Edition 03 (June 2019)

AFA connect

ASEAN Federation of Accountants

Official Publication of the ASEAN Federation of Accountants (AFA)
Accredited Civil Society Organisation of the Association of Southeast Asian Nations (ASEAN)

Impact of Technology to the Accountancy Profession

Kon Yin Tong
President, ASEAN Federation of Accountants.

You may be reading this on a handheld device while sipping a cup of coffee or enjoying food delivered to you without having to leave your seat. You may also have used the same device to search the best rate for your next holiday without having to talk to a travel consultant.

Do you remember when was the last time you browsed the classified advertisements or job vacancies on your local printed newspaper; or pay your bills at the post office? Looking back, technology has indeed changed how we live, work and play.

The accountancy profession is no exception. The introduction of automation such as Artificial Intelligence (AI), big data analytics and block chain is transforming different aspects of businesses, including its accounting and finance functions.

Technology and the Accountancy Profession

At the Vietnam Association of Accountants and Auditors (VAA) Conference in Vietnam last month, I shared with fellow Vietnamese accountants on how Industry 4.0 would change the way accountants work. Algorithms can be programmed to carry out specific tasks such as data entries. Softwares can glean intelligence from huge amounts of data, which can be extracted easily and real-time, thereby improving productivity and efficiency. In addition, drones and video analytics can assist with inventory counts, alleviating the manual processes involved, for example, in counting stockpiles of minerals.

As a result, technology and automation would free accountants and book keepers to assume higher-value tasks. Accountants in business such as finance teams, can use data analytics to understand and discover patterns in customer behaviours and advise businesses on the best course of action in decision making. Auditors can use data analytics to carry out more comprehensive audits by interrogating complete sets of data, rather than just testing samples. Isn't the profession going through exciting times!

Adapt and Upskill

Systems and machines doing jobs that are currently done by accountants may well become a reality. Thus, it is important that accountants of the future have the ability to adapt and upskill and provide greater value at work. At the recent IAI-AFA-IAESB International Conference 2019 held in Bali in May 2019, experts discussed about how the advent of technology is demanding new sets of skills and competencies.

Against this backdrop, in this issue of the AFA Connect, I am pleased to share with you Malaysian Institute of Accountants (MIA)'s experience in developing a "Digital Technology Blueprint" to prepare Malaysian accountants for the digital economy. You will also find other interesting articles contributed by our AFA member organisations on disruptive technology and how it impacts our profession.

I wish you a fruitful read.

Thank you.

Follow us!

afasecretariat @iaiglobal.or.id
www.aseanaccountants.org
@AFA_Accountants
ASEAN Federation of Accountants
ASEAN Federation of Accountants

MIA Digital Technology Blueprint:

Preparing the ASEAN Accountancy Profession for the Digital Economy

Dr. Nurmazilah Dato' Mahzan
CEO, Malaysian Institute of Accountants (MIA).

Front cover of the MIA Digital Technology Blueprint

Digital is a tremendous source of growth for ASEAN. According to the Google-Temasek November 2018 report e-Conomy SEA 2018: Southeast Asia's internet economy has hit an inflection point, and is expanding faster than expected. As of the end of 2018, the region's internet economy was valued at US$72 billion. By 2025, it's expected to hit US$240 billion, US$40 billion more than earlier projections.[1]

To help accountants in Malaysia manage sweeping changes arising from the digital economy and Industrial Revolution 4.0 (IR4.0), MIA launched its MIA Digital Technology Blueprint at its inaugural AccTech Conference 2018. However, we strongly believe that this Blueprint can also be utilised by all

1 ttps://www.thinkwithgoogle.com/intl/en-apac/tools-resources/research-studies/e-conomy-sea-2018-southeast-asias-internet-economy-hits-inflection-point/?_ga=2.178764196.1814961885.1553397692-1193298381.1553397692

accountants in ASEAN who are embarking on tech transformation, especially those in emerging economies.

The Origins of the Blueprint

MIA keeps our finger on the digital pulse, and we predicted early on that technology would be a game changer for the profession. We initiated this Blueprint because we observed that accountants were uncomfortable with technology, and to respond to our members' need and thirst for information and guidance.

Members kept asking this question: which technologies relate to us and which ones do we take up first – artificial intelligence, robotic process automation, cloud computing or big data analytics? The answer to this lies in analysing your own organisational circumstances, and customising tech solutions to fit your needs.

Mapping the Blueprint

So, how should one use the Blueprint? First, the Blueprint takes a bird's eye view by laying out the landscape of Industry IR4.0, the Internet of Things, and the macro digital economy and how these impact accountants in four categories – commerce and industry, public practice, public sector and academia. This is important to familiarise accountants with the strategic deployment of digital and technologies as an enabler for economic and social development and nation building.

Next, instead of being prescriptive, the Blueprint outlines five principles for each accountant to consider and kickstart their thought and technology adoption processes. Principles are important as each and every accountant works within their own ecosystem and their companies and businesses have their own strategies.

The Blueprint's Five Principles

These are applicable to all accountants in all organisations and economies who are contemplating embarking on a digital journey of technology adoption and investment.

1. **Assess digital technology trends**. First, be aware of what are the current technologies available out there. Get the information and learn more about these technologies. Through our events and learning platforms, MIA strives to educate accountants on these trends and assess their impact on the profession.
2. **Identify capabilities**. Put another way, this means identifying the person within your organisation who can champion and take actions to implement these technologies. Who should be assigned to lead this? Who should be doing certain specific tasks? MIA will support accountants and our members by providing training and the relevant certification for members to enhance their capabilities.
3. **Harness digital technologies**. Put a plan in place to start adopting and start using these technologies. MIA will help by promoting digital technology adoption and exploring collaboration with relevant stakeholders.
4. Determine **funding** needs and identify funding options. MIA's survey on technology adoption found that cost is a major barrier. To overcome this challenge, MIA encourages accountants to draw up a plan for funding technology investment and building the business case. For example, if your organisation is unable to invest now,

consider adopting technologies three years down the road and start putting aside your budget for that.

Do engage with your respective governments and policymakers to identify and enhance incentives and grants for technology adoption.

Another cost-effective option that can be rolled out fast is cloud computing and Information Technology as a Service (ITaaS) solutions. These offer attractive economies of scale and make it more affordable and easier especially for SMPs and SMEs to harness technology.

5. Comply with good **Governance** and cybersecurity practices including IT and data governance, as well as the relevant rules, laws and regulations. Usually defined as a subset of corporate governance that is focused on information and technology, IT governance provides a structure for organisations to ensure that IT investments support business objectives. This is very important for business continuity and sustainability.

