Centre for International
Governance Innovation

Digital
Policy Hub

Digital Policy Hub — Working Paper

AI Standards Transparency: Decoding the Next Corporate Disclosures Frontier

Joseph Scarfone

Fall 2024 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

Mitacs

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Key Points

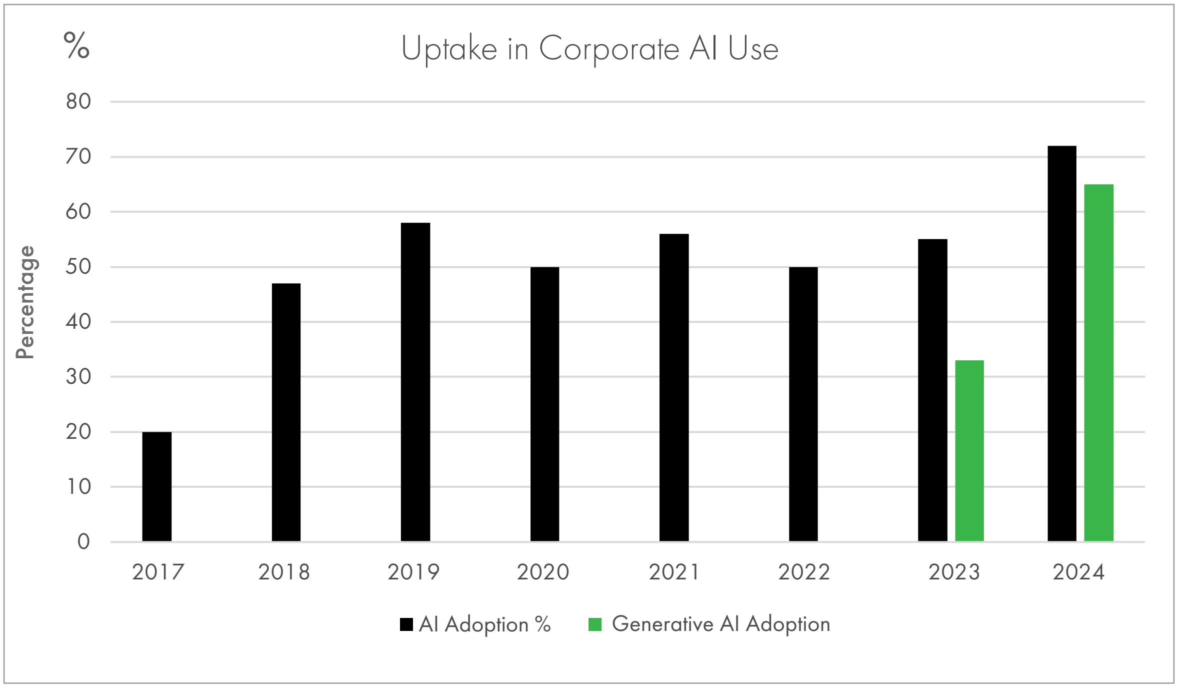
- Corporate adoption of artificial intelligence (AI) has surged, with 72 percent of Fortune 500 companies integrating AI technologies in 2024, amplifying concerns about ethical risks such as bias, privacy violations and lack of accountability.
- Corporate digital responsibility (CDR) offers a focused framework for managing digital-specific risks, addressing challenges such as algorithmic fairness, data security and ethical AI governance. Unlike broader corporate social responsibility (CSR) efforts, CDR emphasizes internal coordination among technical, legal and leadership teams to ensure responsible digital practices.
- Existing disclosure standards from the Sustainability Accounting Standards Board (SASB) and International Financial Reporting Standards (IFRS S1 and S2) do not sufficiently account for AI-related risks and opportunities, leading to inconsistencies in reporting across industries. Current frameworks often rely on qualitative measures, which lack the comparability and rigour required for effective oversight.
- Standardizing AI disclosures requires integrating industry-specific metrics that reflect AI's unique operational and ethical challenges. Examples include tracking algorithmic bias in advertising, energy efficiency in AI-driven infrastructure and data breach mitigation outcomes.
- Enhancing disclosure frameworks to include AI-specific metrics and transparency measures would improve corporate accountability and stakeholder trust. A cohesive approach to CDR ensures organizations can navigate the complexities of digital transformation while aligning with societal and regulatory expectations.

The Rise of Corporate AI

A recent survey from McKinsey & Company (2025) revealed a staggering 72 percent AI adoption among Fortune 500 companies in 2024 compared to 20 percent in 2017 and 50 percent in 2022 (see Figure 1). This surge underscores the transformative potential of AI technologies, from machine-learning algorithms to natural language processing tools, which are increasingly central to decision-making processes in industries as varied as finance, health care, retail and manufacturing. However, this rapid advancement brings significant ethical and governance challenges. The potential for biased algorithms, data breaches and opaque AI decision-making processes necessitates a commitment to transparency and accountability.

Yet, as AI systems become more sophisticated and pervasive, the call for enhanced corporate transparency grows louder. Stakeholders, including customers, regulators and investors, are increasingly concerned about AI's ethical implications, such as bias, privacy and accountability. To address these concerns, companies must implement robust transparency measures. The growing complexity of AI systems exacerbates these challenges. As models evolve from rule-based systems to deep learning networks, their decision-making processes become less interpretable, making accountability more difficult to enforce (Li et al. 2022). This opacity underscores the need for robust governance frameworks.

Figure 1: Corporate AI Use Over Time



Source: Based on data collected from the McKinsey Global Survey on AI, based on 1,363 participants at all levels of Fortune 500 organizations (McKinsey & Company 2025).

This need is becoming more widely recognized. Investors, for instance, are beginning to recognize that unchecked technological risks can translate into financial vulnerabilities. Underpinning this realization is environmental, social and governance (ESG) investing, which has amplified calls for corporate transparency more broadly (Eccles, Ioannou and Serafeim 2012). Regulators, too, are stepping up efforts to mitigate digital risks through policies such as Canada's Digital Charter in 2022. Consumers and civil society organizations have also exerted pressure, demanding that corporations align their digital practices with ethical norms and societal values.

