Re-inventing Internal Controls in the Digital Age

April 2019

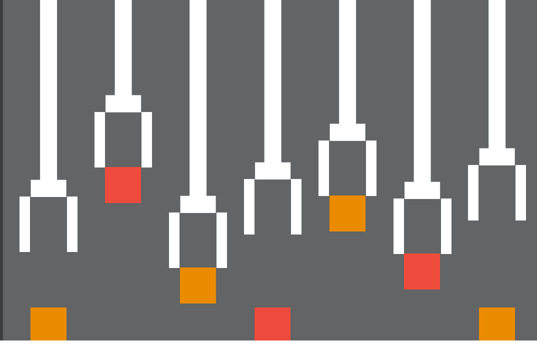
pwc

ACCA Think Ahead

INSEAD The Emerging Markets Institute

Contents

Acknowledgements



We would like to thank the following roundtable participants and interviewees for their knowledge contributions and valuable insights:

Eric Ang, Senior Vice President, Group Compliance, United Overseas Bank Limited

Daniel Berenbaum, Vice President Finance, Group Compliance, Asia Pacific Chief Financial Officer, Globalfoundries

Dietrich Benjes, Vice President & General Manager APAC, Varonis Systems Ltd

Sudeep Chatterjee, Associate Vice President, Partnerships, MetricStream Inc

Kevin Fitzgerald, Regional Director, Asia, Xero

Anirban Kumar Ghosh, Asia Pacific Controller, Jones Lang La Salle

Rajeev Gupta, Regional Financial Controller, Avaya Singapore Pte Ltd

OoiLing Hon, Vice President Operations Finance Asia, Finance – FSAP, Four Seasons Hotels Ltd

Helen Kim, Head of Customer Sales, ALEX Solutions

James Lee, Director of Finance, Sofitel

Shawn Leong, Director, Handshakes

Lim Soon Hock, Managing Director, PLAN B ICAG, Adjunct Professor, National University of Singapore

Sarah Nabaa, Vice President, SE Asia & ANZ, VeChain.org

Vincent Lim, Chief Financial Officer - Asia Pacific, Datalogic

Rajendra Kumar Shreemal, Chief Financial Officer, QuEST Global Engineering

Cherie Sim, Regional Finance Manager, Owndays Co. Ltd

Joyce Tong, Director Finance & Procurement, Info-communications Media Development Authority

Wah Yee How, Deputy Director, Finance (Shared Services), Public Utilities Board

Andrew Watson, Regional Financial Controller, ASEAN ANZ, Association of Chartered Certified Accountants

Wong Kiew Kwong, Head of Internal Audit, SMRT Corporation Ltd

Foreword: Vision of the Future

Companies put in place internal controls to safeguard assets, prevent fraud, verify financial records, monitor organisational performance and ensure efficient and uninterrupted flow of business.

Digital technologies are transforming traditional industries and business models. They are also impacting common control procedures, the overall control environment, risk management and audit.

Some companies are using sensors to monitor the quality of their manufacturing plants and operations. Others have implemented distributed ledgers to track their supply chain from raw ingredients all the way to end products. Robotic Process Automation (RPA) is being used by finance and operations to automate controls and improve precision, whilst Artificial Intelligence (AI) is allowing organisations to continuously monitor and visualise enterprise risks in real time and propose actions.

In this report, we consider how contemporary technologies are allowing improvements to business processes and control environments to be realised.

Referencing COSO's[1] integrated internal control framework, we see how organisations are using predictive analytics and experimenting with blockchain and drones to strengthen their controls.

However, introducing new technologies comes with risks, particularly around cybersecurity and data privacy. We show that it is critical to balance innovation with safety and security to mitigate the risks.

[1] The Committee of Sponsoring Organisations of the Treadway Commission (COSO) is a joint initiative to combat corporate fraud. It was established in the United States by five private sector organisations, dedicated to guide executive management and governance entities on relevant aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. COSO has established a common internal control model against which companies and organisations may assess their control systems. COSO is supported by five supporting organizations: the Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI)

Executive Summary

Key Findings

1. Internal control concepts and principles, such as those in COSO's Integrated Internal Control Framework, will continue to be applicable and relevant in the digital age. In fact, technology can make internal controls even more effective, efficient and pervasive.

2. Even basic automation can improve internal controls by instilling discipline in organising and standardising processes. However, a process and its controls must be designed appropriately before automation is considered. Automating a poor process is counter-productive and may increase risk. Technology can also give rise to new risks that may not be adequately addressed by current internal control systems.

3. Many organisations are already deploying or exploring emerging technologies for control tasks or processes, for example, AI for anomaly detection, or drone technology for inspections and aerial surveillance (refer to page 14). In the future, we expect these technologies to be used more widely for control purposes.

4. When supply chains are connected to blockchain and the Internet of Things (IoT), controls span across an entire ecosystem of companies and individuals interacting through technology. The boundary between internal and external controls will be blurred. As a result, the concept of "internal" controls may have to be rethought and revised accordingly.

5. In the digital age, data governance and control culture will become more important as more controls become embedded in automated systems. Beyond this, a level of professional skepticism must remain to challenge the systems and be able to identify when the system could be wrong. The CFO and finance function plays a key role in both embedding a data-driven control culture and maintaining a skeptical mind-set.

6. Continuous testing and monitoring of controls requires interdisciplinary teams and skill sets of audit specialists (for testing controls), business process owners (for overseeing their processes) and technical staff (for building the technology enabled control systems).

76%

of CEOs believe data is critical/important to understand the risks to which the business is exposed, but only 22% feel their data is comprehensive enough for this.

Source: PwC's 22nd Global CEO Survey 2019

> "As you would expect, the risk of human error is high with manual processes. Additionally, you don't always achieve the level of transparency that you would like. Many finance departments in Singapore are still working on Excel spreadsheets - even basic automation would significantly improve controls and transparency.
>
> Daniel Berenbaum, Vice President Finance,
> Asia Pacific Chief Financial Officer, Global Foundries

The world is buzzing with new technologies. Organisations are adapting their strategies and business models as new players capture parts of traditional value chains. Much focus has been on the growth benefits of technological innovation, but risk and control functions are also starting to derive benefits. In this report, we share examples of companies using technology to reinvent internal controls, while reducing risk and cost at the same time. The latest technologies companies use include:

- Cloud Computing – Near limitless processing power of cloud computing allows powerful machine learning algorithms to analyse all transaction data and identify anomalous activities.
- Robotic Process Automation (RPA) – Software bots can run certain processes and control activities with greater reliability and at lower cost than human staff.
- Artificial Intelligence (AI) – Natural Language Processing (NLP) algorithms (a form of machine learning) can scan large text documents and check for values, accuracy and consistency with other documents.
- Drones – Unmanned vehicles equipped with video cameras can be used to verify the quality and quantity of assets in hard to reach locations, such as tall buildings, construction sites and out at sea.
- Blockchain – A distributed ledger of cryptographically secured transactions in a supply chain network can mitigate risks of unauthorised alteration of records.

> “JLL Property is a data company, so we have to protect the data. As a Proptech company we can do valuations of a London property from our desks in Singapore using IoT sensors. We put sensors in our buildings and analyse the data remotely and continuously. We do not need to send our people down to sites to physically check if anything is faulty.
>
> Anirban Kumar Ghosh, Asia Pacific Controller
> Jones Lang LaSalle

The use of these technologies will create more data, raising concerns around cyber and information security risk, as well as fair, ethical and permissible use of data.

Putting in place AI to augment or replace human decision-making in a responsible way will require four key components to be assessed – fairness, explainability, safety and accountability.

Internal controls will impact multiple stakeholders. Technology will impact how management and other lines of defence operate. Audit committees have a role to play in defining expectations, tone and control culture. Traditionally seen as providing oversight, this may also verge on accountability for achieving a high level of precision on an organisation’s control environment.

External bodies, such as auditors or regulators, will change the way supervisory activities are performed. This creates an opportunity to collaborate effectively, harmonise and align assurance efforts among stakeholders.

The key challenge that organisations must overcome arises not from technology, but from its adoption. Some people in the organisation may resist change due to fear of being replaced, others may not use the tools effectively due to lack of skills or training. A well thought through change programme, supported and driven from the top, is critical to transform control functions and prepare them for the future.

Ultimately, organisations that embrace change will not just be able to manage risks more effectively, but will experience significant benefits to their growth and bottom line.

> “I expect more companies to adopt technology, including data analytics, to enhance business performance, risks management, controls and governance but the speed of adoption is the challenge.
>
> Wong Kiew Kwong, Head of Internal Audit
> SMRT Corporation Ltd

Methodology

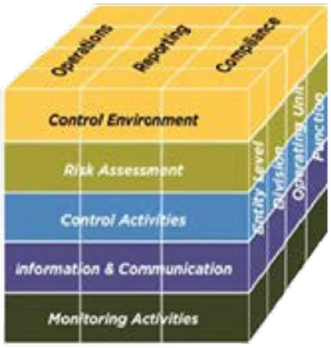
In order to better understand how organisations have implemented and operated internal controls using new technologies and to study their impact on stakeholders (including CFOs, Auditors, Audit committee members and others), this research used a variety of methods to gather feedback and data.

A roundtable discussion was conducted with CFOs in October 2018. An online survey was distributed in December 2018 and January 2019. Concurrently, interviews with CFOs, auditors and others were conducted. This was supplemented by desktop research. The full list of participants of the roundtable and interviews can be found in the Acknowledgements (page 3).

Integrated Control Framework

The most widely recognised internal controls framework is the COSO framework, which was incepted in 1992. While it has been updated since then, the fundamentals have not changed. COSO defines internal control as follows:

"Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance."



The well-known COSO cube[2] defines five integrated components across three categories of objectives and different levels of organisational structure.

Even with the advent of new technologies, from cloud computing to AI, COSO's framework remains relevant and effective. The framework recognises that technological innovation creates both opportunities and risks.

Technology, used in the right way, can enable organisations to address COSO's 17 principles across five components more effectively.

The COSO guidance further explains that, *"The principles in the framework do not change with the application of technology. This is not to say that technology does not change the internal control landscape. Certainly it affects how an organisation designs, implements, and conducts internal control, considering the greater availability of information and the use of automated procedures, but the same principles remain suitable and relevant."*

This is evident in the first component - Control Environment. COSO breaks down the Control Environment into five principles which companies should apply to deliver effective control. One of these principles is, *"The organisation demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives."*

Through the use of predictive models on employee movement or behavioural analytics to identify candidates with the right cultural fit, companies are now enabling strategic workforce planning with greater sophistication. E.g. controls can proactively address competency retention. Singaporean bank, DBS, uses analytics to predict with very high accuracy whether a sales person will quit over the next nine months.