As the developer and regulator of the Malaysian accountancy profession, MIA strongly advocates for overall good governance and risk management including in emerging digital areas, to protect the public interest.

Tone from the top will be essential to managing governance risks arising from digital transformation. Do establish technology steering committees and assign clear responsibilities, guidelines and accountability for technology transformation.

It is also worthwhile to check whether your organisation's rules for IT governance are still relevant and able to support tech adoption internally as part of your enterprise risk management systems.

Using these five principles as a starting point, I advise accountants to formulate a checklist and carry out your own SWOT (strengths, weaknesses, opportunities and threats) analysis unique to your own context and situation.

Global Recognition and Support

Here at MIA, we are very proud of this pioneering blueprint which is a first for the global profession. It is the culmination of two years' worth of intense research and several engagements with stakeholders, combined with numerous articles and resources from the International Federation of Accountants (IFAC) that we adapted to fit the local context.

We are also very grateful for the acknowledgements and support that we have received for our Blueprint from various quarters.

We are honoured the then IFAC President Rachel Grimes, who delivered the keynote address and launched the Blueprint at AccTech 2018, commended MIA for initiating the Blueprint. She remarked that the Blueprint is not just an ASEAN first, but '*also one of the first around the world*' that she had seen. She noted that ASEAN and broadly Asia are racing ahead of other regions by developing events and courses to make people aware of and embrace technology.

Launching of MIA's Inaugural AccTech Conference

Launching of the MIA Digital Technology Blueprint

Other accolades for our Blueprint include a recent recognition of excellence award from OpenGov Asia for creating a document to provide accountants with the knowledge to manage their profession in a more digital ecosystem.

We hope that all accountants in ASEAN will be able to benefit from the Blueprint, and we would be delighted to collaborate with and advise our ASEAN partners and stakeholders on how to move the needle on their digital initiatives.

The Blueprint was prepared by the MIA technical team with inputs and guidance from MIA's Digital Economy Task Force. The Blueprint can be downloaded from MIA's website - https://www.mia.org.my/v2/downloads/resources/publications/2018/07/12/MIA_Technology_Blueprint_Spreads_format.pdf

Cybersecurity Risk – Time for Auditors to Take Heed?

Fua Qiu Lin
Senior Manager, Quality Assurance, ISCA.

This article was first published in the IS Chartered Accountant, May 2018. Reproduced with permission from the Institute of Singapore Chartered Accountants.

The global interest in cybersecurity is growing. As we move into the cyber age, technology has become a huge part of both our everyday lives and today's business environment, as more and more businesses increase their online presence and digital exposure by leveraging technology for almost every aspect of their business. But just as technology presents opportunities to many businesses, it also presents threats and challenges. Over the years, cyber attacks have continued to occur, escalating in frequency, severity and impact. These incidents have impacted every industry from financial services to retailers, entertainment and healthcare providers. For example, in a biggest known breach of a company's computer network, state-sponsored hackers attacked all three billion user accounts of Yahoo! in 2013, and made off with names, birth dates, phone numbers and passwords of users that were encrypted with security that was easy to crack. Following the disclosure of the cyber attack, Yahoo's Internet business was acquired by Verizon Communications at a substantially-reduced price that was US$350 million lower than the original US$4.8 billion agreed price.

Elsewhere, criminals gained access to certain files in Equifax, a credit rating agency's system, by exploiting a weakness in its website software, resulting in a data breach involving highly sensitive and personal information

belonging to 148 million customers. Its Chief Financial Officer said in November 2017 that this had cost the US credit bureau nearly US$90 million, a figure that was set to rise further. Health service organisations in the United Kingdom were hit by the WannaCry ransomware attack in 2017, which scrambled data on computers and demanded payments of US$300 to US$600 to restore access, affecting the delivery of healthcare services.

In Singapore, the WannaCry ransomware attack was on a much smaller basis, and limited only to shopping malls and stores. In 2017, a breach in an Internet-connected system at the Ministry of Defence resulted in the theft of the personal data of 850 national servicemen and employees. Earlier in 2014, the personal data of over 300,000 karaoke company K Box's customers were leaked as a protest against the government's announcement to match Malaysia's toll hikes at the Causeway. K Box was ordered by the Personal Data Protection Commission (PDPC) to pay a fine of S$50,000; PDPC's investigations had shown that the company did not have a sufficiently robust IT system. Undeniably, cyber attacks can have a huge impact on businesses. Given the changes in the business landscape and the hype over cybersecurity, it is worthwhile to explore whether financial statements auditors need to consider the cybersecurity risk of their clients.

Cybersecurity Risk: an Essential Audit Consideration

Perhaps due to its constantly evolving nature, cybersecurity risk remains complex and abstract to many. There may also be a perception that cybersecurity risk is not relevant to small businesses, hence, cybersecurity risk may not have been considered and addressed in all financial statements audits. But let us think about this: risk assessment is a crucial part of audit planning and auditors are required under the auditing standards to obtain an understanding of business risks that may result in risks of material misstatement of the financial statements. Just as auditors would consider an entity's business risks in a financial statements audit, cybersecurity risk is an equally important risk area that cannot be ignored. Perhaps even more so, given the broad extent to which cyber attacks can cause fundamental enterprise-wide damage to organisations, and for some attacks, even a huge impact to the financial statements. Cybersecurity risk is hence an essential consideration in any financial statements audit.

Cybersecurity risk can affect many different areas of a business. For financial statements audit, the auditor only needs to consider the risks that could impact the financial statements and the entity's assets. It would not encompass a comprehensive evaluation of cybersecurity risk and controls across the entity's entire IT environment. For example, an online retailer experienced a cyber attack to its online retail platform, resulting in customers being unable to place online orders for a short period of time. Noting that the retailer has yet to increase protection of its system, the auditor may assess the possibility of another cybersecurity breach as higher. However, this represents a business risk to the retailer, with an opportunity cost of lost revenue when the system is down rather than a direct impact to the financials of the entity. On the other hand, if the online retail system is connected to the entity's system that stores its confidential data and information, an attack like this can also expose the entity to other potential vulnerabilities. This may then require further assessment by the auditor.

