CPA Australia Ltd

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677

Website cpaaustralia.com.au

3 July 2020

Financial Reporting Council
Jason Bradley
8th Floor
125 London Wall
London
EC2Y 5AS
United Kingdom

Via online submission: AAT@frc.org.uk

Dear Jason

Discussion Paper: Technological resources – using technology to enhance audit quality

CPA Australia represents the diverse interests of more than 166,000 members working in over a 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

Technology is altering the audit environment substantially, and this change is accelerating. We consider that it is critical for audit firms, both large or small to medium-sized, to embrace this digital transformation to remain high-quality service providers, and to be competitive and relevant. In our view, technological change will enable improvements in audit quality and transformation of the audit product to better meet entities' expectations and financial statement users' needs into the future. It would be preferable if standard-setters and regulators were enablers of, rather than onlookers to, that transformation. Therefore, we welcome the Financial Reporting Council (FRC)'s consultation.

Although CPA Australia's members work predominantly in Australasia and Asia, we are responding to the FRC's consultation paper as it raises important issues which audit firms are facing and which need to be, and to varying degrees are being, considered by other national standard-setters, as well as the International Auditing and Assurance Standards Board (IAASB). Discussion and thought leadership on effective use of technology in the audit, and removal of impediments of its use for auditors whilst managing the risks, are important. However, solutions need to avoid creating new impediments to innovation.

To inform this submission CPA Australia conducted outreach to members and other stakeholders in Australasia, principally comprising an online questionnaire, followed by meetings with a number of the respondents to gain deeper insights. Uptake of technological tools in audits in Australasia is still in its early stages for many firms, but is rapidly increasing, with small to medium-sized firms either using less sophisticated tools or being more reliant on third-party providers than the larger firms, which are using tools predominantly developed in-house. Whilst this may enable small to medium-sized firms to be more agile in their use of technology, it also exposes them to greater risks due to that reliance on third parties.

Our detailed responses to the questions raised in the paper are contained in the attachment to this letter.

If you require further information on the views expressed in this submission, please contact Claire Grayston, Policy Adviser Audit and Assurance at [redacted] or Dr Jana Schmitz, Policy Research Analyst at [redacted]

Your sincerely

[redacted]

Dr. Gary Pflugrath
Executive General Manager, Policy and Advocacy

Attachment

Question 1: Do you agree that the increasing use of technological resources, including AI and other advanced tools, enhances the quality of audits, beyond the benefits derived from efficiency gains. If so, what are the indicators of enhanced quality?

We believe that the use of technologies such as Robotic Process Automation (RPA), Artificial Intelligence (AI) and Data Analytics (DA) in audit has the potential to increase audit quality. The potential positive impacts on audit quality stem from a range of opportunities provided by these tools. For example, technology enhances the auditors' ability to extract and navigate client data at a faster rate and to identify material exceptions based on the analysis of the full population of clients' transactions, which provide deeper insights and frees up time to develop more in-depth risk assessment and understanding of the client. Below, based on the feedback we received from CPA members and other stakeholders, we elaborate in more detail on identified indicators of enhanced audit quality. However, while we acknowledge the potential of technology to have positive effects on audit quality, we also note several potential concerns.

- **More holistic and structured audit approach**: Through the use of technologies such as RPA and DA in the audit process to extract, filter and review client data, it becomes possible for auditors to start analysing client data early in the audit process. In turn, this enables auditors to better tailor the audit approach, review and re-assess audit evidence on a continuous basis, and deliver higher quality audits. More advanced AI-enabled technologies support a forward-looking, dynamic process of identification of anomalies and fluctuations, thereby pointing auditors towards higher risk areas.

  Members and stakeholders have told us that by using technological tools – either built in-house or provided by third-party technology vendors (see also our response to **Question 13**) – audit firms are pursuing a progressively more structured approach where several audit tasks are automated, and the execution of the audit process is tracked by predesigned templates. These templates allow each assigned auditor to keep track of the different stages of the audit process, and to understand analysed data.

  However, the use of technology may lead to auditors only focusing on the issues identified by the employed technologies and not to consider other factors or issues not identified by those technologies. Auditors' overreliance on technology may in fact have negative effects on audit quality (see our response to **Questions 3** and **8**).

