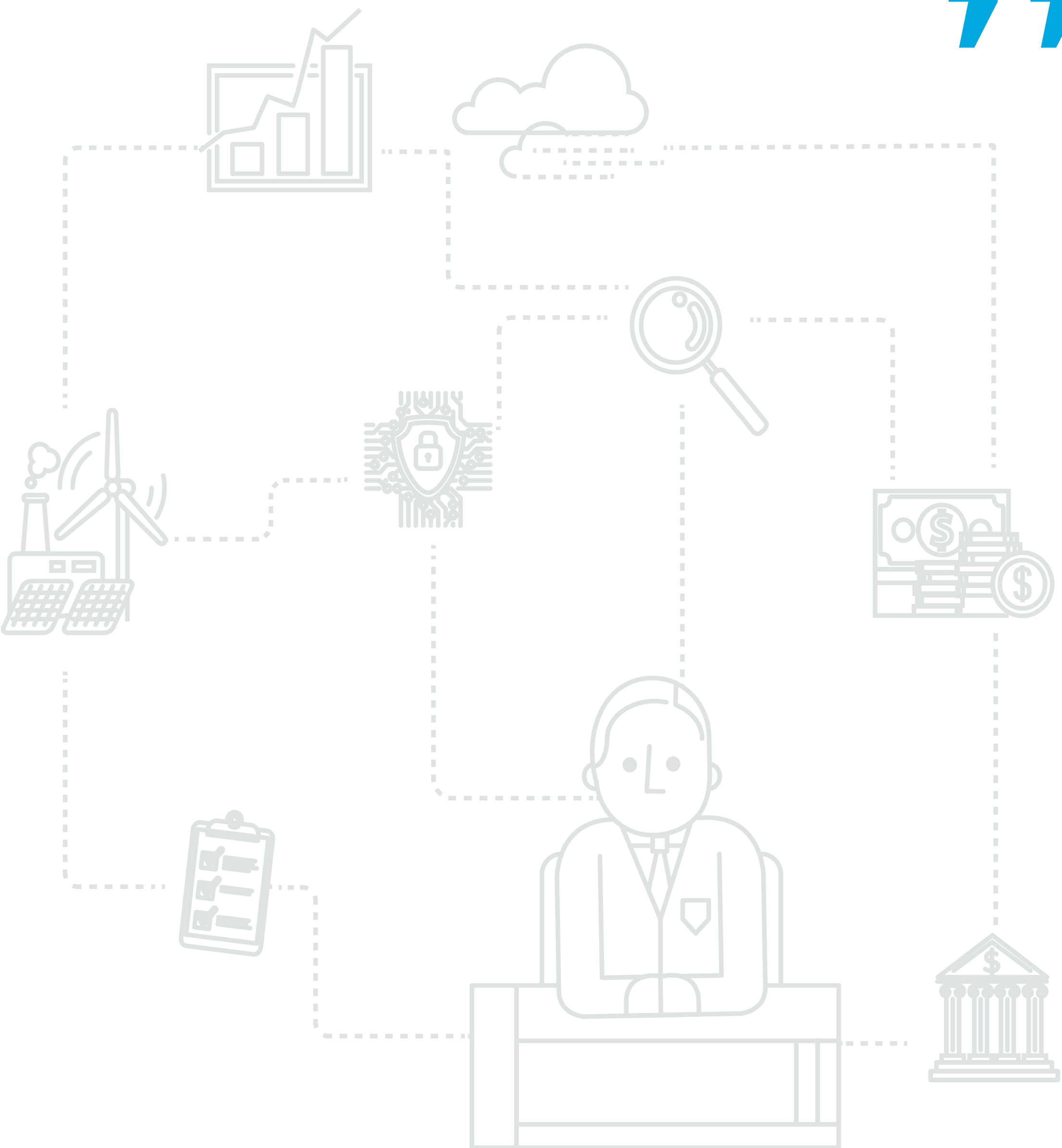
BEYOND COMPLIANCE:
Why more non-financial factors are keeping directors up at night

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

Celebrating 100 Years in Australia Est.1922

RSM

> **Directors face increasing expectations that they will not just uphold a duty of care to their shareholders, but also other stakeholders including employees, customers and local and global communities, and the environment.**



CONTENTS

BEYOND **COMPLIANCE**

Gone are the days when directors were merely responsible for mitigating balance sheet risks and ticking off on compliance.

The overriding duty of a director is to act in the best interests of the company, honestly and in good faith, and with due care and diligence. [1,2]

While this remains true, the scope of what constitutes an organisation's best interests is broadening significantly, and can vary depending on the industry, stakeholders and regulatory regime.

In setting the risk appetite, strategy and culture of an organisation, directors are faced with a growing number and scale of contemporary and emerging risks – beyond the balance sheet.

> Directors face increasing expectations that they will not just uphold a duty of care to their shareholders, but also other stakeholders including employees, customers and local and global communities, and the environment.

Australia's corporate watchdog, the Australian Securities and Investments Commission (ASIC), has highlighted the importance of non-financial risk management. In the wake of the Banking Royal Commission, then-Chair of ASIC James Shipton told an Australian Institute of Company Directors' (ACID) Essential Director Update that if mismanaged; non-financial risks had "very real financial implications for companies, their investors and their customers – particularly if not identified and prioritised early enough".

"The truth is that all risk ultimately has financial consequences," he said.[3]

It is no longer sufficient to simply follow the law. Companies are increasingly judged on whether they have acted in line with societal expectations and in support of ethical values.

For organisations, compensation claims, litigation, reputational damage, and the loss of social licence can all become the costly consequences of inattention to non-financial risks.

[1] https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp2122/Quick_Guides/DirectorsDuties
[2] https://asic.gov.au/regulatory-resources/insolvency/insolvency-for-directors/
[3] https://asic.gov.au/regulatory-resources/find-a-document/reports/corporate-governance-taskforce-director-and-officer-oversight-of-non-financial-risk-report/foreword/

Amid a rising tide of public and regulatory scrutiny alongside shareholder and stakeholder activism, director's individual responsibilities are in the spotlight like never before.

For example, the revised Work Health and Safety regulations put the financial penalties on the directors where the organisation is found to be in breach.