Cybersecurity Risk is Relevant to Almost Every Entity

For an entity operating with a traditional business model with no online presence, intuitively, one may think that cybersecurity risk does not apply. But this cannot be further from the truth. Unless the entity runs entirely on manual processes without any technology intervention or Internet connectivity, cybersecurity risk will come into play albeit in varying degrees. A small mom-and-pop provision shop, for instance, could be using a point-of-sales system and technology to monitor its inventories and hence, is also exposed to cybersecurity risk.

While most of the reported cyber attacks affected big businesses, small businesses also suffer from cyber attacks even though these may be less reported. For small businesses, the likelihood of experiencing cyber attacks is just as high if not higher, as their defences are typically less sophisticated and easier to penetrate. In fact, the impact could be more devastating or it may even go undetected. While larger businesses may have the resources to recover from the attacks, the chances of making a full recovery for smaller business may be much lower. Potentially, it could even put them out of business. Cybersecurity risk consideration is hence relevant to almost every entity, be it big or small, and with or without an online retail market.

As part of understanding an entity's objectives, strategies, operations and risks, auditors would be able to identify the related business risks that may give rise to risks of material misstatements of the financial statements. Depending on the entity, cybersecurity risk may or may not be one of such risks. In the previous example of the provision shop, cybersecurity risk is unlikely to be a key risk area identified by the auditor as part of risk assessment, unless an actual cyber breach has occurred. In comparison with another example – a corporation adopting new-age digital technologies – cybersecurity risk would likely be one of the key risk areas. Therefore, auditors need to have a good understanding of the entity's business and its IT environment, and determine the relevance of cybersecurity risk to the audit. Whether it is a provision shop or a corporation using the latest technologies in all aspects of its business, it would still be necessary to demonstrate that this has been considered and assessed.

Changes in the risk environment and the ways in which businesses operate also mean that business risks do not remain constant. In one year, cybersecurity risk may not have been identified as a key business risk that may result in risks of material misstatement, but this does not mean that the same goes for the next year. Take the example of a brick-and-mortar retail shop selling clothes which switches to online retail – the extent of exposure to cybersecurity risk would have changed with the change in its business model; it is hence important that cybersecurity risk be assessed from year to year.

Effects of Cyber Attacks: More Than What You Think

Cybersecurity risks are broad and connected. The impact of cyber incidents may not be isolated or contained within single systems or networks, hence creating potential systemic risks. Pigeon-holing cybersecurity risk as merely IT risks also makes it difficult to recognise the full business impact of security breaches. The potential costs to an entity of a successful cyber attack can include loss of intellectual property, theft of confidential information, breach of customer data privacy, reputational damage, service and business disruption, damage to physical infrastructure (example, corrupted servers), alteration to financial records and transaction logs as well as the huge costs in response to the attack, such as lawsuits and settlements, regulatory inquiries, and more.

While not all the earlier cyber incidents mentioned appear to have a direct impact on the financial statements or the entity's assets, incidents that relate to unauthorised access to financial reporting applications, data and digital assets recorded on the balance sheet clearly would. Even where the cyber incident does not directly impact the financial reporting applications and data, such as the common attacks involving theft of customer data, the auditor would still have to consider, among others:

- Remediation costs that the entity would have to incur, such as costs to repair the system damage, and compensation offered to customers to maintain business relationships;
- Regulatory inquiries and penalties for breaching data privacy;
- Potential lawsuits from affected customers and associated legal fees;
- Reputation and brand damage, and its impact to revenue, value of inventories, intangibles (impairment issues);
- Going concern issues.

Hence, when a cyber attack does occur, it is unlikely to be business as usual, either for the entity or the auditor, unless it is clearly insignificant and isolated.

No Cybersecurity Risk Identified = No Breaches?

Cybersecurity risk may not have been identified as a key risk area by the auditor as part of risk assessment, but this does not necessarily mean that no breach has occurred. Auditors should still maintain their professional scepticism when carrying out their audit as there could be events or conditions that may indicate a possible breach. Some businesses with weak IT programmes and controls may not even realise that they have been the subject of a breach. Auditors should hence conduct their audit with a mindset that recognises the possibility that an actual cyber attack may have happened. Through the performance of the usual audit procedures, it is still possible to identify such cyber incidents.

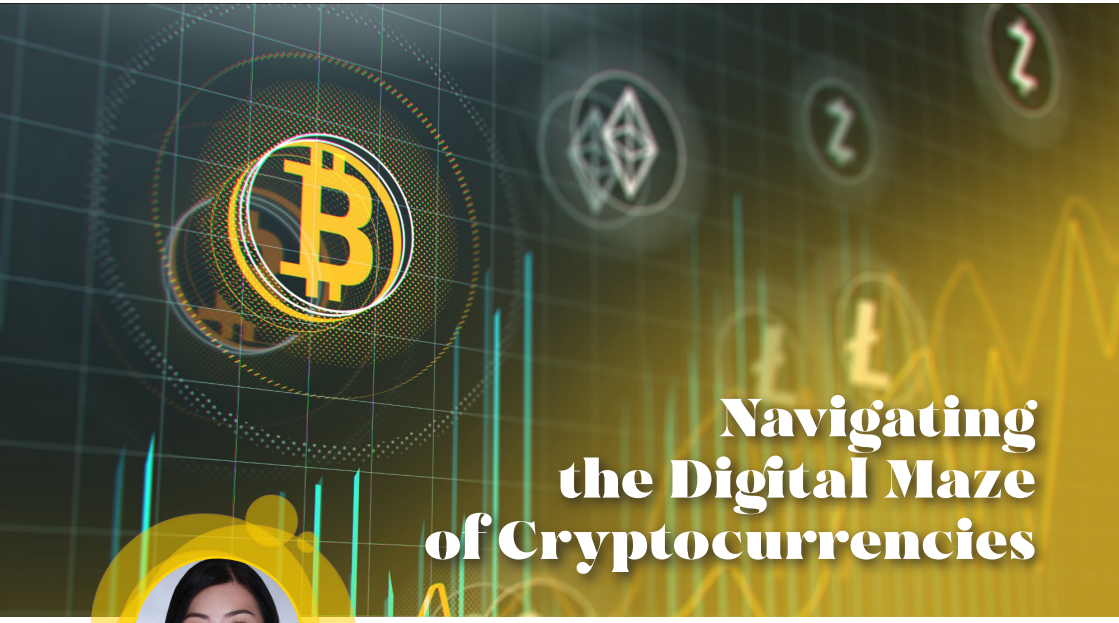
Let us assume that a traditional manufacturing company has no online presence. The auditor had performed the risk assessment and did not identify cybersecurity risk as a key risk area that might give rise to material misstatements of the financial statements. Accordingly, the auditor obtained an understanding, designed and performed testing over the relevant IT general controls. IT specialists were not engaged to perform additional work on cybersecurity testing. During the course of the audit, while

performing testing of the revenue accounts, the auditor noted exceptions to the norm. Upon enquiries and further investigations, the entity then discovered that it had been the subject of a cyber attack which deleted some of its sales transactions. Without appropriate data backups and recovery contingency plans, the entity might not be able to present complete and accurate financial data.