- **Full population testing**: Technologies' capabilities to test entire populations of transactions allows auditors to assess broader sets of data and, therefore, produce more reliable audit evidence. Importantly, by automating the processing of data and executing audit tests on the full population of records, RPA can more efficiently detect anomalies and offer auditors the opportunity to more precisely measure the risk of material misstatement in a timely manner. However, technologies may produce large volumes of exceptions, which may, or may not, negatively affect audit efficiency and quality (see our response to **Question 12**).

- **More time for high-value tasks**: Outsourcing mundane audit tasks to deployed technological tools can free up time for auditors to concentrate on complex issues and concerns that require professional judgement.

Question 2: Do you believe that challenger firms are currently at a disadvantage in the use of new technology? If so, what remedies would you suggest?

We observe that primarily large audit firms are making significant investments in developing and building technological tools in-house. The underlying technologies of these in-house built tools range from Excel add-ins and automated audit data extraction tools, to more sophisticated DA and data visualisation tools, as well as AI-tools with integrated ML capabilities. Many challenger firms (we refer to them as small and medium-sized audit firms) have historically been disadvantaged as they may not have access to the required financial and/or human resources to build and implement such tools in-house. In-house tools often involve high development and/or implementation costs of technology, as well as a required level of expertise and provision of in-house training. Therefore, these small and medium-sized audit firms have been lagging behind in the technological advancement of the audit profession. This may lead to concerns that the audit profession will experience an increased inequality in the technological advancement between the larger audit firms and the small and medium-sized audit firms.

However, we see this imbalance starting to shift as the availability of affordable solutions from external software and IT service providers start to proliferate, making technological solutions increasingly accessible to small and medium-sized audit firms. Those representatives of small and medium-sized audit firms who responded to our outreach activities, explained that their firms invested significant amounts in “off-the-shelf” tools provided by third-party technology vendors. Some of those third-party technology providers/tools named by respondents are: Teammate Analytics, Power Bi, UiPath, CaseWare, MindBridge, inflo, AuditDashboard and IDEA. Whilst services provided by third-party technology providers allow small and medium-sized audit firms to leverage the advantages of technological tools for the audit, often at a lower price than building tools in-house, there are several challenges associated with the use of those tools that must be considered. For instance, small and medium-sized audit firms may face challenges in the implementation and utilisation of such tools and may become dependent on third-party technology providers to train auditors how to use them. In turn, this could drive small and medium-sized audit firms into an undesired dependence on third-party technology providers. Further, as users of such tools, small and medium-sized audit firms are exposed to potential risks and challenges relating to data security and data ownership. We address those and other issues and challenges in our response to **Question 13**.

Question 3: Other than investment, what do you believe are the key challenges auditors face in the increasing utilisation of automated tools and techniques within the audit process? Again, what remedies would you suggest to overcome these challenges?

Based on feedback received, we identified several key challenges auditors face when utilising different technologies in the audit process. Those challenges are related to: (1) clients’ unwillingness to provide data, (2) data provided in unusable form, (3) overreliance on technology, (4) assurance over controls, (5) compliance with auditing standards, (6) data security, and (7) stakeholder confidence.

- **Client unwilling to share data:** As audit clients are often not sufficiently technologically advanced, it is not unusual for them to be hesitant to provide data digitally through client portals or audit technology platforms, particularly if those portals or platforms are cloud-based. Often, this is due to clients’ data confidentiality and data privacy concerns. From respondents’ feedback it also emerged that clients often express concerns about the storage of competitively sensitive data on the cloud and the risk of data security breaches in this regard.

- **Format and consistency of client data:** The format and consistency of data provided by clients can be problematic with it often being uploaded onto the audit firms’ technology platform in an unusable form. In such situations, auditors are required to undertake extensive data cleansing, which is often conducted manually. When auditors are required to intervene in the extraction or ingestion process manually, audit efficiency may be impacted. Respondents reported that the challenges of extensive manual data cleaning can be overcome by using RPA tools that identify the relevant data from client data uploaded onto the auditors’ technology platform and populate the required data fields. If greater levels of automation are desired, AI-enabled RPA tools can be employed, which may be even more useful for data extraction or ingestion purposes as the AI algorithm self-evolves based on the client data characteristics (see also our response to **Question 8**). According to respondents, this requires auditors to understand how, and on which historical client data, the AI-algorithm trains itself.

