KPMG

UAE Internal Auditors Association
JOIN, LEARN & SHARE

ARAC

Cracking the code: Continuous Audit Continuous Monitoring

7 March 2022

KPMG Lower Gulf Limited

With you today

Firas Haddad

Firas is a Partner in the Advisory practice of KPMG Lower Gulf Limited.

Firas has over 20 years of audit and business advisory experience. Certified Public Accountant (CPA), Certified Information Systems Auditor (CISA) and a member in the Institute of Internal Auditors and in the Information Systems Audit and Control Association.

Mahendra Khiani

Mahendra is an Associate Director and has 12+ years of experience in Risk Advisory.

Mahendra is a Chartered Accountant from India, MBA (Strategy) from Indian Institute of Management and holds Post Graduate certificate in Data Sciences.

Your expectations!!

Disruption on all fronts

- **Audit way of working has not taken a quantum leap**
- **Technology** provide **better, faster** and **cheaper** alternatives to traditional audits
- **Stakeholders perceived value** of audit is **dropping drastically**
- **Audit not agile enough to cope with business innovations**

1995+

Music
Photograph
Video rental
Entertainment

2005+

Print Media
TV
Travel
HR

2015+

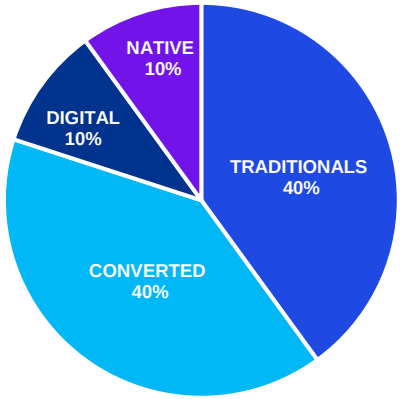
Retail
Automotive
Travel
Education
Telco

2025+

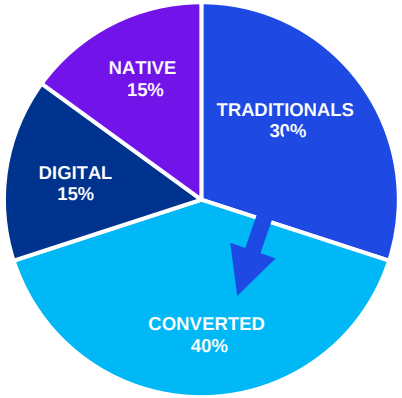
All Safe Havens will be subject to Digital disruption

Companies are transforming and shifting…

Business segments today



Segments within 3 Years



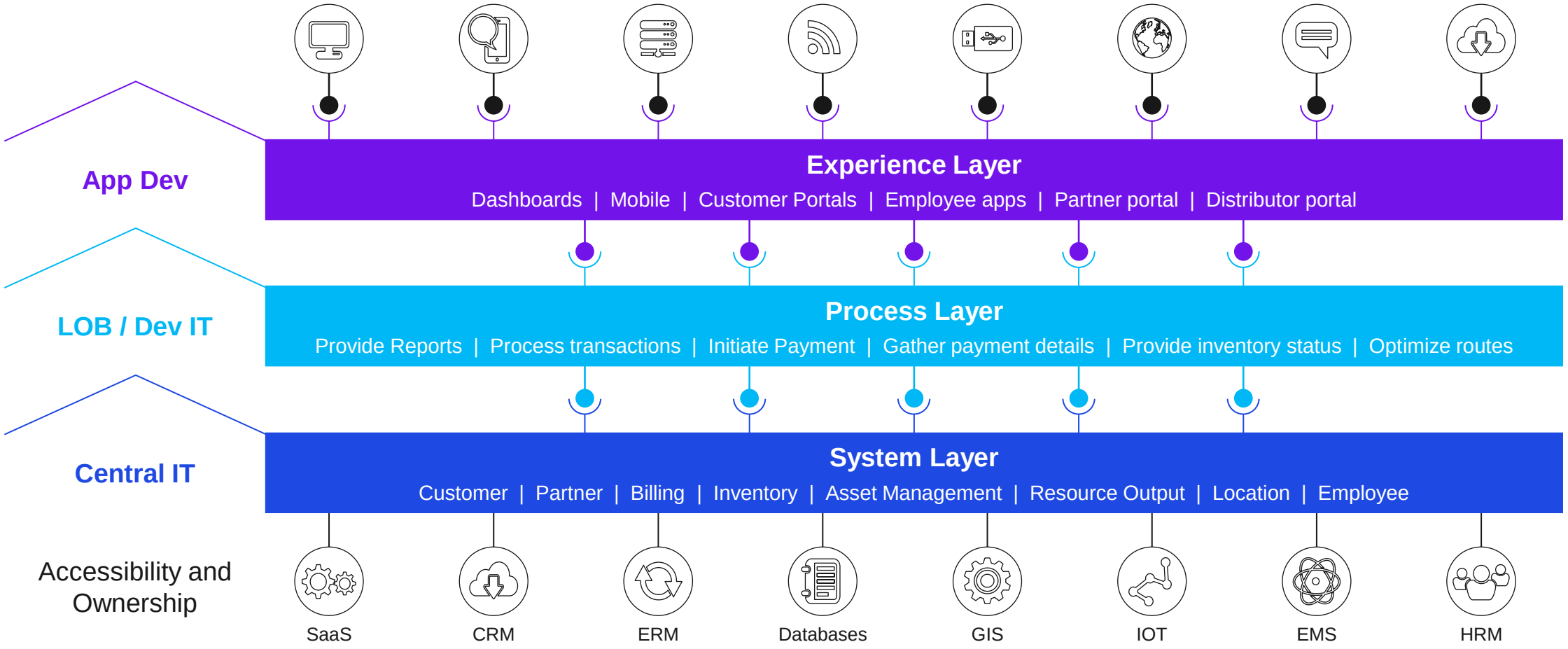
We divide business segments into 4 categories based on their digital maturity

- **TRADITIONALS:** Companies that are not yet transforming
- **CONVERTED:** Companies that will still need 3-5 years till transformed
- **DIGITALS:** Companies already advanced in their transformation
- **NATIVES:** Companies born in the digital era