Financial Statements Auditors Do Have a Part to Play

Financial statements auditors are not IT experts who can perform more sophisticated and detailed cybersecurity testing, which requires a special set of skills. However, financial statements auditors should consider and assess cybersecurity risk as part of risk assessment for every audit, as well as the possibility that breaches may have occurred. The conclusion may be that cybersecurity risk is not a key risk area that requires special audit attention, but the assessment is still required nonetheless to make such a determination.

Where cybersecurity risk has been identified as a key risk area that may give rise to material misstatements of the financial statements, the auditor should consider involving subject matter experts. Where a cyber incident has occurred, auditors would have to evaluate and understand the causes and determine whether additional audit procedures or an alteration in audit approach is necessary, evaluate the impact and severity of losses involved and the impact to the financial statements.



Navigating the Digital Maze of Cryptocurrencies

Wang Zhumei
Manager, Technical: Audit & Assurance, ISCA.

This is an updated version of the article which was first published in the IS Chartered Accountant, October 2018. Reproduced with permission from the Institute of Singapore Chartered Accountants.

From an Accounting and Auditing Perspective

Since inception, cryptocurrencies have been described as everything from the future of money to elaborate Ponzi schemes. Regardless of the diverse opinions, it is undeniable that cryptocurrencies are the "in" thing right now, and it is crucial for us to understand them in order to account for and audit them in this digital age.

What is Cryptocurrency?

Cryptocurrency is a virtual currency that is not linked to any currency backed by any government, central bank or legal entity, and does not have any underlying asset or commodity. Transactions rely on a key technology called blockchain technology (see AUDIT RISKS AND CONSIDERATIONS section).

Timeline of Key Events

The birth of Bitcoin in 2009 sparked the development of cryptocurrencies in the decade that followed, and here are some of the notable milestones[1]:

2009

The first Bitcoin transaction occurs when Satoshi Nakamoto, the supposed creator of Bitcoin, sends computer programmer Hal Finney 10 Bitcoins.

2010

A Bitcoin user pays 10,000 Bitcoins (worth roughly US$41 at the time) for two large pizzas, attaching a monetary value to cryptocurrency for the first time. At the current transaction price of Bitcoins (approximately US$6,500 per Bitcoin), these are currently the most expensive pizzas in history.

2011

Bitcoin is reportedly used on Silk Road, an online black market known as a platform for selling illegal drugs. Cryptocurrencies gain notoriety from their association with illicit activities.

2013

Bitcoin experiences its first big bubble, surpassing US$1,200 on one exchange. Meanwhile, various countries attempt to work out the best approach towards cryptocurrencies – at the extreme end, China bans financial companies from Bitcoin transactions, while Vancouver, Canada launches the first Bitcoin ATM.

2014

Tokyo-based Mt Gox, the largest Bitcoin trading exchange at the time, files for bankruptcy after losing US$470 million in a hack. Bitcoins continue to grow in popularity, with big companies such as Microsoft and Expedia accepting Bitcoin payments.

2015

New cryptocurrencies emerge including Ethereum, which is slated to be Bitcoin's main rival. San Francisco-headquartered digital currency exchange Coinbase raises US$75 million in a funding round, the largest amount for a Bitcoin company.

2016

The DAO, a stateless venture capital fund on the Ethereum blockchain, raises $150 million in crowdfunding, only to be hacked a month after its launch with a third of its assets siphoned off.

2017

Initial Coin Offerings (ICOs) and token sales take off at sky-high amounts. On December 17, the price of one Bitcoin reached a record high of US$19,783. Countries continue to diverge in their approaches towards cryptocurrencies – both China and South Korea ban ICOs, while Japan legalises Bitcoin as a payment method.

On local shores, the Monetary Authority of Singapore (MAS) does not regulate cryptocurrencies but monitors the activities surrounding them that may require regulatory response as a financial regulator, such as fundraising through Initial Coin Offerings.

To date, it is estimated that there are more than 1,500 different cryptocurrencies in circulation. The meteoric growth of cryptocurrencies is problematic for accountants and auditors,

1 With reference to *A decade of cryptocurrency: from bitcoin to mining chips* by Rosemary Bigmore published on 25 May 18 in the Telegraph.

with existing accounting and auditing frameworks seemingly insufficient to deal with them. In this article, we explore some of the challenges faced.

An Accounting Predicament

As there are no specific financial reporting standards on cryptocurrencies, the accountant can draw guidance from existing standards with a scope that includes items with similar characteristics as cryptocurrencies. We consider whether it is plausible for an entity reporting under Financial Reporting Standards in Singapore (FRSs)[2] to account for the holdings of cryptocurrencies under the following FRSs:

As cash and cash equivalents in accordance with FRS 7: Statement of Cash Flows

FRS 7.6 states that cash comprises cash on hand and demand deposits, and defines cash equivalents as short-term, highly-liquid investments that are readily convertible to known amounts of cash and which are subject to an insignificant risk of change in value.

Although fiat currencies are accounted for as cash as suggested by FRS 32: Financial Instruments: Presentation AG3, cryptocurrencies are not entirely comparable to traditional fiat currencies due to their relatively limited acceptance and usage commercially as a currency of exchange. They also may not meet the definition of cash equivalents as price volatilities may result in significant risk of changes in value and consequently, entities may not hold them for purposes of meeting short-term cash commitments.

2 Entities can also consider alternative financial reporting frameworks such as Singapore Financial Reporting Standards (International) (SFRS(I)s).

As a financial asset in accordance with FRS 39: Financial Instruments: Recognition and Measurement

If cryptocurrencies are not cash, depending on the facts and circumstances, another possible approach may be to account for them as financial assets at fair value through profit or loss (P&L). However, cryptocurrencies do not meet the relevant definition of a financial asset under FRS 32.11(c), as it does not give the holder any contractual right to receive cash or another financial asset.

As an intangible asset in accordance with FRS 38: Intangible Assets

FRS 38.8 defines an intangible asset as an identifiable non-monetary asset without physical substance. Cryptocurrencies appear to meet this definition as they can be traded or transferred individually (identifiable), are neither money held nor assets to be received in fixed or determinable amounts of money (non-monetary) and are in virtual form (without physical substance)[3].

