Cataloguing the Marketplace of Assurance Service Areas

Tim Bauer
University of Waterloo
tdbauer@uwaterloo.ca

Efrim Boritz
University of Waterloo
jeboritz@uwaterloo.ca

Alec Cram
University of Waterloo
wacram@uwaterloo.ca

Krista Fiolleau
University of Waterloo
krista.fiolleau@uwaterloo.ca

Bradley Pomeroy
University of Waterloo
bpomeroy@uwaterloo.ca

Adam Vitalis
University of Waterloo
avitalis@uwaterloo.ca

Pei Wang
University of Waterloo
p252wang@uwaterloo.ca

September 30, 2021

We acknowledge the support of CPA Canada and the University of Waterloo Centre for Information Integrity and Information Systems Assurance ("UWCISA"). We thank Basil Abo Alya, Khadeeja Arif, Ji Woo Choi, Christine Jing, and Alice Wang and Shumiao Wang for their research assistance. We benefitted from comments provided by Rosemary McGuire, Yasmine Hakimpour, and Taryn Abate of CPA Canada and Antonio Pecora of the Canadian Public Accountability Board (CPAB).

Cataloguing the Marketplace of New Assurance Service Areas

ABSTRACT

We report findings from an extensive search of web-based information to catalogue the marketplace of assurance service areas beyond financial statements audits. We identify 33 new service areas sorted into two broad categories: technology-related and technology-neutral service areas. We also document some of the key contextual features of each service area and offer some observations based on what we learned from the cataloguing exercise. The paper serves as a resource for researchers interested in conducting research on new assurance service areas.

Keywords: auditing; assurance; new service areas; technology; web search

I. INTRODUCTION

The marketplace for assurance beyond financial statement audits is a topic of importance to accounting firms as many new service areas emerge in response to technology changes (CPA Canada 2018). It is also a topic of interest to researchers seeking to understand the development and contextual features of new service areas like sustainability reporting assurance (O'Dwyer 2011; O'Dwyer, Owen, and Unerman 2011; Cohen and Simnett 2015). However, the audit literature has provided little insight on many other new service areas, particularly those relating to technology like artificial intelligence, blockchain, and cloud computing. This paper documents the process we followed to catalogue 33 new service areas and reports our observations from the exercise. By doing so, the paper serves as a resource for researchers to consult as they seek opportunities for launching studies that advance the literature on new service areas.

A line of research on assurance services investigates how accounting firms expand into new service areas and the outcomes of doing so. Such studies highlight that firms cannot always replicate their success in the financial statement audit context to these new service areas (Gendron and Barrett 2004) and that successful expansion into new areas is context dependent (Andon et al. 2015). For example, an assurance provider's independence will not necessarily be valued as highly in a new service area as it is in the financial statement audit context (Jamal and

Sunder 2011). While the literature provides insights into the contextual features of many new service areas (see Andon et al. 2015 for a review), much is left undone because it is difficult for researchers to keep track of the abundance of new areas opening in response to change – like in technology (CPA Canada 2018). This paper contributes to the literature by conducting an extensive web search to identify new service areas, many of which have not yet been examined by audit researchers. We also document some key contextual features of these service areas.

Our study was prompted by CPA Canada's "Foresight" initiative, the purpose of which is to help determine a new strategic direction for the Canadian accounting profession (CPA Canada 2018). We responded to CPA Canada's call for research proposals, which focused on reviewing technology-related assurance solutions offered by accounting firms and non-accounting firms. Our proposal was selected for funding and we agreed to prepare a database of service areas and to produce a report. To prepare the database, we conducted an extensive internet search focused on accounting firm websites, as well as many other websites, identified through Google searches using a variety of assurance-related search terms. We then categorized the service areas identified from our search into two broad categories: technology-related and technology-neutral. Technology-related service areas focus on technology-based systems and processes or require the use of technology in the service delivery process (e.g., System and Organization Controls (SOC) reporting services), whereas technology-neutral service areas do not necessarily focus on technology systems or the use of technology (e.g., valuation services).

The output of our search was a worksheet with a row for each service area we identified and multiple columns that summarize what we learned about each area. Later, we took the data contained in the worksheet to produce summary sheets (i.e., Word documents) that describe the services offered in each area, its key contextual factors, and our observations. We identified a

total of 33 service areas, including 20 (13) that are technology-related (technology-neutral), with a brief description of each of these service areas provided in Appendix 1 (2).

In addition to identifying new service areas for researchers to investigate in future studies, the contextual features we documented about each service allowed us to arrive at some preliminary observations grounded in a comparison of these features to the financial statement audit context. These observations offer opportunities for future research. For example, we observed that the services we identified vary in terms of the number of criteria available for measuring and evaluating the relevant subject matter. Research is needed to understand why some services have many criteria whereas others have few and the circumstances under which generally accepted criteria emerge. Research could also examine the circumstances under which accounting firms seek to expand into service areas with established versus contested criteria. We also observed that the firms are present in some service areas but are mostly absent in other areas. Research could investigate why firms are able to gain considerable market share in some service areas, while struggling in others. Prior research provides some insight into this question (e.g., Andon et al. 2015), but it is not clear how the firms decide to invest resources in expanding into some service areas and fewer (or no) resources in other areas. Finally, we observed that some service areas involve subject matter within (outside) the professional accountant's traditional competencies in financial measurement, disclosure, and controls. Research could provide insight into how the firms decide whether to train their existing staff or hire new staff in preparation for expansion to new service areas outside the accountant's circle of competence.[1]

[1] The phrase "circle of competence" is often traced back to Warren Buffet's letter to the shareholders of Berkshire Hathaway dated February 28, 1997.

This study contributes to research on new assurance services beyond financial statement audits. Whereas prior studies document findings from in-depth investigations of individual services, this paper differs from such studies in that we scan the broader landscape for a range of new service areas that are at various stages of development. We also gather information on key contextual features of services offered in these service areas. Many of the services we identify emerged in response to advances in technology. Growth opportunities for accounting firms in these new service areas will be hard-fought as they also represent opportunities for non-traditional competitors, including consulting and technology firms. Also, it is not clear whether the firms can train their staff to be capable of delivering high quality assurance in service areas outside their traditional area of expertise – financial statement auditing.

A key outcome of our study is a catalogue of the marketplace of assurance service areas beyond financial statement audits, which researchers can use to identify services to investigate in future studies. Just as accounting firms seek out opportunities to expand into new service areas, the audit literature would benefit by investigating these new areas. These new service areas offer opportunities not only to examine research questions that compare the financial statement audit context to other assurance contexts, like how the concept of materiality is applied in different service areas (cf. Cohen and Simnett 2015), but also to ask new questions, like how the firms determine what new areas to pursue and which ones to ignore. We hope the multitude of new services identified in this paper will serve as a starting point for researchers interested in learning what other assurance worlds are out there, waiting to be explored (Chapman and Peecher 2011).

The remainder of this paper is organized as follows. Next, we discuss the motivation for a study that catalogues the market for assurance services beyond financial statement audits. We then describe our approach to scanning the landscape for new services areas. Next, we report our

findings based on our efforts to document key contextual features for each service we identified. Finally, we conclude the paper with a discussion of some overall observations based on our cataloguing exercise, including opportunities for future research.

II. MOTIVATION

In 2018, CPA Canada launched the "Foresight" initiative aimed at understanding the technological and other changes taking place in Canada and globally and to identify their implications for the accounting profession (CPA Canada 2018). The initiative included extensive consultations with leaders from business, accounting practice, academe, and government and resulted in several publications as well as calls for research to delve into areas requiring deeper analysis.[2] Among its conclusions are that: (1) the assurance discipline has not kept pace with the real-time economy and is at a critical juncture; (2) the evolving expectations of stakeholders in a data- and technology-driven economy will dramatically reshape the services professional accountants are expected to provide; and (3) to ensure the profession is viewed as a leading provider of trust in the digital world and is well equipped to fulfill this role, it needs to consider future forms and uses of information and to explore new ideas for assurance services and how those services are being delivered (CPA Canada 2018).

To contribute to these initiatives, we proposed a study aimed at cataloguing the marketplace of assurance service areas and solutions currently offered by accounting firms and non-accounting organizations (e.g., consulting and technology firms) and documenting their characteristics. Our proposal directly responds to a call for such research by CPA Canada. In our proposal, we defined assurance services broadly, as follows (Elliott 1997, p. 63):

[2] Information about Foresight can be found on CPA Canada's website (https://www.cpacanada.ca/en/foresight-initiative).

> "Assurance services are independent professional services that improve the quality of information, or its context, for decision makers."

In addition to audit-level and review-level assurance, various other degrees of comfort can be provided through services such as agreed-upon procedures (AUPS), compilations, and reading and assessing information while applying subject matter expertise and professional skepticism. Thus, the scope of our proposal covered these kinds of assurance-related services as well.

The scope of our proposal also included coverage of both technology-related and technology-neutral assurance services, relevant frameworks and standards, and reporting methods for communicating assurance or providing comfort to intended users of the information (e.g., non-binary reports such as graded reports, ratings, and maturity levels). This paper focuses on technology-related service areas but provides some discussion of technology-neutral service areas. Audiences for assurance services can be stakeholders that are internal and external to the entity, along with stakeholders in the private and public sectors. The private sector includes publicly traded and private companies. The public sector includes all levels of government and non-governmental not-for-profit entities. Our proposal addresses both private and public sector audiences. However, current assurance service areas on financial statements or portions of financial statements or related documents such as contractual agreements and capital market-related services were deemed to be outside the scope of this research.

We started our cataloguing exercise by brainstorming about the different service areas (or topics), like non-GAAP measures, where assurance services may be demanded or provided and identified several technology-related and technology-neutral services. Based on our team discussions, we identified an initial list of service areas to cover in the exercise. We then consulted with CPA Canada staff to ensure our list was reasonably complete, which resulted in adding several new service areas.

The outcome of the cataloguing exercise was a database and a report that documents the service areas we identified, and the services offered in these areas. For example, we identified auditing of public key infrastructure (PKI) as a service area, and WebTrust for Certification Authorities (CAs) is a service offered in this area. Upon delivery of the first draft of our report, CPA Canada staff asked us to expand our search terms to focus not only on the service areas listed in Tables 1 and 2, but to add keywords associated with assurance such as audit, assurance, certification, validation, and verification. By doing this, we were able to obtain a more complete understanding of the marketplace of assurance services and solutions, broadly defined, currently being offered by accounting firms and non-accounting firms in the service areas we identified.

