17 July 2020

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

Via email: aat@frc.org.uk

Dear Jason,

Re: Financial Reporting Council's (FRC) Discussion Paper - Technological Resources: Using Technology To Enhance Audit Quality

The Corporate Reporting Users' Forum (CRUF) welcomes the opportunity to comment on the FRC's discussion paper, *'Technological Resources: Using Technology To Enhance Audit Quality'.*

Responses to the questions raised in the consultation that relate to the issues that concern investors are set out below.

Key points:

1. In our view these questions are about the digital transformation of the audit world, from less sophisticated automated or computerised processes on which accounting standards have been based, to more sophisticated processes carried out by smart technology with less intervention from the auditor. This transformation has many benefits but some significant challenges that, if not addressed, will adversely affect audit quality. Our key observations are listed here, followed by our fuller responses to each of the questions.

2. We believe that the use of technology in audits will provide both increased efficiency and enhanced quality. This is a result of larger financial data populations being covered, repetitive audit tasks (for example: checking the adding up of ledger entries; checking completeness; confirming period cut offs) being automated, and audit time being freed up to get answers to more searching and challenging questions of an audited entity.

3. It is unclear just how widely Artificial Intelligence (AI) and other advanced tools are being used, mainly because it is still early days in the world of AI. Most AI and advanced tools are still computer automated in the sense of being binary and the result of more sophisticated decision trees in programs. Even with generally used audit technology, there is a need for audited entities to improve their accounting record systems and financial data, including through adopting appropriate data standards. Investors seek greater clarity over the type of automation used.

4. A new version of ISA 315 was released on the 8th July 2020[1]. Appendices 5 and 6 contain a lot of useful information on technology risk and control. They explain well, the 'what' and 'why' of what auditors need to be aware of but do not explain sufficiently clearly how the assessment of IT controls will be carried out and to what quality. The revisions seem to omit items related to audit reforms that affect other aspects of ISA 315, perhaps because we still await Government's decision. But because technology underpins every aspect of business and, increasingly, of audits, the interplay between technology, fraud, and ESG expectations need to be identified, otherwise technology will be the elephant in the room, silently dominating proceedings but ignored in deliberations.

5. Older forms of computing made audits more efficient but did not significantly alter the role of the auditor or audit. Recent technical advancements mean that broader, deeper audits are possible, providing insightful assurance to all stakeholders which was not previously possible. Technology is replacing people in evaluating data and formulating conclusions. There are benefits to this, such as fuller assessments, but this subtly alters the role of the auditor from being the direct verifier of financial statements to being the verifier of computers' assessments of the financial statements.

6. Older and new forms of computing continue to make audits more efficient and significantly alter the role of the auditor or audit away from repetitive checking and box ticking. Recent technical advancements mean that deeper and complete data analysis is possible, providing improved insightful assurance to all stakeholders. These technical advancements also need to be assessed and verified, audited if you will, in order to be used in audits. Technology is replacing people in evaluating data and formulating conclusions across many industries, so investors want to make sure that any subtle alterations to the role of the auditor, from being the direct verifier of financial statements to being the verifier of computers' assessments of the financial statements, are avoided. As investors, we require auditors to remain responsible for the quality of the audit, from initial scope through to sign-off. Auditors will still need to verify the financial statements and demonstrate how they have done this.

7. If any part of the technology or data is in error, then the quality of the entire audit is suspect. Data errors, created through human error, remain a fact of life but now we have to acknowledge that the increasing use of AI/Machine Learning (ML) may generate new equivalents, creating some false positives about the quality of the assurance and audit. (Over-)reliance on the technology might prevent closer scrutiny and/or allow a new sort of gaming by companies that hides the scale of financial weaknesses. We require clarification of how this will be dealt with to prevent issues from being missed. Therefore, audit assurance needs to cover the technology and digital data being used in audits to mitigate such risks of error and their negative impact on audit or assurance quality.

8. Auditing standards require a qualified auditor, carrying out mandatory audits to find and record evidence to support their audit opinion. Now it is the computer that is finding and recording a

[1] ISA (UK) 315 (REVISED JULY 2020): Identifying and Assessing the Risks of Material Misstatement

large proportion of audit evidence. If 3rd party technology is used, those 3rd parties become a key part to the audit, not to provide audit judgements, but to ensure those judgements can be made.

