A CAE's guide to emerging technology

Keeping pace with the IT risk landscape and the world of your Chief Information Officer (CIO) can be daunting. Disruption from the pandemic has permanently changed how we work, shop and access services. Most organisations have reacted to this by accelerating their digital business models.

Here is a summary of the latest thinking, top risks and considerations into how audit leaders might approach technological assurance in the digital age.

Current thinking 2025

Key risks

Regulatory landscape

Future thinking 2030

Assurance

Current thinking | 2025

As you read this section, think about your organisation's IT strategy: is it simply maintenance, is it transformational or is it inspiring? The CIO needs to balance strategic and operational needs while also taking account of the external environment as digitalisation accelerates (read the Chartered IIA's Risk in Focus 2022 report for more on this).

- Microsoft ends supports for Windows 10 in October 2025. Organisations who have not migrated will be exposed to increased cyber risk without patch updates.
- Cloud computing continues to increase across all three aspects due to scalability, cost and efficiency;

software/infrastructure/platform as a service. Security should be tested where rapid deployment took place over the last two years to enable remote working. It is important to match risk appetite with the use of public, private and hybrid clouds. What does cloud risk management look like in your organisation?

- Digital transformation is being accelerated through the use of low-code development platforms that enable the creation of software apps using graphical interfaces instead of hand coding them. This reduces dependency on overstretched IT functions but potentially introduces new vulnerabilities and makes managing innovation harder. Entry-level quantum computers launch late 2022 while higher specification versions will be available in 2023 for sectors such as finance, energy and technology. It is comparable to the invention of the wheel and the industrial revolution in terms of its impact. An immediate concern will be the redundancy of passwords. Is your organisation ready to switch to biometrics?
- Industry experts Gartner warn of cyberattacks designed to harm people or damage assets rather than typical data theft, disruption and ransomware. Along with weaponising operational technology such as robotics, wearable tech and environment systems like filtration and air conditioning. A duty of care concern for all but particularly organisations providing goods or services and the potential for litigation. Is your second line thinking about this?
- The Internet of Things (IoT) continues to grow and has spawned a new acronym - Internet of Behaviour (IoB). IoB is the natural evolution of wearable tech, combining data with personal information to drive behaviour from health monitoring, to personalised advertising to targeted charity campaigns. Today a beep reminding you to get up and walk around…tomorrow the Syfy world of the film Minority Report. How might this create workplace opportunities?
- Volatility across supply chains has become the new normal. Futurists suggest that alongside investigating shorter chains, there is rising use of digital supply chain technology to address visibility and resilience issues; artificial intelligence, blockchain and automation.

Key risk considerations

- Cyber: Processes, controls, infrastructure or skills that fail to protect data consistently the top risk, for the last 4 years, in the Chartered IIAs annual Risk in Focus report
- Cloud transition: Imbalance of maintaining control and reducing IT cost base
- Skills: Inability to attract, develop and retain talent necessary for future success
- Obsolescence: Cautious digital transformation with lost efficiency, agility and innovation
- Strategy: IT strategy does not enable sustainability of organisation/is not fit for purpose
- Digital disruption, new technology and AI was cited among the top five risks by 45% of CAE's contributing to the Chartered IIA's Risk in Focus 2022 report, 8% put it as their top risk.

Monitoring the regulatory landscape

As we look ahead, these are four areas of potential emerging risk to keep an eye on.

- Outcome of government consultation on data reform anticipated for 2022, which includes: overhaul of the Information Commissioners Office, tackling algorithmic bias and a more flexible framework to reduce perceived bureaucracy created by the EU's General Data Protection Regulations.
- Progressing digital governance and regulation as part of the National AI Strategy with the planned publication of a White Paper.

- Scrutiny of big tech; progression of the Online Safety Bill world-leading proposed legislation to make internet service providers responsible for content. Although principally aimed at the tech giants, experts warn of the impact to global organisations and also many UK based businesses. To avoid costly compliance regimes organisations may decide to remove functionality that falls within scope or restrict access to content for UK IP addresses.
- Governance concerns over blockchain transactions have slowed mainstream adoption in the financial sector although banks continue to pilot and explore opportunities. While unregulated and with no immediate signs of change, the Financial Conduct Authority does manage a sandbox for innovation within the sector that includes blockchain entrepreneurs.

Future thinking | 2030

Disruptive technology and the pace of innovation make it challenging to think about the future of the workplace. The technology highlighted here is real, in use today, and will be part of our daily lives by 2030 in addition to driverless cars, drone deliveries and nanotechnologies to name but a few.

Keep these questions in mind when reading about the technology detailed in this section are:

1. Am I sufficiently aware of how this impacts my organisation today? Is this an opportunity or a threat?
2. How might this change my organisations business model over the next five years?
3. Are my digital skills and those of my team ready for the future that is here and now?