> Some commentators have suggested the responsibility on directors has shifted to impose **personal liability on directors**, potentially judged on the basis of what they should have known or done, instead of what directors actually knew or did.

Directors of the world's biggest iron ore miner, Rio Tinto, came under significant and enduring internal, public and investor scrutiny following the 2020 destruction of ancient rock shelters in Juukan Gorge and an internal investigation that found no single person accountable.

Reputational damage has come from stakeholders or even beneficiaries turning their backs on corporate sponsors. Recent examples include the parting of ways between Netball Australia and Hancock Prospecting, Cricket Australia and Alinta Energy ending their partnership from next summer, and Perth Festival and Chevron to cease their enduring sponsorship deal from 2023.

Further, in an emerging area of litigation internationally, environmental campaigners are targeting directors like never before, alleging it is "reckless" not to incorporate the known risk of climate change into company strategy.[4]

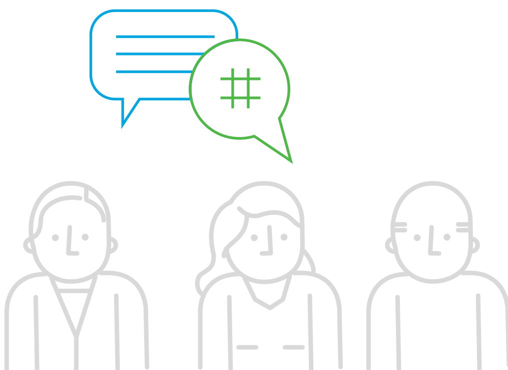
For boards, responding to these challenges requires new director knowledge and skills, as well as obtaining external advice from experts. It is to be expected that these issues will be more regularly elevated to board level for input and guidance.

This report sets out some of the biggest contemporary issues facing boards.

Climate change, cyber security, digital transformation, ESG and global risks are among the challenges and opportunities in focus.

These echo the top-of-mind issues for Australian directors. The Governance Institute of Australia this year found the top external challenges for boards in 2025 will be climate change, the ongoing fallout from COVID-19, economic instability, technological disruption and cyber security risk.[5]

We acknowledge the challenges ahead. But by approaching this with an attitude of continuous learning, curiosity, adaptability and openness, we are confident Australian directors have the attributes and knowledge to set the strategies required to weather these storms.



[4] https://cpd.org.au/2019/03/directors-duties-2019/

[5] https://www.governanceinstitute.com.au/news-media/media-releases/2021/nov/a-director-s-roadmap-to-2025-governance-institute-launches-board-of-the-future-report/

one

CLIMATE **CHANGE**

WHAT YOU NEED TO KNOW

The Australian Government has legislated an emissions reduction target of 43 per cent from 2005 levels by 2030, and net zero emissions by 2050. The Australian policy to achieve net zero includes significant upgrades to Australia's energy grid, the development of a "green metals" industry, electric vehicle take up and new technologies.

Likewise, there is growing momentum for the introduction of mandatory climate reporting for large businesses with a harmonised global standard for sustainability reporting. **While the ASX Corporate Governance Principles and Recommendations** currently recommend listed entities disclose material exposure to environmental risk, it is expected that the International Financial Reporting Standards will be upgraded to include a specific obligation to report climate-related disclosures, based on the recommendations of the Task Force on Climate-Related Financial Disclosures (TCFD).

At AGMs, the **Say on Climate** movement has also focussed on forcing companies to report emissions disclosures and reduction plans. Legal challenges also abound. There is an Australian legal bid to **force the Commonwealth Bank** to reveal board documents that detail finance arrangements for oil and gas projects, as well as the threatened claim against Shell board members personally from UK activist group, ClientEarth, alleging they failed to manage climate risk.

The Climate Change Act was passed in September 2022.

- While there are no specific obligations on companies yet, the laws set the framework for decarbonisation targets and emissions reductions. New project approvals may be considered in light of their emissions profiles, and sector-specific regulations may emerge.
- ASIC and the Australian Competition and Consumer Commission (ACCC) have declared they will focus on investigating claims of "green-washing", the exaggeration of the organisation's positive environmental impacts.
- Companies are being targeted with legal challenges to their operations or their environmental claims, such as the Australian Centre for Corporate Responsibility case against **Santos**.

Climate change has emerged as one of the key issues facing global society. The 2022 United Nations Climate Change Conference, COP27, reiterated the need to make all efforts to decarbonise as it announced a plan for a "loss and damage" fund for developing nations. Despite calls for increased action, the decision did not call for a phase down of fossil fuels. A group of 18 nations including Australia, the US, UK and France signed an initiative to achieve net zero public sector emissions by 2050.

No longer just a scientific issue, climate change is a social, financial, and regulatory issue that is expected to impact all aspects of society into the future. Businesses and governments are increasingly expected to respond with transition plans to cut emissions and develop low-carbon options. Best-practice governance includes incorporating climate into strategy with board-level oversight, conducting climate scenario analysis, risk management and processes, emissions tracking and disclosures, and science-based target setting.

ANALYSE AND MITIGATE THE RISKS OF CLIMATE CHANGE

Climate change risks and opportunities should be assessed across your business operations and the supply chain.

There are operational risks. For example, how would your organisation reach communities during a natural disaster? What mitigation is in place if elements of the business's supply chain were impacted by climate-related events in other countries?

There are also transition risks as we progress to a low-carbon economy. Could customers reject your products or services on climate grounds? Would investors seek a net zero alternative? Or could activists threaten project developments and your social licence? What additional regulation could be imposed? These are all issues for directors to consider.

Directors should oversee comprehensive risk assessments to analyse the broad range of possibilities from climate change, and the transition to a low-carbon future. This could include scenario analyses, both qualitative and quantitative, to set the foundation for future strategy and risk management. This framework will also help to reduce the uncertainty surrounding change. Response to climate impacts should be fully integrated into strategy and business decisions.

SET EMISSIONS REDUCTIONS TARGETS IN LINE WITH SCIENCE

To become a leader on climate requires action. Ambitious Australian corporations have committed to the Science-Based Targets initiative to reduce their emissions in line with the Paris Agreement, including Dexus, Goodman Group, Intrepid Travel, Investa Office Management, Mahindra Automotive Australia, Origin Energy, Taylors Wines, Telstra and Woolworths Group.