- **Overreliance on technology:** Our survey results have shown that auditors are often not overly “tech-savvy.” Where auditors lack technology expertise it poses the behavioral risk of overreliance on technology, whereby the use of technology may diminish the development of appropriate critical thinking, application of professional scepticism, and manual intervention. In particular, junior audit staff with limited experience in exerting professional scepticism and lacking expertise in using technology in the audit process, may adopt a higher degree of overreliance on technology compared to more experienced auditors with an extensive history of practicing professional scepticism. For such reasons, it is essential to not only teach auditors how to use technology in the audit process, but to also educate them about the limitations of technology (see our response to **Question 5**).

- **Assurance over controls**: Two assurance-related challenges were identified through our outreach activities. One challenge is the inability to obtain assurance on controls over, or the logic of, underlying data extraction tools. Control over the integrity of the data extraction tools is critical and often overlooked. The other identified challenge is the inability to obtain assurance over the operating effectiveness of controls within the technology, pre-determined algorithms within analytical tools (such as DA and RPA) or algorithms which evolve during the audit process (such as AI and ML). The key issue is that due to the complexity and continuous self-evolution of AI and ML tools the basis of their decisions is not always evident to auditors. Consequently, auditors are confronted by the risk of relying on technological tools that are inaccurately processing data, processing inaccurate data, or both (see also our response to **Question 8**). This could be overcome by the auditor seeking an expert report on the controls or logic within the systems used to extract and process data.
- **Compliance with auditing standards**: When using technology in the audit process, auditors need to be confident that the technology enables compliance with the auditing standards. Whilst some of our respondents argue that the current audit model is not broken and that auditing standards are, in fact, sufficiently 'flexible' to allow for the deployment of technology in the audit, others have expressed concerns over the way that the use of technologies may lead to required adjustments to certain aspects of auditing. For example, these adjustments may affect the understanding of materiality and risk factors. In particular, the use of off-the-shelf services provided and controlled by third-party technology vendors may create challenges (see our response to **Question 13**). The IAASB expressed concerns about third-part technology services posing challenges not adequately addressed by current standards (see also our response to **Question 4**).
- **Data security challenges**: The challenge of audit staff gaining access privileges beyond those necessary to perform their assigned duties is another challenge faced by audit firms. We address this issue in our responses to **Question 6** and **Question 13**.
- **Stakeholders' confidence in audit results:** When audit firms advertise their use of technology to, for instance, inspect the full population of transactions, investors' and other stakeholders' expectations may change. That is, their expectations may move from believing that auditors are providing reasonable assurance towards auditors providing "full assurance." In other words, references to 100 per cent testing may be misleading in some instances.

Based on feedback received from CPA members and other stakeholders, we propose the following "**remedies**" that may be helpful in addressing some of these challenges:

- **Controls over data extraction tools**: The logic of data extraction tools should to be reviewed on a frequent basis and confirmed by a specialist to ensure that the data extracted is accurate. Care must also be taken that inappropriate changes are not made to the logic, either accidentally or deliberately. In cases where the audit procedures are very sensitive, access should be limited to selected audit staff and/or the analysis code for critical test steps can be encrypted so that full security is maintained.
- **Guidance material:** We emphasise the need for guidance material to assist in the purposeful use of technology for audit. Such guidance material should elaborate on:
  - the way technology can and should be employed in the audit process
  - the level of disclosure of how and to what extent technology has been used in the audit
  - what monitoring controls audit firms should put in place for the different technologies (e.g. DA, AI, RPA) and different levels of technologies (e.g. assisted, augmented or autonomous AI)

  - how frequently the technology employed is monitored and, if necessary, adjusted (e.g. code in RPA bots is changed)
  - how data security is ensured
  - the ethical principles auditors to which need to adhere, and
  - what controls should be put in place to ensure that the output of technologies is compliant with auditing standards.

  The Audit and Assurance Standards Board (AUASB) in Australia is currently developing guidance material to respond to emerging issues related to the use of technology in audit. The objective of this guidance material is twofold: (1) to support the use of technology by auditors in executing audits, and (2) to support auditors in auditing the outputs of technology used by their clients in areas critical to the audit. As other jurisdictions are also working on standards and guidance for auditors, including the Canadian standard-setter and the American Institute of CPAs, we encourage the UK FRC to foster cross-border collaboration between national standard-setters to leverage each other's work (see also our response to **Question 4**).

- **Managing stakeholders' expectations:** Auditors should provide some level of transparency about the kind of technology used in the audit process (e.g. RPA, AI, DA), the extent to which that technology or those technologies have been used (e.g. assisted, augmented or autonomous AI), and for what parts of the audit process technology has been used (e.g. client data extraction, full population testing). Transparency about the capabilities and limitations of technologies used would assist in establishing a common expectation of the level of assurance provided in an audit environment that utilises technologies.

