A JOINT PUBLICATION BY

Australian Institute of Company Directors | Allens | Centre for Business Analytics | The University of Melbourne Melbourne Business School

Data Governance Foundations for Boards

Key principles for director oversight and value creation

MAY 2025

Contents

Case studies and director reflections

Foreword

In an era defined by digital transformation, data has emerged as a critical asset for organisations across every sector of the Australian economy. Boards have an important role in navigating this opportunity and complex challenge, where the ability to govern, leverage and protect data increasingly shapes strategic success and organisational resilience.

For directors, data governance is no longer a technical function delegated to the IT department – it is a business-critical issue requiring board-level engagement and oversight. The potential value of data is immense – providing insights that can transform business models, enhance customer experiences, drive operational efficiencies, and unlock new revenue streams. Conversely, poor data governance can result in significant financial, legal, reputational or regulatory consequences.

Data Governance Foundations for Boards explores the multifaceted nature of data governance, recognising that it requires that boards balance innovation and strategic vision with risk management and ethical considerations.

The recommendations and insights presented are grounded in practice, informed by consultation with senior directors, Australian companies and data experts, and reflect leading domestic and international approaches.

We are delighted that this guidance is brought to life through case studies from leading Australian companies CAR Group, Coles Group, Ramsay Health Care and national charity Fitted For Work. We also thank senior directors and AICD members Jason Blackman GAICD, Carmel Mulhern GAICD, Fiona Pearse FAICD, Wendy Stops FAICD and David Thodey FAICD for their contributions to the case studies and the individual director reflections.

As the shift to a digital-first world continues, data governance will remain a growing area of board focus. This publication supports directors in engaging with these issues and encourages innovation and strategic thinking in building data-driven organisations.

We would like to acknowledge and thank staff from AICD (Simon Mitchell), MBS (Anita Arbogast) and Allens (Emily Cravigan, Nick Li and Maddison Ryan) for their hard work to produce this publication.

Mark Rigotti MAICD
CEO and Managing Director
Australian Institute of Company Directors

Professor Yalçın Akçay
Melbourne Business School,
Director of the Centre for Business Analytics

Valeska Bloch
Partner and Head of Cyber, Allens

Snapshot

The boards of all Australian organisations have a central role to play in ensuring that key organisational data is viewed and treated as a strategic asset, and this asset is protected and harnessed in a manner that meets regulatory requirements and stakeholder expectations.

This publication recognises that key organisational data is increasingly the foundation of effective business operations, strategy and risk management. When used effectively, data can enhance productivity, improve products and services, drive financial returns, and support the monitoring and management of risks. It is, however, vulnerable to theft, manipulation and inappropriate use.

Effective data governance at the board level not only ensures that key organisational data is viewed and treated as a strategic asset, but is also foundational to protecting this key asset, meeting regulatory requirements, and preserving stakeholder trust.

The guidance recognises that board oversight of data governance, cyber security resilience and the oversight of AI (**artificial intelligence**) go hand in hand.

AICD resources on cyber security and AI

Where relevant, this publication references the following AICD resources on cyber security and AI.

- **Cyber Security Governance Principles** (2024) (in partnership with the Cyber Security Cooperative Research Centre)
- **Governing Through a Cyber Crisis** (2024) (in partnership with the Cyber Security Cooperative Research Centre and Ashurst)
- **Directors' Guide to AI Governance** (2024) (in partnership with Human Technology Institute at the University of Technology Sydney)

Rather than replicating guidance, we direct readers to where further detail exists on specific topics.

Summary

The following outlines the key points from each of the principles in the publication and lists the Top 10 questions for directors to ask to assist in overseeing data governance at the organisation.

REGULATORY OBLIGATIONS

1. Oversight of data governance forms part of directors' existing fiduciary duties under both common law and the *Corporations Act 2001* (Cth).
2. Boards should also have oversight of how the organisation meets its key regulatory requirements relevant to data, including the *Privacy Act 1988* (Cth).

PRINCIPLE 1: KEY ORGANISATIONAL DATA IS A STRATEGIC ASSET

1. Boards should promote the effective use of key organisational data as a significant business enabler.
2. A robust data strategy aligns data governance practices with organisational priorities, supporting growth, innovation, regulatory compliance and stakeholder expectations.
3. To be effective, AI systems require high-quality data that is accurate, complete, consistent and timely.

PRINCIPLE 2: DEFINE CLEAR DATA GOVERNANCE ACCOUNTABILITY

1. Clear roles and responsibilities form the foundation of effective data governance.
2. Comprehensive and clear board reporting – including engagement with management and updates on emerging trends – supports board oversight of data use and protection.
3. External providers play a growing role in data collection, management and protection, and boards should have visibility over these providers' data handling and protection settings.

PRINCIPLE 3: THE DATA LIFECYCLE AND EFFECTIVE RISK MANAGEMENT

1. Identify the key data the organisation holds, including where it resides, how it is utilised, who has access to it and how it would impact business operations if compromised.
2. A data governance framework is a key mechanism by which the boards of all organisations can effectively oversee data management practices.
3. There are practical and low-cost controls that all organisations can utilise to mitigate risks associated with the data lifecycle.

PRINCIPLE 4: EMPOWER A DATA-DRIVEN ORGANISATIONAL CULTURE

1. Boards set the tone from the top for a data-driven culture through championing the effective, ethical, and secure use of data – including in board decision making.
2. Education and training are essential for directors and staff to apply data effectively and foster an analytics mindset that promotes informed decision making, while managing associated risks.
3. Boards should promote data-informed decisions, including supporting organisational investments to use data to drive performance, innovation, and risk management.

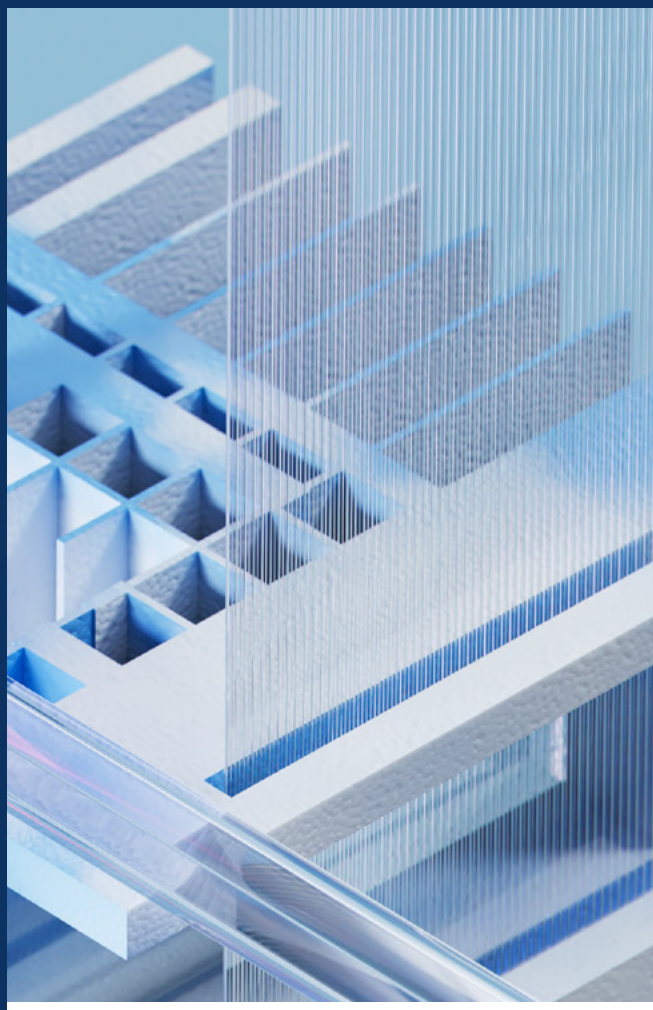
PRINCIPLE 5: ENABLE EFFECTIVE DATA INCIDENT RESPONSE AND RECOVERY

1. The board and management should proactively plan for a variety of plausible data incidents.
2. A clear and transparent approach to communications with impacted individuals and other stakeholders is key to mitigating reputational damage, complying with regulatory requirements and facilitating an effective recovery.
3. Data incidents can be an opportunity for organisations to substantially improve data governance practices.

TOP 10 DIRECTOR QUESTIONS

1. Has the board reviewed a data strategy that clearly outlines how the organisation will enhance the collection, management and use of data?
2. Does the organisation have the resources needed to implement data initiatives or effectively harness existing data?
3. Does the board understand its oversight role in data governance, including via board committees?
4. Does the board understand the role of key external providers in the organisation's data governance?
5. Does the board understand what data the organisation collects, generates, holds and discloses, why it is collected, and where it is held?
6. Does the board understand the data security controls deployed by our organisation as well as by our key digital providers?
7. Do we as directors use key business data and analytical approaches to inform our decision making?
8. Does the organisation understand our stakeholders' expectations for how we collect, protect, use and disclose their data?
9. Does the organisation have an incident Response Plan that is regularly tested and uplifted following simulation exercises?
10. In the event of data loss or theft, how will we communicate with customers, notify regulators, and meet our Notifiable Data Breaches (**NDB**) scheme requirements?

Introduction



In today's digital landscape, data is one of the most valuable assets an organisation holds. For boards, oversight of data governance is a core component of organisational performance, risk management and regulatory compliance.

Boards have a central role to play in the governance of data – ensuring it is properly managed, secured, and used to drive business performance. As regulatory demands intensify, and risks related to data privacy, cyber security, and ethical use increase, strong governance frameworks are essential.

Australian governance research in 2023 revealed widespread limitations in how boards oversee the collection and management of data.[1] Since then, the volume and strategic importance of data has only increased, elevating the role of the board in governing and safeguarding these key assets.

With the proliferation and adoption of AI and machine learning to drive productivity and innovation, it is important to recognise data as the foundational input. Without a high-quality data foundation, the effectiveness of these technologies is constrained.

Our focus: Governance of key organisational data

For the purposes of this publication, our focus is on the board level governance of key organisational data. This governance encompasses how a board oversees the collection, use, protection, and disposal of key organisational data, and has confidence that this aligns with the strategic direction of the organisation

'Data governance' is a commonly used term that does not always denote a board-level involvement. Rather, it generally refers to an organisation's internal structures and processes that guide how data is managed within an organisation. **Box 0.1** provides definitions to help distinguish between data governance and, separately, data management.

1 Governance Institute of Australia, Data Governance in Australia, 2023, available **here**.

What is key organisational data?

Key organisational data is information that influences strategic decisions, customer experiences, operational efficiency, and regulatory compliance. Its importance is determined by both its value-generating potential and the magnitude of negative consequences if compromised, corrupted, or mismanaged. The key categories of data are summarised in Table 0.1.

TABLE 0.1: Categories of key organisational data

Type	Summary
Customer, client or beneficiary data	Information about customers, clients or beneficiaries, including their behaviours, preferences, and interactions with the organisation.
Employee data	Employee information, performance metrics, compensation, and organisational structure.
Financial data	Financial performance of the organisation, including revenue, expenses, assets, liabilities, cash flow, and investment information.
Operational and product data	Metrics on product and service performance, business processes, production, and resource use.
Intellectual property	Patents, trademarks, copyright, and trade secrets.
Intelligence	Competitive landscape, industry trends, and market conditions.
Legal and regulatory data	Information collected, stored, or processed to meet legal and regulatory requirements.
Partner and supplier data	Information on supply arrangements, contracts, and other third-party interactions.

BOX 0.1: What is data governance?

The policies, frameworks, and decision-making steps that guide the collection, availability, usability, integrity, and security of data at an organisation. It encompasses the people, processes, and technologies used to effectively control and maximise the value of an organisation's data throughout its lifecycle.

What is data management?

The collection, organisation, storage, protection, and use of data to support the organisation's operations and strategic objectives.

NOTE TO READERS

References to legislation and key resources are current as of May 2025. However, given the pace of change of privacy, AI and cyber security regulatory reforms, readers are encouraged to stay informed of developments.

This publication is intended as general guidance and does not constitute legal advice. The partners recommend seeking independent advice on legal, regulatory and technical matters.

We are interested in hearing from users of this publication about their experience, and invite feedback by email to policy@aicd.com.au

Intersection with cyber security resilience

Data governance and cyber security resilience are closely linked. At most organisations, boards will consider these key non-financial risk areas in tandem.

While data governance traditionally focuses on collection, quality, accessibility, and compliance, it also provides the foundation for effective cyber risk management. Classification and mapping of data assets directly supports the implementation of cyber controls, enables risk assessment, and helps prioritise protection based on data sensitivity and business value. In turn, strong cyber security practices underpin how data is protected.

Examples of the synergy between data governance and cyber security include:

1. Documented data location, classification and usage, assists the implementation of robust cyber security controls, including the principles of least privilege, zero trust, and increases the ease and speed with which organisations can respond to cyber incidents;
2. Defined data lifecycle management practices help mitigate cyber security risks by ensuring sensitive information is retained only as necessary and disposed of securely; and
3. When cyber security incidents occur, strong data governance frameworks (for example, comprehensive data inventories and classification schemes) enable faster identification of affected assets and fulfillment of regulatory reporting obligations.

MORE INFORMATION – CYBER SECURITY GOVERNANCE PRINCIPLES

Further guidance on least privilege, zero trust and effectively preparing for, and responding to, a cyber security incident is available in the AICD CSCRC Cyber Security Governance Principles.

Consumer behaviour versus community expectations

In Australia, directors need to be aware of the growing tension between consumer behaviour and broader community expectations around data privacy. Consumers often trade personal data for rewards, discounts, and tailored services (see **Box 0.2** for an example).

While consumers might be initially comfortable with the exchange, they may not fully grasp how their data is being collected, stored, and shared. The immediacy of benefits can outweigh long-term privacy implications. This passive consent creates an ongoing challenge for directors in balancing regulatory requirements with the broader ethical implications of how consumer data is handled.

BOX 0.2: Trade off example – Loyalty schemes

Loyalty schemes, which are highly popular across Australian retail sectors, encourage consumers to share information about their purchasing habits, preferences, and even demographic details. These programs offer tangible benefits – discounts, exclusive offers, and personalised recommendations.

Schemes, such as Flybuys and Woolworths Rewards are used by millions of Australians, indicating a high level of engagement and consumer willingness to exchange data for benefits. This reflects a behavioural pattern where consumers see the immediate advantages and may not fully consider the long-term implications of their data being collected, stored, or shared.

The ease of signing up for loyalty programs often leads to a passive form of consent.

Small businesses and not-for-profits

Small businesses, not-for-profits (**NFPs**), and charities in Australia face unique data governance challenges, particularly due to limited resources and expertise. However, there are still opportunities to unlock powerful insights from data that can drive product and service innovation.

Guidance for directors of small and medium enterprises (SMEs) and NFPs

In each of the principles there are practical data governance steps for directors of SMEs and NFPs. These steps are collated in the SME and NFP Board Checklist at **Appendix C.**

CHALLENGES

Small organisations often lack dedicated IT staff or data specialists, making it difficult to properly classify, secure, and maintain sensitive information about donors, beneficiaries, or customers.