9. Assigning accountability for the quality of the audit technology will be key. In the same way as computer audits have to assess and attest a company's computer controls and data, the auditor will have to provide the same assurance on their audit technology. A UK-style set of attestations, based on the USA's Sarbanes-Oxley Act, known as SOX, has been muted as part of audit reform. Under SOX, organisations provide information on the scope, adequacy and effectiveness of internal controls and procedures relating to financial reporting, with auditors attesting to internal control and procedural effectiveness. IT controls may need to be specifically highlighted to avoid being lost within a general statement on controls. Otherwise, how can anyone, making judgements about the data, analysis and results, remain able to do so where technology does so much of the work?

10. Our answers to the questions are based on the technology we understand is available today, but we feel it is important to point out that the rapid technology advances are likely to make obsolete any agreed approaches to improving audit quality before they have become established. One example is quantum computing.

11. Quantum computing is developing rapidly. Proof of concepts are showing efficiency and savings in a number of commercial activities, although we have not found evidence yet in auditing. Quantum computing is driven by physics, not logic. This will be a game changer across all sectors in how we use and manage computers and associated security. The capacity of each 'classical computing' bit, that can hold either a value of 1 or zero, is doubled in quantum computing, where the equivalent of the bit can hold 2 values simultaneously[2]. That, excuse the pun, is a quantum leap. It impacts security because the time needed to crack encryption codes and passwords will diminish, making conventional controls over access potentially useless. Quantum Machine Learning (QML) is also being developed, taking the path of innovation to higher levels even more quickly. However, this is an example and depending on your view may be quickly adopted in audit depending on affordability and usefulness or take longer than expected.

The CRUF UK responses to questions:

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?

12. Yes, we do agree technology will enhance audit quality, subject to a number of caveats set out throughout our response. AI, coupled with ML and structured and unstructured Datasets, are all part of a growing family of smart technology contributing to broader and deeper interrogations. Voice Recognition and Natural Language Processing (NLP) are, as a minimum, a more sophisticated form of recording meetings, enabling the computer to transcribe and then

[2] Google Claims a Quantum Breakthrough That Could Change Computing

incorporate conversations into automated analyses. As a result, we will have more intense scrutiny over the financial and free-form data for clearer insights.

13. There will be time-efficiency gains in obtaining and analysing evidence, and refining audit judgements. But additional tasks will also become necessary to ensure the technology is trustworthy and its outputs sound.

14. Technology can potentially change how the results of the audit are communicated. It allows for real-time updates and continuous auditing. In theory, it makes the end-of-year report redundant as the overheads of bringing together all necessary information disappears. In reality, refining this in any meaningful way for investors is still some way off. Investors will still need an annual report and an auditors' statement that the figures in there are correct, as investors typically will not receive continuous updates, nor be able to make useful sense of a company's financial statements in that manner. Regular publications are absolutely necessary in order to have a boundary.

15. The new version of ISA 315 is very welcome, identifying the type of IT risks and controls auditors should check for, laid out in Appendices 5 and 6. The one omission is insufficient information on how the assessment of IT controls will be carried out and to what quality. It is unclear how 'future-proof' ISA 315 is, given proposed reforms on the audit scope and process. These, along with the 'how', need to be addressed or else the interaction between other aspects of ISA 315 and technology may become simplistic, creating an elephant in the room silently dominating proceedings but ignored in deliberations. One solution is that technology is also "audited" within the scope of the audit.

16. Technology is moving beyond its traditional, transactional approach, which made repetitive tasks, following pre-designed rules, extremely productive compared to manual processing. It made audits more efficient but did not substantially alter the role of the auditor or audit.

17. Traditional computing remains prevalent in what we term 'legacy systems'. Its key drawback is the lag time in applying changes in line with evolving business requirements. It frequently introduces, however inadvertently, processing errors alongside functionality. Whilst deliberate sabotage was always possible, perpetrators were more obvious to spot because control over the technology was contained within an organisation.