KPMG

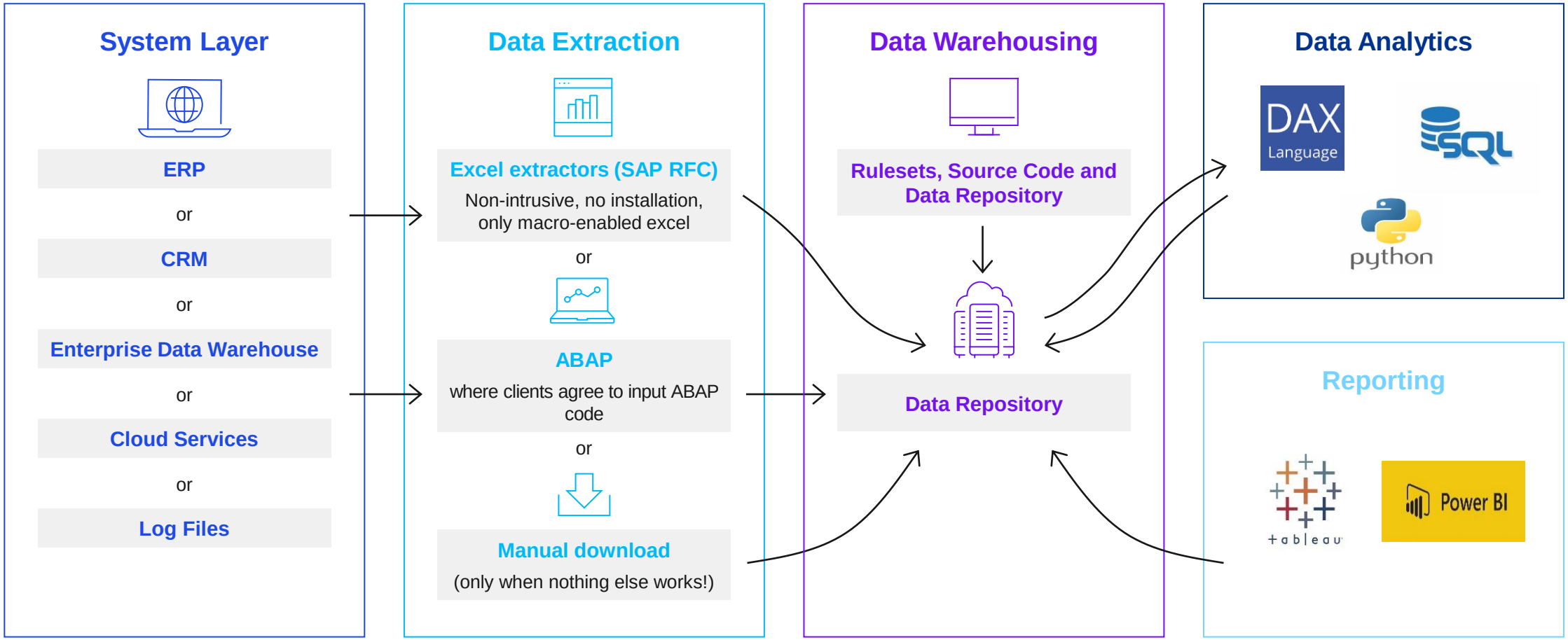
© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Information Technology 1ø1



© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Data Analytics Infrastructure

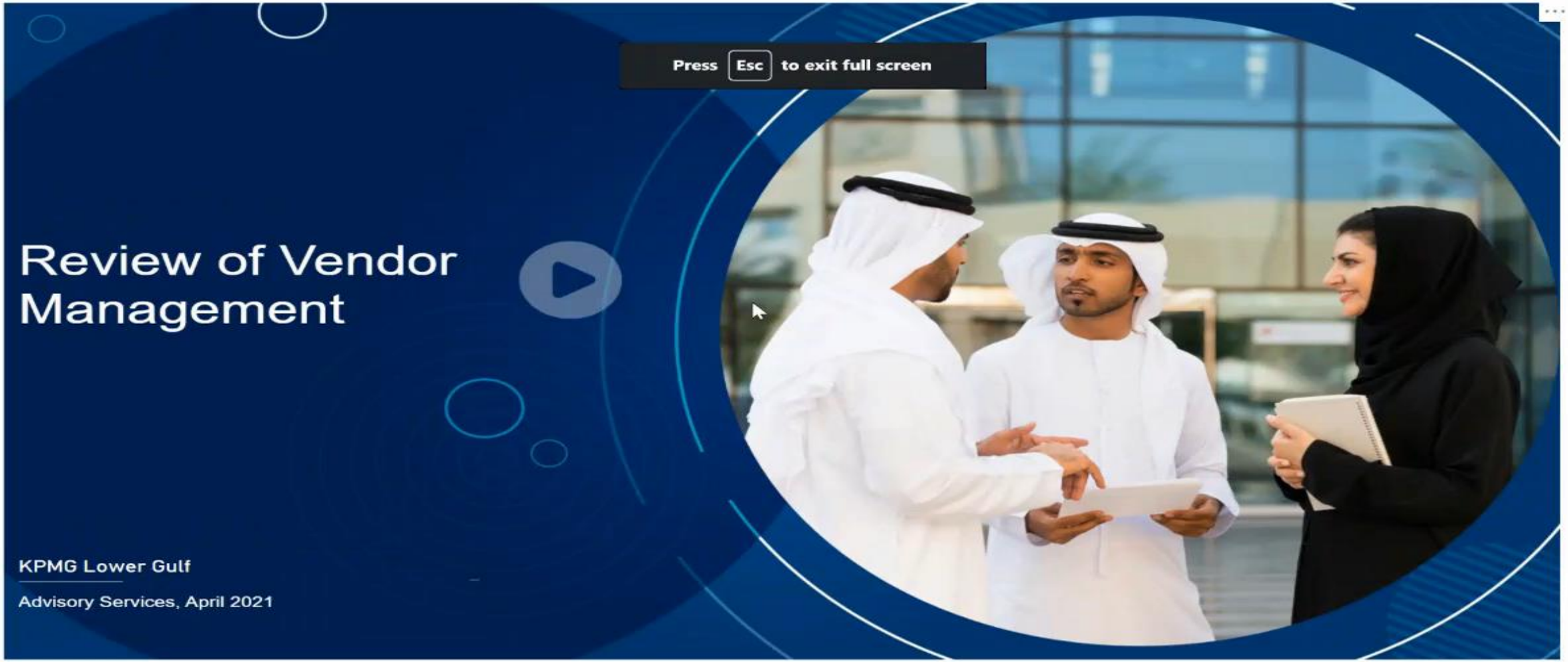


© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Use Case – Automation of IA Tests

