EMERGING TECHNOLOGIES AND THEIR IMPACT ON ACCOUNTING AND ASSURANCE

MILAN SHETH | RAGHAV SHUKLA
Chartered Accountants

INTRODUCTION

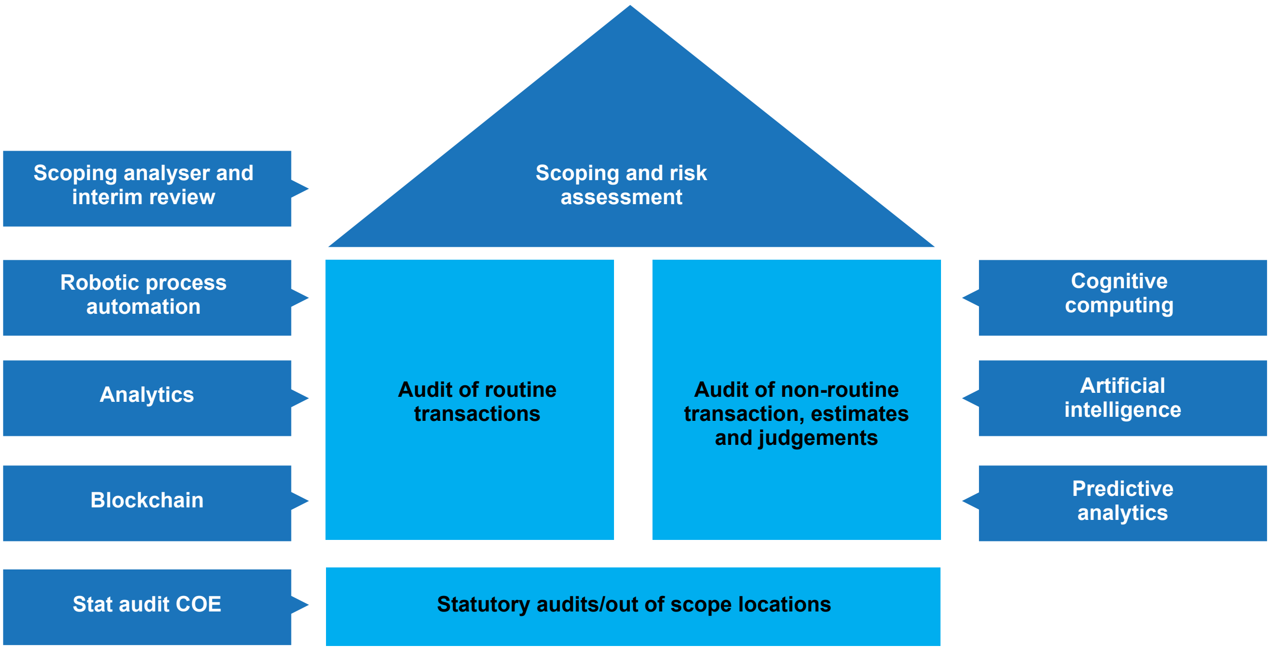
Emerging technologies such as Robotic Process Automation (RPA), Cognitive & Artificial Intelligence, Analytics and Blockchain present significant opportunities for both improving our world and creating competitive advantage but they all bring with them new risks that need to be understood, managed and assured.

The speed, ubiquity, complexity and invisibility of technological change has driven holes through and paths around our traditional three lines of defence. Without new approaches to accounting and assurance, there is the danger of a breakdown in the willingness of people to engage with technology and to share data — an erosion of the 'digital trust' which is increasingly important to the success of organisations, economies and societies.

Just as technology is enabling business to do things they have never done before, so it is for auditors. The basic premise of audit today remains what it has always been; to give assurance to the capital markets that a company is correctly reporting its financial results. Nevertheless, auditors are now using powerful technological tools to deliver more comprehensive and even higher-quality audits.

These tools also save time that can be spent focusing on complex areas of the audit and those that require judgement. And because the tools enable the analysis of a complete data population, they allow the auditor to add value by commenting on processes and discussing related business issues with audit committees and company boards.