    - Virtual and augmented reality (V/AR) will continue to grow annually by c20% according to estimates and reach $80bn before the end of the decade. The pandemic shifted expectations on physical presence and locations. In addition to gaming and leisure there is already uptake in use for training, education, retail and the hybrid workplace. Increasing environmental concerns may also lead to more remote experiences to avoid the need for travel.
    - Two internet developments are in progress. The metaverse uses V/AR to create a virtual world where users share experiences and interact in real-time with simulated scenarios via avatars. It may become a hybrid environment where cryptocurrency, blockchain and the real world coexist. The other development is more of a revolution. Backlash to the tech giants has led to noise that the next generation of internet Web3.0 could utilise blockchain technology to decentralise power and control. One to watch as a battle between regulation and social disenfranchisement may surface.
    - Continual evolution of artificial intelligence will change the workplace. In 2015, as part of a broader survey the World Economic Forum asked business leaders when AI might replace corporate auditors. Although their response of 2025 may have been premature, remote auditing experiences during the pandemic may have increased the likelihood of this and other ‘service’ roles being transitioned to cheaper and unemotive alternatives. As organisations start to buy AI services, (hopefully not for IA!) new procurement risks emerge – here is a useful guide for all sectors developed by the UK government.
    - One of Dubai’s strategic goals is that 25% of all buildings will be built using 3D printing by 2030. It has already opened the world’s largest printed building, 640sq.m. of municipality office space. 3D printing has the potential to reduce costs across supply chains, manufacturing and construction by eliminating waste and labour issues. Scaling the technology is a challenge but with the pressures of the climate crisis might this be a solution?

- Automation and robotics are commonplace in manufacturing and will extend further with advances in AI and technology. Interactions with ‘smart’ machines will increase. Digital skills are fast becoming prerequisite in the workplace and organisations will need advanced IT, programming and maintenance skills to keep pace with their environment.
- In 2022 a UK research company showcased Ameca the humanoid robot. Elon Musk has also estimated that his humanoid, Optimus, will be in low volume production by the end of 2023. The extent to which humanoids will be about human and computer integration or replacement is one of debate and ethics rather than capability. It could bring life changing support to those with assisted living needs and is a physical extension of chatbots already used in service, retail and leisure sectors.

Technological assurance

It is almost impossible to think about what might be included in a relevant, risk-based intern audit plan in five years. It is difficult enough to think ahead six months!

There are, however, some fundamentals that audit leaders may want to include in technology related audits regardless of subject matter: trust, collaboration and relationships.

If we think about the technology of tomorrow it is quite a leap of faith – driverless cars, digital currencies, virtual reality and humanoids. Trust is essential. And it begins today with the chatbots, website interactions and apps that we all engage with. Reputations take time to build (and seconds to lose).

All organisations are developing their digital capabilities. Digitalisation is built on a resilient and efficient IT foundation. A building without foundations cannot safely expand and is unlikely to last long. In our digital future, IT could be most important factor in establishing trust and reputation.

Trust is about data protection, cyber risk management and ensuring privacy is respected.

All of these are on the audit plan today but what is the objective of the assurance being provided? Does it go far enough? Do your internal auditors look ahead to what is needed, to provide foresight as to future

needs? Does the assurance you provide help maintain the status quo or create an IT function that is fit for the future?

It is not all about the IT function. The digital age requires collaboration; business and IT working together to drive and deliver innovation. The culture of the IT function will be influential in how collaboration tools are deployed and change is managed.

“The risk I see is the IT infrastructure itself. We do a lot of internal development today because we don't want to be too dependent on a vendor. We have an innovation team that is not part of IT, it's in a grey zone. You have risks that are created because of developments not being sufficiently tested, documented or formalised because the business wants to use agile methods.”

Risk in Focus 2022 - Chief Audit Executive, French Private Bank

Think about your organisation - does the strategy exploit technological opportunities or does IT support the strategy? Of the active IT projects today, what percentage are maintenance/catch up versus advancing capabilities? Does the board’s risk appetite curtail the head of IT or is there a general lack of innovation? How does internal audit address such issues in its assurance?

Effective third-party relationships require trust and collaboration. They will be increasingly critical as digitalisation continues the trend continues to cloud based services, blockchain and the metaverse. All but the largest of organisations will purchase tech services from or partner with third-party providers in the coming years.

How do you provide assurance over third party services today? Is there over reliance on contractual arrangements and SLAs? Do you have an assurance map to highlight gaps and duplication across the three lines? Consider the organisations risk exposure today and how this might grow in the next three years? What appetite does the board have for this risk?

And finally, here is a reminder of the questions posed by the Chartered IIA in Risk in Focus 2022 relevant to thinking about the future of technology.

- Is the IT function fully aware of all digitalisation projects and sub-projects underway across the organisation?
- Is the organisation allowing end-user development using low-code? If so, are access rights and version rollouts managed to avoid unintentional errors?
- Does current digitalisation activity match the organisation’s risk appetite? From a back-to-basics perspective, does this digitalisation meet the established standards adopted by the organisation? Are the standards themselves fit for purpose?
- How much oversight do digitalisation projects have from the IT and IT security functions?
- Are agile methods delivering practical results at the expense of risk management? For example, are new applications being sufficiently security tested?
- Is there a programme in place for automatically patching any low-code apps that are in use?

Closing thoughts

Our digital futures will be defined by the integration, to varying depths, of technology, people and processes. Audit leaders will need to keep pace with this to ensure that assurance remains relevant, risk-based and doesn’t fall into silos. Future technology can seem a little too Syfy to be our reality if you were born before

1990 and grew up without the internet and mobile phones! But it is also an exciting time – are you ready to embrace it?

"The science of today is the technology of tomorrow"

Edward Teller, Physicist