Camenzuli**, Head of Environment and Planning

The development of any successful major project goes through several stages.

Many proposed projects fail at an early stage, usually because they are not economically viable. Others pass through these stages yet fail to achieve their economic objectives, including failing to properly take account of environmental, social and governance (ESG) matters.

The various stages of a project include:

1. Acquiring the title or rights which underpin the project.
2. Obtaining environmental and planning approval.
3. Capital raising.
4. Conducting further due diligence on the project's viability, including considerations associated with project finance.
5. Obtaining final approvals for the project, including all environmental, development and construction approvals.
6. Constructing infrastructure necessary for the project, ensuring that the time, cost and quality of the construction meets required standards to achieve project viability.
7. Operating the project.
8. Selling or decommissioning the project.

Below, we explore the ESG matters that should be carefully considered at each of these stages.

Establishing the property rights necessary for the project to proceed

The project proponent must do sufficient due diligence to satisfy itself that it is obtaining clear title to the necessary assets or rights which underpin the economic purpose of the project.

First Nations rights and interests in land are formally recognised over around 50 percent of Australia's land mass. For projects being developed on First Nations lands or seas, genuine engagement with First Nations people is paramount. To protect against the future operational, regulatory, reputational and, ultimately, financial risks, project proponents should identify and consult First Nations people with connections to the land, sea and sites of cultural significance to obtain free prior and informed consent (**FPIC**) before finalising project plans.

FPIC has both procedural and substantive requirements. It is a principle derived from the right to self-determination, articulated in the United Nations Declaration on the Rights of Indigenous People (**UNDRIP**), and required as an indication of respect for Indigenous peoples, to enable them to realise their rights and to ensure their protection. FPIC should be realised before any rights are impacted, which means well before the project begins. Engaging in respectful consultation with impacted First Nations communities to obtain consent will assist in the planning and permit process and help prevent operational delays. It is also an important part of a social licence to operate. The Federal Court has recently demonstrated a willingness to identify principles consistent with FPIC in legislated consultation processes.[1]

Fulsome community engagement and a deep understanding of the potential impact of project externalities on the local community more broadly, and in particular more vulnerable members of that community, is also becoming increasingly critical.

1 See the Federal Court's decision in *Tipakalippa v National offshore Petroleum Safety and Environmental Management Authority (No.2)* [2022] FCA 1121 (the **NoPSA case**) and the Full Federal Court's clarification of the requirements for consultation on appeal, *Santols NA Barossa Pty Ltd v Tipakalippa* [2022] FCAFC 193. See also Corrs article, *FPIC in the Australian context: now and into the future*, 1 May 2023.

> Fulsome community engagement and a deep understanding of the potential impact of project externalities on the local community is becoming increasingly critical.

This year, some major projects have been affected by injunctions or other allegations that relate to ESG matters. Subsequent claims that there has been a failure to properly take account of ESG issues can lead to very significant delays to the critical path to completion of the whole project. This is particularly so in a current regulatory environment where there has been a significant widening of the gap between social expectations and legal obligations necessary to operate. Delays to completion, and therefore income generation, will lead to a consequential diminution in the net present value of the project. In serious cases, such a delay can result in the assumptions in the business case being falsified to the extent that the project is no longer viable.

Environmental and planning approvals

It is also important to ensure that there are no fundamental environmental issues which will preclude the proposed project. These issues are also important at the time of establishing rights to the necessary property for the project. If there is a known environmental issue that will preclude development, the acquisition should not proceed.

Increasingly, public interest groups are searching for failures by project proponents and regulatory authorities in the approval process. If relevant environmental and planning approvals are not properly obtained, serious delays to the project can occur. Moreover, the existence of an approval from a regulatory authority does not guarantee that the approval will survive judicial scrutiny. Where a challenge is successful, the approval can be effectively scuppered. As has occurred recently in Australia, projects can also stall pending the determination of a legal challenge due to uncertainty about future outcomes, causing delay and loss.

Relatedly, equity participants purchasing an interest in the project after, and in reliance upon, approvals which have been granted, ought to complete their own due diligence to ensure that all proper processes were undertaken by the regulatory authority when issuing the approval and question whether the regulatory regime in the context of the relevant project is fit for purpose. In circumstances where the law in the project approvals space is being tested in novel ways, administrative law appeal risk should be evaluated at the outset and through the assessment and approval process.

Capital raising

Investor engagement over the project lifecycle brings its own ESG demands. In many cases investors are signatories to international standards such as the *Equator Principles Association Equator Principles EP4* (July 2020), the *International Finance Corporation Environmental and Social Performance Standards* (2022), or the *United Nations Principles for Responsible Investment* (2006). Investors who commit to these standards are required to undertake a level of due diligence and understand project performance across a range of environmental and social standards including climate and biodiversity, labour and working conditions, land acquisition and resettlement, cultural heritage and Indigenous peoples.