The cost of implementing comprehensive data security controls, including meeting privacy requirements, can be burdensome for organisations operating on tight budgets. Additionally, staff training on data handling best practices can often take a back seat to more immediate operational concerns.

Critically, many charities and NFPs may also face heightened data governance risks due to the nature of the data they collect on individuals. This data may be particularly sensitive and confidential and relate to vulnerable members of the community. These organisations are rightly obligated – and expected by stakeholders – to secure this sensitive data.

OPPORTUNITIES

Despite these challenges, smaller organisations can harness data to drive organisational improvements.

Size and limited resources should not be an insurmountable barrier to using accessible and low-cost data solutions. For instance, cloud-based analytics tools and user-friendly visualisation platforms have become more affordable and accessible, enabling smaller organisations to gain valuable insights without requiring extensive technical expertise. Additionally, utilising cloud or SaaS solutions and infrastructure can bring not just data analytics benefits but also improve an organisation's cyber security posture.

> Without a high-quality data foundation, the effectiveness of technologies like AI and machine learning - and their potential to drive productivity and innovation - is constrained.

Regulatory landscape

KEY POINTS

1. Oversight of data governance forms part of directors' existing fiduciary duties under both common law and the *Corporations Act 2001* (Corporations Act).
2. Boards should have oversight of how the organisation meets its key regulatory requirements relevant to data, including under the *Privacy Act 1988* (Privacy Act).

Director duties

Board-level oversight of data governance and management, compliance and risk management form part of a director's existing duties under the Corporations Act. The Australian Securities and Investments Commission (**ASIC**) has emphasised the importance of board oversight over data management and related cyber security risk settings.

The AICD practice statement **Directors' oversight of company compliance obligations** and supporting legal opinion published in October 2024, outlines directors' duty of care and diligence. This duty is central to how a board approaches non-financial risk, including data governance.

Table 0.2 provides an overview of the key duties and obligations that a director should be aware of in the oversight of data governance.

TABLE 0.2: Core director duties

Duty to act with care and diligence	Directors have a duty to act with care and diligence to guard against key organisational risks. This includes being satisfied that appropriate systems and processes are in place to effectively oversee data management and risks.
Duty to act in good faith and in the best interests of the corporation	Directors must exercise their powers and discharge their duties in good faith in the best interests of the organisation, and for a proper purpose. In making decisions about data governance on behalf of the company, directors must consider the impact of those decisions on shareholders/members, and stakeholders including employees, customers, suppliers and the broader community.
Reliance on information and advice provided by others	While in some circumstances directors may rely on information or advice provided by others, or delegate certain data governance matters to a board committee or management role, this does not absolve directors of their accountability for decision making. In addition, a director may not have any specialty knowledge or expertise in data governance, however this does not mean that a director's standard of care is reduced.

INCREASED REGULATION AND GREATER REGULATORY SCRUTINY

Regulators are evolving their expectations, closely scrutinising data handling practices, and using enforcement tools to hold organisations to account.

Recent reforms to the Privacy Act enable the Office of the Australian Information Commissioner (**OAIC**) to impose significant penalties for contraventions of the Privacy Act, which is likely to increase enforcement activity. For serious breaches, the OAIC can seek penalties of up to $50 million; three times the benefit gained from a breach; or 30 per cent of the organisation's adjusted turnover if the value of the benefit cannot be determined by the court.

The OAIC has increased its enforcement activity, including by bringing proceedings against Meta Platforms, Australian Clinical Labs and Medibank Private.

While the OAIC is Australia's privacy regulator, it is not the only regulator taking action in relation to data practices. Other regulators with a focus on data governance include:

- the ACCC, which has successfully brought proceedings for misleading statements made about data handling practices;
- ASIC, which is actively investigating directors in connection with cyber incidents, and which has brought proceedings against RI Advice and FIIG Securities;
- the Foreign Investment Review Board (**FIRB**) which often imposes conditions requiring data (including personal information) to be stored in Australia and not accessed by overseas related entities; and
- Australian Prudential Regulation Authority (**APRA**), which has interrogated and audited data handling practices as part of its supervision of *CPS 234 Information Security*.

Key regulation overview

Appendix A provides a visual overview of key regulatory requirements relevant to data governance and management.

PRIVACY ACT

In Australia, privacy and the handling of personal information is primarily governed by the Privacy Act. The Privacy Act applies to federal government agencies and private sector organisations with an annual turnover of $3 million or more, as well as certain other entities (e.g. health service providers).

The Privacy Act contains 13 Australian Privacy Principles (**APPs**) governing:

- the collection, use, protection and disclosure of personal information;
- an organisation or agency's governance and accountability;
- integrity and correction of personal information; and
- the rights of individuals to access their personal information.

A key feature of the Privacy Act is the Notifiable Data Breaches scheme (**NDB scheme**) that imposes mandatory notification requirements in relation to certain data breaches.

For directors, the APPs serve as a baseline – but public expectations often surpass regulatory obligations.

OAIC GUIDANCE

More information on compliance with the Privacy Act, including the APPs, is available on the OAIC website here.

PRIVACY ACT REFORMS

In November 2024, the Australian Government passed the first tranche of reforms to the Privacy Act, based on proposals set out in the Attorney-General Department's *Privacy Act Review Report* (2022).[2] Key amendments included:

- the introduction of a tiered penalty regime for contraventions of the Act;
- a statutory tort for serious invasions of privacy; and
- new transparency requirements for organisations regarding automated decision making.

Many of the most significant proposed changes (including the proposed removal of the small business exemption, removal or modification of the employee records exemption, and the introduction of a 'fair and reasonable' personal information collection test) have been deferred to future reform tranches.

GENERAL DATA PROTECTION REGULATION (GDPR)

The **GDPR** is the European Union's comprehensive data privacy and security law. It establishes strict rules for how organisations must collect, process, store, and protect personal data of individuals in the EU – regardless of where the organisation is based.

Australian directors should be aware that the GDPR may apply to their organisation, even without physical EU presence, if the organisation offers goods or services to EU residents or monitors their behaviour. While similar to Australia's Privacy Act, the GDPR imposes stricter requirements, for example regarding breach notification and data subject rights.

Directors of large multinational organisations should have a working understanding of the GDPR and the differences in regulatory frameworks across the jurisdictions in which they operate. Directors should oversee decisions on whether data handling practices are uniform across the global business (for example, taking the most robust applicable law as the minimum standard) or whether a regional approach is more appropriate.

CYBER SECURITY AND SECTOR-SPECIFIC REQUIREMENTS

Australian organisations are subject to a range of regulatory requirements and standards that are relevant to data governance – these can vary by industry, sector and even state/territory. Depending on the industry, these obligations can be overlapping and complex.

Organisations should have a detailed understanding of the applicable requirements as part of a comprehensive data governance framework (**Principle 3**) and, separately, data incident response planning (**Principle 5**). The following is a non-exhaustive, high-level list of certain cyber security and sector specific requirements:

- *Cyber Security Act 2024*, particularly ransomware payment reporting requirements;
- *Security of Critical Infrastructure Act 2018* (**SOCI Act**), which applies to critical asset owners and includes specific risk management program obligations;
- APRA prudential requirements, including *CPS 234 Information Security and CPS 230 Operational Risk Management*;
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*;
- The *My Health Records Act 2012, Healthcare Identifiers Act 2010* and state/territory health records legislation, which apply to certain organisations in the healthcare industry; and
- the Consumer Data Right in the *Competition and Consumer Act 2010*, which currently applies to the banking and energy sectors.

2 Privacy Act Review Final Report (2023) and the Government Response (2023) are available **here**.

PRINCIPLE 1:

Key organisational data is a strategic asset

KEY POINTS

1. Boards should promote the effective use of key organisational data as a significant business enabler.
2. A robust data strategy aligns data governance practices with organisational priorities, supporting growth, innovation, regulatory compliance and stakeholder expectations.
3. To be effective, AI systems require high-quality data that is accurate, complete, consistent and timely.

The board has a key role in promoting organisational data as a strategic asset that drives innovation and growth across Australian organisations of all sizes.

Focus on the data that matters

Effective data governance at the board level starts with the board focusing on the data most critical to organisational success. Not all data is created equal. Boards should prioritise data that materially impacts strategy, performance, risk, compliance and stakeholder trust. Data-driven key decisions, digital transformation initiatives, and regulatory compliance should receive focused attention. Without this focus, oversight becomes diluted, reducing the effectiveness of governance.

Boards should not attempt to oversee the handling of all data. Instead, directors should support management in identifying and stewarding the organisation's key data assets – often referred to as 'crown jewel datasets'. Doing so enables a more focused and risk-based approach that supports strategic decision making, and alignment with business priorities.

For smaller organisations, identifying critical datasets may be simpler but is no less important. The board can encourage straightforward practices, such as creating a data register or asking management to highlight the top data assets that are critical to operations – like donor or client records, employee details, or grant reporting information.

Harness data and analytics for strategic impact

Organisations generate vast amounts of data through customer interactions, supply chain activities, internal operations, financial transactions, regulatory reporting, and market intelligence.

When systematically managed, and analysed, data provides insights for strategic planning and decision making. Effective data analytics can optimise operational efficiency, drive innovation, and strengthen risk management. To harness the full potential of data, it is useful to distinguish between four key types of analytics, as detailed in **Table 1.1**.

By applying these analytics techniques, Australian organisations across different industries can:

- Develop new products and services tailored to customer needs.
- Optimise operations by streamlining processes, reducing costs, and improving efficiency.
- Enhance risk management through early detection of fraud, cyber security threats, or operational risks.
- Drive continuous improvement by identifying trends and opportunities for innovation.

OPPORTUNITY EXAMPLE 1: PERSONALISED CUSTOMER EXPERIENCE

Effective customer personalisation enhances engagement, drives repeat business, and strengthens brand loyalty – creating long-term value for the organisation. Boards play a critical role in overseeing the strategic use of data and AI to ensure that personalisation initiatives align with the organisation's objectives, ethical considerations, and regulatory obligations.

For example, Netflix leverages advanced recommendation algorithms to personalise content based on user viewing history and engagement patterns, increasing retention and customer satisfaction.

Beyond recommendations, AI-driven personalisation extends to customer engagement strategies. Sephora, for instance, uses AI-powered chatbots to provide tailored beauty advice based on individual preferences.

TABLE 1.1: Core data analytical methods

Type	Summary	Example
Descriptive analytics – 'What happened?'	Examines past data to identify trends and patterns.	A retailer analyses sales data to determine which products sold best in the last quarter.
Diagnostic analytics – 'Why did it happen?'	Going beyond what happened, diagnostic analytics explores the causes of past events.	A bank identifies a rise in customer complaints and traces it back to a system outage that delayed transactions.
Predictive analytics – 'What is likely to happen?'	Using historical data and statistical models, predictive analytics forecasts future outcomes.	A healthcare provider predicts patient demand for services based on seasonal trends and past appointment data.
Prescriptive analytics – 'What should we do?'	The most advanced type, prescriptive analytics recommends actions based on data-driven insights.	An airline adjusts ticket prices dynamically based on real-time demand, competitor pricing, and weather forecasts.

UNLOCK THE POTENTIAL OF AI AS A STRATEGIC DATA CAPABILITY

Unlike traditional analytical methods that follow predefined rules, AI systems learn from data and improve over time. AI can significantly enhance business analytics, allowing organisations to move beyond basic reporting to real-time insights, predictive modelling, and automated decision making. AI technologies run the spectrum from agentic and generative AI to machine learning and robotic process automation.

However, poor data governance – such as underlying data quality issues – can lead to misleading insights, flawed decision making, and unintended biases – such as discriminatory customer profiling or hiring practices. As regulatory scrutiny around AI and data privacy intensifies, insufficient oversight can expose organisations to compliance risks. Additionally, AI systems are vulnerable to cyber security threats, including data breaches and adversarial attacks, further underscoring the need for robust data protection measures.

Boards play a critical oversight role in ensuring AI is deployed effectively, responsibly and ethically. This involves confirming that AI initiatives align with strategic objectives, are based on rigorous and verifiable datasets, comply with legal and regulatory requirements, and uphold principles of fairness, transparency, and accountability.

MORE INFORMATION – DIRECTORS' GUIDE TO AI GOVERNANCE

Further guidance on the governance of AI is available in the AICD HTI **Directors' Guide to AI Governance**.

Build a data strategy to treat data as an asset

WHAT IS A DATA STRATEGY?

A data strategy is a plan for how an organisation intends to harness its existing, and new, sources of data to support its broader strategic objectives. It provides a roadmap to transform data into a valuable asset, supporting innovation, operational efficiency, and competitive advantage. Depending on the organisation, a data strategy may sit under the umbrella of a broader data governance framework (**Principle 3**), or be a separate distinct program of work that is alongside a data governance framework.

For boards, a robust data strategy offers assurance that data initiatives align with strategic goals and are underpinned by measurable outcomes, such as improved efficiency and enhanced customer experience.

A data strategy can also be a core component of broader digital transformation initiatives, such as significant software platform upgrades. Without one, organisations risk adopting digital technologies without a clear understanding of how to effectively use and manage the resulting data.

Key questions that can help guide the development of a data strategy include:

- **What data is critical for achieving strategic objectives?** Identifying and prioritising the most valuable data assets ensures resources are focused on what drives value.
- **How and where will data be securely stored?** Data storage solutions must balance security, compliance, and accessibility to meet operational and regulatory needs.
- **How will data support decision making?** Will the right people have access to the right data at the right time to support informed decision making?

OPPORTUNITY EXAMPLE 2: CHURN PREDICTION

A machine learning algorithm can help organisations predict customer churn by analysing historical data and identifying patterns that indicate when a customer is likely to stop using a product or service.

Machine learning models can detect complex, non-linear relationships between multiple variables that may not be obvious to human analysts, making them more accurate and dynamic in predicting churn.

By recognising these patterns, the model assigns a churn probability score to each customer, helping businesses detect those at risk of leaving. This allows the business to take proactive steps, such as offering personalised incentives or targeted customer support, to improve retention and reduce revenue loss.

- **How will data from multiple sources be integrated?** A unified approach to data integration removes silos, enhances accuracy, and creates a single, comprehensive organisational view.
- **How and when will outdated or unnecessary data be safely disposed of?** Data retention and disposal policies ensure compliance and mitigate risks associated with data hoarding.
- **What governance policies and practices will guide data management?** Strong data governance frameworks promote ethical, legal, and responsible data use, reducing privacy, security, and bias risks.

ESTABLISH YOUR DATA BASELINE

Before developing and implementing a data strategy, it is good practice for an organisation to undertake a detailed data inventory, stocktake or mapping exercise. This provides an overview of the key datasets and their locations.

The inventory or stocktake should be presented to the board to assist directors in understanding the organisation's data landscape, informing the data strategy and aiding in data risk management.

WHAT MAKES A DATA STRATEGY EFFECTIVE? CORE COMPONENTS TO CONSIDER

The essential components of a comprehensive data strategy are outlined in **Table 1.2**.

