Governance Institute of Australia

Data governance in Australia

2023 Report

governanceinstitute.com.au

Contents

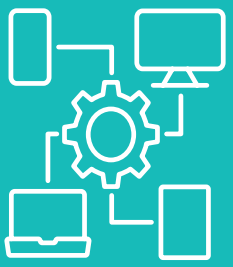
Key learnings

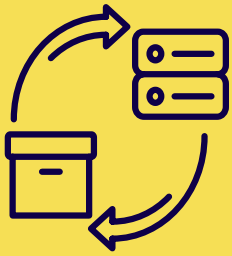
60%

Almost 60% say the board does not have an understanding of the organisation's current data governance challenges.

>50%

More than half of organisations do not have a data governance framework, mostly due to lack of capacity or resources.





1/3

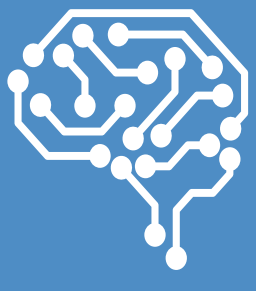
Just under a third of organisations regularly purge data, most common is annually

Cyber attacks

The standout risk around data governance is cyber attacks followed by emergent technologies and AI

Siloed data

Siloed data holdings, underestimating the value of data and not having proper data governance frameworks are key issues for organisations in 2023

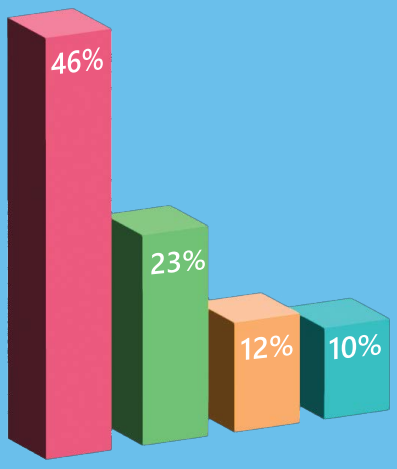


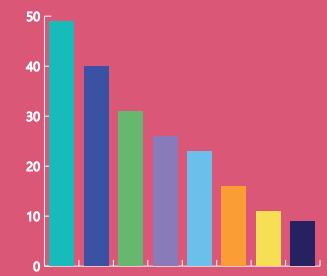
1/3

A third of organisations don't have data governance on the risk register

Opinions differ as to the most effective committee structure

- **46%** think it should be included as part of existing audit and risk committee
- **23%** think it should be included at the board level
- **12%** as part of a separate risk committee
- **10%** as part of a separate technology committee





Responsibility

Little consistency on who is responsible:

- Senior management/CEO
- IT function
- The risk function
- The board
- The Information and data function
- The financial management function
- Outsourced service by external parties
- Other

Letter from Governance Institute of Australia Chair

Pauline Vamos FGIA FCG

President and Chair of Governance Institute of Australia Ltd and of the Australian Division of The Chartered Governance Institute

We are delighted to share with you the Governance Institute of Australia's key thought leadership project for 2023 — Data governance in Australia. This report forms the fifth in the Governance Institute's digital thought leadership series.

This project also heralds the commencement of key strategic partnerships for with Governance Institute with Macquarie University's DataX Research Centre and the CSIRO's National AI Centre. The purpose of these collaborations is to enable our members to address some of the major challenges and risks technological advancements are having on organisations.

Data is an increasingly valuable asset. It is critical that organisations design, introduce and implement an effective data governance framework to maximise customer service and commercial value of data while also minimising risk particularly reputational risk.

In this year's survey, the Governance Institute asked its members to examine how organisations are making appropriate decisions about their data. The results have revealed a number of important insights into the challenges of keeping pace with technological advances, reporting to the board, protecting assets and maintaining the trust of stakeholders.

In relation to the role of boards, while we have seen a small rise in the number of board directors with experience in the technology sector, it's clear that there are very differing opinions as to the most effective board structures to best navigate data governance. The most commonly cited structure is to include it as part of the existing audit and/or risk committee, but fewer than half of the respondents selected that option. Twenty-three per cent think should be elevated to the board level, 12 per cent as part of a separate risk committee and 10 per cent recent as part of a separate technology committee.

Just under three quarters of organisations link data governance to the overall governance/risk management strategy. Less than half report data governance to the board, and if they do, the variation on the frequency of reporting is significant.

With data analytics, machine learning and generative AI now an integral part of running a business, how an organisation manages the data it uses, alters and shares is crucial to its long-term viability.

The majority of respondents are not that positive about how their organisation manages and protects data. While 34 per cent said it was excellent or very good, 57 per cent rated it only average and four per cent said it was poor. But 88 per cent have plans for improvement, which is why reports and road maps like this are essential to help bring directors and leaders up to speed.

The results, while skewed somewhat towards the not-for-profit sector, indicate that it's often the smaller organisations with fewer resources that are likely to be more exposed to risks due to a lack of data governance structures.

As we have seen in recent times, high-profile data breaches have had a sizeable impact on action, with 56 per cent of companies having changed their process and procedures since those events took place. But it's the smaller companies that are less likely — due to resourcing constraints — to have been able to make these changes.

An effective data governance framework is critical in protecting an organisation from potentially catastrophic internal and external threats and ensures a responsible, legally compliant and efficient use of data assets. We also cannot underestimate the role of governance as we move towards safe, responsible and ethical creation and usage of AI and the protection of vital data. We know there is a skills and knowledge gap that organisations must address as a matter of urgency.

I would like to sincerely thank our sponsors of this thought leadership advisers, PKF, for recognising the urgent nature of these issues.

The following report analyses the results of the survey. It has been prepared by the DataX Macquarie Research Centre, with contributions from:

Professor Niloufer Selvadurai, Macquarie Law School

Professor Hanlin Shang, Department of Actuarial Studies and Business Analytics

Professor Bamini Gopinath, Macquarie University Hearing

A/Professor Babak Abedin, Department of Actuarial Studies and Business Analytics

A/Professor Jessica McLean, Macquarie School of Social Sciences

A/Professor Michael Proctor, Department of Linguistics

A/Professor Anthony Chariton, School of Natural Sciences

I would also like to thank our panel of expert advisers in this space who have provided insightful contextual analysis around the report's findings.

They are:

Ken Weldin FGIA FCG, Partner, PKF

Karin Geraghty FGIA FCG, Non-Executive Director, Strategist, Digital Transformation Consultant

Stuart Harrison, General Manager Cyber Defence, nbn Australia

Sue Laver FGIA, Company Secretary, Telstra

Eve Lillas, Senior Associate, Gadens

Andrew Methven, Head of Risk and Compliance, Hearing Australia

Joanne Moss, Board Chair, Non Executive Director, and Gadens Partner

Megan Motto FGIA FCG, CEO Governance Institute of Australia

We recommend that you use this report to better identify threats and challenges, understand the broader data governance environment, and design effective data governance policies and procedures to support the responsible, legally compliant and efficient use of data.

Pauline Vamos,
Chair, Governance Institute of Australia

Sponsors and Research Partners

PKF is part of a global network, where dynamic business advisers can belong, grow, and thrive. In Australia, with more than 100 partners and 800 talented people, we deliver advisory, audit and tax solutions to create powerful opportunities for our clients, our people and our communities

PKF

MACQUARIE University
SYDNEY·AUSTRALIA
DATAX RESEARCH CENTRE

The **DataX Research Centre** aims to transform approaches to research in science, health and society through the development and application of new advanced data analytics and machine learning methods. DataX will both develop new methods in data science and enable new research in a range of challenging application domains.

Expert panel contextual analysis

On the benefits of data governance

Sue Laver

The here and now on data governance is know your data and don't keep it for longer than you should.

Megan Motto

Twenty per cent of the respondents were from health and social assistance and another 13 per cent were from financial and insurance services. These are organisations that are holding critically sensitive data. It may well be that it's the not-for-profit sector that's the least well equipped. But it is also actually the highest risk, because of the nature of the data that it holds.

Andrew Methven

I see data governance as much more of a whole of business problem rather than stopping the baddies getting in and then noticing when they're there. When that happens to you — not if — but when it happens to you, your data governance will give you a really good handle on what you've got, where it is, what the implications might be.