There is evidence to show that strong ESG management by the project proponents can lead to a reduced cost of capital of up to ten percent. Investors and financiers have historically relied upon approvals given by regulatory authorities as evidence that any environmental issues associated with the project have been resolved. However, governmental approvals have recently been challenged because the process required of the relevant authority was not followed.[2]

Accordingly, there is a heightened need to ensure that approvals satisfy relevant legal requirements and otherwise satisfy the reasonable expectations of various stakeholders affected by the project. These matters involve issues beyond the satisfaction of strict legal requirements and generally extend to issues relevant to the social licence to operate, as discussed below.

Debt funding

Project financiers will be very interested in ensuring that adequate title to the relevant rights is available and that the interests and rights of First Nations people have been dealt with in a way that ensures the project's success.

Likewise, the financiers will need to be satisfied that the environmental and planning approval process is sufficiently advanced, such that the risks associated with approvals are manageable. Even if the current problems inherent in some vague language used in legislation are resolved, it is apparent that community interest groups will be imaginative in ensuring that there is strict compliance with any relevant ESG requirements mandated by law.

Obtaining final planning and environmental approvals

Prior to construction commencing on site, all of the final environmental approvals and pre-construction certifications are required.

These approvals generally relate to minor issues such as how construction is to be performed without unduly disturbing the local environment (for example, regulating construction of a pipeline across an existing stream). Nonetheless, these approvals are important and, if not obtained in an orderly fashion, can delay the project and increase costs or otherwise where not complied with result in actions being taken that are still unlawful.

Construction

The construction of any major project requires a sensitive approach to matters arising under State and Commonwealth legislation. However, environmental and social issues that go beyond legislative and regulatory requirements can arise if stakeholder expectations are not met. This may arise in respect of the expectations of First Nations people regarding certain projects. Nevertheless, the management of these expectations extends to other stakeholders and can relate to matters involving material selection, water consumption, human rights and procurement practices. Despite significant efforts to identify heritage issues prior to commencement of construction, it is necessary to manage new heritage issues which arise as a consequence of discovering matters of Aboriginal heritage during construction.

Unknown heritage issues can also give rise to the abandonment of projects, even after construction has commenced. The proposed construction of the Hindmarsh Island Bridge in South Australia is an extreme example. Objections were raised by Doreen Kartinyeri and others that it would desecrate a site of traditional Aboriginal secret women's business, which could not, for cultural reasons, be disclosed to men. Owing to these heritage issues, in 1994 the Federal Aboriginal Affairs Minister Robert Tickner issued an order stopping the project. But after an unsuccessful High Court challenge by the objectors, construction of the bridge recommenced and it was officially opened on 4 March 2021, a delay of 27 years.[3]

2 See the NoPSA case (supra).

3 Kumarangk Coalition, 'Stop the Bridge: respect and protect Kumaranggk / Hindmarsh Island', State Library of South Australia, 1994.

Operation

When operating a project facility, solid environmental and human rights due diligence management plans should be in place. This includes modern slavery due diligence programs that allow the project proponent to be confident that the facility is not exposed to modern slavery and that any modern slavery disclosures are verifiable. The facility should also consider ensuring operational grievance mechanisms are in place to manage human capital and human rights risks within the workforce, and within the community impacted by the project. Environmental and social impact assessments may no longer suffice to identify all the ESG risks to which a project is exposed.

While not always a legal issue, the social licence to operate is also an important consideration. A failure to have regard to these issues, which in many cases will exceed the legal requirements, may cause significant reputational damage or even loss of the project.

Decommissioning

Issues associated with the decommissioning of projects are becoming apparent, as facilities and infrastructure past their economic life are increasingly being decommissioned. Examples include AGL's decommissioning of the Liddell Power Station and Energy Resources Australia's decommissioning of the Ranger uranium mine in the Northern Territory.

Often overlooked 30 or 40 years ago, the costs of decommissioning are very high and are to be borne by the project proponent(s). The relevant State Government authorities will often require bonds to ensure that the relevant decommissioning work is done properly.

Accordingly, it is important, both at the outset of the project and during its operation, to understand the cost implications associated with decommissioning and to make provision for it. During the course of operation, it may also be appropriate to manage the project in a way which limits decommissioning at the end of the asset's life.

Looking ahead

Strong ESG risk management brings significant benefits, not only to the environment and stakeholders impacted by the project, but also to project proponents. Strong stakeholder engagement can help to identify and address concerns, as well as any issues that arise early in the project cycle.

Consideration of human rights, including FPIC and environmental (including climate and biodiversity) risks, helps minimise any external project impacts and also identifies and mitigates risks that may arise in the development and operation of the project. In the past, ESG risks and impacts have been considered as non-financial risks. However, there is now little question that many of the risks arising (for example, climate risks) are considered material to the business with both commercial and financial implications. Organisations that ignore the need for strong ESG management do so at their peril.

05

A ‘renewed focus’: key whistleblowing considerations for boards and directors

By **Abigail Gill,** Head of Investigations and Inquiries, **Sarah Clarke**, Partner, **Andrew Lumsden**, Partner, **Marisa Orr**, Special Counsel and **Clare Mould**, Special Counsel

With the Australian Securities and Investments Commission (ASIC) set to intensify its regulatory focus on whistleblowing, now more than ever, it is crucial that organisations continue to undertake careful reviews of their whistleblower program to ensure they are compliant.

