Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

2025 AASB Research Forum

Accounting and Reporting in the Digital Era

Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

The Future of Financial Reporting?

Data + Judgment + “Storytelling” = Relevance & Insight

Professor Michael Davern, FCPA

Australian Government
Australian Accounting Standards Board

The Challenge

THE UNIVERSITY OF MELBOURNE

- **The Existential Threat:**
  - AI (cheap, fast and agentic)
  - Ubiquitous real-time data (albeit noisy)
  - Computational resources
- **The Accountant's Defence:**
  - Professional Judgment
  - Contextualised data "storytelling"
  - Trust and Credibility (relational)

Are we ready?

- Are current standards fit for this defence?
- Do we have the required Expertise?
  (Policymakers, Regulators, Preparers, Auditors and Users)

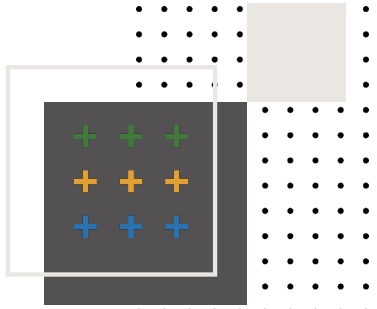
Australian Government
Australian Accounting Standards Board

Research to Inform Policy

THE UNIVERSITY OF MELBOURNE

Concepts where principles and practice are in tension

1. Materiality and Relevance
   (e.g., AASB Research Report 21)
2. The Reporting Entity in a hyperconnected, sustainable economy
   (e.g. GHG Scope 3 reporting)
3. Measurement uncertainty
   (e.g. Intangibles)
4. Sector-neutrality
   (e.g., Leases, Sustainability Reporting)
5. Users and User Needs/Expectations
   (Leases, Sustainability Reporting)



Australian Government
Australian Accounting Standards Board

Research to Inform Policy: Some Examples

THE UNIVERSITY OF MELBOURNE

- **Tolerate Measurement Uncertainty to encourage use of judgment**
  - Explore expanded recognition of Intangibles (1,3,5)
  - Rethink the recognition vs. disclosure decision (1,3,5)
  - Explore how to effectively communicate uncertainty (3,5)
  - How to encourage judgment, without loss of trust and credibility

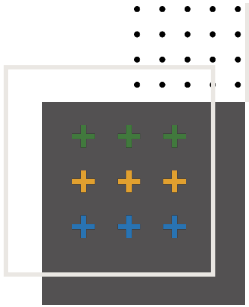
- **Service Performance Reporting and Sustainability Reporting**
  - How “connectivity” between financial and non-financial metrics can enable contextualised “storytelling”(2,4,5)
  - How do we apply our financial reporting expertise in broader reporting regime? (1,2,4,5)
  - Who are our users and what are their needs in the context of the reporting entity? (1,2,4,5)

Australian Government
Australian Accounting Standards Board

Attack is the best Defence:

THE UNIVERSITY OF MELBOURNE

- **Revisit Sector Neutrality!**
  e.g. Public sector and NFP: AASB 16 Leases is not fit for purpose
- **Prioritise Advancing Service Performance Reporting!**
  Meaningfully report on the activities of all entities
- **Embrace measurement uncertainty!**
  Relevance and materiality should drive recognition
- **Enable and encourage professional judgment!**
  It's where there is the most value add
- **Adopt digital reporting (XBRL)?**
  To maintain our role as the business data storyteller



Australian Government
Productivity Commission

Harnessing data and digital technology

AASB Research Forum – 17 November 2025

Julie Abramson, Commissioner

pc.gov.au

The Productivity Commission acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to their Cultures, Country and Elders past and present.

The data and digital opportunity

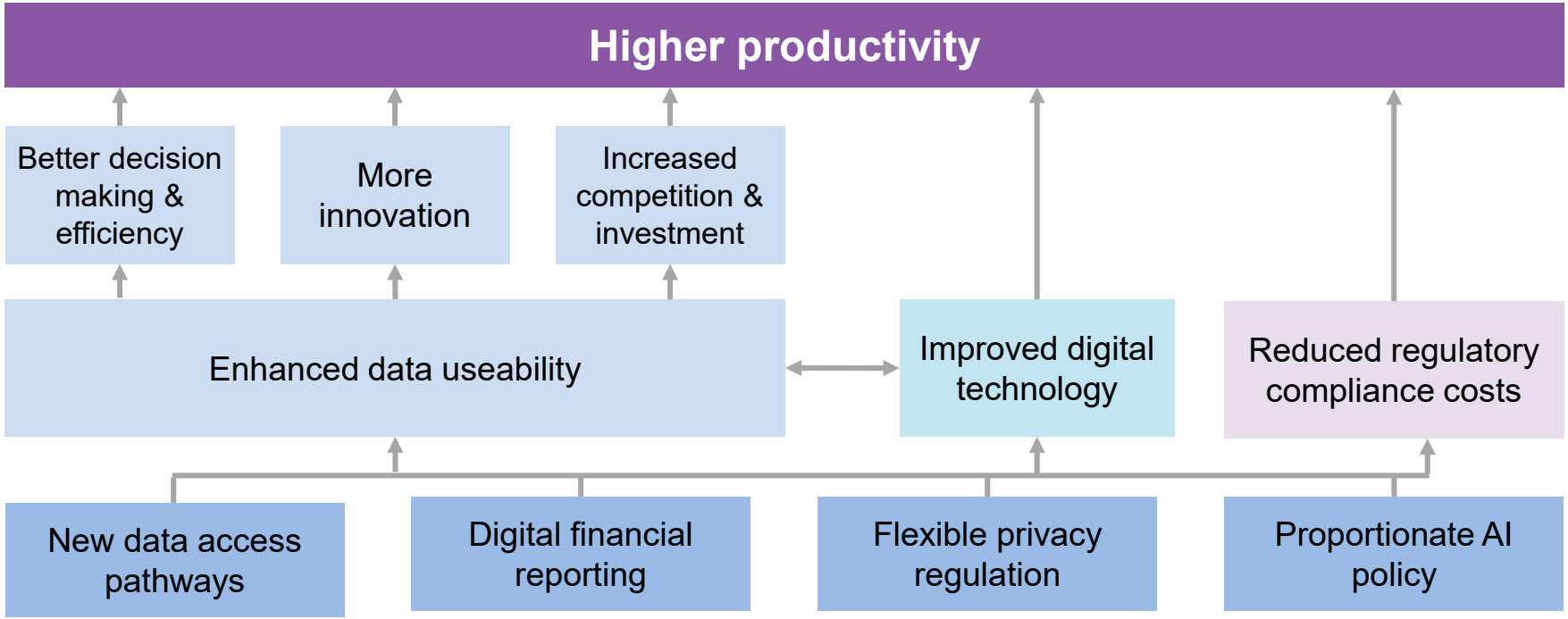
Data and digital technologies are the modern engines of economic growth

Past	Present	Future
ICT contributed up to **0.3 percentage points** to growth in the late 1990s	**Digital activity** contributes **6%** to GDP	**AI** could add **$116B** to GDP
Internet and mobile phone adoption raised GDP per capita by **3%** 2004-2014	**Data formation and analysis** are worth **10%** of investment	A **mature data sharing regime** could add up to **$10B** to GDP

Source: PC calculations, PC (2004, p. 7), Qu et al. (2017, pp 66-67), ABS (2024), Smedes et al. (2022)

How do our reforms boost productivity?

Our package of reforms



Our timeline

Artificial intelligence

AI is already being used throughout the Australian economy

Participants told us they use AI for:

- Teaching and training tools
- Writing software code
- Identifying cyber threats and maintaining cyber security
- Responding to customer inquiries
- Making scheduling and admin work easier

We found examples of it being used in many industries:

- Alerting bank customers of potential scams, and identifying if customers have been coerced
- Drafting legal material and research
- Sorting avocados
- Prioritising deliveries and routes
- Cataloguing Aboriginal rock art
- Inspecting coastlines for fishing net waste

The productivity benefits of AI for Australia are uncertain, but could be large – perhaps a 4.3% boost to labour productivity growth over the next decade

Analyse regulation to identify AI gaps before considering economy-wide AI regulation

Where could there be gaps?

Can existing regulation bridge the gap?

Some of this work is already under way or complete

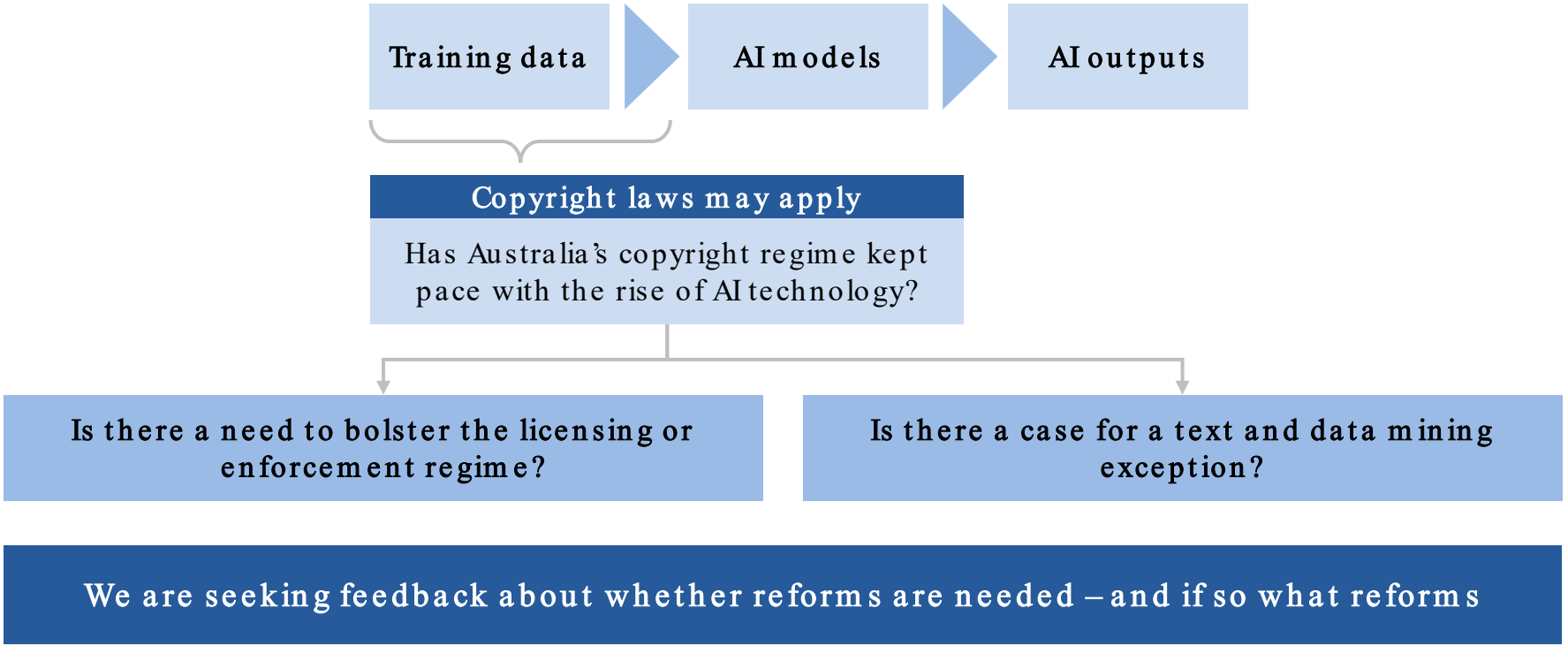
- Department of Health
- TGA
- Treasury
- Attorney General's Department

If not, then consider:

What new regulation might be needed?