In a recent interview with Strategy+Business[3], Piyush Gupta CEO, DBS explained, *"It [AI system] uses data science. We can track basically everything that signals the employee's engagement or disengagement: what time do they come to work, how many times do they access email. We send a list to the managers and say, "We think these are the people who are likely to quit in the next year," and the manager has the choice of whether to engage with the person ahead of time."*

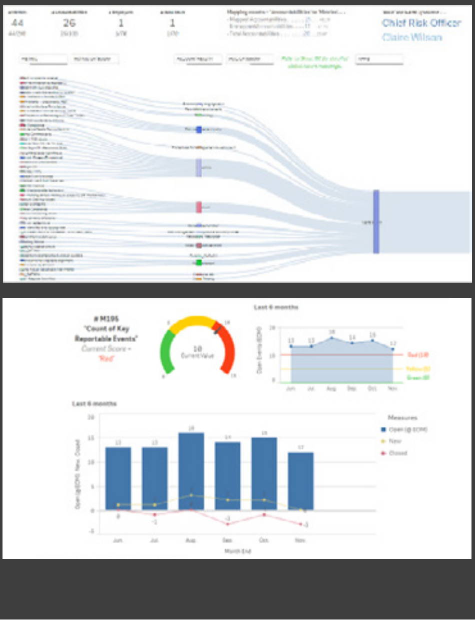
[2] https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf

[3] https://www.strategy-business.com/article/Transforming-a-Traditional-Bank-into-an-Agile-Market-Leader

Within the control environment component, COSO also has a principle around accountability of performance and internal controls. In recent times, shareholders and communities have raised concerns around lack of accountability, which sparked regulators to step in to encourage and enforce accountability.

In response, organisations are using data intelligence to provide transparency and visibility into key accountability indicators and tracking these quantitatively. This gives real time transparency to appropriate controls, delegation and problem management and even whether individuals are exhibiting the right behaviours and conduct.

Figure 1: Dashboard for continuous monitoring of senior role KPIs

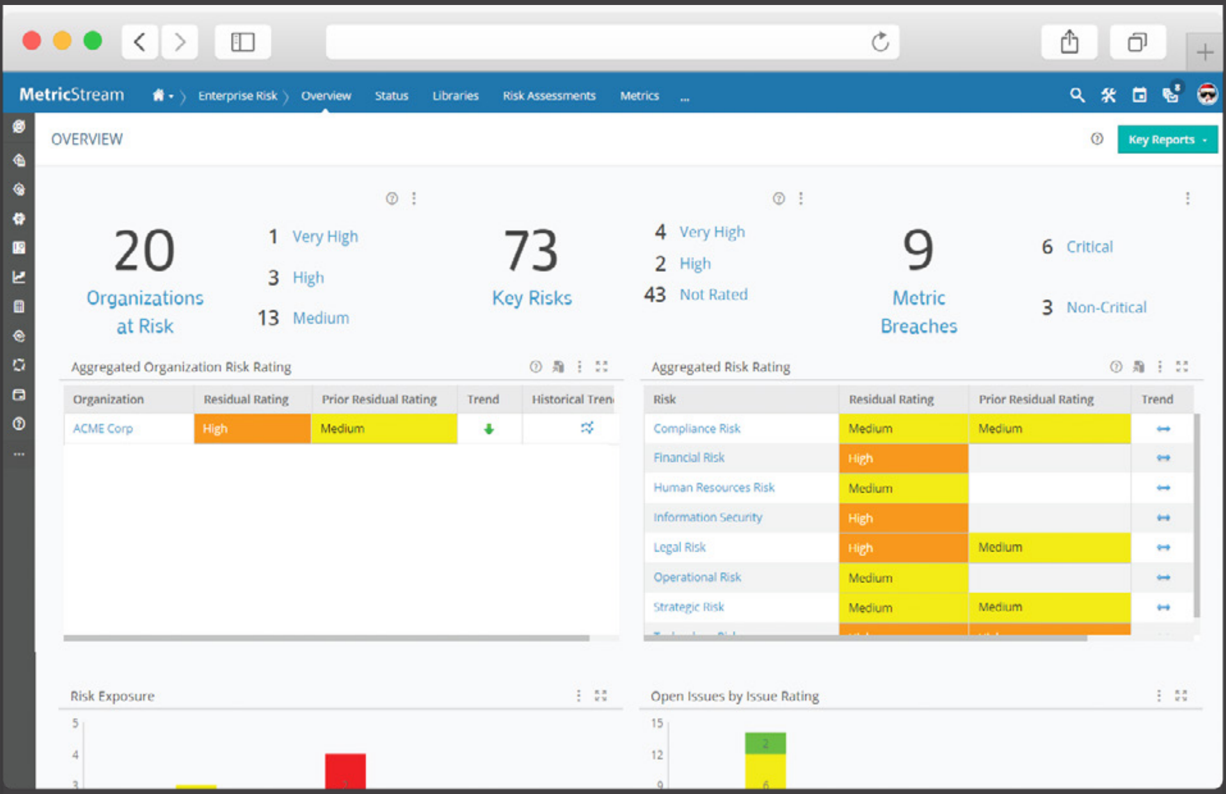


Organisations are using data analytics to track accountabilities assigned to senior roles, and their respective delegations.

The metrics are used to measure and track the performance and activity against accountabilities and responsibilities.

Ultimately, the way organisations design and operate controls can be disrupted with technology. Every layer of internal control is being transformed, and modern day Governance Risk and Compliance (GRC) technologies (e.g. Figure 2) are illustrations of how businesses are digitising their entire approach to control governance, including culture and conduct.

Figure 2: MetricStream enables monitoring of entity-wide risks



Aggregated Organization Risk Rating

Organization	Residual Rating	Prior Residual Rating	Trend	Historical Tren
ACME Corp	High	Medium	↓	

Aggregated Risk Rating

Risk	Residual Rating	Prior Residual Rating	Trend
Compliance Risk	Medium	Medium	↔
Financial Risk	High		↔
Human Resources Risk	Medium		↔
Information Security	High		↔
Legal Risk	High	Medium	↔
Operational Risk	Medium		↔
Strategic Risk	Medium	Medium	↔

Contemporary GRC solutions use technology to tie various components together. Some organisations use platforms such as MetricStream to manage their enterprise governance, risk and compliance functions. The process for enterprise **Risk Assessment** leverages MetricStream to provide a continuous view of risks throughout the organisation. These are updated dynamically, allowing the company to respond, adapt and remain agile. Through case management, frameworks of risk taxonomies and regulatory obligation & policy repositories, the system helps the second line of defence to communicate and enforce **control activities. Monitoring** of control activities is enabled through self-assessments and audit management capabilities. By centralising and making available all the data, this helps the organisation achieve adequate **information and communication.** Ultimately, GRC technology enables senior management to have clearer visibility of their risk profile and internal **control environment**, achieving greater responsibility and accountability, and driving better business performance.

Key Technologies and Associated Risks

Technological advancement impacts how organisations operate. While the focus on transformation is often prioritised on customer facing operations, companies are starting to realise that in order to have greater business resilience, they must disrupt the organisation (including internal controls) pervasively.

The core elements of people, processes, technology and data thread through any activity. Addressing each of these within an organisational culture that supports innovation and creativity is important for harnessing emerging technologies.[4]

The following section explores how modern technologies will impact internal controls.

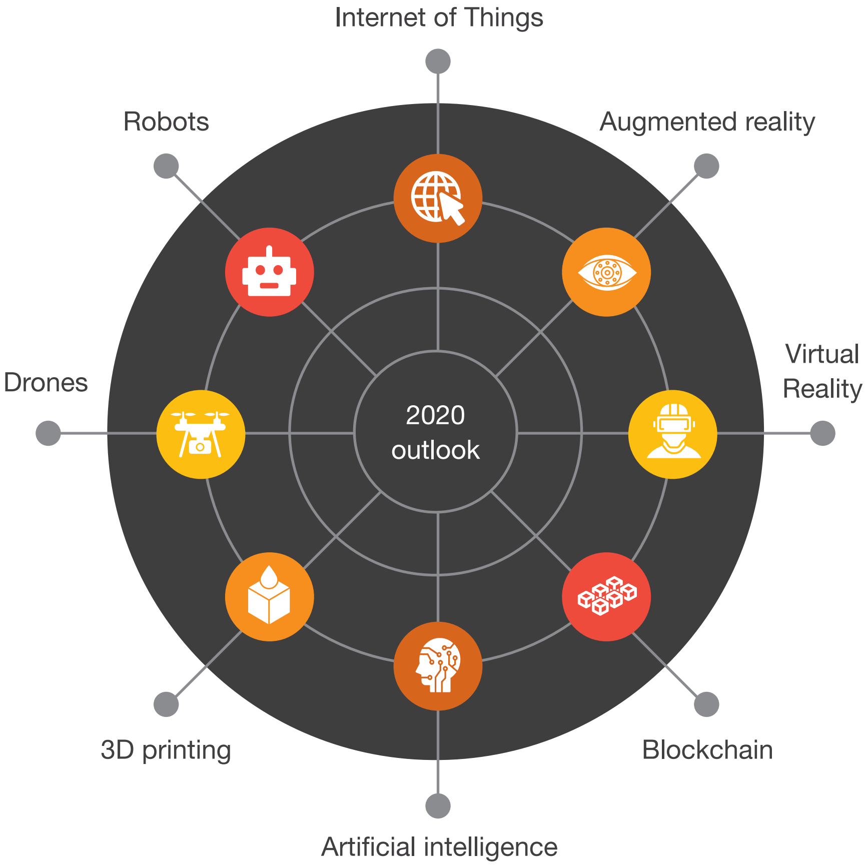
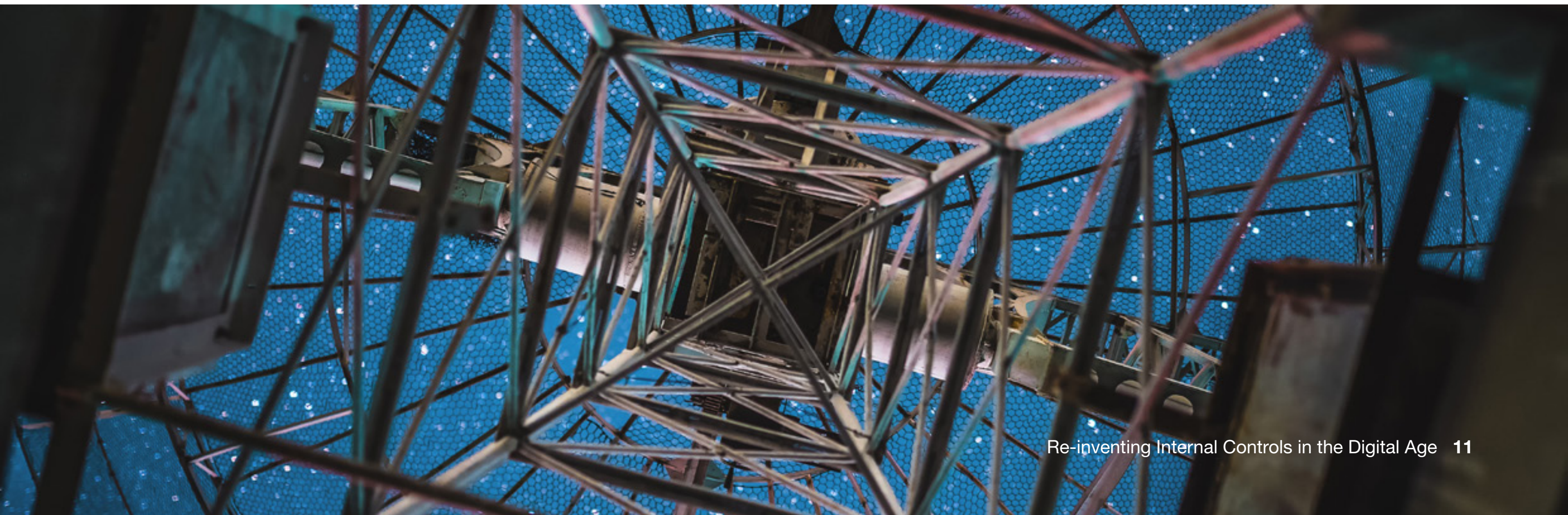


Figure 3: PwC's Essential Eight

PwC's Essential Eight are technologies that every organisation should consider to derive business impact and have strong commercial viability.