DIGITALLY TRANSFORMED AUDIT & ASSURANCE FUNCTION


Scoping analyser and interim review
Robotic process automation
Analytics
Blockchain
Stat audit COE
Scoping and risk assessment
Audit of routine transactions
Audit of non-routine transaction, estimates and judgements
Statutory audits/out of scope locations
Cognitive computing
Artificial intelligence
Predictive analytics

RPA: TRANSFORMING AUDIT DELIVERY MODEL

Robotic process automation (RPA) – the automation of rule-based processes and routine tasks using software applications known as "bots" – is one of the digital enablers of the transformation of the audit. RPA is a fast, accurate and efficient way of processing structured data from bank accounts and financial systems. It can be used to perform general ledger analysis – for example, finding journal entries that do not balance, are duplicated or are of a particularly high value – and to create audit-ready work papers.

Benefits of RPA in audit include global consistent quality, analytics driven approach, accelerated audit start and reduced burden on audit team and client. Some of the audit activities where RPA is being increasingly adopted by companies globally includes:

1. Data preparation:

- Automated and streamlined data capture from multiple systems
- Data mapping
- Reconciliation of data
- Check completeness of data

2. Audit procedures

- Analytical review
- Sample size calculation and selection
- Automation of basic audit procedures
- Analysis of trial balance, journal entries, application of agreed risk criteria and materiality levels
- Audit confirmations from vendors, financial institutions *etc.*

For example, in Australia, over 50% of leading auditor's bank audit confirmations for the recent 30 June year-end were lodged by a robot. The robot submitted confirmation requests, managed the process (including exceptions) and provided work papers back to the audit team, along with the formal confirmation. This allowed the audit teams to focus on judgmental areas rather than administration, accelerated and identified issues earlier, reduced potential audit surprises, and improved client service. Further solutions that employ RPA are now being developed.

AI: WELCOME TO THE MACHINES

Artificial Intelligence (AI) could be a game-changer for business generally, and professional services in particular. With the rapid developments in machine learning, data mining and cognitive computing, the next decade promises to see huge leaps forward.

While the excitement over the potential applications of AI is understandable, there are some misconceptions – and indeed fears – developing. Central to that is the fear that AI will in fact replace humans in the value chain – doing the tasks we currently do, but faster and more accurately, and thus rendering many of us redundant.

We are currently at the beginning of that journey. Following a lull in the pace of development, the last three years have seen applications of AI becoming more mainstream across professional services.

Take, for instance, the issue of lease accounting. This is a hot topic, given the recent accounting changes that demand that companies scrutinise their position with regard to leases and recognise related liabilities.

Until now, analysis of lease accounting has mainly been performed using human review. However, current pilot programs indicate that AI tools may allow the analysis of a larger number of lease documents in a much shorter timeframe. These pilots show that AI tools would make it possible to review about 70%-80% of a simple lease's contents electronically, leaving the remainder to be considered by a human. With more complex leases (in real estate, for instance), that figure would be more like 40%, but as the tools improve, and the machines learn, it is likely that more complex contracts and data can be read, managed and analysed.

This illustrates some of what narrow AI can deliver. It cannot, as yet, replace the judgement, scepticism or experience that humans bring to their work. Making comparisons or value judgements is not the function of this type of AI

But the real benefit we are now beginning to see through this type of application is in its predictive value. We recently used deep learning technologies to "learn" from seven years of financial statements through six machine learning algorithms. This enabled us to survey enough data to better evaluate where restatement risks lie. The technologies make it possible to predict where future risks may occur and enable audit teams to revisit and refine their approach. They also present intriguing possibilities for the detection of fraud.

That predictive ability marks the next step in the evolution of AI, and allows auditors to carry out work like this more efficiently and with greater accuracy.

AI can do a lot, but there's also a lot it cannot do, and we cannot rely on it to deliver scepticism and judgement.