400+

businesses certified as Climate Active

45%

of directors have embedded climate change into risk management frameworks

Strategies should address both operational and supply chain emissions. Operational emissions reductions can be achieved through reducing energy waste, sourcing renewable energy, electrification of buildings and transport and offsetting residual emissions. Globally, targeted interventions to reduce your supply chain (scope 3) emissions are currently considered best practice.

> Care should be taken to make responsible public statements about the sustainability of services and products, especially financial products, given regulator crackdowns on **green-washing**. The ACCC has warned it is alert to false and misleading claims in this area, a potential breach of the Corporations Act.

NEXT STEPS

Educate directors and allocate responsibilities

Almost half the directors (46%) who responded to an AICD and Climate Governance Initiative survey in 2021 wanted to do more about climate change but didn't know where to start. Education and training can deepen awareness and understanding.

Conduct scenario analysis and build a strategy

Scenario analyses map out the possible implications of each climate scenario on an organisation. Include directors and executives to understand the process, outcomes and impact.

Report climate metrics and set targets within operational plans

Knowing the baseline is essential for future climate action. Climate consultants can assist to assess current settings and plan a low-carbon transition strategy. Plans could include a communications plan to stakeholders that is clear, defendable and supported by actual actions taken in the organisation.

Set KPIs and incentives for achieving targets

Asia-Pacific companies that incentivised sustainability-related targets for their executive and management teams were four times as likely to achieve them, according to a report by CDP.

Assess the opportunities

Assess the emerging opportunities from the climate change transition. This could be the attraction of institutional investment, developing sustainable products and services, or benefits from lower-emission energy sources.


01110001
00101000101001
0111000110110100110
00011010100111011111000

two

CYBER
SECURITY

WHAT YOU NEED TO KNOW

Cyber security has emerged as a critical business risk globally. The Australian Government this year doubled the number of critical infrastructure assets subject to its Security of Critical Infrastructure laws.[6] Added to defence, health, utilities and other infrastructure, the increased regulatory oversight and requirements now include sectors such as critical broadcasting, data storage, banking, superannuation and insurance, hospitals and education, freight, energy and aviation. The laws impose new obligations on responsible entities to devise and hold a critical infrastructure risk management program, as well as greater cyber security obligations.

In the financial sector, directors should already be aware of their obligations. APRA's Prudential Practice Guideline CPS 234 requires information security controls to protect systems, with "heightened expectations" for directors to safeguard the information held.

The Security Legislation Amendment (Critical Infrastructure Protection) Act came into force in April, 2022.

[6] https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-security-legislation-amendment-critical-infrastructure-protection-act-2022.pdf

- It obliges "regulated entities" to report cyber breaches to the government and register as critical infrastructure assets.
- Critical infrastructure will also be required to develop and implement a cyber security risk management program for their assets to identify and mitigate risks, minimise the impact and develop governance and oversight.
- Cyber security risk is becoming critical for directors, given rising regulatory oversight and high-profile attacks.

CYBER IS, UNDERSTANDABLY, KEEPING DIRECTORS UP AT NIGHT

The cyber security threat environment is rapidly escalating. Ransomware, extortion and data theft are major and growing crimes that can not only bring operations to a halt within minutes, but leave businesses exposed to serious enduring financial and reputational damage. A breach that cripples an organisation's IT capabilities can quickly bring financial and operational systems to a halt. For this reason, cyber security should be understood, monitored and measured to ensure ongoing business continuity.

72%

of directors cite cyber security as a high priority for the board

43%

of boards did not receive any cyber security training

The Australian Cyber Security Centre reported a 13 per cent increase in cyber crime in the 2021 financial year, with self-reported losses from those crimes totalling more than $33 billion. The cyber criminal world has reached an industrial scale, with an ecosystem of criminal businesses offering initial hacks, data for sale, ransomware-as-a-service and extortion. Enabled by remote work and the availability of cryptocurrency, extortion has become a method of choice for high-profile attacks.

Boards are becoming increasingly accountable. In May 2022, the Federal Court found RI Advice breached its financial service license obligations by not having adequate cyber security risk management systems, following a series of cyber attacks, in what was a precedent in cyber governance. The Optus cyber breach in September 2022 and the ransomware attack on Medibank in October 2022 also added pressure to board oversight of cyber risk.

> "Directors need to have a clear understanding of what cyber risk they are carrying and find out if it aligns with their risk appetite."
>
> *Ashwin Pal, Director, Cyber Security & Privacy Risk Services*

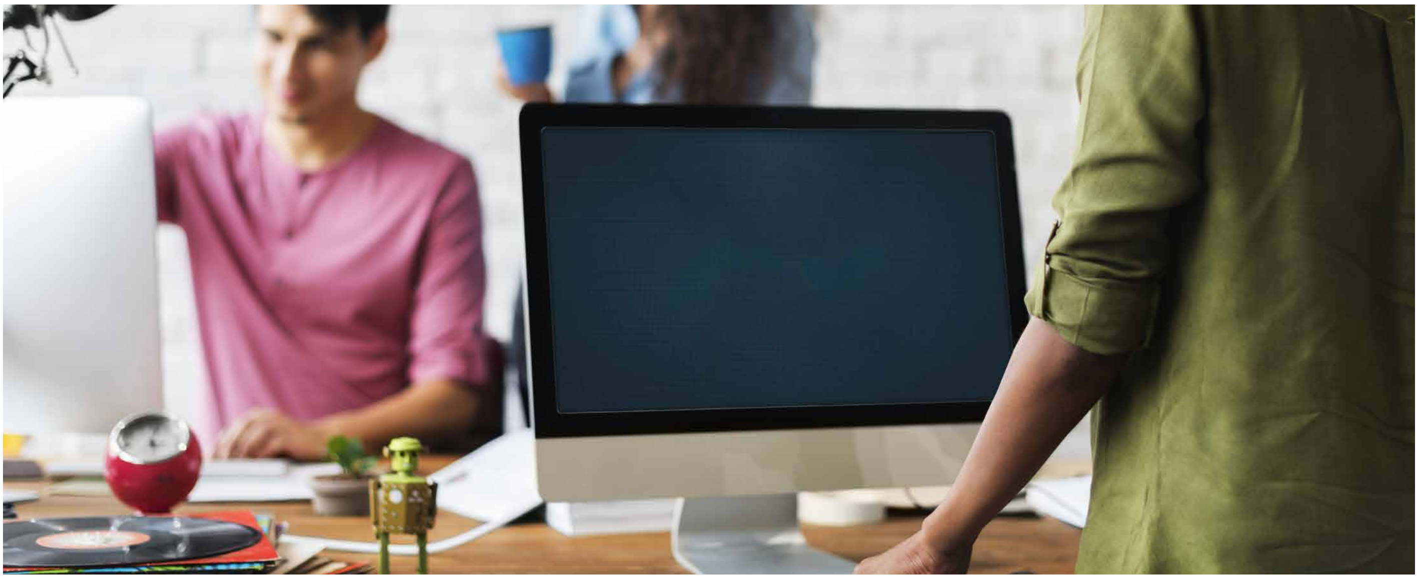
Directors are being personally targeted. Using information gleaned from social media profiles, cyber criminals are seeking to infiltrate the personal accounts of directors and executives in order to exert maximum pressure on the organisation. Further, directors and their oversight responsibilities are in the crosshairs of regulators that could attribute director acts or omissions as a contributor to liability in the event of a cyber breach.