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Use Case – Reporting

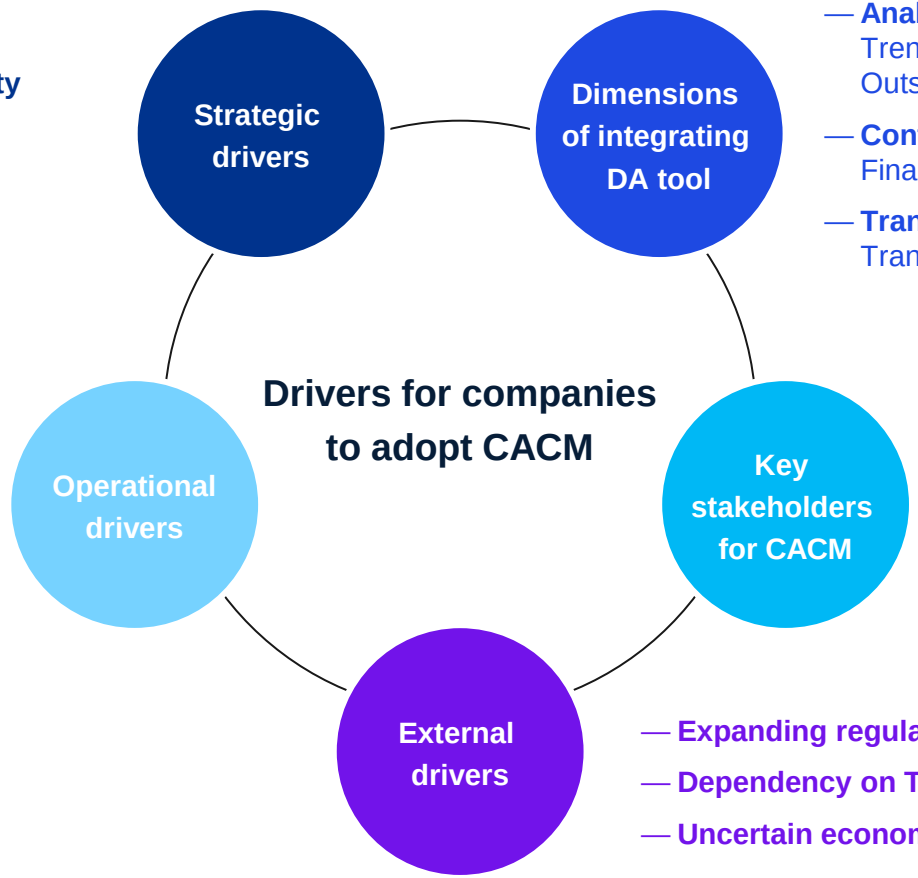


© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Continuous Auditing & Continuous Monitoring

- **Need to improve performance / accountability**
- **Need to enhance transparency**
- **Improve Risk Management e.g. ERM**

- **Occurrence of risk, fraud, waste or abuse**
- **Reduction of cost or waste**
- **Budget reductions**
- **Improve leverage of IT Investments**



- **Analytical Dimension**
  Trends, patterns, results (e.g. Days Payable Outstanding, etc.)
- **Controls Dimension**
  Financial Controls Management, Segregation of Duties
- **Transaction Dimension**
  Transaction based exception analysis

- **Chief Financial Officer**
- **Chief Information Officer**
- **Chief Compliance Officer**
- **Head of Departments**
- **Internal Audit Director**

- **Expanding regulatory and risk environment**
- **Dependency on Third Party Contractors**
- **Uncertain economic environment e.g. Covid-19 Pandemic**