Existing analyses need to be completed, and may need to be expanded

Case study: copyright law in the age of AI

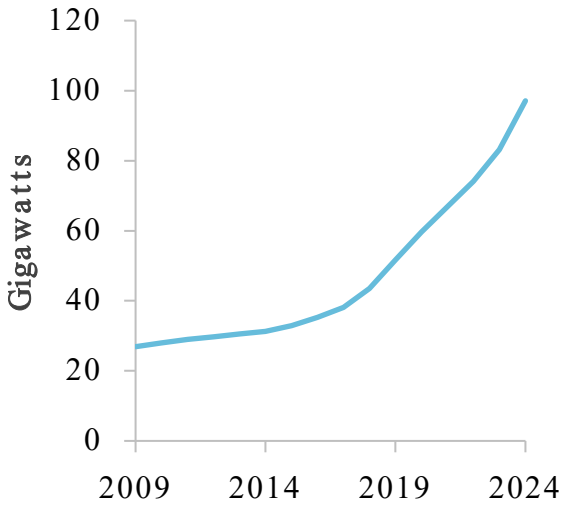


New pathways for data access

The inability of individuals and businesses to access data that relates to them is holding back productivity gains

The volume of data creation is increasing exponentially …

Global data center capacity



…but individuals & businesses can't easily put it to use

Data holders can deny access…

..and make it difficult use data

- unstructured (pdfs)
- view-only
- incompatible

PDFs

Unlocking data could help to power productivity growth

Switching between providers

Linking related products / services

More personalised services

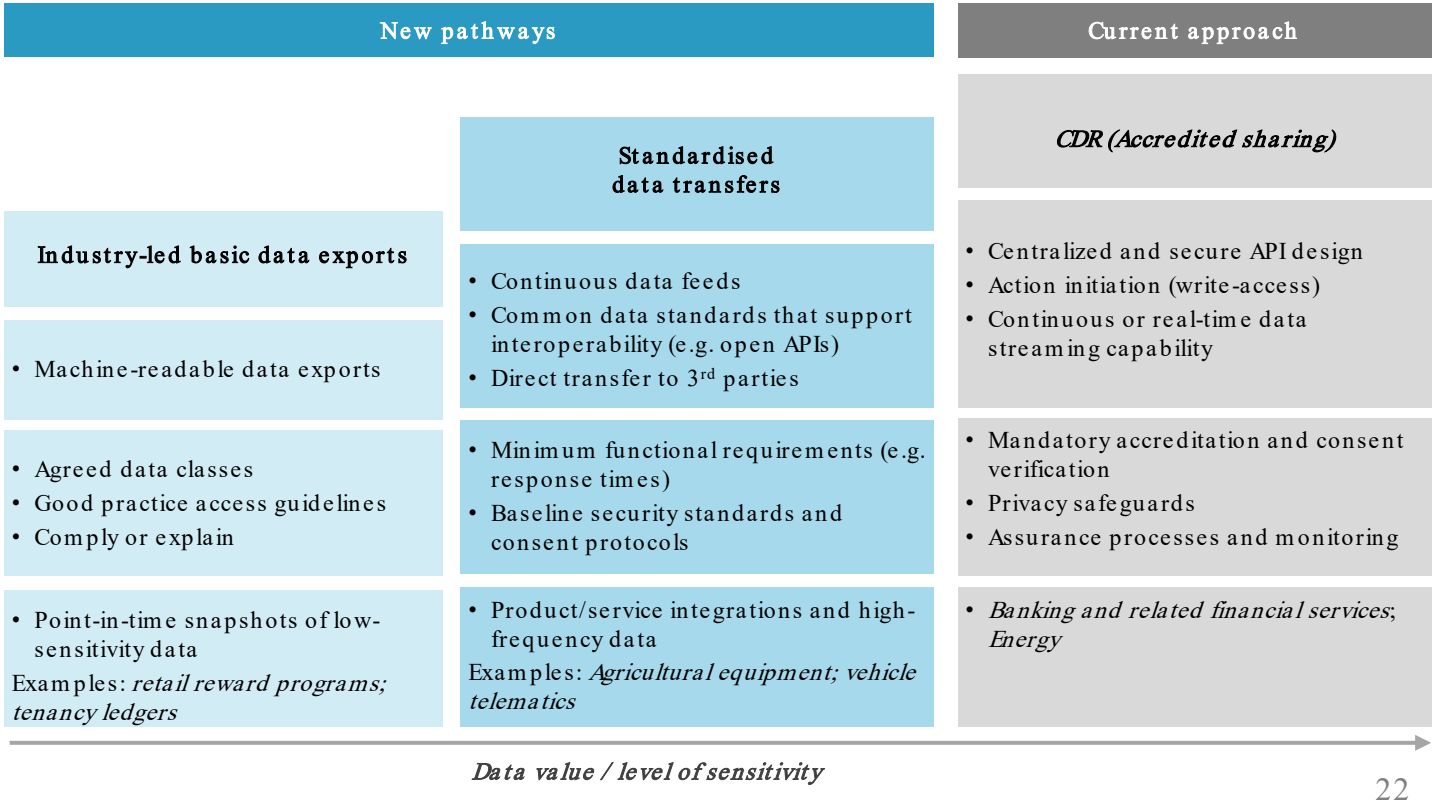
Improved data access could add up to $10 bn to GDP

Source: IEA (2025)

New pathways to expand data access

New lower-cost and flexible pathways are needed to enable individuals and businesses to readily access and use data that relates to them, while allowing the obligations on data holders and the functions that governments perform, to vary.

Efforts should begin with sectors where improved data access is of high benefit but relatively low cost; and there is clear value to consumers



Pathways in action

Rather than imposing onerous requirements on data holders or a rapid overhauling of existing technology, pathways will operate to formalise existing best practice to create more consistent and useable access to data for individuals and businesses across the economy in the longer term.

	Current state	Effect	Potential application of pathways
 **Agricultural machinery and equipment data**	Data captured by different equipment manufacturers is **often incompatible.**	Farmers can be ***'locked in'*** to particular brands, or be forced to pay for **unofficial tools** that collate data from multiple providers.	The **Australian Farm Data Code**, which was designed to support trusted data sharing and the adoption of digital technology, could be bolstered by obliging manufacturers through the **standardised data transfer pathway** to provide data in line with existing standards.
 **Residential real estate tenancy data**	Requests for a rental ledgers can **take up to seven days** to be fulfilled, and the **layout** and **information** included **varies**.	Ledgers can be difficult for **tenants to understand and reconcile**.	The **industry led pathway** could oblige property managers to provide rental ledgers on demand in an **easy to read and standardised** file format, enabling it to be easily attached to future rental applications and enable banks and fintechs to **quickly verify rent payments for loan applications**.
 **Retail loyalty rewards data in digital form**	Retail loyalty programs typically provide digital receipts in **unstructured PDF** or **'read only' formats.**	Consumers cannot readily use the data to **compare prices** or **track their spend**.	The **industry-led basic data exports** pathway could enable consumers to export transaction data from their digital receipts, allowing them to **share it with third party apps** that offer **budgeting, habit tracking, tax reporting**, and other **personalised tools.**

Privacy regulation

The Privacy Act in a changing data landscape

Stakeholder views on the functioning of Australia's privacy laws

Reform can be win-win: effective protection for individuals and lower cost for business

Some businesses find the Privacy Act to be overly burdensome

'overly complex and challenging to interpret and comply with'

'the notice-and-consent model is simply not sustainable'

Participants also said the Privacy Act does not adequately protect individuals

'the blunt instrument of consent is often used as a take it or leave it option'

'privacy self-management ... places an overwhelming burden on users'

'overly prescriptive requirements also contribute to consent fatigue'

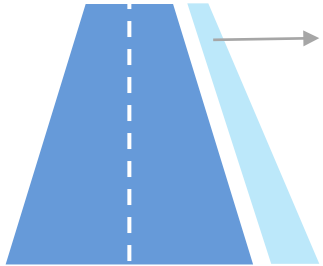
Sources: Inquiry submissions to PC, responses to PC questionnaire, submissions to Privacy Act review.

