Toward Rebuilding Data Trust

日本語版も入手可能
www.isaca.org/currentissue

External auditors should be trusted members of the business community. They analyze structured data (e.g., log files, transaction records) and unstructured data (e.g., interview responses and reports) to draw conclusions about the veracity of an enterprise's systems and controls for cybersecurity, compliance and quality, and finance. Ultimately, they provide assurance—to the public, in some cases—that an enterprise is well managed.

However, some of the world's biggest audit firms are struggling with their most important obligation: to be a trusted source of independent information about the state of an enterprise. The Enron and WorldCom scandals have not been forgotten, and there has been a series of more recent high-profile events: One of the world's largest audit firms is being sued for US$830 million and has been charged with misconduct,[1, 2] and two other leading audit firms have been caught cheating.[3, 4]

As audits become more data-driven, audit firms can be exposed to risk if the client enterprise fails to adhere to good data management practices. A key question for the data-driven auditor is how to assess the reliability (e.g., accuracy, completeness) of the data captured by a client's system and the methods of data acquisition used by that system.[5] This question applies not only to auditors, but also to banks, insurers, securities traders, retailers, telecommunications organizations and even social media enterprises—all entities that people trust with their data.

The data trust domain is vast (**figure 1**), even as a subset of the immense digital trust domain. Poor data management in general, and poor data quality in particular, can have negative impacts on data trust and, thus, on digital trust. But there are steps enterprises can take to improve their overall levels of trust based on the data management discipline and the principles of trustworthiness.

The Poor State of Organizational Trust

The world is becoming less trusting partly because of failures related to poor data management. The Facebook-Cambridge Analytica scandal is a case in point, specifically from a privacy perspective.[6] Businesses are actually the most trusted organizational type—more trusted than nongovernmental organizations (NGOs), governments and media.[7] However, there is a global trust crisis in business, with two thirds of senior executives believing that trust between people and the enterprises and institutions they deal with is declining because of enterprise data misuse, corporate scandals and misrepresentations of the truth.[8]

This is not a recent phenomenon. Trust in the US government has been declining for 70 years.[9] Trust has simultaneously been declining in business enterprises, media and NGOs since 2017, with the average level of trust across dozens of countries in all four organizational categories combined being less than 50 percent.[10]