TABLE 1.2: Building blocks for a data strategy

Component	Description	Key considerations for boards
Governance	Establishes policies, roles, and accountability for data management, ensuring compliance, security, and ethical use.	Does the organisation have clear governance structures to manage data responsibly and meet regulatory obligations?
Architecture and infrastructure	Defines how data is collected, stored, integrated, and accessed across the organisation, including cloud, on-premises, or hybrid solutions.	Is the data infrastructure scalable, secure, and aligned with the organisation's long-term needs?
Quality and integrity	Ensures data is accurate, complete, consistent, and reliable for decision making and operational use.	What measures are in place to monitor and improve data accuracy and reliability?
Security and privacy	Protects sensitive and critical data from breaches, cyber threats, and unauthorised access while ensuring compliance with privacy regulations.	Are risk management frameworks in place to mitigate cyber security and privacy risks?
Accessibility	Ensures the right people have access to the right data at the right time, balancing security with usability.	How does the organisation manage data access to prevent misuse while enabling efficiency?
Integration and interoperability	Enables data from multiple sources to be matched or consolidated into a single, unified view to support analytics and decision making.	Are systems integrated effectively to eliminate silos and improve cross-functional insights?
Analytics and business intelligence	Leverages data analytics, AI, and reporting tools to generate insights that drive strategy, operations, and competitive advantage.	Is data being used effectively to inform decision making and innovation?
Lifecycle management	Defines policies for data creation, retention, archiving, and disposal to ensure compliance and efficiency.	Are there clear processes for managing data throughout its lifecycle to reduce risk and cost?

Resources to support strategic data use

A clear understanding of existing and required resources by the board is fundamental to implementing a successful data strategy.

INTERNAL RESOURCES

Strong internal data capability relies on clear leadership and governance. In larger organisations, this may be led by a Chief Data Officer (**CDO**) or senior executive responsible for data strategy. Data management teams typically include data engineers, database administrators, and compliance officers who ensure data is appropriately collected, stored, and secured.

Some organisations also invest in specialised analytics and AI expertise – such as data scientists – to convert raw data into actionable insights, driving decision making and innovation. Underpinning those functions is the technology infrastructure, including data lakes, cloud platforms, and analytics tools that provide the foundation for efficient data storage and processing.

EXTERNAL RESOURCES

External resources play a vital role in supplementing internal capabilities, particularly where specialised knowledge is needed. Consultants and industry experts can assist in developing data strategies, implementing AI solutions, and ensuring regulatory compliance.

Organisations increasingly rely on external providers for key technological and data infrastructure, such as cloud-based storage solutions. Outsourcing digital and data functions can bring technological expertise and cyber security benefits. However, when considering outsourcing data functions, boards should balance the potential benefits (e.g. greater technological capacity) with the associated costs and data-related risks.

SMEs and NFPs – Key organisational data as a strategic asset

- Understand what is the current, and future, key organisational data that will move the needle for the organisation and customers/clients.
- Form a view on the capability of the organisation, including staff, to effectively use data.
- Identify where improvements in data collection and use can be made, including through the use of low-cost and accessible data analytics tools.
- Support strategic investments and initiatives to build data capability, including the capacity of staff/volunteers to use analytical methods.

APPLYING DATA AND ANALYTICS IN SMEs AND NFPs: TURNING INSIGHTS INTO IMPACT

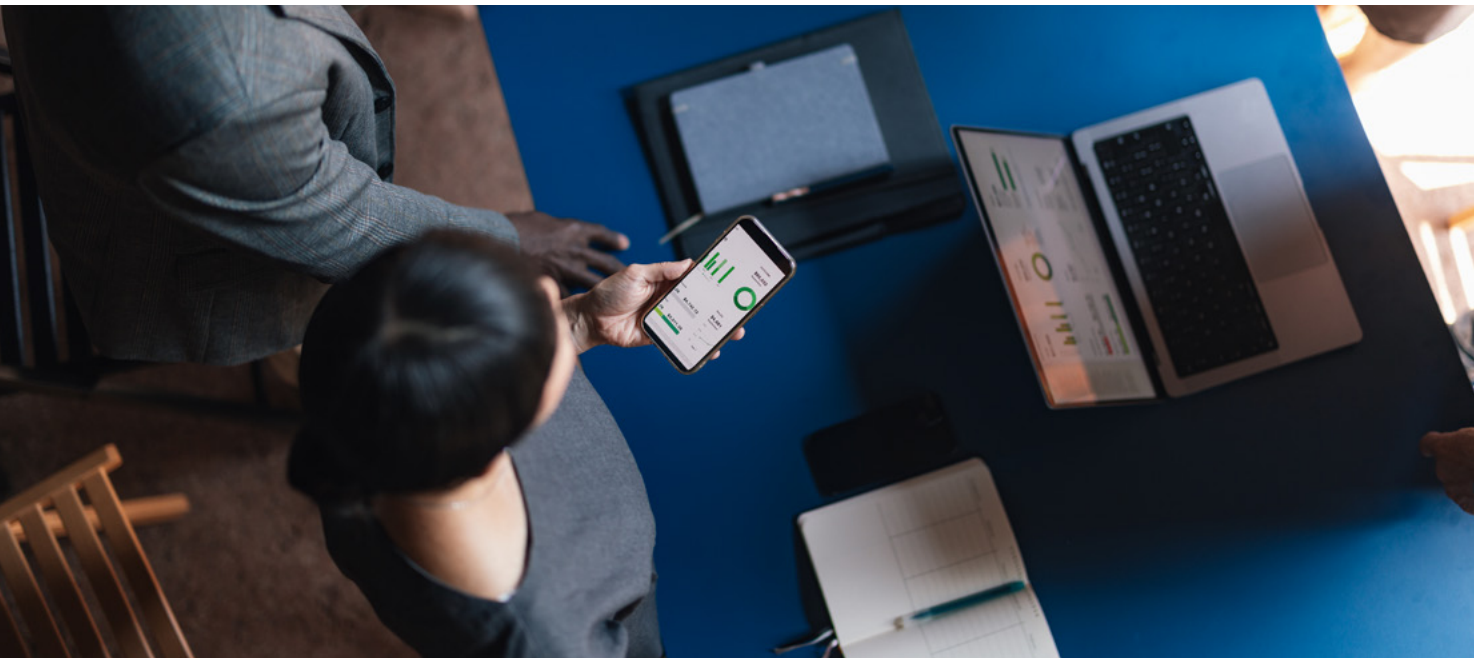
Smaller organisations typically operate with limited resources, making effective data use even more critical. Boards of SMEs and NFPs should actively explore innovative data uses to enhance product and service delivery and ensure optimal resource allocation.

Data responsibilities at an SME or NFP often sit with staff who wear multiple hats, such as an operations manager or IT lead. Affordable, user-friendly cloud platforms and external support – such as pro bono advisors, government-funded programs, or sector-specific resources – can help bridge capability gaps.

Table 1.3 provides examples of how standard data analytical approaches can have application in a small organisation. By integrating these different types of analytics, smaller organisations can make more informed decisions, promote growth and, in the case of NFPs, maximise impact.

TABLE 1.3: Analytical approaches for SMEs and NFPs

Descriptive	A bakery analyses monthly sales data to identify which meals and beverages are ordered during different seasons, helping it optimise inventory and staffing.
Diagnostic	A mental health NFP may notice a spike in crisis calls and use diagnostic analytics to identify that this increase was driven by recent funding cuts to social services.
Predictive	A food relief charity can analyse economic indicators and past distribution patterns to forecast which communities will experience higher food insecurity in the coming months. By pre-positioning stock in those areas, the organisation ensures timely support.
Prescriptive	A grocery store automatically adjusts weekly inventory orders based on weather forecasts, upcoming holidays, and local events, reducing both waste and gaps in shelves.



Measuring the strategic impact of data initiatives

A board, with management, should assess whether the organisation's data strategy is effectively supporting decision making, operational efficiency, innovation and value creation.

Table 1.4 outlines key assessment areas to assist the board in measuring the success of a data strategy and identifying opportunities for improvement. It may not always be possible to measure success by metrics such as ROI until after a project has been implemented and sufficient time has passed.

TABLE 1.4: Key board assessment areas for evaluating data strategy success and improvement opportunities

Area	Key considerations	Why it matters for boards
Quality and integrity	Is data accurate, complete, consistent, and timely? Are errors identified and corrected?	Poor-quality data leads to unreliable insights, increasing operational and strategic risks.
Utilisation and decision making	Is data actively used across the organisation to inform decisions? Are predictive models improving forecasting and decision making?	Data should assist operational and strategic decision making. Boards should monitor adoption rates and assess whether insights lead to better business outcomes.
Strategic and operational impact	Are data initiatives improving efficiency, reducing costs, and supporting innovation? Is data helping manage risks such as cyber security and fraud?	Data investments should translate into tangible benefits, enhancing performance, innovation, and risk management.
Regulatory compliance and ethical data use	Is the organisation compliant with the Privacy Act? Are AI models audited for fairness, transparency, and security? Do the data benefits outweigh potential privacy risks?	Regulatory and ethical data lapses can lead to financial penalties and reputational damage.
Return on investment (ROI)	Are data initiatives generating financial returns, improving productivity, or reducing operational costs? How is ROI measured?	Data investments are evaluated in terms of value creation, cost savings, and competitive advantage.

Why data-related initiatives fail

Despite the growing investment in data and AI initiatives, research suggests that over 80 per cent of data science and AI projects fail to achieve their intended goals.[3] Boards should be aware of the common pitfalls that lead to data-driven initiatives failing to generate value.

Common reasons for the low success rate include:

1. **Lack of a strategic alignment:** Many organisations launch AI and data projects without first identifying a business problem or strategic goal. When initiatives are not directly linked to organisational priorities, they often become technology-driven experiments rather than solutions that drive measurable impact.
2. **Poor data quality and accessibility:** Many organisations underestimate the effort required to ensure data is accurate, complete, and well-structured. Data silos, inconsistent formats, and incomplete datasets can lead to flawed insights and unreliable decision making.
3. **Lack of skilled talent or data-driven culture:** If the organisation lacks the right expertise, such as business analysts, projects may be poorly executed. Additionally, without a strong data-driven culture, teams may resist adopting new tools and insights, leading to poor take-up and underutilisation.
4. **Poor change management:** If leaders fail to prepare teams for new data-driven workflows and decision-making models, employees may struggle to effectively adopt them.

A common mistake is treating AI and data initiatives like traditional IT projects. Unlike standard IT deployments, AI and analytics projects involve continuous learning, experimentation, and refinement. Many failures occur when organisations expect immediate results without accounting for the complexities of deployment, integration, and monitoring.

Boards should expect change management strategies to be in place, along with clear responsibilities for the effective and efficient implementation of data initiatives.

Understanding these risks allows boards to ask critical questions about strategic alignment, resourcing, and effective governance. By being proactive, boards can support the organisation to avoid common pitfalls and instead reap the benefits of data as a competitive advantage.

PRINCIPLE 1:

Questions for directors to ask and governance red flags

QUESTIONS FOR DIRECTORS TO ASK

1. Does the organisation understand the underlying quality and accessibility of key business data?
2. Has the board reviewed a data strategy that clearly outlines how the organisation will enhance the collection, management and use of data?
3. How do data initiatives align with the organisation's strategic priorities?
4. Does the organisation have the resources needed to implement data initiatives or effectively harness existing data?
5. Does the board have quantifiable metrics that will assist the organisation to measure the success of data initiatives?

GOVERNANCE RED FLAGS

1. Data initiatives are not clearly linked to the organisation's strategic goals and business outcomes.
2. Data silos persist across teams and departments, hindering accessibility and the ability to extract meaningful insights.
3. Reliance on legacy or inadequate data infrastructure and tools, limiting the organisation's analytical capability.
4. Lack of a structured approach and dedicated resources for implementing data initiatives.
5. Lack of board visibility and oversight with no regular reporting.

3 Melbourne Business School Centre for Business Analytics, Why Do Analytics And AI Projects Fail?, August 2024, available here.

CASE STUDY 1:
Fitted For Work

Data is central to charities demonstrating impact and securing financial stability

National charity Fitted For Work (**FFW**) demonstrates both the challenges that charities can face with effectively harnessing data but also the opportunities.

FFW's purpose is to help women and gender-diverse jobseekers to become work-ready and find meaningful employment and, ultimately, economic independence. It does this through practical services, including assisting with developing resumes, skills development, job interview preparation, providing professional clothing and, importantly, helping clients regain self-esteem and confidence.

As with many charities, FFW is focused on securing its financial future and is moving to a revenue model that is less reliant on one-off grants to one that is focused on corporate partnerships and social enterprises. Central to this strategy is being able to utilise the data it collects on its clients and their outcomes to demonstrate its effectiveness to partners.

The FFW board has played a hands-on role in building the digital and data capability of the organisation, including via a Board Technology Committee. Critically FFW has made important progress in building its cyber security controls, recognising the sensitive information it collects and holds on clients. This has been done through significant investments and contracting with external providers.

The board has now turned its attention to building the data capability of the organisation, including accessing personal contacts and networks to provide FFW with external expertise.

A particularly acute challenge recognised by the board is recruiting people with the necessary data and technological skills. FFW uses Salesforce as its key customer relationship management software and more work needs to be done in supporting employees in inputting consistent, high-quality data and being able to extract insights.

Unlike a director role at a large company, directors have been far more actively involved in prompting and challenging management to improve data management practices, including asking:

- Do we ask the right questions of our clients and accurately input data as the client moves through different services?
- Do we understand what the data are telling us about our clients and the use of our services?
- Are we collecting the right data to accurately assess impact and success over time?
- Can we accurately report data to inform our decisions and revise our strategy?

Despite challenges, FFW has a powerful story about its impact. It has helped over 47,000 clients since 2005. According to the independent report *20 Years of Economic Impact*, FFW clients find employment within an average of 13 weeks, compared to an average of 53 weeks based on Australian Bureau of Statistics data. Using a median between these two, FFW has delivered $2.19 in direct net economic benefit to society for every $1 invested. However, there is broad awareness that more can be done to strengthen data practices in line with FFW's purpose and to better scale its impact.

Wendy Stops GAICD, Chair Fitted For Work, NED Coles Group and Chair, Industry Advisory Board at MBS' Centre for Business Analytics, contributed to the development of this case study.

CASE STUDY 2:
CAR Group

A data-driven culture should be underpinned by robust data governance

In Australia, there are few companies that compare to CAR Group (CAR) in the volume and complexity of the data that flows through the organisation and how central this data is to the ongoing success of the business.

CAR was founded in 1997 (as carsales.com) at the dawn of consumer e-commerce in Australia, with a business model focused on moving automotive print classifieds to the internet. It has since grown to become an ASX 50 company with significant businesses in Australia, the United States, South Korea, Chile and Brazil. This growth, and the increasing international complexity of the business, has necessitated a close focus by the board and management on the data governance practices of the group and its subsidiaries.

CAR, from the board down, has sought to promote a data-driven culture as key to driving innovation and meeting the needs of customers. The NEXT team is a dedicated standalone unit that is focused on developing and implementing innovative solutions across the group, including new uses of data to drive enhanced customer experiences of the future. Additionally, all employees are encouraged to take time out of regular business duties to work on individual side projects and there are separate incentives and prizes for innovation. This organisational focus on the opportunities of data is motivated by the highly competitive dynamics of digital classified markets and the need to be laser focused on the evolving expectations of customers.