Ken Weldin

Quite often organisations will have all the best intentions, typically supported by a set of granular policies but at the same time, lack a centralised, strategic perspective or input based on what data it holds. This ability to step back and see the bigger picture is at the heart of good governance and underscores the benefits of good data governance. Recent experience points to this discovery or identification of data assets (and in some cases, liabilities) as being a long and difficult process. As with most things in life of that nature however, once you do it, you have a better platform to move forward from.

Joanne Moss

Companies and their boards need to have a more comprehensive understanding of the data and personal information they collect and handle, the way is it used and the relevant governance and legal obligations that apply to the relevant data. Once businesses have mapped the data they handle and have the appropriate governance frameworks, policies and controls in place, they are able to engage in conversations at the board level around how the business is using data from a strategic commercial perspective and how it can be appropriately leveraged and effectively used as an opportunity for the business.

Data governance and risk management

Stuart Harrison

There there's a bit of 'she'll be all right mate' kind of shining through. There are some scary statistics in this picture like 'has your management team done anything?' Forty-four per cent of people said no.

Ken Weldin

What's actually changing? If you can't be influenced by Medibank, Optus, Latitude and move away from that complacency, then what will influence you? I would be disappointed if we saw this in five years' time. Something has to change.

Data governance and the board

Joanne Moss

The board is ultimately responsible for the oversight ofgovernance (including data governance). Importantly, the CEO should be accountable to the board and it's committees for overseeing management's roll out throughout the business of the data governance initiatives (such as policies and procedures). I was surprised by the survey results on data governance that general counsel were not as actively involved as I would have expected, particularly given the complex legal landscape regarding the use of dataand personal information (including under the Privacy Act and relevant legislation that governs specific data such as financial information and health information) as well as considerable legal risks associated with non-compliance with laws. Typically, where you have high risk and emerging issues that relate to governance, the board and executive will seek guidance from the general counsel. Notably, there were not many general counsel that participated in the survey.

Eve Lillas

The Privacy Act is currently under review, with proposals to change the civil penalty regime to a tiered approach, where penalties would also apply to low level contraventions of the Privacy Act or breaches of the act that were not 'serious' or 'repeated'. Recent changes to Privacy Act last year also saw a significant increase in the penalties that can be imposed for serious or repeated interference with privacy (up to $50 million or three times the benefit obtained as a result of the contravention or if that is unable to be determined by a court, 30 per cent of the companies adjusted turnover during the breach turnover period for the contravention). We would expect that this will result in data governance becoming more of a priority at that board level and perhaps having a champion on the board who was more informed of the complexities regarding data governance and legal obligations.

Andrew Methven

On the one hand, 58 per cent of the respondents say the board doesn't have sufficient understanding, yet only half of the respondents are actually reporting anything to their board. I think there's an opportunity to call out the necessity for making sure that — be it the committees boards, a separate risk committee, a separate technology committee — that we have the people with the right skills involved.

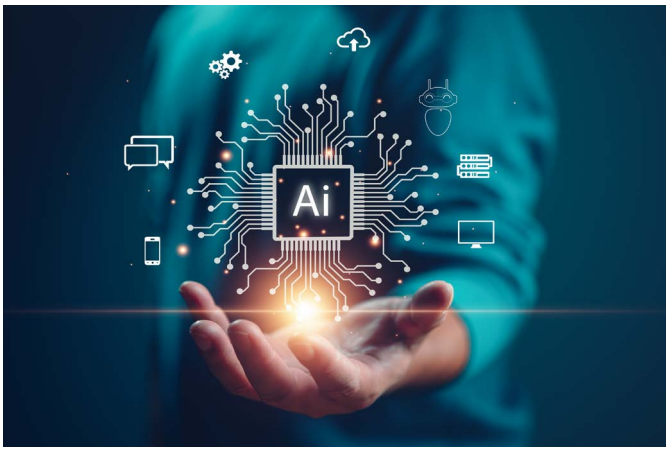
On AI

Karin Geraghty

It was more viewed as something that would be important in 2030 — I'm thinking we might be underestimating the velocity of things here.

Megan Motto

If you don't know how people are currently using generative AI in your organisations, you better quickly get on to an audit and find out who's using it and why, where and how. Start the conversation now because people are already playing around with ChatGPT and other AI tools.



Joanne Moss

We have seen an increase in disputes-related legal advice and training we provide to client companies on generative AI. A large proportion of this advice has been in relation to data and data handling practices given businesses are concerned about employees inputting personal, commercially confidential or legally privileged information into generative AI systems, to create a contract or to create an advice or piece of work. The risks apply to both open and closed source systems, albeit in different ways. We are seeing disputes emerge in the US in particular to data and data breaches relating to AI.

Sue Laver

I wonder if AI has moved so quickly that there's a lag in the catch up of perceptions of both use and risk. But the uptake of generative AI has been so great that you might be more worried about it from a consumer perspective ironically from an organisational perspective. Consumers don't get to see how the organisation is using it to their advantage, by making the access to information so much more effective.

On data as an asset

Stuart Harrison

It's all about assets. It's about the value you place on something which shapes how much you care about it. If you've miscalculated, have a system to correct calls quickly. But all data is not equal. So the fact that it isn't really high on everybody's list was pretty surprising. And I think boards are going to have to think more and more about that. Is your value chain, is your supply chain all on the same page? Does everybody understand that it's your brand and reputation and you can't outsource the liability around that because you have a supply chain? If this was a cybersecurity discussion that would be a top priority.

Ken Weldin

'Data is power' may sound like a cliché but if it wasn't true, then why would bad actors want to access it so much? It drives every decision or certainly should drive every decision rather than just relying on gut feel. Put to one side one's own internal management of data, often the biggest risk can come from the outside and the interactions with third parties. These interactions can exponentially increase the volume of data in your ecosystem and from that, its value in driving better informed decisions.

Karin Geraghty

Data is a different type of asset and people don't necessarily realise that it behaves differently: If you have a wallet and someone steals your wallet, you're going to know because it's physically gone. If you have data and someone steals it or copies it, you may not know because it's still there. It doesn't behave like other assets. On the positive side, it is one of the few assets that if shared, doesn't decline. At the same time, that is also one of the drawbacks and one of the reasons we are seeing an increase in cyber crime.

Stuart Harrison

Prioritisation is key. Defining that value statement around the data incorporates how much do you trust any one data set. Just have a think about that world that we're entering into. And then get cracking with your plan of action and get to work with the cyber teams and IT teams.

Who's accountable for data governance?

Ken Weldin

I recall hearing back in 2016 that data protection and cyber was now a non-delegable risk for the CEO. The impact of recent events certainly demonstrates the significant time, effort, cost and inconvenience that can follow from getting this wrong. As such, it's hard to argue that the board should not be actively overseeing how this risk — and opportunity — is being managed. At the same time, the fact that one erroneous click can expose the organisation and shut down operations underlines that data governance is a team sport encompassing everyone in the organisation.

Joanne Moss

Ultimately, the board is responsible for data governance so let's ensure we have the right people sitting on the board from a skills matrix perspective.
The business needs to consider reporting structures and processes at an executive level and assess who is providing information to the board and the CEO in relation to data related activities and initiatives.
Businesses are starting to incentivise and structure reporting to ensure issues and opportunities related to data are taken seriously.

Sue Laver

I would always put the board as having that oversight role rather than what I would call 'accountability' — because that sits with management in terms of getting staff to put the program together for the board to overseeing it.

Ken Weldin

It has to be with the CEO. The board provides oversight, monitoring, assessment, checking and holding people to account, as well including how and when they communicate with the organisation with sensitive information. It's a team sport.

On data retention

Stuart Harrison

There was one statistic that I wish I'd seen placed much higher — purge. If you don't need it, delete it permanently. Don't have it in slow storage for a gazillion years. Everybody has finite resourcing, so unless it's an organisational priority of the highest order, this is going to go to the back of the queue. And if you add cybersecurity requirements and all the other stuff that businesses need to be run and be profitable, I think some tough trade-offs are going to have to be made. You're going to have to accept some risk somewhere.