Renewing the focus on privacy outcomes

We recommend an alternative compliance pathway focused on outcomes

Dual-track

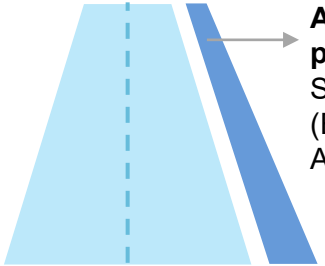
Main pathway:
Existing Privacy Act controls



Alternative pathway:
Defence
(Outcomes-based obligations)

(a) 'Defence' model

Main pathway:
Outcomes-based obligations

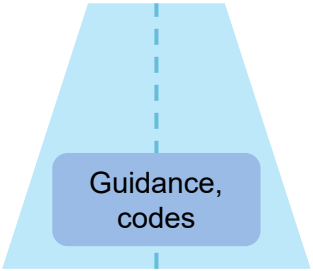


Alternative pathway:
Safe harbour
(Existing Privacy Act controls)

(b) 'Safe harbour' model

Single-track

Compliance pathway:
Outcomes-based obligations



(c) 'Single pathway' model

Digital financial reporting

Digital financial reporting allows financial information to be extracted and analysed at scale

Non-digital financial reports

- Hard copy or electronic file (PDF or HTML)
- Can be read by humans
- Difficult to extract and analyse information at scale

	2024 US$m	2023 US$m
Net book value		
At 1 January	**797**	826

Digital financial reports

- XBRL or inline XBRL (iXBRL) file
- Can be read like a non-digital report
- Financial data 'tagged' and can be downloaded and analysed at scale

	2024 US$m	2023 US$m
Net book value		
At 1 January	**797**	826

and

Tag	ifrs-full:Goodwill
Fact	797,000,000

Source: Rio Tinto, *2024 Annual Report*, p. 182.

Australia is missing out on the benefits of digital financial reporting

Companies have been able to lodge digital financial reports voluntarily since 2010, but as of June 2025, none have been submitted

	Improvements to existing activities	Enabling of new activities
Report preparers	Improved information processing	Visibility of report preparers in global capital markets
Report users (such as investors and analysts)	Less time-consuming and more accurate data extraction and analysis	'Big data' analysis
Auditors	Earlier detection of anomalies and emerging financial issues	Novel data-driven audit methodologies
Regulators and other government agencies	More effective risk targeting (such as in audit inspections)	New enforcement and analysis techniques

What we heard from inquiry participants

Participants identified a range of benefits of digital financial reporting …

"[Digital financial reporting] improves market transparency and strengthens investor oversight"

"[Digital financial reporting could] improve transparency, reduce compliance costs, and attract capital"

…identified barriers to uptake …

"There is little incentive or value in an individual company voluntarily producing a digital report where others do not"

"High implementation costs, …challenges around software availability, and a shortage of qualified personnel"

…and suggested different ways to promote uptake

"Mandate digital financial reporting"
"Make digital reporting the default"
"Mandatory …digital financial reporting"

"Consider the evolving role of AI in financial reporting"

Financial reporting should be digital by default

A mandate should cover disclosing entities as defined in the *Corporations Act 2001* (Cth), which includes publicly listed companies and certain other public interest entities

Greater uptake is unlikely to occur under the existing voluntary scheme

Globally, digital financial reporting has only been widely adopted when it is mandated

The cost of digital financial reporting falls as preparers gain experience

A mandate will give report preparers and users the certainty they need to invest in digital financial reporting infrastructure and processes

AI and other digital technologies are a complement, not a substitute

These tools need the structure of digital financial reporting data to work effectively

The final report will consider how mandatory digital financial reporting could best be implemented

Specifying the mandate's scope
Which **entities** should be required to submit digital reports? Which **reports** should be submitted digitally?
Setting requirements for report preparation
Is Australia's existing digital reporting **taxonomy** fit-for-purpose? What **format** should reports be prepared in?
Establishing the infrastructure and procedures for report submission
Where and how should reports be submitted?
Supporting the provision of high-quality, accessible digital financial data
What measures should be implemented to ensure that digital financial reports contain **high-quality data**? What measures are needed to ensure that digital financial reports are **accessible** to users?

pc.gov.au

5pillars@pc.gov.au

Adelaide University

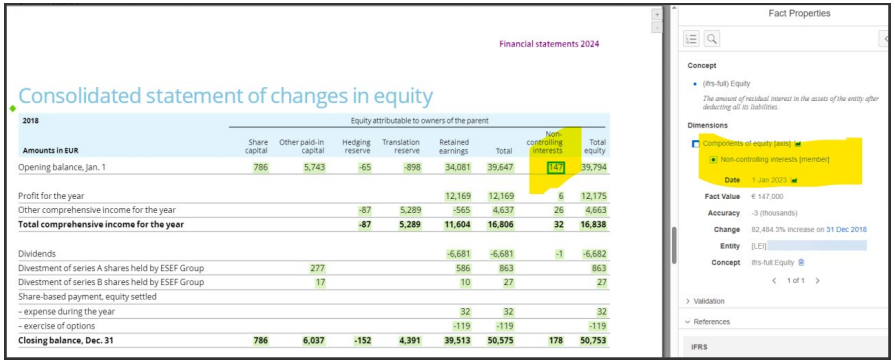
Digital corporate reporting practice

Challenges, implications and lessons for policy development

Professor Indrit Troshani, Adelaide University

What is digital corporate reporting?

- Process where accounting data are structured in ways that enable ***machine readability***
- Facilitates ***automated*** reporting, extraction and analysis
- Digital reports are created via ***tagging*** process, attaching meaning to disclosures



Source: https://www.lucanet.com/en/insights/software-use-cases/understanding-different-types-of-xbrl-reports-11-07-2024/

- Infrastructure
  - Tagging software to ***mark-up*** corporate report information
  - Tags specified and classified in ***taxonomies***-based on accounting standards and regulation
- Underlying data standard is XBRL/iXBRL
- ***What are the current digital reporting practices, challenges and implications?***

Adelaide University

Data sources

- Interviews (November 2023 – October 2025, but ongoing…)

Category	Interviewee identifier	No of interviews (incl. 3 follow ups)	No of organisations
Advisors (tagging agencies, vendors, auditors)	A1-16	15	11
Multinational preparers	MP1-12	9	8
Professional bodies	PB1-2	2	2
Users (e.g., regulators, data providers)	U1-7	8	7
Total	37	34	28

- Documentary evidence (e.g., standard-setters, regulators, software vendors)

Adelaide University

Digital corporate reporting

Adelaide University

Perceptions of regulation

- Regulation is ***key driver*** of digital corporate reporting uptake

- But dominating ***perceptions*** are that
  - regulators are ***only*** interested that digital reports be ***filed by deadline***, and they are ***not interested in digital report content***
  - digital data are ***not used*** by regulators and investors
- So, digital reporting perceived as compliance issue, rather than as value-adding activity

- Implications
  - Addressing 'no use' perceptions critical

Preparation cost

- Investment in ***DCR capacity***
  - infrastructure and expertise (e.g. software, skilled staff)
  - ongoing DCR time (for tagging, quality reviews, sign-off)
  - audit fee (where DCR assurance required)
- Year 1 tagging costly, but
  - costs ***decline from year 2*** (e.g., roll-forward effect, learning)

Modes of preparation

Engaged

- In-house expertise
- DCR quality

- Less expensive, but limited DCR capacity

Bolt-on preparation

- Short-term DCR capacity investment,
- But long term reporting efficiency gains

Built-in/integrated preparation

- High level DCR reviews, sign-off
- Quality risks

Detached

Adelaide University

Tagging practices

- Tagging ***can be challenging*** (!) and requires,
  - specialised knowledge (e.g., taxonomy, tagging software), and
  - judgement – interpreting if and how taxonomy tags reflect accounting meaning of disclosures
- ***Good news*** (!) – tagging software capability to assist with tagging (e.g., ML support)

Adelaide University

Tagging practices

- 'Tell own story' versus 'being comparable':
  - To use custom tags or not?
  - Open *versus* closed taxonomy systems

  - Closed taxonomy system may "help" (?) with comparability outcomes,
  - but ***are comparisons meaningful*** when there's risk tagging can become an exercise of "fitting a square peg in a round hole"?

- Open taxonomy systems, allow custom tag use, but
  - regulators "***discourage***" excessive use; question use if suitable tags exist in taxonomy
  - tagging agencies and auditors "***demonise***" custom tags: perceived to complicate tagging and digital reports

Adelaide University

Tagging practices

- IFRS Foundation 'Common Practices' project and illustrative examples
- Industry, tagging agencies, and regulator-led initiatives (e.g., France/Italy, Japan, Taiwan)
- Taxonomy ***revisions*** by standard-setters
- EU's ESMA require custom tags be '***anchored***' (i.e., linked) to core ESEF taxonomy tags

The ESEF Taxonomy however does not have a concept for "Flight equipment". The closest wider ESEF taxonomy concept for "Flight equipment" is "Property, plant and equipment" since the even wider element "Non-current asset" has a much wider accounting meaning than "Property Plant and Equipment", and the documentation for "Other property, plant and equipment" explicitly excludes "separately disclosed items" from this element.

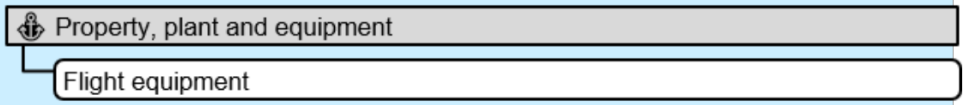


Figure 1: PPE and Flight Equipment

Therefore, the extension concept for "Flight equipment" should be anchored to the closest wider accounting meaning concept identified above. The extension concept is the 'target' of this relationship as is indicated in the diagram above by the indented item.

Source: https://www.xbrl.org/guidance/esef-rules-anchoring-extensions/

- Overall, ***greater taxonomy conformance trends lead to greater comparability***, but is this ***compromising preparer flexibility to 'tell own story'***?

Adelaide University

Digital data quality

- Digital data quality is multi-dimensional
- Technical validity
  - Does digital report comply with XBRL technology rules?
- Regulatory validity:
  - Does digital report comply with regulatory rules?
- Accounting validity:
  - Do applied tags reflect accounting meaning of disclosures, consistent with accounting standards/taxonomy and corresponding disclosure in human-readable report?

- Implications of validity rule violation *severity* classification (‘errors’ vs ‘warnings’)

Quality control and assurance

- Quality *is* ***preparer's responsibility***, regardless of preparation approaches (!)

- Assurance – required in EU but not in other jurisdictions such as US and UK
  - Requirement (or lack thereof) and compliance failure repercussions ***shape*** preparers' quality commitment

- Preparers conduct internal reviews, but engagement varies
  - Validation ***challenges***
  - Tag choices (e.g., custom tag use: avoid them or agree across industry)

Quality control and assurance

- Auditors assure digital report
  - Automate validation but accounting quality checks require judgement
  - Need for DCR internal control and audit procedure revisions?
  - Need to reconsider materiality assessment?