The question is no longer whether corporations should address the governance challenges associated with AI and big data but rather how they can do so effectively. The answer lies in moving beyond ad hoc or reactionary measures to establish a coherent framework for CDR.

Corporate Digital Responsibility

Early discussions on digital responsibility began with concerns about privacy and surveillance, as articulated by seminal works such as Alan F. Westin's *Privacy and Freedom* (1967) and later by Roger Clarke (1988), who introduced the concept of "dataveillance" to describe the systematic monitoring of individuals through data. These concerns expanded with the advent of big data, as researchers such as Shoshana Zuboff (2015) highlighted the exploitative practices of "surveillance capitalism." AI has further complicated the ethical landscape, with scholars such as Reuben Binns (2018) and Brent Daniel Mittelstadt et al. (2016) addressing algorithmic bias and opacity issues. The increasing prevalence of algorithmic decision making in critical sectors such as health care, finance and criminal justice has underscored the need for governance frameworks that extend beyond traditional CSR approaches to encompass digital-specific risks. Some key developments toward CDR include the 2018 European Union's General Data Protection Regulation (GDPR) as the global benchmark for data privacy and accountability and the Partnership on AI (2016),[1] established by leading technology companies to promote responsible AI practices.

While CDR and CSR share the common goal of embedding ethical practices into corporate strategies, they differ significantly in scope, stakeholder focus and methodology. CSR traditionally addresses broad ESG concerns, such as climate change, labour rights and community development, providing a framework for corporate accountability on wide-ranging societal issues (Carroll and Shabana 2010). In contrast, CDR emphasizes digital policy. Another key distinction lies in the focus of stakeholder engagement. CSR initiatives typically emphasize external stakeholders, such as communities, non-governmental organizations and regulators, to build trust and foster positive societal impacts. CDR, on the other hand, necessitates a stronger emphasis on internal alignment. It requires coordination among technical teams responsible for system design, legal departments that ensure regulatory compliance and corporate leadership that oversees ethical governance strategies (Jobin, Ienca and Vayena 2019).

The frameworks and metrics used for reporting further distinguish CDR from CSR. CSR often relies on well-established reporting standards, including the Global Reporting Initiative,[2] the SASB, and, more recently, the IFRS S1 and S2, for non-financial disclosures. CDR, by contrast, is still in its formative stages and lacks standardized metrics for evaluating digital responsibility. As organizations and policy makers work toward formalizing these standards, significant gaps remain in defining how companies should measure and report their digital ethics practices (Witzel and Bhargava 2023). For example, while a CSR initiative might involve efforts to reduce a company's carbon footprint through energy efficiency programs or renewable energy adoption, a CDR initiative would focus on ensuring that AI systems used in hiring processes are free from biases or that consumer data collection complies with privacy regulations such as GDPR.

Non-financial Corporate Reporting

One of the most significant recent developments in corporate disclosure practices is the introduction of the IFRS S1 and S2, which is taking effect in 2024–2025. These standards streamline sustainability-related disclosures, ensuring public companies in countries such as Canada provide consistent information.

However, applying these standards to AI presents several challenges. IFRS S1 and S2 are largely based on the SASB framework, which provides industry-specific metrics for

[1] See https://partnershiponai.org.

[2] See www.globalreporting.org/standards/.

sustainability disclosures. For example, the energy sector may focus on carbon emissions and renewable energy use, while the financial sector may highlight cybersecurity and data privacy risks.[3] Incorporating AI-related disclosures into these standards requires carefully considering what constitutes materiality — that is, which aspects of AI are deemed significant enough to impact a company's performance or value.

AI-related risks and opportunities vary widely across industries. In finance, AI is often used in algorithmic trading, fraud detection and risk management. In health care, AI applications may involve medical diagnostics and treatment recommendations, where ethical concerns around accuracy, patient safety and algorithmic decision making come to the forefront (Rai 2020). The lack of industry-specific AI disclosure guidelines complicates consistent and comprehensive reporting.

Challenges in Standardizing AI Disclosures

Standardizing AI disclosures within the existing frameworks is particularly challenging for several reasons. First, AI is a rapidly evolving field, with new technologies and applications emerging regularly. As a result, what is considered material today may change in the near future. For instance, AI systems that automate routine processes may not have been deemed material for disclosure purposes a few years ago, but as AI systems become more integral to strategic decision making, the need for transparency around their use has grown (Binns 2018).

Second, AI-related risks are multifaceted and vary significantly by industry. In some industries, such as manufacturing, AI applications might focus on automation and efficiency gains, where the material risks are related to job displacement and operational transparency. In other sectors, such as finance, using AI in high-stakes decisions, such as credit scoring and investment strategies, introduces fairness, bias and accountability risks. Defining a one-size-fits-all standard for AI disclosures is problematic because it fails to account for these nuanced differences in AI applications (Ananny and Crawford 2018).

Moreover, the proprietary nature of AI systems further complicates disclosure efforts. Companies may be reluctant to disclose too much about their AI technologies due to concerns over intellectual property and competitive advantage. This creates a tension between the need for transparency and the desire to protect sensitive business information (Pasquale 2015).

Another challenge lies in determining which aspects of AI should be considered material for disclosure purposes. Under existing financial reporting standards, "materiality" refers to information that could influence an investor's decision making. Applying this concept to AI is difficult because AI's impact is often indirect and not immediately quantifiable. For example, the reputational risks associated with AI bias may not have a direct financial impact but could

[3] See https://sasb.ifrs.org.

influence consumer trust and long-term brand value. This raises questions about measuring and reporting such intangible risks (Veale and Edwards 2018).

The Role of Voluntary and Involuntary Corporate Disclosures

Given the challenges of standardizing AI disclosures, the current landscape is characterized by both voluntary and mandatory disclosures. Some companies choose to proactively disclose how they use AI, often to demonstrate ethical practices or technological leadership. For example, Microsoft released reports detailing its AI governance frameworks.[4] However, these disclosures are often selective and tailored to emphasize the company's strengths rather than to offer a comprehensive view of AI's role in their operations.