Eve Lilias

The majority of the respondents to the survey indicated they have a policy and a data retention policy in place, but they don't measure it. This highlights a critical issue in relation to businesses putting policies in place that are not effectively managed. While preparing a data retention and storage policy that sets out the minimum retention periods under different legislation is a necessary first step, the policy needs to be actively implemented and managed to assist with data minimisation and compliance with laws regarding how long businesses should retain data.

Sue Laver

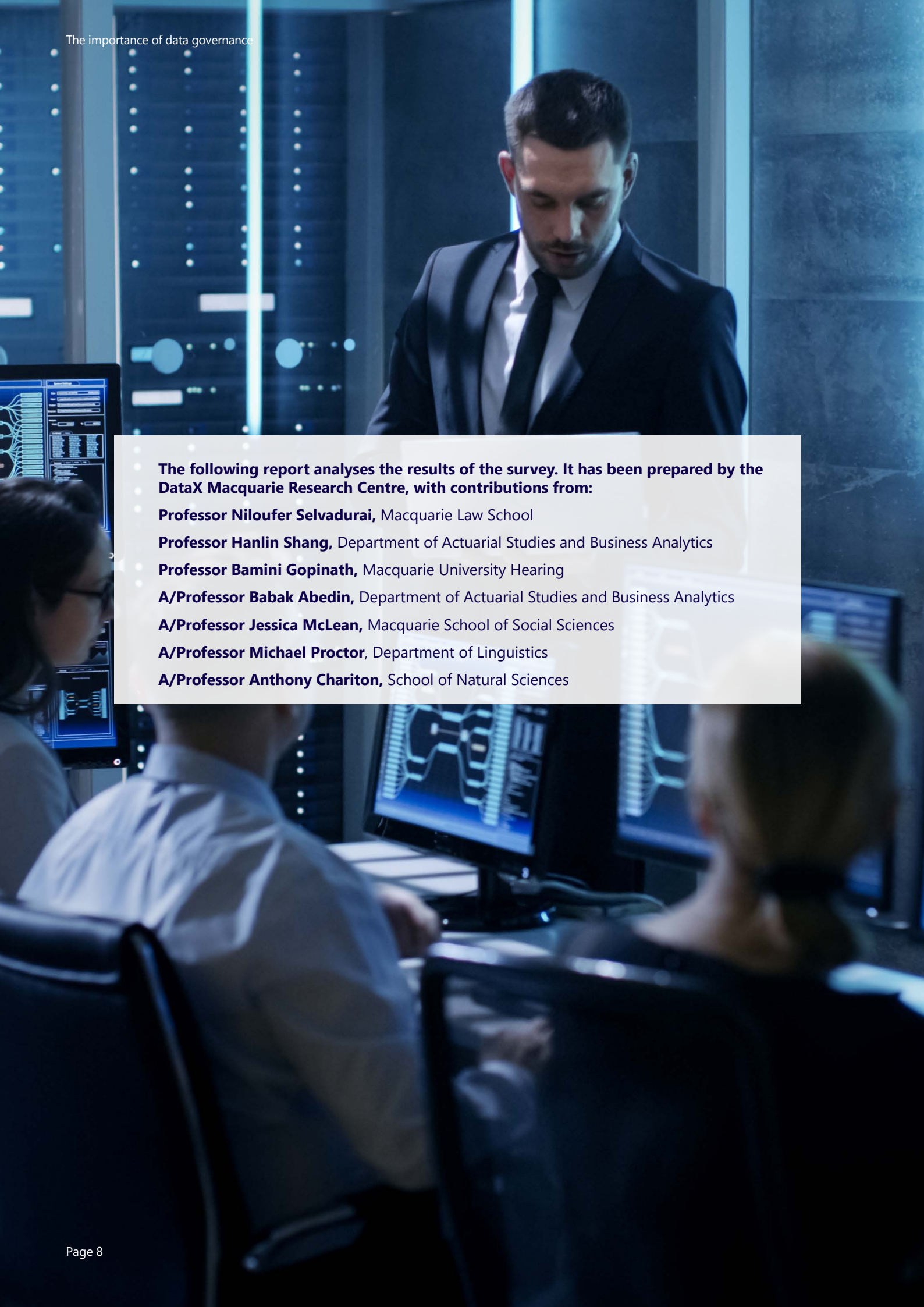
A lot of the legislation is geared towards keeping things much longer than is necessary and that's what needs a review in order to reduce the risks as well.

Andrew Methven

It's hard if you haven't got a lot of money to design a system that can be that subtle around what you do and don't keep. So you end up just keeping everything forever.

Karin Geraghty

People are assuming that organisations have this in hand. People are assuming their data is safe and if it's not, that's a significant expectation gap that isn't going to do anyone any favours when things go wrong. This is why this is such a big issue: once trust is gone, that's your equity gone.



The following report analyses the results of the survey. It has been prepared by the DataX Macquarie Research Centre, with contributions from:

Professor Niloufer Selvadurai, Macquarie Law School

Professor Hanlin Shang, Department of Actuarial Studies and Business Analytics

Professor Bamini Gopinath, Macquarie University Hearing

A/Professor Babak Abedin, Department of Actuarial Studies and Business Analytics

A/Professor Jessica McLean, Macquarie School of Social Sciences

A/Professor Michael Proctor, Department of Linguistics

A/Professor Anthony Chariton, School of Natural Sciences

The importance of data governance

Designing and implementing procedures to support the responsible and legally compliant dealing with data is one of the greatest challenges currently faced by boards of directors. The aim of this report is to assist boards and senior management implement an effective data governance framework. The purpose is to protect data assets and maintain the trust of stakeholders, including customers, suppliers, employees, investors, regulators and government. As data is an increasingly valuable asset, it is critical that organisations design and introduce an effective data governance framework to maximise the commercial value and efficiency of data while also minimising risk.

What is data governance?

Data governance is the exercise of authority, control and shared decision-making (planning, monitoring and enforcement) over the management of data assets.[1] 'Data assets' include information systems, databases, web pages, application output files, metadata and other digital documents of an organisation.

How is it implemented?

Data governance is implemented through policies and processes that describe the responsibilities that attach to different types of data creation and use. It requires identifying parties who have authority and control of data assets, outlining the procedures that should be followed when decisions are made in relation to data assets, and establishing clear lines of reporting, accountability and oversight (Figure 1).

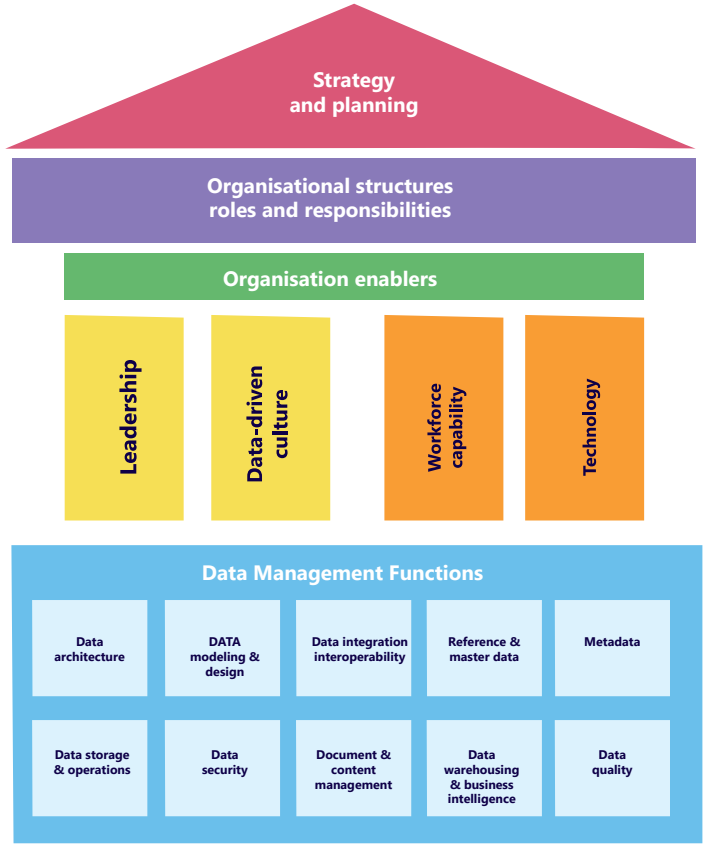


Figure 1: NSW Government, Data.NSW, Data Governance Model
at https://data.nsw.gov.au/data-governance-toolkit-0/module-3-data-governance

[1]M. Brackett, S. Early and M. Mosley (eds). *DAMA Guide to the Data Management Body of Knowledge,* NJ Technics Publications LLS, 2017 (second edition).