ASSESS THE RISKS, MITIGATE, AND GET ASSURANCE

Amid the growing risk, boards have to assess their current organisational cyber posture and risk tolerance. Consider:

- What are the organisation's critical systems and assets, the 'crown jewels', and where is that data stored?
- What is the potential impact and probability of a cyber incident?
- What are the costs of protecting those critical systems?
- How should the overall risk be mitigated, accepted, or should processes change to change the risk?

While directors understand there is a strong and growing risk, there is a significant information gap to overcome. A University of New South Wales study found less than 1% of ASX100 company directors had cyber experience and 16% had general technology experience. Just 18% of ASX debutants in 2020/2021 mentioned cyber security, according to RSM research. Once educated, boards should establish management and mitigation strategies, challenge management on the frameworks, and seek independent assurance that it is appropriate.



NEXT STEPS

Make cyber a priority for directors

Cyber security considerations should be raised to board level, not just in the risk or technology committee. A survey of directors found one in four organisations had cyber as a specific committee focus.[7]

Develop a cyber security strategy

Directors face an increasing responsibility to have a cyber strategy, against which progress is monitored. For organisations captured under the Security of Critical Infrastructure (SOCI) Act, they are also required to "establish, maintain, and comply with a risk management program", including identifying and mitigating material risks.[8]

Make cyber security a key aspect of risk management

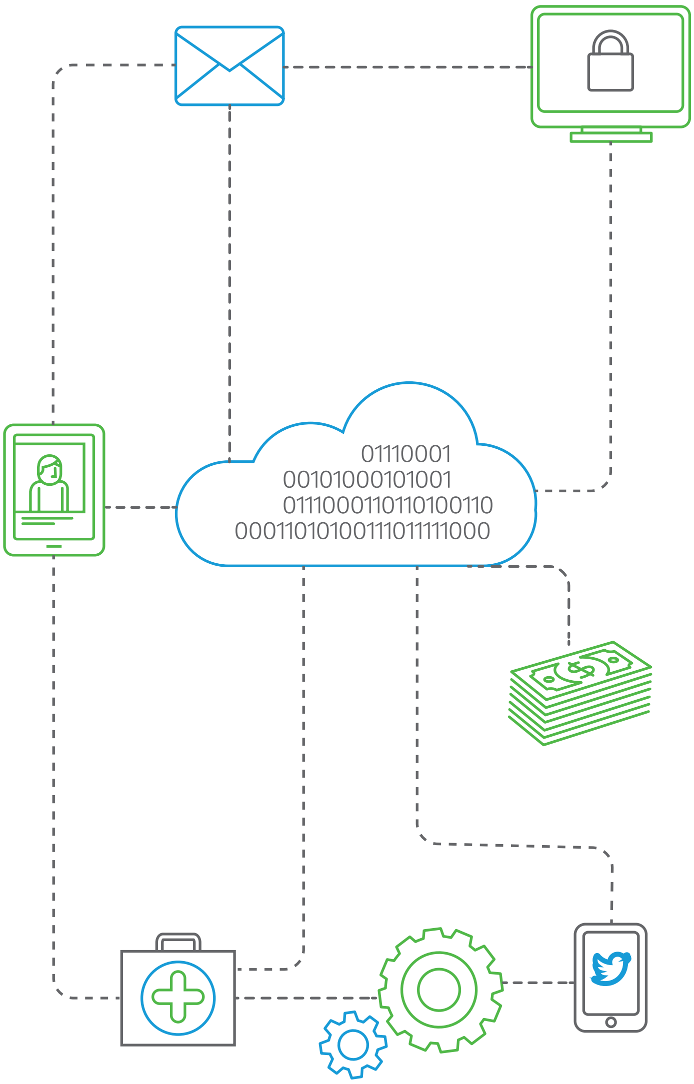
Cyber security should be embedded into the risk management framework across the organisation. Directors should monitor threats and vulnerabilities to the organisation regularly and in a structured way to challenge how effectively the risks are being managed.

Lead a cyber resilient culture

While technological defences can help, cyber security breaches often come down to one individual's choice to click on a link or not. This means a cyber aware culture must be in place across the entire organisation.

Expect a cyber attack and plan for it

All individuals, businesses and organisations are vulnerable to cyber attacks. Simulation exercises, and scenario and penetration testing can highlight the gaps in cyber resilience. This can also prompt updates in response plans, communications plans and other operational plans. The results from these exercises should be communicated to the board.



[7] https://www.aisa.org.au/common/Uploaded%20files/Research/FINAL%2008299-3-5-Cyber-Security-Report-30pp-v3B.pdf
[8] https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-security-legislation-amendment-critical-infrastructure-protection-act-2022.pdf

three

DIGITAL **TRANSFORMATION**

WHAT YOU NEED TO KNOW

Australia has an ambition to become a top 10 digital economy and society by 2030.[9] The Digital Economy Strategy is aimed at enabling all businesses to be digital, all Australians to have access to digital skills and technology, all government services delivered online, and integrated data and technologies that make life easier.