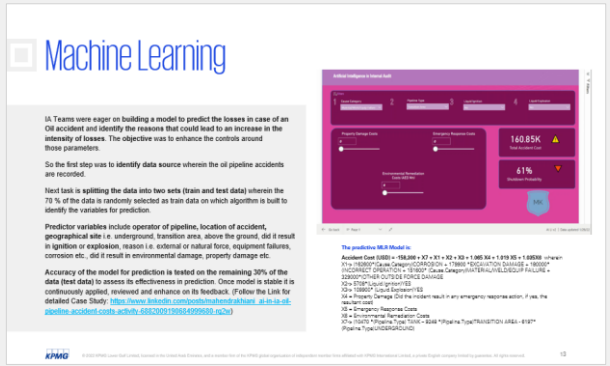
KPMG

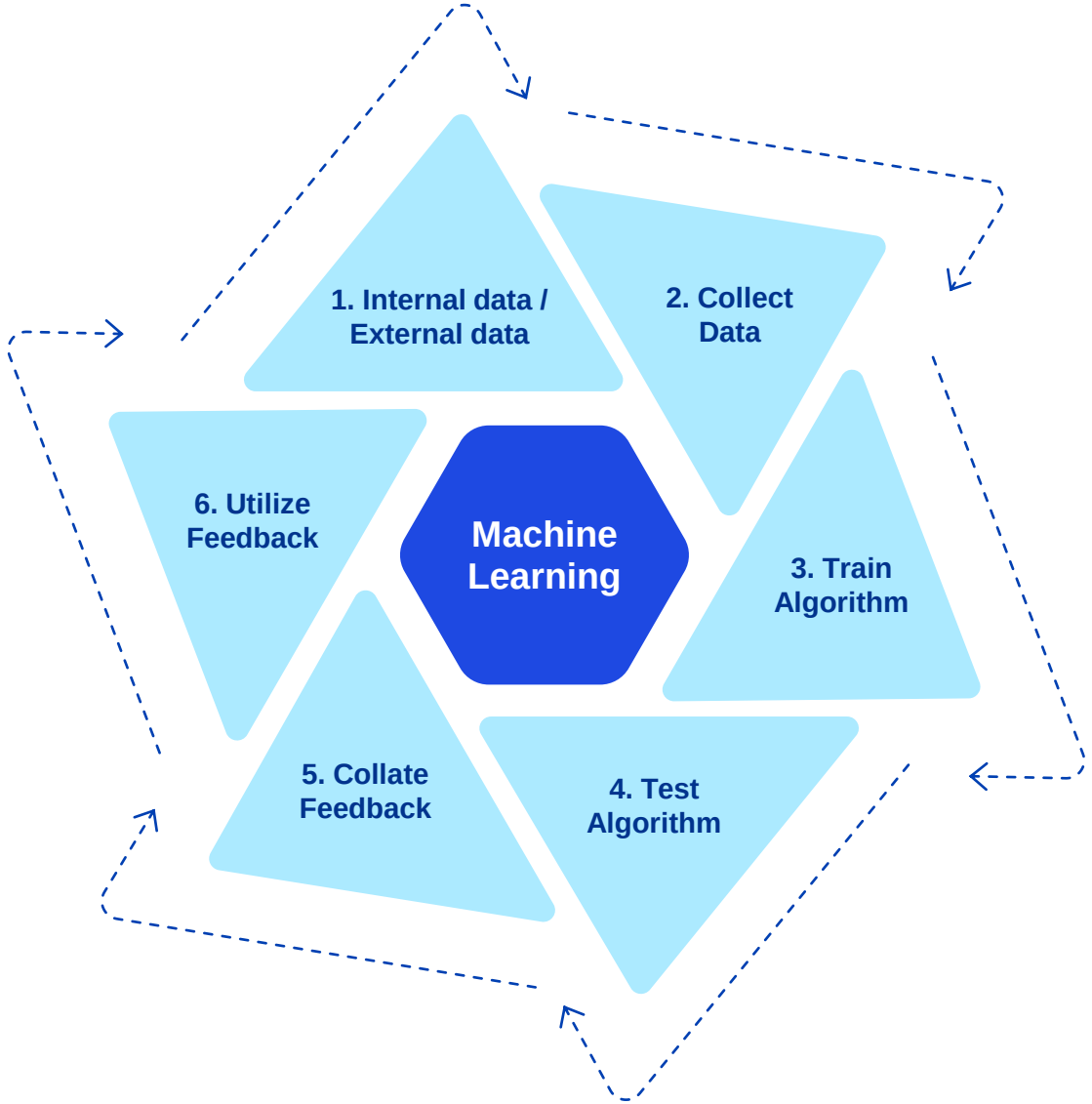
© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Machine Learning

Machine learning is a sub-section of artificial intelligence

It is **iterative in nature**; machines develop **responses to data**, which are then fed back into the system, allowing the machine to provide increasingly sophisticated responses.



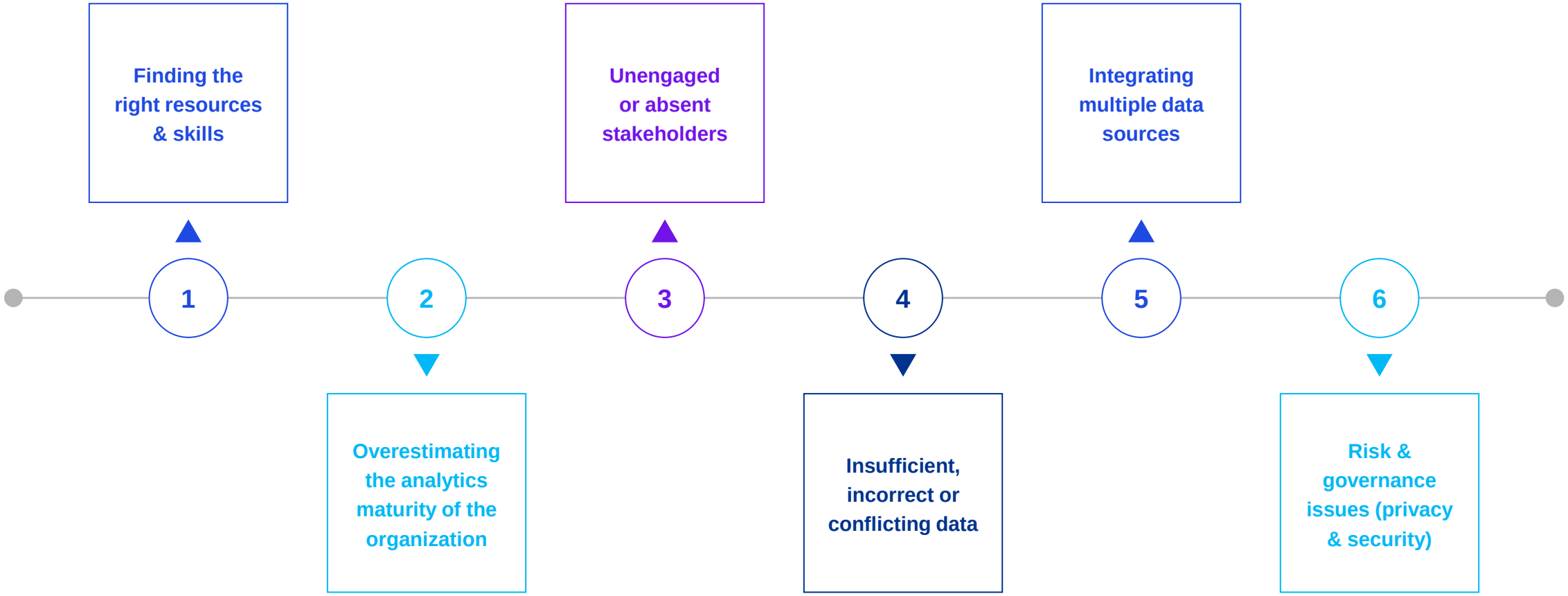


© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Why are IA functions lagging behind implementing Data Analytics?