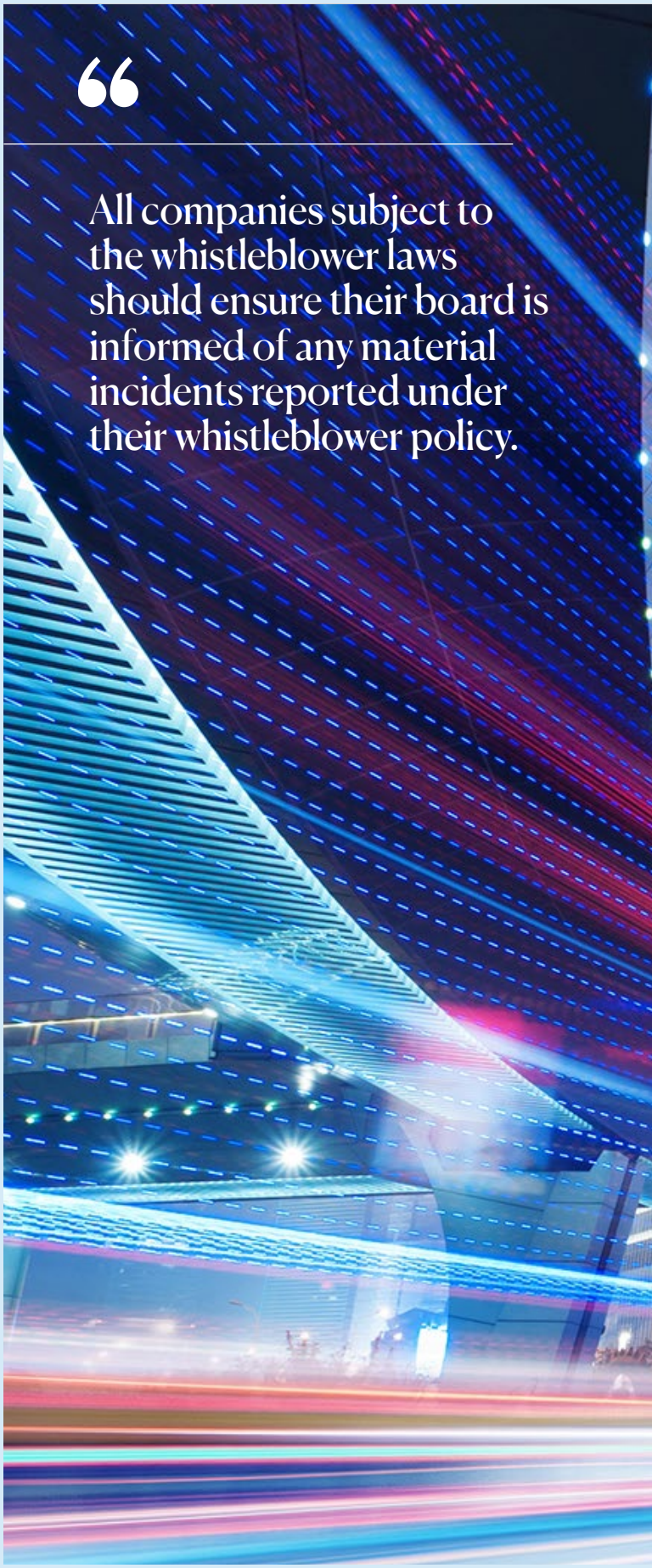
What are the key elements of an effective whistleblower program, and what should executives and directors keep in mind as they evaluate their organisation’s management of whistleblower issues?

Since 2019, there has been a mandated whistleblower regime under Pt 9.4AAA of the *Corporations Act 2001* (Cth) (**Corporations Act**). All companies regulated by ASIC are required to comply with the whistleblower protections, and public companies, large proprietary companies and trustees of registrable superannuation entities are expressly required to have a whistleblower policy that meets statutory criteria. ASX-listed entities should also publish their whistleblower policy and meet the governance requirements set out in the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*.

As a matter of good corporate governance, all companies subject to the whistleblower laws should ensure that their board is informed of any material incidents reported under their whistleblower policy and periodically receives sufficient information to form a view about the effectiveness of the company's whistleblower program.

After a period of time for companies to adopt the 2019 reforms, there are also indications that ASIC will intensify its regulatory focus on whistleblowing within its regulated population:

- in 2020, ASIC undertook a review of 102 whistleblower policies, finding the majority fell short – incomplete / inaccurate information and out of date policies were identified as the most concerning and widespread deficiencies – ASIC responded with a letter to CEOs in 2021, encouraging organisations to evaluate their policies against the statutory requirements;
- in March 2023, ASIC commenced its first enforcement action against a company and senior company employees for breaches of the whistleblower provisions, and has stated that it has current investigations underway;[1] and
- ASIC's recent market review in March 2023 has suggested that many whistleblower policies still do not comply with the Corporations Act, and it has published the results of its review of the effectiveness of a selection of whistleblower programs, focusing on:
  - how disclosures are handled;
  - how organisations are using information their whistleblower program to address operational issues or misconduct; and
  - the level of board and executive oversight of the program.