The COVID-19 pandemic and restrictions catalysed a steep change in digital transformation. Nine out of 10 businesses increased their digital uptake from 2020 to 2022. But analysts continue to warn that Australian businesses will need to continue to transform their operations, supply chains and value propositions in order to harness the benefits of the digital era. Consumers want more individualised digital options, faster, with less friction, all while demanding increased security and privacy.

As the digital transformation rolls out, this will prompt major changes to ways of working, business models and competitive environments including the integration of automation, machine learning and deep learning. This will require new skills and oversight from companies and boards. Regulation is also set to increase, notably the Privacy Act. The privacy provisions laid out in the Consumer Data Rights Rules, currently implemented in banking, are also expected to be expanded to other industries such as energy, telecommunications, non-bank lending and consumer sectors.

As the world becomes more connected, organisations will increasingly rely on digital transformation to meet business needs, regulatory requirements and customer expectations.

- The use of digital tools – and the data they collect – requires oversight to protect the organisation from privacy and reputational damage risks.
- The Australian Government has introduced legislation to increase penalties under the Privacy Act. The bill proposes to raise fines for serious or repeated incidents for major companies to up to $50 million, three times any benefit from information misuse, or 30 per cent of a business's Australian revenue in the relevant period. A broader review is underway.
- Directors should be aware of the place and scale of digital transformation, and the impacts it will bring.

[9] https://digitaleconomy.pmc.gov.au/2022-update/strategy-page.html

BUILD AN EVIDENCE-BASED APPROACH

Digital transformation has changed, and will change, all aspects of Australian society. Digital technologies have advanced more quickly than in any other period of human history, reaching into our healthcare interactions, banking apps and cloud-based business processing platforms. As artificial intelligence, automation and machine learning advances, the speed of change is expected to continue to accelerate. Data analysis can offer an evidence base for strategy. Even free and available datasets, such as the Census, can deliver insights for businesses on emerging local trends or needs.

> Boards need to make sure that when they are digitally transforming, they are doing so safely.
>
> *Darren Booth, National Head of Cyber Security & Privacy Risk Services*

Directors should consider where the company is on the data maturity curve. Most companies are at the level of descriptive analytics, that provides metrics on past events. The next stage, diagnostic analytics, can provide insights into the causation of events. Advanced use of data can provide predictive tools that can inform business or systems intelligence, and prescriptive analytics to optimise processes and offer genuine competitive advantages.

Directors need to ask: How is digital disruption impacting industries around you? What do the technologies mean for revenue generation? What do the technologies mean for revenue generation? What are the innovations affecting your company's performance and processes? How is technology enabling a better customer experience?

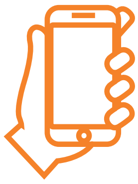
BUT TRANSFORMATION MUST BE DONE SECURELY

Data governance is critical, given the potential reputational and financial risks of breaches. Companies should be aware of their data systems and assess how these are managed. Ahead of more onerous obligations anticipated as the government considers boosting the Privacy Act, businesses should consider setting frameworks for data systems now.

Digital processes can also assist the busy director. Data dashboards visualise company information quickly, while offering granular detail if required. This can assist director oversight of financial, cyber security, compliance and ESG information at a glance. Real-time data use can also help understanding of track emerging risks and costs, supply and other metrics.

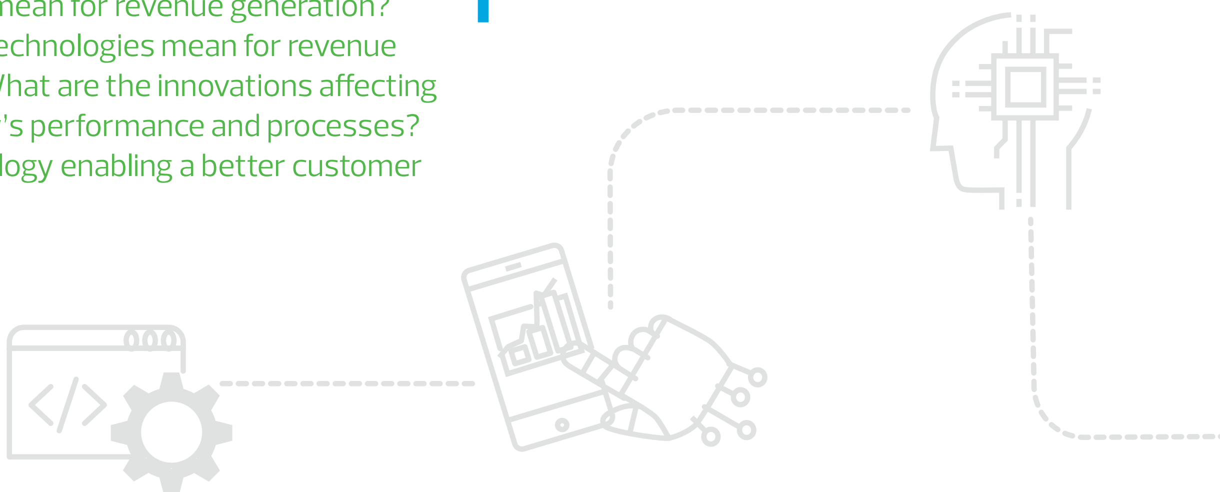
57%

growth in e-commerce in 2020-2021 to more than $50.5bn



$109bn

estimated value of digital activity in 2019-2020 in Australia



NEXT STEPS

Assess the level of digital literacy and maturity

Companies – and individual directors — have varying levels of data and digital maturity, a skill so necessary for future development. A 2021 survey of more than 1000 directors globally for HRB found 94% said they felt they needed more training, but only 58% had it.

Set a clear strategy to embed digital at the heart of the business

While the focus is often on cost savings, digital systems can also create new market opportunities,for example, through the use of data and a greater understanding of customer needs, and to improve cyber resilience. Almost four out of five respondents to a 2022 Governance Institute of Australia (GIA) survey said digital transformation was underway or on the radar.