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Implementation challenges of Data Analytics



© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Q&A

Firas Haddad

Partner | Advisory Services

KPMG Lower Gulf Limited
E: fhaddad@kpmg.com

Mahendra Khiani

Associate Director | Advisory Services

KPMG Lower Gulf Limited
E: mkhiani@kpmg.com

www.kpmg.com/ae
www.kpmg.com/om

Follow us on:

@kpmg_lowergulf

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Machine Learning

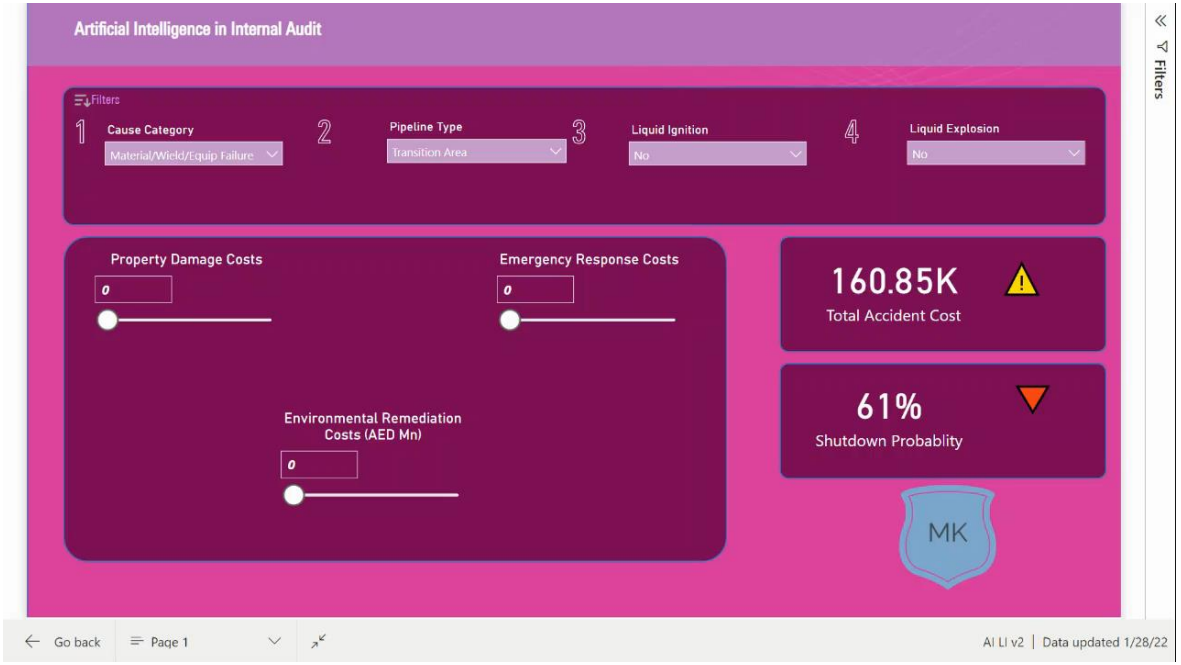
IA Teams were eager on **building a model to predict the losses in case of an Oil accident** and **identify the reasons that could lead to an increase in the intensity of losses**. The **objective** was to enhance the controls around those parameters.

So the first step was to **identify data source** wherein the oil pipeline accidents are recorded.

Next task is **splitting the data into two sets (train and test data)** wherein the 70 % of the data is randomly selected as train data on which algorithm is built to identify the variables for prediction.

Predictor variables include **operator of pipeline, location of accident, geographical site** i.e. underground, transition area, above the ground, did it result in **ignition** or **explosion**, reason i.e. external or natural force, equipment failures, corrosion etc., did it result in environmental damage, property damage etc.

Accuracy of the model for prediction is tested on the remaining 30% of the data (test data) to assess its effectiveness in prediction. Once model is stable it is continuously applied, reviewed and enhance on its feedback. (Follow the Link for detailed Case Study: https://www.linkedin.com/posts/mahendrakhiani_ai-in-ia-oil-pipeline-accident-costs-activity-6882009190684999680-rg2w)



The predictive MLR Model is:

Accident Cost (USD) = -158,300 + X7 + X1 + X2 + X3 + 1.065 X4 + 1.019 X5 + 1.035X6 wherein
X1-> (162600*(Cause.Category)CORROSION + 179900 *EXCAVATION DAMAGE + 180000* (INCORRECT OPERATION + 151600* (Cause.Category)MATERIAL/WELD/EQUIP FAILURE + 329000*(OTHER OUTSIDE FORCE DAMAGE
X2-> 5708*(Liquid.Ignition)YES
X3-> 109900* (Liquid.Explosion)YES
X4 = Property Damage (Did the incident result in any emergency response action, if yes, the resultant cost)
X5 = Emergency Response Costs
X6 = Environmental Remediation Costs
X7-> (10470 *(Pipeline.Type) TANK – 9248 *(Pipeline.Type)TRANSITION AREA - 6197* (Pipeline.Type)UNDERGROUND)

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Your expectations!!