Source: https://www.pwc.com/gx/en/issues/technology/essential-eight-technologies.html

[4] The Race for Relevance, Technology opportunities for the Finance Function, ACCA, 2017.



Cloud Computing

Cloud computing is not considered an emerging technology anymore, but it is important to first consider this as its use is so pervasive globally.

It has become a business in excess of $250bn[5] in 2018 with many organisations adopting the use of cloud providers for their IT needs, from infrastructure to platforms and software.

Heightened risks could arise through the use of hybrid cloud technology. Organisations must therefore implement appropriate controls to strengthen their IT environment.

Many cloud providers have high standards of controls that can be passed on to their customers, e.g. control certifications and attestations of their technology control environment, along with tools to help organisations deliver their internal control objectives.

Even with these in place, organisations still need to be accountable for their own controls across hybrid and multi cloud environments.

Risks

Some of the key risks that organisations must address revolve around data. Personal data is protected by laws and regulations in many countries, e.g., Singapore's Personal Data Protection Act (PDPA) and the EU's General Data Protection Regulation (GDPR).

On a broader perspective, cybersecurity risks have increased due to the use of third party infrastructure and multiple data centres, where applications and data reside.

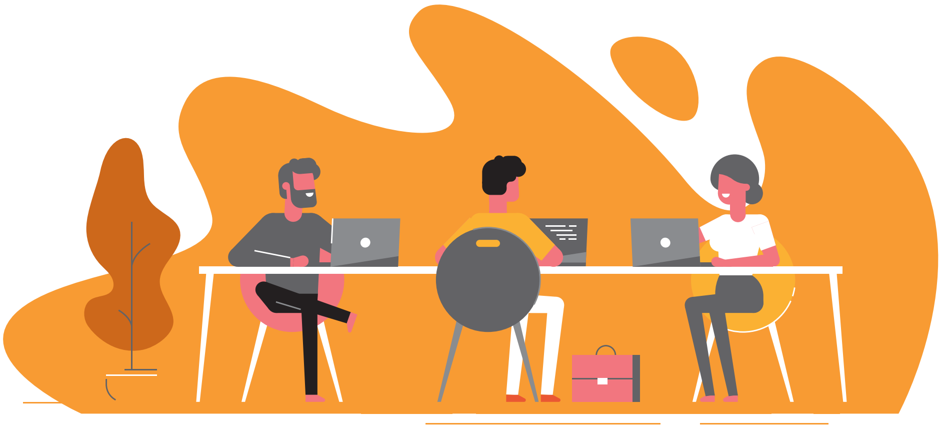
Having the right controls over the infrastructure, platform, applications and data is critical. Working together with the cloud provider to achieve this is necessary.

Some countries, such as China, impose strict laws over data residency. In Singapore, the financial services regulator, Monetary Authority of Singapore (MAS), uses a more pragmatic approach, requesting financial institutions to consider cloud usage from the perspective of Technology Risk Management and Outsourcing Guidelines.

The general message is that organisations must be satisfied with their overall control environment, even when using outsourced service providers such as cloud: *"MAS is amiable to financial institutions leveraging cloud-computing services. As in any outsourcing arrangement, institutions should perform due diligence as well as risk assessments relating to outsourcing and implement appropriate governance framework, processes and control measures to manage and mitigate risks associated with such engagements."* - MAS (2016)[6]

In order to address trust issues around hybrid and multi-cloud environments, every organisation needs to conduct risk and control assessments in line with industry standards, frameworks and best practices and take appropriate remedial measures.

Additional consideration may be required to evaluate unforeseen risks due to an organisation's current lack of familiarity with technology.



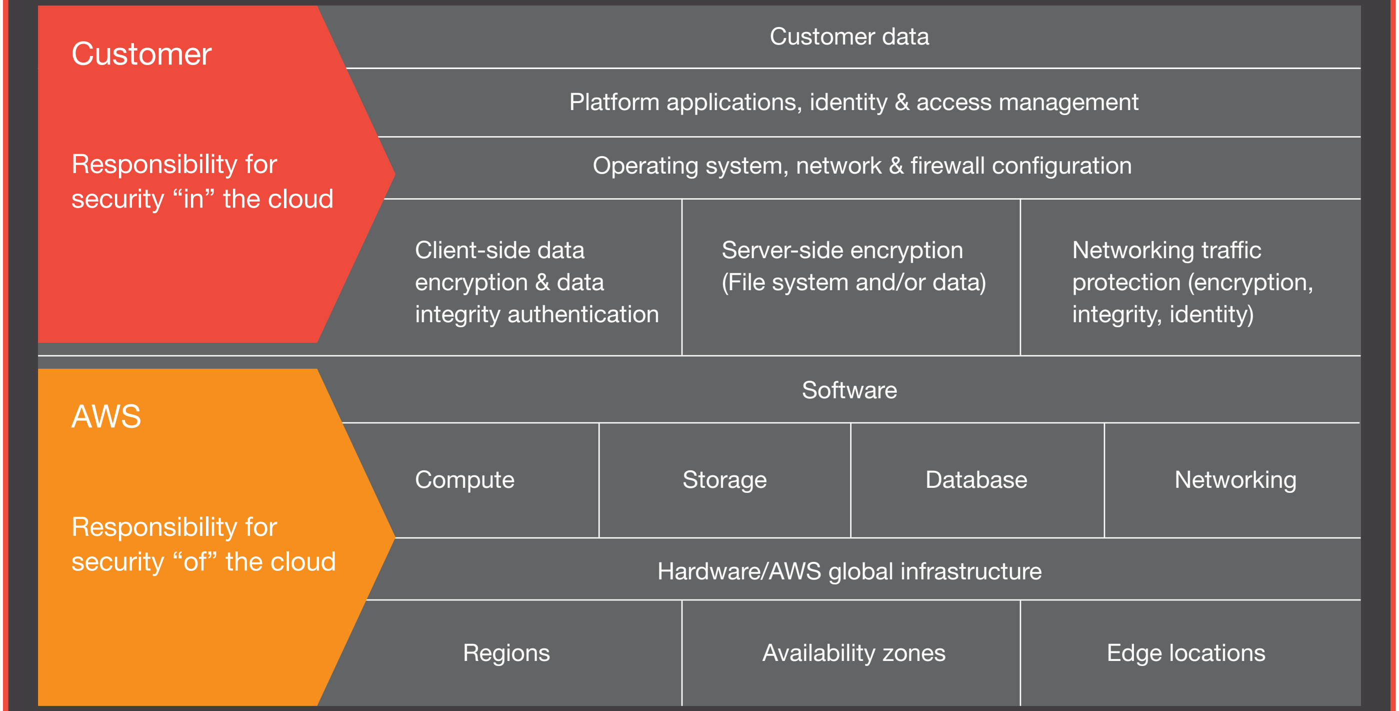
[5] https://www.statista.com/statistics/477702/public-cloud-vendor-revenue-forecast/

[6] http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FAQs/Regulations-and-Guidelines/2016/Regulations-1.aspx

Amazon Web Services (AWS) shared responsibility security framework

When customers engage Amazon Web Services (AWS), responsibility for security is shared. Typically, AWS assumes responsibility for “security **of** the cloud”, while customers are responsible for “security **in** the cloud.” With this model, an organisation’s duties are made simpler as AWS takes on the onus of security for key infrastructure and physical components.

Figure 3: AWS’s shared responsibility framework depicts the customer’s and AWS’s security responsibilities



Customer

Responsibility for security “in” the cloud

Customer data

Platform applications, identity & access management

Operating system, network & firewall configuration

Client-side data encryption & data integrity authentication

Server-side encryption (File system and/or data)

Networking traffic protection (encryption, integrity, identity)

AWS

Responsibility for security “of” the cloud

Software

Compute

Storage

Database

Networking

Hardware/AWS global infrastructure

Regions

Availability zones

Edge locations

To assist customers with their own obligations, AWS provides services to allow customers to protect their data. As organisations migrate and produce more data on AWS, they may look to rich analytics services such as Amazon Macie for data security needs. Leveraging machine learning, Macie allows organisations to discover the sensitive data that resides in their cloud instance. Once identified, the service is able to provide alerts to customers if there are indicators that the data is being accessed or moved in an unusual fashion. The alerts can then be sent for automated remediation and tracking in the customer’s security ticketing system. This can help address risks around unauthorised access or data leaks in relation to Personally Identifiable Information (PII) and Intellectual Property (IP).

Cloud service providers, such as AWS, provide assurance to their customers and other stakeholders via attestations and certifications. Examples are SOC 1/2/3 (control reports) and ISO 27001 (security management controls). Other methods of assurance, such as Singapore’s Outsourced Service Provider Audit Report (OSPAR), go beyond SOC reports by referencing regulatory guidance on outsourcing. However, organisations must keep in mind their own responsibilities, recognise that their own control environment should be suitably evaluated for risks, and address these through independent audits. Furthermore, with tools (e.g. Real-time Insights on AWS) to enable real-time auditing becoming increasingly available, risk profiles can be reduced, allowing controls to become more preventative in nature rather than detective or point in time.

Source: https://aws.amazon.com/compliance/shared-responsibility-model/
https://aws.amazon.com/macie/

Drones

Drones are unmanned aerial vehicles, which can be equipped with a ground based controller and on-board cameras. Data captured, such as videos and images, can be transmitted back to the base for analysis. The benefits include speed of image capture, ability to access remote locations (e.g. out at sea), controlling health and safety risks of humans, and greater precision.

The construction industry has benefitted from drones in multiple areas of internal control. When large assets are being constructed across a vast area (either horizontally or vertically), using drones can help several control objectives:

- Reporting: Used to verify existence, valuation and work in progress of the developments.
- Compliance: Providing a bird's eye view of a site allows surveying to be done quickly to check compliance with stringent health and safety regulations.
- Operational objectives: Acting as a deterrent to workforce cutting corners and to maintain a high quality of work.

Risks

Drones can be subject to specific risks given their aerial nature. Aviation authorities and the industry need to develop complex air traffic management systems for preventing collisions. Cross border risks and flight paths must also be addressed. Data privacy is a concern given that drone operators collect a vast amount of data, including confidential or sensitive information about property or behaviours. Ownership and usage of such data must be carefully addressed.

Stock takes using drones

Drones are being used for car monitoring and stocktaking within a railyard. This has traditionally been time consuming and labour intensive, due to the vast amount of individual elements that can be present. Today, autonomous drones can operate within a pre-defined area, equipped with scanners and cameras to identify particular cars with a real-time flight control system to prevent collisions. This solution is developed to autonomously detect damage to cars, significantly speeding up the inspection and stocktaking processes and cutting the costs of operating and managing a rail fleet.

Stocktaking can be conducted in parallel to the maintenance monitoring process. Precision can be increased by tagging assets with identifying labels, such as barcodes, transceivers or radio frequency IDs. Allowing drones to scan and compare assets against a catalogue of data can identify changes, addressing risks such as abnormalities or absences that could indicate theft.

Source: Clarity from above: transport infrastructure: The commercial applications of drone technology in the road and rail sectors, PwC, Jan 2017

Shipping companies using drones for compliance checks

Increasingly, shipping companies are using drone technology to replace the manual checks that their surveyors and ship inspectors used to conduct. Capturing the images for the ships out at sea enables the company to perform surveys and checks, such as, analysing ship conditions, checking cargo's conformance to contracts and export regulations, and in the co-ordination of the planned loading/discharging of commodities or containers at port.