Build the right team to oversee digital transformation

Digital experts within the leadership and director team can accelerate transformation. People with specialist knowledge can assist with the increasingly important governance and oversight of data management systems, as well as setting future plans. The GIA survey found 93% of respondents believed the board should be involved in tech issues.

Elevate reporting to board level

The GIA survey found senior management or the chief executive officers drive the digital transformation at two thirds of organisations. Forty percent report to the board at every meeting. Not only does this increase oversight, it also raises awareness.

Ensure ethical use of data

Privacy controls are hitting the headlines more and more. Data collection is emerging as a critical risk as cyber-crime increases in lock step with our tech reliance. Appropriate governance, including risk management, policies, codes of conduct and procedures are important to embed controls and maintain confidence.

four

ENVIRONMENT, SOCIAL **AND GOVERNANCE IMPACTS**

WHAT YOU NEED TO KNOW

Companies are coming under increasing scrutinity from regulators, shareholders and stakeholders regarding issues of environment, social and governance (ESG). This includes a broad suite of issues such as community relations, diversity and inclusion, appropriate wages, recruitment, work, health and safety policies, and alignment to stakeholder expectations and standards in terms of corporate culture. There is also critical local environment management, as well as the appropriate governance systems and processes to manage actions, decision making and risks of the organisation.

ESG reporting remains voluntary in Australia but **pressure** rising to make it **mandatory**, in the manner of Modern Slavery reporting. The growing value of ESG reporting, particularly in sectors such as mining and resources, is increasingly aligned with ongoing social licence to operate.

However, the importance of social licence is extending across most industries and was highlighted in the banking royal commission. Directors should understand the expectations of their stakeholders in responding to the various risks and opportunities of ESG, considering matters from ethical sourcing to staff wellbeing and its impact on the local community. Each organisations impacts and response will be unique to them and so need to be considered as such.

While questions over the consideration of environment and social impacts are a regular concern at annual general meetings, so is the diversity of boards themselves. The Governance Institute of Australia has called for greater board diversity, following research that showed 90 per cent of directors were from Anglo-Celtic backgrounds, 22 per cent were aged over 70 years, and 19 per cent of women held 48 per cent of the female positions.

- ESG issues are a key focus for investors, shareholders, regulators and other stakeholders, with an expansion of the issues subject to voluntary and in some cases, mandatory reporting.
- Directors' duties to act in good faith have been interpreted to include "preserving and enhancing" corporate reputation and doing "the right thing" instead of just what's legally required.
- The ASX recommends disclosure of any material ESG risks and management plans.
- Companies are increasingly facing activism on social issues.

CONSIDER LOCAL ENVIRONMENTAL FACTORS

What are the local environmental impacts of operations? Reporting should focus not only on climate and emissions, but also pollution, water and other local considerations that are relevant to communities. Poor environmental conditions often lead to negative consequences for local populations, extending this risk into the social aspects of ESG.

SCRUTINISE COMPANY CULTURE

> Directors should scrutinise the conduct of their organisations when it comes to their social performance, both inside and outside the company. Clear and consistent values should inform cultures and internal strategies and plans.

Safety for staff, as well as the community, is also critical to continuing operations, social licence and reputation. There are legal obligations for directors to ensure a safe working environment, including a workplace safe from bullying and harassment.

The landmark 2020 Australian Human Rights Commission's Respect@Work inquiry recommended the ASX Corporate Governance Council introduce sexual harrassment indicators for reporting. The inquiry also urged education to be developed for board members and company officers on good governance related to gender equality and sexual harassment. New laws introduced this year will put the onus on companies to establish and maintain frameworks for prevention, not just responding after the event.

Further, the Misconduct in the Banking, Superannuation and Financial Services Industry (Banking Inquiry) highlighted that the director's duty to pursue long-term advantage involved, "preserving and enhancing the reputation of the enterprise as engaging in the activities it pursues efficiently, honestly and fairly". Profit should not be pursued at all costs.

There are also ongoing "wage theft" claims that have become commonplace and costly. These all contribute to challenges for company recruitment and retention outcomes in a tight labour market.

> Directors should be looking at ESG in a strategic light. Starting from strategic planning, through the budgeting, objectives and measurements, ESG should be part of everyday business. There are benefits to companies to be on the front foot, instead of waiting for regulation.
>
> *Jacob Elkhishin, National Sector Leader in Energy, Resources and Sustainability*

INTEGRATE EFFECTIVE GOVERNANCE ACROSS THE ORGANISATION

Companies should respond to the risks in their industry and set mitigation strategies in place accordingly. What are the values and principles of the company? What are the environmental, social and governance priorities and material issues? Are there key issues where the organisation can lead? What are the upstream or downstream impacts of the operations or investments?