Question 4: Does the current assurance model or the auditing standards represent an obstacle to technological innovation? If yes, then what specific standards, objectives, requirements or guidance cause practitioners particular difficulties?

We believe that whilst the current assurance model and the auditing standards do not represent obstacles to technological innovations per se, they do not appear to promote or facilitate technological innovation. As we consider that technological innovation is a means to improve audit quality, technology should not be simply possible under the auditing standards, but should be actively encouraged. In addition, technology will be the means by which the audit product can evolve to better meet user needs, such as continuous auditing, full population testing and mining of big data to identify risks or anomalies and gain new business insights. Assistance for auditors by providing clear guidance on the use of technological tools in the audit, and which addresses the identified challenges, would be important to encourage uptake of existing tools in the first instance and future innovation. This guidance material could address the usability, as well as limitations, of different technologies for audit purposes, as well as the challenges. These challenges include, but are not limited to, documentation, evidence of the operating effectiveness of controls over and within the technologies applied (including the underlying algorithms), handling of high volumes of exceptions and the reliability of new data sources, such as big data (see also our responses to **Questions 3**, **8** and **12**).

Question 5: Do you believe the current level of training given to auditors – both trainees and experienced staff – is sufficient to allow them to understand and deploy the technological resources being made available?

Respondents to CPA Australia's outreach activities strongly agree that auditors require further training in technology to obtain sufficient technical competence to understand how each technological tool works. As well as knowing about tools' limitations, auditors need to know how to effectively implement it, use the output appropriately as audit evidence, identify the gaps in evidence and apply professional scepticism in an informed way, so that the technology improves audit quality. As mentioned earlier, insufficient understanding of technologies and their key functions and limitations may lead to auditors' overreliance of technology in the audit process.

Technology training, as the results of our outreach activities suggest, should either be delivered in-house – provided that audit firms have capacity to provide educational training – or provided externally by universities and professional accounting organisations (PAOs).

Participants suggest that PAOs should play an instrumental role in offering auditors opportunities through conferences, webinars, continuous professional development programs or other focused learning engagements, to acquire technology skills. Respondents also agree that professional qualification programs, such as the CPA Program, would be a suitable platform to provide learning and training material to support auditors to acquire relevant skills in the increasingly technological auditing environment.

Further, we believe that the audit profession would benefit from universities embedding technology-related subjects in their accounting curriculum. That does not imply that accounting degree graduates need to know how to code. However, they should be educated about how different technologies work and what their benefits and limitations are in the context of auditing. These educational steps would help equip the upcoming generation of accounting graduates with skills relevant for the future of the profession. We are aware that several universities have partnered with third-party technology providers. While we generally support this development, we also emphasise the need to develop technology skills more broadly. Teaching how to use a particular third-party technological tool may create competitive disadvantage in talent acquisition for those audit firms which do not employ that particular tool.

Microcredentials, which are basically mini-qualifications that demonstrate skills in a specific subject area, have also been mentioned as source of potentially providing required technology training.

Lastly, respondents highlight that due to the fast pace of technological advancement, the suggested sources of learning and training should adopt a lifelong learning model, which captures the latest technological developments.

Question 6: What firm-wide controls do you believe are appropriate to ensure that new technology is deployed appropriately and consistently with the requirements of the auditing standards, and provides high quality assurance which the firm can assure and replicate more widely?

Respondents to our outreach activities emphasise that controls over technology deployed by the audit firm need to address:

- leadership responsibility and approval process for deployment of new technology
- staff training and communication regarding new or ungraded technology
- adoption of strict data policies
- restricting physical and logical access to technology and client data to protect confidentiality, privacy, data security
- testing the functionality of the technological tool, including the coding and algorithms to ensure it operates as designed
- manual checks of selected client data sets processes by technological tools to ensure the functionality of those tools
- mapping of technological tools deployed to previous audit procedures which they are replacing, audit assertions they address and the specific requirements of the auditing standards, and
- for technology from third-party providers (see also our response to **Question 13**):
    - contractual arrangements with third party providers and evidence of compliance to address risks, such as confidentiality, privacy, data security (including firewalls, anti-virus software, backups and physical security), data ownership, continuity, technical support, and
    - testing for trial periods prior to implementation.