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG

UAE Internal Auditors Association
JOIN, LEARN & SHARE

ARAC

Cracking the code: Digital risk

7 March 2022

KPMG Lower Gulf Limited

With you today

Abhisek Bhattacharyya

Partner | KPMG

abhattacharyya1@kpmg.com

Dimitrios Petropoulos

Partner | KPMG

dpetropoulos1@kpmg.com

Suleiman Gammoh

Associate Director | KPMG

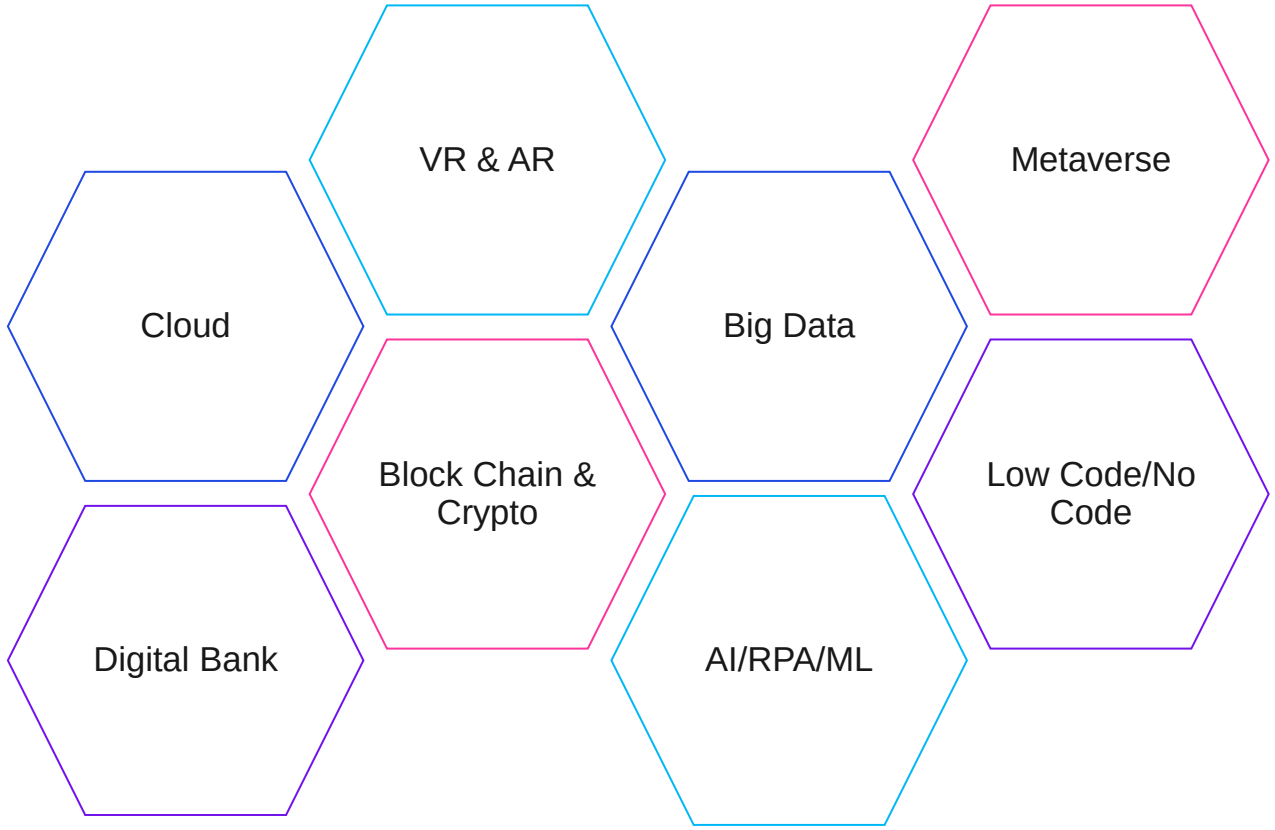
sgammoh1@kpmg.com

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Evolving technology internal audit function

The years 2020 & 2021 have been years of significant challenge and transformation as we are still living in the "COVID 19" era. While our ways of working have changed, organizations are still advancing complex transformational activities that represent new challenges to the IT Internal Auditor to stay relevant and provide value to the organization.

Digitization is increasingly becoming vital for a business's success, and companies are continuing and, in many cases, accelerating their digital journey. Whether it's increased use of robotic process automation or artificial intelligence to support optimization, further use of evolving cloud technologies, or the evolution of cyber strategy to combat emerging threats, business leaders responsible for governance need deep technology audits to manage those risks.



© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

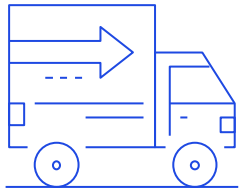
Attacks on organizations are changing

Direct

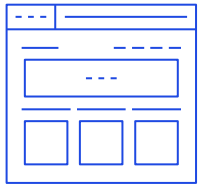
- System Vulnerabilities
- Abuse of Cloud Services
- DOS Attacks
- Data Loss
- Communication with CSP's
- Shared Technology Issues
- Data Breaches
- Poor IP Protection
- Malware Injection
- Malicious Insider Threats
- Insecure API's
- Inadequate Identity and Access Management
- Insufficient Due Diligence
- APT's