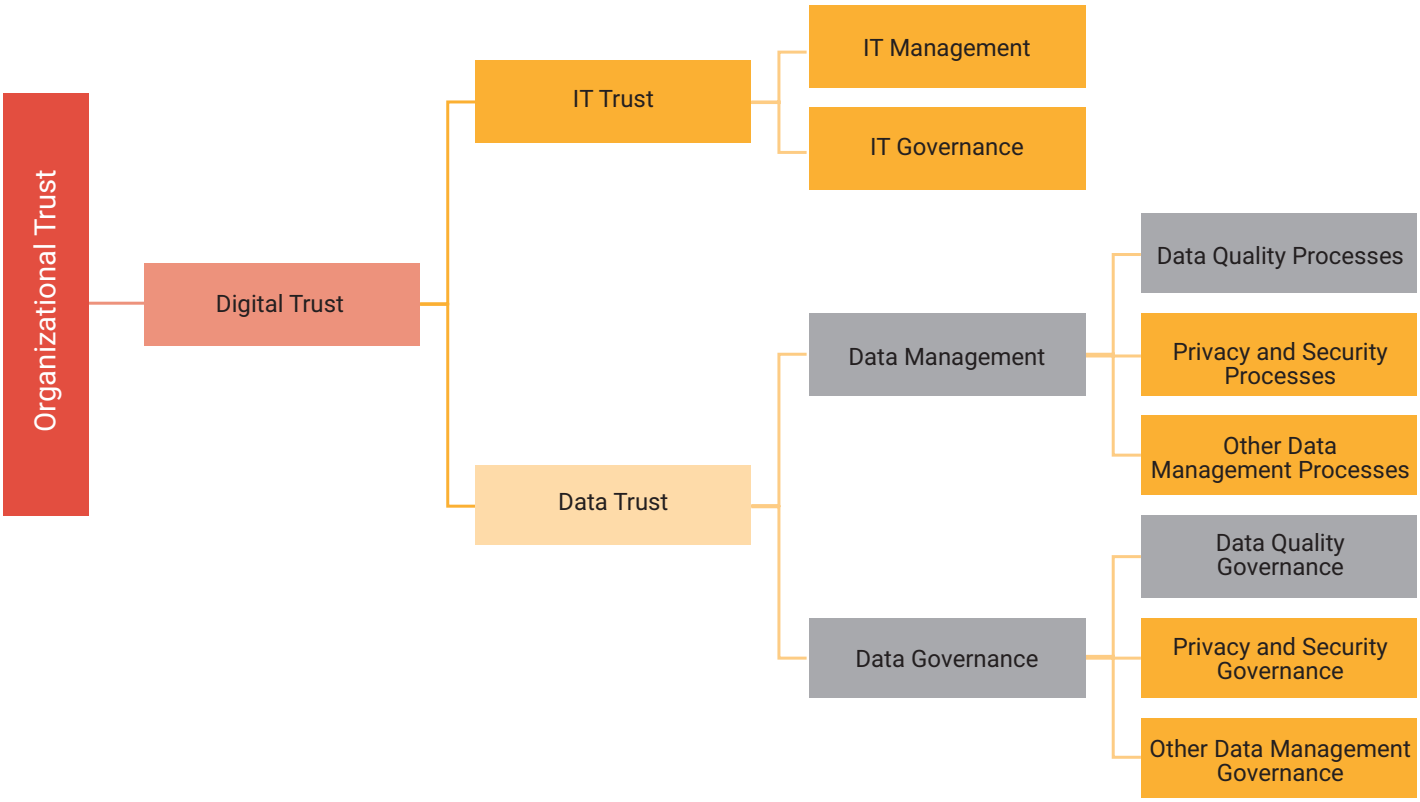
The Poor State of Data Trust

When discussing data trust in a digital trust context, a useful analogy is that data are like water and IT is like plumbing. Data trust is like trusting that the water is

GUY PEARCE | CGEIT, CDPSE

Has an academic background in computer science and commerce and has served in strategic leadership and governance capacities mainly in the services sector; IT governance; and enterprise governance capacities, mainly in financial services. He is a career-long digital innovator balancing the creation of two-way value—customer and organization—while ensuring the effective integration of emerging technology and its beneficial adoption. He has been active in digital transformation since 1999, focusing on the people and process integration of emerging technology into organizations to ensure effective adoption. Pearce was first exposed to artificial intelligence (AI) in 1989, and he has followed the evolution of the discipline from symbolic AI to statistical AI during the intervening decades. He was awarded the 2019 ISACA® Michael Cangemi Best Author award for contributions to IT governance, and he consults in sustainable IT architectures and the respectful, compliant use of data bounded by sound governance, digital transformation, data governance and IT governance.

FIGURE 1
Data Trust Domain



potable, and IT trust is like trusting that the plumbing functions properly. Just as water cannot flow or be stored without the right plumbing, data cannot flow or be stored without IT. Digital trust is about trusting the entire data and IT ecosystem.

Whereas "digital trust focuses on how trust manifests in a digital context,"[11] data trust is exclusively about the data context of the digital ecosystem, including, but not limited to, the data components of privacy and security. Data trust includes data management aspects such as data quality, metadata management, master and reference data management, content management (unstructured data) and data consumption mechanisms (e.g., reporting, analytics, artificial intelligence [AI]). Specifically, data trust means that data management activities produce verifiably healthy data.

More than three quarters of consumers say that sharing data with enterprises is a necessary evil.[12] Worse, 78 percent of consumers say their trust in an enterprise's ability to protect their data has stayed the same or declined over the past two years.[13] Worst of all is that 55 percent of enterprises believe that consumers' trust has increased over the same period.[14] There is clearly significant dissonance between enterprises and their customers when it comes to data trust.

The use of third-party personal data—when an enterprise buys personal data from another enterprise to augment its own data on individuals—has been identified as a major cause of declining trust.[15] It can lead to inaccurate representations of customers because of inaccurate data and the guesswork involved in merging data and possibly not following regulations. In addition, the purchase, processing and use of the integrated data are not transparent to the end user, and transparency is a requirement for building (or rebuilding) organizational trust.[16]

However, it is important to note that trusted enterprises do not need transparency.[17] Rather, distrusted enterprises need transparency to recover from distrust. The current president of the European Central Bank and former chair and managing director of the International Monetary Fund reinforced this sentiment by saying, "In my experience, the best tonic for depleted trust is heightened transparency."[18] In other words, transparency is needed where trust has been eroded, not where trust is intact. For example, the medical profession is considered a bastion of trust, so

one trusts a physician's opinion without demanding transparency about how that opinion was reached.