PREDICTIVE ANALYTICS: SHORTCUT TO TOMORROW

Data analytics is being increasingly applied to almost 100% of transactions at various stages in audit by companies to bring enhanced insight and value. This includes planning, interim as well as year-end audit procedures.

Data analytics provides auditors with an enhanced ability to:

- Focus on areas of risk
- Ask better questions
- Detect unusual items
- Strengthen professional scepticism

Predictive analytics combined with data visualisation and reporting is being applied in the following audit activities using both structured as well as unstructured data:

1. Scoping

- Dashboard reporting for stakeholders
- Repeatability and audit trail
- Work-paper generation

2. Interim Financial Statement Review

- Flexible period comparison
- Intelligence on group operation
- Core 'not significant' BS and IS analysis

3. Single and Multi-dimensional trending analysis of Key Performance Indicators/Key Risk Indicators:

- Financial
- Non-financial
- Intra-component
- Inter-component

BLOCKCHAIN: BUILDING BLOCKS OF THE FUTURE

Blockchain may be best known as the distributed ledger technology that underpins the digital currency Bitcoin, but it could also be used for a host of other purposes that involve transmitting data securely. These include payment processing, online voting, executing contracts, signing documents digitally, creating verifiable audit trails and registering digital assets such as stocks, bonds and land titles. Its potential for application within the transaction-based financial services industry is particularly vast, but it is relevant to organisations in every sector.

Going a stage further, blockchain could even overturn entire business models in certain sectors by empowering the growth of "virtual organisations," also known as decentralised autonomous organisations (DAOs). DAOs operate through computer programs known as "smart contracts" that carry out the wishes of human shareholders by automatically executing the terms of a contract – for example, transferring money or assets.

In the future, finance teams could make use of distributed ledgers – together with artificial intelligence – to automate a range of processes, from payments through to foreign exchange trades and the filing of tax returns. For greater efficiency, finance functions could even outsource parts – if not all – of their routine work to DAOs.

Finance teams could work with blockchain in different ways, observes Professor Nigel Smart from the department of computer science at the University of Bristol in the UK. "They could have multiple distributed ledgers, each one doing something different. Or they could have big distributed ledgers, with lots of different things going on within one ledger. Some data may be visible to everybody, while other data may be encrypted so that it is only visible to a small group of people."

Since the data stored in distributed ledgers is authenticated by multiple parties and continually updated, it offers finance teams the possibility of both real-time reporting to management and external auditors, and being able to work more effectively with their external audit and tax providers.

It's likely that auditing will also be revolutionised by blockchain. Key to the technology is its record of transactions, which enables something akin to real-time auditing by default. Indeed, blockchain has been dubbed "digital era double-entry bookkeeping" because of its similarity to old accountancy principles.

Blockchain might also be able to replace random sampling by auditors, by making it easier and more effective to check every single transaction using code. This would also make it easier to investigate fraud, since real-time systems could highlight and investigate anomalies.

Blockchain's rise doesn't mean the end of the finance or audit team. Real-time auditing and reporting will release CFOs and their teams from certain routine, time-consuming tasks so that they can play more strategic, creative roles – and focus on new ways to deliver future business value, rather than keeping track of past costs. And human interpretation of data and transaction patterns will still be needed to generate the new insights that can lead to business growth.

Blockchain's rise doesn't mean the end of the finance or audit team.

EMERGING TECHNOLOGY CHALLENGES FOR ASSURANCE

There are four common characteristics of emerging technology that have made designing appropriate assurance techniques increasingly challenging:

1. Speed

The pace at which new technologies such as Blockchain and AI are evolving drives three main challenges:

- 'Pilots', 'proof of concepts', 'agile' and other quick ways of implementing emerging technology means that it has often landed and is in use inside an organisation before the assurance implications have been considered

- By the time technical assurance training has been developed and rolled out (with equally beautiful PowerPoint slides), the technology has often moved on. Traditional methods for developing and delivering training haven't kept pace with the rate at which technology is evolving

- Regulators and professional bodies have yet to develop frameworks and approaches for guiding how these should be considered, implemented and assured

2. Ubiquity

The extent of the potential, and in some cases actual, adoption of these technologies creates a further challenge. Simply put both the likelihood and impact of emerging technology risks are increasing:

- The likelihood increases as the breadth of adoption increases. For example Gartner predicts that AI will be in almost every new software product by 2020[1].