In contrast, involuntary disclosures arise from regulatory requirements and are generally less flexible. Companies will face greater pressure to disclose under new regulatory requirements. However, they may also struggle to determine how much detail to provide without clear guidance on what constitutes material AI information. This uncertainty could lead to inconsistent reporting across industries, undermining the goal of creating a level playing field for AI disclosures (Weber 2020). Although these mandatory disclosure requirements are not the optimal way to report on a company basis, they provide the best means for comparing companies in aggregate.

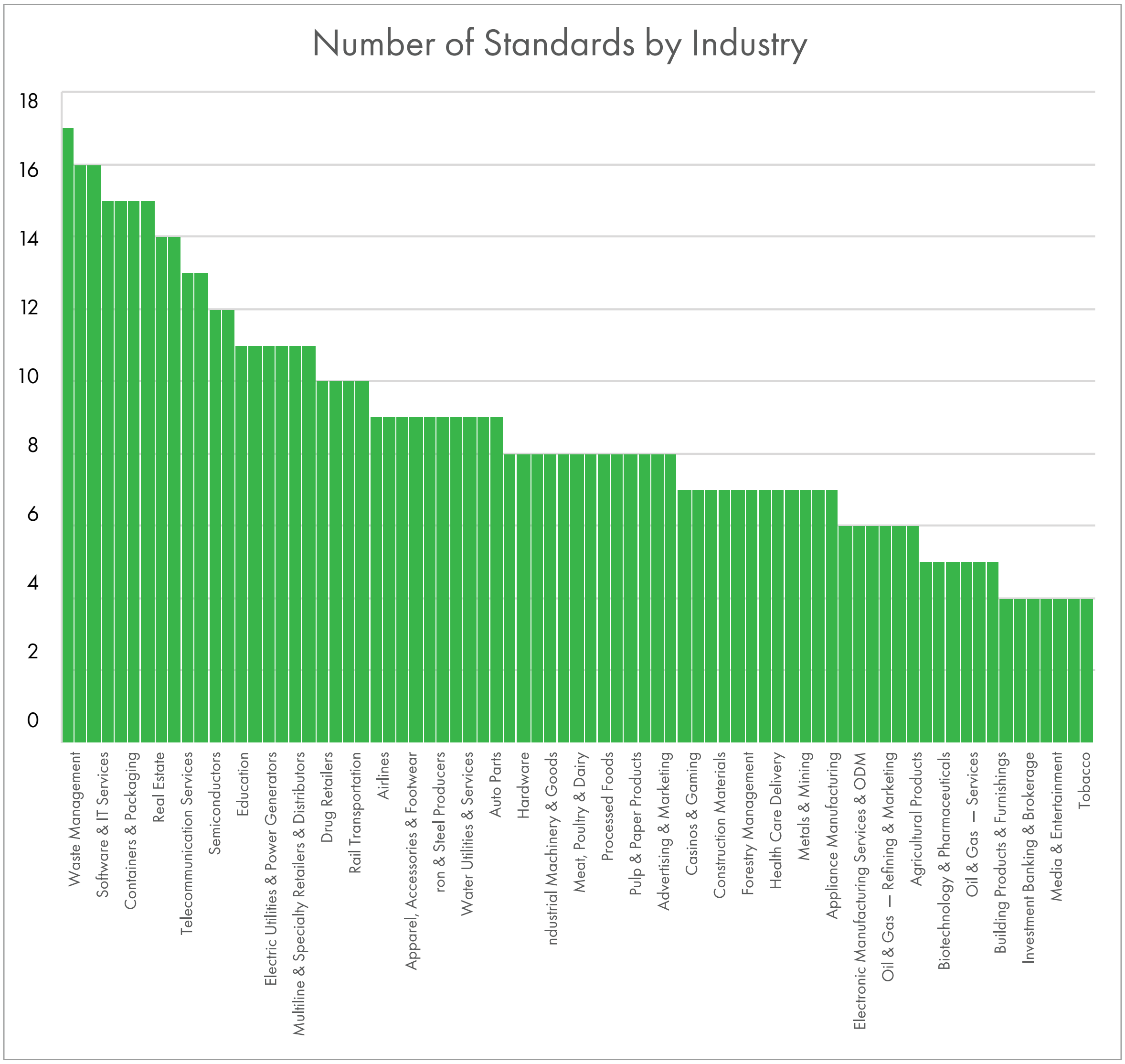
Methods

The first step in this research involves a comprehensive review of the IFRS S1 and S2 standards, which will come into effect in 2024–2025. IFRS S1 and S2 are primarily designed to address sustainability disclosures, providing stakeholders with material information on ESG issues. They are based on 665 specific SASB rules across 77 specific industries (see Figure 2). However, while these standards focus heavily on climate-related disclosures, they do not fully address AI-related concerns. This gap represents a critical opportunity to explore how AI might be incorporated into the evolving sustainability disclosure frameworks. It will focus on identifying areas where AI-related risks and opportunities could be material. For example, IFRS S2 focuses on climate-related disclosures. Still, its emphasis on forward-looking information and risk management could be extended to AI, particularly in industries where AI is a key driver of business strategy or presents significant operational risks.[5] By mapping SASB's existing industry-specific metrics to AI-related risks and opportunities, this research will identify which industries are most likely to consider AI disclosure material and which aspects of AI should be reported. In preparation for writing this working paper, all industry standards under SASB/IFRS S1 and S2 were downloaded to the most recent published versions.

[4] See www.microsoft.com/en-us/ai/responsible-ai.

[5] See www.ifrs.org/.