Cryptocurrencies that fall within the scope of FRS 38 can be accounted for using the cost or revaluation method.

Since cryptocurrencies may be considered to have an indefinite useful life in the context of FRS 38, such cryptocurrencies accounted for under the cost method would be subjected to annual impairment assessment as required by FRS 36: Impairment of Assets, with impairment charges recorded in P&L.

3 Notwithstanding this, broker-traders who trade cryptocurrencies as commodities should consider FRS 2: Inventories, paragraph 3(b), which states that commodity broker-traders should measure their inventories at fair value through P&L.

The revaluation method can be used only if there is an active market in which the cryptocurrency is traded. An active market is defined in Appendix A of FRS 113: Fair Value Measurement as a market in which transactions for the asset or liability take place with sufficient frequency and volume to provide pricing information on an ongoing basis.

Under the revaluation method, increases in fair value are recorded in other comprehensive income (OCI), while decreases are taken to P&L. However, to the extent that an increase in fair value reverses a previous decrease in fair value that has been recorded in P&L, that gain is recycled to P&L. Similarly, a decrease in fair value that reverses a previous increase is recorded in OCI.

Until standard-setters provide further clarity on the appropriate accounting treatment for cryptocurrencies, more rigorous disclosures may be necessary to alert users.

Disclosure in financial statements

Given the complexities surrounding cryptocurrencies, entities with material amounts of cryptocurrencies should consider additional disclosures to enhance the understanding of users, which may include but are not limited to:

- Description of the characteristics of the cryptocurrency, the purpose of holding it and how doing so fits into the entity's business model;
- Considering the price volatility, it may be informative to disclose historical prices of the cryptocurrency and price changes after financial year end, and
- How technology risks surrounding the cryptocurrency (such as cybersecurity risks) are mitigated.

Audit Risks and Considerations

Like accountants, auditors also have to grapple with the uncertainties surrounding cryptocurrencies. Before we delve into the auditing concerns, it is essential to understand how the technology behind cryptocurrencies work.

A digital wallet is an application that stores cryptocurrency. It contains a public and private key – the former being the digital address of the wallet and the latter being the password/digital signature used to access the wallet and authenticate transactions. A blockchain, in its simplest form, is a distributed ledger which contains the relevant details for every transaction that has ever been processed[4].

Figure 1 is a simplified pictorial flow of how cryptocurrency is transferred between digital wallets through the blockchain.

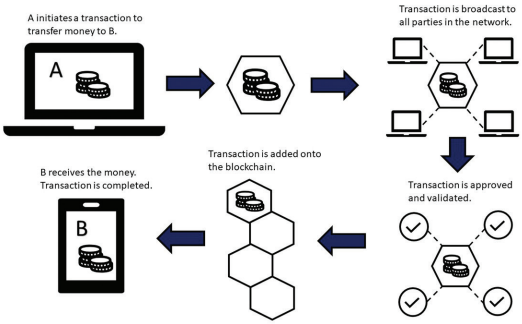


Figure 1 How cryptocurrency is transferred between digital wallets through blockchain

4 For more information on blockchain technology, the reader can refer to "Making sense of bitcoin, cryptocurrency and blockchain" by PwC US.

Existence/Rights & obligations, and completeness of transactions

While cryptocurrency protocols are designed such that they can be used anonymously in principle, most businesses providing related custodian, trading or wallet storage services require proof of identification to comply with anti-money laundering/counter-terrorism financing regulations. As such, we would expect entities holding cryptocurrencies with legitimate service providers to be identifiable, but auditors need to verify that.

For cryptocurrencies held by custodians or exchanges, the auditor can request a confirmation in accordance with SSA 505: External Confirmations, similar to that of a bank confirmation when auditing cash balances held at banks. However, the auditor has to assess the reliability of the response and in the event of non-responses, perform alternative procedures to obtain relevant and reliable audit evidence. For cryptocurrencies that are stored in a digital wallet, ownership of the private key to access the cryptocurrency is critical and the auditor will have to verify this aspect.

A critical concern relating to cryptocurrencies is cybersecurity risk surrounding private keys. When private keys are lost (example, due to system failure, a private key that is stored in a computer is inadvertently erased), the related cryptocurrency can no longer be accessible to anyone in the cryptocurrency network and will effectively be out of circulation. Another risk is the private keys being stolen by hackers and the genuine holders of the cryptocurrency lose their right to the digital currency. As such, audit processes should incorporate an understanding of the cyber environment as part of risk assessment, with considerations such as whether the entity has effective IT backup and restoration procedures, and IT security processes in place to mitigate risks of external attacks[5]. In addition, the auditor has to consider if there are adequate controls in place to safeguard and prevent unauthorised access to the private keys to prevent misappropriation of the cryptocurrency.

For cryptocurrencies held by custodians or exchanges where private keys are safeguarded by these external parties, auditors may need to consider the custodian or exchange's IT controls under SSA 402: Audit Considerations Relating to an Entity Using a Service Organisation.

To verify the occurrence and completeness of cryptocurrency transactions, a logical approach would be to rely on the blockchain, since it stores information on all the transactions that have been processed since day one. A stumbling block is that the cryptocurrency blockchain itself is not audited. While proponents of blockchain argue that it provides irrefutable history and integrity, can we trust the blockchain simply based on the technology behind it? Or does the blockchain need to be audited?

Arising from the IT complexities surrounding cryptocurrencies, the engagement partner should also consider if team members possess the relevant IT knowledge to perform the audit engagement in accordance with professional standards and if there is a need to engage IT experts in accordance with SSA 620: Using the Work of an Auditor's Expert.

5 For further guidance on cybersecurity risks, please refer to "Cybersecurity Risk Considerations in a Financial Statement Audit" issued by ISCA in June 2018.

What price is right?

Although the intuitive approach to the fair value of a cryptocurrency (assuming that it is actively traded) would be the trading price on an exchange, varying prices across exchanges is an issue. For instance, take the prices of Bitcoin from the top exchanges (in terms of volume) as of 9.27 a.m. SGT, 24 April, where the difference between the highest and lowest price was about 12%.

