International Journal of Innovation and Economic Development
ISSN 1849-7020 (Print)
ISSN 1849-7551 (Online)

URL: https://doi.org/10.18775/ijied.1849-7551-7020.2015.92.2001
DOI: 10.18775/ijied.1849-7551-7020.2015.92.2001

Volume 9
Issue 2
June, 2023
Pages 7-23

The Golden Age of the Big Data Audit: Agile Practices and Innovations for E-Commerce, Post-Quantum Cryptography, Psychosocial Hazards, Artificial Intelligence Algorithm Audits, and Deepfakes

[1]Suresh Sood, [2]Angela Kim

[1] University of Technology Sydney, Australia
[2]Women in A.I. (WAI), Australia

Abstract: Since the audit of the Parthenon in the 5th century, the audit has remained unchanged, focusing backward on financial statements. Global regulatory pressures are mounting for audit professionals and public accounting firms to make structural changes. In the 21st century, a new type of audit, the EPSAC value audit, is emerging, focusing on non-financial information, including operational data from company business functions and processes, and big external data, including social media. In addition, EPSAC focuses on the critical engagement areas of e-commerce, post-quantum cryptography, psychosocial hazards, artificial intelligence and machine learning, and tackling deepfakes. While a talent shortage of subject matter experts exists, auditors can use artificial intelligence knowledge bases to deliver the value audit. Such knowledge bases extend to the key EPSAC domains of cybersecurity and ESG, creating proxies for virtual team members. For example, industry 5.0, combining A.I. and IoT innovations, requires auditors to augment their skill sets with knowledge bases beyond traditional financial expertise to effectively navigate the complexities of the changing business environment, enhance the quality of audits, and provide valuable insights and assurance to stakeholders.

Keywords: Audit, Big data, Cybersecurity, Deepfakes, E-Commerce, ESG, Algorithm, Machine Learning, Post-Quantum cryptography, Psychosocial hazards

1. INTRODUCTION

During the fifth century, the Athenian golden age of sculpture and architecture, much expenditure on public works signals this time of beauty, happiness, peace, and prosperity. During this period, audit verifies revenues and expenses, including the construction of the Parthenon over 2500 years ago, helps uncover frauds, audits even the highest office bearers responsible for funds, and helps inform the public on managing their funds (Costouros, 1978). That was then. This is now. While the critical idea behind auditing has remained the same since ancient Greece, prevailing headwinds of regulation conspiring against auditors are hobbling the growth of new talent and innovative practices within audit work. Furthermore, the core concept of auditing has been decades since it has seen updates. Nevertheless, the traditional financial audit remains largely backward-looking, standards-driven, and focuses almost exclusively on financial statements.

Global regulatory pressures are mounting for audit professionals and public accounting firms, as seen from a variety of government hearings and reports (U.K. et al., 1992; Business, Energy and Industrial Strategy Committee, 2019; Australian Parliament, 2020) dating back to the last century on the regulation and future of audit. On an ongoing basis, the United States accounting watchdog, the Public Company Accounting Oversight Board (PCAOB 2022), conducts inspection reports identifying areas of non-compliance of audit work with standards, rules, and professional standards across the globe. Continuing the woes of the big four accounting firms, the PCAOB found significant shortcomings in auditing Chinese companies listed on U.S. stock exchanges by PWC and KPMG (Horowitz, 2023).

Annual audits are a statutory requirement for public listings and enable listing or listed companies around the world to add a stamp of credibility to the financials. Hence, regulators scrutinize auditing firms concerning conflicting interests, especially when creating a lack of independence, such as consulting engagements with existing audit customers. This desire for a structural separation of the compliance activities of audit and tax from consulting is far from new, with the consulting side of businesses previously divorcing from audit, as in the cases of KPMG to the tech-centric Capgemini in 2000, Accenture acquiring Andersen Consulting in the same year while IBM purchasing PwC in 2002. Twenty years later, in 2022, EY is positioning to create a “free-standing audit firm” (Lacone, 2022), splitting with advisory (Ball, 2022).

Beyond issues of independence, regulators and shareholders witness the failure of audits in uncovering frauds or mismanagement as in high-profile cases. These cases include Brazilian Banco do Nordeste (Menezes, 2023), Lojas Americanas (Ruffo, 2023), German Wirecard declaring insolvency in 2020 as the "Enron of Germany" (Browne, 2020), U.K. Carillion (Neate and Davis, 2020), Australia's Big Un collapse (Powell, 2018) and British Telecom Italy (Sweney, 2022). Such cases spur the need for change, innovation, and new product development for auditing. Creating stand-alone audit practices on a global scale be seen by the forthcoming EY split between consulting and audit businesses; innovations and extending the reach of audit beyond existing clients promises a change far overdue. However, these changes have yet to demonstrate the efficiency and independence of audits. Nevertheless, despite the proposed changes, the vert needs to determine whether a stand-alone audit firm can deliver more effective audits and if the resulting businesses from a separation of practices are separate and independent.

Despite the disaggregation plans or other structural changes of audit and consulting businesses in a reversal of fortune, audit businesses are moving to become the jewel in the crown of consulting in the 21st century. A golden age of new audits is awakening (Ghandar, 2019). Owing to an explosion of data representing a diversity of non-financial information (NFI) or big data, a new type of audit, the value audit moves towards reality. Unlike the traditional audit focusing on financial information, the value audit builds on the non-financial information available to all businesses, including operational data from company business functions and processes (table 1) and big external data, including social media.

Table 1: Operational areas of business and sources of big data

Operational data (internal)	Source of big data
Accounting	Invoice description, GPS, and time of delivery
Customer service	Call center voice records, email, and social media
Marketing and sales	Web site, e-commerce analytics, GPS sales reps
Supply chain and inventory	RFID, temperature, logistics center CCTV
Human Resources	Job descriptions, diversity, and inclusion
Leadership management	ESG (Environmental et al.) with Social (S) from the workforce's wearables

1.1 Value Audits of EPSAC

This article focuses on moving beyond the traditional financial audits to the new sophisticated value audits of EPSAC (Figure 1), adding a new strategic dimension to audits utilizing big data (table 1).

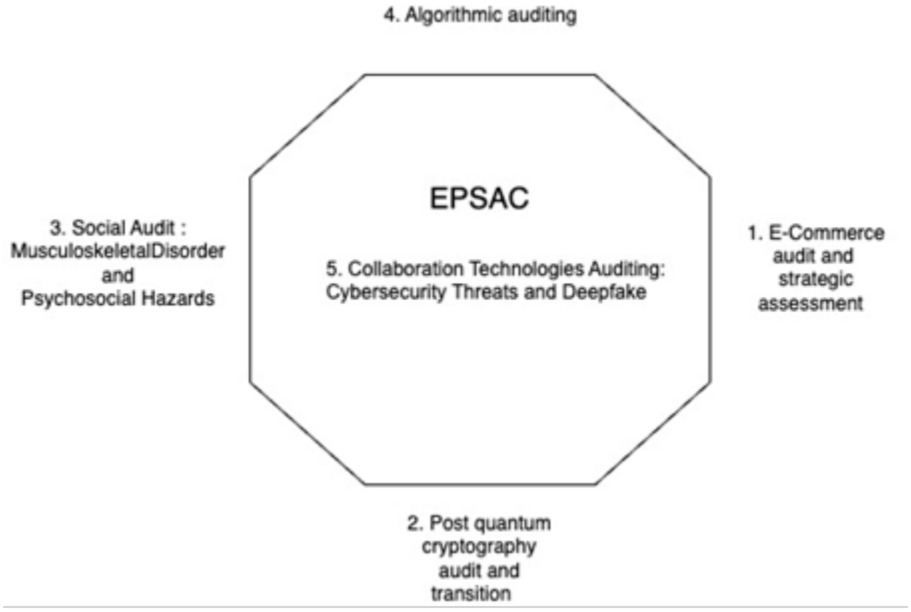

4. Algorithmic auditing
EPSAC
5. Collaboration Technologies Auditing: Cybersecurity Threats and Deepfake
3. Social Audit : MusculoskeletalDisorder and Psychosocial Hazards
1. E-Commerce audit and strategic assessment
2. Post quantum cryptography audit and transition