But data trust involves more than transparency; it also includes value delivery and acceptance of consequences—that is, the trust a person places in an enterprise's data practices.[19] Consequence acceptance is a major element of data governance through an enterprise's culture and its management structures, specifically insofar as they relate to accountability and responsibility.

LOOKING FOR MORE?

- Read *Defending Data Smartly*. *www.isaca.org/defending-data-smartly*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

There are many critical attributes for effective data management that are missing in enterprises that are struggling with data management initiatives.

Data trust requires healthy data, and healthy data are clean, appropriately accessible, understandable, up-to-date and traceable.[20] Each of these criteria is a subset of effective data management. In other words, well-managed data drive data trust; unhealthy data—that is, data with lower than desired levels of quality because of poor data management—cause low levels of data trust.

The Poor State of Data Management

In general, data management details the tasks and activities required for a healthy data environment, while data governance defines accountability and responsibility for those tasks and activities based on a defined policy and, generally, with respect to defined processes. Both elements are in response to a data strategy aligned with an enterprise's overall strategy.

The Capability Maturity Model Institute (CMMI) found that ineffective data management negatively impacted 100 percent of the technology failures it surveyed, and technology initiatives experienced a 50 percent failure rate.[21] An academic study of the factors causing the failure of AI projects found that earlier studies cited data management issues as a significant factor.[22]

Although these findings are indicative of failure on the process side of data management, failure is also happening from a people and governance perspective. For example, the 2010 promise of big data being key to competition remains unfulfilled because enterprise leaders still have not recognized that data are important to everyone, not just a few data-oriented managers.[23] A decade later, the tide may finally be turning, with a renewed focus on self-service business intelligence and data democratization—making data accessible to all, "irrespective of their technical know-how"[24] and giving them appropriate permissions—increasingly enabled by metadata-driven data fabric platforms and the domain-led data products of data mesh architectures.

The overall result of these failures is that 90 percent of data governance projects fail to perform well.[25]

There are many critical attributes for effective data management that are missing in enterprises that are struggling with data management initiatives, including:[26, 27, 28]

- Senior executive sponsorship
- Clear objectives linked to measurable organizational value; half of all enterprises do not assess, monitor or measure their data governance initiatives[29]
- Integrated data strategy with a shared language and consistent expectations shared by all relevant stakeholders
- Focus and commitment; that is, attention to the meaningful rather than the menial
- Manageable scope driven by prioritization
- Defined operational accountabilities and responsibilities and shared responsibility for operational success

- Data governance and data management expertise
- Recognition that data management is an ongoing operational responsibility, not just a project
- Balanced rather than overt focus on tools and technology
- Focus on communication, transformation and change management from the start

Many of these attributes are related to data governance. For example, the UK government's coronavirus data were flawed and misleading, negatively impacting public understanding and government decision-making.[30] One of the problems was termed a technical glitch that led to thousands of positive results being omitted from the calculation of national coronavirus cases. The glitch was said to be "a data file exceeding its maximum file transfer size."[31] There were other issues as well, such as inflated figures that necessitated recalculation.

Given this assessment, it seems that some of the data governance questions not asked or answered may include:

- Who was responsible for validating the file transfer?
- Was there a process in place for that person to follow with respect to file identification and data transport validation? If so, was the process approved?
- Was the process for calculation validated by the identified stakeholders?
- Were there clear and agreed-on definitions for variables such as dates (e.g., day of report vs. day of death) and when data were to be captured, including accommodation for weekends? If so, were the definitions approved?
- How were data inputs and data outcomes approved? Attestation or certification? (Presenting data without supporting information means that interpretation is left to the observer.)

Even if data management (the process) is sound, failures in data governance (accountability and validation) can mean that all data-reliant efforts come to naught. Data management and data governance need to function in tandem for data to be sustainably fit for purpose.

Even if data management (the process) is sound, failures in data governance (accountability and validation) can mean that all data-reliant efforts come to naught.

The Poor State of Data Quality

Given the poor state of data trust and data management, it should be no surprise that data are unhealthy. Poor data quality cost the US economy US$3 trillion in 2016, a cost driven by decision makers, managers, knowledge workers and data scientists having to accommodate unhealthy data in their everyday work.[32] The accommodation of unhealthy data by these individuals includes understanding, correcting and preparing the data to make them usable for their intended purpose.