- ***Significant data quality variation***
  - assurance practices across jurisdictions ***prioritise*** different quality dimensions

- ***Lack*** of international DCR ***audit standards***, and different national regulator ***stances to quality*** (e.g., in EU) are problematic

- Implications of ***tight filing deadlines***

Adelaide University

Digital data usage

- ***Uncertainty*** if and how digital data is used
- Quality issues undermine confidence in digital data and exacerbate lack of use perceptions
- Evidence of data providers sourcing digital data from regulators to populate their databases, ***after curating for quality***
- ***Mixed*** evidence if custom tag disclosures are used by data providers
- Evidence regulators use digital data, including adopting AI models for monitoring
- (Non)institutional investors use?
  - free tools provided by some regulators and XBRL consortia,
  - but limited functionality constrains non-institutional users from taking advantage of digital data benefits (e.g., large scale extraction), and
  - free tools are not always easy to use for non-professional, less sophisticated users

XBRL rules!

Thank you!

Australian Government

Australian Accounting Standards Board

Accounting for Investments in Artificial Intelligence: Evidence from current trends

Nafiz Fahad[a], Mehnaz Laura[a], Tom Scott[b]

[a]Massey University
[b]University of Auckland

Problem

- 84% of Australians in office jobs report using AI at work
- Significant investments by non-AI companies (estimated at 5-20% of IT budgets)
- If AI is a game-changer, then disclosure of investments in it is relevant!
- Some regulators are concerned about *AI-washing*
- Should expenditures be an expense or an intangible asset?
- Software is the comparable asset

Example

Wesfarmers CTO explains how AI is transforming customer and team experiences

by Emily Bencic

At Bunnings, for instance, our team has focused on 34 promising use cases from an initial list of more than 130 possibilities. One of the most developed of these is a new AI-powered information service for our in-store team called 'Ask Lionel', which has already been developed and trialed with the aim of providing fast access to data, insights and announcements to help our team **better respond to customer** queries.

Bunnings, Kmart and WesCEF have also enjoyed being early adopters of Microsoft 365 Copilot, driving **significant productivity** gains across many business functions.

Example

Digital Nation (/digital-nation)

Bunnings pilots AI for its 55,000-strong workforce

Central to building this understanding is Workday Skills Cloud, which runs on the **vendor's AI technology**, which it calls 'Illuminate'.

Our skills journey is still in its **infancy**," Rodway said.

We've run a couple of **pilots** that have been successful. We're really understanding how Skills Cloud works.

Combined, the technology is **expected** to "significantly reduce time-to-hire and associated costs" with constantly looking externally for staff, Rodway said.
Rodway also flagged future implementations of two analytics tools - People Analytics and Prism Analytics - to help business and HR staff respectively understand the workforce.

Intangible assets

- An identifiable, non-monetary asset without physical substance:
  - controlled by an entity as a result of past events.
  - expected to generate future economic benefits for the entity.
- An intangible asset shall be recognised if:
  - it is probable that the expected future economic benefits that are attributable to the asset will flow to the entity; and
  - the cost of the asset can be measured reliably
- An asset is identifiable if:
  - is separable, i.e. is capable of being separated
  - arises from contractual or other legal right

Issues for Software

- Can the costs be measured reliably?
- Future benefits (project feasibility – R&D accounting)
- Hardware component is PPE (separation of software vs hardware)
- Technical obsolescence (useful life, especially for websites)
- Software-as-a-Service (control issues?)
- Maintenance vs. Enhancements (cybersecurity updates?)
- Cannot be revalued upwards – may not reflect the true value
- Training/Staff costs

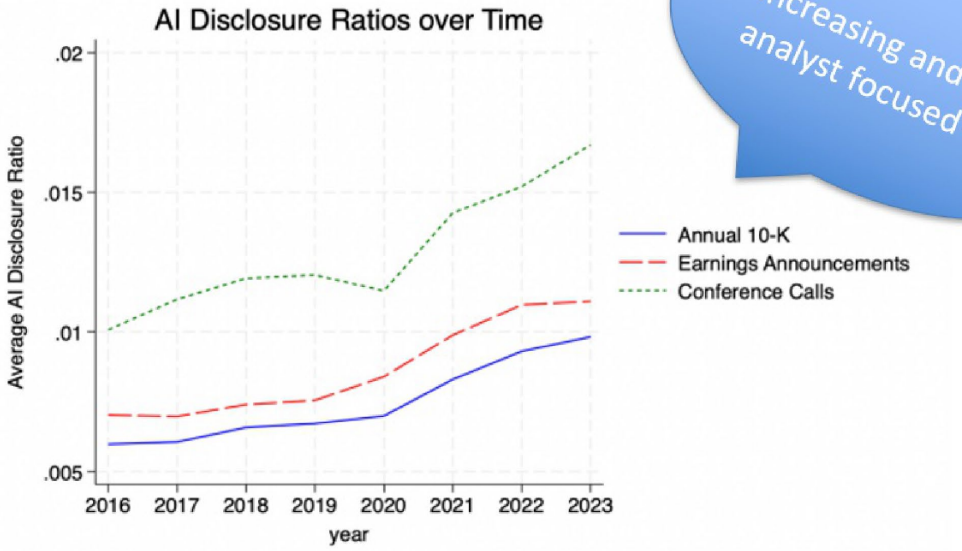
Even worse for AI!

- Future benefits are even more uncertain
- Hosted on cloud
  - PPE for storage/processing?
  - SaaS (control/vendor rights)
- Buy a foundation model but train it further
  - Capitalise AI training costs but not training staff (robots can't leave you!)
  - Who owns data/data acquisition costs
- Even more uncertainty about whether projects are feasible?
- A very limited lifespan?
- As AI is reiterative, learning vs enhancements is more blurred

Is accounting investments in AI a growth area for consultants?

- **Yes, accounting for investments in AI is a growing area for consultants**, and here's why:
  - **1. Rapid AI Adoption**
    - Companies across industries are investing heavily in AI technologies – both for internal operations (like process automation) and customer-facing products (like AI-driven apps).
    - These investments raise accounting questions, because AI spending can be *software, R&D, or intangible assets*, and companies need guidance on proper recognition, amortisation, and disclosure.
  - **2. Complex Accounting Standards**
    - Current accounting standards (like IAS 38 for intangibles or ASC 350/730 under US GAAP) were *not specifically written for AI*.
    - Determining whether AI spending should be capitalised, expensed, or disclosed requires *specialist knowledge*.
    - Many firms *lack in-house expertise*, creating demand for consultants.

Disclosure over time



Prior Research

- 2/3 of large Australian companies capitalize software development costs – about the global median (Dionysiou et al., 2021)
  - But when they do, it is the largest as a proportion of assets!
- Capitalising software typically improves the usefulness of accounting information
  - Leads to lower information asymmetry (Mohd, 2005), and reduces IPO underpricing (Givoly and Shi, 2008)
- AI-related disclosures in 10-Ks are associated with firm value, growth, investment, and operational efficiency – especially when not AI-wash (Basnet et al., Cao et al., Barrios et al., 2025)
  - Provides information about actual AI spending (e.g., AI job advertisements)

RQ: How do firms disclose investments in artificial intelligence and what is disclosed?

Setting and Sample

- Annual reports of ASX200 over 2023 to 2024
- Excluding financials, REITs, and funds $\Rightarrow$ 280 observations for both years
- No "AI" companies
- **Step 1: Recognition**
  - Manually check balance sheet (B/S), income statement (I/S), and notes for any AI-related words
  - Nothing found
  - AASB 101 97 When items of income or expense are material, an entity shall disclose their nature and amount separately.
    - *So AI is non-material (aggregated with IT?)*

If aggregated.....

Category	N	%	Mean Value (000s)
Intangible Assets	234	83.5%	740,748
ICT related Expense	54	19%	102,332
Software Asset	166	59%	197,261
Technology & non-compete agreements	10	4%	29,964
Domain names / Website and database / Distribution network	6	2%	110,859

Large variation in categorisation – good luck users!

Big range in life and given range (2–3 years to 1–20 years)

AI disclosures

- **Step 2: If not recognised, are they disclosed in the Annual Report**
  - Textual analysis of key AI-related words and extract a paragraph
  - 40% of firms have any mention of an AI-related word (2.7 words mean)
  - For those who do, 1/3 involve a commitment or are specific

AI disclosures

Green = Firm-specific keywords
Blue = Commitment/action keywords

Example 1. AI disclosure as commitment (Label as Yes)

Another key focus area for the Next Generation Mine Mission is utilising **artificial intelligence** (AI) to unlock value. We recognise the potential that AI offers and have established a targeted approach that allows us to scale and unlock value in four areas that support our strategy and create shareholder value: safety, cash generation, exploration, and productivity enablers. We have already unlocked value through AI initiatives at Australia Manganese, Worsley Alumina and Cerro Matoso, with plans to scale to other operations. Our work in AI follows responsible AI frameworks and is underpinned by risk management, governance, cyber and privacy controls. (See page 22)

We continue to see cyberattacks targeting operational technology systems, including those used by mining companies. There has been an increase in hackers targeting personally identifiable information held by third party suppliers and vendors with immature cyber controls. The adoption of **artificial intelligence** (AI), including new developments in generative AI, has 'step-changed' from previous years and is increasing rapidly across various industries. These rapid developments present both opportunities and risks to our business. We are not willing to take risks that will result in a loss of data or disruptions to our operations and projects due to the theft, disclosure or corruption of information. Aligned to our strategy, we will pursue technology and innovation that may have a lower certainty of success where there is commensurate potential for high return on investment. To stay competitive, we position our organisation to effectively identify, develop and adopt sustainable business models, technologies, aligned, value-focused, innovation portfolio. This approach will assist us to deliver on shareholder return expectations and position us for future business opportunities. (See page 32)

(Source: Annual report 2024, SOUTH32 Ltd)

AI disclosures

Example 2. AI disclosure as specific/commitment (Label as No)