In addition, some ports impose strict regulations, requiring ships to be "cleaned" before entering the ports, e.g. "biofouling" ships will be imposed with penalties and ships are not allowed to enter such ports to protect the sea waters. Tighter controls also benefit good actors by creating a fairer playing field.

Drone inspections have provided benefits through greater human safety, precision ,and efficiency and the ability to share video and image with its customers, allowing enhanced level of service.

Other than strengthening the operational controls, this concurrently addresses financial reporting controls by ensuring adequate cut-off, supported by the speed at which these measures can be translated back to financial figures at period end.

Source: A global shipping services company

Robotic Process Automation (RPA)

Not to be confused with industrial robots, Robotic Process Automation (RPA) software is a powerful tool to perform manual, time-consuming, rules-based office tasks at shorter cycle times and lower costs than other automation solutions. RPA replicates end user activities, typically through a Graphical User Interface (GUI) that sits on top of other front-end and back-end applications.

> "I believe that RPA will reduce the risk of human errors in internal controls as well as lessen the labour required for checking. Reducing human error will also improve data accuracy substantially."
>
> Cherie Sim, Regional Finance Manager
> Owndays Co. Ltd

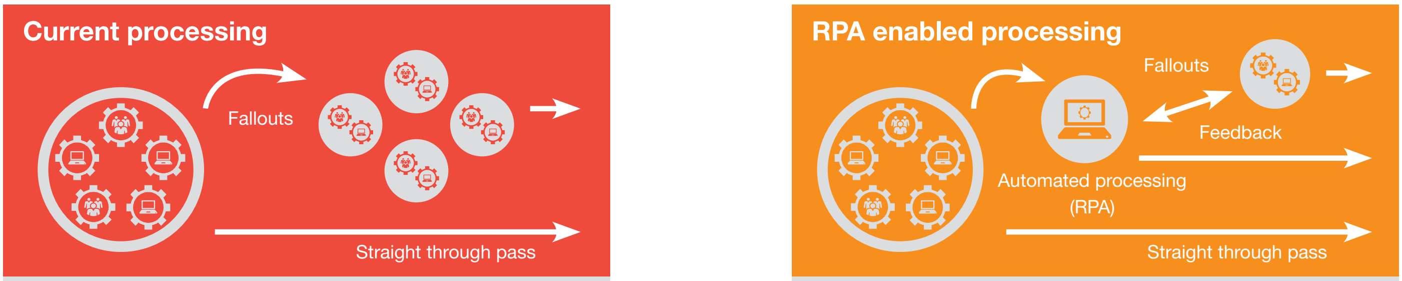
PwC estimates that 45% of work activities can be automated, saving $2 trillion in global workforce costs.[7]

Using RPA allows organisations to digitise expensive, error prone manual processes and internal controls. Every step in the process, every activity performed and all sources of data have a digital audit trail. By carefully planning control processes, a company can embed thresholds and guidelines into the automated processes, expediting testing and risk compliance.

This reduces errors, improves quality, and compliance and customer satisfaction through reduced queries and complaints. RPA is being used by all lines of defence, from operating controls such as reconciliations (first line) to testing controls either as a compliance function (second line) or independently as Internal Audit (third line).

[7] https://usblogs.pwc.com/emerging-technology/briefing-rpa/

RPA enabled processing



High total cost of ownership due to high resource requirement	Cost	Potential reduction to ~10% of current costs
Typically days and hours	Processing time	Minutes and seconds
Typically 1-3% error rate and ROI of over 300%	Quality	Negligible error rate (<0.05%)
Limited scaling and flexability due to resource requirements and manual dependancies	Scalability & flexibility	Provides scalability of solution
Potential for impact to compliance due to manual nature of tasks	Compliance	High process compliance due to automated nature of processing
Staff focussed on low-value, iterative processing tasks	Staff focus	Staff focussed on handling value-added and complex tasks

Source: https://www.pwc.com/ca/en/industries/financial-services/insurance-speak-blog/rise-of-the-robots.html

Risks

Due to its relative ease of use, controlling access to RPA software and IT change management is key. Many business users may treat it as an End User Computing (EUC) element, which inherently may not have strong Software Development Life Cycle (SDLC) and IT general controls in place. Furthermore, as RPA can quickly process large volumes of transactions, ensuring it has been set up and programmed appropriately is important; erroneous setup can quickly affect millions of transactions.

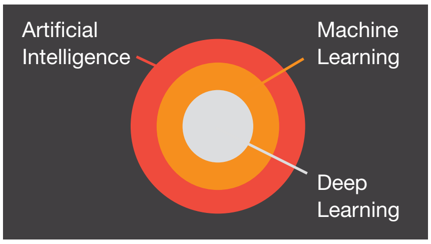
These risks can all be managed within the usual IT controls if followed in a robust manner. Looking at what processes to automate goes beyond IT and organisations should fundamentally consider the design of the underlying process before applying the automation; this will prevent the risk of automating a poorly designed process.

Finally, as RPA may be applied to a subset of an end to end process, it is also important to evaluate the risks that may arise both downstream and upstream of the RPA application.

This may be overlooked when organisations focus too much on the automated tasks in isolation.

Control Analytics and Artificial Intelligence

Figure 4: Types of Artificial Intelligence



Artificial Intelligence

A computer programme that does something smart; replicating human logic and behaviour

Machine Learning

Ability to learn without being explicity programmed

Deep Learning

Algorithms that extract complex representations in layers, emulating the human brain's ability to observe, analyse, learn and make decisions.

Supervised Learning: Technique for building predictive models from known input and labelled response data

Unsupervised Learning: Technique used to draw inferences from datasets consisting of input data without labelled responses.

We typically distinguish three types of data analytics (in order of increasing complexity):

- Descriptive analytics summarises and visualises what happened.
- Predictive analytics anticipates what will happen.
- Prescriptive analytics provides recommendations on what to do.

Many organisations are combining data analytics with automation to help monitor their business. With the data of transactions captured becoming the norm through Enterprise Resource Planning systems, real-time or periodic monitoring can be used as preventive and detective controls to avert risks. Richer sources of data and Big Data technologies are allowing more sophisticated techniques, moving from analysing past performance towards predicting future risks.

AI systems enable predictive methods for analytics, and aim to derive insights from data and propose the best actions to take in order to achieve a given goal. They can learn to adapt their behaviour through analysing the effect on the environment based on previous actions.

Organisations are using AI systems to perform cognitive functions (based on perception, reasoning, learning and problem solving) and to assist and augment human decision-making. In recent years, most of the advances in AI have come from the field of machine learning, in particular deep learning and reinforcement learning.

The hospitality sector is one industry that uses AI and data analytics extensively. Hotel chains operate globally and deal with millions of customer records and transactions. To protect customer data, such organisations are looking to data analytics technologies to continuously scan their systems, to ensure they minimise threats and keep the systems up to date.

Another risk in this sector is in the food & beverage operations, which are particularly susceptible to frauds.

Continuous monitoring using data analytics allows patterns such as application of discounts, void transactions and splitting of cheques to be identified and investigated early and proactively.

The banking sector is also a target for fraud. Credit card providers have long been using analytics to detect suspicious activities, e.g. large values of overseas transactions. However, detection only happens after the transaction has occurred. Contemporary methods based on predictive analytics are able to generate alerts and block suspicious transactions in real time. Machine learning algorithms have taken on a more preventive and proactive role in helping credit card institutions to detect unseen/unknown types of fraud at early stages by analysing wider sets of data sources.

Risks

One key risk is the black box nature of AI. Will an organisation be able to trust a computer to operate controls when it is not immediately visible or explainable how the machine reaches its decisions? Technical approaches to produce transparency and to explain AI can be used to "open up the black box".

> "You cannot take away the human verifiability quality; only a human can give the assurance.
>
> James Lee, Director of Finance
> Sofitel

Predictive maintenance in the airline industry

Companies with large assets (e.g. trains or lifts) that need maintenance have traditionally relied on scheduled maintenance activities to control risks of mis-functioning or malfunctioning. Modern techniques use device sensors to collect continuous feeds of data relating to the assets and its environment.

Aviation companies, such as Singapore Airlines, employ predictive analytics to enhance their maintenance controls, generating cost savings from preventing flight delays. American conglomerate, Honeywell, is working with Singapore Airlines to deploy Internet of Things (IoT) devices which monitor a variety of components (e.g. wheels and brakes) and systems (e.g. air-conditioning and pressurisation). Machine learning can help to identify components that are likely to fail, alert maintenance personnel and prevent delays from happening.

"The airlines will not only receive better and more predictive maintenance services that will reduce mechanical delays and cancellations, the use of connectivity and analytics will make flying more efficient and cost effective."
- Brian Davis, Vice-President, Airlines, Asia Pacific & Aerospace Leader, Honeywell International

Source: https://www.straitstimes.com/business/companies-markets/honeywell-singapore-airlines-group-seal-3-long-term-deals-to-boost

Banks' second line of defence leverages AI

United Overseas Bank (UOB) applies analytics in their compliance function to enhance its Anti-Money Laundering (AML) surveillance.

The use of advanced data analytics within UOB's AML framework has enabled the bank to identify risks that may arise from triggers such as new sanctions faster and more accurately.

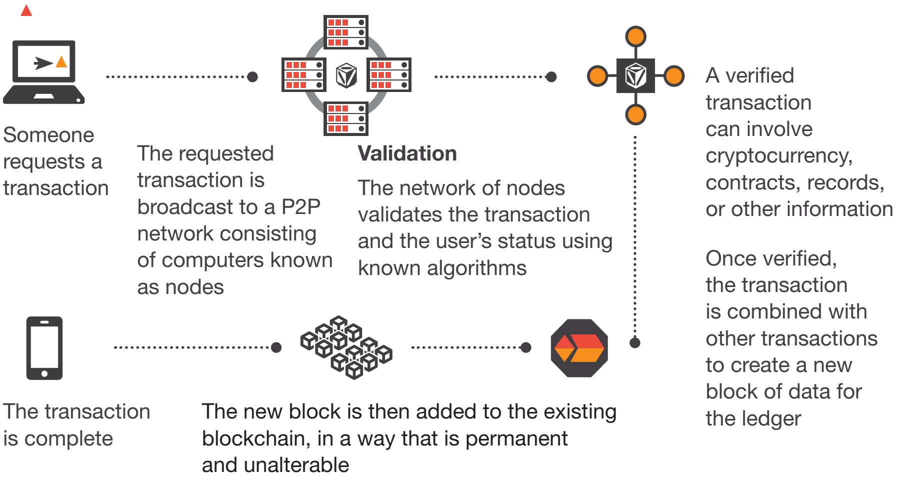
The bank is also using advanced analytics such as statistical programming languages and visual analytics to determine targeted risk areas to better prioritise business reviews on potential high risk clients or transactions. Transactions of concern that are identified from these reviews are fed back into the AI-driven data analytics solutions to improve the way in which it identifies risks.

UOB plans to deepen the way in which it is using AI in compliance, such as exploring deep learning to provide contextual analysis on news articles. These automated and intelligent searches can then feed into the risk profiles of customers to enhance the Know Your Customer (KYC) process.