1 Speech by ASIC Commissioner Sean Hughes at the 3rd Australian National Whistleblowing Symposium, 'Whistleblower policies and the compliance gap', 11 November 2021.

ASIC's expectations of board oversight continue the focus on directors and senior officers as 'gatekeepers' with the responsibility to set the tone and monitor an organisation's response to issues like whistleblowing.[2] Whistleblowing also supports ASIC to perform its role by enabling early identification of harm to consumers and investors and swift intervention to address misconduct. The value of whistleblowing to ASIC's ability to meet its enforcement mandate is evident from the statistics it has reported. In FY 2018/19 (before the protections commenced), ASIC reportedly received 278 whistleblower reports. That rose to 644 reports in FY 2019/20 and 817 in FY 2020/21 (a 194% increase over two years).

Aside from being an important regulatory requirement (and an enforcement risk if not implemented according to legal requirements), a whistleblower program that is operating effectively helps an organisation to identify instances of serious misconduct, systemic issues and areas where corporate culture is not aligned to the entity's purpose, values or strategic objectives. For example, a protected disclosure about unauthorised use of personal or protected information may identify that an entity's cybersecurity controls are lacking, and a failure to identify this issue early could have consequences under cybersecurity or data privacy laws. Further, a breach of confidentiality when handling a whistleblower report could give rise to other legal risks, including under employment, privacy / cybersecurity and other laws, particularly where an organisation does not have adequate processes or systems in place to protect confidential information. It is therefore essential that boards and senior executives have a good understanding of their own obligations within the company's whistleblower framework and their company's internal policies and processes for managing whistleblower disclosures.

An effective whistleblower program will always need to be 'fit for purpose' – there is no one size fits all. ASIC has noted that an effective whistleblower program will incorporate the following elements (in summary):

- it has a strong foundation with embedded processes and a culture that supports whistleblowers;
- there is information and training provided to those who handle disclosures which addresses how to protect whistleblowers and confidentiality;
- the program is monitored and outcomes from whistleblower reports are used to identify continuous improvement opportunities (for the program);
- information is used to respond to underlying harms; and
- directors and officers have oversight and accountability for the program.

2 See 'Gatekeepers' to the board: regulators' changing expectations of General Counsel' on page 7 of this publication.

Key elements of an effective whistleblower program

Below are some observations about the key elements of an effective whistleblower program (informed by the matters ASIC has highlighted in its review) to guide executives and directors as they evaluate their organisation's management of whistleblower issues.

1. The policy and operational guidance documents

All companies – irrespective of size, nature or scale – need operational documents to support their whistleblower program, and a formal whistleblower policy that provides strong assurance that the organisation's expectations for whistleblower management are clearly spelled out. It will also instil a degree of confidence amongst employees as to its commitment to effective whistleblower management, whether or not the entity has a statutory requirement to have one.

A whistleblower policy that meets the requirements under the Corporations Act must incorporate a number of specified criteria. It must:[3]

- describe the protections available to whistleblowers;
- explain how to make a qualifying disclosure, including to whom;
- set out the entity's measures to support and protect whistleblowers;
- provide information about how the entity will investigate whistleblower disclosures and ensure fair treatment of individuals named in disclosures (or about whom the disclosure is made); and
- state how the policy will be made available to officers and employees.

The appropriate processes beyond a policy will vary depending on the organisation. Operational documents may include workflows or process maps for staff involved, protocols (e.g. for handling and investigating disclosures, assessing / monitoring risk of detriment and storing information), whistleblower conversation guides (e.g. for staff who can receive protected disclosures) and consent forms.

These operational documents mitigate risks that may arise when the process is not fully understood and the firm relies on the skill and experience of a limited number of individuals.

2. Training and communication

ASIC has indicated that best practice should include training, which should be tailored to the audience and aligned with the entity's policy and procedures. At a minimum, training for eligible recipients (including directors) on how to handle disclosures and respond to whistleblowers in line with legal requirements will mitigate the risk of adverse treatment of whistleblowers, such as a breach of confidentiality. Further, ASIC has noted the importance of providing proportionate, specialised training to all staff with specific responsibilities under the firm's whistleblower policy and program, such as those responsible for investigating concerns.

To embed an understanding of the requirements and encourage a strong culture of compliance, policies and procedures should also be promoted within the organisation. This might be achieved through a number of channels such as a staff-wide email campaign reinforcing key messages, intranet posts, town halls about whistleblowing, routine policy updates and the promotion of whistleblower information (e.g. contact details for internal eligible recipients on posters where employees gather and dedicated intranet pages).

3. Reporting

Many companies direct potential whistleblowers to report their concerns via one channel, such as an external hotline. This can be an efficient process for triaging reports and it also lowers the risk of non-compliance with whistleblower laws, as well as the confidentiality requirements and potential victimisation that may apply under other laws when handling and investigating matters. Where other grievance channels exist (e.g. for HR complaints), staff handling or investigating those matters must be able to identify potential protected disclosures and follow a process for passing them on immediately to the whistleblowing function.

To ensure the program is working effectively, monitoring of disclosure volumes and channels used, downloads or page views and rates of employees' self-reported willingness to speak up via employee perception surveys can provide important feedback and a measure of assurance for executives and directors who are responsible for oversight of the program and ensuring that it is operating effectively.