Figure 1: EPSAC audit components

2. NFI and International Standard on Assurance Engagements (ISAE) 3000

NFI is increasingly important for business and investment decision-making, helping inform stakeholders in financial markets. Investments increasingly focusing on a sustainable economy require transparency on companies' environmental, social, and governance (ESG) non-financial performance impacts. To this end, the International Standard on Assurance Engagements (ISAE) 3000, Revised, acts as a key mechanism supporting the ambition to transition to a sustainable economy by assuring opinions on non-financial information such as ESG metrics for sustainability reporting. Hence, the ISAE 3000 standard deals with assurance engagements other than audits or reviews of historical financial information. ISAE 3000 (Revised) maintains a strong profile aligning with the assurance of sustainability reporting when providing independent expert advice for such NFI reporting in return for a professional services fee to review the process of compiling the sustainability reporting targets and metrics. The assurance engagements are performed similarly to an audit opinion (reasonable assurance) or as a limited assurance engagement generated from less evidence.

The E.U. Corporate Sustainability Reporting Directive (CSRD) mandates the adoption of limited adoption standards before October 2026 with reasonable assurance standards by October 2028. ISAE 3000 (Revised) provides an ideal tool to provide opinions on ESG and meet the CSRD requirements for assurance of sustainability information to support the EU Green Deal and move to a climate-neutral economy.

The opportunity for assurance undertaken under the basic principles and procedures of ISAE 3000 (revised) applies to a range of subject matters, including e-commerce, post-quantum cryptography, psychosocial hazards, artificial intelligence and machine learning, and tackling deepfakes. Taking on such diverse subject matter allows audit professionals to move strategically and beyond the assurance of financial statements and non-financial ESG information. The remainder of this article focuses on the highlighted subject matters and potential opportunities for assurance engagements bringing about a golden age of audit.

3. E-Commerce Audit and Strategic Assessment

The proliferation and analysis of richer and deeper datasets of non-financial information or big data provide predictive power, helping determine the future financial health of economies, industries, and organizations. Examples include the monthly ANZ Truckometer (ANZ 2017), wherein surprisingly light traffic data helps predict New Zealand GDP six months ahead of time (N.Z. Government 2015), TripAdvisor rankings (Brinzan, 2016) impact hotel revenues in future periods (Anderson and Han, 2016), online reviews help predict future sales (Choong, 2016) and highly engaging web site visitors as seen from Google Analytics tracking and reporting website traffic (G.A.s; Google, 2017a) lead to greater precision with demand forecasting (Google, 2017b). Amongst the variety of NFI, a natural starting point is the website data of any business, no matter the organization's size. The website traffic directly represents future intentionality to purchase a product or service.

Considering the importance of non-financial information to help predict future revenue possibilities and G.A.s in particular, the external assurance of such data is a crucial area of interest for business owners and investors. However, the pitch decks of start-ups, including Uber (Mannes, 2017) seeking investment, rarely contain any assurances. Instead, focus on a dynamic or information-centric sales presentation building on a total addressable market (TAM) concept. This measure represents the total size of an opportunity available to a product or service and seduces investors as the estimation is often a considerable market size. Hence, the availability of any website traffic is a more helpful estimator than contemplating a marketplace monopoly or TAM. In the case of Germany's Wirecard, the availability of website traffic for existing and future B2B customers of the payment service has yet to be noticed, even with two decades of website traffic.

Furthermore, looking beyond financial accounting data, the role of professional accountancy moves from a narrow focus to greater participation in the business on an ongoing and significant basis following a trajectory whereby "big data can offer accountants and finance professionals the possibility of reinvention, the chance to take a more strategic, "future-facing" role in organizations" according to Faye Chua, the ACCA [Association of Chartered Certified Accountants] head of future research (Tokc-Wilde, 2016).

Potential revenue opportunities exist for consultancies from new audit services encompassing big or non-financial data not traditionally forming part of accounting practice services. Assurance helps validate the quality and reliability of information for decision-making. External assurance plays a valuable role in helping ensure that the provision of non-financial information is reliable. In light of this, the accounting or audit practice opportunity exists to create demand for private external assurance report generation using the principles in International Standards Assurance Engagement (ISAE 3000; IFAC 2017) and expanding assurance services beyond generating financial statements for existing and new clients.

The steps for Creating an Advisory service report for a practice or business unit financial group as an "Initial Strategic Assessment," Industry Online Audit, or Industry Report for Existing Customers and Potential Clients verified by a Chartered Accountant and in line with ISAE 3000 are as follows:

1. The final document supports a title indicating the report is an independent assurance report aligning with ISAE 3000 and indicates the addressee and the practitioner (include firm name and location of performance of the work)
2. Identification that the information under investigation is Google Analytics data about the specific website URL

3. Specify client objectives using the report, e.g., acquisition of new clients, business expansion beyond existing borders, or e-commerce growth.
4. Specify and break down the work performed in these steps together with outputs generated at each stage.
5. Audit comprising market intelligence and a report narrative using the Websites and services of SimilarWeb.com and or Alexa.com (an Amazon company). This part of the audit includes competitive websites and audience demographics generated automatically using these external information sources.
6. Use Google Trends (Google, 2017c) to understand interest over time by location, topics, and related keyword queries.
7. Obtain login details for G.A.'s account from the company business contact or website manager. Review website data directly by logging into G.A.s using the username and password allocated. Log into Microsoft Power B.I. (PBI) using the content pack for G.A.s, verify if the data is the same as at source by logging into the content pack using the same login credentials. Alternatively, use Google Looker Studio (Looker). Use predictive, data visualization, and artificial intelligence capabilities of G.A.s or PBI.
8. Integrate further insights from G.A.s using performance indicators, including sessions, page views, and bounce rate.
9. Enrich reporting with existing financials and quick insights using Power B.I. and an "out of the box accounting content pack" for Xero, Sage, Quickbooks, SAP Hana, and associated systems (Microsoft, 2017). The content packs use the same login as provided by the client for directly logging into the relevant accounting system.
10. Prior to the completion of the report, any additional industry information from a verifiable source such as IBISWorld helps set the context for the report and analysis.
11. Overall a written assurance report is generated by assembling data from the Google Analytics report (assuming the provision f access), the public data from SimilarWeb/Alexa, IBISWorld sourced narrative, and the latest financial verification by a Chartered Accountant (CA). An example report is available for Review (see Appendix I).

The output of the report is additional to existing audit work and suitable for input into a pitch deck where the website of the business already exists or as part of an alternative approach to fundraising, including crowdfunding (Australian Tax Office 2017), but unlike the TAM builds on actual data available on the company's web site.

Beyond G.A.s, the use of Martech (marketing technology) tools provides wisdom from past analysis of data from similar websites to the company under investigation and suggests online tenure leads to more spending per customer; high engagement leads to more orders and more categories purchased (Fanplyr, 2017).

