Technology Landscape: Focus on Data Governance

Introduction

This publication forms part of the IESBA's Technology Working Group's Phase 2 Report, which documents the impacts of disruptive and transformative technologies on the work of professional accountants, and provides extensive analysis and insights into the ethics dimension of those developments.

Specifically, this publication surveys the technology landscape in relation to Focus on Data Governance and summarizes the outcomes of the Working Group's fact-finding into the trends, opportunities, and impact/ risks related to ethics implications of such technologies.

The Working Group comprises Brian Friedrich, IESBA Member and Chair of the Working Group; Vania Borgerth, IESBA Member; David Clark, IESBA Technical Advisor; Christelle Martin, IESBA Member; and Sundeep Takwani, former IESBA Technical Advisor.

The full Phase 2 Report also discusses the relevance and importance of the overarching principles and specific provisions in the *International Code of Ethics for Professional Accountants (including International Independence Standards)* (the Code) in laying out the ethics guardrails for professional accountants as they face opportunities and challenges in their work as a result of rapid digitalization.

This publication does not amend or override the Code, the text of which alone is authoritative and reading it is not a substitute for reading the Code and is not intended to be exhaustive and reference to the Code itself should always be made. This publication does not constitute an authoritative or official pronouncement of the IESBA.

Technology Landscape

This section covers the trends, opportunities, and impact/risks of the following technologies and related issues: Robotic Process Automation (RPA), AI, blockchain, cloud computing, and data governance, including cybersecurity. Key ethics-related concerns arising from these technologies and issues are covered in the subsequent subsection entitled *C: Potential Ethics Impact on the Behavior of PAs*. The Working Group notes that most of the ethics-related impact/risks and key concerns are addressed by provisions in the extant Code and proposals in the Technology ED. Those that the Working Group believes can benefit from further guidance are outlined in *Section III: Insights and Recommendations*.

Stakeholders report that the most common emerging technologies and technology-related issues currently impacting business processes are RPA, AI (including intelligent process automation (IPA)),[1] cybersecurity (including data privacy), and blockchain. It was consistently reported, however, that the uptake by organizations of AI and blockchain-related technologies is slower than expected and slower relative to the publicity these technologies receive. Based on stakeholder and TEG commentary, as well as

desk research, it appears that most organizations are finding these technologies challenging to effectively implement as a result of process fragmentation, resources being allocated to other priorities, difficulties in establishing business cases (for example, a lack of understanding of the return on investment (ROI) arising from the technology or a belief that the ROI is too slow), and the general lack of maturity, and accordingly lack of understanding, of the technologies.

Nevertheless, accelerated implementation of transformative technologies has been observed – particularly in the past couple of years – often connected with mitigating business issues related to the COVID-19 pandemic, such as RPA, cloud computing, tools to support remote working and access, and addressing cybersecurity concerns.

Focus on Data Governance

1. Data governance is foundational to building and maintaining organizational value at both strategic and operational levels. It has become critical in today's data- and information-driven world, where technology and related decisions rely on quality data. Quality data has three characteristics: accuracy, completeness, and reliability.

2. Most organizations are flooded with data. Almost every action anyone takes leaves a digital trail. On top of this, the amount of machine-generated data is also growing rapidly. Data is generated and shared when "smart" home IoT devices communicate with each other or with their home servers. Industrial machinery in plants and factories around the world are increasingly equipped with IoT sensors that gather and transmit data.

3. Data itself is increasingly seen as a commodity and a source of strategic advantage, despite its not (yet) being recognized as an "asset" on the traditional balance sheet. However, the mere possession of abundant amounts of data is not enough. What is foundational is the ability to refine, process, and evaluate data and capture meaning from unstructured data that can tell a story to provide both strategic and operational value to an organization. In this regard, the level of activity (and type of value provided) in the data and analytics space over the last two years has generally evolved around four categories:[2]

(a) Descriptive, focused on what has happened.

(b) Diagnostic, focused on why it has happened.

(c) Predictive, used to forecast what could happen.

(d) Prescriptive, analyzed to help determine what should be done.

4. As outlined in the discussions on *RPA* and *AI* technology trends, opportunities and impacts/risks, organizations are also increasingly automating traditional manual, human-led processes, as well as utilizing AI for such data manipulation.