3 Section 1017AI of the *Corporations Act 2001* (Cth).

4. Investigations

The program should have a sound but flexible investigation process that can be adapted to the type of disclosure received. A clear definition of the responsibilities for key roles (e.g. for protecting disclosers and assessing / monitoring risk of detriment, for investigating, reporting etc.) are mechanisms to avoid conflicts of interest where staff hold more than one role.

Through its review in 2023, ASIC considered how information from substantiated allegations was being used to address underlying harms and to improve company performance. The kind of remedial actions highlighted included:

- improving internal processes and practices;
- sharing de-identified information about the matter and outcome with relevant business units;
- imposing disciplinary outcomes on those involved in misconduct in line with the firm's consequence management framework;
- considering involvement in misconduct raised by whistleblowers when making executive variable pay decisions; and
- demonstrating transparency by sharing data on whistleblower trends in annual reports and other publications.

The information received via an organisation's whistleblower program is an important data point for evaluating culture and identifying ongoing or system issues. Implementing a process for collecting data on matters such as the types of allegations or issues raised in disclosures, who made the disclosures (e.g. employees or others), how disclosures were finalised, and the locations, business units, or departments involved is a first step to help organisations identify emerging areas of risk, or opportunities to improve operations.

5. Executive oversight and accountability

Given the valuable insights that can be gained about culture and emerging risks from the results of whistleblower reporting and investigations, it is not surprising that ASIC has emphasised the importance of senior and executive accountability and oversight of the whistleblower program.

ASIC is encouraging companies to have an accountable senior manager (typically holding a legal, compliance or risk-related position, and distinct from the person responsible for the policy) with a direct reporting line to the board committee overseeing the program. The involvement at executive level will inevitably be a factor of the size of the organisation and the volume of reporting received. For example, ASIC has identified executives being involved in complex or sensitive disclosures (e.g. if the matter meets a particular risk threshold), issues relating to the handling of disclosures and structural reviews of the whistleblower program and director engagement.

It is common for an organisation's board risk or audit committee to oversee the whistleblower program and for this oversight function to be described in board charters or terms of reference. As a matter of good practice, the kind of information that may be shared with the board could include periodic information about how the program is working, statistical analysis of disclosures and outcomes to inform directors about emerging risks or themes, reporting on disciplinary outcomes for substantiated allegations as well as ongoing training on directors' obligations in relation to whistleblowing.

ASIC has a renewed focus on whistleblower programs. Now more than ever, it is crucial that organisations continue to undertake careful reviews of their whistleblower program to ensure that they are compliant, are implementing good practices and have appropriate oversight mechanisms to identify and manage emerging risks, both in terms of potential detriment to whistleblowers, and within the organisation more broadly.

06

Investment treaties and the energy transition: challenges and opportunities

By **Nastasja Suhadolnik,** Head of Arbitration, **Franka Cheung**, Special Counsel and **Samuel Kay**, Senior Associate

There is growing recognition that Australia, like other countries around the world, must encourage foreign investment to achieve its clean energy transition goals. Investment treaty protections have long been seen as an important tool for attracting foreign investment. However, amidst concerns about governments' ability to execute on their energy transition goals, this traditional view is increasingly being challenged.

Recent developments are prompting a close examination of the role investment treaties play in promoting renewable energy investments and the relevance of investor-state dispute settlement as a risk mitigation tool for foreign investors in renewable energy projects. As traditional energy sources continue to get replaced by renewable ones, one thing is clear – change is on the horizon.

According to Austrade, '[f]oreign direct investment is supporting Australia to lower carbon emissions and move towards sustainable energy sources'.[1] This is consistent with the Paris Agreement, in which Contracting States (including Australia) recognise that finance flows are required to lower greenhouse gas emissions and support climate-resilient development. Globally, the International Energy Agency estimates that in order to reach net zero emissions by 2050, annual clean energy investment worldwide will need to more than triple by 2030 from the current US$1.4 trillion to around US$4 trillion annually.[2]

On the other side of the ledger, we are already seeing new and increasing export markets for Australian energy products – hydro, wind, solar and hydrogen – and for key components of low-emissions technologies, capitalising on Australia's abundant rare earth and critical mineral deposits. As BHP's Chief Executive recently commented, "the chase [for mining investment is] now on and… many other nations are competing for capital". That competition was ramped up in August 2022 by the passage of the Inflation Reduction Act in the United States, which pledges A$520 billion in the pursuit of energy transition.

Recognising the "big risk with the inflation Reduction Act… that you would see capital leave Australia to go to the United States", Prime Minister Anthony Albanese recently struck a compact pursuant to which the United States would recognise Australia as a domestic source for critical minerals and clean energy, allowing qualifying Australian companies to access (via facilitative legislation) subsidies and other benefits under the Inflation Reduction Act. The compact's emphasis on critical minerals, storage and hydrogen technologies plays to Australia's unique opportunity as the nation with some of the world's largest reserves of the critical materials that will be crucial to the global energy transition. The compact has been backed by the Australian Government's recent A$2 billion commitment to the new Hydrogen Headstart program to ensure that Australian remains in the race to become a global clean energy superpower.