18. Smart technology enables computers to analyse, make decisions, implement them and track outputs and outcomes to refine approaches for the next iteration. NLP not only can transpose the spoken to the written word, and vice versa, it can pick up breaking-news bulletins as they occur and incorporate them into existing Datasets for immediate analysis. That makes any data interrogation immediately more effective, through seeing patterns and predicting outcomes not possible for humans to do. That can help identify ambiguities and fraud. These tech advancements mean that broader, deeper audits are possible to provide insightful assurance to all stakeholders. This smart approach is currently used in agriculture[3], for example irrigation is

[3] 5 Applications of IoT in Agriculture - Making Agriculture Smarter

based on using weather forecasts and previous experience. The technology can be programmed to water crops based on its assessment with or without monitoring, or to suggest watering is necessary. The question is, should technology be allowed to make decisions when it comes to audits? Does it already? Investors will want to know how much of this smart capability is already being used in audits, and the reliance auditors place on it. We expect auditors to take decisions based on technology's suggestions amongst any other relevant factors.

19. We have found it difficult to provide examples of enhanced quality indicators. An adjunct to quality is efficiency, related to quality in a purely value-for-money way. We realise the question already acknowledges this but have listed them in case they are useful in a broader sense:

    - Time needed to complete complex audits. The time required should reduce compared to carrying out the same audit without these advanced tools.
    - Greater breadth and depth of audits. For an equivalent time, a larger audit scope can be met.
    - Ability to assess auditees against local and global accounting standards. Multi-nationals need to meet differing nations' accounting and regulatory requirements.
    - Comparing narrative in reports with other narratives and actual numbers, for example: evaluating the front half narrative and notes to the accounts with the back-half numbers; or evaluating strategic, performance and risk metrics to check consistency and contradictions.
    - Number of auditors needed. Fewer? Or the same but covering more?
    - Range of auditor skillsets used to fulfil the audit scope.

20. But there will be downsides. The key one is GIGO – garbage in, garbage out. If any part of the technology or data is in error, then the quality of the entire audit will be suspect. Finding this out may not be possible because the underlying processing is impenetrable to the auditor. We believe two specialist roles should be/are already part of audits: the information systems auditor to provide assurance about the quality of IT systems; and a data scientist to check the validity of the data prior to its use. As well as these two roles assessing and assuring the adequacy of a company's technology and data, they will also be needed to assess and assure any audit technology and data used in forming an audit opinion, allowing auditors to remain the verifier of financial statements.

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?

21. Small firms probably are disadvantaged because they lack resources and economies of scale necessary for developing and integrating advanced technological tools. Maybe these firms are not even being considered as challenger firms but is worth noting because of the pressures on increasing market competition in the audit market. The larger challenger firms are less likely to be disadvantaged, in fact may even have an advantage. Their use of smart technology could give them a Unique Selling Point (USP) of cheaper audits of equal quality. Mixed views:

a) In comparison to the big four firms, all other firms are probably disadvantaged to a degree because they do not have the same economies of scale. We recognise that the larger firms will have more resources, in terms of both money and people (and therefore possibly time), to develop technological resources, especially AI and other advanced tools.
b) Some of us have observed no disadvantages to small firms because the level of automation used in audits, that enhances audit quality, should be accessible to challenger firms.
c) Others believe small firms probably are disadvantaged because they lack resources and economies of scale necessary for developing or purchasing and integrating advanced technological tools.

22. However, many of us do not believe AI and other advanced tools are prevalent yet in audits. Therefore, challenger firms appear to be at a disadvantage in developing AI and other advanced tools but not in using new technology in audits. This is borne out with, for example, Grant Thornton who, we believe, have invested significantly in their audit automation. In fact, the larger challenger firms may even have an advantage. Their use of automated and, in future, smart technology could give them a USP of cheaper audits of equal quality. Over the coming years, technology may be the great leveller as it becomes affordable to smaller firms, potentially demolishing the barriers to smaller firms taking on larger audits

23. That could change the audit market, creating more competition as technology fills the capability gap currently identified as a reason for small firms' exclusion to FTSE company audits. It would alter Deloitte's website statement that "Delivering the audit product of the future, which meets the evolving needs of society and investors, requires the depth of skills and investment capacity that is only possible with the scale that comes from being a multi-disciplinary partnership firm."[4] However, the main barrier to challenger firms may not be technology but the mindset of the selectors of auditors. Changes required to the audit market, especially in the areas of quality, competition and choice are being considered elsewhere. Remedies for mitigating any challenger firm disadvantage in using new technology include:

a) Using affordable third-party technology.
b) Partnering with a large firm to pool resources, especially if 'joint audits' are introduced.
c) Being a first follower rather than leader, taking advantage of commercially available tools as an operational, rather than a strategic, investment in technology.
d) FRC providing a list of acceptable, affordable tools.
e) Making use of open-source software to build tools.
f) Hiring specialists for the technological aspects of the audit.