5. Successful automation is driven in part by consistent data, but a major challenge encountered by stakeholders is that typically there are legacy systems in organizations that are set up differently from each other. This increases the risk of error as the data are often both unstructured and not standardized.

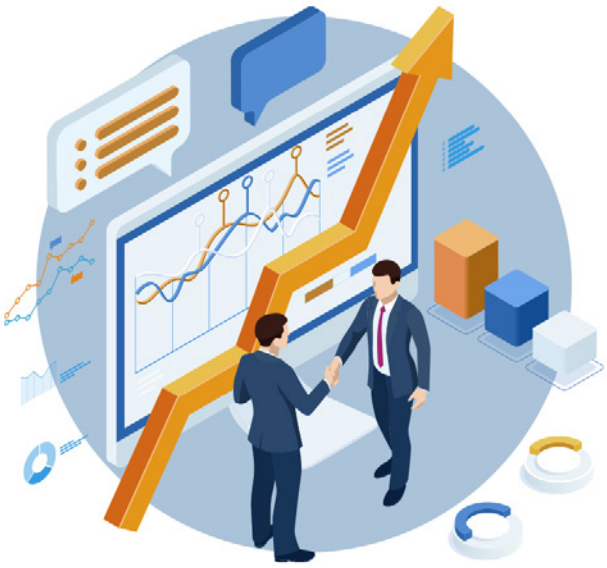
6. In this regard, stakeholders reported that they expect PAIBs to be more involved in broader data governance matters to ensure quality data prior to relying on its use, whether for decision-making or as an input to automation. This is because PAIBs are well-positioned vis-à-vis their professional work for the organizations they support (i.e., internal controls and processes) and their involvement at every stage of the data governance cycle (i.e., from data generation or collection through to its use, transfer, storage, residency, dissemination, and lawful destruction). It is also because it is part of a PA's professional duty as data flows into the preparation and presentation of financial statements.

7. Accordingly, PAs are seen by some stakeholders as being accountable for the quality of such data. For example, some stakeholders indicated that it is critical for PAs to ensure that the data being used is accurate, complete, and reliable, regardless of whether the technology processing and storing such data was developed internally or sourced externally (i.e., hosted by an external cloud service provider or processed by externally developed bots).

8. In addition to data quality issues, the use of data raises potential ethics challenges.[3] For AI to produce the most valuable and accurate insights, training models need "real" data. However, stakeholders have questioned whether the use of actual data for this purpose engages the Code's fundamental principles of integrity and confidentiality. For example, even if a firm or a company obtains the consent of a client or customer to use data collected while performing a professional activity for the purpose of training an AI system under development, is this sufficient to meet the requirements of the Code's fundamental principle of confidentiality? Does this answer change if the data is anonymized first? Would this be considered similar to a request by third parties to use de-identified (i.e., anonymized) client information for purposes of publishing benchmarking data or studies?[4]

9. To meet the expectations for data quality and its use, stakeholders noted that it is important to have a data governance and information stewardship framework in place that ensures, among other outcomes, the accuracy, objectivity, consistency, and completeness of data for use in decision-making and/or sharing with a third-party. When designing such frameworks, for example, as part of considering the appropriateness and effectiveness of internal controls over financial reporting, stakeholders highlighted that PAs should consider the appropriateness of governance around:

- Controls over data integrity, that is, the source of data and whether it has been modified subsequent to its creation, collection, or acquisition.
- Whether the data is representative for the purpose and population it is being used to serve or model.
- Understanding the nature of the data being created, collected, or acquired – including the related implications for compliance with professional obligations and jurisdictional legislation or regulation with respect to confidentiality and privacy.[5] This includes understanding, for example, where the data will reside and how it will be eventually disposed.
- Distinguishing between commercial and personal or individual information that could be potentially sensitive and have differing legal implications, for example, innovative intellectual property or medical information.
- Emerging issues such as the "ownership" of "new" data created from big data mining and applying AI to existing data sets.
- Reasonableness of risk identification procedures pertaining to the data governance cycle, controls to address such risks, documentation requirements, and ongoing management.
- Collateral risk assessments of breaches in confidentiality and privacy that such breaches, or cyber-attacks or ransomware, demand, as well as related contingency plans.