III. APPROACH

Scope and Output of the Cataloguing Exercise

As discussed above, the scope of our cataloguing exercise is assurance service areas offered by accounting firms and non-accounting firms that focus on events, conditions, or processes other than financial statement audits and reviews. We identified 33 service areas. Table 1 lists the 20 technology-related service areas and Table 2 lists the 13 technology-neutral service areas we identified.

The output of our cataloguing exercise is a worksheet for CPA Canada that, for each service area identified, categorizes the areas (e.g., technology-related versus technology-neutral), describes the services offered related to this area (e.g., the purpose of the service), and documents demand and supply characteristics (e.g., who provides the service) and the relevant standards and regulation. We also added to the worksheet a summary of our overall findings related to each service area identified (e.g., whether accounting firms are a major versus minor

player). In some cases we added insights gained from reviewing the research literature both inside and outside the field of accounting and auditing.

After completing the cataloguing exercise, we decided to organize what we learned about the services offered in each area using a standardized framework for documenting their key contextual features.[3] Specifically, using the definition of an assurance engagement other than audit or review of financial statements (CASE 3000; ISAE 3000) as a framework, we identified the following contextual features of services offered in each area to be recorded in a worksheet.

- **Engagement:** A brief description of the nature of the assurance engagement.
- **Underlying subject matter:** "The phenomenon that is measured or evaluated by applying criteria" (CSAE 3000, para. C12). For example, whether controls operate effectively in accordance with a specified framework.
- **Criteria/standards (including guidelines, frameworks and regulations):** "The benchmarks used to measure or evaluate the underlying subject matter. The 'applicable criteria' are the criteria used for the particular engagement" (CSAE 3000, para. C12).
- **Subject matter information:** "The outcome of the measurement or evaluation of the underlying subject matter against the criteria; that is, the information that results from applying the criteria to the underlying subject matter" (CSAE 3000, para. C12). For example, results of applying tests of controls in a SOC engagement.
- **Responsible party:** "The party(ies) responsible for the underlying subject matter" (CSAE 3000, para. C12).
- **Practitioner:** "The individual(s) conducting the engagement…" (CSAE 3000, para. C12).
- **Communication:** The product (e.g., report) of the assurance engagement.
- **Intended users:** "The individual(s) or organization(s), or group(s) thereof that the practitioner expects will use the [communication]. In some cases, there may be intended users other than those to whom the assurance report is addressed" (CSAE 3000, para.

[3] CPA Canada staff did not ask us to complete this organizing activity. We, the research team, decided to do this so that we could organize what we learned from the cataloguing exercise such that it could identify the key contextual features of the services offered in each area we identified for researchers to use a starting point for designing future studies on new services.

C12).

- **Observations:** What the researchers learned from reviewing publicly available information about the engagement on the web and from some of the related research.

The description of the services offered for each technology-related and technology-neutral service area we identified can be found in Appendix 1 and 2, respectively. The complete set of contextual features (except for observations) is compiled into a database that CPA Canada will make publicly available on its website. Exhibit 1 provides examples of the full set of contextual features of services documented for the following technology-related service areas: 1.4 Smart Contracts (Network Related); 1.6 Cybersecurity Risk Management Programs (SOC Related); and 1.18 Real-Time Internal Audit (Data Integrity Related). Exhibit 2 provides an example of the full set of contextual features of services for a technology-neutral area: 2.5 Valuations. The complete set of contextual features, including observations, is also compiled in a supplement that is available from the authors upon request.

Cataloguing Process

The cataloguing process began in Fall 2020 and was completed during Spring 2021. The process contains two stages. During the first stage, we hired three undergraduate accounting student research assistants (RAs) to collect data from the Internet to generate an initial understanding of each identified assurance service area. To ensure the RAs understood the process, we prepared detailed instructions for all the information being sought (i.e., specific details about each service area, as described above) and walked the RAs through an example at an initial meeting. For each service area, the RAs first went to professional or practitioner websites (e.g., Big 4 and occasionally the next tier of accounting firms, the Institute of Chartered Accountants in England and Wales (ICAEW), the Center for Audit Quality) and then performed generic Google searches to find information on the area. We met with the RAs weekly to review

the worksheet and resolve any issues they had. The worksheet was shared via Microsoft Teams to ensure all members of the research team had access to the same up-to-date version of the worksheet and had an opportunity to verify the accuracy of the search records on a test basis.

During the second stage, we hired two undergraduate accounting student RAs to help us search for and collect additional data for each service area. Each member of the research team was assigned a subset of service areas and performed the searches as well. Broadly, as requested by CPA Canada staff, the goal of the second stage of the cataloguing process was to expand our initial search to identify a larger universe of potential service providers and to sharpen our documented understanding of the service areas identified. Specifically, we performed Google searches for each service area by combining the name of the area (and alternative terms in some cases) with a set of assurance-related keywords like audit, assurance, verification, validation, and certification. While the searches were reasonably comprehensive, they were still constrained by design. For example, we documented findings from the first 10 pages of Google search results only, for each combination of terms. We read the information for each result and assessed its relevance to our understanding of the service area in question. We documented the company name offering a service related to the service area in question, the website link to the result, and other information to help us evaluate the key contextual features of each service.[4]

Throughout the cataloguing process, we made efforts to ensure the quality of the final output. For the items that we assigned to RAs, we reviewed their findings on a weekly basis, met with them to provide feedback and helped them resolve any issues they encountered. One of the

[4] Some of the search results for the service areas were not related to assurance but information services, commercial offerings, and so forth. Some of the assurance related keywords used with the service services were not always indicators of independent assurance services being offered. Sometimes they were used in connection with consulting and advisory services, process quality assessments, and insurance.

research team members stayed in touch with CPA Canada staff to provide updates about our progress and to obtain feedback. The members of the research team met at least bi-weekly to discuss progress on the project, feedback from CPA Canada, and tasks to be completed. The discussions led to several refinements of the worksheet during the web search stage as we tried to capture additional aspects of the service areas and as we discovered new potential areas such as: 2.8 Business Model Descriptions; 1.15 Data Trust; 1.14 Crypto Asset Holding – Proof of Reserves; and 1.20 Gene and Biocomputing Assurance. In addition, CPA Canada staff provided their input on the service areas identified and requested that we add areas they were interested in, some of which were outside of the assurance area but involve the provision of comfort through the exercise of subject matter expertise and professional skepticism (e.g., 2.2 ESG/CSR/Sustainability – Assurance Focused – Other Activities, 2.6 Value Creation Services – Indicators; and 2.9 MD&A/Press Release).

IV. FINDINGS

We identified 33 assurance service areas from the cataloguing process. Next, we briefly describe the services offered in the service areas we identified, starting with the technology-related areas followed by the technology-neutral areas.

Technology-Related Service Areas

Overview

We identified 20 technology-related service areas during the cataloguing process. For discussion purposes we organize the services offered for the technology-related areas under three headings: Network Related; SOC Related; and Data Integrity Related (see Table 1).

Network Related

One network related service area is auditing of PKI, which includes WebTrust for Certification Authorities (CAs), an established assurance service provided around the world by accounting firms under license from CPA Canada. This service has contextual features similar in several respects to the financial statement audit context. For example, like financial statement audits for public companies, this service is mandated as browsers (e.g., Chrome, Safari) require CAs to undergo a WebTrust audit to be included in their list of trusted root certificates. If a website has a certificate that is excluded from a browser's list, visitors to the website will receive a warning from the browser that the website they are about to enter is not secure. While accounting firms are the major provider of WebTrust audits, the market for this service is small as only about 100 CAs provide certificates for all websites around the world (Digicert 2021).

Another area is blockchain assurance. Although blockchain is a widely touted technology we found no evidence of accounting firms providing assurance services for information systems that function via blockchain technology (e.g., a system which stores and shares data on a blockchain). Some firms provide a blockchain-based platform/system for companies to simplify workflows and save time on verification of data (e.g., Accenture n.d.; IBM n.d.). Other firms help companies evaluate their options for adopting blockchain technology in their businesses. However, we identified several potentially viable assurance opportunities related to blockchain. For example, a potentially valuable assurance opportunity relates to validation of attributes of physical items being added to blockchain records that could subsequently be traded through exchanges and online markets. That is, while blockchain technology is suggested as a potential solution to maintaining data integrity, management is still responsible for ensuring that, before data is recorded on a blockchain, it is valid and accurate. There may be a demand for auditors to assure that the data representing physical property (e.g., real estate, art, non-fungible tokens or

NFTs) and stored on the blockchain is isomorphic with the property that it purports to represent, although assurance providers will need to employ specialists with the requisite knowledge and skills to value and assess the attributes of those assets (Alles and Gray 2020).

Another potential service relates to the risk of error in smart contracts. Many technology consulting firms offer services aimed at helping companies design, review, and test their smart contract code. Some firms provide software tools for code review, though accounting firms appear to have limited presence in this area. Similarly, although opportunities exist for providing assurance over controls that build security into IoT devices, or testing and validating IoT devices, we find no evidence that accounting firms are providing services in this area.

SOC (System and Organization Controls) Related

Both small and large accounting firms offer SOC reporting services, including readiness services. These services cover a range of internal control elements (e.g., financial statement audit-related services – SOC 1; technology services – SOC 2, e-commerce services – SOC 3; cyber risk management – SOC for cybersecurity) that provide assurance to organizations and their stakeholders, including business partners. However, the market is fairly congested with other similar forms of services (e.g., Payment Card Industry Data Security Standard International Organization for Standardization, Cybersecurity Maturity Model Certification) offered by technology service providers. Moreover, differentiation between the various services is not always clear in the (online) descriptions. Generally, SOC offerings appear more opaque than non-SOC offerings, which tend to be more transparent in their underlying elements and requirements. SOC 2+ offerings can be very challenging for report preparers, assurance providers and report recipients due to the combination of multiple sets of criteria from multiple standard setters (NDNB n.d.).