[4] Deloitte continues to invest in skills, technology and audit quality as it reports revenue growth of 10.9% to £3.97bn

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?

24. The key challenge is appreciating technology's limitations regardless of how smart technology of both the auditee and the auditor is. Despite AI, the technology still is programmed by someone somewhere based on a design (known as a use case) by someone somewhere else. The technology, therefore, will always have constraints on the calls asked of it. This adds a layer to testing. The first layer is the usual audit one of determining the sample size requiring testing, from 1% - 100% of all auditee activity within scope of the audit. The second layer is deciding the sample size of the computer output to test as verification of the absence of GIGO.

25. If 2nd layer testing fails, there are three investigations needed. The first is checking the approach applied to obtain those quality checks: how relevant were they? The second is checking the configuration of the tools used: what access, security, data extraction and change management processes were applied? The third is verification over the trustworthiness of the auditees' technology: was the source data relevant and valid? To overcome them, firms will need to work with an IT governance or assurance specialist. The larger firms may have an internal resource. The BIG 6 (PwC, Deloitte, EY, KPMG, BDO and Grant Thornton) certainly do.

26. Another remedy will be having appropriate data standards as intimated in paras 19 and 20 of your discussion document (see Question 9).

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?

27. We do not know enough detail about the current assurance model or the auditing standards, as non-audit practitioners, to know if they represent an obstacle to technological innovation. Our perception is that they should not be as the automation, in general use in audits and still being developed, enhances the previously manual processes envisaged by the model and audit standards. In any case, if auditing standards have been developed on a principles basis, they should be capable of being applied to both manual and technology situations and therefore should never be an obstacle to technological innovation. This appears to be the case so far.

28. But we are not aware of any minimum standards applying to the tools and technology used, nor how the results from the technological outputs are verified. If not an issue now, it may become so in the future.

29. It is for practitioners to answer the second part of the question. Where you may find more insight into any obstacles to technological innovation as a result of this consultation, we would be happy to provide feedback on any practitioner suggested required amendments to specific standards, objectives, requirements or guidance to reduce or remove any obstacles.

30. Whilst acknowledging the benefit from technology, some of us feel it is unclear if and how audit quality is impacted currently through using different bespoke or propriety audit technology. It would be interesting to know if variants in the technology used have contributed to notable assurance failures (Wirecard is the latest to hit the headlines), to provide understanding of consistency of approach. Maybe tools need to conform to an official set of criteria, equivalent to the card payment industry's "Payment Card Industry Data Security Standard (PCI DSS)".

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?

31. If the technological resources available remain binary and subject to binary decision tree processes, we believe the level of training is sufficient. We understand that trainees and qualified staff are required to pass the chartered accountancy qualification, and this includes reasonably up to date training and exams in technology and computers. Also, computer auditors, specialists in auditing auditee computers, will have the required training for both computer audits and assessing and assuring audit technology.

32. However, we recognise that auditors spend many years training to understand financial statements and audit methods and their technological training may be superficial. This should be mitigated by computer auditors. Technology is more complex than accounting but presented in ways that makes it easy to use. We must not confuse usability with simplicity. The easier a tool is to use, the greater the complexity of the underlying technology. Therefore, where technology is involved, auditors should take nothing for granted.

33. The ICAEW states it includes blockchain as part of its ACA syllabus[5]. Auditors need to understand how those transactions are recognised in the financial statements, and how judgements over valuations are decided. This approach will need to expand for other technologies.

34. There are three levels of training needed. The first is how to use the tool. The second is how to verify the tool produces valid results. The third is assurance that the tool is properly and securely configured, a specialism in its own right, requiring separate training and experience to provide that assurance.

35. If the ICAEW is representative of thinking, then the accounting and audit professions are aware of the training challenges. From a user perspective, appreciation of "The increasingly complex models on which valuations of assets and liabilities are based means that auditor skills will need to keep up" is helpful in recognising, "Auditors will not only need to understand accounting, they will also need to understand information process flows and data, and they will need to have modelling skills, all of which involve maths and statistics."[6]

[5] Blockchain and the future of accountancy

[6] Data analytics for external auditors

Artificial Intelligence, Machine Learning and Natural Language Processing

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?