Source: United Overseas Bank

Blockchain

How it works



Someone requests a transaction

The requested transaction is broadcast to a P2P network consisting of computers known as nodes

Validation

The network of nodes validates the transaction and the user's status using known algorithms

A verified transaction can involve cryptocurrency, contracts, records, or other information

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger

The new block is then added to the existing blockchain, in a way that is permanent and unalterable

The transaction is complete

Benefits

- Increased transparency
- Accurate tracking
- Permanent ledger
- Cost reduction

Unknown

- Complex technology
- Regulatory implications
- Implementation challenges
- Competing platforms

Blockchain is a decentralised ledger of all transactions across a peer-to-peer (P2P) network. It allows participants to transact with each other securely and transparently without the need for a central authority. Blockchains can be categorised based on the permission model.

If anyone can read from and write to a blockchain, it is permissionless (public). If only particular users have reading and writing rights, the blockchain is permissioned (private). Permissionless blockchains have no central authority and everybody can participate. There are economic incentives (typically earning some type of cryptocurrency) to participate in the consensus mechanisms that secure the network. In a permissionless blockchain, the ledger and full transaction history are public. Bitcoin, Litecoin, Ethereum, DASH, Ripple and Hyperledger are examples of popular public blockchains.

Permissioned blockchains use the same distributed architecture as permissionless blockchains, but only selected participants are allowed to record and/or read transactions on the ledger. The consensus mechanism can be adapted to the level of trust between participants. Banks, logistics, insurance and health care firms have all built prototypes of private blockchains.

It is a common misinterpretation to assume blockchain networks are "trustless" environments. While there is no trusted third party certifying transactions in permissionless blockchain networks, there is still a great deal of trust needed to work within a blockchain network. One of the biggest barriers to corporate blockchain adoption is the lack of trust in the technology, especially around reliability, speed, security, scalability, interoperability and regulatory oversight.

From a regulatory compliance or audit perspective, blockchain technology holds great promise. Rather than having to trust a central authority (e.g. government or bank), counterparties can transact with each other directly via a decentralised ledger. Once a transaction is validated by all nodes through a consensus mechanism and added to the ledger, it cannot be altered without compromising the entire chain – it is permanent.

Although many prototypes have been built in the last ten years, blockchain is still a few years away from widespread application at scale. The technology struggles with inefficiencies, high energy costs for mining, trust concerns and lack of standardisation. Recent declines in investments and cryptocurrency prices have led to a certain (some might say well overdue) shake-up and consolidation of the sector.

However, as of early 2019 many promising projects are moving ahead and interesting products are being built for supply chain, trade finance, insurance, health care, land registries, KYC, self-sovereign identity and data sharing.

If transactions are on blockchain, certain control activities (either within a company or in the entire ecosystem of participants) will become easier. VeChain is a distributed business ecosystem platform for logistics, supply chain, product lifecycle and data management. Using blockchain technology allows VeChain to provide transparency in supply chain and in turn protects client brands and enables verification and traceability of products.

This addresses risks around product verifiability and integrity, country of origin and transaction lifecycle. It establishes trust in industries such as food & beverage supply. Vintage wine, for instance, is a valuable asset and needs to be protected from tampering, diluting and counterfeit.

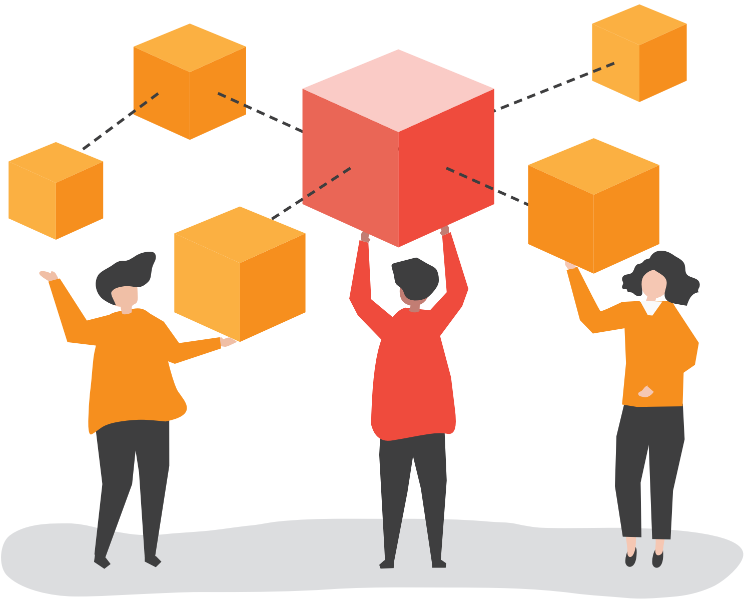
Risks

While blockchain technology in itself is highly secure and reliable, it does not provide account/wallet security. Credential and key management is crucial to protecting digital assets stored on the blockchain.

Smart contracts bridge the gap between the physical world and the digital world by encoding complex business, financial and legal arrangements onto the blockchain. These contracts, just like traditional business rules, are subject to errors in coding and in interpreting intended outcomes.

Furthermore, as with any automated system, most failures will occur at the hand-offs.

No matter how secure the blockchain technology is, organisations will have to carefully consider who will have access to the data and encryption keys.



Wine traceability through blockchain

DNV GL is a company that has created a blockchain solution using VeChain. Wine bottles have a QR-Code, allowing consumers to see the full history of the product and its journey from grape to bottle.

“My Story illuminates products and their supply chain for the benefit of consumers, who will have instant and in-depth access to key product characteristics such as quality, authenticity, origin, ingredients, water and energy consumption and more, all verified by DNV GL along the entire transformation process,” says Luca Crisciotti, CEO of DNV GL – Business Assurance.

Crisciotti continued to explain that using My Story would allow stakeholders within the supply chain to gain trust across various aspects, such as environmental and ethical considerations.

This is an example of how blockchain is providing trust at a consumer level. The story of the grape’s journey has the added effect of creating uniqueness in the participating wine producers (at least initially) which may have the ability to command premium prices in the market, generating impact throughout the value chain. If successful, such technology could be valuable for industries subject to counterfeiting, with high applicability to e-commerce marketplaces.

Source: https://www.dnvgl.com/news/dnv-gl-launches-my-story-the-blockchain-based-solution-to-tell-the-product-s-full-story-113549

Auditing a blockchain

Even though blockchain itself is designed to be tamper-resistant, it usually connects to peripheral layers (e.g. data entry, access management or storage), which are subject to risk. Auditors traditionally inspect readily available, historic data ledgers or audit trails; blockchain environments, however, are real-time and do not include historic ledgers that allow for audit.

PwC's "Blockchain Validation Solution" solves this by integrating a "read-only" node on the corporate blockchain to monitor and log all transactions as they occur in order to apply appropriate controls and continuous testing of all transactions. Transactions that meet specific criteria can be flagged for user review and escalated as needed. Stakeholders can view customised reports via a dashboard.

1

Assess risks and controls

Following the framework, which covers six domains, the company considers questions like how permission is granted to the network and what type of encryption is used. The answers determine the risk and control objectives and testing parameters the company requires to validate its blockchain transactions.

2

Customise software

The software is set up to reflect the company's risk thresholds and meet the needs of its different users. E.g. does the organisation want to monitor all transactions or only a targeted sample? What information do internal audit teams need and which is appropriate for business leaders?

3

Install a read-only mode

The solution establishes a read-only node that is connected to their blockchain infrastructure, enabling it to "see" transactions as they occur.

4

Log and test transactions

As transactions occur, the software automatically logs them and applies controls and testing criteria. Transactions that meet certain criteria are flagged as exceptions for user review.

5

Provide monitoring and reporting

Users view reports via customised dashboards, where they view validated transactions and exceptions. Flagged transactions can be documented or escalated, as needed.

6

Refine approach

As risk and control objectives change, the company can adjust the software settings to meet its new requirements for blockchain validation.

Other key emerging technologies

There are many emerging technologies that can shape the future business landscape. In addition to those discussed previously, let us share a few more.

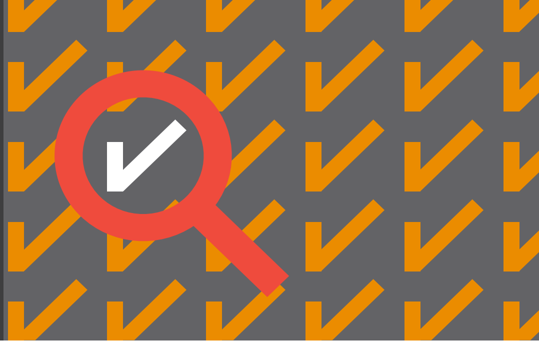
Other emerging technologies	Application and benefits
Augmented Reality (AR) and Virtual Reality (VR): AR bridges the digital and physical worlds, providing a digital overlay to the real world. VR is a fully computer rendered three-dimensional immersive experience.	Visualising data, such as building plans, on mobile devices or helmets helps construction teams in the field understand how various systems and components fit together during construction. AR can place a model of the structure directly into the view of a site in real time, allowing workers to see the exact location, assembly instructions, materials information, warnings and other information associated with a project. This makes the entire construction process easier and faster. By combining data gathered through drones with AR capabilities, workers can get access to the most current information about where and when to install the next piece of a structure or repair a broken part. While AR can help construction teams, VR helps designers and architects visualise a structure to see how everything will look. They can make instant changes smoothly and see the effects immediately without risking delays or serious errors.
Internet of Things (IoT) describes the network of physical objects embedded with sensors, software, connectivity and computing capability to collect, exchange and act on data. Placing sensors on “Things” can help to collect data about them and their environment.	More connected devices means more data to analyse, and this has provided commercial benefits in a range of industries. Examples include predictive maintenance in the transport industry (see page 17) or precision farming techniques in agribusiness, where data on soil and weather forecast can help distribute water for irrigation precisely. However, there are risks associated with connected devices. Most devices are simple sensors without strong security mechanisms in place. Hacking of connected devices is becoming reality. Vendor support may be lacking or unstable, especially if vendors operate in a niche area. However, there are risks associated with connected devices. Most devices are simple sensors, without strong security mechanisms in place. Hacking of connected devices is becoming reality. Vendor support may be lacking or unstable, especially if vendors operate in a niche area.
3D printing allows three-dimensional objects based on digital models by layering or “printing” successive layers of materials.	In the manufacturing industry, companies can better manage inventory by printing what is needed “on demand”. In the medical domain, printing human parts can assist to provide prosthetic limbs, or creating personalised replicas of organs that can be used to simulate interactions with them for medical procedures. This can help mitigate risks of ineffective procedures within real life surgery.

Technology and its impact is profound and presents a plethora of possibilities. All technologies discussed will come with risks related to the data proliferation, hacking and responsible use.

Organisations must consider these risks as they adopt technologies. Some risks can even be mitigated by using technology itself.

> “There will be 20.4 billion connected things by 2020. Total spending on endpoints and services will reach almost $3 trillion in 2020.”
>
> **Source:** Gartner (January 2017)

Key Risks



Cyber and Information Security

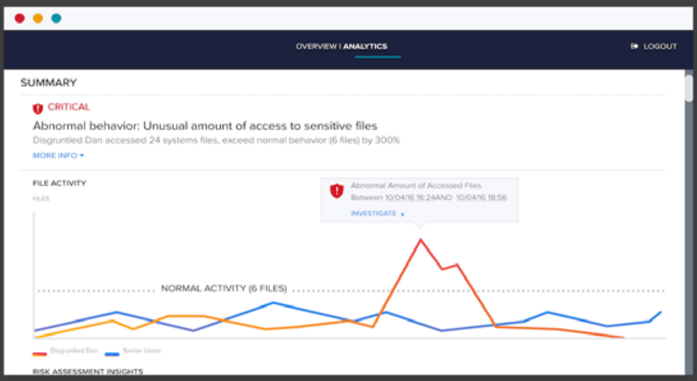
Earlier, we shared some of the risks related to each emerging technology. An overarching concern is cyber and information security. Data that is created through digitisation is invariably at risk of being hacked, accessed by criminals, lost or exposed to unauthorised users, both internally and externally.