Assuming that the causes of dirty data (a subset of unhealthy data) are similar in all large developed economies, the cost of dirty data for all countries in 2016 can be estimated as:

$$\text{Estimated Cost of Dirty Data}_{\text{In 2016}} = \frac{\text{Country}_{\text{GDP In 2016}}}{\text{US}_{\text{GDP In 2016}}} * \text{US\$3 trillion}$$

The gross domestic product (GDP) of the United States (the total economic value produced) in 2016 was US$18.7 trillion.[33] Using this equation, the cost of dirty data for other major economies can be estimated (column B in **figure 2**). Large economies such as Brazil and China were excluded from this analysis because comparable data were not available from the sources used and because of their developing economic status.[34]

Next, it is possible to determine the impact of poor data quality on employees—that is, the extra work they must perform to clean and prepare data for use. Based on the number of economically active people in each country (column C in **figure 2**), the average cost of dirty data per employee can be calculated (column D in **figure 2**). Note that because the data for **figure 2** were collected in different years, this introduces a timing error into the estimate. Based on the average wage per employee (column E in **figure 2**),

FIGURE 2

Time Spent Cleaning Dirty Data per Employee in Selected Large Economies

Country	A	B (from the equation)	C	D = B/C	E	F = D/E
	GDP (in US$ Trillions, 2016)[a]	Calculated Annual Cost of Dirty Data in US$ Billions (2016)	Number of Employees in Millions (2021–22)[b]	Calculated Cost of Dirty Data per Employee per Year in US$ Thousands	Average Wage per Employee in US$ Thousands (2020)[c]	Calculated Average Percent of Time Fixing Data per Employee
United States	$18.7[d]	3,000[e]	158.1	19.0	69.4	27 percent
Japan	$4.9	786	67.2	11.7	38.5	30 percent
Germany	$3.5	561	45.4	12.4	53.7	23 percent
United Kingdom	$2.6	417	32.7	12.8	47.1	27 percent
France	$2.5	401	29.0	13.8	45.6	30 percent
Italy	$1.8	289	23.0	12.6	37.8	33 percent
Canada	$1.5	241	19.6	12.3	55.3	22 percent

Sources: a) World Bank, "GDP Current US$," *https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?order=wbapi_data_value_2010+wbapi_data_value+wbapi_data_value-last&sort=desc*; b) SME Finance Forum, "MSME Economic Indicators," *https://smefinanceforum.org/data-sites/msme-country-indicators*; c) OECD Stat, "Average Annual Wages," *https://stats.oecd.org/Index.aspx?DataSetCode=AV_AN_WAGE*; d) Countryeconomy.com, "United States (USA) GDP—Gross Domestic Product," 2016, *https://countryeconomy.com/gdp/usa?year=2016*; e) Redman, T. C.; "Bad Data Costs the U.S. $3 Trillion Per Year," *Harvard Business Review*, 22 September 2016, *https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year*

the average percentage of time each employee spends on data quality issues can be calculated (column F in **figure 2**). Some jobs involve more work with data than others, but the average provides an estimate of the extent of the problem at the per-person level.

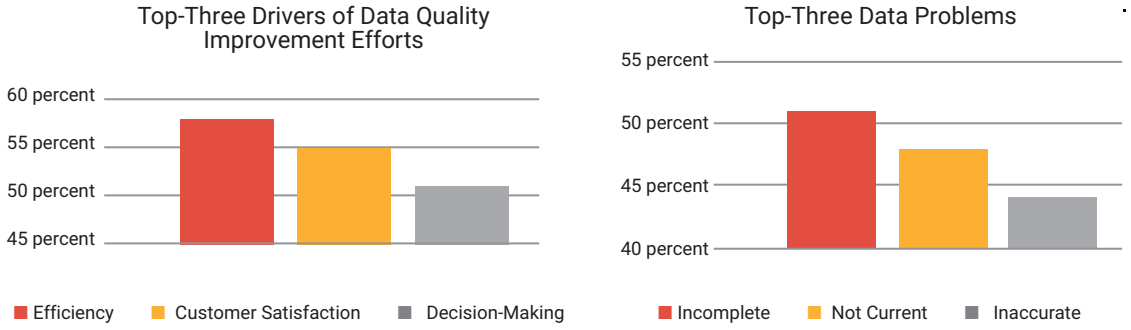
This means that between one quarter and one third of the average employee's time is spent accommodating the vagaries of dirty organizational data—that is, up to one third of every day, week, month and year that could be better spent adding value to the enterprise's customers. The cost of dirty data is approximately 15- to 25-percent of revenue for most enterprises.[35] Reputational risk is often cited as a risk of dirty data,[36] and dirty data have damaged the reputations of 21 percent of enterprises.[37]