As seen from these six steps and the use of data analytics tools, significant data analysis proficiency is not a prerequisite for success in the audit of NFI and external data sources (SimilarWeb et al.) together with GAs, Looker or PBI and company financials readily help capture value when taken together with financials and G.A.s web site data. As big data grows dramatically, practice and assurance services opportunities increase. In addition, NFI is a valuable asset enhancing any client product or service, including the opportunity to grow practice revenues and participate strategically in the accelerating growth of big data and e-commerce.

Moving from a fragmented world of high-profile audit failures and the split of audit away from consulting to some golden age seems impossible. However, the previous steps in analyzing behavioral data from e-commerce websites help reinforce the way audit changes moving into the golden age. Focusing on one financial scandal Wirecard an oversight of € 2 billion is avoidable by analyzing the big data on website traffic especially given the company's focus is online payment transactions. Extending audits beyond financial statements offers a lens to reflect on the business's ongoing viability.

4. Post-Quantum Cryptography Audit and Transition

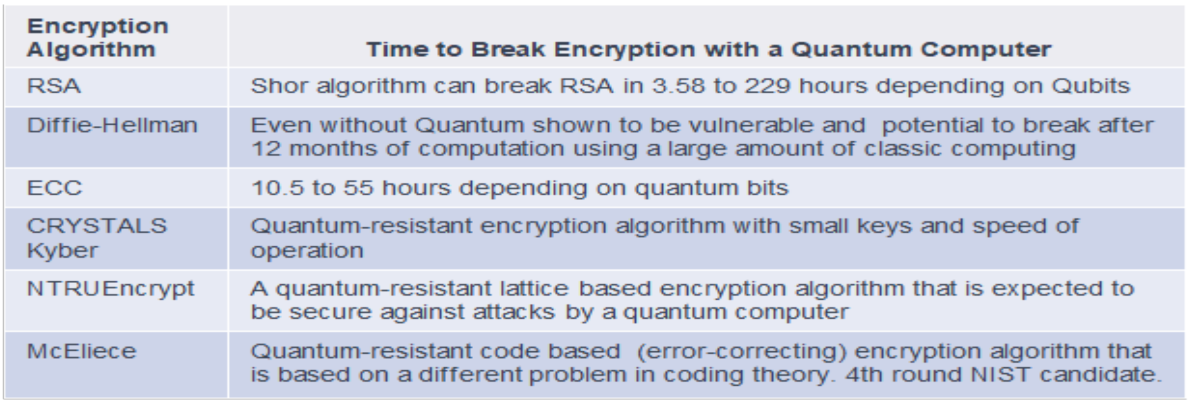
Between 2025 and 2030, quantum computers can break the encryption of sensitive data, including bank accounts, medical records, national security secrets, messaging systems such as WhatsApp, and even Bitcoin cryptocurrency. The applications and data are vulnerable to attack from quantum using the famous RSA and Diffie-Hellman methods, and Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) for cryptographic protection. However, Symmetric-key crypto (AES, SHA) impacts are less. These traditional encryption algorithms rely on mathematical problems challenging to solve for classical computers taking, for instance, billions of years to crack RSA. However, a fast algorithm capable of running on a quantum computer takes just a few hours for a solution (Campbell, 2023). This impact of quantum computing on data security represents a significant threat to global trade and security. However, no matter how well into the future quantum computing becomes available to adversaries, the issue of stealing encrypted sensitive data today provides the opportunity for decryption later when quantum becomes a reality. Under this scenario, McKinsey believes the "finance, banking, insurance, and government sector are at risk before 2025"(McKinsey, 2022). Such entities maintain sensitive data under government data retention obligations for 2-6 years for telcos and banks in Australia and U.K., so data capture under a cyber attack by an adversary in 2025 will likely still be relevant when decrypting the data using quantum in 2030 and beyond.

In 2016, the United States National Institute of Standards and Technology (NIST) commenced a post-quantum cryptography (PQC) standards multi-year competition calling for quantum-resistant or safe cryptographic algorithms for new public-key cryptographic standards for signatures and encryption keys (NIST, 2023). Several algorithms are emerging as "good choices" (Moody, 2022). A further PQC requirement is to be software swap implementable with existing systems, networks, and protocols. Other properties are resistance or countermeasures to side-channel attacks extracting secret information using traces of physical signals from acoustic, electromagnetic, power, or timing analyses (Johnson, 2023). Through 3 rounds (2017-22), the NIST selection for standardization is CRYSTALS-KYBER owing to security and performance for key management (table 1). A fourth-round considers vital mechanisms such as McEliece (see Table 1) with PQC standards available in 2024. As with traditional encryption, the standards will appear as Federal Information Processing Standards (FIPS) publicly announced standards. Each algorithm will have its document with special publications (S.P.) containing more technical details.

While, in theory, the desire is to swap out a hackable encryption algorithm with a quantum-resistant one, this process is far from being simple, and Gartner technology research and consulting notes, "Not one of the new post-quantum algorithms is a drop-in replacement for existing cryptography" (Horvath et al., 2022). Inevitably, the transition to PQC involves significant changes to the encryption system, including updating the encryption software and hardware. Moreover, given the extent of existing infrastructure invoking traditional encryption in many organizations, a significant investment in coordination, resources, and time must be allocated for planning and building the PQC systems.

Using the principles and process to support assurance engagements, auditors can take ownership of the PQC transition. For example, initial risk assessments on potential quantum attacks with an awareness of hackers targeting long shelf life data with the mindset of “harvest now, decrypt later” (Horvath et al., 2022) suggests a timeline of urgency and a narrow window to commence audits for transition planning.

Table 2: Traditional and Quantum Resistant Encryption Algorithms



Encryption Algorithm	Time to Break Encryption with a Quantum Computer
RSA	Shor algorithm can break RSA in 3.58 to 229 hours depending on Qubits
Diffie-Hellman	Even without Quantum shown to be vulnerable and potential to break after 12 months of computation using a large amount of classic computing
ECC	10.5 to 55 hours depending on quantum bits
CRYSTALS Kyber	Quantum-resistant encryption algorithm with small keys and speed of operation
NTRUEncrypt	A quantum-resistant lattice based encryption algorithm that is expected to be secure against attacks by a quantum computer
McEliece	Quantum-resistant code based (error-correcting) encryption algorithm that is based on a different problem in coding theory. 4th round NIST candidate.

At the first stage (2023-25), an education program relating to a walk-through highlighting why the breaking of traditional algorithms occurs and the need for transitioning to quantum-resistant or safe cryptographic systems catalyze to commence the PQC transition. For auditors, this work can start by jointly working with professionals responsible for securing data in the workplace, including cybersecurity.