A somewhat related but relatively new assurance service area is cybersecurity ratings. There appears to be a narrow group of companies offering formal cybersecurity ratings or scores, and they are not accounting firms, but we did find evidence of both accounting and non-accounting firms providing cybersecurity risk assessments. It appears that accounting firms are considering cybersecurity risk related to the financial statement audit and requirements for audits subject to PCAOB standards. Furthermore, this cybersecurity risk assessment has been expanded to include the impact of COVID-19 on the design and implementation of controls (e.g., EY 2020). However, research on disclosure of cybersecurity risks provides mixed evidence on the value and reliability of those risk assessments (Berkman, Jona, Lee and Soderstrom 2018).

Another emerging service area within cybersecurity is Cybersecurity Maturity Model Certifications (CMMC) of cybersecurity processes and practices. Such certifications are required in certain sectors such as defense, health, and critical infrastructure to, for example, bid on contracts (Defense Acquisition Regulations System, Department of Defense 2020). A CMMC Accreditation Board authorized by the U.S. Department of Defense accredits auditors and manages a dispute resolution process. There are several variations of CMMC such as CMMI (Cybersecurity Maturity Model Integration) that can be applied in various other contexts.[5] CMMC services are provided by many accounting firms, as well as numerous consulting firms. Services include training, risk, and control assessments, CMMC readiness assessments, and CMMC certifications regarding the level of maturity achieved by the entity. Self-assessment tools such as smart checklists and questionnaires are also available from various providers.

It is noteworthy that the AICPA has developed a SOC 2 service for providing assurance on the security of a service organization's system and a SOC for Cybersecurity Risk

[5] For an example of CMMI, see https://www.isaca.org/enterprise/cmmi-cybermaturity-platform.

Management Program (CRMP) service for providing assurance on the entity's CRMP, and related Trust Services Criteria (TSC) to be used in providing such services and which have similarities to CMMC engagements (AICPA 2017). However, it has not developed a maturity model to use with the TSC engagements. Also, the concept of reporting on maturity levels is unfamiliar to most accountants and creates uncertainty in connection with the criteria and maturity judgments involved in applying TSC to assurance services aimed at reporting on maturity levels.

The introduction of Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), has created a market for Privacy by Design certification (Cavoukian 2011; European Union 2016). While accounting firms do not provide the certification, they do provide services like Privacy by Design assessment reports that assist companies in demonstrating to accredited certification bodies their compliance with the seven foundational principles of Privacy by Design.[6] It was not clear from our search what professional standards practitioners follow when performing a Privacy by Design assessment. Also, we were unable to get a sense of the potential demand for this service and the degree to which accounting firms are competing with non-accounting firms for position in this market.

Our search for information on AI-related assurance uncovered information on AI as a diagnostic tool, for example in medicine. We found some information on how AI can be used as a tool within an audit, but very little information on external assurance-related services on the AI systems. Analysis of AI systems themselves is primarily the responsibility of the internal audit function of the organization, focusing on whether the AI is functioning in the way intended and

[6] For an example, see https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF.

whether there is bias in the decision making of the AI. We noted the AI Fairness 360 toolkit that can help detect and remove bias in machine learning models (Varshney 2018).

Cryptocurrency mining is another SOC related service area. In May 2021, Tesla CEO Elon Musk raised the possibility that renewable energy audits could alleviate some concerns about miners' energy usage (Crooks and Bloomberg 2021). An energy audit is a potential assurance engagement that could be offered in the future. Also in May 2021, the Bitcoin Mining Council was established to focus, among other things, on promoting transparent disclosure of energy usage (e.g., use of renewable energy sources versus fossil fuels) and sustainability initiatives. The Council characterizes itself as "a voluntary and open forum of Bitcoin miners committed to the network and its core principles" (Bitcoin Mining Council 2021). The Council first met in June 2021, and it is not yet clear whether the Council ultimately will recommend energy audits for miners. We did not identify in our searches any examples of accounting firms or non-accounting firms offering energy audits. However, accounting firms have developed technology-enabled tools to support financial statement audit teams in evaluating material mining-related transactions and balances.

Data Integrity Related

There exists concern about the integrity, privacy and confidentiality of marketing data, supply chain data, and data used in AI development.[7] Internal and external assessments of data integrity, including completeness and accuracy, are also of increasing importance given the focus on data and its distribution to the cloud and data warehouses. Such concerning or important issues represent potential subject matter for data integrity assurance. Ironically, machine learning

[7] For example, see https://martechtoday.com/analytics-audit-101-identify-issues-and-correct-them-to-ensure-the-integrity-of-your-data-242211; Trust but Verify....because without data trust is just an opinion - Technical Process Management (zimmark.com); Data Auditing Building Trust in Artificial Intelligence (isaca.org)

(ML) has been suggested as a potential method of tracking data and identifying issues for follow-up, but an ML algorithm itself must be periodically evaluated to assure its processing integrity.

Data integrity of crypto assets and liabilities has also become a priority area for accounting firms if for no other reason than their need to provide assurance on the financial statements that report such assets and liabilities (Pimentel, Boulianne, Eskandari, and Clark 2021 in press). For financial assets and liabilities that are in units based on cryptocurrencies, accountants and auditors need to have the required knowledge of accounting principles and competencies for valuing those assets and liabilities. Indeed, accounting firms have developed tools to facilitate the audit of company financial statements that contain material cryptocurrency (or, more generally, digital asset) balances (e.g., PwC's Halo; EY's Blockchain Analyzer). These tools demonstrate that accounting firms are attempting to respond to concerns raised by CPA Canada (CPA Canada n.d.; CPAB 2019), and other stakeholders about the accounting for cryptocurrency balances.

Some accounting firms offer assurance services related to internal control evaluation (design of controls), SOC reporting, and agreed-upon procedures for digital and cryptocurrency assets. Some accounting and consulting firms are providing Proof of Reserves audits that provide users of a cryptocurrency exchange with assurance that the exchange has sufficient assets on hand to cover the user balances (i.e., that assets are being appropriately held).[8] In May 2021, the Chamber of Digital Commerce (2021) published a practitioner's guide that discusses best practices and the applicability of existing AICPA assurance standards for performing Proof of

[8] For example, Armanino LLP completed a Proof of Reserves agreed-upon procedures report for gate.io dated May 25, 2020 (https://www.gate.io/en/proof_of_reserves).

Reserves audits. Contributors to the guide include several accounting firms, which suggests the firms are seeking a leadership role in this service area.

Another area related to both financial statement and data integrity assurance pertains to XBRL-coded financial statements that are becoming required in many jurisdictions. While our search yielded little, if any, evidence of assurance over the integrity of XBRL data currently being provided,[9] there are many companies that provide either a service to help generate the XBRL reporting or software related to XBRL. While accounting firms are represented in the list of providers, there is much competition from both accounting firms and non-accounting firms. XBRL for ESG (Environmental, Social and Governance) reporting is an emerging topic of interest in this area.[10]

Several sets of criteria for evaluating, auditing, and certifying data integrity of non-financial statement information have been proposed (e.g., AICPA Criteria for Describing a Set of Data and Evaluating its Integrity). Related (competitive) criteria are contained in ISO/IEC 27701:2019 standard for managing "the processes for protecting the capture, accountability, availability, integrity, and confidentiality of personal data." However, the area is not settled and, surprisingly, we identified few accounting firms offering non-financial statement data integrity assurance services.

Somewhat related to data integrity assurance is assurance on data trusts (Zarkadakis 2020). Data trusts are legal entities created to hold data and provide access to it in accordance with specified terms. The key aspects of data that data trusts aim to manage are data protection,

[9] But please refer to Boritz and No (2009), Srivastava and Kogan (2010), Boritz and No (2016) and XBRL Assurance (aicpa.org).

[10] Information on XBRL-related issues is available at https://www.xbrl.org/the-standard/.

privacy, confidentiality, intellectual property rights, and contractual obligations.[11] The UK's Open Data Institute (ODI), founded in 2012, works with companies and governments to develop principles of data trusts. In 2021, the province of Ontario announced that it plans to create a Data Authority to hold provincial data. Data and Information Transfer Systems - Audit and Certification of Trustworthy Digital Repositories (ISO TRAC) outlines actions a repository can take to be considered trustworthy. A technology-enabled solution that has been proposed to protect access to data repositories is zero-trust architectures (Kerman 2020). Oxford Insights (2019) identifies aspects of data trusts that would be candidates for audits/certifications. This is an evolving area for data integrity assurance, but we found virtually no discussion of it by accounting firms.[12]

Several seals and trust marks have been proposed with subsets and variants of the data integrity criteria listed above (e.g., Internet Society n.d.). This is ironic given the accounting profession's attempt to enter this service area with its now-abandoned consumer-oriented WebTrust service.

Given recent concerns about the accuracy of information on social media sites, we observed a number of service providers offering fact checking services, credibility ratings for news content (including images, video and textual information) and tools for fact checking. Change records are also available to track the alterations and origins of information to help judge its credibility. Significant resources are available through journalism and library organizations. Standards are also being established worldwide to provide credibility to published information. However, we did not find evidence of accounting firm assurance services offered in this area.

---

[11] See also Trust Principles for Digital Repositories: https://www.nature.com/articles/s41597-020-0486-7.
[12] A repository of data trust audits and audit reports is available at: https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits

With the growth of interest in biotechnology, gene editing, and bio computing and the need for reliable information in this area, we searched for nascent data and process integrity-related assurance service offerings related to this area. We found a few entities offering services or tools for bioinformation assurance on controls over common lab processes aimed at potential risks of errors in processing genetic materials and data. However, we found no providers of biological computer assurance. Although this is a specialized area, at the same stage of development that environment-related assurance was several decades ago, over time it may develop into a fast-growing field similar to the development of ESG-related reporting and assurance.

Finally, we also considered real-time or continuous internal and external audit services. The former falls under the umbrella of advisory (not assurance) services for most accounting firms. As such, many firms offer services to help companies perform internal audits in real-time. Non-accounting firms also provide these services in addition to automated technology tools (ATTs) that companies can leverage to monitor and react to data processing anomalies on a continuous basis. We also found an abundance of websites, blogs, and practice-oriented articles devoted to broad education of what real-time or continuous audits mean and the impact they will likely have on the future of internal audits. However, we rarely found real-time or continuous external audit services – only one example was identified in the crypto currency area (Buxton and Nau 2019). Some firms offer tools and software that can be used in external audits to manage data in real-time but most of these firms are not traditional accounting firms. Non-accounting firms also provide management systems to assist companies to schedule and keep continuous track of external or internal audits (more of a project management tool). Often

offerings did not distinguish between internal and external audit, and in those cases the services were more internal audit focused.