10. Additionally, stakeholders indicated that the ease with which mis- and disinformation is spread is a pervasive issue in society that should be considered as part of data governance and information stewardship.[6] In this regard, the Working Group notes that PAs can think of meeting professional obligations for objectivity, integrity, professional competence and due care, and their public interest responsibilities in the face of bias and mis- and disinformation in terms of four layers: [7]

- Layer 1: Taking care to produce information that is accurate and objective.
- Layer 2: Ensuring that information the PA relies on is reliable.
- Layer 3: Not passing on mis- and disinformation.
- Layer 4: Proactively countering bias and mis- and disinformation.

11. The main challenges that stakeholders reported facing with respect to data governance arise from the volume and quality of data, the number of data privacy policies to be complied with across jurisdictions (e.g., the European Union's General Data Protection Regulation (EU GDPR)), the multitude of communication platforms (i.e. shadow IT platforms[8] such as Slack) and what is being communicated over such platforms (i.e. confidential agreements shared through such platforms due to a lack of related formal guidelines), and cybersecurity risks associated with data transmission and storage.[9]

Cybersecurity

12. Cyberattacks have become an organizational reality and stakeholders observe three frequent targets: (a) financial systems, (b) intellectual property, and (c) intelligence, for example, information and analysis about an organization, individuals, or a jurisdiction.

13. In most cases, security gaps are created by human behavior, for example, an individual unknowingly clicking a malicious weblink or installing an insecure device.[10] Digitalization and remote working are affecting all organizations, increasing the available cyberattack surface area, namely the available points that are exposed for attackers to target.[11] For example, the connection of generally less secure IoT devices within corporate digital ecosystems creates potential gaps in enterprise security.[12] Similarly, increased digitization leads to greater potential for social engineering where inadequately trained employees also have access to increasingly complicated, and interconnected, systems.

14. Stakeholders highlighted that PAs and others in the organization need to work together to ensure data protection, confidentiality and, where relevant, the privacy of organizational data. Despite an exponential increase in cybersecurity risk, stakeholders observed frequent challenges within individual organizations to obtain sufficient investment budget and resources to address such risk, often finding that enhanced mitigations are implemented only after a breach or other failure.[13]

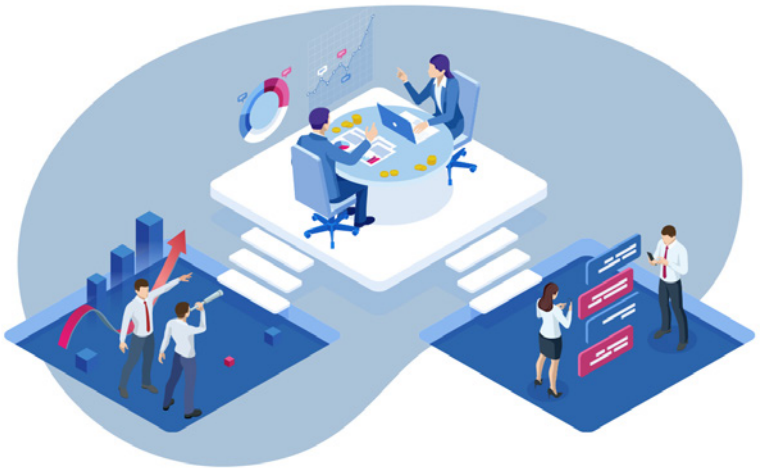
15. Stakeholders indicated that it is crucial for organizations to recognize that, often, customer data are the most valuable assets that organizations can hold, and that although investment in cybersecurity to protect such assets might be costly, the aftermath of a cyber breach is typically an order of magnitude more costly and more challenging to address. It was observed that the biggest advocates of cybersecurity tend to be TCWG, such as audit committees and internal audit groups. Risk committees, where they exist, also help to drive the cybersecurity agenda, but might have challenges with quantifying the likelihood of cyberthreats.