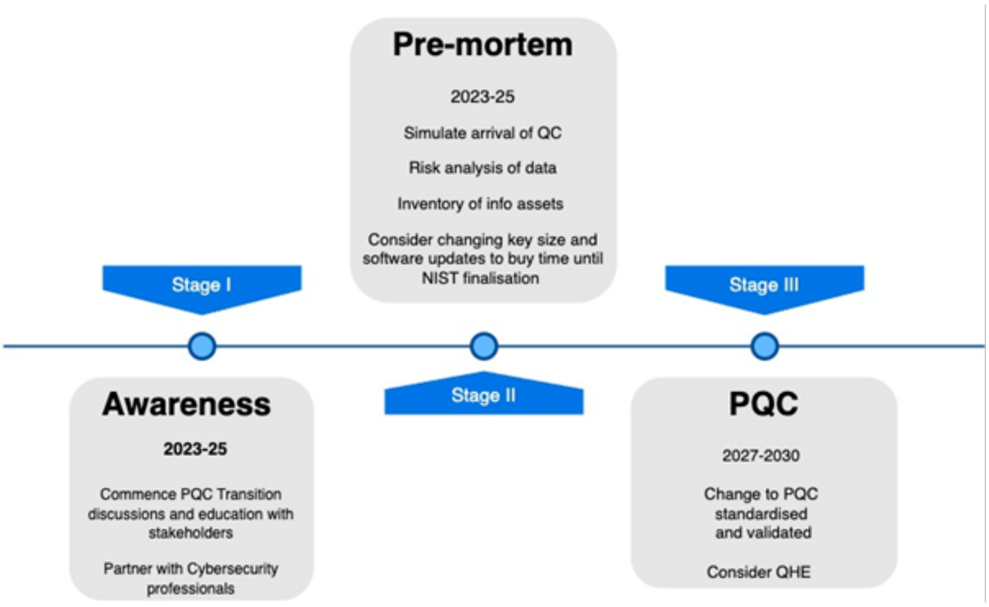

Pre-mortem
2023-25
Simulate arrival of QC
Risk analysis of data
Inventory of info assets
Consider changing key size and software updates to buy time until NIST finalisation
Stage I
Stage II
Stage III
Awareness
2023-25
Commence PQC Transition discussions and education with stakeholders
Partner with Cybersecurity professionals
PQC
2027-2030
Change to PQC standardised and validated
Consider QHE

Figure 2: Roadmap PQC Stages I - III

The second stage (2023-27) is a pre-mortem (Klein, 2007) beyond the first stage of education awareness simulating the arrival of quantum computing prior to 2030 and an understanding of risks to data using scenario analysis. Also, while realistic, the scenarios under consideration should not expect "crypto agility" (Jasmine, 2018) as a readily available featurseamlessly e to change and interoperate different encryption mechanisms within the existing cryptographic infrastructure. Previous migrations exist, reminding the difficulties in migrating encryption such as DES to triple DES to AES (Larson, 2014). The move from triple DES appears to have taken place owing to the inherent shortness of the encryption key with 56 bits, while AES offers 128-bit, 192-bit, and 256-bit options. This previous move in encryption builds on the understanding that the time required to crack an encryption algorithm directly relates to the length of the key.

This second stage II requires an inventory of information assets and the type of public-key cryptography used with metadata. The metadata specifies the critical type, owner, how generated, generation date, algorithm, and crypto-period of validity. As part of the post-mortem, note the actions to move to newer encryption as if PQC is available and determine steps to re-encrypt with quantum-resistant algorithms. Since PQC is evolving and dependent upon the inventory findings, a move to larger keys and software patches may be necessary during this stage, with further Review closer to 2030.

The third stage (2027-30) commences with swapping to PQC as systems are standardized and validated by NIST, building on actions from the previous stage. While PQC is driven by a ticking time bomb for organizations and governments as we move into 2025-30, an opportunity exists for auditors to enable companies to affect game-changing capability and make the PQC transition simultaneously.

Cloud service privacy and security concerns dominate discussions amongst auditors in a world of rising cyberattacks and quantum computing capability. Homomorphic Encryption (HE) is a solution enabling the secure processing of sensitive data using public cloud services. Homomorphism relates to the property of specific encryption algorithms allowing the performance of computations and manipulations on encrypted data. An ability to work on encrypted data and circumvent a process of encryption-decryption represents a sea change in thinking about the relationship between processing data and privacy. Decryption is realizable later, outside the prying eyes of any service provider by the trusted party with access to the secret decrypting key. Using HE is a paradigm shift for society without compromising privacy. Furthermore, HE has significant implications for new cloud service providers, business models, and finance and accountancy professionals across the globe with audit and assurance responsibilities. Regarding quantum resistance, some HE scheme designs are QHE and resistant to attacks by quantum computers, and suitable for providing quantum-enhanced data security for various computations.

5. Social Audit: Musculoskeletal Disorder and Psychosocial Hazards

ESG (Environment et al.) measures help employees, investors, regulators, and customers determine if companies truly embrace sustainability practices. Often, the practices are high profile, such as environmental and managing greenhouse emissions with the support of a sustainability (or carbon) report. Social efforts align with public statements on diversity, equity, and inclusion (DEI), ethical supply chains free of slavery, and support of LGBTQ+ rights. Governance seeks diversity on the board and manages an organization's resilience to adapt to changing conditions or face disruptions. Hence, most corporate sustainability efforts at a basic level focus on managing a few material ESG risks and opportunities. These efforts include environmental directives like minimizing greenhouse gas (GHG) emissions and their environmental impact, promoting sustainable supply chains, and conserving biodiversity. Social efforts include improving diversity, equity, and inclusion (DEI) to support social sustainability and justice. In addition, governance encompasses more complex factors such as human rights, human capital management, and resilience.

These aspects are essential for businesses to incorporate into their models and goals, but implementing or measuring environmental or governance improvements may take some time. Especially the social aspect of ESG involves an organization's relationships with its employees. In a nutshell, "S" ensures that the company prioritizes optimal working conditions for their employees and avoids sacrificing worker wellbeing. What better way to show that an organization cares about the health and safety of their employees than with quantitative data proving good ergonomic conditions exists in the workplace? Are auditable, traceable reports showing efforts to improve the work environment continuously?

One rapid and practical approach to commence the social aspect of ESG is implementing an ergonomics program to reduce workplace-related musculoskeletal disorder (WRMSD) risk. Musculoskeletal conditions affect 1.71 billion people globally (Global Burden of Disease data; GBD), representing a leading global workplace injury. MSDs are among the most common and debilitating injuries in the workplace, affecting thousands of people each year. MSDs such as rotator cuff tears, back strain, and carpal tunnel syndrome are the largest category of workplace injury. Ergonomic injuries result from risk factors, including forceful exertions, awkward or static postures, and repetitive movements. Affecting one-quarter of the global population, MSDs impact business efficiency and workers' ability to live their entire lives. As green technology accelerates, the next generation of workers, such as renewable energy technicians working offshore on wind energy, are at risk from MSD resulting from overhead work, heavy tools, and wearing protective equipment. Interestingly, blue-collar software developers adopt bad postures and partake in long sedentary periods during work contributing to WRMSD (Jasmine et al., 2020). No doubt, the same applies to consulting or advisory firms.

A company cannot honestly claim to be working toward ESG as a goal when employees are struggling physically at work. Implementing ergonomics gives businesses a tangible way to prove that they are not just providing lip service to employees, the public, or investors. Mature companies with ESG initiatives already recognize reducing MSDs as a critical factor in business performance, as seen from the "MSD Pledge" by the U.S. National Safety Council (NSC, 2023).

Monitoring psychosocial factors are a natural evolution of work-related musculoskeletal disorders (WRMSDs) activities. A growing body of evidence (e.g., EU-OSHA; European Agency for Safety and Health at Work) links psychosocial hazards and workplace musculoskeletal disorders (WRMSDs)—the U.K. Health and Safety Executive (HSE) recognizes, much as EU-OSHA, the stress-related impact between psychosocial risk factors increasing muscle tension or high job demands leading to rushed movement and WRMSDs.