Figure 2: Indicators Across All 77 SASB Industries

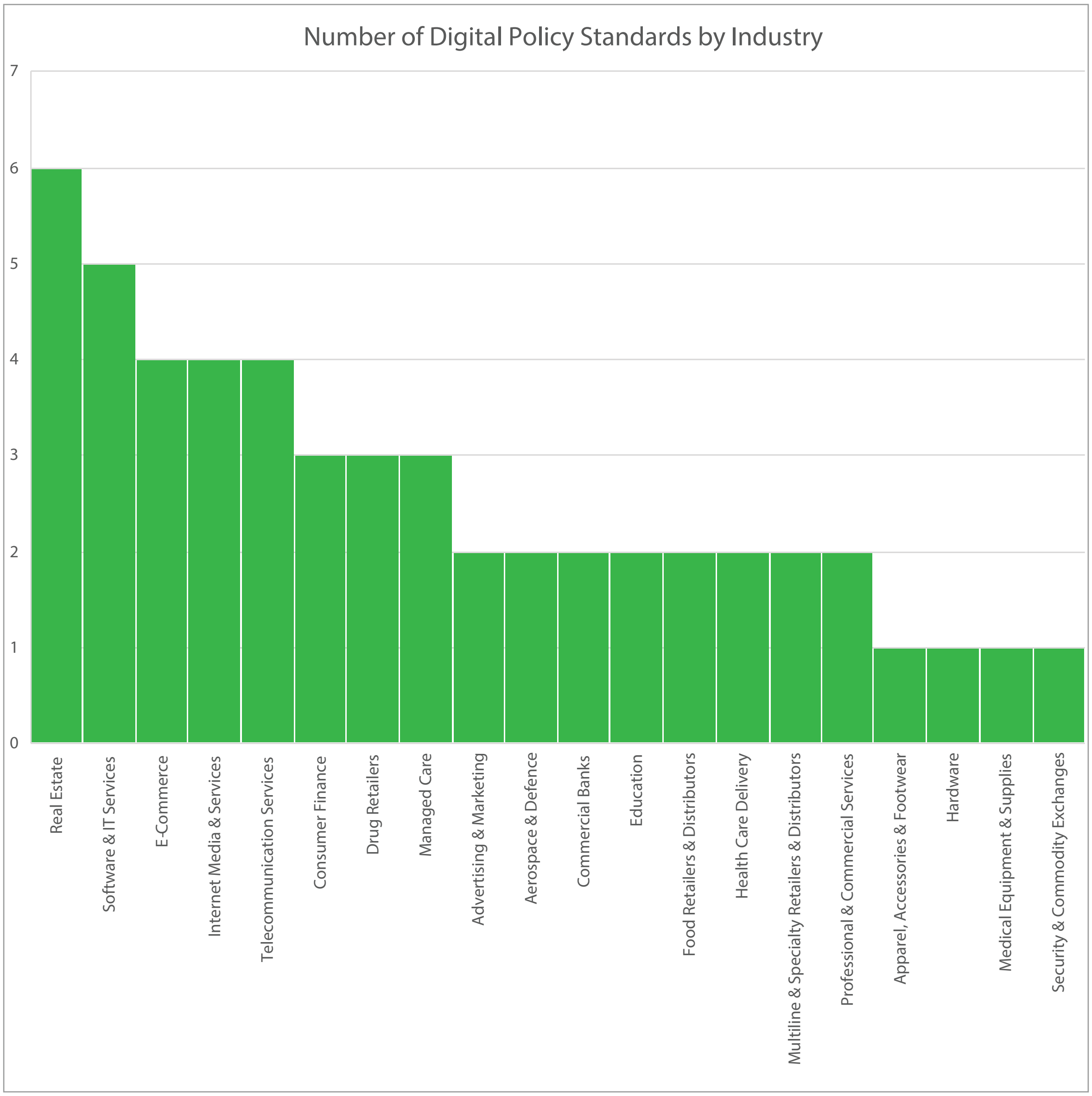


Source: https://sasb.ifrs.org.
Note: IT = information technology; ODM = original design manufacturer.

SASB standards cover 77 specific industries, yet only 20 industries have some form of mandatory corporate disclosures around facets of CDR. As expected, many of these disclosures are related to consumer privacy and software industries. Surprisingly, real estate has the most robust requirements for digital policy disclosures. However, the type of these disclosures varies between the general standards and those in digital policy.

A major point of contention is the increased reliance on discussion and analysis metrics instead of objective quantitative metrics within existing SASB requirements on CDR. While discussion and analysis are vital, it is difficult to clearly compare company to company at scale as is possible with quantitative metrics. They are also less effective in audit or assurance third-party verifications that are vital for corporate legitimacy and trust.

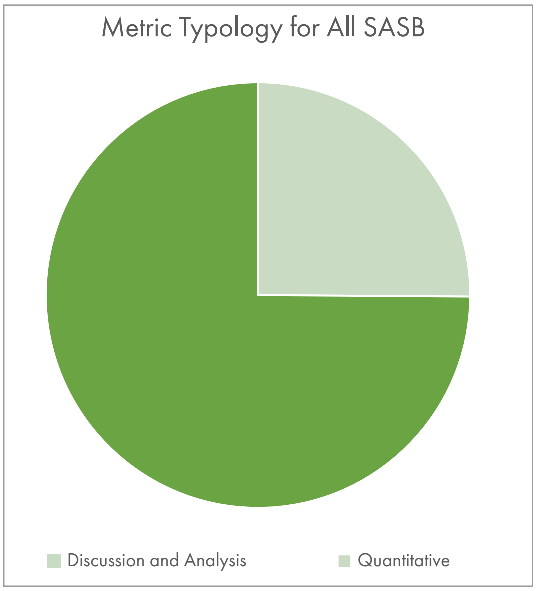
Figure 3: AI-Related Indicators Across SASB Industries



Source: https://sasb.ifrs.org.
Note: IT = information technology

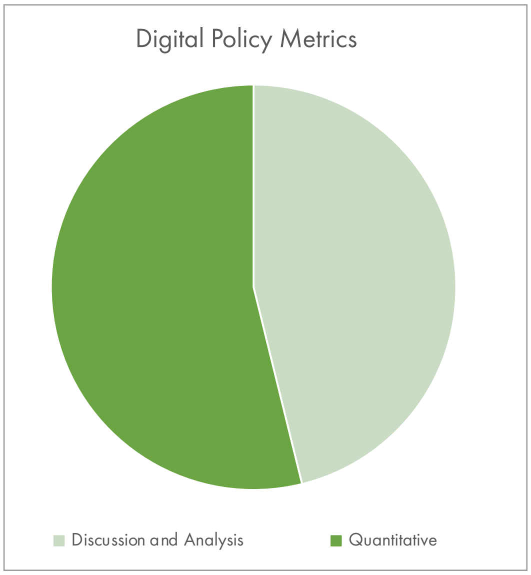
However, the quantitative metrics used in digital policy disclosures tend to be easier to analyze and more generalizable across industries, which is ideal for establishing general corporate benchmarks. When the SASB metrics were first created, CDR was not considered as material as today. Therefore, it is important to analyze the existing requirements to see what, if any, low-hanging fruit is available to roll out at scale as a CDR disclosure guideline. Appendix 1 provides detailed guidance on all the CDR-related disclosure metrics under the current rules as of December 2024.