End points risks

Indirect



Supply chain attacks



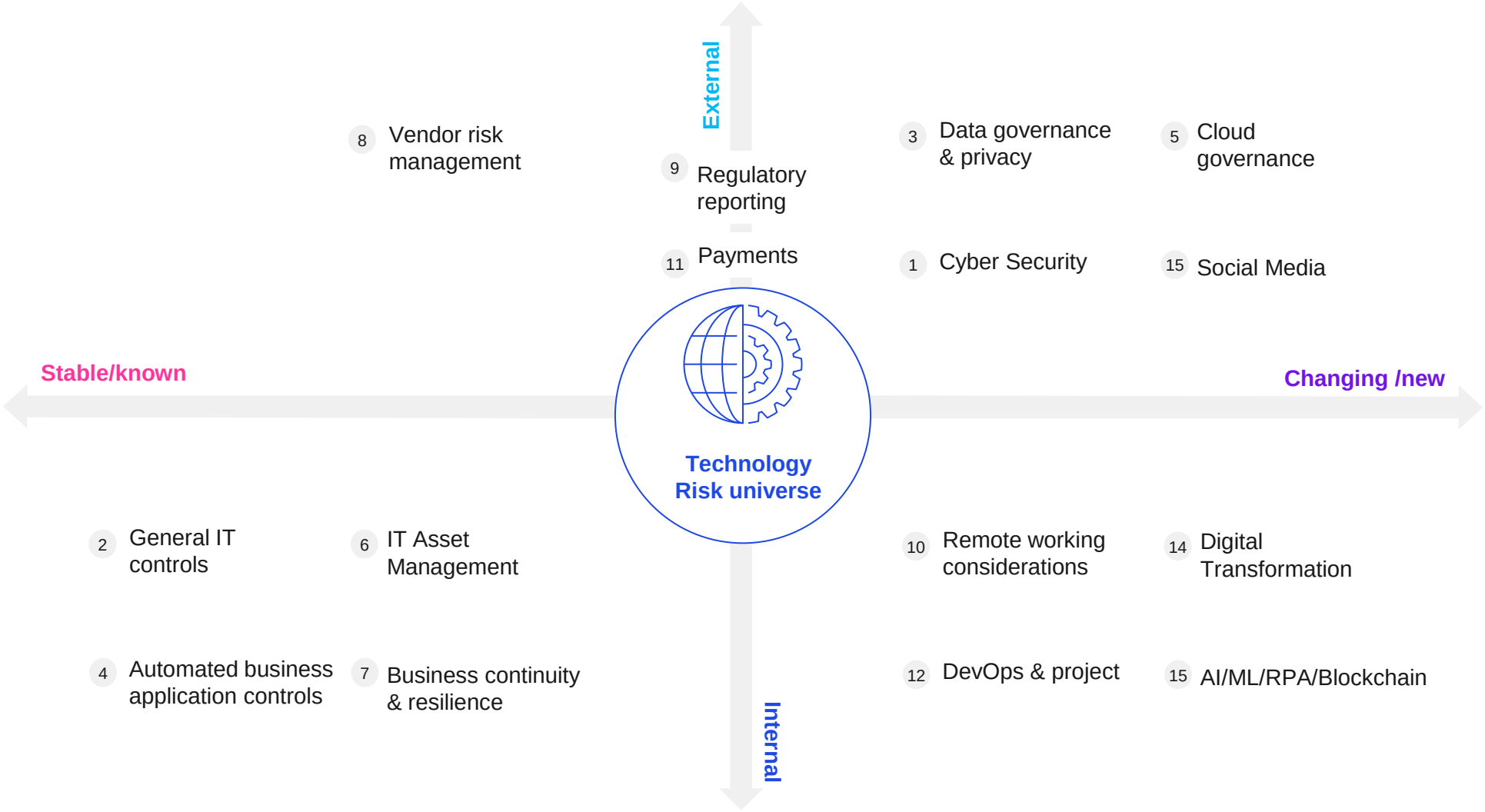
Third party software

Third party risks

KPMG

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Technology risk universe



© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Cyber Security

Emerging Risks
Recent cyber attacks in the public domain such as SolarWinds and Qualys demonstrated supply chains provide an increasingly interconnected attack surface. This has renewed the focus on how firms are accounting for supply chain attacks as a part of their threat modeling, especially related to third parties and the cyber supply chain.

IA should consider the following in the scope of their review activities:

- **Identity access management** – Assess the organization's controls related to authentication, privileged access, and monitoring of privileged accounts.
- **Network configuration and system hardening** – Assess the organization's process for securely configured network components, patching and monitoring these components.
- **Insider threat** – Understand and assess the malicious threat risk coming from inside the organization.
- **IT vendor cyber resiliency** – Assess and understand the cyber resiliency of critical IT vendors by focusing on vendors' capacity to mitigate against large-scale disruptive events, cyber resiliency preparedness, recovery capability and capacity, oversight of subcontractors, vendor recovery point objective (RPO) and recovery time objective (RTO), data confidentiality agreements, oversight of fourth parties, IT, and cyber insurance.

Cloud

Emerging Risks
A dynamic factor driving hybrid cloud application deployments is the increased use of application containers, which provide a level of portability for deploying across different environments. The use of containers may be unfamiliar to security teams with a whole new lexicon of security components from sidecar proxies to API gateways and service meshes.

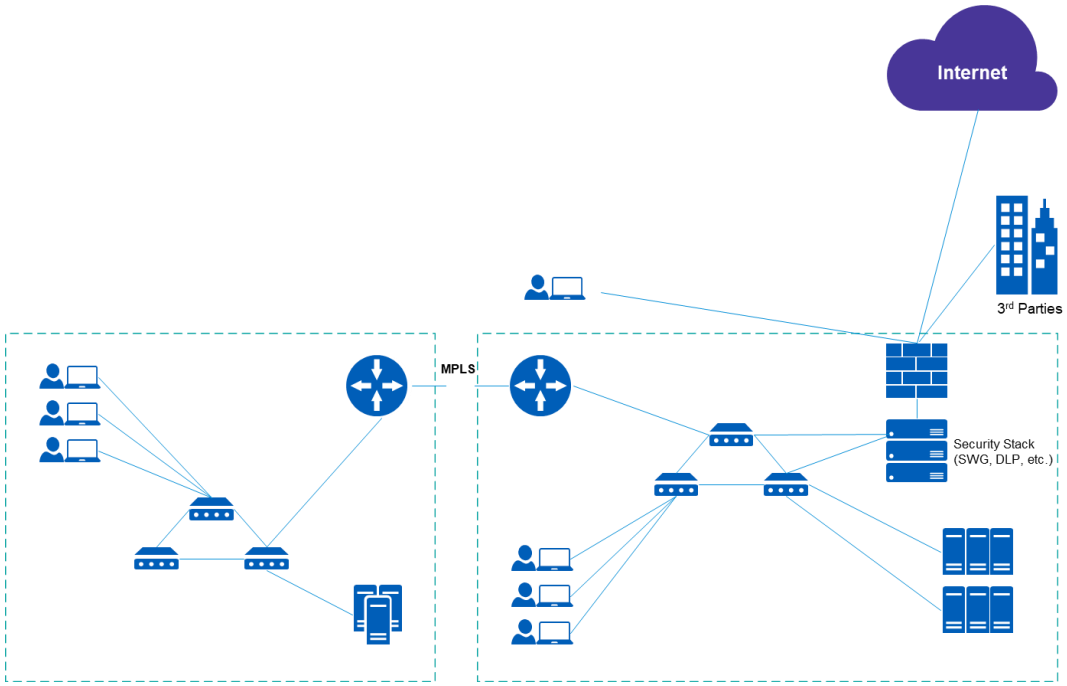
IA should consider the following in the scope of their review activities:

- **Cloud strategy and framework** – Assess the organization's cloud strategy including target operating model, governance, resources, strategic cloud architecture, cloud standards, training, and the process to assess cloud-related risks and controls.
- **Cloud adoption, onboarding, and implementation** – Assess the organization's process for identifying, adopting, and implementing cloud solutions.
- **End point protection and vulnerability management** – Assess the capabilities and controls in protecting various types of workloads such as virtual machines, containers, and serverless.
- **Security monitoring** – Assess the organization's alignment of cloud security standards to preventive and detective controls across the cloud services being used.