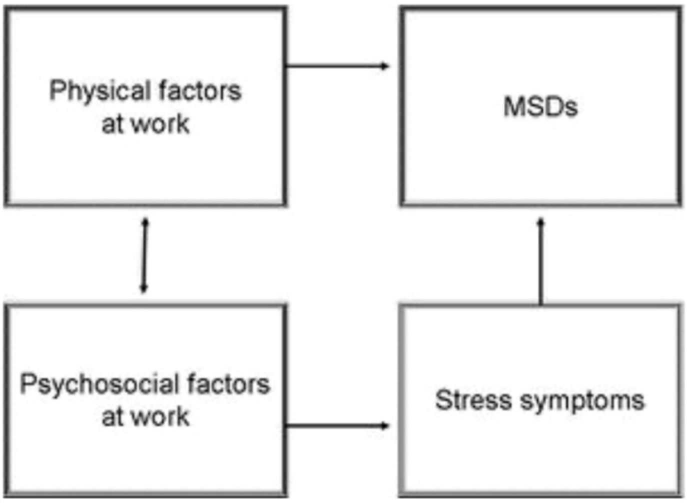


Figure 3: Possible Associations between psychosocial factors at Work and MSDs

Adapted from: OSHWiki

Both UK and Europe are pointing towards an approach for a model of wellbeing at work as articulated by the United States NIOSH Total Worker Health (TWH; CDC, 2022) and ISO 45003 guidelines for managing psychosocial risks provides a global standard and framework for managing psychological (includes mental, emotional and social) health and safety in the workplace.

In Australia, academics and governments increasingly understand the link between psychosocial risk factors and MSDs, ranging from Comcare to the NSW Centre for Work Health and Safety. Amendments to the model work health and safety (WHS) laws providing for an Australian national framework introduce psychosocial hazards, risk identification, and control. In addition, each Australian State and Territory modifies Occupational Health and Safety legislation adopting WHS laws to become legally binding, e.g., NSW Work Health and Safety Amendment Regulation 2022 and Vic Occupational Health and Safety Amendment (Psychological Health) Regulations.

Mental health issues emerging from psychosocial factors in the workplace are essential issues impacting safety in the workplace. Many organizations and researchers use the gold standard Copenhagen Psychosocial Work Environment (short) Questionnaire (COPSOQ) to help auditors target and capture psychosocial variables.

Once a baseline set of survey data is acquired, behavioral analytics determines the validity of data available without using a survey instrument, substituting with biometrics such as voice to gather stress influences as indicators or proxies of wellbeing. Solutions exist (e.g., www.voicesense.com) to assess patient wellness from the actual voice and the acoustics, not the textual information conveyed. Detection of stress from voice information commands considerable interest and solutions amongst a wide range of literature reporting on voice stress analyses obtained from voice acoustics or break down of the voice into Fourier components using Mel Frequency Cepstral Coefficients (MFCCs). However, the causal relationship between psychosocial factors and wellbeing could be clearer.

Just as COPSOQ provides a gold standard for risk assessment in the workplace, the gold standard of psychology-based natural language processing is Linguistic Inquiry Word Count. With over 19,000 research citations, Linguistic Inquiry Word Count (LIWC pronounced "Luke"). This framework allows an ability to establish links between linguistic patterns, personality, and psychological state of the individual when communicating vocally or using the written word. LIWC requires very little computational power and counts the percentage of total words in the text provided against several grammatical, psychological, and content categories representing psychological processes in individuals. Receptivity (www.receptiviti.com/api) provides an API providing signals of language psychology from written texts and voice, insights into emotions, Big Five personality, DISC, mental health, cognitive processes, toxicity, interpersonal, and much more. Mental health quantifies wellbeing with psychological indicators associated with mental health and distress. An API makes implementation time immediate for auditing. LIWC provides the potential for extracting signals of depression and suicidal tendency from writings shifting attention to health records and online content risk detection, and providing the potential for proactive intervention.

Taking a holistic approach of psychosocial (COPSOQ), psychological (LIWC) +physical (WRMSD risk assessment) in the workplace enables a "safety membrane ."Incorporating a set of guiding safety principles into the membrane defines how an organization treats a worker or employee and protects the individual from unintended consequences of poor safety practices by the organization using intelligent workplace technologies. Analytics and reporting from the safety membrane provide real-time feedback on employee emotional wellbeing, engagement, unknown risks, and other measures of an emotional workplace. The role of audit is critical not only on an ongoing basis but at the early stages of introducing new physical, emotional, and wellbeing metrics into the workplace. Some information sources are likely known to auditors and represent platforms the workforce interacts with daily, including company knowledge bases and sharing using collaboration tools such as Google Documents, Notion, Slack, Microsoft Teams, or Zoom. The Total Wellbeing Audit of an organization is within reach of the audit profession.

6. Algorithmic auditing

Algorithms help make A.I. smart and occupy a significant aspect of our personal and work life. The algorithms exist in many IoT appliances such as intelligent assistants OF Amazon Alexa, Google Home, or Apple HomeKit and many online services. Personalized recommendations built on past preferences allow viewing videos without allocating decision-making time. The same benefits translate directly with food or grocery shopping, building on previous ordering and shopping. However, the recommendation algorithms are capable of harm. For example, the study YouTube Regrets (Mozilla, 2021) contends that the "recommendation algorithm has helped spread health misinformation, political disinformation, hateful diatribes, and other regrettable content to people around the globe" (ibid). Avoiding harm to individuals or society is only realizable through algorithmic auditing of systems embedding algorithms. The harm is significantly more impactful in sectors such as aviation and health than social media.

The A.I. Incident Database (AIID 2023) is already operational and indexes the collective history of harms or near harms in the real world by deploying artificial intelligence systems. Like aviation and computer security databases, the A.I. Incident Database learns from experience to prevent or mitigate bad outcomes.

The audit involves, as a minimum, three critical areas of assessment:

1.) Inspection of the inner workings of the algorithm with a particular focus on fairness
2.) Review of all documentation, inclusive of any patents
3.) Testing outputs of algorithms, including all data sources

We refer to algorithmic auditing as distinct from traditional financial audits subject to regulation and the use of formal frameworks. While regulation in algorithmic auditing is emerging, many investigations by regulators and consultants are signposting the way forward.

Consider the work of Trivago, a metasearch engine helping consumers compare hotel prices online. The booking process completes by connecting booking sites or Online Travel Agency (OTA). The Australian Competition and Consumer Commission found that rankings of hotels paying higher commissions achieve a superior recommendation over the cheapest (ACCC 2020).

O'Neil Risk Consulting and Algorithmic Auditing (ORCAA) represents a nascent algorithmic audit market player. Conducting an audit of the Olay Skin Advisor is rather illuminating (ORCCA 2021). The Skin Advisor analyses pictures of faces to provide personalized product recommendations. The software does not perform facial verification or facial identification. Furthermore, the system does not identify individuals based on their faces or match faces to a database. The key driving force of the audit is the evaluation of concerns around fairness and bias. Also, an expectation is an audit to identify any unintended consequences of Skin Advisor. The main findings of the audit focus on making the Advisor more robust in treating skin tone, age, and gender. The audit findings suggest Skin Advisor could be more inclusive, driving more equity and inclusion. Achieving this requires updating the training dataset with more age and skin tone diversity. While the Advisor focuses on offering Women's skin product recommendations, expanding the Advisor training data to incorporate users of any gender, including those with facial hair, evolves the tool for users of any gender.

However, more pressing than the audit of existing algorithms is the regulation and auditing of the A.I. engines or Large Language Models (LLMs) similar to Open AI ChatGPT generating representations of human written text responding to questions, text summarisation, language translations, and even voice to text conversions of podcasts and text to image or video generation.

More importantly, generative A.I. learns from existing data to generate entirely new artifacts similar to original data or models. However, a vital risk of the engines is the unforeseen hallucinatory capabilities of fabricating information not verifiable from facts but blatantly incorrect(Azamfirei et al., 2023). One practical step in minimizing hallucinations is identifying and understanding the underlying causes. For example, language models like ChatGPT tend to hallucinate due to knowledge gaps (Zhang et al., 2023).