Figure 4: Metric Typology Across All 665 SASB Indicators



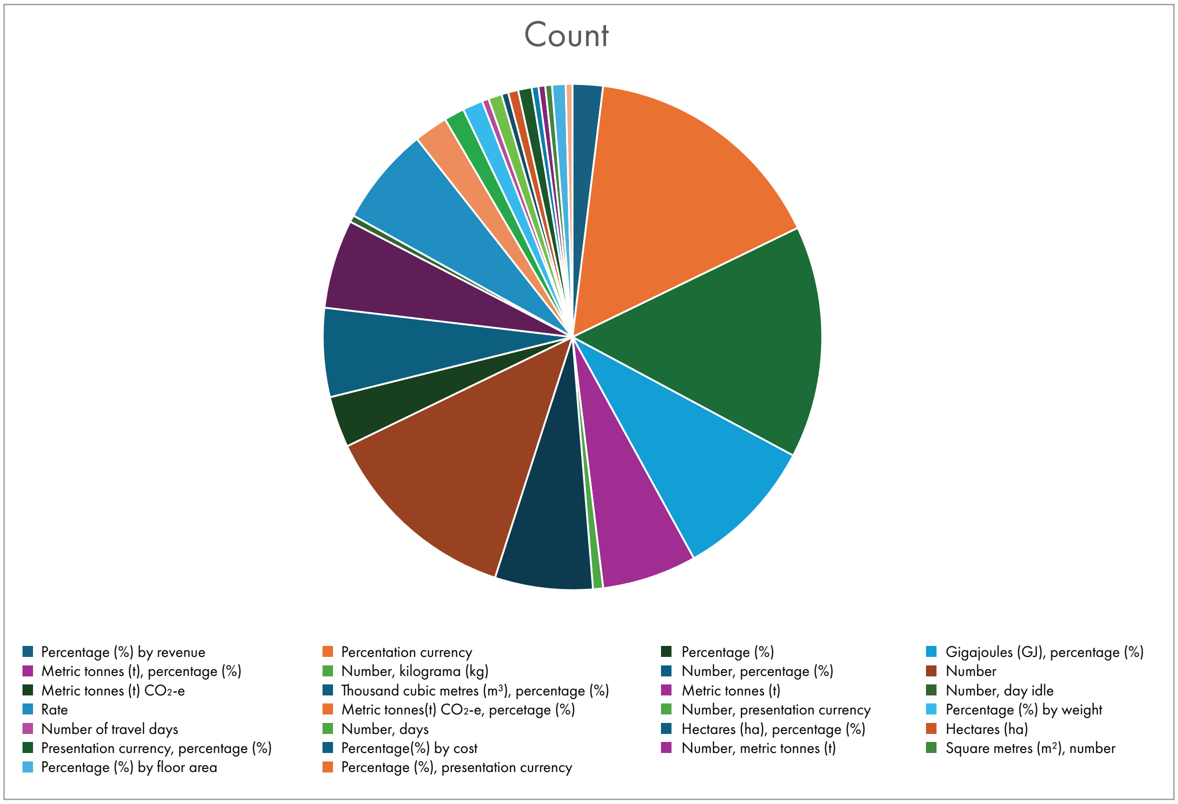
Source: https://sasb.ifrs.org.

Figure 5: Metric Typology Across SASB Indicators for CDR



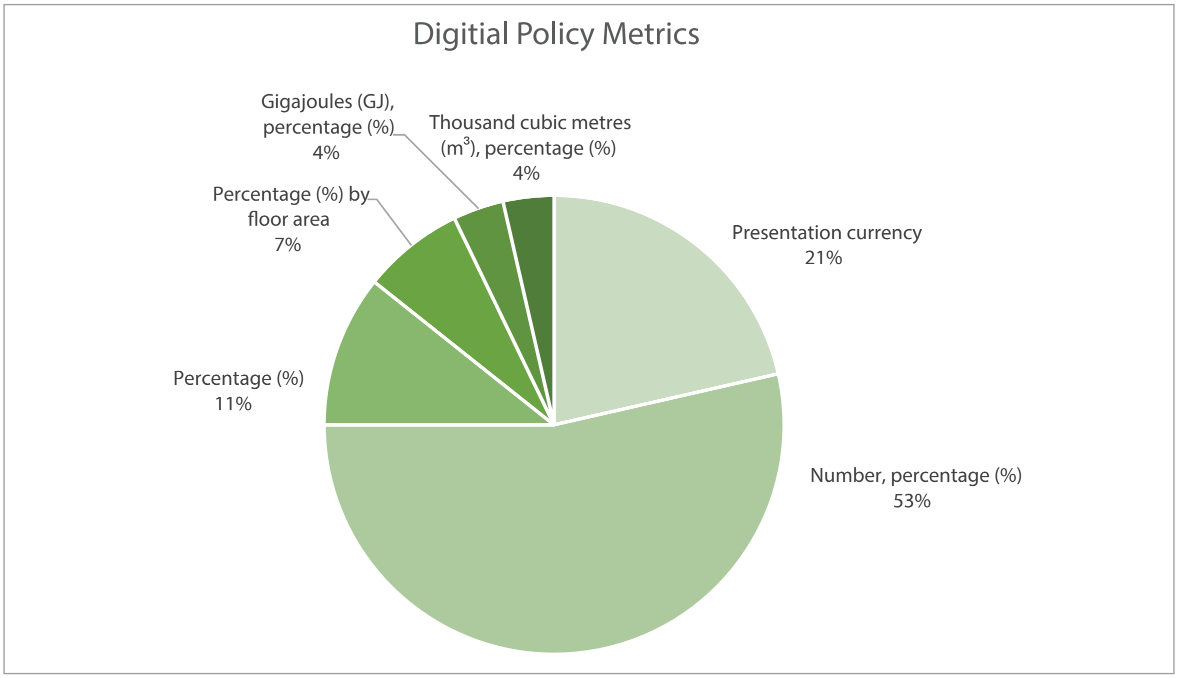
Source: https://sasb.ifrs.org.