What initiatives are driving data quality improvement efforts, and what major problems are they attempting to solve? Fifty-eight percent of enterprises cite greater efficiency as a primary reason to improve data quality; 55 percent cite enhanced customer satisfaction; and 51 percent cite informed decision-making (**figure 3**).[38] Furthermore, enterprises struggle with data that are incomplete (51 percent), out of date (48 percent) or inaccurate (44 percent).[39]

The fact that the cost of poor data management can be quantified (in a top-down manner using enterprise-specific data, as shown in **figure 2**, but potentially in a bottom-up manner as well) means that making a business case for improving data quality is a good place to start. This should involve quantifying the benefits of addressing the issues.

FIGURE 3

Top-Three Data Problems and Reasons to Improve Data Quality



Restoring Data Trust: Where to Start

Poor data quality can compromise organizational economics, operations and customer trust. It can also be a powerful trust builder with the potential to increase trust in business by 3 percent and trust in government by 6.1 percent.[40] There is also a strong argument that better quality data can help close the income divide.[41]

Forty-two percent of respondents to one survey said that organizations are not doing enough to ensure trustworthy information.[42] By addressing data quality, a major part of that trust problem can be resolved.

There are several steps an enterprise can take to rebuild data trust:[43]

- Clean and validate data (data quality).
- Add operational metadata (data management).
- Secure private and sensitive data.
- Ensure data traceability (i.e., lineage and provenance; another aspect of data management).
- Ensure visibility and control of data management processes (transparency).

Increasing data trustworthiness depends on data that are:[44]

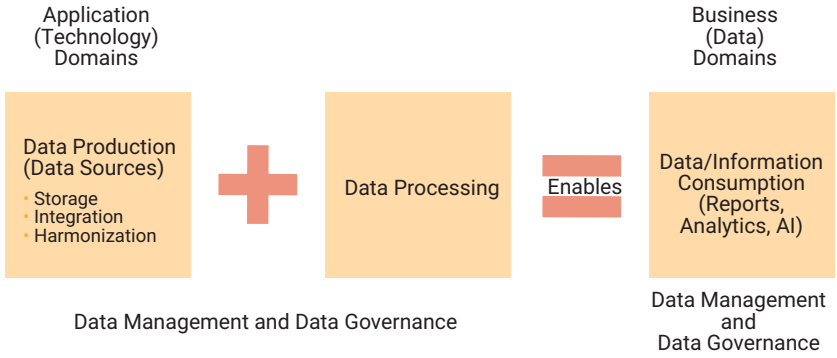
- **Transparent**—Verifiably clean and compliant
- **Thorough**—Providing a complete picture of the relevant domain
- **Trending**—A measurement of data consumption
- **Telling**—Verified and tested

Quality, transparency, traceability and verifiability are recommended points of focus for rebuilding data trust by means of a revised data management program. Thoroughness is an interesting consideration because it entails the best single view of the customer. Measuring data consumption is one of the greatest indicators of success. If nobody is using the platform, the reason is probably a lack of trust.

Many different stakeholders have roles to play in effective data governance, including those involved in data consumption (business) and data production (IT), because fit-for-purpose data are not just an IT function (**figure 4**). Indeed, data owner and data steward are both recognized data management roles. In addition, data consumers' participation in managing the problem fosters greater engagement and buy-in, which promotes trust and legitimacy.[45]

FIGURE 4

Data Production (Sources) vs. Data Consumption (Users)



In analytics, data trust is defined by four trust pillars: data quality, effectiveness of the analytics, integrity of data use (akin to data consumption) and resilience, which is concerned with long-term sustainability, optimization, governance and security.[46] In particular:

> *[R]esilience is key to winning customer trust. It only takes one service outage or one data leak for consumers to quickly move to (what they perceive to be) a more secure competitor.*[47]

Quality, transparency, traceability and verifiability are recommended points of focus for rebuilding data trust by means of a revised data management program.