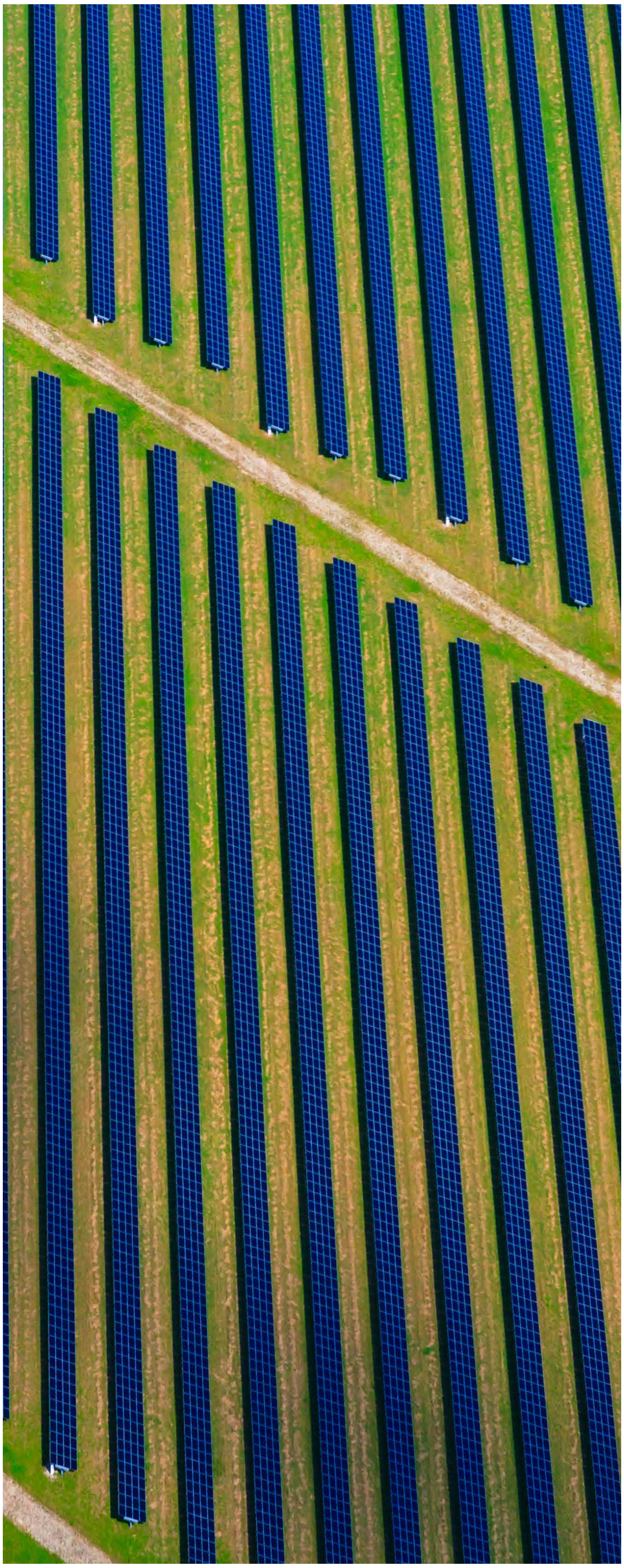
Once the priorities are in place, a framework for implementation, risk mitigation and stakeholder relations should be conducted, along with internal reporting. Industry bodies such as the AICD and GIA conduct regular updates on ESG issues.

$1.54 trillion

was the total value of investments managed in Australia under a "responsible investment framework"

80%

of Millennials say they would be more loyal to a company that helps them contribute to social and environmental issues



NEXT STEPS

Consider integrating ESG issues into strategic planning and risk management

ESG issues are essential to the long-term success of organisations. ESG should be included in conversations around risk appetite, included in strategic risk registers and integrated it into strategy and operations. Investment into ESG is booming, this poses opportunities and risks for organisations.

Assess the risks to business and external stakeholders

Directors should understand the potential risks around ESG, and how they are currently being managed. Does this align with the risk appetite set at the board. Who are the influential, and most highly impacted stakeholders across communities, and have appropriate stakeholder management plans being formulated? What are the environmental impacts, both locally, nationally, and globally?

Is there appropriate governance in place, including policies and internal procedures?

Ensure your systems and process are effective, and that your people have the skills, tools and resources to respond to the ESG changes.

Consider whether your social, recruitment and sexual harassment policies and procedures are up to date and in line with contemporary values Further consider whether the behaviours and actions of your teams align with these and your corporate values.

Set targets and incentivise

Common indicators for ESG include records of environmental incidents, fines or sanctions, any breaches, and safety reporting. For social factors, it could include executive remuneration linked to staff metrics, diversity and inclusion targets, OH&S performance, or professional development rates.

Report and disclose

The ASX advises that understanding a company's governance and accountability mechanisms provides insight to investors. Metrics should be disclosed with the standards applied to determine the materiality.

five

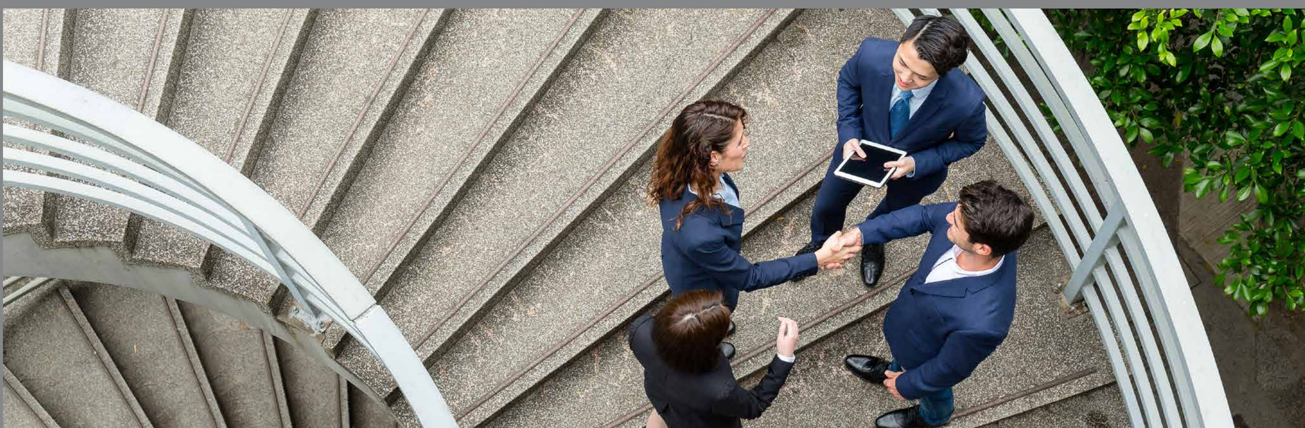
FUTURE **OUTLOOK**

WHAT YOU NEED TO KNOW

The darkest days of the global pandemic may now have passed, but the health emergency has given way to a new and emerging economic challenge. There is a growing fear the world will slip into a major economic downturn next year as Western economies including the United Kingdom, United States and Europe battle cost-of-living and inflation pressures, while China's economy continues to slow amid its zero-COVID policy. This global environment, coupled with the ongoing supply chain constraints, skills shortages and ongoing geopolitical turmoil, continues to build a challenging environment for director strategy setting.