The CAR board and senior management understand that a data-driven culture focused on innovation must have a bedrock of sound data governance. As CAR has grown, including through acquisitions and the associated need for integrating legacy systems, the complexity and volume of data held by the organisation has increased exponentially. This has necessitated an increasingly mature model for the governance and risk management of data.

A key data risk principle that CAR adopts is to apply the most stringent privacy and data regulations in the relevant jurisdiction as the baseline. This principle is central to maintaining customer trust with data handling practices. For instance, in the United States its Trader Interactive business follows privacy laws set in California. Additionally, there are strict limits on how data is shared across international borders. While intellectual property and technological innovations are shared within the Group in certain circumstances, the movement of customer of data is severely restricted.

CAR has a global data policy framework that sets the broad parameters by which data is governed across the group. Additionally, each international subsidiary has an AI and data governance committee with delegated responsibility to oversee data practices in that particular business. In certain circumstances, significant data governance decisions will be escalated to the Global Leadership Team and, possibly, the group board.

A key guiding principle that determines how CAR utilises data is 'just because we can, doesn't mean we should'. This may occasionally entail internal governance structures, or the board deciding not to proceed with, or approve, a particular data proposal from its people.

Jason Blackman GAICD, Chief Information Officer at CAR Group, contributed to the development of this case study.

PRINCIPLE 2:

Define clear data governance accountability

KEY POINTS

1. Clear roles and responsibilities form the foundation of effective data governance.
2. Comprehensive and clear board reporting – including engagement with management and updates on emerging trends – supports board oversight of data use and protection.
3. External providers play a growing role in data collection, management and protection and boards should have visibility over these providers' data handling and protection settings.

Directors should work with management to clearly define roles and responsibilities for data governance and data management. Roles and responsibilities should be captured in a data governance framework.

Role of the board

With clear strategic value in effectively utilising data, directors have an important role in overseeing the collection, use, protection and disclosure of data, and ensuring it is consistent with the organisation's values and strategic priorities.

Directors are expected to work with management to confirm that robust frameworks are in place for:

- the collection, protection, use and disclosure of sensitive information;
- maintaining data quality; and
- complying with relevant regulations such as the Privacy Act and any industry-specific requirements.

The board also approves resources for data governance initiatives and regularly reviews the effectiveness of data management practices, particularly as they relate to risk and strategic decision making.

Beyond compliance and risk management, the board should actively champion a data-driven culture. Directors should seek to understand how data governance impacts business performance and competitive advantage. Boards should also have confidence that the organisation has the talent and technological capabilities to execute its data governance strategy effectively.

In practice, the board's data governance role will overlap with its oversight of cyber security resilience and steps it is taking to enhance its resilience via a cyber security strategy.

Formal governance structures

At larger organisations, it may be appropriate to delegate data governance oversight to a nominated board committee – such as the risk or technology committee. A board committee with a clear mandate to oversee data governance can bring closer attention to the alignment of strategy and data initiatives and, separately, a strengthened focus on risk, including security, privacy and ethical considerations. A committee may also have more flexibility to have external advisors participate in discussions and provide input on key data and technology issues facing the organisation. However, given the dynamic nature of data collection and use, including AI technologies, aspects of data governance may warrant regular attention at full board meetings.

It also common for internal governance committees, forums or working groups to have delegated roles in overseeing data collection and use. These forums typically bring together cross-functional stakeholders to establish and oversee data policies, standards, and procedures. Usually led by senior management, these groups are focused on ensuring that data governance decisions balance business needs, regulatory obligations and stakeholder expectations. Better practice is for these internal, management-led governance forums to report back to a nominated board committee or the full board.

As noted in **Case Study 3**, Ramsay Health Care has established a Data Council to set strategic direction for data across the organisation. Chaired by a member of the Ramsay executive, data accountability is cascaded to data owners and stewards within the company.

Delegated roles through the organisation

In larger organisations, responsibility for data governance is cascaded through management and embedded in specific roles. Individual data responsibilities should be documented in position descriptions or role statements.

It is common for organisations to appoint a CDO, Chief Digital Officer and/or Chief Privacy Officer. A key structural consideration is the reporting line of the CDO. In many organisations, the CDO reports to the Chief Information Officer or Chief Technology Officer – framing data as an IT function rather than a strategic business asset.

Better practice is for the CDO to report directly to the CEO, reinforcing the view of data as a strategic asset, and enabling better integration of data governance, analytics investments, and AI initiatives with organisational priorities.

A frequent challenge is that data governance responsibilities may be shared across different roles or blurred with related functions, such as cyber security and digital/IT operations and projects. Role maps, scenario testing or workshops can support staff to better understand where responsibilities for data sits – and how it overlaps with cyber security, AI and broader digital functions.

Processes should be put in place to keep responsibilities current, especially as organisational structures change or new technologies are introduced.

DATA OWNERS, STEWARDS AND OFFICERS

In larger organisations, designated data owners, stewards or officers are commonly appointed. These individuals serve as the primary custodians of specific data domains or assets. Typically senior managers or subject matter experts, take responsibility for:

- defining data quality standards;
- determining access rights;
- ensuring compliance with relevant policies; and
- advocating for proper data handling practices.

They can often work closely with the CDO or Chief Privacy Officer to align specific data practices with enterprise-wide objectives.

Data owners also play a crucial role in change management – encouraging the adoption of new data practices and fostering a data-driven culture within their teams through regular communication and training.

In smaller organisations, it can be valuable to nominate key staff member(s) with explicit responsibility for data governance functions. For example, in a charity, this might include assigning responsibility for privacy and data security requirements to a staff member, given the sensitivity of the personal information often held by charities.

By embedding these responsibilities throughout the organisation, boards can have greater confidence that data governance principles are being promoted and monitored.

SMEs and NFPs – Data Accountability

- Ensure there is a senior manager with responsibility for key elements of data governance.
- Consider whether a director, or group of directors, should have a more active role in data management and cyber security oversight.
- Identify key digital providers and understand their data management and handling practices and controls.
- Work with management to develop a targeted number of metrics on data use and data risk controls.

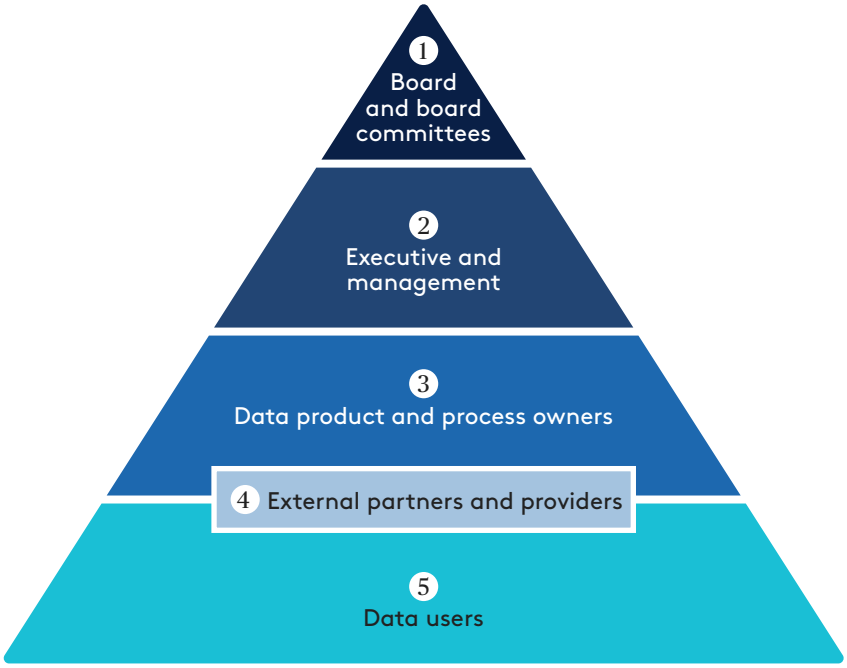
WHOLE OF ORGANISATION

Ultimately, sound data governance is a shared responsibility. Directors, staff and key partners all have a role to play in promoting good practice across the organisation. A whole-of-organisation approach to data encompasses:

- the collection and storage of data consistent with established policies;
- the protection of sensitive information; and
- a mindset that promotes and welcomes innovative data uses and applications.

Figure 2.1 provides a high-level summary of how data responsibilities may be allocated across an organisation.

FIGURE 2.1: Visual representation of organisational data responsibilities



1 Board and board committees

- Jointly set strategic objectives with management on data, consistent organisational risk appetite
- Approve key data policies and procedures, including Data Governance Framework
- Monitor data practices and the effectiveness of risk controls
- Oversee management response to critical data incidents

2 Executive and management

- Hold key responsibilities for data governance across the organisation, for instance with the CTO, CIO, Legal and CRO
- Develop data strategy and lead implementation of key projects and initiatives
- Understand and ensure compliance with regulatory obligations and align data with the organisational values
- Lead response to data incidents

3 Data product and process owners

- Implement data systems and processes
- Categorise and ensure data quality
- Monitor data protection and disposal
- Monitor compliance with regulatory requirements

4 External partners and providers

- Provision of data storage, management and protection of infrastructure and systems
- Expert assistance, advice and support, including during data incidents

5 Data users

- Collect and use data consistent with established policies, processes and regulatory requirements
- Engage with external providers of data on collection, protection and disposal
- Frontline response to data incidents

Role of external providers

Organisations increasingly rely on external providers and suppliers to process, store, and manage their data assets. While these third-party relationships often provide specialised expertise and cost efficiencies, they also introduce additional complexity into data governance frameworks and require careful oversight to ensure regulatory compliance and effective risk management.

Oversight of key providers is treated as an extension of the organisation's own data governance framework.

Data flow diagrams – which map how key data moves between the organisation and key suppliers, including identification of controls and points of internal and external access to the data – can be a useful tool to support board oversight.

Board engagement and reporting

In many organisations, reporting on data governance metrics is integrated into board reporting on cyber security, broader IT initiatives and business operations. For example, reporting might combine metrics on unauthorised access attempts through the organisation's security perimeter with supporting figures on the type of data targeted or exposed in such attempts.

Separately, how customers or clients provide data and modify data – such as through an organisation's website – can serve as both a business operations indicator and a broader data governance metric.

Table 2.1 provides a high-level summary of potential data reporting categories and metrics. Ultimately, the relevant reporting to the board will be dependent on the size and complexity of the organisation and the nature and depth of the data it collects and manages.

Board reporting itself represents a form of data-driven insight. The quality and timeliness of data contained in board packs can serve as an indicator of how effectively data is utilised across the organisation.

The board should work with management to ensure there is a holistic, timely and fit-for-purpose reporting framework in place – one that helps directors fulfill their oversight responsibilities and confirm that data governance practices are well integrated with cyber security settings and overall organisational objectives.

> “The quality and timeliness of data contained in board packs can serve as an indicator of how effectively data is utilised across the organisation.

TABLE 2.1: High-level summary of potential data reporting categories and metrics

Category	Indicators
Data quality and volume	• Growth – number of data entries; source of growth • Accuracy – number of anomalies; anomaly distribution • Completeness – percentage of records with all required values • Consistency – percentage of records with potential mismatches between fields • Timeliness – data currency; time since last update from source
Data use	• Data access rates and volume of data transferred by category or type • Most utilised data categories or types • Most underutilised data assets • Low-value and underutilised data categories • Average storage and processing costs per data product
Privacy Act and compliance	• Identified non-compliance with the Privacy Act requirements • Reportable breaches under the NDB scheme • Number of new and updated privacy notices • Correction and deletion requests • Review of consent forms
Risk and protection	• Cyber and data incident detection, prevention, and response, including incident trend analysis • Staff-related incidents (e.g. staff accessing or misusing data in breach of policies) • Internal audit activities, including outcomes of vulnerability and threat assessments • External assessments, including penetration testing results and benchmarking against peers and international standards
Projects, programs and outcomes	• Program maturity and progress, measured against forecast timelines and estimated utilisation • Resource allocation and costs tracking – monitoring investment and costs associated with data initiatives • Return on investment and impact measurement – linking data governance efforts to tangible business outcomes
Culture	• Number of appointed data champions, officers, owners or stewards • Percentage of staff trained on particular elements of data governance, including Privacy Act compliance • Meetings of internal data governance forums and summary of decisions and matters considered

PRINCIPLE 2:

Questions for directors to ask and governance red flags

QUESTIONS FOR DIRECTORS TO ASK

1. Does the board understand its oversight role in data governance, including via board committees?
2. Are roles and responsibilities for data governance defined and documented?
3. How is data ownership assigned across teams, and what mechanisms ensure data owners understand their responsibilities?
4. Does the board understand the role of key external providers in the organisation's data governance?

GOVERNANCE RED FLAGS

1. Board rarely discusses or considers agenda items on data governance.
2. No clear lines of senior management responsibility for data governance.
3. Unclear who has responsibility for compliance with the Privacy Act across the organisation.
4. Limited understanding of the role of external providers in the collection, use, storage and protection of key business data.
5. Board reporting on data governance is hard to digest and features excessive jargon with a reliance on technical solutions.

CASE STUDY 3:
Ramsay Health Care

At the heart of a data-driven culture is a foundation of clear data accountability

The board of Ramsay Health Care (Ramsay) has over recent years overseen significant investments in the digital and data infrastructure that have enabled the organisation to deliver value for employees, patients and doctors through data-driven actions, decisions, and outcomes. These investments have been focused on treating data as an asset and transforming clinical and non-clinical data into actionable insights to improve patient services and experiences, clinical outcomes, and organisational performance and growth.

To support this, Ramsay Data Hub – a cutting-edge data and analytics platform – was established in 2023 to provide a single, secure source of truth from across Ramsay's disparate information systems. At the time, Ramsay had over 50 information systems and data management was inconsistent and siloed. Data was not easily accessible and not used effectively. Data risks were also not well understood. It is estimated that Ramsay Data Hub saves analysts up to 1.5 days per week as they no longer need to gather data from multiple systems or maintain local data sources.

A hub-and-spoke data architecture was implemented in 2023 together with a central data and insights team. This included centralised data governance with data analysts distributed throughout business. Data governance accountability is provided by the Ramsay Australia Data Council which sets strategic direction and priorities for data across the organisation and is chaired by a member of the RHCA Executive team. Data responsibilities are cascaded to Data Owners and Stewards within the business.

Ramsay Data Hub brings critical data assets together in one place, enabling more effective data management and reducing risk, although some risks remain in the source systems. These data assets are stored securely on cloud technology which is scalable and can cater for increasing volumes and types of data. They are governed consistently, with standardised practices for access management, making data widely available to those who need it when they need it, while protecting patient privacy and other sensitive information.

Insight Suites, Ramsay's interactive dashboards, are built and hosted through Ramsay Data Hub and supported by consistent governance practices. These tools are designed around key user groups, including for example, Hospital Executives, Theatre Managers, Pharmacy Executives and Supply Chain Managers. They bring data and insights into the hands of Ramsay employees to highlight areas for attention and to inform decision making and planning. For example, Insight Suites allow users to manage theatre utilisation, plan resourcing and track admissions growth across Ramsay.