Are there any specific data governance laws?

A variety of different laws and principles relate to data governance. They include —

- Privacy laws — impose responsibilities for the creation, use and sharing of personal information (PI), including with respect to third parties and international entities;
- Notifiable data breach laws— create a duty to report serious breaches of PI to impacted parties and public;
- Confidentiality laws — create a duty to maintain confidentiality of communications;
- Corporations laws — impose duties on directors to exercise reasonable skill and act with due diligence;
- Administrative laws — impose duties of officials to act reasonably when making decisions, not take into account irrelevant considerations and provide an opportunity for parties to be heard;
- Consumer laws — prohibit misleading or deceptive conduct and false representations;
- Sector-specific data laws — impose duties on government, health, finance and other sectors who deal with sensitive information and data;
- Indigenous data sovereignty — the Australian Institute of Aboriginal and Torres Strait Islander Studies outlines how Indigenous data should be 'governed and owned by Indigenous Peoples from the very creation of data to its collection, access, analysis, interpretation, management, dissemination, potential future use and storage' (AIATSIS 2019:51). [2]

What sort of expertise is necessary to design data governance procedures?

The design and evaluation of data governance policies and procedures requires a combination of technical, business and legal expertise. This cross disciplinary expertise is reflected in the composition of the authors of this White Paper.

[2] Walter, M., Lovett, R., Maher, B.L., Williamson, B., Prehn, J., Bodkin-Andrews, G., and Lee, V. (2020). Indigenous data sovereignty in the era of big data and open data. Aust. J. Soc. Issues 56: 1–14, link: *Further reading* - Legal Issues in Information Technology Law, Mark Perry, Michael Adams, Alpana Roy, Niloufer Selvadurai, Monique Cormier and Stephen Mchenzie, Thomson Legal Australia, 2022.

Survey participants and process

In August 2023, the **Governance Institute of Australia** initiated an online survey on data governance. A total of 345 responses were received over a one-month period.

Respondent profile

The largest cohorts of respondents (Fig. 2) were senior governance or risk management professionals (25%) or CEO or C-suite executives (21%). As such, the survey results reflect the strategic thinking and high-level planning of organisations relating to data governance. It would have been interesting to also understand the demographics of the respondent profile through the collection of data relating to age, sex, ethnicity and postcode. These could all have a potential influence over the observed responses.

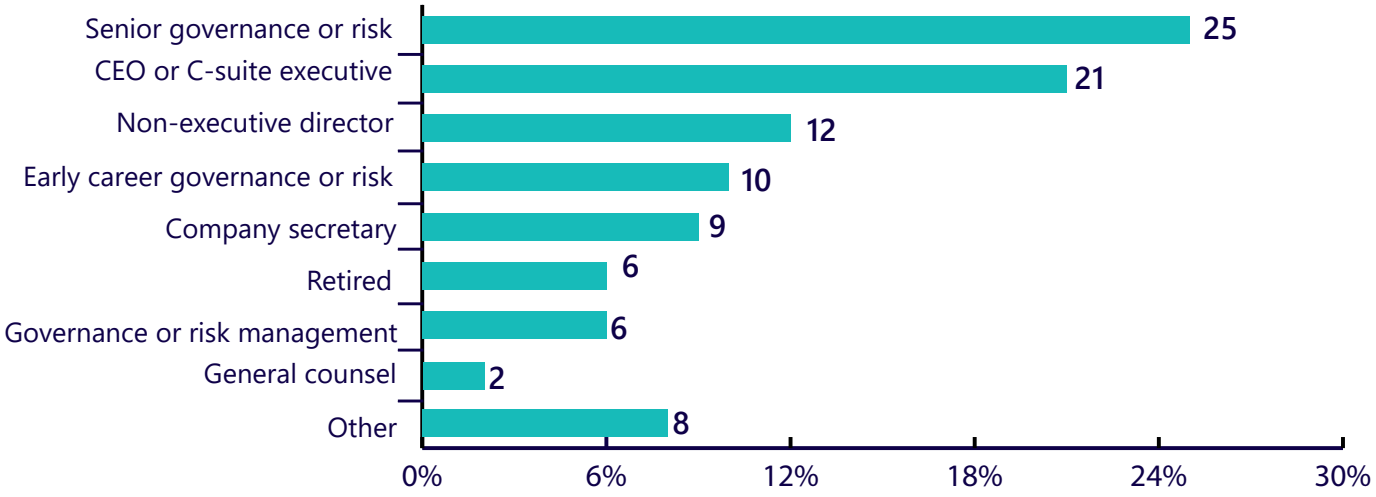


Figure 2: Stage of career

Types of organisations

While the survey respondents represent a diverse set of Australian organisation types, it is dominated by not-for-profit organisations (36%) and government (21%) organisations, with small to medium commercial enterprises forming 18 per cent of respondents and ASX listed companies forming a mere 10 per cent. This may perhaps suggest that the commercial sector is presently somewhat hesitant to engage in data governance discourse. This may further reflect an appreciation of the potential commercial risks and reputational damage associated with not having an appropriate data governance strategy, and the imprudence of communicating on this matter without due consideration and formal endorsement.

As the data governance practices and policies of organisations develop and crystallise, we can expect greater involvement in such surveys by the commercial sector. We have seen such a trajectory in relation to digital data privacy, where initial uncertainty and a reluctance to engage has been replaced with greater confidence and transparency on privacy policies and practices.

In the case of data privacy, the catalyst for this shift was the enactment of the Australian Privacy Principles that mandated that legislated entities enact a Privacy Policy (Australian Privacy Principle 1). As data governance is not the subject of such clear legislative mandate, it may take some time for such practices to become a central part of organisational governance. The findings suggest that there is a need to actively engage with organisations to strengthen awareness of the importance of data governance.

Industry sectors

The survey results (Fig. 3) represent a diverse group of industry sectors, including health care and social assistance (20%), finance (13%), education (11%), science and technology (10%), public administration (7%), energy (4%), manufacturing (3%), information media and telecommunications (3%) and construction (3%). The strong involvement of the health care sector is likely due to this sector's sophisticated appreciation of the highly sensitive nature of health data and the vulnerability of the patients whose data they hold, and the clear health sector requirements in this area. Strong national health guidelines on data governance may also be driving this increased engagement with data governance initiatives, such as this present work by the Governance Institute of Australia. It

is relevant to note that the federal government is currently developing governance arrangements so that researchers and public health policy makers can apply to use My Health Record data. The first step in this process is to establish a Data Governance Board as part of the ongoing governance arrangements required to oversee future My Health Record data research projects. As such, data governance is particularly pertinent and topical for this sector.

In comparison, the strong involvement of the financial and insurance services sector is likely to be driven by an appreciation of the need to maintain consumer confidence, especially considering the results of the recent Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry. Like the health sector, this engagement is also likely to be driven by an appreciation of the highly sensitive nature of financial data, and the substantial financial losses that would be incurred by its inappropriate use or disclosure.

What is surprising is the relatively low involvement of the information services sector. Given the technical and data expertise entities in this sector would most likely possess, it may have been expected that this sector could lead the discourse on good data governance. This is an interesting but also worrying finding.