For several decades, robust investment treaty protections were seen as an important tool for attracting foreign investment, and for protecting domestic investors abroad. This is due to investment protections afforded under investment treaties, which effectively restrict the ability of governments to act in certain ways that may impact the economic interests of foreign investors who seek to invest, or who have invested, in those countries.

However, this traditional view is increasingly being challenged due to the chilling effect investment treaty protections can create on government regulation. More recently, this has manifested in a concern about governments' ability to execute on their energy transition goals. The challenge is demonstrated by a series of recent cases where states were faced with investment treaty claims bought by traditional and renewable energy investors following changes in the states' energy policy.

Investment treaty claims can be brought pursuant to a legal mechanism included in some investment treaties which empowers foreign investors that have suffered certain adverse effects by reason of regulatory measures introduced by the host state of their investment to seek compensation by bringing a claim directly against the host state and having that claim determined by an independent panel of arbitrators. If the measure in issue breaches investment treaty protections, the investor may recover damages for both current and future economic loss (in other words, the measure of damages is not constrained by the usual contractual measure that we are accustomed to in common law jurisdictions).

The challenges emanating from the current international investment treaty regime in the context of the energy transition are multi-faceted in that the regime allows claims to be pursued in response to both fossil fuel phase-outs and policies promoting investment in renewable energy. For example:

- German energy companies Uniper and RWE, owners of coal-fired power plants in the Netherlands, have brought investment treaty claims against the Netherlands in connection with the Dutch government's commitment to reduce the capacity of its remaining coal-fired power stations by 75% and implementing a package of measures to reduce Dutch emissions.[3]
- The UK-headquartered oil and gas company Rockhopper Exploration was successful in its investment treaty claim against Italy in which it challenged Italy's rejection of Rockhopper's application for an offshore exploitation concession based on a new law that introduced a complete ban on offshore drilling in Italy. An arbitral tribunal held in August 2022 that the rejection of the application was an immediate and complete deprivation of Rockhopper's investment in Italy and constituted an expropriation under the applicable treaty (the Energy Charter Treaty).

1 Austrade, 'Foreign investment helping Australia transition to a green future', 18 August 2021.

2 International Energy Agency, 'Net Zero by 2050: A Roadmap for the Global Energy Sector', May 2021.

3 Uniper has since withdrawn the ECT claim to secure a bailout agreed with the German government in the midst of financial difficulties following the drop in supplies of Russian gas. The RWE claim is currently pending, despite a judgment handed down by a German court in September 2022 declaring the ECT claim to be inadmissible under EU law on the basis that the ECT does not extend to intra-EU investor-state disputes.

On the other hand, there have been myriad instances of investors challenging decisions by states to scale back subsidies and other financial incentives originally introduced to attract investment in renewable energy projects. Spain alone has been the respondent in dozens of investment treaty claims after it had retracted some features of its solar energy incentives regime, with many investors arguing that this contravened their treaty-protected 'legitimate expectations' that the favourable regulatory framework would remain in place.

Developments such as these necessitate a close examination of the role investment treaties play in promoting renewable energy investments, and the relevance of investor-state dispute settlement as a risk mitigation tool for foreign investors in renewable energy projects. Several empirical studies have recently been completed or are currently underway looking at these issues. There are also ongoing discussions regarding reforms of the international investment treaty regime, so as to enable it to expedite the energy transition by protecting both foreign investment and climate change regulation.

Several options have been proposed by way of reform. On one extreme, some have called for an abolition of the investment treaty system – although a growing consensus seems to be that the regime (in some form) must be preserved in order to incentivise the investment required to achieve the clean energy transition. If the investment treaty regime is to be preserved, the existing investment treaties may be amended (and new treaties negotiated) to exclude, or enable Contracting Parties to exclude, protections for fossil fuels in their territories. Alternatively, provisions may be negotiated that protect Contracting Parties' ability to introduce more ambitious regulations to mitigate climate change, to the extent these are adopted in good faith and are capable of resulting in emissions reduction. Other proposals include amendments to substantive treaty protections by, for example, clarifying that investors will not be protected when foreseeable climate policies are adopted by host states to comply with their Paris Agreement targets, or when host states discriminate between projects based on their climate impact.

Apart from substantive reforms, some states may opt for limiting access to investor-state dispute settlement. Perhaps in response to experience from overseas, Australia's Federal Government seems to be steering away from dispute settlement provisions in its investment treaties that allow direct claims by investors – in November 2022, shortly after a new Federal Government came to power, Australia's Trade Minister announced that the Government would "not include investor-state dispute settlement in any new trade agreements".

The reality is, however, that while there are a number of alternatives being advanced (including, for example, the establishment of a multilateral investment court), in the absence of an investment treaty including an investor-state dispute settlement mechanism, investors may be left with only domestic (which are limited) or state-to-state dispute resolution options (which are heavily dependent on the political will of the investor's home state). That is typically an unattractive and unrealistic option for most private entities – and one that does not seem to take advantage of the investment promotion potential of investment treaties which is particularly important in the context of the energy transition challenge.