Technology-Neutral Service Areas

We identified 13 technology-neutral service areas. Although not the focus of this paper, we provide high-level details about these service areas below. Broadly, most fall under the umbrella category of expanded business reporting, and we organize these service areas into three categories: ESG/CSR/Sustainability Reporting and Assurance; Value Measurement Reporting and Assurance; and Enterprise Risk Assessment, Internal Control and Compliance (see Table 2).

There is a rich literature on ESG-related services, which has been an emerging service area for the last two decades (e.g. Cohen & Simnett 2015; Maroun 2020; Morimoto, Ash & Hope 2005; O'Dwyer 2011; O'Dwyer, Owen & Unerman 2011). Notably, reporting and assurance of ESG-related information is still voluntary in many jurisdictions. Further, several patterns seen in this service area are evident in the Value Measurement areas, particularly for services that, like ESG, pertain to subject matter further away from the professional accountant's core competencies. For example, there is much competition between accounting firms and non-accounting firms (e.g., consulting, technology, and engineering firms) in not only ESG-related services but also in valuation reporting or value creation services, Business Model Description (BMD) services and services that measure operational performance. This is not surprising given that accounting firms do not have the same competitive or knowledge advantage in this subject

matter compared to the financial statement audit context.[13] Moreover, for areas related to valuations and value creation, finance departments and valuation specialists feature prominently in the services offered by accounting firms. For all these areas, there are also just as many if not more advisory services being offered (e.g., helping companies measure ESG, performance, value, or value creation) as assurance services.

Like services related to non-GAAP measures and MD&A, services in the Internal Control and Compliance area are more related to accounting firms' traditional competencies of financial reporting, business processes, and controls. In these service areas, providers are predominantly professional accountants and accounting firms except for compliance services that pertain to non-financial laws, regulations, and best practices (e.g., health and food safety, real estate). Although they are commonly tied in with financial statement audits, service offerings for non-GAAP measures and MD&A are separate from the financial statement audits and are specified procedures or advisory services similar to those offered for the Internal Control and Compliance categories (e.g., helping companies to be compliant, to establish effective ERM or internal control processes, or to self-assess).[14]

V. DISCUSSION

After documenting the key contextual features of each service area, we were able to draw some observations about the marketplace of new assurance services. Each observation is

[13] There is also competition to be the authoritative source of reporting principles in ESG-related services, as well as in BMD and value creation services. In all cases, competing criteria come from organizations such as the Global Reporting Initiative (GRI) or International Integrated Reporting Council (IIRC, which has merged with the Sustainability Accounting Standards Board (SASB) to become the Value Reporting Foundation (VRF)). Other competitors include the Climate Disclosure Standards Board (CDSB; ESG-related), Financial Reporting Council (FRC; BMD), and the Balanced Scorecard Institute (BSI; value creation).

[14] However, compliance reviews and audits are also common.

grounded in a comparison of the new service areas we identified to our pre-existing understanding of the financial statement audit context.

Some Service Areas Have Multiple Standard Setters & Criteria Competing for Ownership

Some of the service areas we identified have more than one standard setter or certification body competing for ownership or control, including 2.1 ESG/CSR/Sustainability – Assurance Focused; 2.8 Business Model Descriptions (Attest to Integrity of BMD); 2.12 Compliance with Best Practices/Standards; and 1.12 Data Integrity. For example, many ESG standard setters are outside the traditional accounting or auditing fields and have different ways of generating and enforcing authoritative standards and guidelines than is the practice with accounting and auditing standards (e.g. WBCSD 2020; SASB n.d.; CDSB n.d.; B Lab n.d.). They may not be governed by codes of professional conduct and may not require independence, objectivity, and due care on the part of the practitioners implementing their standards or the same level of evidential support for the assurance provided.

Given that some of the service areas we identified have more than one standard setter or certification body, it follows that these areas also have more than one set of criteria. Compared to GAAP and GAAS, which are the familiar territory of professional accountants, the relevance, reliability, and future evolution of the many standards and certifications available may be difficult to determine. Some standards may not be ready for assurance services because they are not "suitable criteria" (i.e., not complete, valid, neutral, or measurable) and others may not be ready for assurance services because professional accountants have not developed competencies, evidence gathering processes, or reporting approaches for them. For example, SOC 2+ services combine criteria established by the AICPA with additional criteria adopted from other "standard setters", such as ISO, government regulators, major cloud service providers, and data center

service providers. Assurance service providers must be cautious when considering combining criteria from diverse frameworks and providing assurance based on their clients' achievement of the base criteria plus the added criteria. They need to ensure that the extra criteria are "suitable criteria" from the standpoint of the standards governing the assurance engagement and to avoid implying that assurance is being provided on a corpus of criteria if only some of them are relevant or if in fact the criteria are only part of a description created by management and not actually part of the assurance engagement.

Accounting Firms are Present in Some Service Areas and Absent from Other Areas

Accounting firms are present (e.g., offering services) in some of the areas we identified, including 1.1 (Auditing) PKI; 1.5 SOC Reporting on Service Organizations & SOC 1, 2, 3; and 1.9 Data Privacy Compliance Service – GDPR. For example, accounting firms appear to have established market leadership in providing services related to the auditing of PKI with WebTrust audits for CAs. While prior research has documented challenges the accounting profession has experienced in promoting the WebTrust seal of assurance to owners of individual websites (Gendron and Barrett 2004), we are aware of little research that focuses on the success of WebTrust for CAs and other established services offered by the firms (e.g., SOC services).

Accounting firms are largely absent from some of the other areas we identified, including 1.2 Internet of Things; 1.7 Cyber Rating Services; and 1.17 Fake News Check. It remains unclear why the accounting firms are not currently involved in these areas, but we did learn that some of the service providers are consulting/technology firms and that some of their employees may be professional accountants. We also learned that the accounting firms are competing with consulting/technology firms in some areas like blockchain assurance service and smart contract

assurance, and that some accounting firms offering services employ non-accountants to provide the services.

Some Service Areas Relate to Subject Matter Within (Outside) CPA's Competencies

Some of the services areas we identified relate to subject matter that is within the CPA's traditional competencies (e.g., financial performance measures, disclosures, and controls) and would represent opportunities to offer new services. For example, assurance related to area 1.15 Data Trust seems like a promising opportunity to explore, as accounting firms have significant experience gained from data integrity assurance practices that could be applied to this area. Nevertheless, accounting firms are not currently visible service providers in this area. Other topic areas we identified that build directly on professional accountants' current competencies and knowledge include assurance over MD&A and press releases, control risk assessments (ERM) and internal control reporting (COSO). These areas provide clear opportunities for accounting firms without significant investment in additional skills and knowledge. While accounting firms have a visible and sizable presence in the latter two service areas, there is limited presence of accounting (or any) firms in the former area.

Other topic areas relate to subject matter that is outside the CPA's current competencies. For example, in area 1.4 Smart Contract Assurance Services, examining the smart contract code is a form of assurance but requires computer coding skills which are currently outside the skills and knowledge CPAs are required to gain. Other topics for which detailed computer coding knowledge is required include services such as 1.2 Internet of Things security and 1.10 (Auditing) AI algorithms and processes. If accounting firms wish to expand into these areas, then additional knowledge and skills may need to be developed which allow them to leverage their assurance knowledge in these new areas.

Some Service Areas Refer to Advisory/Limited Assurance Services as Audit or Assurance

We also observed that the assurance-related terminology professional accountants are accustomed to (e.g., audit, examination, review, validation, verification, certification) has been appropriated by numerous groups and enterprises who use them in various, inconsistent ways. For example, we observed some confusion in terms of how Proof of Reserves (PoR) reports are characterized. A PoR report suggests that some level of assurance is being provided, but many of the examples we identified are, in fact, reports of agreed-upon procedures.[15] In addition, some accounting firms provide Privacy by Design Assessment Reports that assist companies in demonstrating to accredited certification bodies their compliance with the seven foundational principles of Privacy by Design. Such assessments provide comfort, as discussed earlier, but not assurance. Data integrity service areas refer to "data verification," "data integrity assurance," "data audits", and "data assurance." For example, Datatrue (Plans | DataTrue) provides an automated data scanning "data assurance" service on a subscription basis, whereas the AICPA has developed a "data integrity assurance" service that has similarities to its SOC suite of services whereby "data integrity assurance" is provided based on the adherence of the data description to the Data Description Criteria and on the adherence of the described data to the Data Integrity Criteria. Data trust services refer to "data audits," "certifications", and "reviews". For example, Williams (2019) reports on the importance of data trust by citing testimony provided by Deputy Secretary of Defense David L. Norquist as follows:

> "DOD developed "a single authoritative source for **audit** and business data analytics" called ADVANA, a platform that holds more than 15 billion transactions, Norquist said in his testimony. ADVANA, which DOD used to automate the quarterly **review** process, also takes in data from more than 120 DOD systems, hosts at least 7,000 users and

[15] Technically, agreed-upon procedures are not considered assurance services because they do not express a conclusion. However, under the broader definition of assurance services in this paper, they would be considered as improving the quality of information or its context for decision makers.

> creates nearly 300 dashboards. And as DOD continues to have **annual audits**, it will incorporate more automation, especially as it fields new enterprise resource planning (ERP) systems." (**emphasis added**)

Similar terminology confusion is found in technology-neutral services. For example, in connection with 2.3 Non-GAAP measures, some firms give management advice on the best KPIs to use for reporting their performance. However, although it clearly is intended to provide comfort based on the subject matter expertise of the adviser, the advice does not appear to be "assurance" as formally defined. Another example involves the terms used in 2.8 BMD-related services, including "business model audit," "business strategy audit," "business assurance," "business model validation," "business model testing," "business model evaluation," and "business model assessment." Some of the terms are used as metatags on websites that mix assurance and advisory services, creating confusion about the nature of the services offered. Many assurance terms are used in conjunction with services that are advisory services.