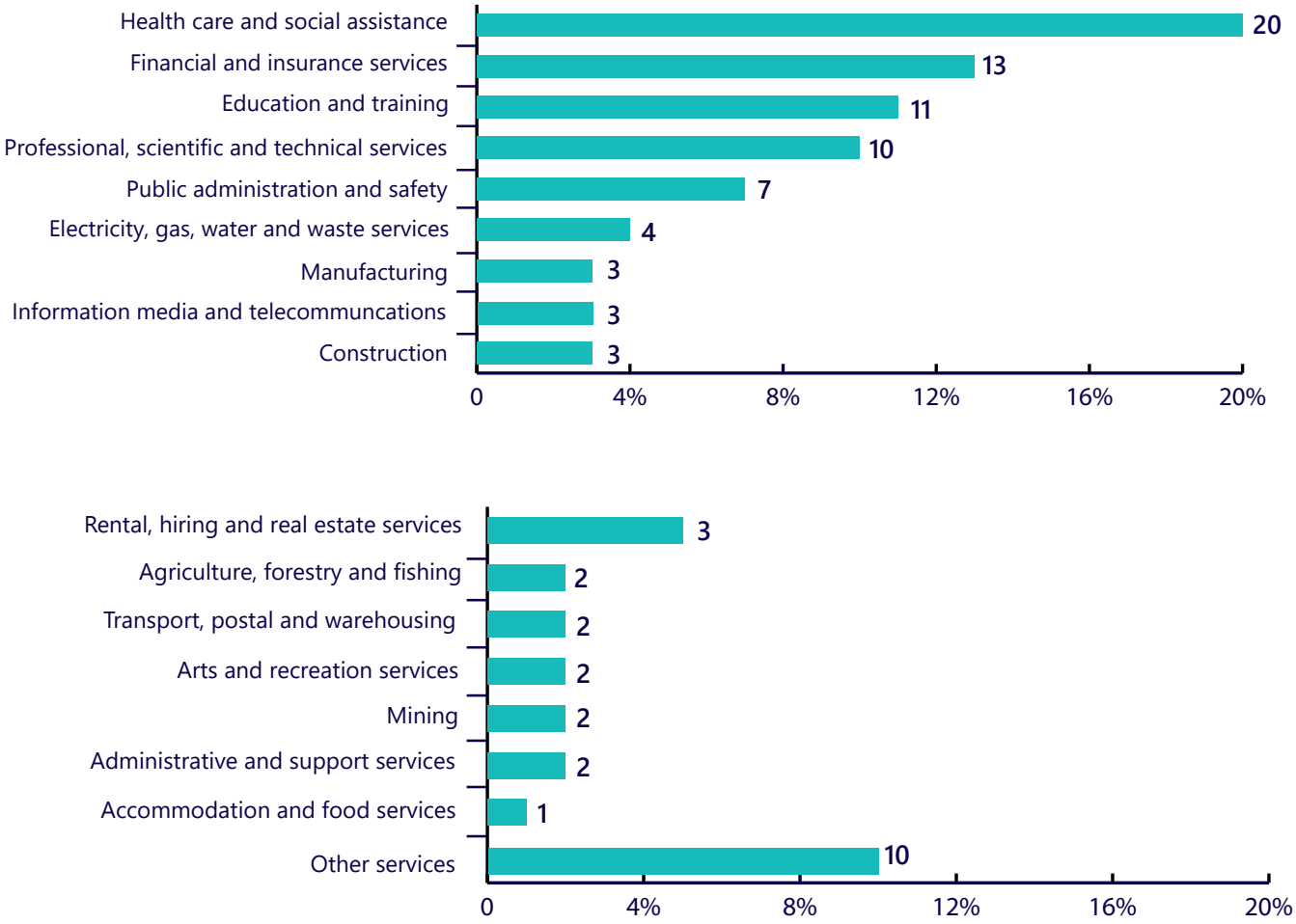


Figure 3: Industry sector, Governance Institute of Australia: Data governance, Stephen Spencer, August 2023, p. 10.

Data governance and the board

Understanding of data governance

An interesting feature of the survey results is its insight into boards and other organisation leaders **understanding of 'data governance'**. Significantly, there was strong consensus in this area, with 70 per cent agreeing that data governance formed part of ICT governance, with a further 68 per cent agreeing that it relates to privacy and security and 68 per cent agreeing that it forms part of information and records management.

But there was no such consensus when it came to the more contentious issue of **whether the board has 'sufficient' understanding** of the organisation's current data governance strategies. Fifty-eight per cent of respondents said 'no' to this question. It would have been useful to have also seen how the 'yes' and 'no' responders align with specific industry sectors.

The main **reason for this lack of understanding** is perceived to be a lack of formal technology skills and education (51%). This is reassuring as it reflects an understanding of the complexity of data governance and the need for specific education. However, it is relevant to note that the reason of 'lack of confidence' in dealing with data governance scored is only 34 per cent, suggesting the level of training and capability is not necessarily aligned to confidence in this area.

A second cluster of reasons for a lack of understanding relate to **priorities**. Data governance not being a priority of boards and the board having more pressing prioritises both scored 39 per cent, presumably from the same responders as these options are probably related. A common reason for a lack of board action is a lack of consensus. In the case of data governance, only 22 per cent of the no responders cited different opinions about strategy or approach as being a reason for a lack of understanding.

Understanding of data assets

While boards and organisations lack an understanding of data governance, a clear majority of respondents (61%) were of the view that their board **understood the organisation's most important data assets and how they are protected**. Such confidence was strongest for ASX listed companies and lowest for non-profit and government organisations.

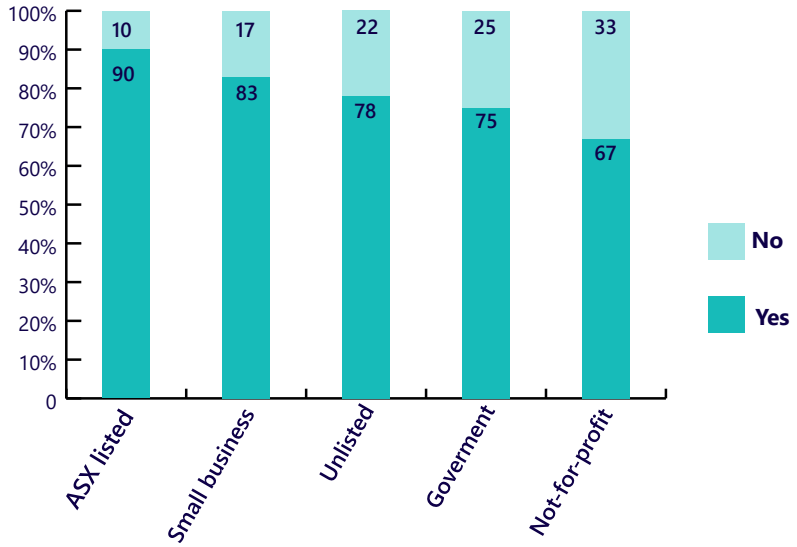


Figure 4: Understanding of board, Governance Institute of Australia: Data Governance, Stephen Spencer, August 2023, p. 29.

The value of data

There are a range of reasons why data is valued by organisations, some relating to intrinsic value and other relating to perception and reputation. Seventy two per cent of respondents believe data is a 'core business asset', echoing the often-quoted Clive Humby words 'data is the new oil'. However, only 47 per cent rated data as a 'financial asset,' suggesting that the value of data is larger than its commercial value. This is supported by the fact that 41 per cent believe its value to be intangible. The much-publicised reputational risks of failing to responsibly deal with data is, not surprisingly, reflected in the 62 per cent who cited reputation as a facet of data value.

Reporting to the board

Concerns have been raised in the mainstream media and scholarly literature as to the lack of board oversight of data-related decisions. There is concern that important data related matters are routinely made by technical experts with limited understanding of relevant laws and principles of accountability and transparency. On the whole, the findings of this survey justify this concern.

While an overwhelming 71 per cent responded that their **organisation's data governance was 'linked' to the organisation's overall governance** and risk management strategy, there was no such consensus on the related question of reporting to the board. Fifty-one per cent responded that data governance was not **reported to the board.** This suggests that while there may be some formal mechanisms for reporting to the board, this is not happening in practice. This is a concerning revelation.

The above problem is exacerbated by the fact that a staggering 78 per cent of those responsible for data governance only **report to the full board on a quarterly or less frequent basis**. Given the substantial damage that can be caused to individuals through data mismanagement or breach, such lack of regular oversight is of concern. Thirty-six per cent of those responsible for data governance only report to the full board on a quarterly basis, with 20 per cent doing so annually and 16 per cent doing so bi-annually. Seven per cent report less than once a year (Figure 5 below).