36. Firm-wide controls should be equivalent to any organisation undergoing digital transformation.

- People management: ensuring the people employed in highly sensitive areas are qualified to do so and continually assessed for integrity and commitment to ensuring new technology meets its requirements.
- Proof of concept: understanding what the accounting standards require, how application of and compliance to them is demonstrably proven and how the technology will contribute to that demonstration.
- Change management: knowing when, how, what, why and under whose authority to install, update, modify or remove part or all aspects of the technology/tool. Change management is usually a proactive and planned activity.
- Data management, covering access to view, move, change, copy, delete the data. This includes not only people but intelligent software and hardware components, the most obvious is printers but there are many more.
- Patch and version update management: swift but thorough due diligence and impact analysis as to what the modifications are. This sort of management is usually ad hoc, based on the software supplier's recommendations and timetable, akin to an Office 365 or antivirus software updates.
- The timing of modifications and updates: this is a crucial balance between the need to have the improved functionality whilst avoiding disruption to an audit already in progress.
- Control management: knowing where embedded controls are within the technology and the conditions under which the technology will alter those controls, for example, AI defining what constitutes a breach based on various thresholds determined by ML.
- Access controls: similar to data management but at the technology system level.
- Business continuity management: business process and data recovery take AI/ML into account.
- Another area of firm wide control that will be needed is in respect of audit evidence with sufficient controls to ensure audits retain, keep accessible and safe technology-based audit evidence.

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?

37. We are aware that AI and ML continues to be developed by the BIG4[7] and that using the combination of AI and ML, for example with IFRS 16 for lease contracts, provides significant

[7] AI in the Accounting Big Four - Comparing Deloitte, PwC, KPMG, and EY

efficiencies. AI and ML appear to be effective in assessing material misstatements and detecting fraud.

38. The ideal is to have reports that still conform to the physical version whilst having reporting tools that disaggregate and reaggregate the information in different ways. There are many data and visualisation tools on the market. Having the data accessible to the users of the reports for self-selecting interrogation is the way to proceed, enabling all stakeholders, from audit committees to shareholders, from regulators to employees, to interrogate the data as they think fit.

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

39. From a user perspective, it will be the level of confidence we have in the integrity of technology used and in the capability of the auditor using that technology.

40. For the audit profession, a key one will be on the role and the number of auditors needed in the future. It could mean fewer auditors working with more data scientists as the balance moves from verification of the financial statements to verifying the authenticity of algorithmic behaviour on Datasets.

41. The new technologies raise certain societal ethical questions[8], such as privacy, bias in decision processes, behaviour manipulation, and inexplicable processes completely opaque to the people relying on their outputs. There is also the question of 'repeating' a particular set of activities. If the computer has learnt from the previous iteration, can the same actions be performed with the same result? It raises the question whether standards for machine ethics are necessary with attestations that a series of agreed rules must always be met to ensure no human, enterprise and other machine is hurt or exploited by the technology. There are several things to consider**:**
    - Understanding the consequences of incorrect observations, such as in fraud detection, and in financial results, for example, in debt ratios.
    - Understanding the importance of challenging the accuracy of the results. What is deemed right from the perspective of the computer, for example, assessing corporate activity against historical pre-COVID-19 conditions, might well be wrong for the post COVID-19 audit.
    - Avoiding GIGO by maintaining accurate and precise Datasets to prevent AI/ML reporting incorrect observations.
    - Recognising the presence of inappropriate AI/ML by understanding, in technical and layperson terms, each feature of the internal workings of algorithms.
    - Recognising that AI/ML need to have security, too, to ensure trust is retained in their purposes and processes.
    - Able to reverse, recreate and rerun AI/ML processes to assist investigations if results are questionable.

[8] Ethics of Artificial Intelligence and Robotics (Stanford Encyclopaedia of Philosophy)

- Creating transition paths to allow auditors to retrain and the audit business model to adapt to a much broader use of technology in the audit scope.