Auditing of LLMs represents a relatively new yet promising approach to addressing the risks of LLMs. The auditing process can help review and assess the model's outputs, flagging instances of hallucinations and providing feedback for improvement. Even though asking misleading questions and noting the outputs helps direct the developers to refine the models and minimize the occurrence of hallucinations. Curating high-quality training datasets represents a further opportunity for improvements through audits. Language models train on large datasets, and the quality and diversity of the training data significantly influence their performance. By curating datasets that cover a wide range of reliable and accurate information, developers can minimize the chances of hallucinations.

Ensuring the inclusion of high-quality sources and authoritative references can improve the model's knowledge base and reduce the likelihood of generating false claims.

7. Collaboration Technologies Auditing: Cybersecurity Threats and Deepfake

Increasingly, the C-suite expects that an audit of "cutting edge" technologies help provide insights into the threat landscape, putting cybersecurity at risk. In particular, cutting-edge technology relates to industry 5.0 technologies representing an interplay of the Internet of Things (IoTs) and artificial intelligence (A.I.) cooperating with human intelligence (Saeid, 2019). Large Language Models (LLMs), regarded as the foundation for A.I., have profound implications beyond text and speech, including computer vision and entering the domain of industry 5.0.

Building on GPT-3 (Generative et al.), DALL E uses text to create images (OpenAI, 2021). Combining text, Video, and images, knowing they generate probabilistically, opens Pandora's box on deepfakes with the emergence of a new industry and deep fake detection technology to protect world leaders (Boháček and Farid, 2022). This scenario, in particular about world leaders, is vividly illustrated by the BBC thriller The Capture, series 2 (BBC One, 2022), highlighting plausible cyber warfare employing deep fake technology (Mellor, 2022), bringing to life a politician using human image synthesis and artificial intelligence.

The increasing use of video-enabled meeting solutions (video conferencing) is a central focus for organizations of all sizes with remote, flexible working for employees. Participants, including students, use techniques to show they pay attention in meetings or lectures, including convincing loop videos (Cole, 2020). Virtual meetings using video platforms (e.g., Zoom, Microsoft Teams, or Google Meet) are not immune from social engineering or computer intrusion using deepfakes. According to the FBI: "Compromising an employer or financial director's email, such as a CEO or CFO, and requesting employees to participate in a virtual meeting platform where the criminal will insert a still picture of the CEO with no audio, or "deep fake" audio, and claim their video/audio is not properly working" (FBI, 2022). Once the lousy actor inserts themselves into the virtual meeting, victims receive instructions to send funds to fraudulent accounts, gain company secrets or even have the CEO admit to a fictitious crime. As described by the FBI public service announcement, this scenario is superseded by cloning oneself on the Video to fake a Zoom meeting (VideoZeus,2020) or using real-time deepfakes disguised as literally anyone in the world (McIntyre, 2020). Advances in deep fake technology create unprecedented cyber security threats, generating not only people that do not exist but events never to happen.

Machine learning, A.I. media manipulation, and voice synthesis techniques allow bad actors to place fake human faces in social media profiles, perform face swaps in videos, or voice impersonate executives or celebrities with just a few keystrokes. Deepfake creation is made possible with some effort using open-source software face swap (https://faceswap.dev/), DeepFaceLab (https://sourceforge.net/projects/deepfacelab.mirror/), and DeepFaceLive (https://github.com/iperov/DeepFaceLive). A day goes by without advances in deepfaking due to A.I., e.g., Microsoft VALL-E text-to-speech clones voice and tone from a three-second audio snippet (https://valle-demo.github.io/). Open-source videos found on YouTube or podcasts help generate training data for lip-syncing using the Wav2Lip model "is almost as good as real synced videos" (Prajwal et al., 2020).

The advent of deepfakes has significant implications for cybersecurity, including:

•Disinformation, e.g., Mark Zuckerberg video (Cole, 2019)

•Identity theft to create a synthetic identity blending identities (Morrow, 2019)

•Pornography with 96% of online deep fake videos (Duffy, 2019)

•Social engineering manipulating people using voice impersonation (Stupp, 2019)

Deepfake detection of content is a relatively new opportunity, with Intel introducing "FakeCatcher" (Intel, 2022; Ciftci et al., 2020). Other solutions that are emerging available include the Deepwater scanner (https://deepware.ai/) and density "Know your Customer and anti-spoofing solutions" (https://sensity.ai/deepfakes-detection/). For auditors to commence research in this area, a repo is available on papers relating to deep fake detection (https://github.com/Daisy-Zhang/Awesome-Deepfakes-Detection) along with deepfakes datasets, tools, papers, and code (https://github.com/Daisy-Zhang/ Awesome-Deepfakes) Note some cloud development environments do not allow the creation of deepfakes, e.g. Google Colab. See FAQs and deepfakes are disallowed from Colab runtimes (https://research.google.com/colaboratory/faq.html)

The problem audit helps us understand that it is only becoming worse with 100x more visual content online by 2027 (LDV Capital, 2021), with synthetic Video accounting for 90% of online Video (Schick, N., 2020). Any audits attempting to solve this issue of information manipulation will be very attractive in the global workplace. Further reinforcement of the importance of countering deepfakes can be seen from the United States Deepfake Task Force Act (S. 2559) to establish a Deepfake Provenance Task Force (Rao, 2021) as well as the Content Authenticity Initiative (CAI) community of companies spearheaded by Adobe promoting the adoption of an open industry standard for content authenticity and provenance (https://contentauthenticity.org/).

8. Where to start with EPSAC?

An approach to uncovering problems and conducting a ‘premortem’ (Klein, 2007) helps determine priority areas for focusing the initial value audit. Through reviewing worst-case scenarios, the collaborating audit team members have an approach to uncovering potential problems and conducting a premortem with clients. This exercise helps understand what the business may choose not to remedy. This activity requires simulating an initiative's failure, understanding the critical success factors, and identifying the known unknowns. Nonetheless, 'unknown unknowns,' such as the global pandemic or the tsunami that destroyed Japan's Fukushima Daiichi Nuclear Power Plant, may never have been planned for by any organization. Planning collaboratively as an audit team with any subject matter experts, such as cryptography or ESG expertise, rather than in silos, will help to reduce the risk of 'known unknowns.' However, the only way to address unknowns is through flexibility and team-wide collaboration with clients when the evidence materializes.

8.1 Considerations Based on Industry

Moving into the EPSAC, one fundamental assumption is that audit teams possess access to knowledge of any subject matter expertise, including data analytics and cybersecurity. Otherwise, the growing demand for new value audits becomes a bottleneck due to needing more specialist talent. Such knowledge or talent may exist in a large language model (LLM) or A.I. knowledge base(Petroni, 2019). Audit team members can interrogate the knowledge bases in plain English and even turn the query into software code for further investigation and analysis using any software tool. The exemplar for such knowledge bases and interaction is ChatGPT. Indeed, the eventual goal is for A.I. to automate an entire EPSAC audit. Such use of A.I. reduces the dependency on subject matter expertise in areas discussed. Over time, the same approach using A.I. knowledge bases extends to the key EPSAC domains of cybersecurity and ESG creating proxies for virtual team members. Everything from undertaking research into a specialist area, developing a project schedule for delivery of value audit from commencing with scoping, preparation of the audit work papers, and subsequent generation of the board presentations for discussion with the C suite on the risk reduction or value creation emerging from conducting the audit are available in response to team members making natural language queries. Acquiring and building expertise using A.I. knowledge bases at the same time helps existing team members move towards developing expertise supported by the A.I. databases and found outside of audit teams providing a career path for audit teams moving into areas of non-financial information such as post-quantum cryptography, e-commerce behaviors, psychosocial hazards, significant language AI-based systems and deepfakes. The evolving landscape of Industry 5.0, combining A.I. and IoT innovations, requires auditors to refrain from acquiring new subject-matter skills but to learn to harness and augment work activities using AI. The same applies to all aspects of conducting EPSAC units.