Figure 2 Bitcoin prices from top exchanges (by volume)

Exchange	Price (US$)	24H Volume (US$)
P2PB2B	5,454.15	61,924,026.08
Coinsbit	5,469.70	27,929,748.97
Bitstamp	5,516.84	58,413,504.90
Kraken	5,517.60	49,142,176.47
Coinbase	5,518.37	106,616,321.04
itBit	5,519.75	14,096,978.71
Gemini	5,521.81	19,010,681.73
EXRATES	5,524.70	28,691,613.60
Bitfinex	5,530.20	109,277,748.63
Simex	5,574.24	9,247,623.70
Independence Reserve	5,615.55	27,623,070.97
LakeBTC	6,084.25	11,295,083.74

Source: Extracted from CryptoCompare website, arranged from lowest to highest price per bitcoin

As prices can be volatile and driven by speculation instead of economic factors, fair value measurement is a key audit risk area. When auditing fair value, the auditor should consider if the accounting policy has incorporated data from different sources of exchanges to address such price differences.

For cryptocurrencies that are not actively traded, fair value measurement may not be so straightforward. As much as possible, an entity should maximise the use of relevant observable inputs, such as prices of buy or sell offers on peer-to-peer exchanges, which are more reliable.

Conclusion

Currently, we are seeing global efforts working towards unified cryptocurrency regulations, such as the G20 calling for international standard-setting bodies to assess multilateral responses during their meeting in March this year. While we await more clarity from standard-setters, we will have to work within the boundaries of the existing standards in the meantime to find the most appropriate approach so as to ensure that the financial statements for companies with cryptocurrency holdings are as reliable and relevant as possible.

Learning to Trust in Artificial Intelligence

As ICAEW launches a new ethics and tech resources hub, its experts talk about the ramifications of using artificial intelligence in business and finance – exploring evolving responsibility, accountability, ethics and more.

This article was first published in ICAEW's Chartech publication, January-February 2019. Reproduced with permission from the Institute of Chartered Accountants in England and Wales

Public discourse around artificial intelligence (AI) has tended to prey on emotion: instilling panic about a robot takeover in the workplace; sowing doubt about trusting self-driving cars and so on.

But for those working in fields that have already started to embed AI, such as accountancy, fears are more specific than generalised. While generating huge volumes of insight that might benefit businesses, algorithms being developed to crunch enormous data sets are so sophisticated they verge on the opaque.

Accountants, driven by professional scepticism, ask: if they cannot understand these systems, should they be trusting the outputs? As the US Defense Advanced Research Projects Agency (Darpa) puts it: "Continued advances promise to produce autonomous systems that will perceive, learn, decide and act on their own. However, the effectiveness of these systems is limited by the machines' current inability to explain their decisions and actions to human users." Furthermore, the fact that algorithms can create outputs that accountants would find biased means the ethical obligations of the profession are being tested on several fronts.

To address issues and dispel the fears emerging around AI, ICAEW has created a new ethics and tech hub. The site brings together expertise from the ethics team and the IT Faculty, as well as the Financial Services and Audit & Assurance Faculties, where data analytics driven by AI is more advanced than

in other sectors. For example, telematics have been used to offer cheaper insurance to people in otherwise high-risk categories in return for having their driving performance tracked.

But there have been examples of algorithms making decisions that led to unintended consequences (eg, accusations of racism) because the algorithm acted on information contained in historic data sets.

Evolving Responsibility

IT Faculty technical manager Kirstin Gillon says the hub's mix of know-how, practical guidance and knowhow will hopefully help members be more comfortable with AI over time. Points raised during ICAEW's Ethics Standards Committee meetings and at topical roundtables are also feeding into faculty work and the hub. Contributions come from people in business, as well as big and small firms. Gillon says that accountants' questions are most often framed around AI's impact on society and the wish to do public good: "They have concerns about surveillance and the impact on privacy."

In effect, practitioners want to know how adoption of AI will affect their ability to stay true to the five core principles of their ethical code: integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. Last autumn, panellists at the World Congress of Accountants (WCOA) debated whether the ethical code needed updating to reflect recent technological advancements.

Ethical conversations are also happening between companies developing AI-enabled systems. The Partnership on AI consortium includes Amazon, Apple, Facebook, Google, IBM and Microsoft. Open AI, a non-profit for research sharing, was co-founded by Tesla's Elon Musk. DeepMind, a UK-based pioneer of neural networks bought by Google in 2014, has an ethics and society arm peopled by academics from Oxbridge and Cornell. It states: "New technologies can be disruptive, with uneven and hard-to-predict implications for different affected groups. We have a responsibility to support open research and investigation into the wider impacts of our work."

"There are plenty of forums for discussion, particularly in the UK where there is a lot of research going on," Gillon agrees. "But because the tech firms are the ones leading on innovation, the debates are heavily driven by their sector. Maybe accountants should have a stronger voice, given our ethical focus and experience."

She says the ethical code doesn't stand alone: "It's embedded in our training and disciplinary systems."

Accountability

Another reason for accountants to be involved in framing the AI ethical debate is their level of accountability, particularly where so-called black box systems are being adopted. Gillon asks: "How do you make sure you're making decisions that are morally correct and error-free, as well as put right mistakes?" Participants in an ICAEW ethics roundtable in May 2018 said: "We are in the spotlight every time a system is to blame." The roundtable suggested the profession would need to be involved in creating assurance frameworks that determine "whether firms/systems are operating in accordance with ethical principles".

ICAEW integrity and law manager Sophie Falcon says: "There has been some high-level discussion at the Ethics Standards Committee about how the code of ethics would apply if you have intelligent machines as part of your workforce. One strand of thought is that they could be considered similar to staff. If you have this kind of 'being' doing work for you, is it analogous to when you're training it and still responsible for reviewing what it produces, and the buck stops with you? Could you look at where the code of ethics refers to 'member' and change it to say 'member or machine'?"

Machines cannot fear being made redundant in the event of causing a particularly bad mistake, but they can be programmed to have particular reactions and learn from them. Falcon says: "Part of professional ethics is that there are consequences if you breach them and you can be disciplined.

"In terms of the general principles, you need to act fairly and you need to be honest and truthful. You need to do a good job and keep things confidential. There is no reason why you couldn't specify those parameters for tasks you were getting a machine to do."

In Theory...

The WCOA panel discussion indicated that adding AI-specific elements to ethical accounting codes is still at an early, theoretical stage. But Falcon agreed the profession would not be able to "absolve itself of the responsibility" of a machine's actions. It could become a real challenge for accountants who want to learn the ins and outs of AI algorithms before they will trust them.

Gillon agrees: "It comes down to a trade-off between accuracy and understandability. There will be times when accountants don't need to understand the AI. And there'll be other times when you really do need to understand how the program has come to this recommendation that you're going to rely upon."