Question 7: Are you aware of the use of new technologies in analysing and interpreting information provided by auditors – including, for example, auditor's reports? If yes, then do you foresee implications for the form and content of auditor's reports?

CPA Australia has been advocating for the electronic lodgement of annual reports with the regulator in Australia so that they can be readily compared and analysed by the market. We consider that transparency and comparability in reporting should improve, not detract from, information quality overall. This would also enable comparisons of auditor's reports, including the wording of key audit matters and modified opinions. We consider the potential downsides of technology being used to compare auditor's reports, such as the potential for boilerplate or copycat reporting, is outweighed by the benefits of transparency. For example, in understanding easily the entities impacted by a material uncertainty relating to going concern or the most common key audit matters identified.

Question 8: What do you see as being the main ethical implications arising from the greater use of technology and analytics in an audit?

With auditors increasingly utilising technologies such as RPA, AI and ML, that often use sophisticated self-evolving algorithms, potential ethical implications and unintended consequences may arise from the choices inherent in the coding of the algorithms.

Auditors' potential **overreliance on technology** is one challenge, where auditors who increasingly use audit technology may make the assumption that the underlying technology not only operates accurately, but that it provides all of the evidence needed. They then assume that it can be relied on, when in fact it requires further evaluation or addresses only certain assertions. Moreover, auditors may assume that the RPA bot or the AI-algorithm always behaves within the desired constraints. Another assumption auditors may make is that the divergence from desired constraints will be detectable and correctable. These assumptions may not always hold, but in fact, result in ethical implications (as well as economic and even legal implications). Academic studies by Skitka et al. (1999) and Munoko et al. (2020) have found that two types of errors can occur when technological tools such as automation are used. These errors could either be of *omission* or *commission*. In the audit, errors of omission may arise when auditors fail to take appropriate action because the technology fails to inform them that such action was required, despite non-automated indicators of the required action. Errors of commission occur when decision-makers follow directives given by the technological tool, even though there are more valid non-automated indicators suggesting that the system is wrong. Hence, as mentioned in our response to **Question 3**, as the utilisation of technology increases, auditors risk relying on technology that is inaccurately processing data, processing inaccurate data, or both. Auditors' overreliance on technology can contradict their exertion of professional scepticism.

Auditors' overreliance on technology may lead to the potential "**deskilling**" of auditors. In other words, as technology is expected to increasingly take over the more routine audit tasks, it is crucial to consider whether these routine tasks provide junior auditors with required learning and experience that shape their skills in adopting critical thinking and applying professional scepticism. For these reasons, and the reasons elaborated on in our response to **Question 5**, we believe that technology education and training should supplement accounting and auditing education and training, but not replace it. This would be a critical step towards ensuring that junior auditors are technically competent and able to utilise technology appropriately, and without its use impairing their professional judgment.

Audit firms' graduate trainee programs should not neglect teaching novice auditors tasks such as the manual checking of transaction records, even though such tasks may be automated. This way, auditors would be more inclined to perceive technology as a complement to their professional judgment and exhibit an appropriate level of professional scepticism. By removing 'manual' or 'routine' tasks from junior auditors' training, their professional judgment may not be as well developed as that of their counterparts who did not rely on advanced technological tools.

Ethical implications on the broader audit profession may also arise from **data security breaches** often caused by **unauthorised access to data**. Such breaches may result in the destruction of data, unauthorised access to confidential, commercially sensitive or private client data, or improper changes to client data. Unauthorised access to data can significantly compromise audit quality. Beyond that, audit clients may lose trust not only in the audit firm and its engagement partners, but in the audit profession more generally. Some of the safeguards we suggest in our response to **Question 13** may address the issues of data security breaches and unauthorised access to data.

Another ethical implication likely to arise from the greater use of technology and analytics in audit is related to audit firms generating economic benefits by collecting and storing significant amounts of client data using technological tools. Such data may encourage and support audit firms' **cross-selling of non-assurance services (NAS)** to audit clients. We emphasised the potential threat to auditor independence and potential conflict of interest emerging from the provision of NAS to audit clients in our 2019 submission to the inquiry by the Parliamentary Joint Committee (PJC) on Corporations and Financial Services Inquiry Regulation of auditing in Australia.

Finally, the process of data extraction or ingestion of client data can involve intensive cleansing of the data to bring it into useable format (see our response to **Question 3**). This process could pose a self-review threat to independence.