16. Suggestions from stakeholders and through other research about how to be aware, vigilant, and prepared include ensuring a sufficient investment budget and dedicated resources so that:

- An incident responder, who already understands the business, is retained and accessible before an issue happens.
- A cyber-response plan is ready for all types of foreseeable cyberattack possibilities (i.e., the plan should consider the speed of an entity's response to an attack and under what circumstances the entity will, for example, pay ransomware, as well as the related policies and procedures it will follow).[14]
- There is frequent and proactive updating of technology and that a layered approach[15] to cybersecurity is applied.
- There are regular cybersecurity assessments or scans conducted to test for vulnerability.[16] For example, continuous intrusion detection and prevention, regularly inventorying IT assets connected to the organization (including how many digital assets there are, who owns them, and who is accountable for them), and periodic penetration testing to understand what is exposed.
- There is ongoing employee education, such as the incentivization of proactive security behavior ("cyber-vigilance") and establishing a security culture across the organization that includes sufficient access protection and appropriate controls over data and private keys or passwords.[17]

17. With respect to cybersecurity issues and the broader area of data governance, stakeholders emphasized that there are significant expectations and opportunities for PAs to play an active role in overseeing the impacts on their organizations and clients, as part of the PAs' ethical obligation to be competent, exercise due care, and act in the public interest.

18. The Working Group notes that the technology landscape as outlined in this subsection is fast evolving and that PAs should maintain an awareness of the developments in technology,[18] and the related opportunities and impact/risks, so that they can better identify threats to compliance with the fundamental principles of the Code, and accordingly, evaluate and address such threats.



Endnotes

[1] IPA refers to the application of AI (including its sub-fields of computer vision, machine learning, etc.) to RPA.

[2] See, for example:

- Yadav, Praveenkumar. "New Era of Data Science in Today's World." *Data Science*, 4 November 2020, https://data-science-blog.com/blog/2020/11/04/new-era-of-data-science-in-todays-world/.
- "4 Types of Data Analytics and How to Apply Them." *Michigan State University*, 8 October 2019, https://www.michiganstateuniversityonline.com/resources/business-analytics/types-of-data-analytics-and-how-to-apply-them/.

[3] As an example of a tool to help identify and manage ethics issues related to data governance, see "Data Ethics Canvas." *Open Data Institute (ODI)*, 28 June 2021, https://theodi.org/article/the-data-ethics-canvas-2021/#1563365825519-a247d445-ab2d.

[4] In this regard, a stakeholder noted that the AICPA Code paragraph 1.700.060 "Disclosure of Client Information to Third Parties" states that threats to compliance with paragraph 1.700.001 "Confidential Client Information Rule" may exist in cases which may result in the client's information being disclosed to others without the client being specifically identified. Such rule states that PAPPs shall not disclose any confidential client information without the specific consent of the client.

[5] Concerns around data collection and use pertain to both internal and external stakeholders. For example, a 2019 Accenture report notes that "While more than six in 10 C-level executives (62 percent) said that their organizations are using new technologies to collect data on their people and their work to gain more actionable insights — from the quality of work and the way people collaborate to their safety and well-being — fewer than one-third (30 percent) are very confident that they are using the data responsibly." See press release that summarizes the results in "More Responsible Use of Workforce Data Required to Strengthen Employee Trust and Unlock Growth, According to Accenture Report." *Accenture*, 21 January 2019, https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.htm.

[6] A significant example of this issue, albeit within a political advocacy context, is described in James, Letitia. "Fake Comments: How U.S. Companies & Partisans Hack Democracy to Undermine Your Voice." *New York State Office of the Attorney General*, 2021, https://ag.ny.gov/sites/default/files/oag-fakecommentsreport.pdf.

[7] "Identifying and mitigating bias and mis- and disinformation." *CPA Canada, ICAS, IFAC & IESBA*, February 2022, https://www.cpacanada.ca/en/foresight-initiative/trust-and-ethics/%20identifying-mitigating-bias-mis-disinformation.

[8] Shadow IT and IoT – the use of unauthorized applications, clouds, and internet of things devices and networks outside an organization's formal IT enterprise environment

[9] "2021 Conversations With Audit Committee Chairs." *Public Company Accounting Oversight Board (PCAOB)*, March 2022, https://pcaobus.org/documents/2021-conversations-with-audit-committee-chairs-spotlight.pdf.