Ramsay Data Hub also supports a growing portfolio of predictive models and AI solutions, including generative AI, which is designed to improve efficiency, reduce manual effort and support Ramsay's growth strategies. User adoption and business impact are measured and tracked routinely to ensure that the investment drives returns for Ramsay, employees and patients.

Ramsay is building a data-driven organisational culture that includes well-established cyber and privacy training. Launching in 2025, Ramsay will run a Data Foundations program to upskill users, starting with Hospital Executives, to enhance data product adoption. In parallel, Ramsay has set up a Data Governance Community of Practice (from October 2024) to foster a culture of secure, trustworthy, and well-governed data and an Analytics Community (from February 2025) to incubate innovation and grow strong analytics best practices across the organisation.

David Thodey FAICD, Chair of Ramsay Health Care, and Dr Rachna Gandhi (PhD) Global Chief Digital and Data Officer, contributed to the development of this case study.

DIRECTOR REFLECTIONS:
Carmel Mulhern GAICD

The board has a key role to play in effecting sound data governance

A focus on data governance at the board level sets the tone from the top by signalling to the organisation that data governance is an organisational priority, according to director Carmel Mulhern GAICD.

The board often plays a multi-faceted role in the data governance settings of an organisation. On the one hand, data is a strategic asset, and the board should be setting the direction for management to explore opportunities to harness data to drive growth and enhance products and services for the benefit of customers or clients. On the other, the board should be a check on more adventurous and risky data practices that may be inconsistent with an organisation's values, community expectations or its legal and regulatory obligations.

Ms Mulhern noted that establishing appropriate board delegations and company policies when it comes to data collection, use, storage, destruction and protection is key to enabling the board to ensure that data is being appropriately managed and protected. This also supports the board having visibility of data decisions and issues that may have a material impact on the business.

Clear management-level responsibilities are essential to enabling the board to hold management to account, regardless of the size, complexity and amount of resources available to the organisation, stressed Ms Mulhern. The Chief Executive Officer, in many instances, will have ultimate accountability for data governance with the expectation that responsibilities are then cascaded through the organisation. In more complex organisations, internal governance structures – such as a Data Governance Forum – may be established to report directly to the board or its committees.

Ms Mulhern drew particular attention to the importance of boards understanding who in the organisation has accountability for compliance with the Privacy Act. The collection, use, protection, disposal, and disclosure of personal or sensitive information consistent with the Privacy Act obligations is a key compliance area. Breaches can carry significant legal and reputational risk, with recently increased financial penalties.

In larger organisations, there may be a Chief Privacy Officer, however even in smaller organisations there should be an individual or individuals who understand the privacy requirements and the obligation to protect personal or sensitive information collected from customers, clients and staff.

Ms Mulhern stressed that all staff should be aware that meeting privacy obligations is critical to maintaining an organisation's trust and confidence with its customers and clients, employees, regulators and other stakeholders. This is particularly pronounced for charities and not-for-profit organisations which often collect and protect highly sensitive information, including about vulnerable people.

Carmel Mulhern GAICD is a director of PwC Australia, Australian Cancer Research Foundation, Telstra Foundation and Methodist Ladies' College. Ms Mulhern is the former Group General Counsel of Commonwealth Bank and Telstra.

PRINCIPLE 3:

The data lifecycle and effective risk management

KEY POINTS

1. Identify the key data the organisation holds, including where it resides, how it is utilised, who has access to it and how it would impact business operations if compromised.
2. A data governance framework is a key mechanism by which the boards of all organisations can effectively oversee data management practices.
3. There are practical and low-cost controls that all organisations can utilise to mitigate risks associated with the data lifecycle.

As prominent data breaches have shown, the loss or compromise of key organisational data can inflict significant damage on an organisation, staff and customers. To mitigate these risks, the board should oversee thorough risk management practices.

Core elements of a data governance framework

A robust data governance framework gives the board confidence that key organisational data is being managed as a strategic asset, with appropriate controls for accuracy, security, and compliance with relevant regulations.

For many organisations, a data governance framework is not a standalone document, but rather a collection of policies, procedures and processes. Each board and the management team should determine how the framework is documented, approved and reviewed. What matters is that the framework clearly sets out how data is managed and protected throughout the data lifecycle.

As noted in **Principle 1**, a data strategy at some organisations may be a component of a framework although it is more common for it to sit separately as a discrete program that seeks to enhance data use at an organisation. The data strategy though should be grounded in the key principles and risk components of the framework. **Table 3.1** outlines the key elements of a framework.

TABLE 3.1: Core elements of a data governance framework

Type	Summary
Data lifecycle: principles, policies, procedures	Clear and comprehensive documentation for why data is collected, how data is collected, used, stored, shared, archived and destroyed.
Roles and responsibilities	Assignment of documented responsibilities for data governance to individuals or teams, holding them accountable for ensuring compliance with the framework. Role-based training should address sound data governance practices.
Data classification	A system or approach for classifying data, based on its sensitivity and importance. This will help to determine how the data should be protected and managed.
Data quality	Determine definitions of data quality, set thresholds and tolerances for acceptable standards based on data classifications, and outline processes for ensuring that data is accurate, complete and up to date.
Internal controls and security	Controls to ensure only authorised parties have access to data, and that data is accessed for authorised purposes only. Includes how data breaches are managed.
Review and update	Data should be reviewed and (if necessary) updated regularly to ensure it remains relevant, is of sufficient data quality, and retention is permitted in light of changing laws, regulations and business needs.

KNOW AND MAP YOUR DATA

An effective data governance framework starts with a comprehensive understanding of the organisation's data – what is collected and generated, why and how it is collected, disclosed and disposed of, and where it is stored. A valuable starting point for the board is requesting management develop a map or inventory of key datasets.

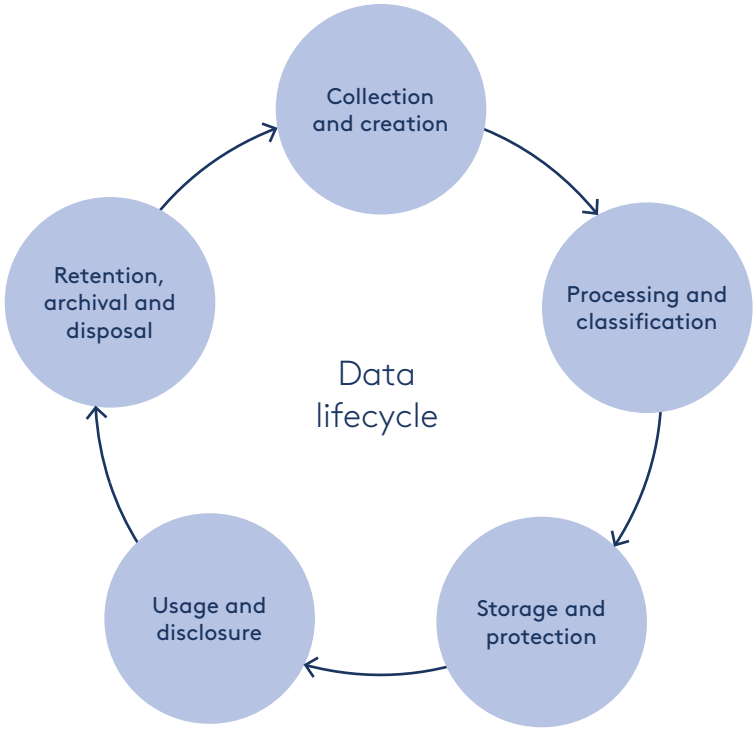
Key components of a data inventory can include:

- **Asset identification:** Each dataset, database or other data asset is identified.
- **Formats:** The technical formats and structures in which data is stored (databases, file types, structured/unstructured).
- **Ownership:** Who owns or controls each data asset, including business owners and technical stewards.
- **Classification:** Based on sensitivity, operations criticality, and regulatory requirements.
- **Location:** Where the data is stored physically or digitally, including on-premises systems, cloud environments, and third-party locations.
- **Lineage:** Where the data originates, how it flows through and entities, and any transformations it undergoes.
- **Usage:** Who uses the data, for what purposes, and how is it accessed.
- **Security controls:** Measures to protect the data, including access controls and encryption.

A data inventory can be complemented by the development of a data map that seeks to visually represent how data enters the organisation, is processed, used and stored, and ultimately archived or deleted.

While the development of a data inventory and data map can be a resource-intensive exercise, it can bring material governance benefits. This foundational knowledge equips a board to understand the organisation's key data assets and provides a basis for further engagement with management on how data is used and protected.

FIGURE 3.1: The data lifecycle – the end-to-end journey of data from creation or collection through processing, storage, usage, sharing, archiving, and disposal.



The data lifecycle

The data lifecycle refers to the end-to-end journey of data – from its creation or collection through its processing, storage, usage, sharing, archiving, and eventual disposal (**Figure 3.1**).

Understanding this lifecycle assists directors with informed oversight of data risks, compliance with regulations and maximising the strategic value of key organisational data.

COLLECTION AND CREATION

Data can be collected or generated from multiple sources and in a variety of ways. For example, it may be:

- collected from the source (whether individuals, organisations or devices) or from third parties, including purchased data;
- solicited or unsolicited;
- historical, static or real-time/live; or
- automated (e.g. data scraping, or metadata) or manually recorded.

As data volumes grow exponentially, good data governance should follow the principle of data minimisation – limiting data collection and retention to only what is necessary for operational and legal purposes. This principle is supported by the Privacy Act (specifically APP 3), which prohibits organisations from collecting personal information unless it is reasonably necessary for one or more of its functions or activities.

PROCESSING AND CLASSIFICATION

Before data can be used effectively, it generally undergoes certain processes including cleansing, merging, matching, classification, tagging and tracking, and correction. As data loads increase, automation of these processes becomes increasingly important.

All data collected, created or stored should be classified and these classifications should be recorded in a register. **Box 3.1** provides an overview of high-level data classifications.

Data classification helps ensure data is appropriately stored, accessed, protected, and disposed of when no longer required. Data classification can also help to inform the decisions made in the event of a data breach (e.g. prioritising breach notifications for particularly sensitive data).

BOX 3.1: Key data classifications

Public
Information that is freely accessible to read, research, review, and store. Carries the lowest level of security.

Internal-only
Accessible based on the role of an individual and security clearance.

Confidential
Accessible to a limited group of individuals or parties and often requires clearance or special authorisation.

Restricted
The most sensitive data classification. It is subject to strict security controls (like data encryption) to limit the number of people with access to the data and backup systems. If compromised, restricted data may pose a risk to public safety or privacy, or the proprietary information of an organisation.

STORAGE AND PROTECTION

The board should have oversight of how and where the organisation's data is stored and backed up, including the geographical location.

Offshore storage can pose additional risks, particularly if jurisdictional issues can limit an organisation's ability to effectively control and protect its data. For instance, regulators or enforcement agencies in other countries may have access rights to the data under local laws.

In some cases, Australian laws may require organisations to take extra precautions when data is stored offshore. This can include:

- transparency obligations under the Privacy Act; or
- addressing risks as part of developing and maintaining a 'Critical Infrastructure Risk Management Program' for certain entities under the SOCI Act.

RISK MANAGEMENT

The effective management of data risk should be a component of an organisation's risk management framework that is documented and overseen by the board. Data should also be called out as a specific risk and detailed on the risk register.

Implementing access and identity management controls is fundamental to protecting data from unauthorised access, disclosure, loss and misuse. These controls should be appropriately monitored and audit processes put in place to ensure such controls are effective. Common data management risk controls are highlighted in **Box 3.2** and risk management considerations relevant to AI are covered in **Box 3.3**.

Many data risk controls overlap with cyber security controls. For instance, the use of multi-factor authentication (**MFA**) for both internal and external users, and tiered privileged access rights, are common controls that serve data and cyber purposes.

BOX 3.2: Data management risk controls

Identity and access management controls include:

- Authentication and user access controls, including MFA.
- Change management for security control configurations;
- Privileged access management; and
- Enforcing appropriate password complexity, preventing insecure or common passwords, and avoiding password reuse across accounts.

Data loss prevention measures include:

- Security Monitoring: Timely detection and response to security incidents and volumetric alerts for large or abnormal data exfiltration.
- Security Assurance Testing: Annual penetration testing, internal audits and control effectiveness testing.
- Application Controls: Effective application controls for critical servers accessing sensitive information.
- Contractor Assurance: Regular audits, inspections, and testing of third-party contractors.

MORE INFORMATION – CYBER SECURITY GOVERNANCE PRINCIPLES

Further guidance on cyber risk controls that are relevant to data risk is contained in the AICD CSCRC Cyber Security Governance Principles.

Data usage and disclosure

Visibility over how data is used is a key component of the board's oversight of the data lifecycle and specific data risks. This visibility assists with:

- facilitating compliance with regulatory requirements (especially the Privacy Act, which prohibits certain uses and disclosures); and
- enabling the organisation to harness data value in an effective way.

Notably, data containing personal information cannot be used or disclosed for a purpose other than the primary purpose for which it was collected unless a relevant exception in the Privacy Act applies (for example, the individual has consented, or the use or disclosure is required or authorised by law).

Other considerations include:

- whether there are any third-party IP rights in the data and the nature and scope of those IP rights; and
- confidentiality obligations which may apply to the data (e.g. under employer-employee agreements, third-party agreements, or non-disclosure agreements).

Retention, archival and disposal of data

Organisations often retain data for extended periods – sometimes indefinitely. This may be driven by perceived commercial benefits, IT system complexity, legal obligations, customer service and potential claims, or the risk of future regulatory action.

However, the more data that an organisation holds, the more difficult and expensive it becomes to monitor, secure and, when no longer required, destroy. More data also increases the risk of a data breach and its potential impact.

The board should understand how the organisation approaches retention, archival and disposal of data. This should be documented.

Australia's data retention laws are also a maze, with over 800 federal and state laws imposing recordkeeping, retention, or destruction requirements (see **Appendix A**). These span tax and employment laws, anti-money laundering legislation and sector-specific obligations.

For larger or more complex organisations, where there may be uncertainty about data retention obligations, it may be appropriate to obtain external legal advice.

Where permanent destruction or deletion is not possible, organisations should consider archiving or putting data 'beyond use'. This typically involves implementing technical and operational controls to prevent the organisation and others from using or disclosing the information.

BOX 3.3: AI and data risk management

Data is the foundation of AI systems. Data, including personal information, is collected and used to train AI systems. It is both an input and an output of a deployed AI system.

The selection of data, particularly its quality, quantity, and representativeness, will significantly affect the performance of AI systems.

This dependence on quality data means that having effective data governance risk controls in place is crucial to the effective ethical use of AI.

To account for the use of AI tools and systems the board should:

- Confirm that data governance policies are updated to account for AI systems' specific characteristics and are aligned with how the organisation intends to leverage AI systems.
- Confirm that cyber security processes and controls have been reviewed and adapted to address AI systems and mitigate misuse.
- Understand the limits or deficiencies of the datasets and the steps management is taking to address these.
- Confirm the organisation's policy with its data being used to train third-party AI and how it is protecting that data.

Transparency and individual control

Transparency in data handling practices, and affording individuals (i.e. customers, clients, beneficiaries) the ability to control their own data, can improve compliance, enhance trust and create stronger business outcomes.