- The impact increases as the depth of adoption increases. For example, IoT technologies are increasingly used to control and protect national infrastructure and AI is being used in healthcare both for diagnosis and recommendation of treatment

3. Complexity

Emerging technologies aren't impacting organisations in nice bite-sized chunks:

- Convergence means these technologies interact (for example, there is no reason you can't use AI to process Blockchain transactions on IoT). The ever increasing interactions between autonomous computer systems may lead to unpredictable and potentially untraceable outcomes and as such technology specific assurance approaches are of limited value

- Extended enterprises mean that these technologies are not controlled exclusively by the organisation and are often adopted through the use of third party services or dictated by the supply chain. Increasingly, the data that is used by emerging technologies is shared between organisations

4. Invisibility

There is a danger that is risks and therefore the need for assurance goes unnoticed:

- The very existence of the emerging technology components may be unclear when it is embedded into things we use. Software may include things such as machine learning and a service maybe delivered using automation e.g. chat bots.

Even where this use is clear, there is often no transparency around the level of assurance that has been already been performed over it.

- The need for assurance may be less visible to teams where the risks created by emerging technology initially impact stakeholders outside of the organisation. For example profiling based on observed data (collected through online activity or cctv), derived or inferred data could cause significant unwarranted reputational damage for an individual.

KEY IMPACTS OF EMERGING TECHNOLOGY ON EXISTING ASSURANCE APPROACHES

Whilst developing approaches to each emerging

[1] *https://www.gartner.com/newsroom/id/3763265*

technology in turn can provide useful guidelines for teams (where they land in isolation and this can be done quickly enough) we believe there are three more fundamental shifts in assurance approaches that need to be considered by assurance leaders:

1. From post to pre-assurance

Assurance after the event is increasingly irrelevant. Whether its machine learning models that can't be retrospectively audited, the risk of almost instantaneously processing millions of items incorrectly (but consistently) with RPA or the immutability of Blockchain. The impact of not assuring emerging technologies before the event will increase in line with the increase of the power and responsibility being entrusted to them as they are embedded into safety critical, or decision making, systems. Perhaps the most quoted example of this is a model used to support criminal sentencing in the US by looking at the likelihood of reoffending.

This significantly under-predicted white males reoffending and over predicted black males based on questions which introduced bias into the algorithm[2]. Considering the impact of this example then merely detecting discriminatory decisions after the event will not be sufficient. Under the accountability provisions of legislation such as GDPR organisations will need to find ways to build discrimination detection into emerging technology to prevent such decisions being made in the first place.

Assurance after the event is increasingly irrelevant.

2. From timely to time limited assurance

Assurance teams spend a significant amount of effort in providing comfort over processes, profits and projects based on how well they are doing at a point in time and provide little comfort as to how long into the future the assurance will remain valid— what is the 'assurance decay'? If a continuously evolving model is working as expected now, what assurance do we have that it won't start producing erroneous decisions and predictions going forward? While this may be an implicit gap in how assurance is reported today, emerging technology will accelerate the need to address this. To achieve this, the scope of assurance plans and reporting need to evolve to address questions such as:

- What are the things that we have assumed remain constant for the assurance to be valid?
- What ongoing monitoring controls are there that the assurance and these assumptions remain valid?
- Are there any specific triggers which would cause us to revisit or revise this assurance as it would not be valid?
- What assurance is there over controls which cover ongoing change management and evolution of systems?