[10] See, for example, "2022 Data Breach Investigations Report" *Verizon*, 2022, https://www.verizon.com/business/resources/reports/dbir/ that found 86% of breaches involved a human element and Razi, Niloo, and Matt Polak. "The Twitter Hack Shows a Major Cybersecurity Vulnerability: Employees." *Slate*, 21 July 2020, https://slate.com/technology/2020/07/twitter-hack-human-weakness.html.

[11] See, for example, Brandenburg, Rico, and Paul Mee. "Cybersecurity for a Remote Workforce." *MIT Sloan Management Review*, 23 July 2020, https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/; Stupp, Catherine. "As Remote Work Continues, Companies Fret Over How to Monitor Employees' Data Handling." *Wall Street Journal*, 21 August 2020, https://www.wsj.com/articles/as-remote-work-continues-companies-fret-over-how-to-monitor-employees-data-handling-11598002202; and Tung, Liam. "FBI warning: Crooks are using deepfakes to apply for remote tech jobs." *ZDNET*, 29 June 2022, https://www.zdnet.com/article/fbi-warning-crooks-are-are-using-deepfakes-to-apply-for-remote-tech-jobs/.

[12] See, for example, Newman, Lily Han. "100 Million More IoT Devices Are Exposed–And They Won't Be the Last." *Wired*, 13 April 2021, https://www.wired.com/story/namewreck-iot-vulnerabilities-tcpip-millions-devices/.

[13] For thoughts on where executives, such as CFOs, should be evaluating risks and the budget needed to cover them, see Ryan, Vincent. "Budgeting for Cybersecurity Requires a New Approach." *CFO*, 7 September 2021, https://www.cfo.com/budgeting-planning/2021/09/budgeting-for-cybersecurity-requires-a-new-approach/.

[14] For commentary on the ethical and legal implications of paying a ransom to cyberattackers, see Srivastava, Vinita. "Colonial Pipeline forked over $4.4M to end cyberattack–but is paying a ransom ever the ethical thing to do?" *The Conversation*, 26 May 2021, https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383; Lopatto, Elizabeth. "Ransomware funds more ransomware, so how do we stop it?" *Verge*, 24 June 2021, https://www.theverge.com/2021/6/24/22545675/ransomware-cryptocurrency-regulation-hacks; and "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." *US Department of the Treasury*, 21 September 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[15] Layered security is a security approach that deploys multiple layers of security control that back one another up in the event one is breached or fails, for example, employing effective network, system, application, human, and physical elements as part of a complete defense strategy. This is particularly important when protecting the most critical data and information within an organization's technology environment.

[16] Additional ideas are contained, for example, in "CSET Ransomware Readiness Assessment." *Cybersecurity & Infrastructure Security Agency*. 30 June 2021, https://www.cisa.gov/uscert/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat.

[17] This might include, for example, "common sense" security procedures for individuals to follow, such as multi-factor authentication (MFA) when accessing data or systems.

[18] Paragraph 113.1 A2 of the Code

ABOUT THE IESBA

The International Ethics Standards Board for Accountants (IESBA) is an independent global standard-setting board. The IESBA serves the public interest by setting ethics standards, including auditor independence requirements, which seek to raise the bar for ethical conduct and practice for all professional accountants through a robust, globally operable International *Code of Ethics for Professional Accountants (including International Independence Standards)*.

The IESBA believes a single set of high-quality ethics standards enhances the quality and consistency of services provided by professional accountants, thus contributing to public trust and confidence in the accountancy profession. The IESBA sets its standards in the public interest with advice from the IESBA Consultative Advisory Group (CAG) and under the oversight of the Public Interest Oversight Board (PIOB).

KEY CONTACTS

Brian Friedrich, IESBA Member and Chair of the Technology Working Group (brian@friedrich.ca)

Ken Siong, Program and Senior Director, IESBA (kensiong@ethicsboard.org)

Kam Leung, Principal, IESBA (kamleung@ethicsboard.org)

IESBA International Ethics Standards Board for Accountants®

www.ethicsboard.org @ethics_board company/iesba

Published by International Federation of Accountants (IFAC), 529 Fifth Avenue, New York, NY 10017