Boards, and board committees, should engage with management on the following:

- privacy policies and statements that are clear and accurate, and (where possible) use terminology or definitions consistent with the Privacy Act;
- critical information is disclosed upfront (not embedded or hyperlinked);
- consent to the use of personal information, where sought and required, is specific, informed, and voluntary;
- where intermediaries are used (e.g. brokers), privacy notices are provided or made to affected individuals – reliance on contractual obligations alone is insufficient; and
- individuals have a degree of control over their data and its uses – for example, via an online portal where they can amend personal details, change communication preferences or withdraw consent.

SMEs and NFPs – The data lifecycle and effective risk management

- Map key data flows and datasets and identify where this data is stored and who has access to it.
- Where possible, invest in cyber security enhancements, such as storing key data and systems with reputable cloud providers or migrating key functions to SaaS providers.
- Use secured devices for collection and storage of data, rather than rely on individual's personal devices.
- Minimise the collection of sensitive personal information and promptly delete it when no longer required.

Third-party risk management

The data and cyber resilience of an organisation is increasingly determined by the strength – or otherwise – of the risk controls that apply to key digital and data service providers.

The board should appreciate that the regulatory obligations and community expectations remain with the organisation – not the supplier or vendor. In other words, a failure by a vendor or supplier is not a defence for non-compliance by the organisation.

Boards should oversee whether internal capabilities and risk management processes are in place to understand the role and resilience of key suppliers.

BOARD VISIBILITY OF KEY DIGITAL AND DATA PROVIDERS

Documented roles and responsibilities should capture the key third-party suppliers and partners who support or manage the organisation's critical data and digital assets.

A Supplier Classification Matrix, categorising suppliers based on criticality and type of service or product provided, can assist in understanding the role of key providers. Categories should cover data storage and processing, software services and hardware providers.

This can be supplemented by data flow diagrams which map how key data moves between the organisation and suppliers – including identification of access points and applicable controls.

> A failure by a vendor or supplier is not a defence for non-compliance by the organisation.

DUE DILIGENCE AND ONGOING MONITORING

Due diligence processes are essential when appointing and monitoring key external providers and should endure through the term of the service arrangements. Boards should seek assurance that providers are meeting contractual obligations and expectations around data management and cyber security.

Key elements of oversight include:

- understanding the provider's location and ownership structure, including interdependencies with other IT systems and infrastructure providers (e.g. the software may be hosted within a cloud system of another company such as AWS or Azure), and any links or cooperation arrangements with foreign governments and foreign intelligence agencies;
- monitoring the provider's data and cyber security posture and settings, encompassing its contractual obligations and adherence to standards benchmarks (e.g. NIST CSF or ISO 27001). For high-risk or critical providers, this may include a vendor security risk assessment that is refreshed or repeated periodically;
- gaining visibility over subcontractors or partners used by the provider, and any notification obligations when these subcontracting arrangements change;
- confirming security considerations are reflected in contractual obligations and oversight arrangements, for example, reporting by the provider and notification settings for incidents; and
- confirming the provider's role is appropriately reflected in a Cyber/Data Incident Response Plan (see **Principle 5** for further guidance).

External assurance

External assurance or audit plays a crucial role in strengthening an organisation's data risk management through providing independent verification of control effectiveness.

When qualified third parties evaluate data security protocols, access controls, compliance measures, and incident response procedures, they bring both objectivity and specialised expertise that internal teams may lack.

This independent assessment helps organisations:

- identify vulnerabilities before malicious actors can exploit them;
- meet evolving regulatory requirements; and
- provide stakeholders with confidence that sensitive information is appropriately protected.

For larger organisations this may take the form of a SOC 2 report or benchmarking against international standards such as NIST CSF or the Essential Eight.

Directors of smaller organisations, including charities, should also consider seeking external expertise and assurance, where resources allow. For example through a targeted or narrow review of key data and cyber security controls, particularly in relation to sensitive datasets.

PRINCIPLE 3:

Questions for directors to ask and governance red flags

QUESTIONS FOR DIRECTORS TO ASK

1. Does the board understand what data our organisation collects, generates, holds and discloses, why it is collected, and where it is held?
2. Does the organisation know all of its regulatory obligations to retain, destroy or de-identify data?
3. Has the organisation identified retention periods for data, and do we have processes in place to ensure data is securely destroyed?
4. Does the board understand the data security controls deployed by our organisation as well as by our key digital providers?
5. Are the organisation's data security controls independently tested and verified?

GOVERNANCE RED FLAGS

1. Management cannot identify and explain a purpose for which data is collected and the risks associated with collection.
2. Public statements (e.g. in privacy policies) made about data handling practices do not reflect the organisation's actual data handling practices.
3. Key data risks are not identified on the risk register.
4. Outsourcing to a third-party provider, without understanding where data is stored, how it is secured, and the vulnerabilities of the third party's systems.

DIRECTOR REFLECTIONS:
Fiona Pearse FAICD

Sound risk management is a precondition for effectively harnessing data

Fiona Pearse FAICD views effective data risk management as foundational to every business.

Data collection, storage, transfer, use, reporting, and disposal can result in numerous risks. It is critical that these risks are embedded in existing organisational approaches to risk, including within the board-approved risk management framework, and a regularly reviewed risk matrix. Leveraging existing risk and governance processes, including board reporting, provides directors with visibility that data risks are being managed.

Ms Pearse recommends regular, focused data governance discussions at the board or Risk/Audit Committee to give the board a deeper understanding of data risks, the organisation's data governance architecture, and critical controls.

There is considerable value in an organisation undertaking a data stocktake that is recorded in a data asset register, according to Ms Pearse. This is a baseline exercise where information is recorded, such as what key business data is collected, where it is stored, who has access to it, how it is utilised by the business, and when it is destroyed. The data register should be updated on an ongoing basis. Focused reporting based on this stocktake and register allows the board and executive to understand critical business data risks and controls.

In large, data-rich organisations, Ms Pearse observed that it may be appropriate to establish a data governance committee at the management level. The data governance committee would have responsibility for the data asset register, data governance role delineation, and data lifecycle policies, principles and processes. Oversight of the resulting data governance system and policies would lie with the board Risk/Audit committee. Internal audits can provide the board with assurance that data governance systems are operating as expected.

With external providers increasingly being engaged to undertake various aspects of the data lifecycle – such as collection, storage and processing – it is critical that the board satisfies itself that management understands and is managing key vendor risks, according to Ms Pearse. Due diligence of key vendors is a key part of effective risk management and includes:

- contractual terms to cover data security, retention, destruction, and breaches; and
- external assurance of vendor data security controls, including the use of audits and assurance (such as a SOC 2 report) before contract, and at regular intervals during contract.

Ms Pearse stressed that small businesses, NFPs and charities must also take proactive steps to mitigate data-related risks. Limited resources do not lessen an organisation's obligation to protect often personally sensitive and confidential information. Boards of these organisations should ensure that management obtains the necessary external expertise to assist in data and cyber security risk management. She added that for many small businesses, NFPs and charities, using reputable third-party SaaS providers and cloud storage (preferably in Australia), in conjunction with a SOC 2 report, can materially reduce risk compared to holding data on in-house servers and systems.

Fiona Pearse FAICD is Chair of U Ethical, NED of Monash Health, NED of Smart Parking, and an independent member of the Victorian Parliament Audit Committee. Ms Pearse's former roles include NED of World Vision Australia, and a finance executive career at BHP and BlueScope Steel.

PRINCIPLE 4:

Empower a data-driven organisational culture

KEY POINTS

1. Boards set the tone from the top for a data-driven culture through championing the effective, ethical, and secure use of data – including in board decision making.
2. Education and training are essential for directors and staff to apply data effectively and foster an analytics mindset that promotes informed decision making, while managing associated risks.
3. Boards should promote data-informed decisions, including supporting organisational investments to use data to drive performance, innovation, and risk management.

Building a strong data-driven culture, from the board down, can help organisations better harness the value of data while managing emerging risks.

What is a data-driven culture?

A data-driven culture treats data as a strategic asset, embedding it into decision making, operations, and innovation. It reflects a commitment to harnessing analytics to generate insights, develop foresight, and drive evidence-based decisions.

Such a culture is built on ethical, legal, and secure data practices, reinforced by strong governance and stewardship to maintain trust, compliance, and accountability. Encouraging experimentation and responsible risk-taking fosters agility, continuous learning, and innovation, allowing teams to adapt and thrive in a rapidly evolving landscape.

A commitment to ongoing skill development ensures that both employees and directors are equipped to interpret, question, and apply data effectively. Together, these elements create an organisational culture where data propels strategic success and innovation.

> “Organisations with strong board support and executive sponsorship of data initiatives experience higher returns on analytics investments and outperform those where leadership engagement is lacking.

Setting the tone from the top

A data-driven culture is grounded in strong leadership from the board and senior executives. Their actions signal the importance of data as a strategic asset across the organisation. By fostering a data-driven culture where data is central to decision making, boards can help strengthen organisational resilience, improve competitiveness, and drive long-term sustainable growth.

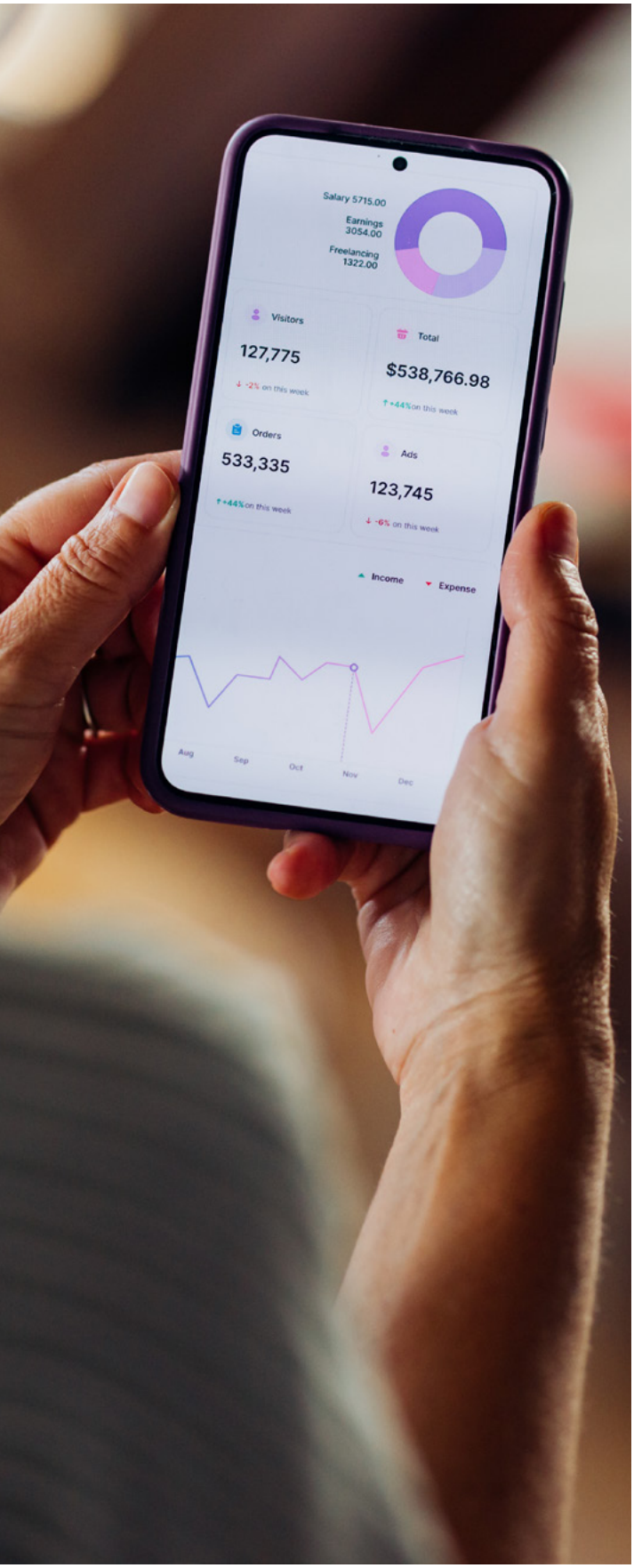
Research by MBS and Kearney found that organisations classified as ‘analytics leaders’ demonstrate clear C-suite and board-level commitment to embedding data into strategy, operations, and governance.[4]

Boards play a pivotal role by:

- ensuring that data and analytics are standing items on the agenda;
- allowing for consistent alignment with the organisation’s objectives; and
- regularly reviewing whether data initiatives are driving growth, innovation, and operational efficiency, supported by metrics and dashboards.

Where appropriate, the board should sponsor and support targeted investments in data initiatives. This includes areas such as technology infrastructure, analytics talent, and employee training. The MBS–Kearney research found organisations with strong executive sponsorship of data initiatives experience higher returns on analytics investments and outperform those where leadership engagement is lacking.

4 Melbourne Business School Centre for Business Analytics and Kearney, The impact of analytics on the triple bottom line, January 2021, available here.



OPPORTUNITY EXAMPLE 3: USING DASHBOARDS FOR REAL-TIME INSIGHTS – A BALANCED APPROACH

Interactive dashboards provide boards with real-time visibility of financial, operational, and risk data, enabling directors to monitor market trends, customer engagement, cyber security threats, and compliance metrics.

These tools can be powerful for tracking progress against strategic goals, identifying risks early, and responding proactively to emerging issues.

However, it is important for directors to be mindful of the limitations of dashboards:

- **Correlation versus causation:** Dashboards often present simple visual correlations that can be misinterpreted as causal relationships. Directors should question the underlying data and analysis to understand the true drivers behind trends.
- **Univariate thinking in a multivariate world:** People naturally interpret data in a univariate manner – focusing on one variable at a time – while real-world organisational dynamics are often complex and multivariate. Boards should recognise that outcomes are influenced by multiple interconnected factors.
- **Over-reliance on surface-level insights:** Dashboards may not capture the full context or nuances behind the data. Directors should engage management in deeper discussions to understand what is driving performance.

To make the most of dashboards, boards should treat them as decision-support tools rather than definitive answers.

INTEGRATING DATA INTO BOARD DECISION MAKING

For a board to set the tone for a data-driven culture, it must also demonstrate data-informed decision-making processes. This results in board activities that are grounded in evidence-based insights rather than intuition or precedent. Boards can adopt the following structured approaches to integrating data into their governance and decision making.

1. **Expect data-backed board reports and presentations:** Board materials should be supported by high-quality, relevant data. Directors should require management to present KPIs, data visualisations, trend analyses, and predictive insights – not anecdotal or subjective reports. Reports should provide clear, actionable insights rather than raw data.
2. **Embed data-driven discussions into board meetings:** Where appropriate, data should be a central part of board discussions, with directors actively questioning the integrity, relevance, and implications of the data presented. Boards should ask:
    - What does the data tell us that we did not already know?
    - Are we seeing long-term trends or short-term fluctuations?
    - How does this data impact our strategic priorities and risk management?
    - What data gaps exist, and how do we address them?
3. **Apply predictive and scenario analysis for strategic planning:** Boards should move beyond reviewing historical data by encouraging the use of predictive analytics and scenario modelling. These techniques help assess potential risks, market shifts, and investment opportunities.
4. **Use benchmarking and external data for context:** Boards should not rely solely on internal organisational data. Using industry benchmarks, publicly available competitor data, regulatory reports, and economic indicators provides valuable context. Boards should expect that management compares company performance against industry peers and incorporates external data sources where relevant.
5. **Ensure responsibility for data-driven decisions:** To reinforce a data-driven culture, boards should set expectations for measuring the success of data initiatives and hold management accountable for implementing decisions and acting on insights. Regular post-decision reviews should assess what can be improved.