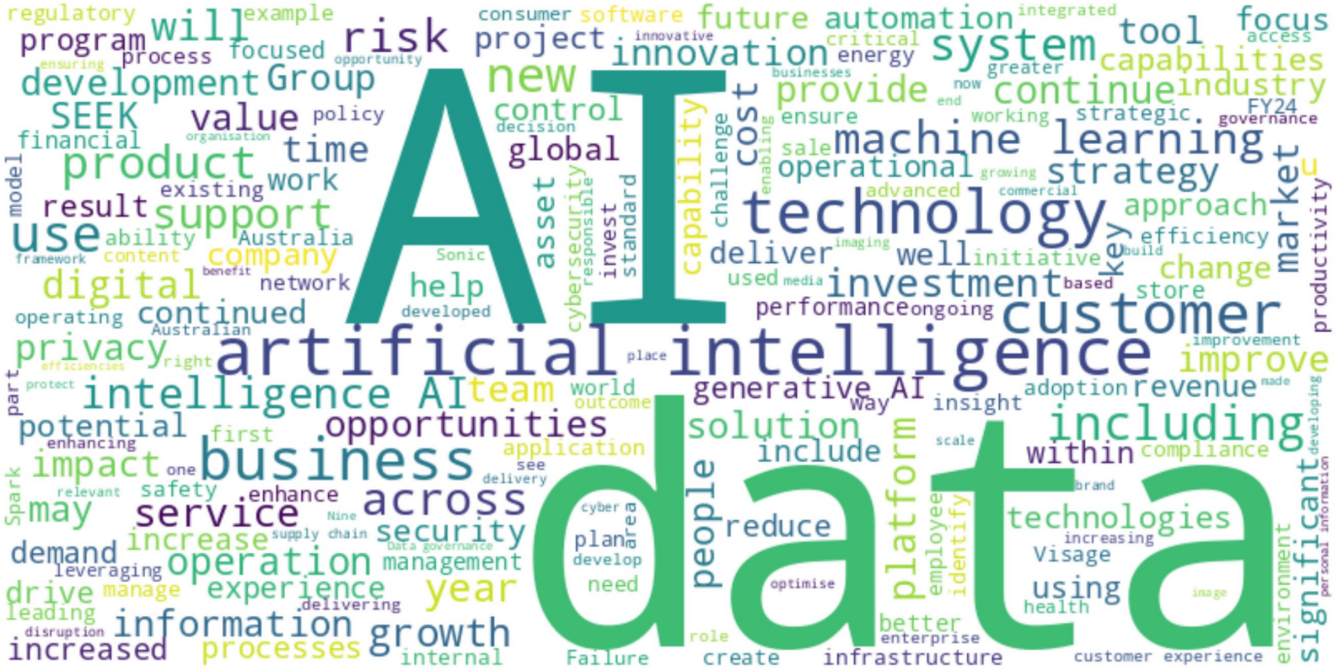
All industry sectors ended the year in positive territory. after experiencing falls over the prior period, technology stocks were the standout performers the sector surged more than +30% as interest in the future applications of **artificial intelligence** rapidly gathered momentum. The utilities and health care sectors were the share markets laggards, gaining just +2.3% and +5.7% respectively as investors overlooked stocks with more defensive attributes. (See page 3)

In Australia, all industry sectors delivered positive returns for the year. technology was the best performing sector with +32%, regaining lost ground from last year and boosted by investor optimism around potential productivity gains due to the use of **artificial intelligence**. The materials sector returned +22%, with particular pockets of strength in lithium and gold stocks, and energy rose +20%. health care and utilities were the laggard sectors, although still marginally positive. (See page 16)

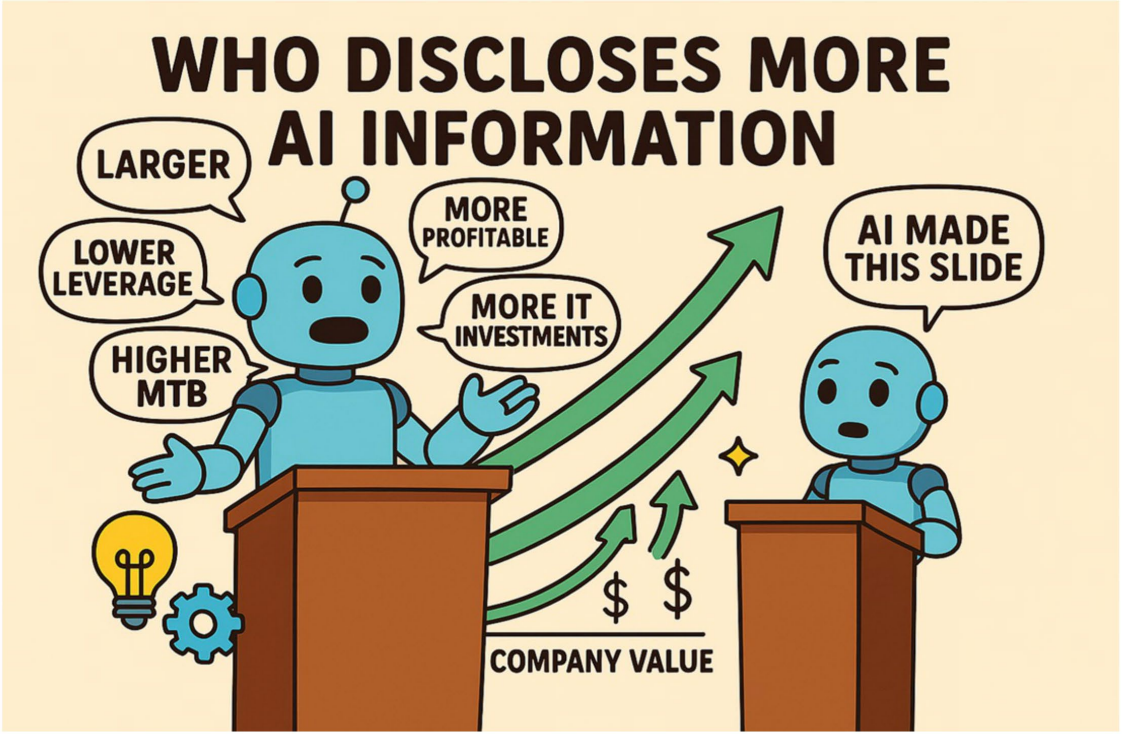
(Source: Annual report 2023, Argo Investments Ltd)

Word Cloud

Word Cloud for AI Related Extracted Paragraph

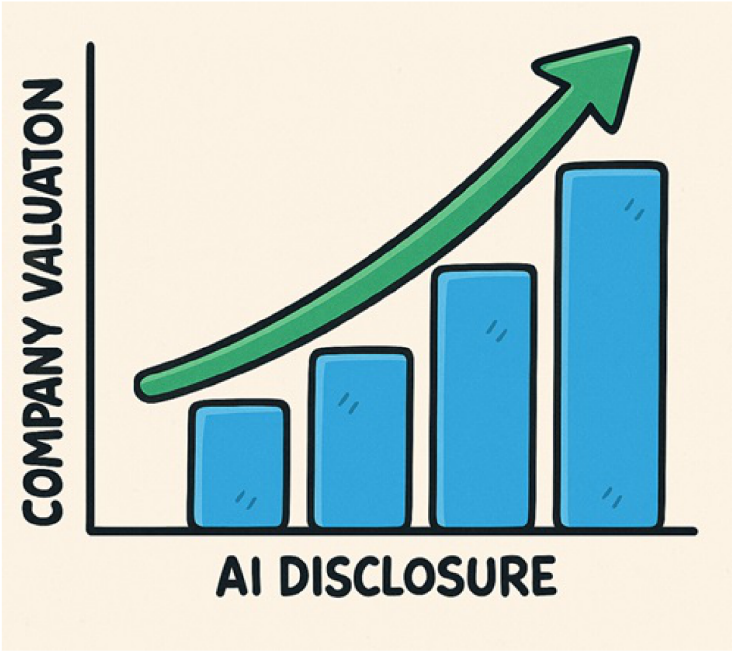


Determinants



Does it matter?

- *Price = NI + BVE + Loss + Year + Industry*
- The market values earnings and assets higher if there is more AI disclosure
- Stronger if committed or specific disclosure, which increases value by themselves
  - Does the market see through AI-washing?



Conclusion

- Outline the problems and current state of AI accounting (currently very limited!)
- Contribute to the literature on AI-related disclosures by examining non-AI firms in Australia.
- Regulator concerns about AI-wash overstated?
- Standard-setters might consider targeted AI guidance on lifecycle/maintenance/ training issues

Regression Results

VARIABLES	OLS (LN_AI)	Logit (AI_DUMMY)	Tobit (AI_DUMMY)	OLS (LN_AI)	Logit (AI_DUMMY)	Tobit (AI_DUMMY)
ITINVEST	5.988	25.260***	7.142***	3.750	13.722*	3.000*
	(-1.223)	(-4.236)	(-4.529)	(-0.636)	(-1.902)	(-1.945)
SIZE	1.606***	0.666***	0.288***	1.830***	0.816***	0.328***
	(-10.311)	(-4.891)	(-5.062)	(-5.271)	(-3.685)	(-4.531)
LEVERAGE	-2.579**	-2.543***	-1.016**	-1.844*	-3.029***	-1.188***
	(-2.284)	(-2.779)	(-2.464)	(-1.683)	(-2.671)	(-2.649)
ROA	6.522**	3.729*	1.976*	6.060*	-1.575	-0.866
	(-2.297)	(-1.737)	(-1.669)	(-1.823)	(-0.547)	(-0.742)
LOSS	0.772	0.326	0.205	0.832	-0.016	0.010
	(-1.271)	(-0.677)	(-0.934)	(-1.454)	(-0.025)	(-0.041)
MTB	0.439***	0.073***	0.031***	0.400***	0.066*	0.027**
	(-15.664)	(-3.151)	(-3.285)	(-5.531)	(-1.770)	(-1.989)
ANALYST	0.380	0.151	0.122	0.199	0.448	0.203
	(-1.092)	(-0.504)	(-0.897)	(-0.363)	(-1.207)	(-1.220)
BIG4	0.062	1.174	0.676*	0.282	1.396*	0.709**
	(-0.081)	(-1.389)	(-1.762)	(-0.298)	(-1.860)	(-2.052)
Constant	-21.164***	-16.334***	-7.278***	-26.437***	-18.546***	-7.510***
	(-6.826)	(-5.535)	(-5.784)	(-3.861)	(-4.032)	(-5.191)
Observations	280	280	280	280	280	280
R-squared / Pseudo R^2	0.631	0.193	0.202	0.689	0.271	0.281
Year FE	NO	NO	NO	YES	YES	YES
Industry FE	NO	NO	NO	YES	YES	YES
Clustered	NO	NO	NO	Firm	Firm	Firm