9. Conclusion

The golden age of audit for non-financial information requires auditors to augment their skill sets with A.I. knowledge bases beyond traditional financial expertise. Auditors must embrace data science, understand cryptography and e-commerce behaviors, and possess or access the knowledge of psychosocial hazards and significant language AI-based systems. By cultivating these new skills using A.I. knowledge bases, auditors can effectively navigate the complexities of the changing business environment, enhance the quality of audits, and provide valuable insights and assurance to stakeholders. Embracing this golden age of audit enables auditors to fulfill a leadership role as trusted advisors in a world of non-financial information with clients and auditors having to deal with deepfakes.

References

- ACCC (2020). Trivago misled consumers about hotel room rates.[Press Release]. January 21. https://www.accc.gov.au/media-release/trivago-misled-consumers-about-hotel-room-rates
- A.I. Incident Database (AIID) (2023). A.I. Incident Database. https://incidentdatabase.ai/
- ANZ Bank New Zealand Limited (2017). "ANZ Truckometer," accessed August 31, 2017, [available at https://www.anz.co.nz/about-us/economic-markets-research/truckometer/]
- APB (1992). "The Future Development of Auditing." In A Paper to Promote Public Debate, London: Auditing Practices Board.
- Australian Parliament (2020). "Regulation of Auditing in Australia: Final Report", November. https://www.aph.gov.au/-/media/Committees/corporations_ctte/RegulationofAuditing/Regulation_of_Auditing_in_Australia_-_Final_Report.pdf?la=en&hash=7A5F8CCFA82421E0B96940686272998C9A6FE178
- Australian Tax Office (2017). "Crowdfunding," June 21, accessed August 31, 2017, [available at https://www.ato.gov.au/individuals/income-and-deductions/income-you-must-declare/crowdfunding/].
- Azamfirei, R., Kudchadkar, S., and Fackler, J. (2023). Large language models and the perils of their hallucinations. Critical Care. 27:120. https://ccforum.biomedcentral.com/articles/10.1186/s13054-023-04393-x *CrossRef*
- Baumgärtner, L., Klein, B., Mohr, N., Pflanzer, A., and Soller, H. (2022). "When—and how—to prepare for post-quantum cryptography," 4 May. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/
- BBC One (2022). The Capture (Season 2). [T.V. series]. BBC Studios.
- Boháček, M. and Farid, H. (2022). "Protecting world leaders against deepfakes using facial, gestural, and vocal mannerisms." PNAS. https://www.pnas.org/doi/10.1073/pnas.2216035119 *CrossRef*
- Brinzan, D. (2016). "TripAdvisor's 2016 Ranking Algorithm Update: What You Need to Know," accessed August 31, 2017, [available at https://www.hermesthemes.com/tripadvisors-2016-ranking-algorithm-update/]
- Ball, S., (2022). PwC to quadruple partner poaching from EY amidst split. ERP Today. December 5. https://erp.today/pwc-to-quadruple-partner-poaching-from-ey-amidst-split/

- Browne, R. (2020). "The Enron of Germany: Wirecard scandal casts a shadow on corporate governance." CNBC, June 29. https://www.cnbc.com/2020/06/29/enron-of-germany-wirecard-scandal-casts-a-shadow-on-governance.html
- Business, Energy and Industrial Strategy Committee (2019). "The Future of Audit," House of Commons, April 2, HC 1718. https://publications.parliament.uk/pa/cm201719/cmselect/cmbeis/1718/1718.pdf
- C.A. Kairos (2017). "Systems of Insight Training," accessed August 31, 2017, [available at https://www.charteredaccountantsanz.com/member-services/resource-centre/data-and-analytics].
- Campbell, C. (2023). "The Quantum Leap ."Time. January 26. https://time.com/6249784/quantum-computing-revolution/
- Ciftci, U., Demir, I., and Yin, L. (2020). "FakeCatcher: Detection of Synthetic Portrait Videos using Biological Signals." IEEE Transactions on Pattern Analysis and Machine Intelligence P.P. (99):1-1. https://ieeexplore.ieee.org/document/9141516 *CrossRef*
- Cole, S. (2019). "This Deepfake of Mark Zuckerberg Tests Facebook's Fake Video Policies." Vice. https://www.vice.com/en/article/ywyxex/deepfake-of-mark-zuckerberg-facebook-fake-video-policy
- Cole, S. (2020). People Are Looping Videos to Fake Paying Attention in Zoom Meetings. Vice. https://www.vice.com/en/article/7kzq5x/looping-videos-to-fake-paying-attention-in-zoom-meetings
- Costouros, George J. (1978). "Auditing in the Athenian state of the golden age (500-300 B.C.)," Accounting Historians Journal: Vol. 5: Iss. 1, Article 4. https://egrove.olemiss.edu/aah_journal/vol5/iss1/4 *CrossRef*
- Fanplyr (2017). "Convert Browsers To Buyers Real-Time Targeting With Messages And Offers," accessed August 31, 2017, [available at https://fanplayr.com]
- FBI (2022). "Business Email Compromise: Virtual Meeting Platforms ."Public Service Announcement. Alert Number. February 16. Alert Number I-021622-PSA. https://www.ic3.gov/Media/Y2022/PSA220216#retfoot1
- Ghandar, A. (2019). "This is a golden age of audit: Chartered accountants ANZ," Australian Financial Review, February 12, https://www.afr.com/companies/professional-services/this-is-a-golden-age-of-audit-chartered-accountants-anz-20190208-h1b10c
- Google (2017a). "Turn insights into action," accessed August 31, 2017, [available at https://www.google.com.au/analytics]
- Google (2017b). "About E-commerce," accessed August 31, 2017, [available at https://support.google.com/analytics/answer/1037249?hl=en]
- Google (2017c). "Google Trends," accessed August 31, 2017, [available at https://trends.google.com]
- Horvath, M., Lowans, B., and Fritsch, J. (2022). "Preparing for the Quantum World With Crypto-Agility ."Gartner, September 27, ID G00743967.
- Horowitz, J. (2023). "Audits of Chinese companies by KPMG and PwC full of holes, U.S. watchdog finds." CNN Business. May 10. https://edition.cnn.com/2023/05/10/business/us-china-audit-companies-report/index.html
- IFAC (2017). "International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance Engagements Other than Audits or Reviews of Historical Financial Information", accessed August 31, 2017, [available at
- https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga]
- Intel (2022). "Intel Introduces Real-Time Deepfake Detector- Intel's deepfake detector analyzes 'blood flow' in video pixels to return results in milliseconds with 96% accuracy".Intel newsroom. November 14. https://www.intel.com/content/www/us/en/newsroom/news/intel-introduces-real-time-deepfake-detector.html#gs.q8v7by *CrossRef*