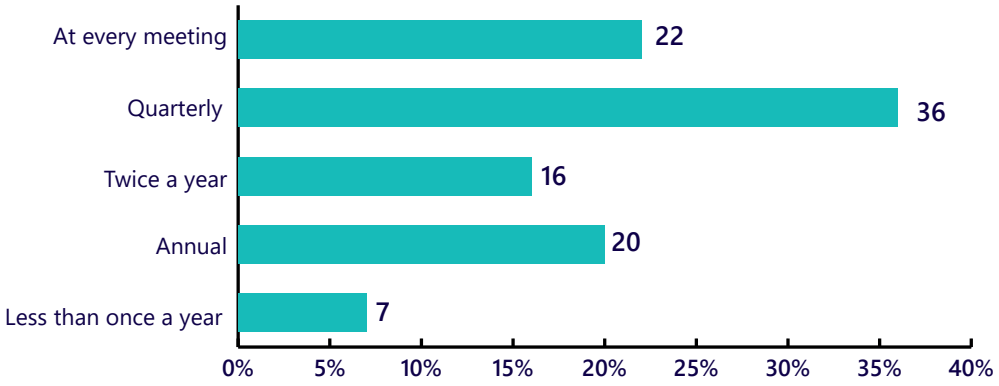


Figure 5: Frequency of reporting data governance to full board, Governance Institute of Australia: Data governance, Stephen Spencer, August 2023, p. 13.

Use of a data governance framework

Compounding this lack of reporting, is the lack of **data governance frameworks**. Only 46 per cent of respondents reported that their organisation has a data governance framework. Lack of capacity was the clear reason for this failure (64%). While the nature of this lack of capacity is not interrogated, the fact that only 25 percent said it was due to a lack of skill may suggest it is a problem of inadequate financial investment. This is consistent with prevalent organisational under-investment in other data related areas such as cybersecurity.

Impact of data breaches on data governance

The reputational damage caused by highly publicised data breaches may opportunities greater action on data governance in the **future**. Fifty-six per cent responded that the management team or board has 'changed … data governance since the Medibank, Optus, Latitude data breaches'.

Risks associated with data governance

The dominant risk identified in relation to data governance is that of cyber security attack (57%). Interestingly, the second most perceived risk relates to human involvement and a lack of staff skill and knowledge (44%). This is reassuring as organisations appreciate that risks relate to both external and internal factors and encompass both the technical and human aspects. The diversity of identified risk is also reassuring (lack of data life-cycle management, siloed data holdings, third party risks etc), as it implies that future strategies to combat risks could be nuanced and holistic.

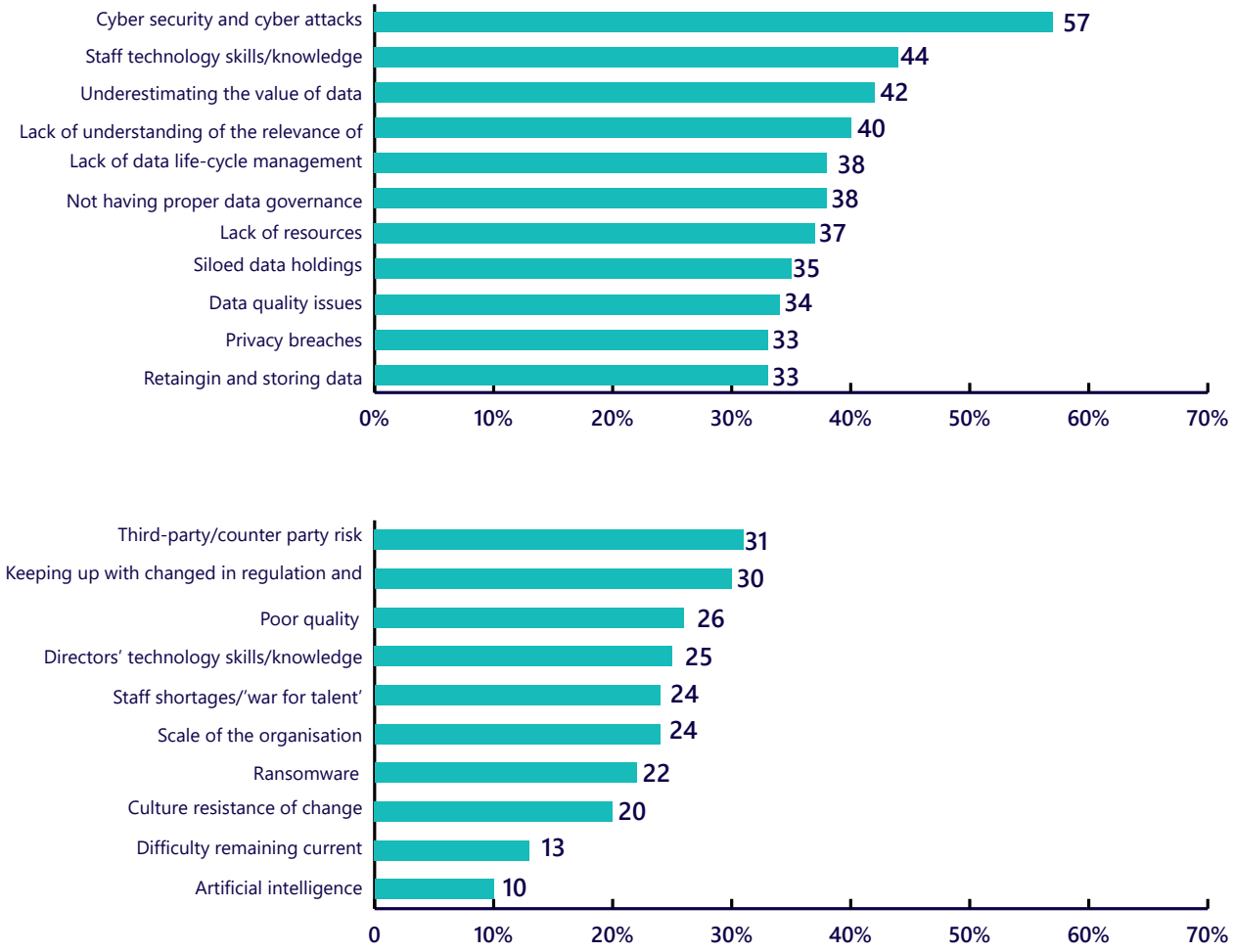


Figure 6: Risks associated with data governance, Governance Institute of Australia: Data governance, Stephen Spencer, August 2023.

However, given widespread familiarity with the centrality of data to society, it is surprising to see 44 per cent believe that this lack of action is due to their organisation underestimating the 'value' of data. This is also somewhat inconsistent as to the above results in relation to value. Further interrogation of the industry sectors responding to these questions may explain this divergence.

Expected 2030 risks

The responses in relation to potential future 2030 risks reflect an understanding of the capacity of institutional and/or individual usage of AI to lead to the misuse of data on a large scale. While this figure is only 10 per cent for 2023, it balloons to 43 per cent in 2030. This is of concern, as it suggests a lack of appreciation of how AI usage can presently lead to data misfeasance. This is not a future problem, it is a real and present danger, and organisations need urgent education on the nature and extent of the current threat presented by AI usage. The continuing prevalence of cyber security (57% in 2023 and 62% in 2030) reveals that organisations clearly understand that this is a continuing long-term threat to be addressed.

Rating of organisation's management and protection of data

A majority of 57 per cent feel their organisation's management and protection of data is 'average'.

How to address data governance risks

Training and financial investment were overwhelmingly perceived as the way to address data governance risks. A majority of 86 per cent cited some form of financial investment, with a further 89 per cent citing training. Reassuringly, an overwhelming 88 per cent responded that their organisation has 'plans in place' to improve data management and protection.