Some Service Areas Involve Use of Unconventional Reporting Formats

Many of the services that we examined involved unconventional reporting formats compared to those used in financial statement audits. For example, 1.5 SOC 2 Reports include a list of control tests conducted and their results, 1.7 Cybersecurity Rating Services provide grades, 1.8 CMM Certifications report on the achievement of cybersecurity process maturity levels. Also, the AICPA's assurance services related to 1.12 Data Integrity report on the data description as well as the data itself while data integrity services related to 1.16 Data/Privacy Seals provide Seals or Trust Marks in addition to or instead of narrative reports. Thus, although financial

statement audits are noted for their binary pass/fail opinions, other assurance areas provide examples of alternative formats to report assurance opinions.[16]

Some Service Areas Involve Use of Smart Checklists and Self-assessment Tools

We noted many offerings of smart checklists and self-assessment tools in several areas including 1.5 SOC Reporting on Service Organizations & SOC 1, 2, 3, 1.8 CMMC, 1.13 XBRL, and 1.17 Fake News Checks, 2.3 Non-GAAP Measures, and 2.4 Measures of Operational Performance. Such tools represent useful and valuable offerings, especially for services such as compliance services (e.g. PwC n.d.; Praxiom Research Group Limited 2021; RiskWatch n.d.). A potential issue of concern for enterprises is that such tools may not include independent review and may not require sufficient appropriate evidence to support the responses to the questions in the self-assessment questionnaires. However, this low level of assurance provided by using smart checklists and self-assessment tools may not be clearly communicated to the user. If users cannot tell the difference between the assurance offered from these tools and the assurance offered by independent firms performing rigorous assurance, organizations will likely prefer these tools due to lower cost. The self-assessment tools also represent potential concerns for CPAs. First, the self-assessment tools can mislead enterprises into thinking that they are getting more assurance than they are receiving and lead them to place less value on professional accounting services.[17] Second, the self-assessment tools may represent assurance areas that can be easily automated,

[16] It can be argued that financial statement audit opinions are not necessarily binary as they can be unqualified, qualified, adverse, disclaimer of opinion, and have an emphasis of matter/other matter paragraphs. We use binary in the sense that audit opinions on financial statements are unqualified or qualified and don't express degrees of fairness of presentation like ratings or maturity models do.

[17] For a discussion of this issue in connection with SOC engagements see FAQs - Effect of the use of software tools on SOC 2® examinations | Resources | AICPA

limiting the opportunities for professional accountants to earn economic returns on investments in such services.

Potential Research Opportunities

The observations we highlighted above helped us to identify several promising opportunities for future research on the marketplace of new assurance service areas.

The Evolving Marketplace: The topic of assurance services is a rapidly evolving area with innovative ideas being generated and numerous participants (e.g., consulting and technology firms), many of whom are not traditional assurance service providers. A question we have is to what extent are new services currently being discussed for future development that do not yet appear in items listed on the internet? For example, supply chain issues have been raised in academic research and in recent AICPA service offerings but were not part of our list of new services. Similarly, Proof of Reserves have recently been identified as a potentially important assurance service related to crypto assets but was not included in our initial list of topics.[18] Hence, the cataloguing exercise we performed is at a point in time and future research is needed to keep pace with changes in the marketplace of services.

Future Assurance Demand: Which areas are expected to experience increased demand for assurance services in the future? According to a Deloitte (2020) article aimed at internal audit practitioners in the financial sector, the following are the top 10 emerging IT topics: 1. Cybersecurity; 2. Operational Resilience; 3. Cloud Governance and Security; 4. Extended Enterprise Risk Management; 5. Transformation & Change; 6. Digital Risk (RPA, AI); 7. Data Governance; 8. IT Strategy and Governance; 9. Payments; and 10. Systems Development.[19]

---

[18] Crypto Accounting Is Changing – How Proof of Reserves Could Improve Crypto Reporting (forbes.com)
[19] See also https://multiviewcorp.com/blogs/how-will-financial-audits-change-in-the-future/ and How Technology Will Change the Accounting Industry (multiviewcorp.com).

Future research could investigate how accounting firms decide which service areas to allocate resources into offering new services and which areas they ignore.

Service Area Threats and Opportunities: What threats and opportunities do the Big 4, next tier, and small accounting firms face associated with the new service areas we identified? What are these firms doing to ensure that opportunities are not lost to traditional competitors (i.e., other accounting firms) and non-traditional competitors like consulting and technology firms? Also, who (or what) are the competitors? For example, we noted the increasing presence of self-assessment tools including AI-based checklists that could be connected to sensors and intelligent agents, automating evidence-gathering procedures that were once performed by human auditors. What threats and opportunities are created by the proliferation of such tools? Future research could investigate how accounting firms evaluate the competitive landscape and whether they are leading or lagging their non-traditional competitors in introducing new services. Anecdotal evidence suggests that profession-wide quality control processes may not be as well developed for non-financial statement services as are in place for financial statement audits (e.g., regulator-performed inspections). This lack may undermine trust in new assurance services. Thus, future research could investgate quality control issues related to various services.

Technology Strategy Robustness: Since many of the emerging services we identified, such as cyber ratings services, relate to developments in business technology, do the accounting firms have overall technology strategies aimed at addressing these developments? Presumably, elements of such strategies would involve technologies, human resources, and processes for delivering the services. Future research could investigate what technologies, specialist or knowledge resources, and processes are available or are being created to support development and roll out of new assurance service areas and how significant is the investment in them.

Technology Tools: Although we noticed in our search that accounting firms discuss the use of tools such as audit data analytics, natural language processing, AI algorithms, wearable devices, and image processing in the provision of some of the services, we saw little information about how the firms deploy these tools or encourage their use in the provision of assurance services. Future research could investigate how firms monitor and evaluate the effective development, implementation, and use of assurance service-related tools. This research could answer questions such as, "what internal quality monitoring processes are used to specifically review and evaluate the use of various tools in relation to assurance service quality?"

Professional Competencies: Future research could investigate what professional competencies are affected by the new services and tools we identified. For example, an IFAC publication (Arnold 2021) raises questions pertaining to the potential conflict between new assurance services and codes of ethics. Future research could consider what technical competencies are required on the part of assurance providers to monitor and evaluate the work of contractors, vendors and third parties to whom IT processing responsibilities are outsourced, as well as what changes are needed to the professional education curriculum for entry level-education to support the provision of new services.

VI. CONCLUSION

We identified 33 new assurance service areas and documented our findings about the key contextual features of those services. Our paper provides a snapshot of the breadth of assurance service areas that are currently being offered. Among the services that we identified in these areas are services that are being offered by non-traditional assurance providers using a variety of both traditional and innovative approaches.

This study has limitations. Our list of new assurance services may not be complete as there may be established services and services under development that are not available on public information sources such as those we used for our cataloguing exercise or that have become available after our initial identification of new services.[20] This presents a research opportunity to build on this study by using more extended information searches and additional information sources such as the news media, interviews, and surveys. Keeping these limitations in mind, our study contributes to our understanding of the many service offerings in the assurance marketplace and raises some issues for consideration, discussion, and research.

[20] For example, our searches did not identify some services that have been investigated in prior research like efficiency audits (Radcliffe 1998) and salary cap audits (Andon, Free and Sivabalan 2014).

REFERENCES

Accenture. n.d. Service: Blockchain. Accenture. Retrieved August 24, 2021 from https://www.accenture.com/ca-en/services/blockchain-index

Alles, M., and G. L. Gray. 2020. "The First Mile Problem": Deriving an Endogenous Demand for Auditing in Blockchain-Based Business Processes. *International Journal of Accounting Information Systems*, *38*, 100465.

Association of International Certified Professional Accountants (AICPA). 2017. Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy Available at Trust Services Criteria (aicpa.org)

Andon, P., C. Free, and B. O'Dwyer. 2015. Annexing New Audit Spaces: Challenges and Adaptations. *Accounting, Auditing & Accountability Journal* 28 (8): 1400-1430.

Andon, P., C. Free, and P. Sivabalan. 2014. The Legitimacy of New Assurance Providers: Making the Cap Fit. *Accounting, Organizations and Society* 39 (2): 75-96.

Arnold, C. 2021. Ethics, Technology, and the Professional Accountant in the Digital Age IFAC. Available at https://www.ifac.org/knowledge-gateway/supporting-international-standards/discussion/ethics-technology-and-professional-accountant-digital-age?utm_medium=email&utm_source=transactional&utm_campaign=GKG_Latest

Bain & Company. n.d. Consulting Service: Sustainability & Corporate Responsibility. Bain & Company. Retrieved June 19, 2021 from https://www.bain.com/consulting-services/sustainability-corporate-responsibility/

Berkman, H., J. Jona, G. Lee, and N. Soderstrom. 2018. Cybersecurity Awareness and Market Valuations. *Journal of Accounting and Public Policy* 37(6), 508-526.

Bitcoin Mining Council. 2021. "Bitcoin Mining Council." Bitcoin Mining Council. Available at: https://bitcoinminingcouncil.com/.

B Lab. n.d. About B Corps. Certified B Corporation. Retrieved August 25, 2021 from https://bcorporation.eu/about-b-corps?

Boritz, J.E. and W.G. No. 2009. Assurance on XBRL-Related Documents: The Case of United Technologies. *Journal of Information Systems* 23(2) (Fall): 49-78.

Boritz, J.E. and Won Gyun No. 2016. Computer-Assisted Functions for Auditing XBRL-Related Documents. *Journal of Emerging Technologies in Accounting* 13(1) (Spring): 53-83.

Buxton, N., and J. Nau. 2019. White paper: Real-time Attest Reporting. Armanino. Retrieved August 23, 2021 from https://www.armaninollp.com/white-papers/real-time-attest-reporting/

Chartered Professional Accountants Canada (CPA Canada). 2018. *The way forward: Transforming insights into action*. Available at: https://www.cpacanada.ca/foresight-report/en/index.html.

Canadian Public Accounting Board (CPAB). 2019. Auditing in the Crypto-Asset Sector – Inspections Insights. Available at: https://www.cpab-ccrc.ca/docs/default-source/inspections-reports/2019-crypto-inspections-insights-en.pdf?sfvrsn=9aa5c0d2_20

Cavoukian, A. 2011. Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario. Toronto, ON. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Chamber of Digital Commerce. 2021. *Proof of Reserves: The practitioner's guide to an emerging standard for increasing trust and transparency in digital asset platform services*. Available at: https://digitalchamber.org/proof-of-reserves-blog/.

Chapman, C., and M. Peecher. 2011. Editorial: Worlds of assurance. *Accounting, Organizations and Society* 36 (4-5): 267-268.