- Jasmine, H. (2018). "What is Crypto-Agility? Cryptomathic".10 August, https://www.cryptomathic.com/news-events/blog/what-is-crypto-agility
- Jasmine, M., Fasna, L., Chellaiyan VG., Raja VP., and Ravivarman G. (2020). "A study on knowledge and practice of Ergonomics among the Software Engineers in a private firm, Chennai, Tamil Nadu." J Family Med Prim Care. August 25;9(8):4287-4291.https://pubmed.ncbi.nlm.nih.gov/33110847/. *CrossRef*
- Johnson, D. (2023). "Post-quantum algorithm vulnerable to side-channel attacks S.C.." Media, February 22, https://www.scmagazine.com/analysis/policy/post-quantum-algorithm-attack
- Klein, G. (2007). "Performing a Project Premortem ."Harvard Business Review, September, https://hbr.org/2007/09/performing-a-project-premortem
- Lacone, A. (2022). "EY Poised to Grow Big Four Audit Market Share in Restructuring," Bloomberg Tax, September 12, https://news.bloombergtax.com/financial-accounting/ey-poised-to-grow-big-four-audit-market-share-in-restructuring
- LDV Capital (2021). "How Visual Tech is Fueling the Creator Economy." LDV Capital Insights 2021. September. http://eepurl.com/hIfXv5
- Loong Choong, A. Li, B., Ngai, E., Ch'ng, E. and Lee, F. (2016). "Predicting online product sales via online reviews, sentiments, and promotion strategies: A big data architecture and neural network approach." Journal of Operations & Production Management, Vol. 36 Issue: 4, pp.358-383, accessed August 31, 2017, [available at http://www.emeraldinsight.com/doi/abs/10.1108/IJOPM-03-2015-0151] *CrossRef*
- Mannes (2017). "Here is Uber's first pitch deck," August 23, accessed August 31, 2017, [available at https://techcrunch.com/gallery/here-is-ubers-first-pitch-deck/]
- McIntyre H. (2020). How to Join Zoom Meetings Using Real-Time Deepfakes! [Video]. June 16. https://www.youtube.com/watch?v=16GX8SBB2Rk
- Mellor, L. (2022). "The Capture May Feel Like Science-Fiction, But Real-Time Deepfake Tech is Here." Den of Geek. September 7. https://www.denofgeek.com/tv/the-capture-may-feel-like-science-fiction-but-real-time-deepfake-tech-is-here/
- Morrow, S. (2019). "Deepfakes and synthetic identity: More reasons to worry about identity theft." CSO Australia. October 2. https://www.csoonline.com/article/3442397/deepfakes-and-synthetic-identity-more-reasons-to-worry-about-identity-theft.html
- Mozilla (2021). YouTube Regrets A crowdsourced investigation into YouTube's recommendation algorithm. July. https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf
- OpenAI (2021). "DALL·E: Creating images from the text." January 5. https://openai.com/blog/dall-e/
- Larson, M. (2020). "What are the differences between DES and AES?" Townsend Data Security Blog, April, https://info.townsendsecurity.com/bid/72450/what-are-the-differences-between-des-and-aes-encryptiondata
- Menezes, F. (2023). PwC faces a lawsuit from investors of a former Brazilian client accused of fraud. The Brazilian Report. January 24. https://brazilian.report/liveblog/2023/01/24/pwc-lawsuit-fraud/
- Microsoft (2017). "Connect to services with content packs for Power B.I.," August 10, accessed August 31, 2017, [available at https://powerbi.microsoft.com/en-us/documentation/powerbi-content-packs-services/]
- Mitchell, S. (2017a). "Amazon entry to Australia will hit retailers, landlords, and economy: UBS report," August 1, accessed August 31, 2017, [available at http://www.afr.com/business/retail/amazon-entry-to-australia-will-hit-retailers-landlords-and-economy-ubs-report-20170731-gxm2ko]
- Mitchell, S. (2016b). "Online retail sales top $20 billion", August 3, accessed August 31, 2017, [available at http://www.afr.com/business/retail/online-retail-sales-top-20-billion-20160803-gqjv0r]

- Moody, D. (2022). NIST PQC: Looking into the Future, NIST, Presentation, November 29, https://csrc.nist.gov/csrc/media/Presentations/2022/nist-pqc-looking-into-the-future/images-media/session-1-moody-looking-into-future-pqc2022.pdf
- NSC (2023). Take the MSD Pledge. https://www.nsc.org/workplace/safety-topics/msd/business-pledge
- Narrative Science (2017). "Simplify Google Analytics Reporting with Quill Engage," accessed August 31, 2017, [available at https://www.quillengage.com/]
- Neate, R., & Davis, R. (2020). "Carillion collapse: two years on, the government has learned nothing, "Guardian, January 15, https://www.theguardian.com/business/2020/jan/15/carillion-collapse-two-years-on-government-has-learned-nothing
- New Zealand Government (2015). "Using the volume of traffic on state highways as an indicator of the momentum of our economy," June, accessed August 31, 2017, [available at https://www.data.govt.nz/case-studies/anz-truckometer/]
- NIST (2023). Post-Quantum Cryptography PQC, March 9, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
- ORCCA (2021). DESCRIPTION OF ALGORITHMIC AUDIT: Olay Skin Advisor. September 16. https://www.olay.com/decodethebias/orcaa
- PCAOB (2022). Firm Inspection Reports. https://pcaobus.org/oversight/inspections/firm-inspection-reports
- Petroni, F., Rocktäschel, T., Lewis, P., Bakhtin, A., Wu, Y., Miller, A., and Riedel, S. (2019). "Language Models as Knowledge Bases?" arXiv. 4 Sept. https://arxiv.org/abs/1909.01066 *CrossRef*
- Powell, D. (2018). "Hooked on a Big Un: How the listed tech company went from all-star to administration in less than a year." SmartCompany, September 24, https://www.smartcompany.com.au/finance/big-un-listed-tech-company-went-all-star-administration-timeline/
- Prajwal, K., Mukhopadhyay, r., Namboodiri, v., and Jawahar, C. (2020). "A Lip Sync Expert Is All You Need for Speech to Lip Generation in the Wild." MM '20: Proceedings of the 28th ACM International Conference on Multimedia. October 12. *CrossRef*
- Saeid, N. (2019). Industry 5.0—A Human-Centric Solution. Sustainability. 11. 4371. 10.3390/su11164371. *CrossRef*
- Schick, N. (2020). Deepfakes and the Infocalypse: What You Urgently Need To Know. Monoray
- Stupp, C. (2019). "Fraudsters Used A.I. to Mimic CEO's Voice in Unusual Cybercrime Case." Wall Street Journal. August 30. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
- Sweney, M. (2022). "PwC fined nearly £1.8m over B.T. fraud audit failures". Guardian. https://www.theguardian.com/business/2022/aug/08/pwc-fined-bt-audit-accounting-frc
- Tokc-Wilde, I. (2016). "The Big Data Effect," March, accessed August 31, 2017, [available at http://www.accaglobal.com/an/en/student/sa/features/big-data.html]
- Varon, L. (2016). "How Big Will eCommerce In Asia Pacific Be In Five Years?", February 23, accessed August 31, 2017, [available at https://go.forrester.com /blogs/ 16-02-23 how_big_will_ecommerce_in_asia_pacific_be_in_five_years/]
- VideoZeus (2020). How To FAKE A Zoom Meeting - Clone Yourself On Video. April 22. https://www.youtube.com/watch?v=eprkLhdqh4U
- Webalive (2017). "Australia's Growing Ecommerce Industry and How It Is Changing Retail Trends," March 5, accessed August 31, 2017, [available at https://www.webalive.com.au/future-of-australian-ecommerce/]
- Zhang, M., Press, O., Merrill, W., Liu, A. And Smith, N. (2023). How Language Model Hallucinations Can Snowball. arXiv. https://arxiv.org/abs/2305.13534.