Notes.

Meeting: ACCA UK Practice Sector Panel

Location: Virtual (Teams)

Date: 13 May 2025, 11.00-12.30 GMT

PRESENT

Carl Reader (Chair), Eriona Bajrakurtaj (Vice Chair), Mandy Bagot, Lee Brocklehurst, Bethan Evans, Adrian Harris, Peter Jarman, Brendan O'Donnell, David Nicholls, Graham Parker, Situl Raithatha, Hannah Simpson, James Slatter, Gavin Spencer, Michelle Westbury, Sach Yadav and Gillian McCreadie (Council).

APOLOGIES

Alex Black, Steve Collings, Faizan Haider, Nick Le Huray and James Lizars (Council).

IN ATTENDANCE

Glenn Collins (Head of Policy, Technical & Strategic Engagement, ACCA UK), Lloyd Powell (Strategic Engagement Lead, ACCA UK), Sophie Hall (Sectors & Communities Manager, ACCA UK) and Pat Delbridge (Sectors & Communities Manager, ACCA UK).

1. WELCOME AND REGULAR BUSINESS

Following brief introductions from all panel members in attendance, Carl Reader shared the news that it was his final panel meeting as Chair as Eriona Bajrakurtaj has accepted the position of Chair with Gavin Spencer accepting the position of Vice Chair from the August panel meeting onwards.

The Panel noted the summary of the Practice Sector Panel and lengths of terms.

2. CYBER SECURITY FOR PRACTITIONERS

The Panel discussed the level of cyber security awareness in accountancy practices and shared their insights into their own practices:

- Any practice using Microsoft Office 365 can take advantage of its security features such as Microsoft Defender for Office 365, Exchange Online Protection, and Microsoft 365 Advanced Threat Protection, to help protect against cyber threats like phishing and malware. Administrators can set rules that control access to Office 365 resources based on user, device and location. Multi-factor authentication can also be enabled. Their Microsoft Entra Admin Centre can give your practice a score based

on certain factors as well as suggestions for how you can improve your cyber readiness.

- The whole team needs to be involved in cyber security. Regular communication around this topic, encouraging the team to question any emails they are suspicious about, forwarding examples of phishing emails to alert the rest of the team, regular cyber security training on the latest tactics used by cyber criminals, etc will help your team minimise the risk of a successful cyber-attack. Your systems will only ever be as good as the people using them.
- To help with staff training, you can use your external IT partner to run a phishing campaign against your own business. It you do not have an external IT partner then you can use free/cheap online tools internally to run that phishing campaign - as long as it is not announced, and you have someone internally who can learn to use one of the tools available, it could be useful without the involvement of external providers.
- Updates and patches need to be applied regularly.
- The level of cyber security awareness and readiness in accountancy practices is lower than in other organisations, yet accountancy practices are a prime target for cyber criminals because of the data they hold – even small practices will be targeted.
- Many practitioners have apps for client emailing on their smartphones – setting face recognition requirements for opening apps as well as opening the phone itself provides an added layer of security.
- Without cyber security credentials, it is hard to win bigger clients and tenders – particularly Government tenders – so it can be a barrier to growth.
- Have IT security as a standing agenda item when meeting with clients.
- With the rise of AI, phishing emails are becoming ever more convincing including those purporting to be from HMRC, Companies House or ACCA.
- Practices would value advice from ACCA on the most important protections to put in place given cost considerations. The real-life examples provided by PureCyber would be helpful if they could be shared more widely.

ACCA is working with PureCyber to produce guidance for practitioners to minimise the risk of having their HMRC agent accounts suspended due to automatic flags that are raised as a result of unusual log in patterns or log in locations, etc.

The Panel asked ACCA to develop guidance on cyber security for new practices. New practices have to weigh up costs so guidance on what is essential would be helpful – the absolute minimum that should be in place from the start.

A poll conducted during the meeting found that the cyber security measures most widely implemented in practices were:

- Multi-factor authentication and least privilege access
- Encryption of data in transit and at rest, especially when sharing client files via email or cloud services
- Application of software updates and security patches.

The cyber security measures least implemented were:

- An incident response plan for cyber incidents including notification procedures and roles – and where the plan is stored
- Regular security audits and penetration tests
- Assessment of security controls of third parties and vendors.

A poll on whether practices hold cyber insurance found that two-thirds of practices have cyber insurance and a third do not. Cyber Essentials certification provides some insurance but a successful claim on that insurance will be dependent on the self-assessment done by the practice as part of that certification being accurate.

Lockton – ACCA's recommended PII broker – has advised that it is becoming increasingly difficult for practices to obtain cyber insurance unless they are able to meet certain criteria such as multi-factor authentication. However anecdotal evidence suggests that cyber insurance is being bundled into PII insurance or otherwise offered without question – the likelihood of any insurance claim for a cyber attack being successful when it hasn't been specified upfront what security must be in place is slim. ACCA was asked to work with Lockton to advise on the questions that every practitioner should ask their insurance provider about the measures they need to have in place to be able to make a claim on their cyber insurance should they suffer a cyber-attack.

4. TAX, REGULATION & COMPLIANCE

ACCA provides ethical guidance to members in relation to taxation via the cross-body Professional Conduct in Relation to Taxation (PCRT) factsheet. Work has been ongoing to provide support in a number of areas where tax practitioners may face ethical issues including AI, research & development and MTD.

The soon to be published updated PCRT asks a number of questions to help tax agents consider the ethical issues and then exercise their professional judgment as to when they should or should not file on behalf of their clients. Interim guidance is now available on ACCA's website.

Now that HMRC has confirmed its digital record keeping requirements, ACCA is working to finalise engagement letters for its members to use.

5. NEXT MEETING

The Panel noted that the next meeting will be a virtual meeting taking place on 19 August at 11.00am.