Falcon and Gillon both refer to explainable AI (XAI), which tech specialist David Gunning of Darpa says will "produce more explainable models, while maintaining a high level of learning performance (prediction accuracy)" and "enable human users to understand, appropriately trust, and effectively manage the emerging generation of artificially intelligent partners".

Such machines, "that understand the context and environment in which they operate, and build underlying explanatory models that allow them to characterise real-world phenomena", are expected to be realised in what Gunning calls third-wave AI systems.

Adapting the XAI concept for accounting, Falcon says: "You wouldn't be checking the technology: you'd effectively check its thought process and whether this was in line with the principles you required."

Ethically Speaking

Those looking to regulate or at least advise accountancy on ethics in future will surely examine how things have played out so far in financial services.

"Technology can help design and distribute better products, and widen access to financial services on sustainable terms by giving a better view of risk," says Philippa Kelly, head of ICAEW's Financial Services Faculty. Tech

firms have long been disrupting traditional banking and insurance providers by meeting demand for cheaper, targeted products through apps and other platforms that rely on customers providing personal data. But the AI that helps to deliver these improvements has been found wanting enough to warrant greater oversight.

Kelly adds that the Senior Managers' Regime (which applies to banks and insurers, and will apply across the whole of the financial services industry from December 2019) emphasises the need for boards to get a handle on where big data and AI are being used. "They need to be responsible for the outcomes the increased use of technology delivers, and they might not presently understand what those are," she says.

There are numerous ethical challenges to face in the financial services sector, for example around offers of credit. Card companies will receive a swipe fee in addition to interest charged on purchases, which means it is in the company's interest for customers to rack up transactions. Reward credit cards trade in a similar fashion, giving bonus rewards or discounts if the spend adds up to a certain monthly level. Kelly notes: "These inducements will likely be offered to customers following an analysis of past card use to figure out where and when you're most likely to spend more. But the ethics of encouraging higher spending are questionable when one in six borrowers is in financial distress."

Another dilemma, first outlined in the Financial Services Faculty publication Audit insights: Insurance in 2015, concerns "the potential to undermine the concept of pooled risk in insurance". A turn towards individualised policies might leave certain people uninsurable. The potential for change is huge in health and life insurance. Kelly says: "If you think about the proliferation of data that people are willingly sharing and generating – from genetic testing (23&Me and other family tree services) to daily heart rate patterns (FitBit and Apple Watch wearers) – it's likely that these developments would further distance those who could most benefit from it from being able to access health and life cover."

The Double Bind

Financial services will definitely benefit as XAI systems come to the fore. Investment managers have employed the same sceptical and cautious mindset as accountants before applying AI models to their portfolios. Kelly says: "One leading investment manager found that an AI liquidity risk model was significantly outperforming traditional methods. However, the type of AI used, neural networks, meant that the reason for the outperformance couldn't be explained.

"This meant the model couldn't be used, as there would have been a lack of effective governance if senior managers weren't comfortable using AI that couldn't be explained."

This outlines a secondary dilemma. Philippa adds: "By not taking the action that makes the best return on their investments, they're not doing the right thing. But their duty of care also means that if they were to use the technology that couldn't be explained, even if it got a better result, they also wouldn't be doing the right thing."

This double bind is the kind of AI problem that ICAEW's AuditFutures programme is concerned with. AuditFutures hosted a

discussion with the University of Edinburgh in November 2018 to consider the challenges and opportunities arising from the development and use of AI systems.

Findings from the two bodies' ongoing collaboration indicate that there is a low tolerance of failure from AI systems, which are expected to make "better than human judgements". The majority of automation has so far occurred at entry level, and AI is not yet able to take over from humans in areas where wisdom, experience, professional judgement, selectivity, instinct and general knowledge must be applied.

But Martin Martinoff, AuditFutures programme manager, argues that it's important to remember that algorithms are more than just lines of code: "They are a powerful means of social control, and their social impact can limit our decisions, signal certainty in uncertain conditions, push us towards actions we would not otherwise have taken, and limit our access to broader information." These realisations drive calls for greater transparency.

Black box technology in AI protects proprietary information in highly competitive markets, but also demonstrates that transparency may be a one-way street. Martinoff says companies are using a range of technologies such as facial and voice recognition, and textual analysis to enable targeted advertising, but this depends on gathering otherwise private information that can even impinge on people's protected characteristics – such as the state of our mental health, sexual orientation, religious beliefs and genetics.

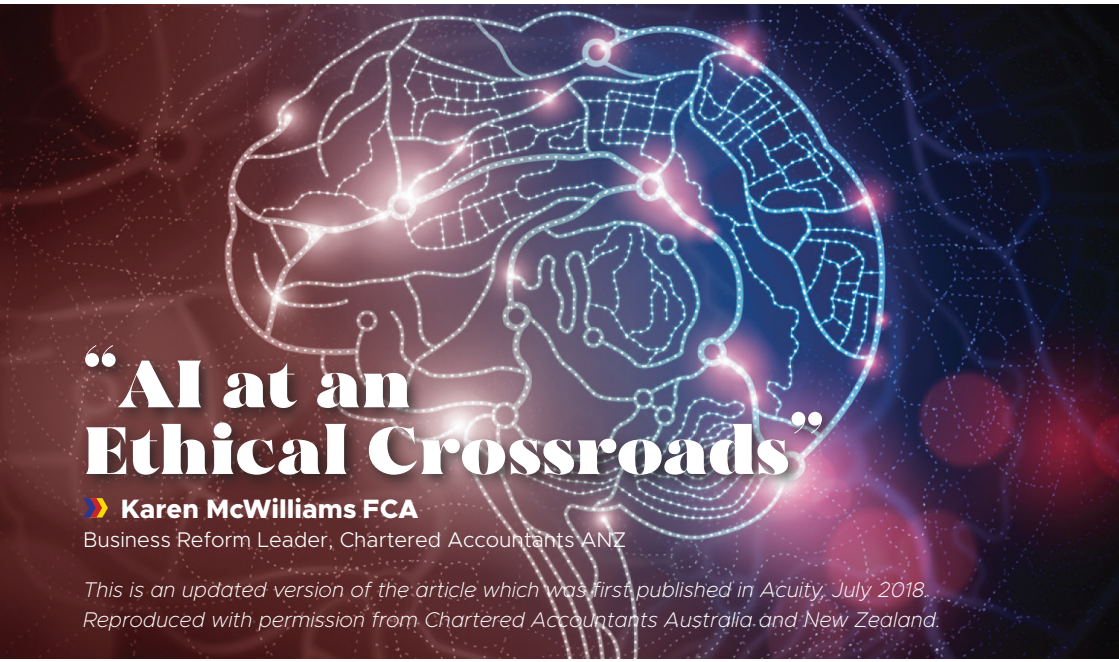
As the adage goes, if you're not paying for the product, you are the product. This becomes a further problem when the data collected for a given purpose "reflects and exacerbates structural biases or introduces new ones". Martinoff says this can lead to the "encoding" of discrimination and particular sets of values within algorithms, which surface as prejudice – and in financial settings these lead to uncomfortable outcomes in areas such as credit scoring.