Question 9: Do you believe there is value in the UK having consistent data standards to support high quality audit, similar to that developed in the US?

No comment.

Question 10: Do you agree that threats to auditor independence may arise through the provision of wider business insights (not as part of the audit itself) drawn from the interrogation of company data? If so, what measures would mitigate this risk from crystallising?

At this stage in the technological advancement of the audit profession, one potential threat to auditor independence we have identified relates to auditors' potential overreliance on technological tools used in the audit (see our responses to **Question 3** and **Question 8**). Another potential threat may emerge from the auditors' intentions to cross-sell services not related to audit (see also our response to **Question 9**). Some audit firms may take advantage of technology to generate wider business insights and identify opportunities for providing NAS to clients. Nevertheless, there are benefits in the auditor sharing with clients the insights they have gained from the DA or AI they have applied in the audit, in much the same way as a management letter. However, ethical concerns arise if the auditor was to try to "sell" to the client the DA they have developed and the client was to become reliant on the auditor's technology to provide management information.

Question 11: Do you agree that audit documentation can be more challenging when an audit has been conducted with automated tools and techniques? If so, please identify specific areas where there is a problem.

Participants in CPA Australia's outreach activities have highlighted that the use of technological tools can often make audit documentation more challenging. Some of the identified issues emerging when technology is used in the audit process, are listed below.

- **Controls over technological tools**: Technological tools employing AI and/or ML applications are often difficult to control due to their self-evolving algorithmic functions that are often described as "black box". This is particularly so when platforms/services provided by third-party technology vendors are used. Auditors often experience difficulties in obtaining controls reports from those vendors documenting that the tool provides reliable and relevant evidence (see also our response to **Question 13**).
- **Unclear documentation**: There is a risk that the auditor does not document sufficiently clearly *how* the technology has been employed, and *what* it has been used for. More precisely, it has been noted that sufficient

detail is not provided about how technology has been used for risk assessments or tests performed as part of the audit.

- **Documenting functionality of tools**: Limitations on access to the criteria and parameters, assumptions, algorithms, functionality and security underlying the tools from external providers, including version control over DA tools applied or AI algorithms, which have the added challenge of being iterative.
- **Data retention**: Determining the extent of client data to be retained and retention periods when large volumes of client data have been extracted, or if the data is not retained, suitable methods of identifying the client data and documentation relied on for the audit. Data retention also creates data security risks.
- **Documenting sampling**: Demonstrating the testing applied, which may be done through a number of filters when high volumes of exceptions are generated.

Question 12: Have you encountered challenges in dealing with the volume of 'exceptions' arising from the use of more complex or comprehensive data analytic procedures?

According to respondents to our outreach activities, the challenges presented when a high volume of exceptions or outliers is generated from use of a technological tool are:

- **Compromised audit efficiency and quality**: Some respondents outlined that when high volumes of exceptions or outliers are detected, auditors are required to perform additional work. Also, due to time constraints, the amount of exceptions and outliers that auditors analyse remains small, and so auditors effectively leave unexplored much of information that is labelled as exceptions and/or outliers. While the former indicates that large volumes of exceptions compromise audit efficiency, the latter indicates that audit quality may be affected if exceptions are unexplored.
- **Requirement for further testing**: Challenges relating to testing of large volumes of exceptions include: the extent of further testing on exceptions needed to reduce risk of material misstatement to an acceptable level, and technological tools identifying false positives as outliers. This can often lead to an increased volume of work for auditors and hence higher audit costs.
- **Determining criteria and parameters**: The determination of suitable criteria and parameters for iterative procedures on exceptions or outliers has also been identified as challenge by respondents.
- **Tolerable rate of deviation**: Large volumes of exceptions and outliers require auditors to re-evaluate and re-define the tolerable rate of deviation.
- **Lack of required competence and expertise**: Several respondents reported that some of the audit staff (junior and senior) are often ill-equipped to deal with large amounts of exceptions, and commonly face challenges from information overload and experience difficulties in distinguishing relevant data.

Overall, CPA members and other stakeholders responding to our outreach activities stated that the development of an efficient work flow management process around exception identification, validation, and resolution is essential to effectively managing volumes of exceptions. In this regard it was further emphasised that while technology is becoming an increasingly essential element in audit, particularly when it comes to full-population testing, manual involvement by auditors remains important in situations where extensive judgment is required and where anomalies, exceptions, and outliers are identified. The perceived benefit gained by auditors through the process of evaluating and filtering those exceptions has been to better understand the client's business and its dataset, which results in improved audit quality. The understanding gained in the initial years of using technological tools in a particular audit enables better filters to be applied or better targeted techniques applied, which results in greater efficiency.