Chartered Professional Accountants Canada (CPA Canada). n.d. About Foresight. CPA Canada. Retrieved August 19, 2021 from https://foresight.cpacanada.ca/about-foresight

Chartered Professional Accountants Canada (CPA Canada). n.d. Blockchain and Crypto-Assets Resources for CPAs. CPA Canada. Retrieved August 23, 2021 from https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/cpa-perspectives-on-blockchain

Climate Disclosure Standards Board (CDSB). n.d. Framework for Reporting Environmental and Climate Change Information. CDSB. Retrieved August 25, 2021 from https://www.cdsb.net/what-we-do/reporting-frameworks/environmental-information-natural-capital

Cohen, J. R., and R. Simnett. 2015. CSR and Assurance Services: a Research Agenda. *Auditing: A Journal of Practice & Theory* 34 (1): 59-74.

Crooks, N., and Bloomberg. 2021. "Elon Musk suggests energy audits can relieve concerns over dirty cryptocurrency." *Fortune*, May 21, 2021. Available at: https://fortune.com/2021/05/21/elon-musk-bitcoin-crypto-audits-energy-use/.

Defense Acquisition Regulations System, Department of Defense. 2020. Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041). Federal Register. Available at https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

Deloitte. 2020. 2021 Hot Topics for IT Internal Audit in Financial Services: Confronting Uncertainty. Available at https://www2.deloitte.com/uk/en/pages/financial-services/articles/hot-topics-it-internal-audit.html.

Deloitte. n.d.. Blockchain Assurance Services. Deloitte. Retrieved June 21, 2021 from https://www2.deloitte.com/ca/en/pages/audit/articles/blockchain-assurance-services.html

Digicert. 2021. What is a CA? Certificate Authorities Explained. Accessed August 21, 2021. https://www.digicert.com/blog/what-is-a-certificate-authority

Elliott, R. K. 1997. Assurance Service Opportunities: Implications for Academia. Accounting Horizons Vol. 11 (4) December 1997: 61-74.

European Union (EU). 2016. General Data Protection Regulaation – Regulation (EU) 2016/679 OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. Intersoft Consulting. Retrieved August 23, 2021 from https://gdpr-info.eu/

EY. 2020. Cyber Security Resilience and Response throughout COVID-19 Pandemic. Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_ie/topics/cybersecurity/ey-covid-19-cyber-impact-assessment.pdf

Gendron, Y., and M. Barrett. 2004. Professionalization in Action: Accountants' Attempt at Building a Network of Support for the WebTrust Seal of Assurance. *Contemporary Accounting Research* 21 (3): 563-602.

IBM. n.d. Blockchain. IBM. Retrieved August 24, 2021 from https://www.ibm.com/blockchain

Internet Society. n.d.. Publications. Internet Society. Retrieved August 23, 2021 from https://www.internetsociety.org/ota/publications/

Jamal, K., and S. Sunder. 2011. Is Mandated Independence Necessary for Audit Quality? *Accounting, Organizations and Society* 36 (4-5): 284-292.

Kerman, A. 2020. Zero Trust Cybersecurity: 'Never Trust, Always Verify'. NIST. Retrieved August 23, 2021 from: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

Li, H., W.G. No, and T. Wang. 2018. SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors. *International Journal of Accounting Information Systems* 30, 40-55.

Maroun, W., 2020. A Conceptual Model for Understanding Corporate Social Responsibility Assurance Practice. *Journal of Business Ethics*, *161*(1), pp.187-209.

Morimoto, R., J. Ash, and C. Hope. 2005. Corporate Social Responsibility Audit: from Theory to Practice. *Journal of Business Ethics* 62, 315–325 (2005).

NDNB. n.d.. SOC 2 for Cybersecurity. NDNB. Retrieved Aug 23, 2021 from https://socreports.com/soc-2-services/soc-2-for-cybersecurity

O'Dwyer, B. 2011. The Case of Sustainability Assurance: Constructing a New Assurance Service. *Contemporary Accounting Research* 28 (4): 1230-1266.

O'Dwyer, B., D. Owen, and J. Unerman. 2011. Seeking Legitimacy for New Assurance Forms: The Case of Assurance on Sustainability Reporting. *Accounting, Organizations and Society* 36 (1): 31-52.

Oxford Insights. 2019. Exploring Data Trust Certifications. Available at: http://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf

Pimentel, E., E. Boulianne, S. Eskandari, and J. Clark. 2021. Systemizing the Challenges of Auditing Blockchain-Based Assets *Journal of Information Systems*, in press.

Practical Assurance. n.d.. Smart Contract Audit. Practical Assurance. Retrieved June 21, 2020 from https://practicalassurance.com/smart-contract-audit

Praxiom Research Group Limited. 2021. Praxiom's Plain English Cybersecurity Audit Checklist. Praxiom. Retrieved August 25, 2021 from https://www.praxiom.com/index.htm

PwC. n.d. PwC's Disclosure Checklist. PwC. Retrieved August 25, 2021 from https://www.pwc.com/us/en/services/audit-assurance/financial-statement-audit/disclosure-checklist.html

PwC. n.d.. Sustainability and Climate Change Services. PwC. Retrieved June 19, 2021 from https://www.pwc.com/gx/en/services/sustainability.html

Radcliffe, V. S. 1998. Efficiency Audit: an Assembly of Rationalities and Programmes. *Accounting, Organizations and Society* 23 (4): 377-410.

RINA. n.d.. Blockchain Smart Contract Verify. RINA. Retrieved June 21, 2020 from https://www.rina.org/en/blockchain-smart-contract-verify

RiskWatch. n.d. Cyber Security Assessment Checklist. Riskwatch. Retrieved August 25, 2021 from https://riskwatch.com/free-cyber-security-checklist/

Sustainability Accounting Standards Board (SASB). n.d. Download SASB Standards. Value Reporting Fountation SASB Standards. Retrieved August 25, 2021 from https://www.sasb.org/standards/download/

SGS. n.d.. ESG Certified. SGS. Retrieved June 15, 2021 from https://www.sgs.com/en/campaigns/sgs-esg-assurance-solutions/esg-verified

SGS. n.d.. ESG Optimized. SGS. Retrieved June 19, 2021 from https://www.sgs.com/en/campaigns/sgs-esg-assurance-solutions/esg-optimized

Srivastava, R.P. and A. Kogan. 2010. Assurance on XBRL instance document: A conceptual framework of assertions. *International Journal of Accounting Information Systems* 11(3): 261–273.

Szabo, N. 1997. Formalizing and Securing Relationships on Public Networks. *First Monday*. Available at: https://firstmonday.org/ojs/index.php/fm/article/view/548

Varshney. K. R. 2018. Introducing AI Fairness 360. IBM Research Blog. Available at https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/

Williams, L.C. 2019. Norquist: Data Trust Key to Improving DOD's Audit. Retrieved August 24, 2021 from Norquist: Data trust key to improving DOD's audit -- FCW

World Business Council For Sustainable Development (WBCSD). 2020. Reporting Matters: Maintaining Ambition Amidst Disruption - WBCSD 2020 Report. Available at: https://docs.wbcsd.org/2020/10/WBCSD_Reporting_Matters_2020.pdf

Zarkadakis, G. 2020. "Data Trusts" could be the Key to Better AI. Available at https://hbr.org/2020/11/data-trusts-could-be-the-key-to-better-ai

Exhibit 1
Example of Technology-Related Assurance Services Documented in CPA Canada Database

Panel A – Network Related Service

Smart Contracts

Solution Category	**Solution Type**
Blockchain	Technology-related service

SOLUTION DETAILS

Engagement Description	A smart contract is a computerized contract that self-executes contract terms written in lines of code (Szabo 1997). Assurance over smart contracts seeks to establish that they are properly setup to produce the intended results - service providers typically examine the smart contract code and do test runs (e.g., Deloitte n.d.; RINA n.d.). Since smart contracts use blockchain technology, smart contract assurance services are considered a subcategory of blockchain assurance services.
Underlying Subject Matter	The underlying code for the smart contract.
Subject Matter Information	Because the execution is controlled by the code, transactions are trackable but irreversible. Hence, it is important for organizations to have information about whether the code & contracts function as intended.
Responsible Party	Company management that uses or intends to use the smart contract.
Intended Users	Internal and external users of the smart contract.
Communication	Service providers typically report the testing procedures and results of the smart contract testing. The report may include risks and problems identified and action plans to address them (e.g., Practical Assurance n.d.; RINA n.d.). Click for examples

SERVICE PROVIDER DETAILS

Practitioner	Big Four or Non-Big 4 Accounting Firms General Consulting Firms Technology / Cybersecurity Companies
Practitioner Details	Practitioners may be certified as a Chartered Bitcoin Professional (CBP) or Crypto Currency Security Standard Auditor (CCSSA)

STANDARDS AND REGULATIONS

Criteria / Standards	N/A – no uniform standards exist currently

Exhibit 1 (continued)

Panel B – SOC Related Service

Cybersecurity Risk Management Program

Solution Category	**Solution Type**
Cybersecurity	Technology-related service

SOLUTION DETAILS

Engagement Description	The purpose of the engagement is to provide users with information on an entity's cybersecurity risk management program. Depending on the particular engagement (e.g., SOC for Cybersecurity, ISO, HITRUST), this information generally provides an understanding of cybersecurity risk, resiliency, and compliance, and the processes in place to establish controls to help mitigate potential adverse impact of threats and/or assess effectiveness of cybersecurity measures.
Underlying Subject Matter	The cybersecurity risk management program description and the controls (and processes) intended to achieve its objectives.
Subject Matter Information	For SOC for Cybersecurity, the independent CPA will conclude if the cybersecurity risk management program description (provided by Management) is presented in accordance with the required description criteria and if the controls were effective throughout the period to achieve the entity's cybersecurity objectives. This subject matter will vary for other engagement types.
Responsible Party	Company management
Intended Users	Company management, Board of Directors, shareholders.
Communication	SOC for Cybersecurity communication consists of the independent accountant's report on the cybersecurity risk management program. Communication varies for other engagements. Click for examples

SERVICE PROVIDER DETAILS

Practitioner	Big Four or Non-Big 4 Accounting Firms General Consulting Firms
Practitioner Details	Accounting (consulting) firms often perform SOC for Cybersecurity (other) services. Practitioners may hold a variety of certifications – e.g., Certified in Risk and Information Systems Control (CRISC).

STANDARDS AND REGULATIONS

Criteria / Standards	For SOC for Cybersecurity, the criteria used in evaluating the description of the cybersecurity risk management program are the Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program and the criteria for the control evaluation are the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy. These criteria will vary for other engagements.