ETHICAL USE AND STAKEHOLDER EXPECTATIONS

The board plays a key role in setting the principles for the ethical use of data, extending beyond compliance with the Privacy Act.

Boards should not just ask '**can we?**' – but importantly, '**should we?**'

This critical heuristic – or ethical lens – is central to the governance role. It may, in some cases, mean that a board chooses not to approve or support certain data practices that are inconsistent with the organisation's values or reputation.

Further, with increasing automation in data analytics and decision making – including the use of generative AI systems – the board also plays a key 'human' oversight role that challenges more adventurous or risky data uses and applications. In undertaking this role, the board will need to balance diverse stakeholder expectations regarding data practices. Customers, employees, investors, regulators, and communities each bring different perspectives on what constitutes responsible data use.

SMEs and NFPs – Data-driven culture

- Invest in basic data literacy training for all staff, and volunteers where appropriate, focusing on practical applications rather than technical complexity.
- Identify data champions who can advocate for data solutions, monitor risk settings and support their colleagues.
- Create visible wins by selecting one business challenge to solve through data, demonstrating tangible benefits that build enthusiasm.
- Lead by example through asking for data analysis and reference data in decision making.
- Celebrate and recognise employees and volunteers who use data effectively to improve processes or outcomes.

Benefit: Unlocking opportunities

A data-driven culture thrives on collaboration, experimentation, and the strategic availability of data to uncover and act on opportunities with speed and precision.

In such a culture, experimentation is a central practice. It enables organisations to test new ideas in small, measurable ways to uncover what works and what does not. This approach reflects the cultural emphasis on learning through data and encourages a **'fail fast, learn fast'** mindset, where insights from failures are as valuable as those from successes.

By relying on data to validate hypotheses and refine approaches, experimentation becomes a driver of continuous improvement and innovation. Data-driven organisations embrace this iterative process to adapt quickly to market changes or customer needs.

This culture also fosters collaboration by breaking down silos and promoting data as a shared resource across teams. Cross-functional teams can combine insights to uncover opportunities that may not be visible from a single team's vantage point.

Benefit: strategic risk management

A strong data-driven culture significantly enhances an organisation's ability to manage risks by embedding data-driven practices into every stage of the risk management process, from identification and assessment to mitigation.

This approach transforms risk management from a reactive process to a proactive, forward-looking capability. Organisations leverage data and advanced analytics – such as predictive models – to detect emerging risks and early warning signs of potential threats, ranging from financial fraud to supply chain disruptions.

High-quality data allows organisations to quantify risks more precisely and empower the board and the leadership to address vulnerabilities before they escalate.

Education and training

A strong data-driven culture is built on a foundation of data literacy and fluency across all levels of the organisation, including the board and senior executives. Education and training empower staff to understand, interpret, and apply data effectively, creating a shared language and mindset around data-driven decision making.

For a data-driven culture to thrive, education and training must extend beyond technical roles that directly engage with data, such as analysts or data scientists. All staff, regardless of their function, benefit from an understanding on how data creates value, impacts their work and contributes to the organisation's objectives.

This universal approach breaks down silos and enables cross-functional collaboration, ensuring that data practices are embedded throughout the organisation's operations.

Crucially, commitment to data literacy must start at the top. The board and senior executives should actively participate in data training. This signals the strategic importance of data and positions data education as a business enabler rather than an optional or box-ticking exercise.

Training on data should be a component of continuous learning, helping staff stay ahead of emerging trends, tools, and technologies. Proactive upskilling and reskilling builds organisational resilience and agility, enabling the workforce to respond effectively to future challenges and opportunities.

TRAINING ON DATA PROTECTION AND CYBER SECURITY

Training and education should also address compliance obligations, including Privacy Act requirements, as well as data risk control practices. Best practice is for all staff in organisations subject to the Privacy Act to undertake regular training on the core obligations.

Even where the organisation is exempt (e.g. revenue less than $3 million per annum) it is advisable to still educate staff on expected practices for handling personal information.

Mandatory cyber security training and testing exercises are also key to sound data governance. Cyber security and data protection training should go beyond the induction or orientation process for new staff, including directors. It should occur at least annually. Boards should receive regular management reporting on training participation and results, including differences between business areas.

MORE INFORMATION – CYBER SECURITY GOVERNANCE PRINCIPLES

> All staff, regardless of their function, benefit from an understanding on how data creates value, impacts their work and contributes to the organisation's objectives.

Further guidance on cyber security training and education is contained in the AICD CSCRC Cyber Security Governance Principles.

PRINCIPLE 4:

Questions for directors to ask and governance red flags

QUESTIONS FOR DIRECTORS TO ASK

1. Do we as directors use key business data and analytical approaches to inform our decision making?
2. Does the organisation understand our stakeholders' expectations for how we collect, protect, use and disclose their data?
3. How are new data investments and solutions received in the organisation? Is there a culture of openness and innovation or one of resistance?
4. Does the organisation have a program of data training and data literacy that includes senior management and directors?

GOVERNANCE RED FLAGS

1. Data and analytical tools are not regularly used in board discussions or decision making and board packs lack data rigour.
2. Low digital and data literacy among board members and no plans to support directors obtain greater knowledge.
3. Limited or no training and support for staff on the collection, use and protection of data across the organisation. For example, no mandatory training on Privacy Act obligations.
4. Cultural resistance to utilising data in decision making and an unwillingness to adopt new data analytical software and tools.

CASE STUDY 4:
Coles Group

Enhancing an organisation's data capability can improve performance and competitiveness

Coles Group (Coles) has undergone a significant digital and data transformation over the past five years, focused on strengthening its competitive proposition in retail. With support and advocacy from the board, Coles has made significant capital and operational investment to harness the vast volumes of data it receives from customers, employees and suppliers. The board and senior management have also been key in promoting a data-driven culture, where decisions across the vast organisation are increasingly grounded in data analytics.

With more than 1,800 retail outlets across Australia, 115,000 employees, 8,000 suppliers and millions of customers per week, a huge volume of data flows through Coles daily.

To help boost on-shelf availability, Coles is leveraging a sophisticated AI system to forecast demand 100 days in advance, generating 109 billion daily data predictions. Along with making sure Coles is ordering only what it needs, when it needs it, the business has also rolled out a network of automated distribution centres (ADCs) and online customer fulfillment centres (CFCs) across Australian states. These investments support more efficient in-store stocking and, critically, the processing of its growing online business.

Further, Coles is also exploring generative AI, including a virtual assistant that can provide team members with responses to common HR queries. What is currently a very manual process, with responses taking up to 48 hours, will eventually result in team members getting answers within seconds.

These data-focused innovations are now resulting in tangible improvements in productivity and business performance. However, these are the results of major digital and data transformation projects – backed by significant financial investment, and management and employee focus – that take time to bring to fruition.

Although the board reviews and approves significant data governance decisions based on specific thresholds or delegations, and exercises its oversight of risk management in the organisation, it also became necessary to establish robust data governance processes and structures led by management.

The introduction of an internal Data Governance Council is a key mechanism by which Coles' senior management ensures a consistent approach to data governance, controls and the assessment of AI use cases across the business. This structure assesses not just the business case for certain data applications, but also the responsible use and ethical development of AI technology and models. Further, Coles has developed its own ethical AI framework that is aligned with the Australian Government's Ethical AI Principles.

The Coles board recognised the importance of supporting management with its digital and data transformation journey, while ensuring appropriate data strategies and governance guardrails were in place. By enhancing Coles' data capabilities, the board aimed to strengthen organisation's competitive position and improve financial performance.

Wendy Stops GAICD, NED of Coles Group, Chair of Fitted For Work and Chair, Industry Advisory Board at MBS' Centre for Business Analytics, contributed to the development of this case study.

PRINCIPLE 5:

Enable effective data incident response and recovery

KEY POINTS

1. The board and management should proactively plan for a variety of plausible data incidents.
2. A clear and transparent approach to communications with impacted individuals and other stakeholders is key to mitigating reputational damage, complying with regulatory requirements and facilitating an effective recovery.
3. Data incidents can be an opportunity for organisations to substantially improve data governance practices.

The board plays an essential role in both preparing for and responding to data incidents. When an incident occurs, the board's role lies in balancing strategic oversight and operational enablement. This is done by overseeing critical decisions on stakeholder communications, regulatory notifications, and reputation management, while empowering management to execute a swift tactical response.

Spectrum of data incidents

A board should be aware that there are a variety of data incidents that impact an organisation's business operations, employees, customers and brand reputation. This spectrum is summarised in Table 5.1.

TABLE 5.1: Spectrum of potential data incidents

Incident	Summary
Cyber-attack and resulting data breach	• Unauthorised access to sensitive information • External hacking, ransomware or malicious data activity • Exposure of personal, financial, or critical organisational data
Data loss or compromise	• Accidental internal corruption of data • Hardware/software failures causing data loss • Insider actor undertakes malicious data tampering
Data leakage or unintentional release	• Unintentional public disclosure of information • Misconfigured or incorrect access permissions
Privacy Act breaches	• Non-compliance with data protection regulations • Improper handling of personal information • Improper collection, use or disclosure, or inadequate protection, of personal information
Human error	• Accidental deletions • Mishandling of sensitive information
Operational failure and disruptions	• System downtime or degradation prevents data input or extraction • Critical data unavailability

Plan and prepare

The board has a key role in ensuring an organisation is prepared for a critical data incident.

A strong starting point is a robust data governance framework, underpinned by a current data inventory or map. Visibility of key datasets and holdings will assist the board in overseeing the planning for a potential critical data incident. This knowledge also enhances an organisation's ability to respond quickly to an incident.

A key control is the maintenance of reliable backups of key data and systems. Regular testing and refreshing of backups can minimise the impact on business operations during an incident.

Given many data incidents stem from cyber security events, better practice is to develop an organisation-wide cyber security and data incident response plan (**Response Plan**). The AICD publication **Governing Through a Cyber Crisis** has extensive guidance on planning for a significant cyber or data event, including the key elements of a Response Plan and the importance of backups.

Boards should confirm that a Response Plan:

- extends beyond technical considerations to include comprehensive communication strategies for stakeholders, regulatory disclosure requirements, and business continuity measures that minimise operational and reputational damage;
- is subject to regular testing and simulation exercises, including board participation; and
- identifies weaknesses in risk controls/defences and gaps in organisational knowledge (e.g. who has access to legacy data/systems).

MORE INFORMATION – GOVERNING THROUGH A CYBER CRISIS

Further guidance on preparing for a significant cyber/data event is contained in the **AICD CSCRC Ashurst Governing Through a Cyber Crisis**.

Incident response

The board should oversee the key decisions of management during the immediate response phase of a significant data incident.

While management, or the crisis management team at larger organisations, typically leads the response to the incident until it is contained, the board – depending on the severity of the incident – should receive regular updates and be clear which decisions must be escalated to the board for approval.

The board will also play a critical role in reviewing and probing the assumptions and decisions made by management. Depending on the significance of the data incident, central issues for the board include:

- Confirming whether the organisation has triggered the appropriate response plan(s) and has a robust cadence of meetings, updates and action items. For listed companies, the continuous disclosure sub-committee should also be convened.
- Assessing that affected areas of the organisation have been identified and an understanding of the impacts on business operations, employees and customers has been established.
- Assessing the accuracy, completeness and timeliness of communications to employees, customers and third parties.
- Evaluating the nature and sensitivity of compromised data and confirming whether a data breach has occurred. Checking that regulatory notifications or continuous disclosure obligations have been considered and actioned.
- Confirming that key third-party providers are prioritising and assisting on the incident.
- Identifying what resources (internal and external) are available to support.
- Ensuring insurers are notified and insurer consents have been obtained, where required.

SMEs and NFPs – Effective data incident response and recovery

- Prepare a Response Plan that covers critical cyber security and data incidents
- Conduct a simulation exercise, war game or hypothetical exercise to test various scenarios against the Response Plan.
- Communicate honestly, clearly and empathetically with impacted stakeholders.
- Consider whether compensation, such as product or service discounts, for impacted customers/clients may assist in rebuilding reputation.
- Learn from the incident and take practical steps to improve data governance practices.

Communications

A central component of a comprehensive Response Plan is a communication and notification strategy. This should:

- identify key stakeholders;
- outline regulatory notifications; and
- include template notifications, where possible.

Depending on the severity of the incident, the board may approve select communications – such as an ASX disclosure – or directly communicate with key stakeholders (e.g. government representatives).

Organisations should notify affected individuals as soon as practicable, communicating the available information – while noting it may later prove to be incorrect. This transparency is important to enable individuals to mitigate any risks they may face. Investigations by cyber forensic teams can take weeks or months, especially if monitoring and logging capabilities are inadequate or have been tampered with by threat actors.

It is important for directors and management to balance the limited information they have with the need to communicate transparently with affected individuals. The following steps can assist:

- when making public statements or notifications about an incident, clearly outline known facts, unknowns, and next steps for affected individuals and stakeholders;
- avoid speculation; and
- ensure all statements are reviewed by legal advisors.

REGULATORY NOTIFICATIONS AND THE NBD SCHEME

In the event of a critical data incident, organisations may have mandatory reporting and notification obligations. The nature and type of the reporting will differ based on the particular laws applying to the organisation. These should be identified and documented in the Response Plan, and the board should oversee and have visibility of how these obligations are being met.

In respect of a data breach involving personal information, the key obligation is notification under the NDB scheme to the OAIC, and notifying impacted individuals when the breach is likely to result in serious harm.

In addition to the NDB scheme, an organisation may often have numerous other related notification requirements, particularly if the data incident is connected to a cyber security incident. For example, if the organisation is a critical asset owner, it will have notification obligations under the SOCI Act. Separately, if the organisation has paid a ransom associated with a ransomware incident, it must report this to the ASD and the Department of Home Affairs.

MORE INFORMATION – CYBER INCIDENT REPORTING

More information on cyber incident reporting is available on the ASD website **here**.

More information on the NDB scheme is available on the OAIC website **here**.

Supporting impacted individuals

The board should promote an incident response that recognises the human impact of a critical data incident – on employees, customers and broader stakeholders.

An organisational response that is grounded in empathy and overseen by the board is more likely to mitigate reputational damage and be more effective.

Directors should confirm that management is:

- communicating transparently and empathetically with impacted employees and customers/clients;
- providing assistance to impacted individuals, including (where possible) financial support to replace government-issued identifiers and documents;
- using social media, website FAQs, or a dedicated telephone line; and
- considering the range of appropriate remediation options for impacted individuals.