Getting Ahead

The Financial Services Faculty will lead on the publication of a series of thought leadership papers about ethics and AI in 2019. The first instalment of Ethical use of big data in financial services will look in more detail at scenarios where big data has presented ethical dilemmas, as well as share principles for financial services firms and their boards, and information for consumers. The IT Faculty is also working on a paper, and expects to develop a webinar in due course.

The Ethics Standards Committee will continue to feed in to the International Ethics Standards Board for Accountants, along with ICAEW staff who met with the Board in January, in anticipation of any long-term project to address ethical updates to the code.

Accountants won't be the only professionals grappling with the philosophical debates around AI as its use continues to expand. But by starting the hub now, while discussions about updating ethical codes are still young, it means accountants will have the necessary means to prepare.



"AI at an Ethical Crossroads"

Karen McWilliams FCA
Business Reform Leader, Chartered Accountants ANZ

This is an updated version of the article which was first published in Acuity, July 2018. Reproduced with permission from Chartered Accountants Australia and New Zealand.

In Brief

- Artificial intelligence is revolutionising our world but we need to ensure we also flourish as human beings alongside it
- AI brings with it a range of ethical considerations and we all need to be part of that dialogue
- Accountants can help to test and build artificial intelligence industry standards for design, audit, algorithms and transparency

---

From smart cars to smart phones, artificial intelligence (AI) has invaded every aspect of our lives. In the digital age, this new technology is raising ethical issues unlike any we have had to consider before.

To date, the media focus on AI has been characterised by two extremes. At one end, the focus is on the tremendous benefits and exciting opportunities AI can deliver for how we live and work. At the other end, robots are going to take over our jobs in a world of big brother surveillance. These differing perspectives show the need for an ethical framework to help shape developments.

The Fourth Revolution

Machine learning has been referred to as the fourth industrial revolution. Machine learning is a subfield of AI which is focused on designing

systems that can learn from and make decisions and predictions based on data.

Recent advances in machine learning now bring us to an ethical crossroads where we need to decide the role AI and machine learning will play in shaping our future. To present a more holistic snapshot of this fast-paced technological movement, Chartered Accountants Australia and New Zealand has published *Machines can learn, but what will we teach them?*

According to the report, the rapid progress being achieved in AI means that super intelligent machines are now seen as the next development stage, where these machines will learn to write code for themselves. "This is how machines can possibly become independent of programmers and where, perhaps, even greater risks lie," the paper says.

The growing range of AI services and products means that individuals need to better understand how AI is impacting upon them.

The rise of fake news created by bots and its distribution, along with hate speech, on platforms such as YouTube, Twitter, Facebook and Instagram has shown how technological advances can undermine the foundations of democracy. The Cambridge Analytica data scandal was a wake-up call to humanity and, for the first time, we collectively asked: "How much do the machines know about me?"

In the commercial world, it is essential for businesses and other organisations to have an AI ethics code or refreshed governance protocols to outline what the algorithm is expected to do as well as its limitations. Ideally these should be shared with customers, so they can make informed choices about who they are doing business with.

Ethical Concerns

At the societal level, we need to consider how we will overcome issues such as the transparency and bias of algorithms. For business, there are a number of ethical concerns about designing and implementing technology, including fairness and privacy. In addition, interventions will be needed to transition the workforce to an AI-enabled economy, including upskilling and reskilling. The potential for humans to work alongside intelligent machines will provide the greatest opportunities for both increased productivity and increased human satisfaction from the new services and products that can be designed. Tomorrow's business world will need to develop and nurture a balance of artificial and human intelligence.

Ethical Frameworks

There is also a need for a global agreement around developing an ethical framework for AI and we are already starting to see progress. For example, in May 2019, the Personal Data Protection Commission in Singapore released the first edition of a proposed AI governance Framework, an accountability based framework to help chart the language and frame the discussions around harnessing AI in a responsible way. In Australia, the government has begun consultations on the development of a national Ethics Framework and a Standards Framework "to guide the responsible development of these technologies".

However, the development of ethical frameworks is typically slow compared to the pace of technological change, as Professor Nicholas Agar of Victoria University of Wellington points out: "Our pace of ethical reflection tends to be slow and deliberate, typically slower than the pace of technological progress. We need to have open conversations around the ethics of AI and share different ethical perspectives. These open conversations should address many different scenarios about what hasn't happened yet but could in the future. We need to think creatively about what we are and can be. That way we can make regulations that protect what we really care about."

How Accountants Can Help

The accounting profession has a pivotal role to play in ensuring that business information is sound and that business decisions are in step with wider societal values. They can help to build consensus around AI industry standards for design, auditing and transparency, as well as identifying techniques to increase public trust in these new technologies.

As Peter Williams FCA, Chief Edge Officer, Centre for the Edge at Deloitte Australia notes: "AI can show us things, but we need humans to identify what we do about it. When organisations make assertions about an algorithm, the role of the auditor will be to test those assertions to ensure the algorithm does what they asserted it did. Software code is not infallible, mistakes can happen and on vast scale. Accountants are in the box seat to continue to act as trusted advisers to interrogate the systems and processes that underpin the acquisition, management, analysis and disposal of this information."

The profession will need to commit to continuous learning in the area of AI to ensure it has the expertise and knowledge to meet the fundamental ethical standards including duty of care and competency.

Artificial intelligence augments our abilities, enabling us to achieve greater efficiencies and higher levels of performance. However, it is also changing us in ways we are not fully aware of. It is clear that we have reached the point where we need to start considering these ethical implications and proactively take steps to prepare with global and local frameworks. We need to tune our ethical antenna to ensure we take the right road at the right time. Failing to build an ethical dimension into each stage of our AI journey, could bring serious consequences that prove difficult to reverse.