How the anticipated reforms unfold will be important to cross-border investors in new energy projects. Investment treaties that contain investor-state dispute settlement mechanisms can and do play a part in the management of risk for foreign investors. Renewable energy investors will be well advised to explore how best to structure their investments to avail themselves of the most robust investment treaty protections. At the same time, investors with existing investments should consider how amendment or termination of investment treaties which might have underpinned their investment decisions will affect their future ability to enforce treaty protections.

While the ultimate characteristics of a reformed investment treaty regime remain uncertain, it is clear that changes are on the horizon and that they will impact the manner in which the interests of foreign investors are protected as traditional energy sources get replaced by renewable ones.

> "Renewable energy investors will be well advised to explore how best to structure their investments to avail themselves of the most robust investment treaty protections.

07

Dynamic due diligence: managing new and emerging acquisition risks

By **Andrew Lumsden,** Partner, **Gaynor Tracey**, Partner, **James North**, Head of Technology, Media and Telecommunications, **Dr Phoebe Wynn-Pope**, Head of Responsible Business and ESG, **Rhys Jewell**, Head of Tax, **Eugenia Kolivos**, Head of Intellectual Property, **Madeleine Kulakauskas**, Special Counsel and **Michael Murdocca**, Lawyer

Recent well-publicised incidents of cyberattacks, breaches of whistleblower requirements, environmental, social and governance (ESG) issues, breakdowns in governance of tax risk, rapid developments in artificial intelligence (AI) and associated intellectual property (IP) issues, and an increased government focus on supply chains are demanding a more dynamic approach to M&A, both as a driver for acquisitions and as a fundamental requirement to better manage acquisition risk.

In one sense, this is not new – M&A professionals have always known that acquisition due diligence needs to be bespoke. What has changed, however, is the list of matters that can have a material impact on the value of that target post-acquisition and on the buyer's own brand.

Unsurprisingly, buyers are focused on how they can best capture opportunities and achieve maximum value while also assessing a heightened and expanded risk matrix. This may take the form of straight risk assessment or integration diligence to dovetail the acquisition with their own processes.

Below is a discussion of new and emerging trends in cyber security, ESG, supply chain management, tax risk, AI and IP that require greater attention in acquisition due diligence.

Cyber security

In the field of cyber, buyers must be diligent in assessing cyber risks during due diligence.[1] Any vulnerabilities in the target's IT systems may be exploited by malicious actors, and buyers should be conscious that companies are often unaware that they have suffered a cyberattack for many months after it occurs.

A failure to identify a cyberattack during due diligence will put the buyer's own systems at risk when completion of the transaction occurs. Further, the buyer may well become liable for significant penalties imposed by regulators on the target (including under the *Privacy Act 1988* (Cth)) and susceptible to shareholder or consumer class actions. In addition, buyers should review the technical defences of the target and the robustness of its incident response plans and other organisational frameworks to prevent and recover from cyber incidents.

ESG

Now widely accepted as a key consideration for dealmakers on acquisitions, ESG due diligence goes beyond compliance to include a qualitative review of systems and processes that address underlying ESG risk management. Some buyers use ESG due diligence as a tool to protect existing ESG portfolios that require certain ESG thresholds to be met in any new deal. Others see ESG as an opportunity for value add and value creation and, in these cases, ESG due diligence is much more than a box ticking exercise.

Poor ESG decisions and processes can have reputational, financial and legal consequences for the buyer. Buyers are looking for due diligence that includes a distinct ESG focus and is multi-disciplinary across advisers. That due diligence must be designed to both understand the risks and to identify value opportunities.

Supply chain management

The impact of 'homecoming' and 'decoupling' on the target and its key suppliers and customers is on the rise. Increasingly, we are seeing government industrial policies that are designed to build redundancies and resilience in supply chains both at home and in 'friendly' destinations to reduce the impact of potential conflict and economic coercion.

These friend-shoring commitments have the potential to be extremely important to some industries. Through the Quadrilateral Security Dialogue, Australia, India, Japan and the United States are building resilient supply chains for COVID-19 vaccines, semiconductors and emerging and critical technologies, including those related to clean energy.

Tax risk

Tax risk in the context of M&A due diligence is well known. But like so many other disciplines, the increasing emphasis on the application of the ESG lens requires buyers, more than ever, to focus on tax risk from the perspective of a number of stakeholders, including investors, employees, customers and regulators. These stakeholders have a heightened interest in a company's social contribution by way of complying with its tax obligations.

The risk of reputational and financial contagion to a buyer's existing business in an era of increased tax transparency and the attention given to specific risk areas (particularly in areas of interest to the Australian Taxation Office such as transfer pricing, research and development and intellectual property), should not be underestimated. Tax due diligence now requires a more nuanced and qualitative approach (rather than just the traditional quantitative exercise) and buyers are more regularly asking advisers for an assessment of the appropriateness of the target's internal tax function, the approach to tax risk management and governance more generally, and the process adopted for the selection of suitably expert and reputable tax advisers.

> It is clear that effective and focused due diligence has the potential to create, preserve and identify value in the acquisition process.