It is also common, following a data incident, for affected individuals to exercise their right to:

- request access to the personal information that an organisation holds about them (under APP 12) – this may or may not be limited to the specific information compromised in the incident; or
- require correction of personal information held about them (under APP 13).

MORE INFORMATION – CYBER SECURITY GOVERNANCE PRINCIPLES

Further guidance on human focused communication following a critical cyber/data incident is contained in the AICD CSCRC Cyber Security Governance Principles.

Assessing compromised data after an incident

A board should understand how the organisation will assess compromised data, the timeframe for assessment, and what external assistance may be required.

An organisation's ability to rapidly understand the data that has been compromised in a data incident and the impact on the business, individuals and others, is critical to any incident response – yet it is often overlooked in cyber and data incident planning.

It can often take weeks, if not months, to make an assessment. The pressure to accelerate the process frequently results in increased errors which can quickly attract the ire of affected customers, regulators, and the media, resulting in regulatory compliance breaches (especially notification requirements).

The challenges of assessing compromised data reinforces the importance of having comprehensive backups in place to assist in recovery.

UNSTRUCTURED DATASETS

A board should understand that assessing compromise or damage to unstructured datasets (e.g. the contents of compromised email accounts or documents in network drives) can be particularly challenging.

Reviewing this data is more fraught than a typical document review or discovery exercise because affected individuals need to be accurately identified, and then information about a specific individual – which often sits in multiple files or documents – needs to be correlated. This increases the risk of generating false positives or negatives. A careful mix of algorithmic or AI tools, human oversight and review is often required.

Lessons learnt

The board should oversee a comprehensive post-incident review. A full review should be sponsored by the board with the final report and recommendations considered at board-level. In large complex organisations, it is good practice for the review to be undertaken by an independent third-party expert.

Regardless of the nature of the incident – whether a data breach or systems failure – a review would generally cover the key areas outlined in Box 5.1.

Following such a review, the board should monitor and regularly assess management's progress in addressing issues and implementing recommendations. A rigorous lessons learnt process is essential to rebuilding reputation and demonstrating to internal and external stakeholders that both the board and organisation have learnt from the incident.

BOX 5.1: Key components of a post-incident review

1. **Initial detection and response timeline**: assessment of how quickly and effectively the incident was detected and addressed
2. **Breach scope and impact:** what data was compromised, which systems were affected, and how many customers/users were impacted
3. **Technical cause analysis:** what failed or was exploited
4. **Incident response process evaluation**: effectiveness of the Response Plan
5. **Third-party/vendor involvement:** assessment of external parties involved in the response efforts
6. **Regulatory compliance and reporting:** evaluation of compliance with relevant requirements
7. **Customer/stakeholder communication:** effectiveness of communications
8. **Remediation steps**: how we assisted impacted stakeholders
9. **Recommendations**: specific improvements to prevent similar incidents and strengthen data governance

MORE INFORMATION – GOVERNING THROUGH A CYBER CRISIS

Further guidance on preparing for a significant cyber/data event and post-incident reviews is contained in the AICD CSCRC Ashurst Governing Through a Cyber Crisis.

PRINCIPLE 5:

Questions for directors to ask and governance red flags

QUESTIONS FOR DIRECTORS TO ASK

1. Does the organisation have an incident Response Plan that is regularly tested and uplifted following simulation exercises?
2. In the event of data loss or theft, how will we communicate with customers, notify regulators, and meet our NDB scheme requirements and other regulatory notification requirements?
3. Do we have data and systems backups we can access to restore operations?
4. Do we know what external support we may need to access to assist with response?

GOVERNANCE RED FLAGS

1. There is no Response Plan that is regularly reviewed, tested and updated.
2. The Response Plan has been prepared by the Technology team with limited or no input from other relevant functions.
3. Comprehensive system and data backups are either not in place or are out of date.
4. The approach to response and communications is overly technical and legal with no consideration of the human impact of the incident.
5. No lessons-learnt process or active steps taken to enhance data governance practices.

APPENDIX A:
Regulatory requirements

PRIVACY AND DATA HANDLING

Upcoming: Further reforms to the Privacy Act

Privacy Act, including APP 11.1 and 11.2[1]

Australian Consumer Law, including undisclosed data practices[2]

APRA CPS 234 Information Security

APRA CPG 235 Managing Data Risk

ASIC Act[3]

Spam Act

Do Not Call Register Act & **Telemarketing Standard**

Consumer Data Right[4]

Over 800 federal and state laws impose overlapping record retention and destruction obligations

National Consumer Credit Protection Act 2009 & **Financial Accountability Regime Act 2023**

GOVERNANCE AND RISK MANAGEMENT

Privacy Act including APP 1.2[5]

Corporations Act

APRA CPS 234 Information Security

APRA CPS 230 Operational Risk Management (once commenced)

APRA CPG 235 Managing Data Risk

APRA CPS and SPS 220 Risk management

Other APRA Prudential Standards and Guidance

Financial Accountability Regime Act

FIRB requirements

1 **Australian Privacy Principle *(APP)* 11.1** – obligation to destroy and de-identify personal information; **APP 11.2** – obligation to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure.

2 **Australian Consumer Law *(ACL)*** contained in Sch 2 of the Competition and Consumer Act 2010 (Cth) – the Australian Competition and Consumer Commission has a broad remit to investigate 'undisclosed data practices' – bringing a sharp focus on to transparency of data practices.

3 *Australian Securities and Investment Commission Act 2001* (Cth) ss 12DA and 12DB.

4 Consumer Data Right, established through Part IVD of the Competition and Consumer Act 2010 (Cth). The regime was slated to be rolled out to insurance – although it is unclear when this will occur following the consultation on proposed changes to the regime last year.

5 APP 1.2 – obligation to put in place policies, procedures and practices to ensure compliance with APPs.

6 ***Privacy Act 1988* (Cth), Part IV Notifiable Data Breach scheme** – mandatory notification to OAIC / individuals when a data breach is likely to cause serious harm.

7 ***Security of Critical Infrastructure Act 2018* (Cth)** – SOCI bound entities must notify the Australian Cyber Security Centre (ACSC) within 12 hours of a cyber incident with a significant impact, or within 72 hours of a cyber incident with a relevant impact.

DATA AND CYBER INCIDENT RESPONSE

Privacy Act, including the NDB scheme[6]

TFN Rule

Security of Critical Infrastructure Act[7]

Corporations Act, including reporting obligations, continuous disclosure obligations and directors' duties[8]

Terrorism financing, financial crime and sanctions laws[9]

Competition and Consumer Act[10]

APRA CPS 234 Information Security[11]

Cyber Security Act, including the mandatory ransom payment reporting obligations[12] (once commenced)

Organisations may also need to comply with other sector-specific legislation or licensing requirements.

APRA CPS 230 Operational Risk Management (once commenced)[13]

DATA PROTECTION AND OPERATIONAL RESILIENCE

Privacy Act APPs 1.2, 11.1 & 11.2

ASIC Act

APRA CPS 234 Information Security

Security of Critical Infrastructure Act

APRA CPS 230 Operational Risk Management (once commenced)

8 ***Corporations Act 2001*** **(Cth)** ss 180, 181 duties of directors; ss 292, 299 reporting obligations; s 674A continuous disclosure obligations.

9 Organisations must not make payments to a threat actor or deal with assets if the threat actor is a designated person or entity (e.g. *Criminal Code Act 1995* (Cth), State based crimes acts, *Proceeds of Crimes Act 2002* (Cth), *Autonomous Sanctions Act 2011* (Cth), *Charter of the United Nations Act 1945* (Cth)).

10 ***Competition and Consumer Act 2010*** **(Cth)** s 18 – prohibition on misleading and deceptive conduct. Consider disclosures/statements made in the wake of a cyber incident.

11 ***CPS 234*** paragraphs 35 and 36 – notification to APRA as soon as possible (or within 72 hours) after becoming aware of an information security incident that has, or could have, a material effect, or which has been notified to other regulators; and within 10 days of becoming aware of a material information security control weakness that it cannot remediate in a timely manner.

12 ***Cyber Security Act 2024*** **(Cth)** – reporting business entities must report ransomware and cyber extortion payments within 72 hours of making the payment or becoming aware that a payment has been made. Obligations will commence on 29 May 2025. Consultation for the content of any mandatory report closed in February 2025.

13 ***CPS 230 (Operational Risk Management)*** paragraph 33 – notification to APRA as soon as possible (or within 72 hours) after becoming aware of an operational risk incident that is likely to have a material financial impact, or a material impact on the organisation's ability to maintain critical operations.

APPENDIX B:
Resources

1. AICD
   a. **Cyber Security Governance Principles** (in partnership with the CSCRC)
   b. **Governing Through a Cyber Crisis** (in partnership with the CSCRC and Ashurst)
   c. **Directors' Guide to AI Governance** (in partnership with Human Technology Institute (HTI) at the University of Technology Sydney)
   d. Director tool: **Data and privacy governance**
   e. **Cyber Security Handbook for Small Business and Not-for-Profit Directors** (in partnership with AISA)
2. MBS Centre for Business Analytics
   a. **Why do analytics and AI projects fail?**
   b. **Enterprise AI Governance for Senior Executives**
   c. **The Impact of Analytics on the Triple Bottom Line** (in partnership with Kearney)
3. Allens
   a. **AI Governance Toolkit for General Counsel and Boards**
4. OAIC
   a. **Australian Privacy Principles guidelines**
   b. **Data breach preparation and response**
   c. **Privacy for not-for-profits, including charities**
   d. **Guidance on privacy and developing and training generative AI models**
5. Cyber and Infrastructure Security Centre
   a. **Overview of Cyber Security Obligations for Corporate Leaders**
6. Office of the National Data Commissioner
   a. **Foundational Four – Starting an ongoing data improvement journey**
7. Governance Institute of Australia
   a. **Data governance in Australia (2023)**
8. International Organization for Standardization
   a. **ISO/IEC 38505-1:2017 – Information technology – Governance of IT – Governance of data**
   b. **ISO/IEC 27001:2022 - Information security, cyber security and privacy protection — Information security management systems**

APPENDIX C:
SME and NFP Board Checklist

PRINCIPLE 1:
Key organisational data is a strategic asset

- Understand what is the current, and future, key organisational data that will move the needle for the organisation and customers/clients.
- Form a view on the capability of the organisation, including staff, to effectively use data.
- Identify where improvements in data collection and use can be made, including through the use of low-cost and accessible data analytics tools.
- Support strategic investments and initiatives to build data capability, including the capacity of staff/volunteers to use analytical methods.

PRINCIPLE 2:
Define clear data governance accountability

- Ensure there is a senior manager with responsibility for key elements of data governance.
- Consider whether a director, or group of directors, should have a more active role in data management and cyber security oversight.
- Identify key digital providers and understand their data management and handling practices and controls.
- Work with management to develop a targeted number of metrics on data use and data risk controls.

PRINCIPLE 3:
The data lifecycle and effective risk management

- Map key data flows and datasets and identify where this data is stored and who has access to it.
- Where possible, invest in cyber security enhancements, such as storing key data and systems with reputable cloud providers or migrating key functions to SaaS providers.
- Use secured devices for collection and storage of data, rather than rely on individual's personal devices.
- Minimise the collection of sensitive personal information and promptly delete it when no longer required.

PRINCIPLE 4:
Empower a data-driven organisational culture

- Invest in basic data literacy training for all staff, and volunteers where appropriate, focusing on practical applications rather than technical complexity.
- Identify data champions who can advocate for data solutions, monitor risk settings and support their colleagues.
- Create visible wins by selecting one business challenge to solve through data, demonstrating tangible benefits that build enthusiasm.
- Lead by example through asking for data analysis and reference data in decision making.
- Celebrate and recognise employees and volunteers who use data effectively to improve processes or outcomes.

PRINCIPLE 5:
Enable effective data incident response and recovery

- Prepare a Response Plan that covers critical cyber security and data incidents.
- Conduct a simulation exercise, war game or hypothetical exercise to test various scenarios against the Response Plan.
- Communicate honestly, clearly and empathetically with impacted stakeholders.
- Consider whether compensation, such as product or service discounts, for impacted customers/clients may assist in rebuilding reputation.
- Learn from the incident and take practical steps to improve data governance practices.

APPENDIX D:
Glossary

Term	Definition
ACCC	Australian Competition and Consumer Commission
Agentic AI	AI system that can autonomously set goals, make decisions, and take actions to achieve complex objectives with minimal human intervention
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
Cloud computing	A service model that enables network access to a shared pool of computing resources such as data storage, servers, software applications and services
Essential Eight	The eight essential mitigation strategies that the ASD recommends organisations implement as a baseline of cyber security resilience
FIRB	Foreign Investment Review Board
Generative AI	AI system that produces new content – such as text, images, and code – based on existing data
ISO 27001	International Organization for Standardization: Information security, cyber security and privacy protection — Information security management systems
Least privilege	A security model in which users, processes, and systems are granted only the minimum permissions necessary to perform their required functions
Machine learning	Algorithms that identify patterns in data to make predictions and automate decisions
MFA	Multi-factor authentication – a method of access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism
NDB scheme	Notifiable Data Breaches scheme
NIST CSF	National Institute of Standards and Technology – Cybersecurity Framework
OAIC	Office of the Australian Information Commissioner
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment
Robotic Process Automation	Automates rule-based, repetitive tasks such as data entry, compliance reporting, and invoice processing, improving efficiency and accuracy.
SaaS	Software as a Service – a cloud-based software delivery model where organisations subscribe to applications rather than purchasing and installing them locally
SOC 2	A security framework that specifies how organisations should protect customer data from unauthorised access, security incidents, and other vulnerabilities
SOCI Act	*Security of Critical Infrastructure Act 2018*
Zero Trust	A security model that requires strict identity verification and continuous authentication for every user, device, and application attempting to access resources within a network

ACKNOWLEDGEMENT OF COUNTRY

The Australian Institute of Company Directors, Melbourne Business School and Allens acknowledge the Traditional Custodians of the Lands on which we are located and pay our respects to the Elders, past and present. We acknowledge the First Nations people across this Country and recognise their unique cultural and spiritual relationships to the Skies, Land, Waters, and Seas and their rich contribution to society.

ABOUT AICD

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and not-for-profit sectors.

ABOUT MBS

Melbourne Business School is home to Australia's best MBA and business analytics degrees, as well as executive education courses for professionals and custom solutions for organisations. As part of MBS, the Centre for Business Analytics was founded in 2014 to address the worldwide demand for AI and analytics research, knowledge and education. To learn more and engage with the Centre for Business Analytics, please visit our **website**.

ABOUT ALLENS

Allens is a leading international law firm with a long-standing reputation for shaping the future through pioneering legal work, regulatory insight, and a commitment to impact across the community. Our firm has a strong track record advising on high-stakes digital initiatives – from data governance and the responsible use of AI, to complex tech procurement, large-scale transformation projects, and cyber risk management and incident response. We bring sharp legal insight and deep sector knowledge to help clients deliver with clarity and confidence in an evolving digital landscape.

DISCLAIMER

COPYRIGHT

For more information:

T: 1300 739 119
E: **policy@aicd.com.au**

JOIN OUR SOCIAL COMMUNITY

CCT-1591_25