3. From data analytics to data dialectics

Over the last decade assurance teams have increasingly attempted to use data analytics to improve the way they scope, risk assess and deliver their work. Even basic analytics have driven additional insight and comfort in areas ranging from fraud (e.g. ghost employees) to commercial benefits (e.g. duplicate payments). While many aspire to move towards more advanced analytics such as continuous controls monitoring, emerging technology significantly increases a challenge that has already slowed progress for teams in this area. Simply put:

- The 'black boxes' are getting darker. As we move into areas such as AI it is becoming harder to understand how systems are processing things; and
- The 'data exhausts' are getting bigger. Exponentially more data is being generated by technologies such as IoT.

While there will no doubt continue to be a role for traditional analytics moving forward (including over emerging technologies such as RPA), we believe that assurance teams should also develop a data dialectics approach — focusing less on testing what the system has done and more on what it could and should have done. To bring this to life:

Assurance teams should also develop a data dialectics approach — focusing less on testing what the system has done and more on what it could and should have done

- A simple example of generating an independent expectation in practice has been to predict store level revenue based on weather, footfall and advertising campaigns and using this to highlight stores reporting revenue out of line with central expectations.

[2] *Angwin, Julia. Make Algorithms Accountable. The New York Times, 1 August 2016*

- A simple example of using an appropriate questioning approach is querying a machine learning model to understand its sensitivity to changes in training data and for specific outcomes understand which features are most heavily driving this outcome and what would have to change to change the outcome. Even where the underlying model is inscrutable a data dialectics approach provides a step towards better algorithmic assurance.

SKILLS AUDITORS NEED & ARE CAs PREPARED FOR THAT?

This technology is already impacting our organisations and this will only increase — we need to quickly develop a plan that navigates a path between waiting (and potentially being too late) or over focusing on this at the cost of other areas that require attention. The reality is we have neither the luxury of doing nothing nor doing everything we would want to. We suggest three steps to consider in developing a practical response to assuring emerging technology risks.

1. Develop a rough map and start skirmishes

Starting work in this area is important both to address existing emerging technology risks as well as developing capability and confidence to deal with this as it increases in the future. In our work in this area we have found there are four key corners to considering developing a rough map:

- Verifiability: What are the consequences of doing nothing now on our ability to assure but more importantly control this area in the future — will the horse already have bolted?

- Visibility: To what extent is the technology already understood with robust guidelines in places to how it can be assured and controlled?

- Value at risk: What is the likely impact in the future of risks not being addressed in this area including the current direction of regulation (e.g. privacy)?

- Velocity: What is the speed of likely adoption and impact of this technology in the organisation in the future?

Having developed a view of where we should focus our efforts, it is important to start skirmishes early when we believe there will be an issue rather than when they believe there will be an issue.

2. Train the troops

From our own experience in developing approaches to assuring emerging technology we suggest three areas of focus to enable our teams to build the right skills to remain relevant to their organisations:

- Give them first-hand experience: '*The map is not the territory*' — teams can't prepare to deal with emerging technologies just by reading whitepapers (however well written and informative they might be…), attending breakfast briefings or webcasts. Training your entire team in becoming technical experts in data science isn't realistic either. To truly understand and be able to assure emerging technologies the team needs to get hands-on with them — this means seeing it in action, playing with it and gaining more than a superficial knowledge.

- Develop effective communication and relationship skills: The shift to pre-assurance may seem like a sensible step but for it to work involved up front. To do this they need more than ever to be able to build the relationships that will allow them to be invited to the table at the right time to stand shoulder-to-shoulder with the rest of the business — relying on assurance dictates and stage gates alone won't be enough to achieve this. Therefore as the deployment of emerging technologies increases so does the need for effective communication and relationship building skills in assurance teams.