Exhibit 1 (continued)

Panel C – Data Integrity Related Service

Real-Time Internal Audit

Solution Category	**Solution Type**
Business Assessment & Advisory	Technology-related service

SOLUTION DETAILS

Engagement Description	Real-time or continuous internal auditing intends to perform control and risk assessments on a frequent basis. A desire from stakeholders to have accelerated audits or monitoring of activities drives demand for real-time audits. The performance of this engagement typically requires practitioners to have significant technological infrastructure including data analytics tools to evaluate and then conclude on the evaluation of numerous and varied risks, information, transactions, or controls in short order. Real-time internal audits evaluate whether transactions and activities are being performed in accordance with company policy and/or whether systems and controls are operating effectively and as intended. While practitioners may perform this engagement, they also offer tools/software or assist companies to develop their own real-time internal audit processes or programs, to facilitate self-monitoring or self-assessments in real-time.
Underlying Subject Matter	IT systems, transactions, and internal control of a company.
Subject Matter Information	A description of performance metrics (e.g., KPIs) and functioning of systems/controls, which includes the number of exceptions, anomalies, outliers, inconsistencies, etc. detected.
Responsible Party	Company management
Intended Users	Company management, audit committee, shareholders.
Communication	Report that identifies exceptions, weaknesses, etc. Practitioners also typically provide suggestions for improving or remedying gaps, issues, weaknesses. Click for examples

SERVICE PROVIDER DETAILS

Practitioner	Big Four or Non-Big 4 Accounting Firms General Consulting Firms Technology / Cybersecurity Companies
Practitioner Credentials	N/A for real-time internal audit but certification by the Institute of Internal Auditors more generally required.

STANDARDS AND REGULATIONS

Criteria / Standards	Within the IIA's International Professional Practice Framework, its Strongly Recommended Guidance contains Global Technology Audit Guide 3 on Continuous Auditing.

Exhibit 2
Example of Technology-Neutral Assurance Service Documented in CPA Canada Database

Valuations

Solution Category	**Solution Type**
Business Assessment & Advisory	Technology-neutral service

SOLUTION DETAILS

Engagement Description	Valuation reports provide assurance related to the value of a business, which can be used to support decision making (e.g., sale of a business). There are three types of valuation reports that provide varying levels of assurance: comprehensive (high assurance); estimate (moderate assurance); and calculation (low assurance). Depending on the report type (comprehensive or estimate or calculation), the practitioner reviews all relevant information about the business to arrive at their conclusion.
Underlying Subject Matter	The value of shares, assets, or an interest in a business.
Subject Matter Information	Depends on the valuation approach used, but includes capitalized earnings/cash flow, net present value of discounted cash flows cashflows, and fair value of assets and liabilities.
Responsible Party	Company management
Intended Users	Owners and potential buyers of a company.
Communication	CBVs prepare a valuation report to communicate their valuation conclusions. Click for examples

SERVICE PROVIDER DETAILS

Practitioner	Big Four or Non-Big 4 Accounting Firms General Consulting Firms
Practitioner Credentials	Chartered Business Valuator (CBV)

STANDARDS AND REGULATIONS

Criteria / Standards	Practitioners follow the CBV Institute's practice standards (e.g., Standard No. 110) and code of ethics. The practice standards (Appendix A to Standard No. 110) highlight the different approaches to valuation: capitalized earnings/cash flow approach; discounted cash flow approach; and asset-based approaches.

Table 1
Identified List of Technology-Related Assurance Service Areas

Network Related

1.1 (Auditing) Public Key infrastructure
1.2 Internet of Things (IOT)
1.3 Blockchain assurance services
1.4 Smart Contracts

System and Organization Controls Related

1.5 SOC Reporting on Services Organizations (SOC 1, 2, 3)
1.6 Cybersecurity Risk Management Program
1.7 Cyber Rating Services
1.8 The Cybersecurity Maturity Model Certification (CMMC)
1.9 Data Privacy Compliance Service - GDPR
1.10 (Auditing) Artificial Intelligence Algorithms
1.11 Cryptocurrency Mining

Data Integrity Related

1.12 Data Integrity
1.13 XBRL
1.14 Crypto Asset Holding - Proof of Reserves (PoR)
1.15 Data Trust
1.16 Data Seal/Privacy Seal
1.17 Fake News Check
1.18 Real-Time Internal Audit
1.19 Real-Time External Audit
1.20 Gene & Biocomputer Assurance

Table 2
Identified List of Technology-Neutral Assurance Service Areas

ESG/CSR/Sustainability Reporting and Assurance

2.1 ESG/CSR/Sustainability – Assurance Focused
2.2 ESG/CSR/Sustainability – Assurance Focused – Other Activities

Value Measurement Reporting and Assurance

2.3 Non-GAAP measures
2.4 Measures of operational performance
2.5 Valuations
2.6 Value Creation Services – Indicators
2.7 Value Creation Services – Special reports
2.8 Business model descriptions (attest to integrity of BMD)
2.9 MD&A/Press release

Enterprise Risk Assessment, Internal Control and Compliance

2.10 (Control) risk assessments (Enterprise Risk Management)
2.11 Internal Control Reports (COSO, excluding financial reporting)
2.12 Compliance with best practices/standards
2.13 Compliance with laws and regulations

Appendix 1: Technology Related Service Areas

Service Name	Service Description
#1.1 (Auditing) Public Key Infrastructure (PKI)	A Certification Authority (CA) authenticates digital identities of users (ranges from individuals to computer systems and servers) and may also authorize a Registration Authority (RA) to provide users with digital certificates. CAs and RAs need to be trustworthy for users to rely on them to issue keys. That trust can be established via assurance of CAs and RAs; a WebTrust audit can be used to provide this assurance.
#1.2 Internet of Things (IoT)	IoT refers to a system of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human intervention. Assurance services related to IoT may include assessing controls over building the security into the product (more internal audit) or attesting to the effective functioning of the security and/or controls (more external audit). Assurance services may also include testing and validation of the IoT device.
#1.3 Blockchain Assurance Service	Blockchain assurance services involve evaluating the blockchain data quality and the blockchain functionality. Depending on where an organization adopts blockchain technology, the evaluation may be related to financial controls or non-financial controls, and the service can be one-time or continuous (e.g., Deloitte n.d.).
#1.4 Smart Contract Assurance Service	A smart contract is a computerized contract that self-executes contract terms written in lines of code (Szabo, 1997). Assurance over smart contracts seeks to establish that they are properly setup to produce the intended results - service providers typically examine the smart contract code and perform test runs (e.g., Deloitte n.d.; RINA n.d.). Since smart contracts use blockchain technology, smart contract assurance services are considered a subcategory of blockchain assurance services.
#1.5 SOC Reporting on Services Organizations & SOC 1, 2, 3	SOC engagements provide either specific users (SOC 1 and 2) or general users (SOC 3) with information about controls at a service organization. SOC 1 reports are oriented around controls at a service organization that is relevant to the entities' internal control over financial reporting. SOC 2 and 3 reports are focused on controls at a service organization relevant to security, availability, processing integrity, confidentiality, and/or privacy.

#1.6 Cybersecurity Risk Management Programs	The purpose of the engagement is to provide users with information on an entity's cybersecurity risk management program. Depending on the particular engagement (e.g., SOC for Cybersecurity, ISO, HITRUST), this information generally provides an understanding of cybersecurity risk, resiliency, and compliance, as well as the processes in place to establish controls to help mitigate potential adverse impact of threats and/or assess effectiveness of cybersecurity measures.
#1.7 Cyber Rating Services	Cybersecurity rating agencies review a company's security infrastructure and assign a cybersecurity performance score based on how well a company can protect its data assets and information from data breaches. Cybersecurity ratings provide stakeholders with insight regarding a company's cybersecurity risk. A good security rating provides assurance to prospective business partners and existing customers. In contrast, a poor rating can mean the company's data is at risk. Cybersecurity ratings were intended to replace cybersecurity audits or reviews with a quicker and more automatable (yet still credible) assessment approach. Thus, they operate as a competitor to SOC for cybersecurity and as an independent, third-party alternative to cybersecurity self-assessments.
#1.8: Cybersecurity Maturity Model Certifications	Cybersecurity Maturity Model Certifications are required in certain sectors such as defense, health and critical infrastructure. The original Carnegie Melon Capability Maturity Model (CMM) has been adapted for the assessment of Cybersecurity management practices and has been standardized by government agencies such as the U.S. Department of Defense (DoD). There are several variations of the CMM that can be applied in various other contexts. The US DoD has developed a model classifying cybersecurity practices into five levels of maturity and requires that an accredited and independent Certified 3rd Party Assessment Organization (C3PAO) verify and certify the level of maturity achieved by the organization as a pre-condition for seeking to enter into a supply contract with the government that requires that level of maturity.
#1.9 Data Privacy Compliance Service – GDPR	A privacy by design assessment report assists companies in demonstrating they are in compliance with the seven foundational principles of Privacy by Design. This service involves collecting evidence (e.g., review of documentation) to assess the organization using an assessment methodology that is built on the seven foundational principles of Privacy by Design.