Cyber and information security is recognised as a board level risk, and accountability is on the business to protect it. However, the technologies that can expose organisations to the risks can also be used to address these risks.

AI and automation to strengthen cyber controls

Security breaches can result in significant monetary loss and even greater reputational damage. Many organisations allow files and folders to be shared across their organisation. As a result, users have far more access to data than needed to perform their jobs. Embedding strong controls over sensitive data is critical to prevent data theft by outside attackers or even malicious insiders. One health insurance provider has used Varonis, a data security platform, to pass a time-sensitive audit by remediating over 850,000 exposed folders using automation. In a highly regulated environment with sensitive patient data, technology solutions such as Varonis DatAlert can be used to surface alerts to suspicious activity on file servers. The platform uses machine learning to continuously monitor and analyse behavioural patterns to files and data, and define when a user is acting suspiciously, including comparing their activities against their peers, their normal working hours and their individual typical behaviours.

Figure 5: Varonis DatAlert uses machine learning to spot unusual activity to sensitive files to address cyber and information security risks



SUMMARY

CRITICAL

Abnormal behavior: Unusual amount of access to sensitive files

Disgruntled Dan accessed 24 systems files, exceed normal behavior (6 files) by 300%

Abnormal Amount of Accessed Files

Between 10/04/16 16:24AND 10/04/16 18:56

Source: Varonis (https://www.varonis.com/products/datalert/)

Responsible AI

76%

of CEOs are most concerned with the potential for bias and lack of transparency when it comes to AI adoption

Source: PwC's CEO Pulse Survey 2017

Every technology needs to be used responsibly and ethically. AI is no exception. AI systems augment human decision making and continuously learn from their interactions with humans and the environment. In the future, AI systems will likely act more autonomously, making complex decisions that previously required human judgement.

Before humans can fully embrace AI, they need to know whether it can be trusted. In recent years, concerns have grown over how AI could impact privacy, cybersecurity, employment, inequality and the environment. Conventional technologies (e.g., autopilots or industrial robots) run on software that is deterministic and therefore predictable.

Trust is built through testing, auditing, documentation and other means. AI systems, on the other hand, are intrinsically non-deterministic. As the AI agent interacts with the environment and learns, its behaviour evolves. How then can AI be trusted?

Fairness: In the context of AI, fairness typically refers to the minimisation of bias. Bias is a prejudice for or against something or somebody that may result in unfair decisions. Since AI systems are designed by humans, it is possible that humans inject their biases into them, e.g. via the collection of training data. Companies should check datasets and models for bias and put in place suitable bias mitigation methods.

This will reduce the risk of AI-assisted decisions putting certain individuals or groups of individuals at a disadvantage.

Bias in AI policing systems

Several cases of apparent biases observed in real world AI systems have been reported. New Scientist[a] reported on the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) software, which is a decision support tool widely used in the US that leverages AI based algorithms to predict the likelihood of a criminal reoffending. In May 2016, the US news organisation, ProPublica, reported that COMPAS is racially biased. According to the analysis, the system overestimates the risk of recidivism for black defendants and underestimates it for white defendants.

In the UK, several police force have been similarly using AI for identifying future offenders. One system aggregates multiple data feeds as indicators of predicting a re-offender. One particular feature used as data input is the postal code. This has been criticised as re-enforcing existing biases or prejudices in the policing and judicial systems. The continuous re-training, or machine learning, from biased data can further enhance these prejudices.

As reported in Wired[b], Andrew Wooff, criminology lecturer at Edinburgh Napier University, said:

"You could see a situation where you are amplifying existing patterns of offending, if the police are responding to forecasts of high risk postcode areas."

Source: [a]https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/
[b]https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit

Explainability: Consumers want to understand how AI models arrive at decisions, especially if those decisions impact their own lives. However, implementing explainability is non-trivial. There is a natural trade-off between explainability and accuracy of AI models. The development of interpretable algorithms that are able to explain their rationale, strengths, weaknesses and likely future behaviour is currently a top priority of both technology firms and research institutes.

Finance professionals, accountants and particularly auditors need to be able to understand and explain results. Instead of trying to explain AI, others have taken approaches to focus on results rather than the "how."

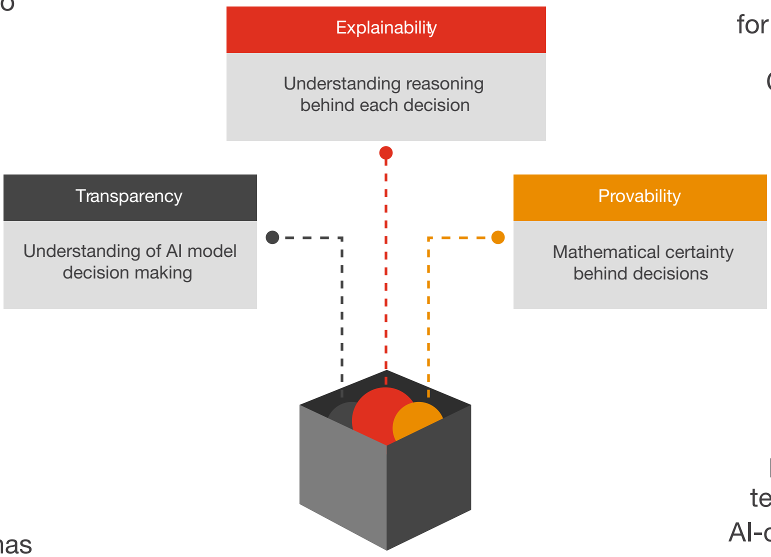
Banks have adopted AML systems that have traditionally flagged suspicious transactions through rules, such as sources of transactions, values etc. While testing modern AI systems, one method has been to compare the outputs of backtesting and considering the accuracy through questions such as:

- Does the AI system produce the same valid alerts that the rule based system did?
- Does the AI system generate any additional valid alerts that the rule based system did not?
- Does the AI system omit false alerts that the rule based system included?

Answering these questions focuses on improvements in the outputs rather than on AI logic.

Safety and Security: Fair and explainable AI systems might still be unsafe to use. Safe AI models incorporate societal norms, policies and regulations that correspond to established safe behaviours. Adversarial attacks (e.g. malicious actors influencing the behaviour of an AI model through altered input datasets) can undermine the security of critical systems.

Figure 6: What it means to look inside AI's black box


Explainability
Understanding reasoning behind each decision
Transparency
Understanding of AI model decision making
Provability
Mathematical certainty behind decisions

Security and robustness of AI can be improved through rigorous model validation, performance benchmarking and continuous monitoring of decision making.

Accountability and controls: Companies need to establish enterprise-wide accountability for AI applications and consistency of operations. This encompasses both internal accountability (e.g. model governance and approval authorities) and external accountability (towards individuals and groups who request information on the inputs for AI decision making).

Controls over AI should cover input data, algorithms, processes and reporting frameworks. Continuous testing and monitoring of controls requires interdisciplinary teams and skill sets of audit specialists, business process managers and technical staff. Ultimately, AI-driven decision making will have to be auditable and traceable, particularly in critical contexts or situations.

The entire process that leads to AI-driven decisions needs to be documented. This can already be achieved today. Over the next few years, internal control departments and external audit firms will develop more sophisticated audit methodologies and mechanisms for AI systems.

Stakeholder Impact

Stakeholder Impact

We have explored the impact of key technologies on controls as well as some of the key risks. Stakeholders will be affected in different ways within an organisation.

Finance Functions - The finance function of the future will use technology to enhance quality of processes and controls. Automation of tasks will allow the finance team to focus on value adding activities to partner the business. The CFO and finance function plays a key role in embedding the control culture and environment throughout the organisation. Other than the financial and reporting controls, finance functions have the ability to work across the organisation in value creation and enhancing performance.

They also have the necessary mind-set of embedding controls to help meet organisational objectives.

One key challenge lies in the willingness and appetite for change. Accountants often have a tendency to want to see things in hardcopy, even where there is automation in place. Trusting systems and AI will need a different mind-set. This might come more naturally to the younger and technology-savvy generation that is about to enter the workforce.

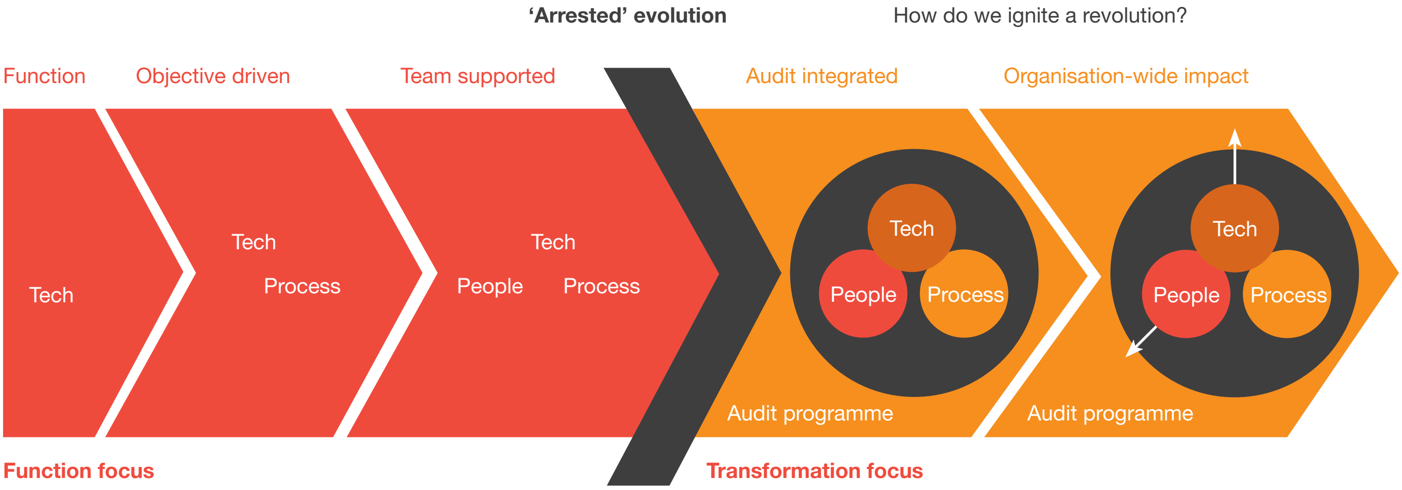
Internal Audit (IA) - Internal Audit functions must see emerging technology from two perspectives. Firstly, as the business adopts technology in their controls organisation-wide, it has to consider new or heightened risks that this may present and how they can provide assurance against these risks.

Furthermore, does the IA function have the right skillset to audit emerging technologies such as AI and blockchain to address these new risks?

Secondly, how can the IA function become a proponent of technology? Besides being consistent with how the enterprise is undergoing transformation, it must also disrupt its traditional ways of testing controls and providing assurance. A focus on technology in isolation will not be successful. Leading IA functions are using technology to lead a revolution in the way they approach the entire audit life-cycle.

Having the appropriate people delivery model and embedding the right processes within the audit programme will accelerate the transformation agenda; which impacts and benefits the entire organisation.