Figure 6: Quantitative Metric Units of Measurement Across All 665 SASB Indicators



Source: https://sasb.ifrs.org.

Figure 7: Quantitative Metric Units of Measurement Across SASB CDR Indicators



Source: https://sasb.ifrs.org.

Discussion and Analysis

Data Privacy and Security: Bridging the Quantitative-Qualitative Divide

SASB data privacy and security standards effectively emphasize quantitative metrics such as the number of data breaches, the percentage of these breaches that involve personal or confidential information and the monetary losses from related legal proceedings. These metrics provide a clear baseline for accountability and comparability across industries. However, the standards underutilize qualitative disclosures, particularly in detailing the strategic and operational approaches employed to mitigate risks. While discussions of policies and practices exist, they are often generic, providing less insight into proactive measures or adaptive strategies.

For example, disclosures about breaches lack nuance regarding severity or organizational responses. While companies are expected to report the number of breaches and affected parties, there is no requirement to disclose whether breaches resulted in operational downtime, regulatory penalties or reputational damage. Furthermore, while third-party cybersecurity standards are mentioned, there is no mechanism for assessing compliance or the effectiveness of these standards. SASB could require companies to disclose the outcomes of risk mitigation practices, including specific case studies that illustrate best practices.

Actionable enhancements to this area include mandating detailed reporting on the nature and scale of breaches and contextualizing data within broader cybersecurity frameworks. Disclosures could also include forward-looking metrics such as investment in cybersecurity infrastructure, training programs and the adoption of advanced threat detection technologies such as AI-driven monitoring systems.

The Environmental Footprint of Digital Infrastructure: An Overlooked Opportunity

SASB's inclusion of energy and water management metrics for digital infrastructure reflects a growing awareness of the environmental costs of data operations. Current standards, such as measuring energy consumption by portfolio area and quantifying the use of renewable energy, are commendable for their specificity and applicability. However, these standards often fail to capture the unique demands of AI-driven infrastructure, which significantly increase energy usage through high-performance computing and extensive training data sets.

Moreover, existing standards do not require companies to disclose whether energy efficiencies or renewable energy sources are attributable to AI optimizations or traditional conservation methods. This omission limits the ability to assess whether companies leverage AI's full potential to reduce environmental impacts. Similarly, while water management standards address withdrawal and stress in high-risk areas, they do not consider the operational specifics of cooling requirements in data centres — a critical factor for AI-based processing.

SASB could integrate AI-specific metrics into its environmental standards. For instance, organizations could report the proportion of AI workloads powered by renewable energy or the reductions in energy consumption achieved through algorithmic optimizations. These metrics would offer more granular insights into how companies align digital innovation with sustainability goals.

Targeted Advertising and Consumer Privacy: A Case for Algorithmic Transparency

Standards addressing targeted advertising and consumer privacy focus primarily on policies and practices without requiring organizations to quantify the impact or efficacy of these measures. While discussions of targeted advertising policies are essential, omitting actionable metrics undermines the ability to evaluate ethical implications. For instance, disclosures do not require organizations to report the prevalence of algorithmic biases or the steps taken to ensure fairness in targeted advertising.

This gap is particularly critical in AI-driven advertising systems, which can inadvertently reinforce discriminatory practices or exploit consumer vulnerabilities. Without standardized metrics for algorithmic transparency and fairness, the current standards fail to provide a comprehensive view of how organizations manage these risks. Moreover, there is little guidance on how companies should balance consumer privacy with the monetization of personal data through advertising models.

To address these shortcomings, SASB could introduce requirements for companies to disclose the results of algorithmic audits, including metrics that assess bias, fairness and transparency. Companies should also report on the ethical frameworks they use to guide AI-driven advertising decisions, providing stakeholders with a clearer understanding of how they mitigate risks.

Freedom of Expression and Ethical AI: Moving Beyond Privacy

The intersection of freedom of expression and digital responsibility is addressed tangentially in the SASB standards, often within the context of privacy and advertising policies. However, the increasing role of AI in moderating content and shaping public discourse necessitates more explicit disclosures. Organizations deploying AI in content moderation face complex challenges, including balancing enforcing community standards with protecting individual rights.

SASB standards do not require disclosures about the ethical considerations of content moderation or the potential for algorithmic suppression of marginalized voices. This gap leaves stakeholders without a clear understanding of how organizations address the broader societal implications of their digital policies. Moreover, the absence of standardized metrics for ethical AI governance limits the ability to evaluate corporate accountability in this area.

SASB should expand its standards to include disclosures on the governance of AI systems used in content moderation. Organizations could be required to report the outcomes of bias mitigation efforts, the mechanisms used to review algorithmic decisions and the involvement of diverse stakeholders in developing moderation policies. These disclosures would provide a more holistic view of how companies navigate the ethical complexities of AI deployment.