Relying on assurance dictates and stage gates alone won't be enough to achieve this

- Train for higher order skills — the need to become more 'human': Ethics is an area where we have clearly stated we need to collectively raise our game as an assurance profession in terms of embedding this into our assurance plans and therefore also in how we train our teams to understand and deal with this. However, we believe developing other higher-order skills will enhance the team's capability for dealing with emerging technology — whether that's in creativity (to help them find new approaches) or perhaps most importantly in how to deal with complexity. Even with today's technology, complexity is a key area where assurance often fails, for example gaps often occur in considering technologies' inter-relationship with other risks (e.g. master data, reports, application controls, and interfaces). This will accelerate in the future and as '*simplicity does not precede complexity* *but follows it*' before our teams deliver off the shelf work programs we need to encourage them to stand back and to consider things such as these inter-relationships (between technologies, suppliers, risks, data to name a few). Therefore training teams to deal with and manage complexity (for example by training them in techniques such as problem-structuring methods) in order to design appropriate assurance will perhaps be the other key skill that makes a difference in the future.

3. Adapt

As technology and organisations adapt we believe assurance functions must also move beyond the 'iteration' of the continuous improvement driven by measures such as effectiveness reviews and audit committee demands if they are to appropriately adapt. An approach we have applied to help assurance functions do this in practice considers adaptation across an additional two dimensions:

- Iteration: This is an area most assurance departments already focus on to drive ongoing continuous improvement in existing processes by making them more efficient and effective.

- Innovation: Choosing a limited number of 'big bets 'where assurance teams can evolve or add value by doing something totally different. For example emerging technologies such as robotics have the potential for some more repetitive controls in frameworks such as SOX to be automated to allow more focus on other areas which require more judgement or are more complex.

- Integration: It is difficult for assurance teams to have the resources to adapt alone and collaboration is another dimension which can allow them to do this more effectively. Working across the organisation and beyond (e.g. suppliers, peers) to keep up to date and where appropriate to collaborate with other initiatives and innovations can allow additional capabilities to be more quickly and cheaply developed and delivered.

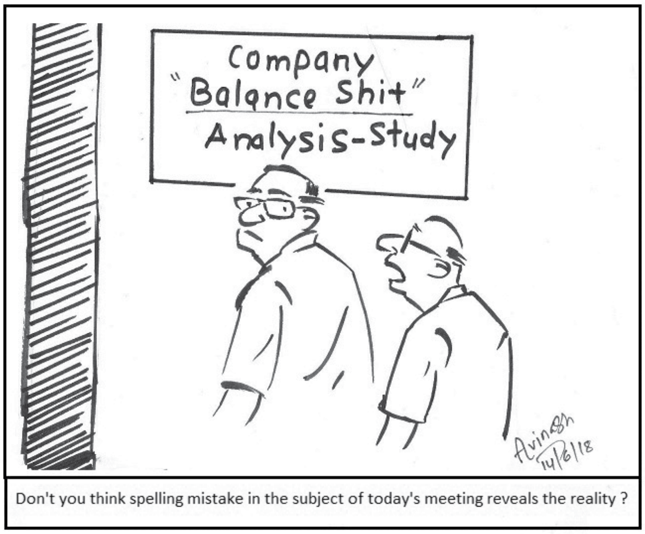
CONCLUSION

To conclude, following are the two key messages which should serve as food for thought for all CA's and audit professionals:

1. Technology: The great leveller: The pace of technological change is bringing with it unparalleled opportunities for companies to disrupt themselves and enter new markets. The promise of greater productivity, efficiencies and the elimination of human error is well documented. Less well documented are the new risks that emerging technologies are creating for organisations. The speed of adoption, complexity and ubiquity of these technologies means that these risks are rapidly increasing in both likelihood and impact and moreover often going unnoticed.

2. Get ready: Current assurance approaches alone are insufficient to address these risks. Assurance leaders urgently need to engage with their stakeholders and the rest of the organisation to understand how emerging technologies impact their organisation now, and in the future. Resulting changes to assurance scopes and approaches require new skills and capabilities that assurance teams need to start developing today to remain relevant for the future.

As part of this, ethical assurance will be key to help ensure that in embracing these new technologies organisations are confident that the way in which they are doing so is consistent with their brand and culture allowing them to demonstrate integrity and build essential digital trust. ■



Don't you think spelling mistake in the subject of today's meeting reveals the reality ?