Data resilience—which involves well-governed data management—is the cornerstone of digital resilience.[48] Data are in constant flux, which means that active risk management by means of appropriate controls is part of a full-fledged approach to data resilience.[49] Data and analytics are constantly evolving and, over time, there can be shifts in the way they are used, their impact and the risk they create.[50] These shifts can impact the data resilience of the enterprise. If they are not monitored, there can be serious negative repercussions.

Privacy and security are just two dimensions of data management; they should not be considered in isolation from the many other elements inherent in the management of data.

In terms of the interoperability of data resilience, it is important that enterprises ensure that their data operations are visible, which is part of trust building. Visibility facilitates identification of the interdependencies and interrelated risk factors across the entire data ecosystem.[51]

In terms of the robustness of data resilience, only 52 percent of 165 data and analytics decision makers surveyed indicated that data could be changed only by those authorized to do so.[52] The others indicated that anyone could change data. It is no wonder that data trust is in such a poor state.

From Third-Party Data to First-Party and Zero-Party Data

One of the challenges in building data trust is breaking the reliance on third-party data supply chains and ecosystems.[53] To limit liability, rebuild customer trust and create more accurate personalization, enterprises need to move away from the use of third-party data.[54] First-party data are the data an enterprise collects on individuals during the usual course of doing business, and zero-party data are data that customers willingly submit, such as by answering surveys.[55]

Growing regulatory pressure may reduce the market for third-party data and reverse the trend of negative experiences individuals have had over the years as a consequence of their use.

Data Trusts and Personal Data Stores

Lack of user, customer or citizen control over personal data in organizational hands fuels distrust.[56] Lack of control (e.g., data on Facebook, Google) leads to the wider problem of decreasing trust in government, institutions and other enterprises.[57] Data trusts and personal data stores (PDSs) are two of the most popular alternative data management models that support enhanced controls, with PDSs supporting enhanced user control.

Based on legal trusts, data trusts are structures that provide independent stewardship of data for an agreed-on purpose.[58] This is not a new concept, and much has been written about the subject. However, a public survey in the United Kingdom indicated that personal control, regulatory oversight and opt-out options were all preferable to data trusts.[59]

The preference for personal control brings PDSs to the forefront of the data management conversation. PDSs store an individual's data, and third parties have access only when the individual provides it. Blockchain-based personal identity products support PDSs. In one survey, PDSs were deemed preferable to six other data management models, with current data management methods scoring the lowest.[60]

Conclusion

Trust in businesses, governments, media and institutions has been declining for years, and trust in their abilities to manage and appropriately use customer data is following that downward trend. Furthermore, there is significant evidence that traditional data management is failing. A major part of this evidence is the poor state of data quality. Combined, these factors have negatively affected data trust, digital trust and overall organizational trust.

Data governance and data management are linked, yet privacy and security are considered mainly from a data management perspective. Missing is an active discussion about their governance, not only with respect to compliance, but also considering metrics such as trust, which are driven by defined responsibilities and accountabilities. Furthermore, privacy and security are just two dimensions of data management; they should not be considered in isolation from the many other elements inherent in the management of data.

To address issues of data trust, digital trust and, ultimately, enhanced organizational trust, the first step is to focus on a subset of data management—specifically, data quality and metadata—in addition to privacy and security. Other important aspects are certification, attestation and increased visibility of the various data management processes. One measure of success would be increased data consumption.

In the information age, good organizational trust depends on good digital trust, and good digital trust depends on enhanced trust not only in the enterprise's IT, but also in its data. From a data perspective, data trust is forged by paying attention to privacy and security, data quality and metadata, and by exhibiting the ability to certify data and information as being fit for purpose.

Endnotes

1 Kinder, T.; "KPMG Sued for $830mn Over 'Appalling' Chinese Audit," *Financial Times*, 5 September 2022, *https://www.ft.com/content/07af027a-a1ed-4847-bcfc-263ce9b48a03*

2 O'Dwyer, M.; "KPMG Hit With Half of UK Accounting Fines as Penalties Reach New Record," *Financial Times*, 28 July 2022, *https://www.ft.com/content/73e48574-673a-4725-9b78-ba940a8060f5*

3 US Securities and Exchange Commission, "Ernst & Young to Pay $100 Million Penalty for Employees Cheating on CPA Ethics Exams and Misleading Investigation," 28 June 2022, *https://www.sec.gov/news/press-release/2022-114*