Recommendations for Enhanced Standards

The analysis reveals several areas where sustainability reporting standards can better evolve to address the challenges and opportunities of digital responsibility. First, there is a need to balance quantitative and qualitative disclosures, ensuring that metrics quantify outcomes and provide actionable insights into organizational practices. Second, the SASB should integrate AI-specific metrics across all relevant standards, reflecting AI's growing influence in shaping digital operations and governance. Enhanced standards will improve corporate accountability and provide stakeholders with the insights needed to navigate the complexities of CDR

About the Author

Joseph Scarfone is a former Digital Policy Hub master's fellow and MES Sustainability Management student at the University of Waterloo, as well as an adjunct professor at Conestoga College. Joseph's research primarily focuses on non-financial corporate reporting and sustainable finance, where he employs machine-learning models for large-scale data mining and textual analytics. At the Digital Policy Hub, Joseph researched on corporate digital responsibility reporting and governance practices from a normative and positive perspective. His research strives to help improve transparency regarding how disruptive technologies and big data are used within companies for regulators and the wider public.

Works Cited

Ananny, Mike and Kate Crawford. 2018. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability." *New Media & Society* 20 (3): 973–89. https://doi.org/10.1177/1461444816676645.

Binns, Reuben. 2018. "Fairness in Machine Learning: Lessons from Political Philosophy." *Proceedings of the First Conference on Fairness, Accountability and Transparency* 81: 1–11. http://proceedings.mlr.press/v81/binns18a/binns18a.pdf.

Carroll, Archie B. and Kareem M. Shabana. 2010. "The Business Case for Corporate Social Responsibility: A Review of Concepts, Research and Practice." *International Journal of Management Reviews* 12 (1): 85–105. https://doi.org/10.1111/j.1468-2370.2009.00275.x.

Clarke, Roger. 1988. "Information technology and dataveillance." *Communications of the ACM* 31 (5): 498–512. https://doi.org/10.1145/42411.42413.

Eccles, Robert G., Ioannis Ioannou and George Serafeim. 2012. "The Impact of Corporate Sustainability on Organizational Processes and Performance." *Management Science* 60 (11): 2835–57. https://doi.org/10.1287/mnsc.2014.1984.

Jobin, Anna, Marcello Ienca and Effy Vayena. 2019. “The global landscape of AI ethics guidelines.” *Nature Machine Intelligence* 1: 389–99. https://doi.org/10.1038/s42256-019-0088-2.

Li, Xuhong, Haoyi Xiong, Xingjian Li, Xuanyu Wu, Xiao Zhang, Ji Liu, Jiang Bian and Dejing Dou. 2022. “Interpretable deep learning: interpretation, interpretability, trustworthiness, and beyond.” *Knowledge and Information Systems* 64: 3197–234. https://doi.org/10.1007/s10115-022-01756-8.

McKinsey & Company. 2025. “The state of AI: How organizations are rewiring to capture value.” McKinsey & Company, March 12. www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai.

Mittelstadt, Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter and Luciano Floridi. 2016. “The ethics of algorithms: Mapping the debate.” *Big Data & Society* 3 (2). https://doi.org/10.1177/2053951716679679.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge, MA: Harvard University Press.

Rai, A. 2020. “Explainable AI: from black box to glass box.” *Journal of the Academy of Marketing Science* 48: 137–41. https://doi.org/10.1007/s11747-019-00710-5.

Veale, Michael and Lilian Edwards. 2018. “Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling.” *Computer Law & Security Review* 34 (2): 398–404. https://doi.org/10.1016/j.clsr.2017.12.002.

Weber, Rolf H. 2020. “Socio-ethical values and legal rules on automated platforms: The quest for a symbiotic relationship.” *Computer Law & Security Review* 36: 105380. https://doi.org/10.1016/j.clsr.2019.105380.

Westin, Alan F. 1967. *Privacy and Freedom*. New York, NY: Atheneum.

Witzel, Mardi and Niraj Bhargava. 2023. *AI-Related Risk: The Merits of an ESG-Based Approach to Oversight*. CIGI Paper No. 279. Waterloo, ON: CIGI. www.cigionline.org/publications/ai-related-risk-the-merits-of-an-esg-based-approach-to-oversight/.

Zuboff, Shoshana. 2015. “Big other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30 (1): 75–89. https://doi.org/10.1057/jit.2015.5.

Appendix 1: SASB Digital Policy Accounting Standards

Industry	Category	Summary	Type	Metric	Code
Advertising & Marketing	Data Privacy	Discussion of policies and practices relating to targeted advertising and consumer privacy	Discussion and Analysis	n/a	SV-AD-220a.1
Advertising & Marketing	Data Privacy	Total amount of monetary losses as a result of legal proceedings associated with consumer privacy	Quantitative	Presentation currency	SV-AD-220a.3
Aerospace & Defence	Data Security	(1) Number of data breaches, (2) percentage involving confidential information	Quantitative	Number, percentage (%)	RT-AE-230a.1
Aerospace & Defence	Data Security	Description of approach to identifying and addressing data security risks in (1) entity operations and (2) products	Discussion and Analysis	n/a	RT-AE-230a.2
Apparel, Accessories & Footwear	Environmental Impacts in the Supply Chain	Percentage of (1) Tier 1 supplier facilities and (2) supplier facilities beyond Tier 1 that have completed the Higg FEM assessment or equivalent environmental data assessment	Quantitative	Percentage (%)	CG-AA-430a.2
Commercial Banks	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of account holders affected	Quantitative	Number, percentage (%)	FN-CB-230a.1
Commercial Banks	Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	FN-CB-230a.2
Consumer Finance	Customer Privacy	Total amount of monetary losses from legal proceedings related to customer privacy	Quantitative	Presentation currency	FN-CF-220a.2
Consumer Finance	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of account holders affected	Quantitative	Number, percentage (%)	FN-CF-230a.1
Consumer Finance	Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	FN-CF-230a.3
Drug Retailers	Data Security & Privacy	Description of policies to secure customers' personal and health data	Discussion and Analysis	n/a	HC-DR-230a.1
Drug Retailers	Data Security & Privacy	(1) Number of data breaches, (2) percentage involving (a) personal and (b) health data, (3) affected customers	Quantitative	Number, percentage (%)	HC-DR-230a.2
Drug Retailers	Data Security & Privacy	Total monetary losses from data security and privacy legal proceedings	Quantitative	Presentation currency	HC-DR-230a.3
E-Commerce	Hardware Infrastructure Energy & Water Management	Discussion of integration of environmental considerations into data centre strategic planning	Discussion and Analysis	n/a	CG-EC-130a.3
E-Commerce	Data Privacy & Advertising Standards	Description of policies and practices related to targeted advertising and user privacy	Discussion and Analysis	n/a	CG-EC-220a.2