42. AI and ML ideally need cross-industry regulations, currently outside the scope of any industry or sector. In response, different sectors are developing individual approaches. The FRC can consider a number of 'rules' to decrease ethical concerns, such as:

    - Bias evaluation: a commitment to check for bias and transparency, explaining how bias occurred, and the impact the bias, and subsequent correction, has had.
    - Demonstrable justifications: improving transparency and explanation over what ML systems do.
    - Consistency and resilience: having processes and related results, that can be reproduced under the same circumstances of the AI/ML combination when required.
    - Trust-by-privacy: protecting data that interact with AI systems directly or indirectly.
    - Data risk awareness: risk mitigants are included and defined to ensure infrastructure, models, algorithms and data are considered during the development of ML.

43. Assigning accountability for the quality of the audit technology will be key. In the same way as computer audits have to assess and attest a company's computer controls and data, the auditor will have to provide the same assurance on their audit technology.

Data Standards and Extraction issues

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?

44. Yes. Users of reports will continue to require consistency to understand the components contributing to the results. This covers each individual item, and how each item has been interrogated and reviewed individually and collectively. Data standards will help address the issues of poor-quality Datasets but, as capability increases to process unstructured data, the more challenging it will be.

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 company data? If so, what measures would mitigate this risk from crystallising?

45. Yes, but this is not a new threat. Auditors, in looking at company data and having conversations with company employees were always at risk of accessing wider business insight information. That is not necessarily a bad thing as it provides a broader context within which to understand the company and the results. Auditors are bound by their professional code to act with integrity which means using judgement when to exclude information that comes their way and when to act upon it even if it appears to be outside their audit scope.

46. With the spotlight on auditor independence and the unacceptability, in terms of the public interest, in relation to cross-selling from audits, it is hard to imagine this risk crystallising. We

imagine that the laws and terms of engagement around professional confidentiality of audit information should also mitigate against this risk.

Audit documentation

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 is a problem.

47. We have come up with two interpretations of the question. One view is we disagree, unless we are missing something. Similar issues will arise for business technology and trying to understand and assess the integrity of that technology and the IT and/or other controls in place to try and ensure that integrity. Auditors should be able to produce required audit documentation on the technology, like any other documentation around technology. If there are problems, they should not use the technology until they can produce the documentation. Another view is that producing the documentation is no different to now, and maybe even easier as the audit tools improve. But verifying its contents might become the problem if too much credence is placed on contents generated by sophisticated tools.

48. Verification of documents may carry greater weight because of the greater role technology plays in the audits. There are three perspectives, that of the auditor, the auditees and the supplier(s) of the technology. The following points do not directly address the Question 11 but link documentation contents to technology assurance mentioned earlier.

Auditor:

- Having an assured, well managed IT environment, covering all IT components.
- Assurance over 3rd party services, such as cloud computing and storage.
- Strong IT controls over change management, access and usage of systems and data.
- Clarity and understanding over the type of technology used.
- Well-written documentation explaining, in layperson's terms, how each piece of the technology contributes to the audit.
- Clarity over what the technology now performs in place of the auditor, covering calculations, analysis, interpretations, x-checking, decisions, and actions.
- A robust audit trail recording the timing and 'before and after' position of each activity undertaken by the technology.
- Evidence of technology testing procedures and results to prove any changes to the technology, from new hardware to updated algorithms, are working as planned.

Auditee:

- Well-documented and demonstrable assurance over the company's IT systems.
- Disclosure about the type and timing of updates to company technology to ensure consistency and integrity are maintained.
- Proof of complete Datasets to ensure a sound basis of the audit.
- Agreements over on-site versus off-site data interrogation.

- Having a defined data extraction process to a secure, separate "interrogation" environment to ensure the integrity of the prime source.
- Understanding of, and agreement to, the scope of auditor's access rights to Datasets and other digitally stored information.
- Requiring proof that accessed data have not been altered by the audit tools used.
- Transparency of the audit process as outlined under the 'Auditor' list.

Supplier:

- Proof of concept is available.
- Proof of active compliance with tech industry standards. Typically, these will be ISO standards (International Standards Organization) found within the 20,000 and 30,000 ranges. The two key ones are ISO 27001, covering information security management systems relevant to all organisations, and ISO 20,000-1 on information technology service management relevant to IT service providers.
- Clear contractual terms and service level agreements between the rights and responsibilities for the supplier, the auditor and the auditee.
- Non-Disclosure Agreements for when the supplier need to provide support during an audit.