4 Ellis, C.; "PwC Canada Fined Over One Million CDN by US, Canadian Regulators," *Canadian Accountant*, 1 March 2022, *www.canadian-accountant.com/content/profession/pwc-canada-fined-by-us-canadian-regulators*

5 Chartered Professional Accountants (CPA) Canada and American Institute of Certified Public Accountants (AICPA), *The Data-Driven Audit: How Automation and AI Are Changing the Audit and the Role of the Auditor*, Canada, 2020, *https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/the-data-driven-audit.pdf*

6 Wong, J.C.; "The Cambridge Analytica Scandal Changed the World—But It Didn't Change Facebook," *The Guardian*, 18 March 2019, *https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook*

7 Edelman, *Edelman Trust Barometer 2022*, USA, 2022, *https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20Global%20Report_Final.pdf*

8 Michels, D.; "The Trust Crisis in Business," Forbes, 17 June 2019, *https://www.forbes.com/sites/davidmichels/2019/06/17/the-trust-crisis-in-business/?sh=5418ceef44a6*

9 Vavreck, L.; "The Long Decline of Trust in Government, and Why That Can Be Patriotic," *The New York Times*, 3 July 2015, *https://www.nytimes.com/2015/07/04/upshot/the-long-decline-of-trust-in-government-and-why-that-can-be-patriotic.html*

10 Harrington, M.; "Survey: People's Trust Has Declined in Business, Media, Government, and NGOs," *Harvard Business Review*, 16 January 2017, *https://hbr.org/2017/01/survey-peoples-trust-has-declined-in-business-media-government-and-ngos*

11 ISACA®, *Digital Trust: A Modern-Day Imperative*, USA, 2022, *www.isaca.org/digital-trust-modern-day-imperative*

12 PricewaterhouseCoopers (PwC), "In Data We Trust: Living Up to the Credo of the 21st Century," *https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/defining-data-trust-strategy.html*

13 *Ibid*.

14 *Ibid*.

15 Bianchi, T.; "First-Party Data Key to Rebuilding Trust in Online Platforms," *AI Magazine*, 23 July 2022, *https://aimagazine.com/data-and-analytics/first-party-data-key-to-rebuilding-trust-in-online-platforms*

16 Morey, T.; T. Forbath; A. Schoop; "Customer Data: Designing for Transparency and Trust," *Harvard Business Review*, May 2015, *https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust*

17 Harrington, S.; "You Can't Build Trust Through Transparency," The People Space, 14 November 2018, *https://www.thepeoplespace.com/ideas/articles/you-cant-build-trust-through-transparency*

18 Lagarde, C.; "There's a Reason for the Lack of Trust in Government and Business: Corruption," *The Guardian*, 4 May 2018, *https://www.theguardian.com/commentisfree/2018/may/04/lack-trust-government-business-corruption-christine-lagarde-imf*

19 Kinch, N.; "Data Trust, by Design: Principles, Patterns and Best Practices (Part 1)," *Medium*, 22 February 2018, *https://medium.com/greater-than-experience-design/data-trust-by-design-principles-patterns-and-best-practices-part-1-defffaac014b*

20 Talend, "What Is Data Trust?" *https://www.talend.com/resources/what-is-data-trust/*

21 Mohrmann, R.; "Most Technology Projects Fail. What Is Your Data Management Plan?" Datafloq, 23 February 2018, h*ttps://datafloq.com/read/technology-projects-fail-data-management-plan/*

22 Westenberger, J.; K. Schuler; D. Schlegel; "Failure of AI Projects: Understanding the Critical Factors," *Procedia Computer Science*, vol. 196, 2022, p. 69–76, *https://www.sciencedirect.com/science/article/pii/S1877050921022134/pdf?md5=2846ce14f794d777a06b39fdcb82781d&pid=1-s2.0-S1877050921022134-main.pdf*

23 Bean, R.; "The 'Failure' of Big Data," *Forbes*, 20 October 2020, *https://www.forbes.com/sites/randybean/2020/10/20/the-failure-of-big-data*