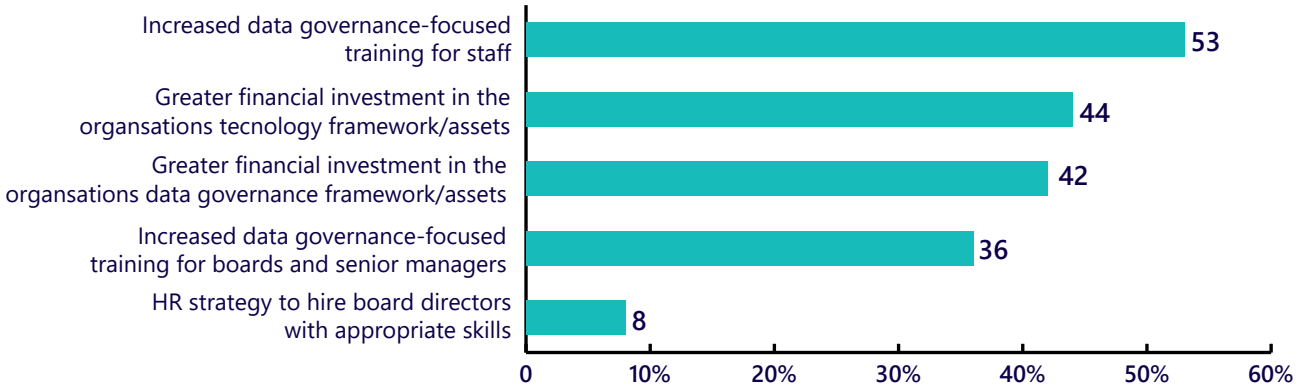


Figure 7: Responses to data governance risks, Governance Institute of Australia: Data governance, Stephen Spencer, August 2023, p. 24.

Perceived benefits of data governance

The results reveal a limited understanding of the benefits of data governance. When it comes to **benefits for the individuals and communities whose data an organisation holds**, privacy and increased security are perceived as the leading benefits. Significantly, other issues such as protecting the financial interests of individuals by preventing the unauthorised monetisation of their data are not noted. Similarly, supporting individual control and autonomy, as well as their psychological well-being by responsibly and safety dealing with their data is not noted. As accountability, transparency, fairness, contestability, reliability and human well-being are among the principles articulated in the Australian Government's AI Ethics Framework, it is likely that such values will flow onto broader data governance in the future. This is likely to broaden organisations' understanding of the benefits of appropriate data governance.

When it comes to **benefits for the organisation** itself, the understanding is more developed, with managing reputational risk, building customer trust, supporting better decision-making and driving change being amongst the many identified benefits.

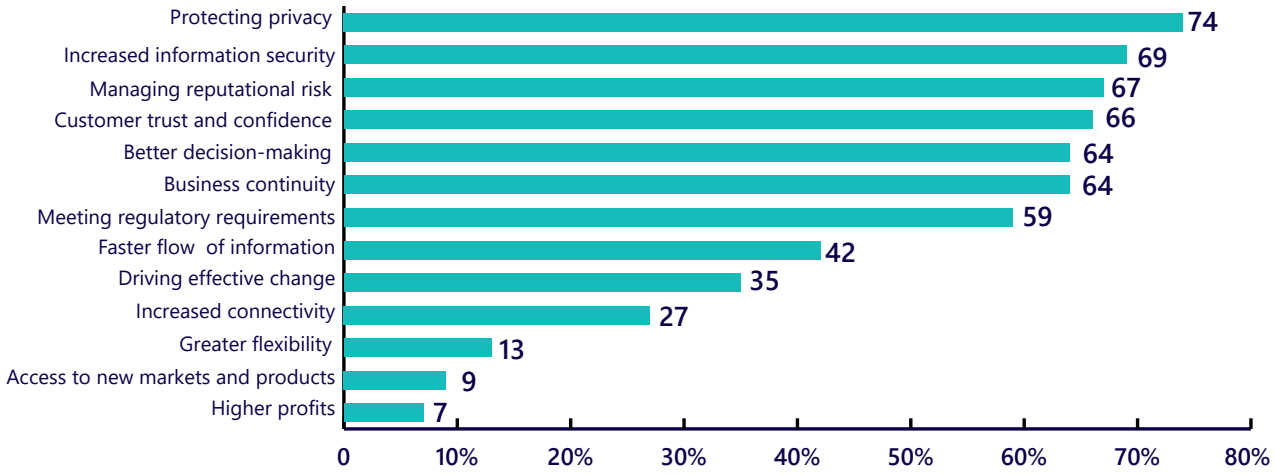


Figure 8: Perceived benefits of data governance, Governance Institute of Australia: data governance, Stephen Spencer, August 2023, p. 25.

Most effective board and committee structure for data governance

Opinions differ as to the most effective means of data oversight and governance. However, a clear majority believe inclusion in existing audit and risk committee to be the most effective option.

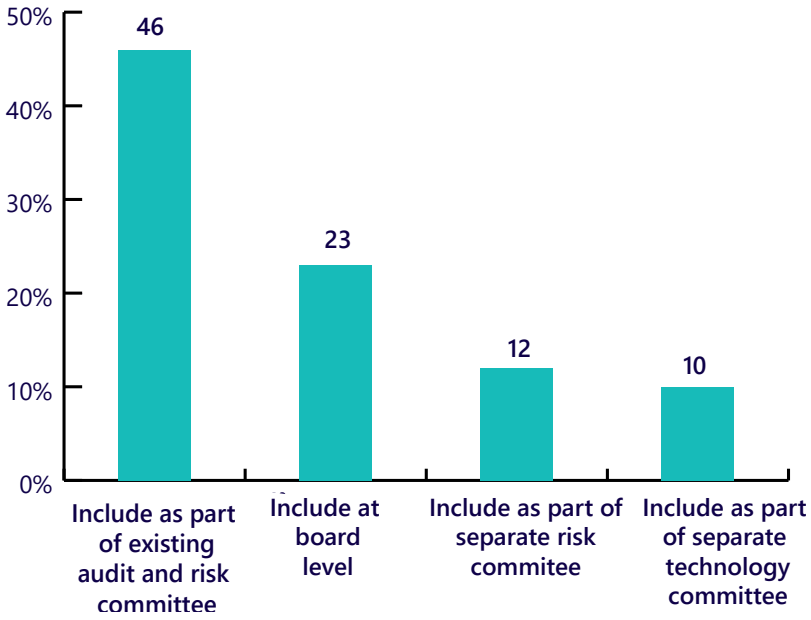


Figure 9: Most effective mechanisms of data governance, Governance Institute of Australia: Data governance, Stephen Spencer, August 2023, p. 27.

Conclusions

Insights

- **Governance structure** — A clear majority of the surveyed organisational leaders are of the view that data governance forms part of wider ICT governance, relates to privacy and security, and should be part of information and records management.
- **Data governance understanding** — However, opinion is divided as to whether the boards of organisations have 'sufficient' understanding' of the organisation's current data governance strategies. For those who believe that the board lacks understanding, this is primarily attributed to a lack of formal technology skills and education and a failure to prioritise data governance.
- **Data assets** — While survey respondents are divided as to whether boards have sufficient understanding of data governance, the majority are of the view that their board understands the organisation's most important data assets and how they are protected. Such confidence is strongest for ASX listed companies and lowest for non-profit organisations.
- **Reporting to board** — While an overwhelming number of respondents believe that their organisation's data governance is 'linked' to the organisation's overall governance and risk management strategy, there is no such consensus on the related question of reporting to the board. A clear majority respond that reporting to the board is done on a quarterly or less frequent basis. In light of the serious loss that can be generated by inadequate data management and breaches, this is of concern and needs to be addressed.
- **Data governance framework** — The risks associated with a lack of reporting to the board is exacerbated by the fact that a majority of respondents work for organisations that do not yet have a data governance framework.

Recommendations

Building on the above analysis, we make the following recommendations for organisations in relation to data governance.