Regression Results – Price Models

VARIABLES	Price	Price	Price	Price
Constant	9.625***	7.107***	4.039***	4.589***
NI	3.182**	0.347	0.857	-0.526
BVE	1.086**	-0.111***	0.240*	0.298
LOSS	-3.013**	-0.494	-1.013	-0.586
AI_DUMMY		0.562		
AI_DUMMY*NI		1.546***		
AI_DUMMY*BVE		1.519*		
SPECIFIC			7.452***	
SPECIFIC*NI			1.505***	
SPECIFIC*BVE			0.965***	
COMMIT				4.965***
COMMIT*NI				2.942**
COMMIT*BVE				0.985**
Observations	280	280	280	280
R-squared	0.706	0.712	0.795	0.903
Year FE	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES
Clustered	Firm	Firm	Firm	Firm

Thank you

Cyber Risk Disclosures in Australia: An Exploration of Current and Best Practice

Dean Hanlon

(RMIT University)

AASB Research Forum | 17 November 2025

Acknowledgement of research funding:

Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

Motivation and Background

Cybersecurity is a rising priority for firms and investors

- Cybersecurity is a critical element of firm governance and risk management (AICD, 2024; ASIC, 2025; Center for Audit Quality, 2016).
- Data breaches becoming increasingly common:
  - OAIC recorded 1,113 data breaches across 2024, a 25% increase from 893 in 2023;
  - Cybercrime expected to cost approx. USD13.82 trillion globally by 2028 (World Economic Forum, 2024)

Evolving cybersecurity reporting requirements locally and globally

- US SEC (2023): Disclosure in annual filings relating to:
  - Material cyber incidents; and
  - Cyber risk management, strategy and governance processes
- ASX (2024): Updated *Guidance Note 8: Continuous Disclosure* with new example and commentary on continuous disclosure obligations relating to cyber incidents or data breaches

Limited Australia-specific evidence on cybersecurity disclosures

- No prior study has examined in depth cybersecurity disclosure practices in Australia
- Mostly U.S., U.K. and Canadian studies (Gao et al., 2020; Berkman et al., 2018; Heroux & Fortin, 2020) with distinct institutional and reporting requirements

Research Questions and Objective

What is the current state of cybersecurity disclosures by ASX Top 500 companies?

What cybersecurity disclosures would be decision-useful for users?

Assess prevalence, location, nature, and quality of cybersecurity disclosures via content analysis of annual reports

Conduct semi-structured interviews with investors and cybersecurity specialists to assess how cybersecurity information needs are best met

Develop key recommendations on cybersecurity disclosures to bridge any gap between current and best practice disclosures

Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

Research Method:

Content Analysis (RQ1)

- **Content analysis** of cybersecurity disclosures based on a glossary of cyber-related terms drawn from prior studies:
  - Extract cyber-related text using the Python program
- **Sample**: Australia's top listed companies (ASX 500) as at 30 June 2022 and 30 June 2023:
  - Based on size (market cap)
  - Reports analysed: FY 2022 and FY2023 annual reports
  - Industry distribution based on GICS

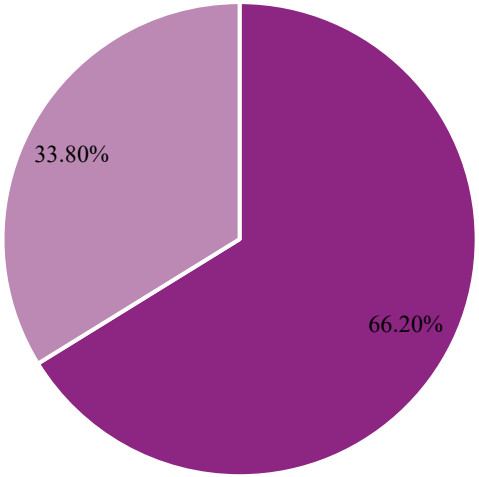
Sector	2022	2023
Communication services	14 (2.8%)	12 (2.4%)
Consumer discretionary	65 (13%)	61 (12.2%)
Consumer staples	21 (4.2%)	18 (3.6%)
Energy	23 (4.6%)	27 (5.4%)
Financials	98 (19.6%)	100 (20%)
Health care	42 (8.4%)	41 (8.2%)
Industrials	51 (10.2%)	53 (10.6%)
Information technology	38 (7.6%)	36 (7.2%)
Materials	132 (26.4%)	135 (27%)
Real estate	13 (2.6%)	13 (2.6%)
Utilities	3 (0.6%)	4 (0.8%)

Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

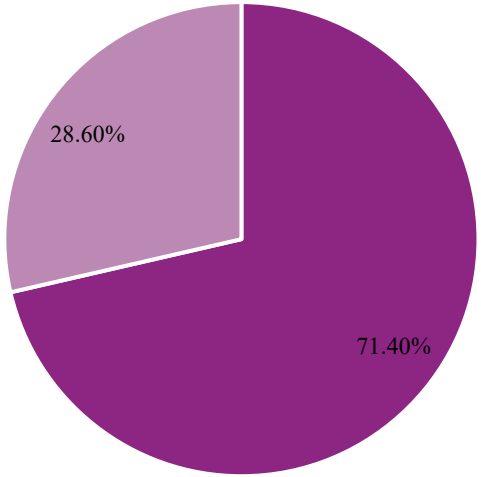
Findings: Prevalence of Cybersecurity Disclosures

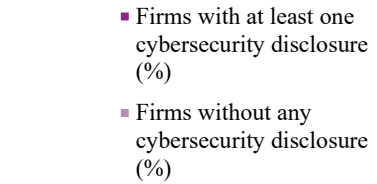
2022 Firm-level disclosures



- Further variation of those with/without cybersecurity disclosures within Top 500:
  - Top 100: 3%
  - Top 101 – 300: 28%
  - Top 301-500: 54%

2023 Firm-level disclosures





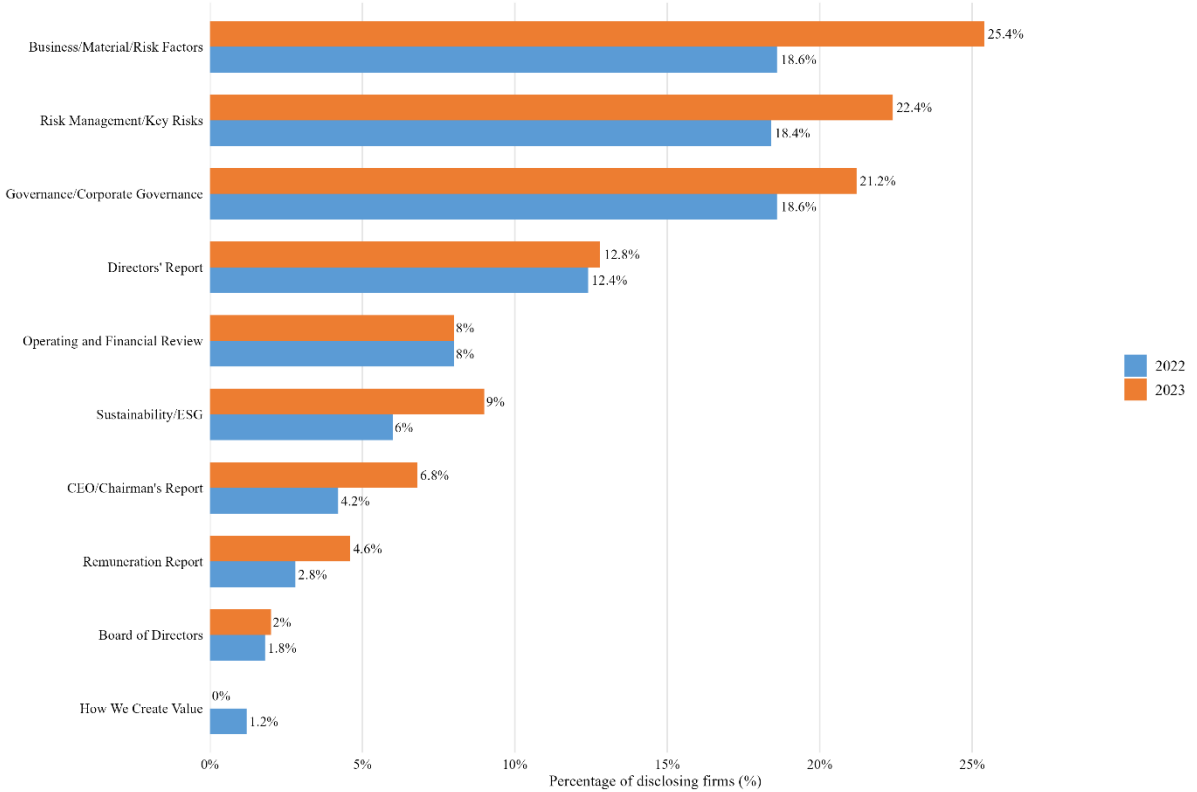
- Further variation of those with/without cybersecurity disclosures within Top 500:
  - Top 100: 4%
  - Top 101 – 300: 22%
  - Top 301-500: 46%

Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

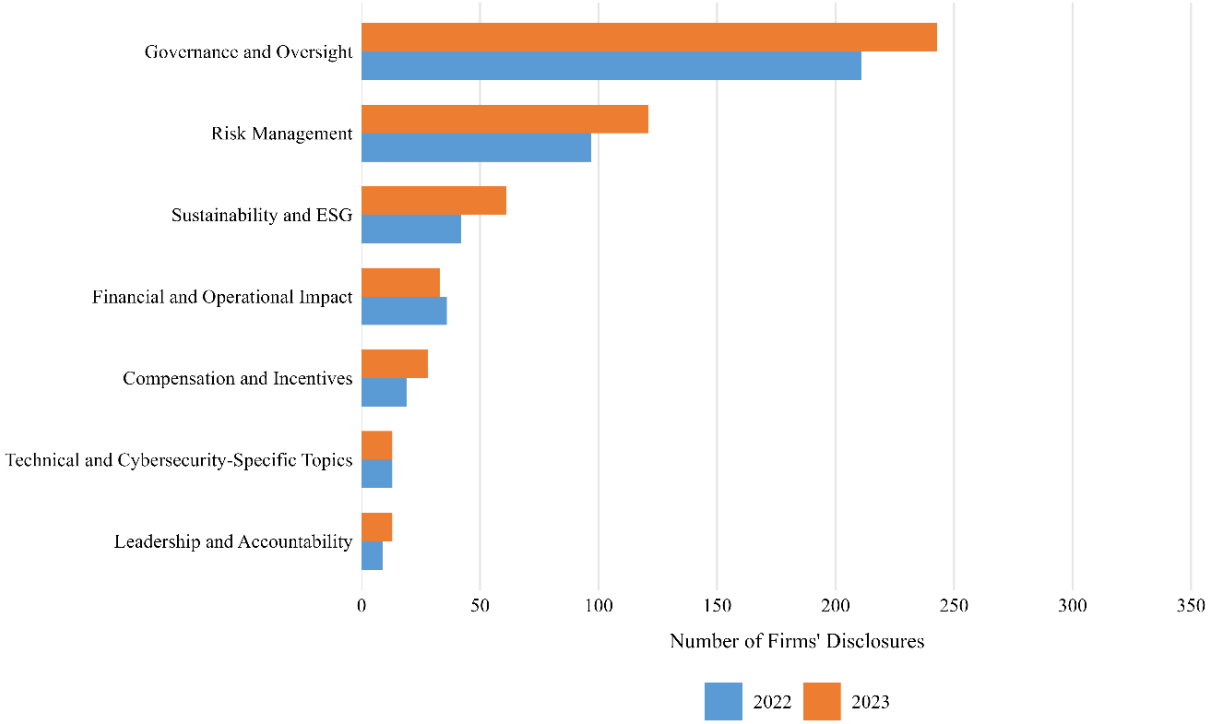
Findings: Placement of Cybersecurity Disclosures in Annual Reports

- Variation in the location of cyber disclosures in the annual report:
  - Less than half identify cybersecurity as a material business risk
  - Companies acknowledge cybersecurity as a (corporate) governance issue
  - Narratives also provided within directors' reports and OFRs
  - Cybersecurity also viewed as a sustainability/ESG issue



Findings: Cybersecurity Disclosure Themes

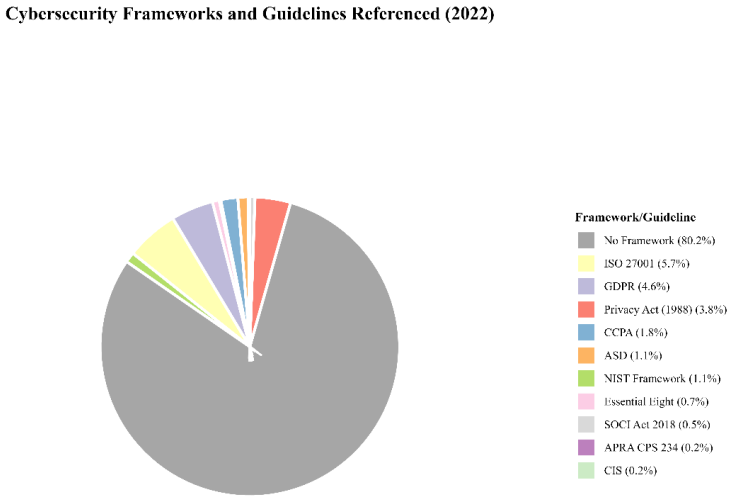
- Based on frameworks proposed in Cheong et al. (2021) and Gao et al. (2020), we group cybersecurity disclosures into eight themes. Top 3 are:
  - **Governance and oversight**: the organisational structures, policies, frameworks, and oversight mechanisms established to govern cybersecurity matters
  - **Risk management**: focus on the identification, assessment, and communication of cyber-related risks and threats facing the company
  - **Sustainability and ESG:** position cybersecurity within the broader context of the company's sustainability strategy, ESG commitments, or corporate responsibility initiatives.

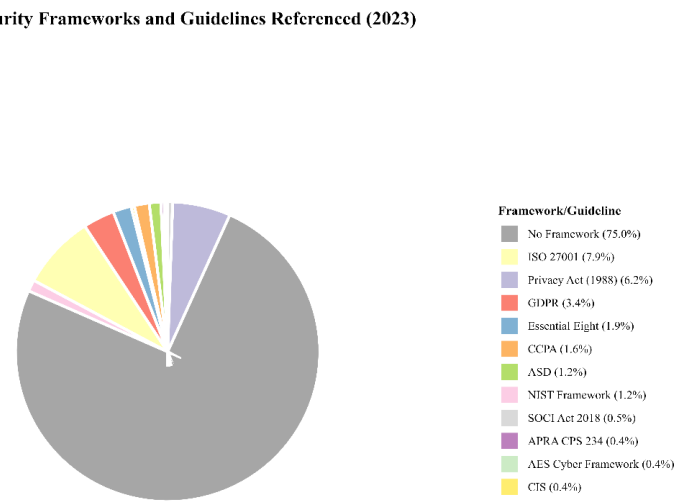


Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

Findings: Use of Cybersecurity-related Frameworks or Guidelines



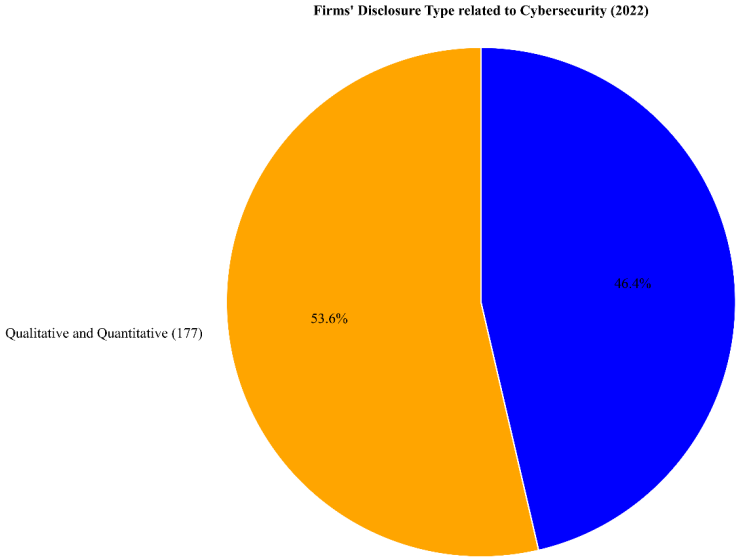


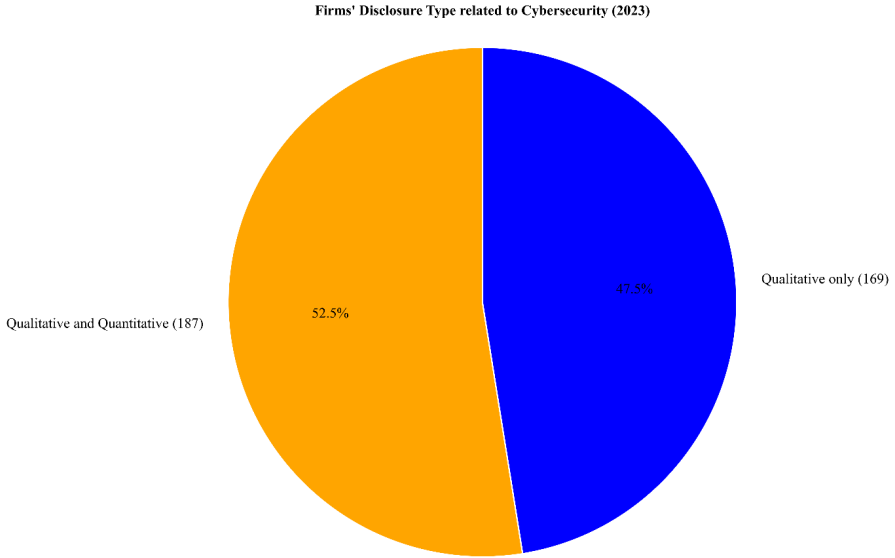
- Thirteen cyber-related frameworks, regulations, standards or guidance identified:
  - Approx. 80% of sample companies applied none of these
  - ISO 27001 was most applied (2022: 5.7% - 2023: 7.9%)
  - EU General Data Protection Regulation (GDPR) and Privacy Act (1988) next most referenced

Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

Findings: Qual. vs Quant. Information in Cybersecurity Disclosures

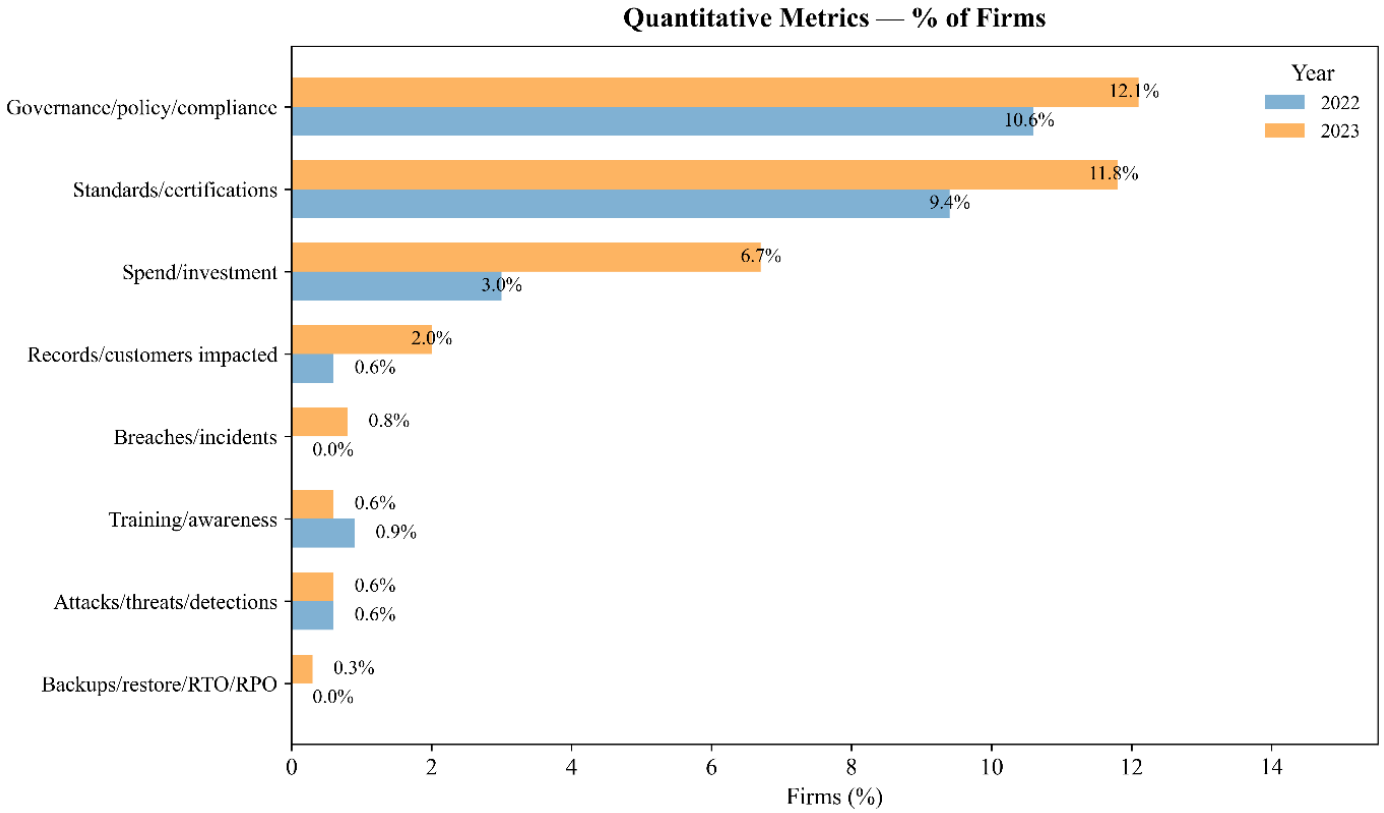




- Split disclosing companies into those providing qualitative statements only (text) and those providing both qualitative and quantitative metrics (text and numeric) relating to cybersecurity
  - Slightly more than half (2022: 53.6.% - 2023: 52.5%) integrate their cybersecurity narrative with supporting metrics

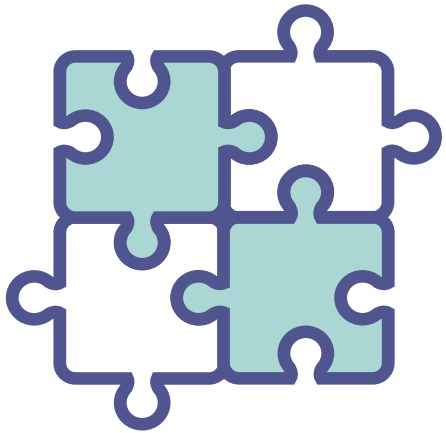
Findings: Types of Quantitative Metrics Used

- We collate quantitative metrics according to what they're trying to demonstrate. Top 4 are:
  - **Governance**: measurable references to regulatory frameworks and compliance milestones such as audit completion rates or policy adoption ratios
  - **Certifications**: number of certifications obtained or renewed
  - **Dollar spend:** cybersecurity resource allocation through reported monetary values of investments, budgets, or cost recoveries
  - **Impact numbers:** affected data subjects or accounts or counts of reported events or attacks blocked.



Summary of Key Findings: Content Analysis

A large minority do not provide cybersecurity disclosures, with further variation according to size and industry

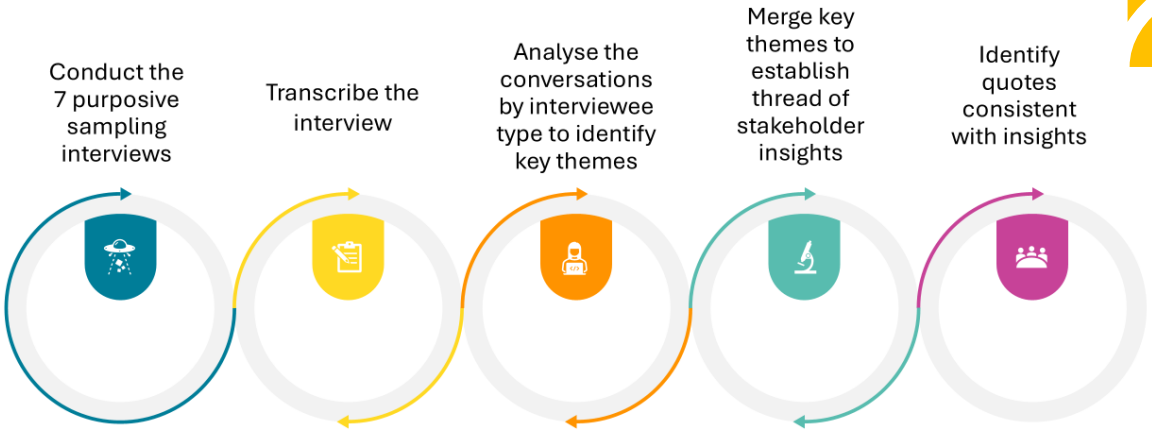


No or inconsistent use of cybersecurity frameworks, hindering maturity level assessments

Disclosures are scattered across the annual report, with less than majority of companies viewing cyber as a material business risk

A small majority use metrics to support their narrative, but vary according to type of metric and often lack methodological transparency

Research Method: Interviews (RQ2)



Interviews

3 Investors

4 Cybersecurity specialists

Is cybersecurity information relevant for investment purposes?

Enables assessment of:

Quality of management and governance processes

"been principally around stewardship. We want to make sure the board is on top of the issue and is holding management to account"

Organisational risk

"the common mantra is that whatever your organisation is, you will have a breach at some point, it's just a matter of when"

Reputation and financial impact

"cybersecurity breaches …start to contribute to a reflection of the reputation of those organisations and does factor into an assessment of the quality of management"

What cybersecurity risks are investors most concerned about?

Hostile actors

Investors have deep concerns over the "*extent of state and non-state actors*" and their "*relentless push for wanting to access data*"

Protection of sensitive data

The protection of private and personal data is a critical concern due to legal and ethical obligations

Infrastructure and supply chain vulnerabilities

Risks tied to physical and digital infrastructure are paramount

Supply chain vulnerabilities are also at the forefront

Financial and reputational impact

Investors are mindful of the financial loss from a cyber breach and potential class actions against an entity

Undetected and unknown cyber risks

The "*big risk is what you don't know*"

Entities are "*underestimating the level of risk they truly face*"

What cybersecurity information is relevant?

Use of cybersecurity frameworks	Governance processes	Future plans, resourcing and strategic goals	Incident history and remediation	Key metrics and benchmarking
Understanding an entity's current state of readiness for cyber incidents, with the use of standardised cybersecurity frameworks considered highly useful	*"the way their governance and oversight works is important"*	Statements on forward-looking strategies, future protection plans, and resource commitments Be generic and use broad language such as "*AI-driven threats*"	Critical to assessing the quality of its governance and management and whether the incident has long-term value implications	Ability to compare cybersecurity vulnerabilities and risk exposure, response plans, resourcing, and future protection plans being viewed as *"critical"*

Key metrics and benchmarking

Contextual benchmarking

As “*threat vectors are quite often sector-driven*”, comparison is most valuable when done within the same operational environment or industry

Quantitative KPIs

Operational metrics

Incident management metrics

Staff awareness metrics

Resource metrics

Use of cybersecurity frameworks

Provide alignment and a common reference point for assessing maturity and readiness across different entities

Need for standardised metrics

Effective comparison requires uniformity in reporting, including the types of metrics used and how they are defined and measured

Challenges in benchmarking

No "*lockdown definitions*"

Resource disparity, with smaller entities reporting "*no security incidents, no beaches*"

Benchmarks "*moving relatively quickly*"

Detail and technicality of cybersecurity disclosures

Location within annual report

Calls for consistency

Separate section within annual report not required, but integrated with other "*material business risk disclosures*" or the "*overall suite of sustainability disclosures*"

Sufficiently specific to assess governance structures and their effectiveness

"we absolutely don't need chapter and verse, but what we do need is enough to give us a sense that management does have a well thought out plan for addressing those issues"

Potential to "*weaponise*" information that is too specific

"If you give enough detail that people can make good assessments publicly, then I think you're actually going down the path of showing them the map to how to get to you"

Knowledge gap

Disclosures should be "*in plain English*" and "*pitched at a level of a layperson with some familiarity of the issues, but not an expert*".

To what extent do cybersecurity disclosures meet information needs?

Current cybersecurity disclosures do not meet investor information needs:

General insufficiency

Current disclosures provide only a "*relatively small amount of useful, comparable, helpful*" information that is available in a standardised form and location

Limited comparability

Current benchmarks lack "*lockdown definitions*" and the terminology is "*not consistent*" across companies, making robust comparison difficult

Investor demand vs commercial sensitivity

Desired detail for investors often conflicts with an entity's cybersecurity posture and competitive interests

Cybersecurity disclosure practices: Key recommendations

1. **Regulators to raise entity awareness of the pervasiveness of cybersecurity as a 'material' business risk**
2. **Best practice disclosures contain an assessment of an entity's cybersecurity program relative to established external frameworks and/or standards**
3. **Best practice disclosures contain a blend of qualitative information to enable an assessment of underlying governance and oversight processes, and quantitative information for benchmarking purposes**
4. **Guidance to be developed on the type, definition, and measurement of industry-based key metrics to enable meaningful comparative analysis**
5. **Best practice disclosures protect against exposing an entity's vulnerabilities and opening pathways for attack**

Closing Remarks

Australian Government
Australian Accounting Standards Board

THE UNIVERSITY OF MELBOURNE

Thank you

Subscribe

Follow

Disclaimer

Any views in this presentation do not necessarily represent the views of the AASB. Its contents do not constitute advice. The AASB expressly disclaims all liability for any loss or damages arising from reliance upon any information in this document. This document is not to be reproduced, distributed or referred to in a public document without the express prior approval of AASB staff.