24 Choudhury, A.; "What Is Data Democratization? Definition and Principles," *Amplitude Blog*, 27 January 2022, *https://amplitude.com/*

blog/data-democratization#:~:text=Data%20democratization%20is%20the%20ongoing,customer%20experiences%20powered%20by%20data
25 Zentao, "Reasons for Data Governance Project Failure," 13 July 2022, *https://www.zentao.pm/blog/reasons-for-data-governance-project-failure-1268.html*
26 *Ibid*.
27 Schmidbauer, S.; "Five Reasons Your Data Governance Initiative Could Fail," Stibo Systems, 24 January 2022, *https://www.stibosystems.com/blog/five-reasons-your-data-governance-initiative-could-fail*
28 Bradshaw, A.; "Why Your Data Governance Strategy Is Failing," Alation, 5 October 2021, *https://www.alation.com/blog/data-governance-strategy-failing/*
29 *Ibid*.
30 Mathieson, S. A.; "UK Government Coronavirus Data Flawed and Misleading," *ComputerWeekly*, 6 October 2020, *https://www.computerweekly.com/feature/UK-government-coronavirus-data-flawed-and-misleading*
31 *Ibid*.
32 Redman, T. C.; "Bad Data Costs the U.S. $3 Trillion Per Year," *Harvard Business Review*, 22 September 2016, *https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year*
33 Countryeconomy, "United States (USA) GDP—Gross Domestic Product," 2016, *https://countryeconomy.com/gdp/usa?year=2016*
34 Worlddata, "Developing Countries," *https://www.worlddata.info/developing-countries.php*
35 Grensquared, "Top 5 Data and Analytics Challenges and How to Conquer Them," 28 March 2022, *https://www.gensquared.com/5-challenges-business-and-it-leaders-face-when-launching-data-analytics-projects/*
36 Pearce, G.; "Quantifying the Impact of Data Projects," The Data Administration Newsletter (TDAN), 5 July 2017, *https://tdan.com/quantifying-the-impact-of-data-projects/21760*
37 RingLead, "The Cost of Dirty Data," *https://www.ringlead.com/blog/the-cost-of-dirty-data*
38 Brooke, C.; "What Is Poor Data Quality Costing You?" Business 2 Community, 9 May 2016, *https://www.business2community.com/marketing/poor-data-quality-costing-01539520*
39 *Ibid*.
40 *Op cit* Edelman
41 *Ibid*.
42 *Ibid*.
43 Bluemetrix, "Five Ways to Build Trust in Data, While Improving Access to Data," *https://www.bluemetrix.com/post/5-ways-to-build-trust-in-data-while-improving-access-to-data*
44 Talend, "Five Principles for Increasing the Trustworthiness of Your Company's Data," *Harvard Business Review*, 30 July 2020, *https://hbr.org/sponsored/2020/07/5-principles-for-increasing-the-trustworthiness-of-your-companys-data*
45 Barzelay, A.; M. Veerappan; M. Lucey; "Promoting Trust in Data Through Multistakeholder Data Governance," World Bank Blogs, 13 December 2021, *https://blogs.worldbank.org/opendata/promoting-trust-data-through-multistakeholder-data-governance*
46 KPMG, "Building Trust in Analytics," Netherlands, 2016, *https://assets.kpmg/content/dam/kpmg/xx/pdf/2016/10/building-trust-in-analytics.pdf*
47 *Ibid*.
48 Pearce, G.; "Data Resilience Is the Cornerstone of Digital Resilience," ISACA Now, 27 July 2022, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/data-resilience-is-the-cornerstone-of-digital-resilience*
49 Pearce, G.; "Real-World Data Resilience Demands an Integrated Approach to AI, Data Governance and the Cloud," *ISACA® Journal*, vol. 3, 2022, *https://www.isaca.org/archives*
50 *Op cit* KPMG
51 *Ibid*.
52 *Ibid*.
53 PricewaterhouseCoopers (PwC), "Data Trust," *https://www.pwc.com/ca/en/services/consulting/cybersecurity-privacy/data-trust.html*
54 *Op cit* Bianchi
55 *Ibid*.
56 Nesta, "The New Ecosystem of Trust," *https://media.nesta.org.uk/documents/nesta.org.uk-The_new_ecosystem_of_trust_-_printable.pdf*
57 *Ibid*.
58 Hartman, T.; H. Kennedy; R. Steedman; R. Jones; "Public Perceptions of Good Data Management: Findings From a UK-Based Survey," *Big Data and Society*, January–June 2020, *https://journals.sagepub.com/doi/pdf/10.1177/2053951720935616*
59 *Ibid*.
60 *Ibid*.