1 See 'Getting incident response right in a changing cyber threat environment' on page 13 of this publication.

AI

Another emerging area requiring greater attention in acquisition due diligence is how the target business is using AI. This is made more difficult by the limitations of the existing legislative environment, which is not designed to address or regulate non-human operations.

In an M&A context, buyers need to recognise the uncertainties of the use and development of AI, and test how the target is using AI, in particular:

- the complexities of what it means to 'own' AI and AI-generated content to ensure that proprietary or intellectual property rights can even be established in the first place and then that they are capable of transfer under a sale agreement; and
- to understand the potential existing risks in a business using AI (e.g. in businesses that are data mining, establishing that no copyright or other intellectual property rights are being infringed in this process).

Buyers also need to understand the future risks of using AI when legislative reform is pending but unknown. This includes understanding the impact on businesses if Australia follows the risk-based approach to AI regulation adopted by the EU or whether it will carve its own path. Existing and future risks need to be properly understood to ensure they translate to the bottom line and are reflected in the deal terms.

IP

In addition to the IP challenges identified in the AI context above, the focus on ensuring the target business owns the relevant know-how, methodologies and other key IP required to continue business operations remains an ongoing challenge in an environment where many organisations outsource the development and ongoing management of key systems, processes and works.

Ensuring key IP has been developed by employees of the target business within the scope of their employment remit or else appropriately assigned into the target business, with relevant moral rights consents secured, remains a continuing area of due diligence focus.

Key considerations for M&A professionals

Having a strong understanding of these new and emerging risks and weaknesses provides a buyer with the opportunity to build and strengthen the saleability and value of the target post acquisition. At a macro level, an acquisition thesis needs to incorporate all different types of risk, but these new risks require a particular focus and a deep understanding of how the transaction will fit and be consistent with the overall strategy of the buyer.

By building consideration of these new issues into the M&A process, acquirers can find assets that address existing issues in the acquirer's business, for example, supply chain vulnerability. Conversely, M&A deal teams and boards are increasingly looking to identify whether new businesses have the potential to create a contagion, undermining the existing business by introducing new risks to the acquirer's business.

Due diligence can of course take many forms but should be undertaken with subject matter expertise and a clear understanding of the interrelation between the myriad risks. Many of these risks require a careful understanding of a wide variety of issues to ensure any risk profile is rigorous and provides the acquirer with an accurate picture in the acquisition documents. In some cases, there may be issues that need to be remedied or certified as conditions precedent to ensure the matters are addressed before completion. In other cases, issues arising at the time of purchase may create opportunities for value creation as the buyer works with the new acquisition to build and strengthen performance.

It is clear that effective and focused due diligence has the potential to create, preserve and identify value in the acquisition process. The nature of many of these risks means this will need to be a bespoke process, both in terms of understanding the underlying issues that the target business faces and how those challenges need to be addressed through appropriate policies and procedures.

Contacts

Abigail Gill

Head of Investigations and Inquiries

+61 3 9672 3262
+61 434 354 188
abigail.gill@corrs.com.au

Eugenia Kolivos

Head of Intellectual Property

+61 2 9210 6316
+61 407 787 992
eugenia.kolivos@corrs.com.au

Adam Stapledon

Head of Banking and Finance

+61 2 9210 6478
+61 414 225 650
adam.stapledon@corrs.com.au

Gaynor Tracey

Partner

+61 2 9210 6151
+61 423 859 363
gaynor.tracey@corrs.com.au

Andrew Lumsden

Partner

+61 2 9210 6385
+61 418 110 665
andrew.lumsden@corrs.com.au

James North

Head of Technology, Media and Telecommunications

+61 2 9210 6734
+61 405 223 691
james.north@corrs.com.au

Andrew Stephenson

Head of Projects

+61 3 9672 3358
+61 498 980 100
andrew.stephenson@corrs.com.au

Katrina Sleiman

Partner

+61 2 9210 6246
+61 405 525 538
katrina.sleiman@corrs.com.au

Dr Louise Camenzuli

Head of Environment and Planning

+61 2 9210 6621
+61 412 836 021
louise.camenzuli@corrs.com.au

Dr Phoebe Wynn-Pope

Head of Responsible Business and ESG

+61 3 9672 3407
+61 418 526 918
phoebe.wynn-pope@corrs.com.au

Mark Wilks

Head of Commercial Litigation

+61 2 9210 6159
+61 419 387 288
mark.wilks@corrs.com.au

Rhys Jewell

Head of Tax

+61 3 9672 3455
+61 407 318 052
rhys.jewell@corrs.com.au

Michael do Rozario

Partner

+61 2 9210 6566
+61 416 263 102
michael.do.rozario@corrs.com.au

Sandy Mak

Head of Corporate

+61 2 9210 6171
+61 412 087 712
sandy.mak@corrs.com.au

Nastasja Suhadolnik

Head of Arbitration

+61 3 9672 3176
+61 405 141 942
nastasja.suhadolnik@corrs.com.au

Sarah Clarke

Partner

+61 3 9672 3388
+61 408 323 426
sarah.clarke@corrs.com.au

CORRS
CHAMBERS
WESTGARTH

Sydney
Melbourne
Brisbane
Perth
Port Moresby

corrs.com.au