In a dour **October World Economic Outlook Report**, the International Monetary Fund said the global economy was facing "steep challenges". "Global economic activity is experiencing a broad-based and sharper-than-expected slowdown, with inflation higher than seen in several decades," it said. President of the World Bank David Malpass went further at the **annual IMF and World Bank Group meetings** in October 2022 to say there was a "real danger" of a world recession in 2023. **IMF Managing Director Kristalina Georgieva** told the IMF and World Bank Group meetings she believed the current challenges were not transitory but are, more worryingly, a potentially dangerous "new normal". "What we see perhaps is a fundamental shift from the world of the last decades that was relatively predictable with strong rules-based international order, low inflation, low interest rates, to a world that is more volatile, more fragile, and with consequences that we have to wrestle with."

- The IMF says 2023 will "feel like a recession" for many people, with more than a third of the global economy to contract this year or next.
- It predicts inflation will peak in late 2022, but will remain elevated for longer than initially expected, reducing to 4.1% by 2024.
- High energy prices, a cost-of-living crisis, currency pressures, supply chain challenges and high borrowing costs are all impacting the global economy.



WHAT IT MEANS FOR AUSTRALIA

> Australian Treasurer Jim Chalmers has cautioned that while Australia is in a strong position to withstand a global downturn, the global economic situation presents a growing risk. "The global economy teeters again, on the edge – with a war that isn't ending, a global energy crisis that is escalating, inflationary pressures persisting, and economies slowing – some of them already in reverse," he said while handing down the Federal Budget in October. "All of this is now reflected in the updated forecasts for global growth – downgraded since the March Budget for this year, next year, and the following year."

Treasury forecasts Australia's economy will grow 3.25 per cent this financial year, but growth will slow to 1.5 per cent in 2023/24, a per cent lower than what was initially forecast in March.

The budget papers revealed Treasury expects inflation to peak at 7.75 per cent later in 2022, before softening to 3.5 per cent in 2023/24 and returning to the Reserve Bank of Australia's target range of two to three per cent in 2024/25.

AND A RECESSION WOULD ADD TO EXISTING CHALLENGES

Amid this gloomy outlook, many companies are currently dealing with a talent crunch, with rising wages, a lack of skilled staff and a zeitgeist heralding "the great resignation" raising concerns about their ability to service contemporary and future staff requirements.

Supply chain management has also become a critical and ever-changing issue, which is expected to continue amid the shifting geopolitical environment. Just-in-time supply chain practices evolved during the years of the pandemic to boost inventory levels, transforming some companies to adopt a just-in-case model. Onshoring key capabilities, such as defence and some technological supplies, is becoming a priority.

2.7%

global growth forecast for 2023, down from 6% in 2021 and 3.2% in 2022

$4 trillion

the IMF forecast for global output loss between 2022 and 2026

NEXT STEPS

Set a clear risk appetite

Different directors may have varying views about the future risk they are willing to hold. High consequence risks should be mapped out and appraised among the board, with a consistent approach embedded in the subsequent strategies.

Understand the skills required for business continuity

What is the outlook for those skills in the Australian economy? Where will the next generation of workers come from? Professional jobs growth is expected to increase 14.7% to 2026, according to the National Skills Commission.

Confirm a skills strategy for the long term

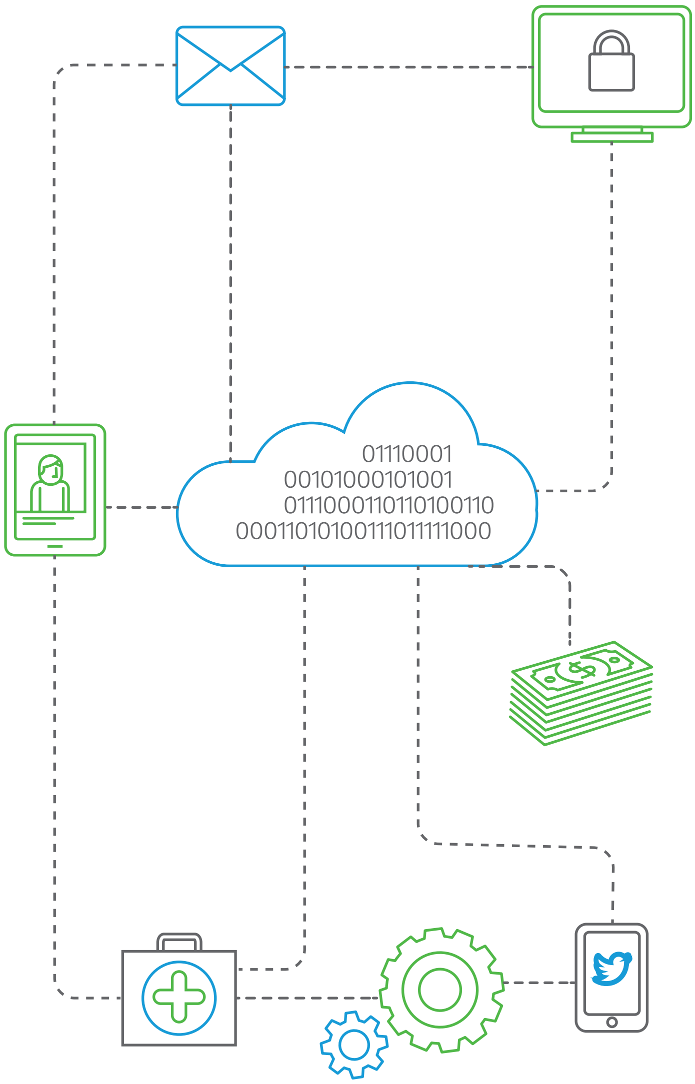
Are skills an emerging issue? Are alternative education and training options available? Is there a role for industry to increase training? More than 90% of future jobs will require post-school education.

Seek to establish supply chain resiliency

Understand how and where critical inputs are sourced, and whether increased resilience is necessary. Determine whether the supply chain for those parts fits the risk profile for the organisation.

Prepare for change

The pandemic highlighted the potential for sudden shocks and the need to prepare for crises, develop resilience and workplace changes.



ACKNOWLEDGEMENTS

These Partners who regularly advise board directors provide guidance in the following areas:

Cyber security
Ashwin Pal
Darren Booth

Data analytics
Matthew Cunneen

Culture
Pippa Hobson

ESG and sustainability
Tim Pittaway
Jacob Elkhishin