Figure 7: Internal Audit functions need to reimagine their entire operating model to accelerate their technology transformation



Internal Audit functions need to reimagine their entire operating model to accelerate their technology transformation

Source: PwC: Revolution, not evolution - Breaking through internal audit analytics' arrested development (2018)

IA functions that are relatively advanced in their use of data analytics have managed to build continuous auditing systems. These are enabled if data analytics tests can be built into scripts. When a process is established to automate the extraction and transformation of the data from source systems and loaded into the scripts, the audit tests can easily be re-run on a regular or continuous basis. Some IA functions have successfully handed over these processes to the first or second lines of defence. If such systems reside with the business, they can be considered continuous monitoring controls whose design can benefit from an IA functions' control mind-set.

Audit Committees - Audit Committees have a requirement to oversee and assist management in their internal control environment. By seeing how organisations change and influence their control culture and behaviours, they can play a positive part in instituting change for organisations that are slower to move. However, they are another set of key stakeholders who need to have the right knowledge and mind-set to be successful. Audit Committees are generally open to innovation and change, but being removed from the business may lead them to underestimate the real feasibility and challenges faced.

One Singapore based organisation experienced challenges to meet their Audit Committee's directive for an analytics driven approach to control monitoring. It was challenging to repurpose legacy systems that were built decades ago on manual processes and system records with limited data analytics capabilities. This made a truly digital and analytics driven approach not achievable within the confines of cost limitations.

External Auditors - External auditors can rely on the controls that management has in place, in addition to doing their own testing, to gain assurance over financial balances. Auditors often rely on IT systems and controls, and a company's use of new technologies does not change the fundamental risks over an IT control environment. However, risks have increased due to more pervasive use of technologies and the ways in which they are used.

For auditors, the key IT control domains are around development, security, change management and operations. In companies ranging from those with SAP automated controls in place, to those where they leverage blockchain for their smart contracts, auditors can focus on these IT domains to obtain assurance over financial reporting objectives. However, approaches may need to be specialised; two or three decades ago audits required SAP specialists, today they may need blockchain expertise.

In addition to knowing the overarching IT control environment, they must also ensure that they are adequately skilled to test the design and operation of the automated elements of the controls. This will require in-depth knowledge of the technologies to provide suitable levels of assurance.

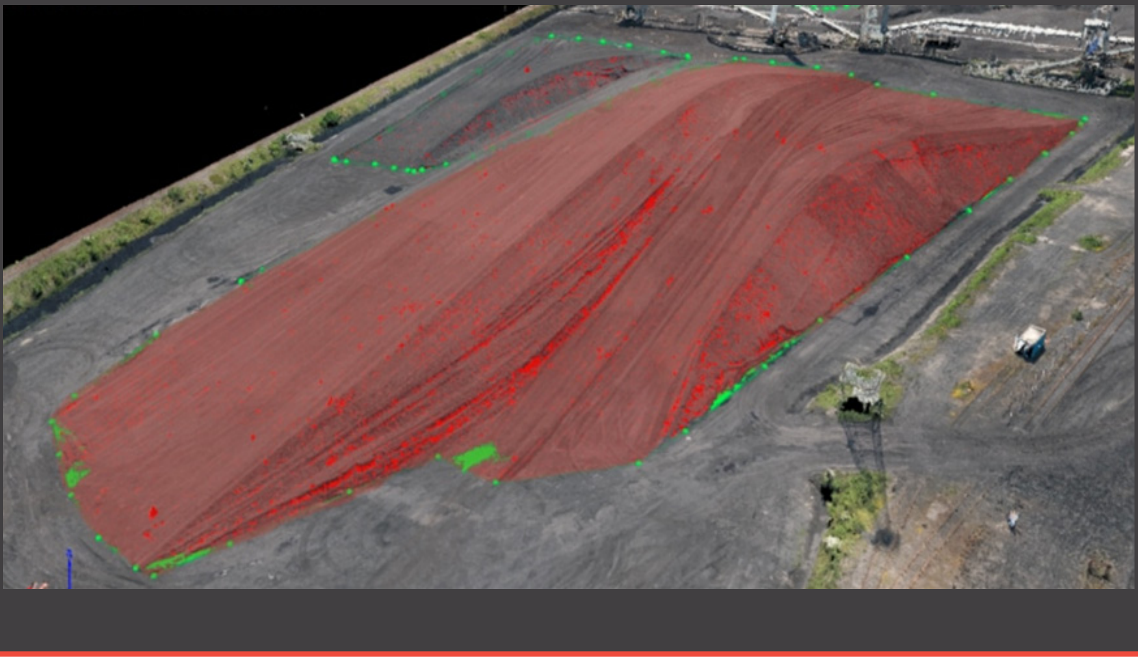
Even where companies have not fully adopted modern technologies, independent audits can be performed using the technology that the auditor brings. Audit tools are becoming sophisticated, e.g. using drones and AI. These provide benefits in the level of assurance that can be attained, leading to a higher quality audit and greater efficiencies in execution.

External auditors using technology for their audits

PwC is using technology to transform the way it conducts audits globally. Auditors embed data analytics systems powered by machine learning to identify anomalies in data that are used as a basis for manual investigation. Being able to interrogate 100% of an organisation's journal or transaction data allows auditors to focus on transactions that exhibit unusual patterns of behaviour, versus traditional methods which relied on random sample testing. The AI element means that the algorithms identify the unusual patterns rather than relying on humans to analyse and identify suspicious activities.

PwC is using drones to perform stock counts to attest to inventory balances reported in a company's financial statements. In one example, a drone captured over 300 images of a coal reserve at one of the UK's last remaining coal-fired power stations Aberthaw in South Wales, owned by RWE, one of Europe's largest energy firms. The images from the drone were used to create a 'digital twin' of the coal pile in order to measure its volume. The value of the coal was then calculated with more than 99% accuracy based on that volume measurement.

Figure 8: "The 'digital twin' created of one of the coal heaps which shows the points measured by the drone"



Regulators - Regulators are also starting to embrace digitisation. Many are not strictly defining what can or cannot be done by organisations and instead are encouraging the fostering of innovation in a safe way. The Monetary Authority of Singapore (MAS), for instance, has issued guidance on how organisations can use technology safely in the Financial Services industry (Technology Risk Management Guidelines, 2013). The MAS has also made regulatory sandboxes available, allowing organisations to experiment and innovate, while containing risks through the inclusion of specific safeguards to contain legal and regulatory impacts.

Similar to IA functions, regulators are also embracing technology for supervisory purposes.

As regulators often collect filings and receive data from multiple companies within their respective industries, being able to attest to data quality and analyse large amounts of data has traditionally been a challenge. Regulators are using Natural Language Processing and machine learning to be able to efficiently sift through large volumes of data, check for accuracy and perform analytics.

Challenges to Organisation Transformation

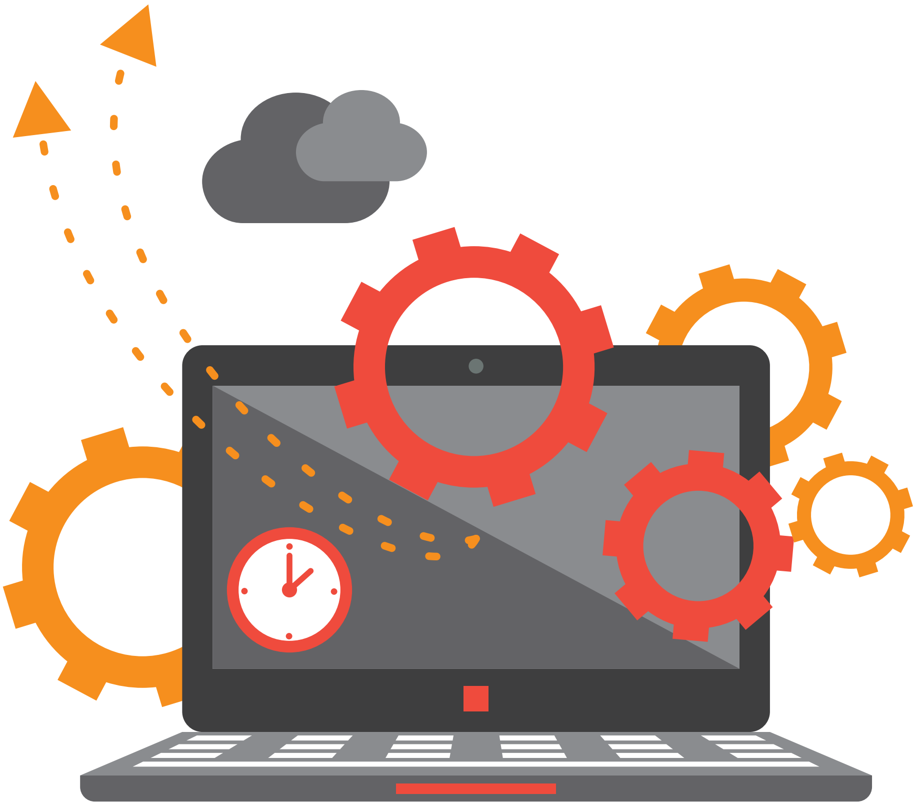
> “Technology alone will not bring the desired control in the organisation. Ultimately, if you want any technology to have impact on the organisation, it depends upon how well it has been embraced by the company’s management. The human element of culture is going to play a larger role in a future technology-driven organisation.
>
> Rajeev Gupta, Regional Financial Controller
> Avaya Singapore Pte Ltd
>
> ”

Organisational Culture - Emerging technologies have fundamentally changed the way man and machine work together, creating new roles, bringing new conflicts and redefining trust.

Companies therefore need to focus on the human experience, consider employee and customer interactions and invest in creating a culture of technology innovation and adoption. Creating better human experiences is critical to raising the “Digital Quotient”. Yet, customers, employees and culture continue to get less attention than strategy and technology, slowing down the assimilation of emerging technologies.

Lack of digital skills is typically named as one of the most important barriers to getting results from investments in emerging technologies. However, capabilities for the workforce of the future go beyond just teaching hard skills; organisations also need to create an environment that will help people develop and flourish. Despite all the talk about automation and AI, companies that want to succeed need to focus on harnessing the talents of the workers who would not be replaced by automation anytime soon.

These people will play pivotal roles in how organisations develop, compete, create and innovate. In a future organisation where technology and humans coexist and collaborate, human skills such as creativity, empathy and ethics will be more important than ever.



> “At UOB, we harness technology to enhance our customer experience and to drive our operational performance. For example, the use of AI in regulatory technology enables us to augment our ability to identify more accurately AML risks. Our targeted approach of identifying where technology can help us to be more effective and efficient enables us to achieve real-life benefits to internal and external stakeholders.
>
> Eric Ang, Senior Vice President, Group Compliance
> United Overseas Bank Limited
>
> ”

Systems and Data - Organisations often realise that a barrier to data analytics lies with the data itself, both in its availability and its quality. Organisations that are not ready cited the absence of data rich systems within their business processes as a key challenge. Some believe that an Enterprise Resource Planning (ERP) system will make them ready. However, with a bit of creative thinking, there are methods to create and enrich data faster than implementing an ERP:

- Data can be acquired from external sources. Some data companies are providing analytics outputs as a service. Others are monetising their own data. Marketplaces are being developed to allow organisations to buy and sell corporate data assets.
- Manual records can be digitised. AI techniques include Optical Character Recognition (OCR) for digitising manual records and Natural Language Processing (NLP) for understanding the context of language within a document. Through this, certain key fields can be captured from unstructured text documents.
- Data can be enriched. Existing corporate data can be used for “feature engineering.” This creates new fields that can be used for analytics. E.g. a new feature could be “time taken to pay an invoice,” which is derived from existing data of “invoice pay date” and “invoice due date.” Using this newly created field, organisations can improve their cash flow through better management of early and late payments or receipts.