#1.10 Artificial Intelligence Algorithms	The AI systems themselves are analyzed for functionality, and in addition the output of the system is also analyzed. Engagements focus on two areas: whether the AI is functioning in the way intended and whether there is bias in the decision making of the AI.
#1.11 Cryptocurrency Mining – Energy Audits	The establishment of a Bitcoin Mining Council was proposed in May 2021. One of the council's objectives will be to promote sustainability initiatives, which could involve renewable energy audits for cryptocurrency miners.
#1.12 Data Integrity	Data integrity can be defined as data with representational faithfulness. With the increasing focus on data and its distribution to the cloud, data warehouses, and machine learning algorithms, external and internal audits of data integrity are becoming essential. Due to the variety of data processed by today's systems, there is a risk of data loss, especially in online systems which requires completeness verifications (e.g., revenue audits). Format mismatches can lead to errors in data processing which requires verification of validity and correctness of the data processed. A data integrity assurance engagement evaluates the completeness and accuracy of a description of the data and provides assurance on whether the data is consistent with the description, including its fitness for the intended use of the data and its completeness, accuracy, validity, and currency.
#1.13 XBRL	XBRL is an international standard for digital business reporting (paper-based reports with more effective, accurate, and useful digital versions). It simplifies the way people use, share, analyze, and add value to data. The service allows unique tags to be associated with reported facts which allows people who publish the reports to be confident that the information contained in the report is usable, accurate, and can be analyzed. It also allows people who use the reports to test it against logical business rules to detect mistakes at their source. It allows convenient reading of reports for people who wish to access them in different languages, alternative currencies and in their preferred style. Typically, engagements are either to support companies in coding their financial statements with the standardized coding scheme, or to help validate the information that has been coded (see summary: https://www.xbrl.org).
#1.14 Cryptocurrency	A Proof of Reserves (PoR) provides assurance that a digital asset platform (e.g., exchanges like Kraken and custodians like BitGO) or custodian has sufficient

Asset Holding – Proof of Reserves	digital assets on hand to cover customer balances (i.e., assets equal or exceed liabilities). Technology-enabled tools have been developed to facilitate the audit of transactions and balances arising from cryptocurrency mining activities. These technology-enabled tools support the auditors in obtaining evidence related to mining-related transactions and balances. For example, these tools can evaluate mining capabilities (e.g., the hash rate) to evaluate the reasonableness of a miner's reported revenues.
#1.15 Data Trust	A Data Trust can steward, maintain and manage how data is used and shared — from who is allowed access to it, and under what terms, to who gets to define the terms, and how. The purpose of a Data Trust is to distribute the benefits arising from data more equitably and create collective power over data. Data Trusts are legal entities created to hold data and provide access to it in accordance with specified terms. An independent person or group of people called 'trustees' take on a duty to make decisions about the data in the best interests of a third group called 'beneficiaries'. The beneficiaries of the data trust include those who are directly provided with access to the data, such as project delivery organizations, researchers and developers. The key aspects of data that data trusts aim to manage are data protection, privacy, confidentiality, intellectual property rights, and contractual obligations. Trustees and beneficiaries also want to ensure the data integrity and security of the Data Trust, which is where audits come in. As the service area is still evolving, the nature and scope of the audits are variable. Some of the audits are more like reviews in terms of the nature, timing and extent of evidence gathered.
#1.16 Data Seal / Privacy Seal	A data seal is attached to data to ensure its authenticity. It is similar to a real seal put on a piece of paper to ensure the authenticity of the document, but instead of a real seal, it is a secured digital seal on a digital document. Privacy Seal is a special type of data seal that certifies that the company is in compliance with the data privacy regulation. The seal is the deliverable for this service.
#1.17 Fake News Check	Fact checking and credibility ratings for news content, including images, video and textual information. Change records are also available to track the alterations and origins of information to help judge credibility. Focus on the veracity of the information using the credibility of the source documentation and evidence of alterations to the source documents including videos and pictures.

#1.18 Real-Time Internal Audit	Real-time or continuous internal auditing intends to perform control and risk assessments on a frequent basis. A desire from stakeholders to have accelerated audits or monitoring of activities drives demand for real-time audits. The performance of this engagement typically requires practitioners to have significant technological infrastructure including data analytics tools to evaluate and then conclude on the evaluation of numerous and varied risks, information, transactions, or controls in short order. Real-time internal audits evaluate whether transactions and activities are being performed in accordance with company policy and/or whether systems and controls are operating effectively and as intended. While practitioners may perform this engagement, they also offer tools/software or assist companies to develop their own real-time internal audit processes or programs, to facilitate self-monitoring or self-assessments in real-time.
#1.19 Real-Time External Audit	Real-time external auditing intends to opine on subject matter in an on-demand manner by collecting audit evidence in real-time. To do so, the service provider requires significant technological infrastructure including data analytics tools. Adoption of real-time external audits also requires that service providers be able to make real-time changes to the audit plan and scope of the engagement. While real-time audit or attest reports typically apply to audit opinions on fair presentation of financial statements, they can also be prepared for review opinions (lower level of assurance) or for agreed-upon procedures and other subject matter (e.g., internal control or compliance audits), provided the assurance provider is an independent external party.
#1.20 Gene & Biocomputer Assurance	Gene assurance services and biocomputer assurance services exist at a theoretical level. Gene assurance corresponds to gene testing and editing processes. Service providers verify the process and the result to ensure the accuracy of the outcome. Biocomputer assurance corresponds to the construction/functionality of a biocomputer. It assures that the biocomputer is constructed and functions as intended.

Appendix 2: Technology-Neutral Services

Service Name	Service Description
#2.1 ESG/CSR/Sustainability – Assurance Focused	Environmental, Social, and Corporate Governance (ESG)/Corporate Social Responsibility (CSR)/Sustainability (here onwards referred to as ESG) assurance services are special assurance engagements that provide assurance over ESG risks by evaluating and verifying an organization's ESG policy, system, data and disclosures (e.g., SGS n.d.; SGS n.d.). There are two types of ESG assurance – ESG verification and ESG certification. ESG verification service providers validate ESG data and disclosures, whereas ESG certification providers assess ESG policy, system, data & disclosure against ESG standards and criteria established by third parties or providers themselves (e.g., SGS, n.d.; SGS, n.d.).
#2.2 ESG/CSR/Sustainability – Non-assurance Focused	ESG non-assurance services are a collection of services that help organizations understand their impact on environment and society, set and achieve their ESG goals, and take advantage of their ESG achievements. ESG non-assurance services include but are not limited to the following aspects (e.g. Bain & Company n.d.; PwC n.d.): 1) Strategic planning, 2) Governance, risk & compliance, 3) Policy & economics, 4) Sustainable development goals, 5) Supply chain & operations, 6) Total impact measurement & management, 7) Reporting, 8) Tax, 9) Investing.
#2.3 Non-GAAP (Financial) Measures	Many entities disclose non-GAAP financial measures (e.g., adjusted earnings, EBITDA, free cash flow). These measures provide users with additional insight into a company's financial position, financial performance, or cash flow. In May 2021, the Canadian Securities Administrators (CSA) released NI 52-112 on disclosures related to non-GAAP financial measures. Auditors could be engaged by the audit committee to perform agreed-upon procedures related to the preparation of these measures and related disclosures. Auditors could also be engaged to perform an engagement to form a conclusion on management's compliance with disclosure requirements like those described in NI 52-112.
#2.4 Measure of operational performance	Generally, performing an audit of measures of performance involves assessing and concluding on the effectiveness of the company's measurement system, and recommending potential improvements to its system. This service is effectively another form of non-GAAP measurement except that it is more about operations and less about other financial measurement numbers that can be provided in an annual report.

#2.5 Valuations	Valuation reports provide assurance related to the value of a business, which can be used to support decision making (e.g., sale of a business). There are three types of valuation reports that provide varying levels of assurance: comprehensive (high assurance); estimate (moderate assurance); and calculation (low assurance). Depending on the type of report (comprehensive, estimate or calculation), the practitioner reviews all relevant information about the business to arrive at their conclusion.
#2.6 Value Creation Services – Indicators	Value creation services in general are intended to help companies understand its various value streams, which include financial or economic, non-financial, social, and environmental activities. These services can also help companies assess the impact of its business on those areas. Such services are non-assurance related and often involve measurement (and to some extent reporting) of value created in the company to provide the company richer information to leverage in making strategic business decisions. However, value creation services can leverage accounting/auditor practitioner skills in financial reporting and measurement to areas other than financial ones – areas where companies have been slow to or ineffective at measuring (and reporting). Deal advisory services sometimes also measure or assess value creation in the process of determining a company's acquisition value.
#2.7 Value Creation Services – Special reports	At least two types of special reports re: value creation could exist: 1) assurance reports on a company's integrated report (which includes areas other than financial reporting) and 2) advisory conclusions on company deals (e.g., related to deal analytics and M&A, tax, or private equity services). If a company prepares an integrated report (IR), practitioners can provide an assurance report on the IR subject matter. If related to deal advisory, practitioners can provide a report with analysis and recommendations on opportunities for value creation (and possibly how to pursue these opportunities).
#2.8 Business Model Descriptions (BMD) – Attest to Integrity of BMD	UK reporting entities must disclose their business model in their Strategic Report to explain how the entity creates value for stakeholders. The IIRC, AICPA, IFAC and IFRS also emphasize the role of business models in external reporting. Business model evaluation services use a framework against which an entity's business model or strategy components are matched, risks are identified and evaluated. Although many such services are called audits, they are performed by a

	variety of service providers, not necessarily CPAs. Business model audit services terminology is also used for evaluations of financial models.
#2.9 MD&A	Public companies are required to file MD&A related to its annual and interim financial statements. Auditors could be engaged to perform an attest engagement to form an opinion or conclusion on whether the MD&A is prepared in accordance with the specified requirements like those described in NI 51-102 and NI 51-102F1.
#2.10 Risk Assessments/ERM (Enterprise Risk Management) Program Assessment	While risk assessment is a common component seen in various assurance or advisory services, the focus here is the assessment of an organization's ERM program. The nature of the engagement may be advisory or assurance but assessing ERM controls is a common internal audit engagement. The purpose of the service is to examine the effectiveness of organizations' ERM and help organizations improve their ERM.
#2.11 Internal Control Reports	The purpose of this service is to assess effectiveness of internal controls implemented by organizations. It may be specific to internal controls over financial reporting, and it may be for internal controls over other areas (especially in digital technologies). This service allows firms to 1) monitor risk and take remediating actions if controls are ineffective; 2) demonstrate their transparency and effectiveness to customers and partners within their supply chain. An assurance report can be generated to document the effectiveness of these controls.
#2.12 Compliance with Best Practices/Standards	These services help companies identify and comply with various best practices/standards in their industry, which may range from production quality to information security to occupational health and safety. An audit that certifies compliance with the applicable standards would cover inspection and testing of processes and frameworks related to the area of business where compliance is desired. Unlike compliance with laws and regulations, compliance with best practices/standards is voluntary.
#2.13 Compliance with Laws and Regulations	These services help companies comply with business- or industry-specific laws and regulations. In order to conduct business, these laws/regs must be adhered to. Beyond reviewing or auditing company policies, procedures, practices, etc. to ensure compliance these services may include assisting companies to create compliance strategies, programs, policies, activities, risk frameworks &

	assessment, and monitoring. Various reports can be issued for such services, depending on the type of laws and regulations and the nature of service. Unlike compliance with best practices/standards, compliance with laws and regulations is mandatory.