Question 13: Do you agree that the use of third-party technology vendors raises potential ethical challenges for auditors and, if so, which potential safeguards would you see as effective in reducing this threat to an acceptable level?

We agree that the use of third-party technology providers increases potential vulnerabilities, which may present a range of ethical challenges for auditors. Ethical challenges highlighted by respondents relate to data ownership, data security policies, and independence issues.

With regards to the **ownership of client data**, results from CPA Australia's outreach activities show that auditors consider third-party technology providers' use of client data to build machine learning tools and train AI-algorithms, presents ethical challenges. Being able to utilise client data for purposes other than those intended (that is, for audit) could mean that third-party technology providers may benefit commercially from the client data to which they obtain access, for example, to attempt to cross-sell their services. The fact that third-party technology providers are working directly with clients to extract data without necessarily being required to comply with the Ethical Standard, reinforces this potential ethical challenge faced by auditors.

Further, what becomes ethically challenging for auditors is when **data security breaches** occur on the third-party technology provider's platform. Third-party technology providers' loss of control over data security can have severe ramifications for audit firms, including regulatory penalties, loss of reputation and damage to business operations and profitability. When using third-party technology software, auditors need to make sure that client data is protected from risks related to the commingling of data from multiple clients. Client data saved on third-party technology providers' cloud storage may be exposed to the risk of commingling of data.

Respondents also mentioned self-review threats to independence if the third-party's technological platform/services becomes integrated by the client in to their management information system, which may effectively form part of their control systems.

Based on these concerns and potential ethical challenges, we propose the following **safeguards**:

- **Involvement of the Risk Committee**: Prior to their use, services provided by third-part technology vendors should be reviewed and approved by the risk committee, which should include IT experts. Understanding and addressing potential risks and challenges as part of a broader and robust risk management approach is an essential step in mitigating the risks outlined above.
- **Data security policy and confidentiality agreements**: Limiting the amount of data provided to third-party technology vendors to only relevant data that is required to perform the necessary processes may – to an extent – prevent third-party providers from repurposing that data. Limiting the amount of data to essential data should also involve removing sensitive data. Further, data handling policies should include the restriction of access to data and the monitoring of when data is accessed and by whom. Whether the third-party provider has adequate data security controls in place to protect client data needs to be assessed prior to their engagement. This information should be captured in the confidentiality agreement as part of the contractual arrangements with the vendor.
- **Storage of data**: Users of third-party technology services should review the provider's data transmission and storage policies. As such, it is relevant to assess where the data resides within the provider's system or cloud. Questions that should be asked are: Does the provider store the data on its own servers? Does the provider use a cloud storage? Does the provider transmit the data using proper encryption? How will data be transmitted between the third-party provider and the firm, and for what part of the transmission process is the third-party provider responsible/at risk? For how long will the data be stored on the third-party technology providers' servers and/or cloud? Whilst many third-party providers store client data on the cloud, users of third-party providers should consider storing the data on-site in addition to using the third-party provider's data storage.

- **Ownership of data**: Audit firms should address ownership issues and the third-party technology provider's right of use of client data. Clearly defining ownership of the data can prevent third-party providers making use of client data to train their algorithms or to use data for purposes other than the audit. Users of third-party technology providers should also be clear on how they can get client data back if the third-party provider goes out of business or when the contract terminates.
- **Applicability of the Revised Ethical Standard 2019:** Ensuring that it is clear whether the Ethical Standard applies to third-party vendors if they are dealing directly with audit clients or handling client data. As the Ethical Standard imposes requirements on the audit team, which includes all audit professionals who are assigned to a particular audit engagement in order to perform the audit task. members of the audit team may become blurred when engaging third-party technology providers. The limitations of the vendor's involvement in the audit engagement as well as the applicability of ethical requirements should be clarified in contractual arrangements.

Question 14: Do you agree that the increasing usage of third-party providers presents challenges in audit documentation and, where relevant, how have you dealt with this?

Similar considerations apply as discussed in answer to **Question 11.** However, when using third-party providers the understanding of the technology employed is likely to be much more limited within the audit firm, so there is an increased risk of the auditor not understanding what to document or how to capture the techniques applied to capture, extract or analyse the data.