Industry	Category	Summary	Type	Metric	Code
E-Commerce	Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	CG-EC-230a.1
E-Commerce	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of users affected	Quantitative	Number, Percentage (%)	CG-EC-230a.2
Education	Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	SV-ED-230a.1
Education	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches,(3) number of students affected	Quantitative	Number, Percentage (%)	SV-ED-230a.3
Food Retailers & Distributors	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of customers affected	Quantitative	Number, Percentage (%)	FB-FR-230a.1
Food Retailers & Distributors	Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	FB-FR-230a.2
Hardware	Product Security	Description of approach to identifying and addressing data security risks in products	Discussion and Analysis	n/a	TC-HW-230a.1
Health Care Delivery	Patient Privacy & Electronic Health Records	Description of policies and practices to secure patient personal health data	Discussion and Analysis	n/a	HC-DY-230a.2
Health Care Delivery	Patient Privacy & Electronic Health Records	(1) Number of data breaches, (2) breakdown by personal data type, (3) number of customers affected	Quantitative	Number, Percentage (%)	HC-DY-230a.3
Internet Media & Services	Environmental Footprint of Hardware Infrastructure	Discussion of integration of environmental considerations into strategic planning for data centre needs	Discussion and Analysis	n/a	TC-IM-130a.3
Internet Media & Services	Data Privacy, Advertising Standards & Freedom of Expression	Description of policies and practices relating to targeted advertising and user privacy	Discussion and Analysis	n/a	TC-IM-220a.1
Internet Media & Services	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of users affected	Quantitative	Number, Percentage (%)	TC-IM-230a.1

Industry	Category	Summary	Type	Metric	Code
Internet Media & Services	Data Security	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-IM-230a.2
Managed Care	Customer Privacy & Technology Standards	Description of policies and practices to secure customers' personal health data	Discussion and Analysis	n/a	HC-MC-230a.1
Managed Care	Customer Privacy & Technology Standards	(1) Number of data breaches, (2) percentage involving (a) personal data only and (b) personal health data, (3) number of customers affected in each category, (a) personal data only and (b) personal health data	Quantitative	Number, percentage (%)	HC-MC-230a.2
Managed Care	Customer Privacy & Technology Standards	Total amount of monetary losses as a result of legal proceedings associated with data security and privacy	Quantitative	Presentation currency	HC-MC-230a.3
Medical Equipment & Supplies	Product Safety	Products listed in any public medical product safety or adverse event alert database	Discussion and Analysis	n/a	HC-MS-250a.2
Multiline & Specialty Retailers & Distributors	Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	CG-MR-230a.1
Multiline & Specialty Retailers & Distributors	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of customers affected	Quantitative	Number, percentage (%)	CG-MR-230a.2
Professional & Commercial Services	Data Security	Description of approach to identifying and addressing data security risks	Discussion and Analysis	n/a	SV-PS-230a.1
Professional & Commercial Services	Data Security	(1) Number of data breaches, (2) percentage involving (a) customers' confidential business information and (b) personal data breaches, 3) number of (a) customers and (b) individuals affected	Quantitative	Number, percentage (%)	SV-PS-230a.3

Industry	Category	Summary	Type	Metric	Code
Real Estate	Energy Management	Energy consumption data coverage as a percentage of total floor area, by property sector	Quantitative	Percentage (%) by floor area	IF-RE-130a.1
Real Estate	Energy Management	(1) Total energy consumed by portfolio area with data coverage, (2) percentage grid electricity, and (3) percentage renewable, by property sector	Quantitative	Gigajoules (GJ), Percentage (%)	IF-RE-130a.2
Real Estate	Energy Management	Like-for-like percentage change in energy consumption for the portfolio area with data coverage, by property sector	Quantitative	Percentage (%)	IF-RE-130a.3
Real Estate	Water Management	Water withdrawal data coverage as a percentage of (1) total floor area and (2) floor area in regions with High or Extremely High Baseline Water Stress, by property sector	Quantitative	Percentage (%) by floor area	IF-RE-140a.1
Real Estate	Water Management	(1) Total water withdrawn by portfolio area with data coverage and (2) percentage in regions with High or Extremely High Baseline Water Stress, by property sector	Quantitative	Thousand cubic metres (m³), Percentage (%)	IF-RE-140a.2
Real Estate	Water Management	Like-for-like percentage change in water withdrawn for portfolio area with data coverage, by property sector	Quantitative	Percentage (%)	IF-RE-140a.3
Security & Commodity Exchanges	Managing Business Continuity & Technology Risks	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of customers affected	Quantitative	Number, Percentage (%)	FN-EX-550a.2
Software & IT Services	Environmental Footprint of Hardware Infrastructure	Discussion of the integration of environmental considerations into strategic planning for data centre needs	Discussion and Analysis	n/a	TC-SI-130a.3
Software & IT Services	Data Privacy & Freedom of Expression	Description of policies and practices relating to targeted advertising and user privacy	Discussion and Analysis	n/a	TC-SI-220a.1
Software & IT Services	Data Privacy & Freedom of Expression	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Quantitative	Presentation currency	TC-SI-220a.3

Industry	Category	Summary	Type	Metric	Code
Software & IT Services	Data Security	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-SI-230a.2
Telecommunication Services	Data Privacy	Description of policies and practices relating to targeted advertising and customer privacy	Discussion and Analysis	n/a	TC-TL-220a.1
Telecommunication Services	Data Privacy	Total amount of monetary losses as a result of legal proceedings associated with customer privacy	Quantitative	Presentation currency	TC-TL-220a.3
Telecommunication Services	Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of customers affected	Quantitative	Number, percentage (%)	TC-TL-230a.1
Telecommunication Services	Data Security	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-TL-230a.2

Source: https://sasb.ifrs.org