Data mining and relationship checking to detect procurement risks

Singapore-based company Handshakes provides data to companies to help them with their relationship checks valuable for KYC risks, credit checks, bid rigging etc. They use data mining techniques on unstructured data, including company registries, news repositories and corporate emails to generate interactive network maps of people and entities.

As reported in The Business Times, Handshakes was used to analyse relationships in government bidding processes. It identified four cases where there were relationships between tenderers of the same jobs. Such relationships included common directors and shareholders, as well as common company secretaries and registered addresses.

Source: https://www.businesstimes.com.sg/government-economy/linked-firms-vying-for-same-public-contracts

Poor data quality can be a hindrance to analytics when companies realise that the output of the analytics does not make sense because the inputs were incorrect. Companies must address this from two angles:

- Cleanse the historic data
  A data cleaning exercise on past transaction data will allow it to be used for meaningful analytics.

  This is both for descriptive (backward-looking) and predictive (forward-looking) analytics.

  Past data can be used as training data to train machine algorithms to be able to predict or forecast into the future.

- Maintain good quality data going forward
  Data governance procedures are put in place to treat data as an asset and enable analytics going forward.

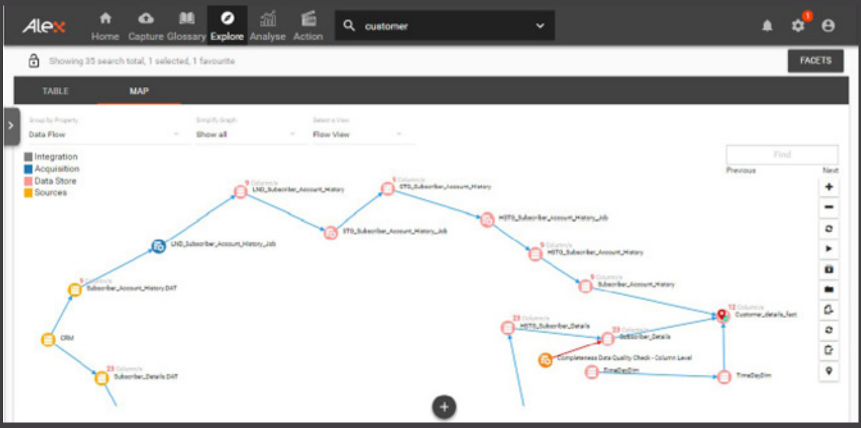
  Organisations must approach data governance holistically, looking at who is accountable and who owns the data, right down to measuring the quality of critical data fields on a continuous basis.

  To oversee the governance process, companies are increasingly setting up Chief Data Officer (CDO) functions as they realise this is a complex task.

> “The question is who owns the data, and who controls it? We need to define who has oversight of the data, how it’s stored and how it’s cleaned before we can rely on it for our control activities.
>
> Andrew Watson, Regional Financial Controller, ASEAN ANZ
> Association of Chartered Certified Accountants
>
> ”

Tracing data lineage through AI

Effective and strategic Data Governance can empower business users to optimise data value through AI applications. Alex Solutions (“Alex”) is a Data Governance solution that can help organisations find, understand, manage and use their own disparate data sources. Alex provides out-of-the-box capabilities to capture end-to-end data lineage, while discovering the locations of sensitive data and personally identifiable information and understanding usage and access behaviour. Australia’s largest telecommunications provider used Alex to greatly accelerate its strategic enterprise data management programme that had originally required large volumes of time consuming manual data asset analysis. Alex automatically identified and classified key data assets, analysed their relationships and impacts, thereby reducing the effort required to map data asset lineage, impact analysis and data asset classification by up to 90%.


Alex
Home
Capture
Glossary
Explore
Analyse
Action
customer
Showing 35 search total, 1 selected, 1 favourite
FACETS
TABLE
MAP
Data Flow
Show all
Flow View
Integration
Acquisition
Data Store
Sources
Find
Previous
Next
LND_Subscriber_Account_History
STG_Subscriber_Account_History
HSTG_Subscriber_Account_History_Job
STG_Subscriber_Account_History_Job
LND_Subscriber_Account_History_Job
HSTG_Subscriber_Account_History
Subscriber_Account_History
Subscriber_Account_History.DAT
CRM
Customer_details_fact
HSTG_Subscriber_Details
Subscriber_Details
Completeness Data Quality Check - Column Level
TimeDayDim
TimeDayDim
Subscriber_Details.DAT

Conclusion

85%

of CEOs agree that AI will significantly change the way they do business in the next five years.

Source: PwC's 22nd Global CEO survey 2019

There is no doubt that technology can enhance the quality, rigour and efficiency of internal controls. Organisations must consider how to embed technology into the control framework in a safe way, while taking into consideration the risks that arise with the use of technology.

Established risks around system development, change management, access and security still applies, but some of them are made more critical by data proliferation and privacy considerations.

Besides addressing risks, organisations must consider how to use technology responsibly and ethically, particularly in a future in which machines will act more autonomously.

They will face many challenges along the way, with organisational culture being a key one. Tone from the top will be critical to guide this journey successfully.

> “There is no turning back on the use of technology and those who do not invest will lose out. People and companies who use technology will be smarter than those who do not, and we are looking at the next internet revolution driven by AI, blockchain and data analytics. We are looking at an epochal development in not just management controls, but also how businesses are run. It is only limited by how fast humans can act.
>
> Lim Soon Hock, Managing Director, PLAN B ICAG, Adjunct Professor
> National University of Singapore
>
> ”

For more information, please visit www.pwc.com/sg

Creating value for our clients, people and communities is at the heart of PwC. With a common purpose to build trust in society and solve important problems, we are a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Our highly qualified, experienced professionals help organisations solve their business issues as well as identify and maximise the opportunities they seek. Our industry specialisation allows us to co-create solutions with our clients for their sector of interest.

PwC Singapore has been recognised as Best in Audit Services (CFO Innovation Awards 2018, 2017, 2015); People & Talent Award (Biennial Singapore Accountancy Awards 2018); Graduate Employer of the Year (Singapore's 100 Leading Graduate Employers Award 2011-2017); Best Practice Award (Biennial Singapore Accountancy Awards 2016, 2015); and Best Tax Advisory (HFM Awards Asia 2015).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.

ACCA Think Ahead

For more information, please visit https://www.accaglobal.com/sg

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants. We aim to offer business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability.

We believe that accountants bring value to economies in all stages of development. We aim to develop capacity in the profession and encourage the adoption of consistent global standards. Our values are aligned to the needs of employers in all sectors and we ensure that, through our qualifications, we prepare accountants for business. We work to open up the profession to people of all backgrounds and remove artificial barriers to entry, ensuring that our qualifications and their delivery meet the diverse needs of trainee professionals and their employers.

We support our 208,000 members and 503,000 students in 179 countries, helping them to develop successful careers in accounting and business, with the skills required by employers. We work through a network of 104 offices and centres and more than 7,300 Approved Employers worldwide, who provide high standards of employee learning and development.

Through our public interest remit, we promote appropriate regulation of accounting and conduct relevant research to ensure accountancy continues to grow in reputation and influence.

INSEAD The Emerging Markets Institute

For more information, please visit https://www.insead.edu

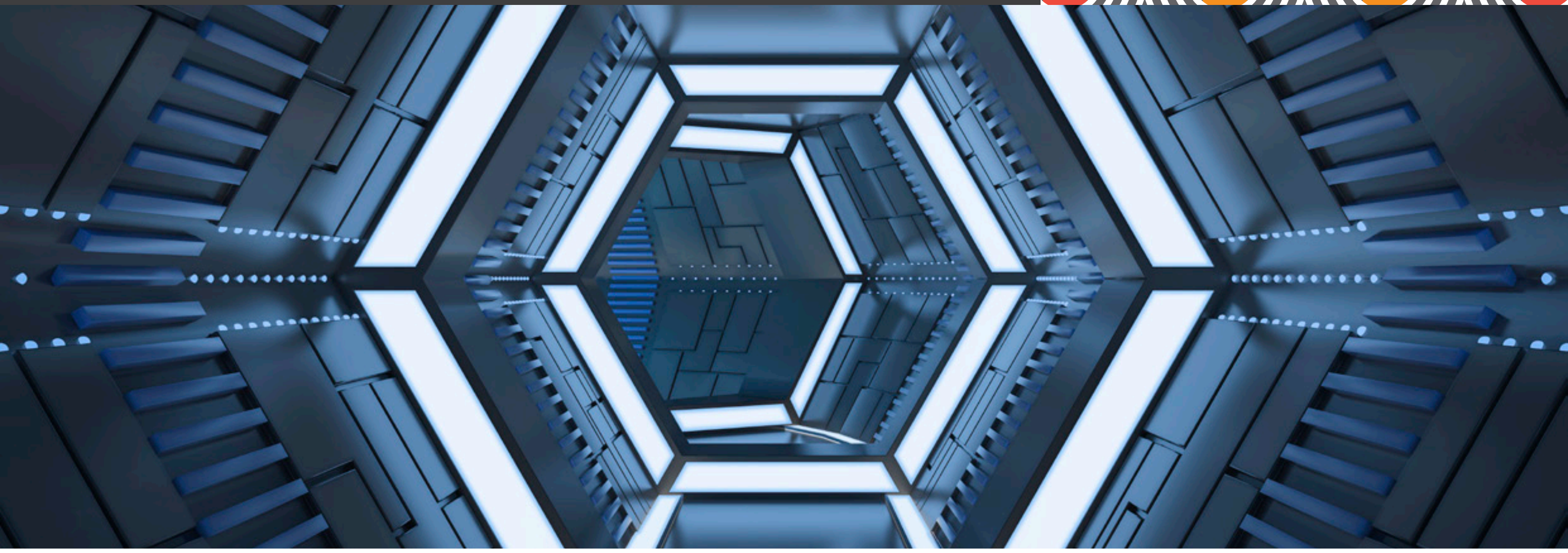
The INSEAD Emerging Markets Institute (EMI) is a leading think tank for the creation and dissemination of credible and timely information on issues related to business management, economic development and social progress in the emerging economies.

This includes the development of cutting edge pedagogical materials, research publications and data sets.

EMI creates knowledge through research and disseminates it for practical application by the individuals, organizations and governments who seek to leverage the opportunities offered by these dynamic economies. Based at the Asia campus in Singapore, and set up in partnership with the Economic Development Board of Singapore, the Emerging Markets Institute reflects the changing focus of global growth and emphasises INSEAD's commitment to the region.

INSEAD's three campuses in Fontainebleau, Singapore and Abu Dhabi provide the unique advantage ofgeographical proximity to emerging countries across the globe.

Contacts



Mark Jansen
PwC | Data & Analytics Leader
mark.jansen@sg.pwc.com

Andre Tan
PwC | Data & Analytics Director
andre.tan@sg.pwc.com

Andreas Deppeler
PwC | Data & Analytics Director
andreas.deppeler@sg.pwc.com

Joseph Alfred
ACCA | Head of Policy and Technical
joseph.alfred@accaglobal.com

Pauline Javani
ACCA | Partnership Manager - Employers
pauline.javani@accaglobal.com

Vinika Devasar Rao
INSEAD | Executive Director,
Emerging Markets Institute
vinika.rao@insead.edu