Data analytic exceptions

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?

49. From a user perspective, we would welcome a conversation with auditors on how they manage this. It will help us understand how they separate 'noise' from 'news' and how exceptions influence audit quality. We would expect there to be dialogue between auditors and the audit committee on this subject.

50. A combination of ML and AI may help reduce the amount of 'noise' but that relies on understanding how the algorithms have developed to become more precise without losing accuracy. For example, there is little point in the computer reporting in detail on materiality if that conclusion was derived from the wrong Dataset.

Use of third-party technology providers

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?

51. Yes, this does pose ethical challenges and also professional ones. Technology is ubiquitous, used by the consumers of technology but created and supported by technology professionals. Nearly

every piece of code is developed by someone who is not the auditor yet has complete control over what the code will perform and under what circumstances. Any software corrections or enhancements will also be provided by the professionals. Each audit tool, however configurable it is by the auditor, will not give the auditor 100% control. That remains buried within the code.

52. So, de facto, the 3rd party is a key part to the audit, not to provide audit judgements but to ensure those judgements can be made. Auditors sign-up to codes of ethics and standards of professionalism as part of successful qualification. IT professionals have no such mandatory requirement and may not even subscribe, voluntarily, to an equivalent professional code. The 3rd party company should have evidence of compliance with best IT practices, encapsulated in relevant ISO standards. As a result, we believe that third technology providers must, as part of safeguards:

    - Comply with at least those two standards, ISO 27001 and ISO 20,000-1.
    - To comply with ISO/IEC CD 23053 once it is published (currently in draft) a framework for AI Systems Using ML.
    - If using ML, explain if the ML is supervised, unsupervised or semi-supervised[9]. Supervised learning is when inputs with known outputs and is used on historical data to predict future outcomes, for example, who is most likely to default on debt. Unsupervised learning is used when there are no assumed answers, allowing the technology to identify data patterns on its own, for example, previously undiscovered risks, concealed from human analysis. The two can be combined to become semi-supervised.
    - Evidence of their own assurance programmes and the role, effectiveness and influence of internal audits.
    - The qualifications held by technical staff, from professional bodies such as ISACA, BCS, ISC2 and many more[10].

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?

53. Probably because the more parties involved, the more complexity exists especially when things go wrong. It provides opportunities to pass the buck, shifting responsibility and accountability on to other parties. But this is a current, not a future, problem so we need to investigate experiences to date, good and bad, to avoid pitfalls and reinventing the wheel. The auditors should be able to provide input. Our responses to Q6, 8 and 11 provide mitigants.

[9] Machine Learning in Auditing

[10] List of Cybersecurity Associations and Organizations

About the Corporate Reporting Users' Forum (CRUF)

54. The CRUF was set up in 2005 by users of financial reports to be an open forum for learning about and responding to the many accounting and regulatory changes that affect corporate reporting. In particular, participants are keen to have a fuller input into the deliberations of accounting standard setters and regulators. CRUF participants include buy and sell-side analysts, credit ratings analysts, fund managers and corporate governance professionals. Participants focus on equity and fixed income markets. The Forum includes individuals with global or regional responsibilities and from around the world, including Australia, Canada, France, Germany, Hong Kong, India, Japan, New Zealand, South Africa, UK and USA.

    The CRUF is a discussion forum. Different individuals take leadership in discussions on different topics and in the initial drafting of representations. In our meetings around the world, we seek to explore and understand the differences in opinions of participants. The CRUF does not seek to achieve consensus views, but instead we focus on why reasonable participants can have different positions. Furthermore, it would not be correct to assume that those individuals who do not participate in a given initiative disagree with that initiative. This response is a summary of the range of opinions discussed at the CRUF meetings held globally. Local country differences of opinion are noted where applicable.

    Participants take part in CRUF discussions and joint representations as individuals, not as representatives of their employer organisations. Accordingly, we sign this letter in our individual capacity as participants of the Corporate Reporting Users' Forum and not as representatives of our respective organisations. The participants in the Forum that have specifically endorsed this response are listed below.

(Signatures)

Sue Milton
UK Shareholders' Association

Charles Henderson
UK Shareholders' Association

Gregory Collett, CFA
Pictet Asset Management

Anna Czarniecka
Financial Reporting Consultant