Provide greater education and training to members of the organisation, including senior leadership, on

- Identifying the various data assets of the organisation
- Quantifying the value of data assets held by the organisation
- Identifying the level of risk associated with each such data asset

Develop guidelines for designing, implementing and maintaining an effective data governance framework, including

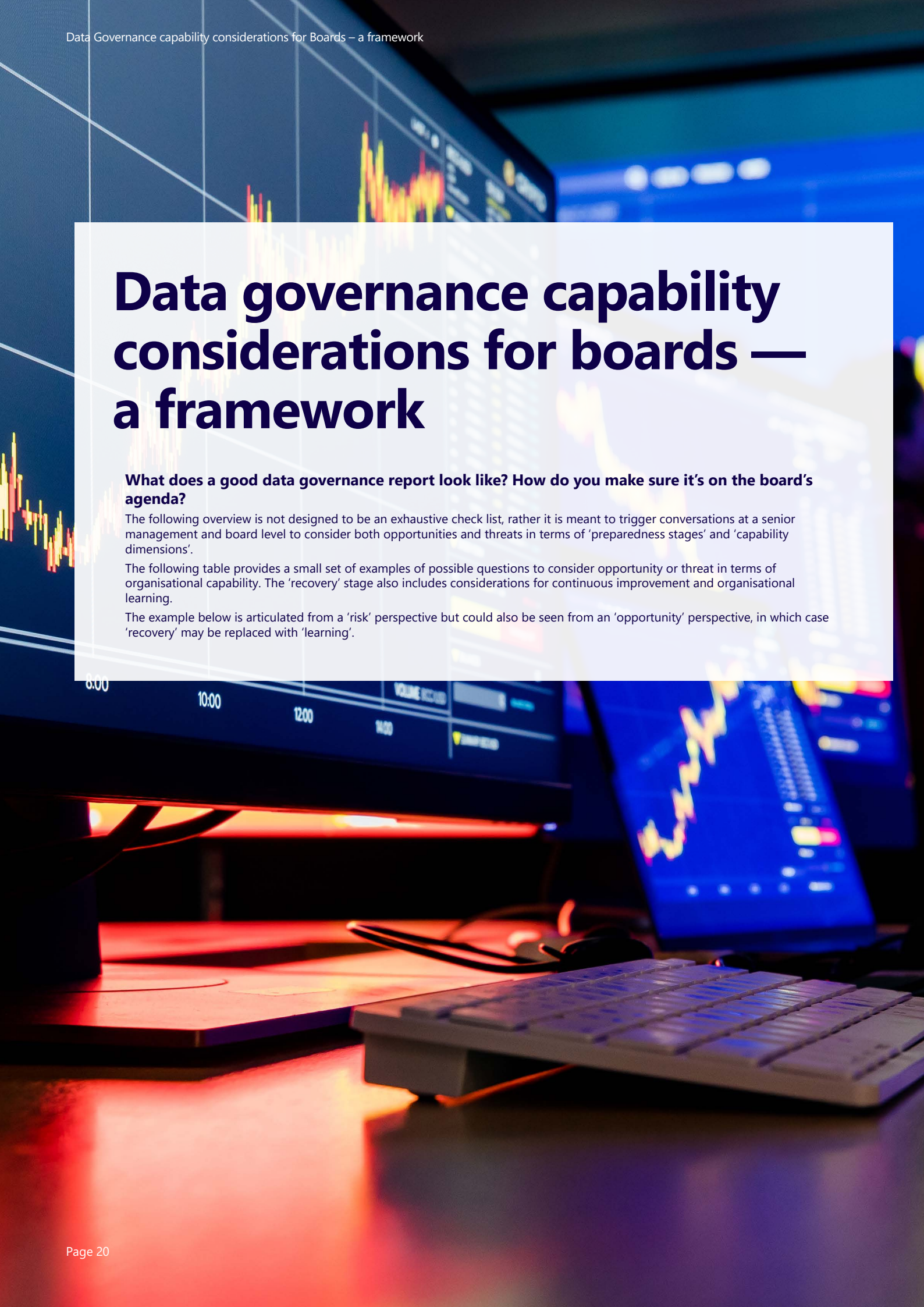
- Identifying the parties within the organisation who are responsible for data
- Delineating the nature and extent of their responsibilities
- Enacting policies and oversight mechanism to support safety and trust
- Formalising lines of reporting and accountability, including to the board

Create mechanisms for collaboration between all relevant parts of an organisation, including

- Delineating the respective roles of technical, financial, risk management, legal, administrative, human resources and others
- Developing a reporting and accountability framework that connects the work of these different domain experts to a central cohesive data management and security plan

Implement methods to measure the success of data governance frameworks, including

- Aligning these measures to an organisation's existing governance and privacy reporting policies and procedures
- Updating the data governance framework, as needed, in light of evolving technologies and emerging threats



Data governance capability considerations for boards — a framework

What does a good data governance report look like? How do you make sure it's on the board's agenda?

The following overview is not designed to be an exhaustive check list, rather it is meant to trigger conversations at a senior management and board level to consider both opportunities and threats in terms of 'preparedness stages' and 'capability dimensions'.

The following table provides a small set of examples of possible questions to consider opportunity or threat in terms of organisational capability. The 'recovery' stage also includes considerations for continuous improvement and organisational learning.

The example below is articulated from a 'risk' perspective but could also be seen from an 'opportunity' perspective, in which case 'recovery' may be replaced with 'learning'.

Issue	Awareness/ Maturity	Planning	Preparedness	Response	Recovery
Information capabilities	• Is the current state known, visible and documented? • Is there an inventory of critical assets (including data/systems/ infrastructure)? • Do metrics exist and are they being monitored? • What is being communicated?	• Is there a plan or strategy for assets? • Are there policies covering establishment, procurement, implementation and acceptable use? • Are there risk assessments? • What is being communicated?	• Is there a plan or strategy for business continuity in the absence of assets?	• Are incident response plans in place and accessible?	• What concludes an incident? • How are learnings captured and communicated? • How are impacts measured? • What changes need to be made?
People capabilities	• What skills are needed? • Are specialist roles or responsibilities needed? • Are staff aware of risks?	• Do plans identify who is accountable? • Do plans identify training needs or skills gaps? • Are plans communicated internally and externally?	• Who are the relevant contacts? • Are people educated or trained? • What scenarios are considered?	• Are roles and contacts for incidents identified and contactable? • Are backup plans in place for relief? • Are internal and external communication plans in place? • Are rosters needed?	• How is internal and external people's recovery assessed? • What additional help is needed? • How do people know 'we're back to normal'? • How is feedback captured?
Process capabilities	• How do new risks and threats get identified • How do new risks get assessed	• Do possible impacts form part of an overall business approach?	• Are processes rehearsed?	• Are escalation and notification requirements known/accessible and documented?	• Are learnings documented to feed into continuous improvement?
Technology capabilities	• What is the technology portfolio? • What monitoring exists?	• Are relevant documents, systems and procedures easily locatable and accessible? • Are there backups? • Are systems designed to 'privacy by design' and 'zero trust'?	• Have backups been tested? • Are regular tests conducted? • Do systems have automatic notifications on exceedences?	• Is mobility available (hardware and networks) if another or 'on location' response is needed?	• Do learnings feed into improvements?
Governance and accountabilities	• What does the board need to know and do? • What does senior management need to know and do? • When do things need to be escalated from one to the other?	• Are roles and accountabilities clear and measured • Are insurances available or needed	• Are insurance covers understood fully? • Are board and management roles defined for BAU and incident scenarios?	• Are claims filed promptly? • Are communication lines and roles to internal stakeholders executed? • Have legislated notifications been issued (data breach, market announcements)?	• Are learnings valued as an asset? • Are identified necessary changes implemented and monitored to execution?
Supply chain capabilities	• What is the contract and supply chain landscape? • Is there concentrated reliance on single providers or countries?	• Are roles between suppliers and the organisation clear? • Are service levels defined and monitored?	• Do escalation clauses/ responsibility matrices exist? • Are out of hours support/response capabilities known? • Are financial impacts known for out of hours support?	• Are direct lines and methods of communication and coordination in place? • Can responders be co-located if needed?	• Do contracts and service arrangements require amendment or clarification?

Courtesy: Karin Geraghty FGIA FCG, Principal Consultant, Stratdigi

Governance Institute of Australia

Governance Institute of Australia Ltd Registered office

National office
Level 11/10 Carrington Street
Sydney NSW 2000

T (02) 9223 5744
E info@governanceinstitute.com.au
governanceinstitute.com.au

ACN: 008 615 950
ABN: 49 008 615 950

State offices

New South Wales & ACT
Level 11/10 Carrington Street
Sydney NSW 2000

T (02) 9223 5744

Queensland
Level 8, 100 Creek Street
Brisbane QLD 4000

T (07) 3211 9190

South Australia, Northern Territory & Tasmania
PO Box 6178
Linden Park SA 5065

T (08) 8379 6771

Victoria
Level 7, 180 Flinders Street,
Melbourne VIC 3000

T (03) 9620 2488

Western Australia
T (08) 9321 8777