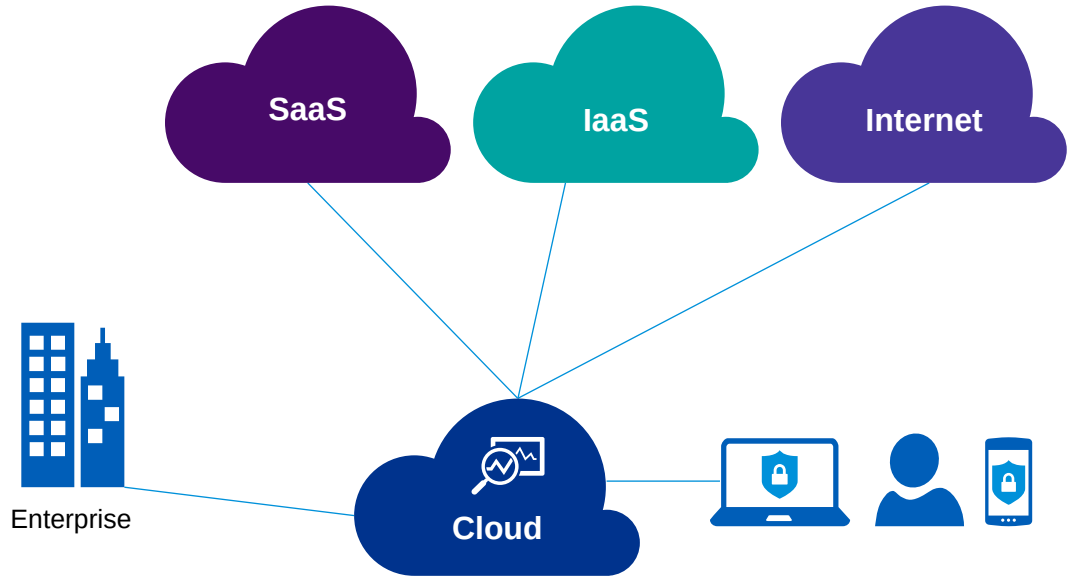
KPMG

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Yesterday



Tomorrow



© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Digital Transformation

Emerging Risks

As digitization continues to increase, it is essential to have the right data analytics tools, machine learning, and AI capabilities. Risk management teams will need to be capable and proactive in reducing design risks and detecting unintended consequences of the new digital landscape. This includes being responsive in their capabilities, methodologies, and tools to effectively audit.

IA should consider the following in the scope of their review activities:

- **Digital transformation governance** – IT Internal Audit should assess the new target operating models, strategic alignment, value delivery, IT governance, performance measurement, and resource management.
- **Pre implementation reviews** – Assess cyber-related risks and controls for new digital platforms that are being implemented.
- **Machine learning** – IT Internal Audit should review ML/ AI methodology, governance, resourcing, intentional/unintentional biases, tolerance limits, training data, change management, and access.
- **RPA/BOT** – IT Internal Audit should review BOT oversight, security design, vulnerability assessment, algo-logic review, access and change management, and roles and responsibilities.
- **No Code/ Low code** – IT Internal Audit should review sensitive data segmentation, entitlements, end point security, customization and change management on applications, no code/low code vendor platform security.

Operational Resilience

Emerging Risks

Challenges posed by third parties that impede resilience include inadequate tracking and managing of concentration risk and fourth-party risk, lack of transparency into the interdependencies between third parties across the value chain of financial products, narrowly focused or appropriate disaster recovery and business continuity planning are some of the emerging themes

IA should consider the following in the scope of their review activities:

- **Vendor risk assessment** – Understand the processes the organization executes to assess risk of vendors by focusing on risk of third parties (e.g., geography, services, and contracting), concentration risk and initial risk ranking of third parties, review of third-party questionnaires and results, and vendor due diligence results and any IT risk acceptances.
- **Assess dependencies between internal and third parties** – Assess how dependencies and interconnectedness between internal and third-party technology are mapped, analyzed, and tested to validate the feasibility of stated recovery time objectives and achieve resumption of the end-to-end business services.
- **IT asset management** – Review the organization's IT asset management process to ensure it supports data classification, privacy mandates, completeness and accuracy checks of assets relative to classifications, and underlying data classifications, and asset to service mappings.

KPMG

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Data Governance & Privacy

Emerging Risks
As firms continue to explore ways to monetize data, data security has become paramount and data governance is emerging as a critical ESG (environmental, social, and corporate governance) risk when evaluating investments in technology across the organization.

IA should consider the following in the scope of their review activities:

— **Data governance framework** – IT Internal Audit should review the overall data governance framework; policy; guidelines; interaction model; roles and responsibilities; skills and culture; metrics/KRIs/KPIs; information architecture, data lineage, metadata management, data taxonomy, and domains.

— **Data quality** – Assess authoritative data sources, business units' adoptions of data management framework, second line oversight, ongoing monitoring of data quality issues, and monitoring tools.

— **Data security** – IT Internal Audit should review firmwide privacy programs, policy and procedures, inventory and data mapping, data classification rules, and compliance to local privacy regulations.

— **Management reporting** – Review senior management and board reporting requirements, review for adequacy, representation from each of the lines of business, trending analysis, funding and technological hurdles, and second line oversight.

General Technology & System Controls

Emerging Risks
It is easy to become overly focused on new market trends and emerging technologies. While it's clearly vital to keep up with the pace of change, it's also important to remain focused on the basics. This is even more important given the evolving remote workplace where basic controls can be tossed aside, and security principles ignored or forgotten.

IA should consider the following in the scope of their review activities:

— **General Tech Controls** – Assess change management, access management, general computer operations, back up and recovery management.

— **Application & System Controls** – Continued focus on business controls in applications, interface programs, reports integrity.

— **Segregation of Duties & Access** - A very high risk and commonly discussed area and often neglected.

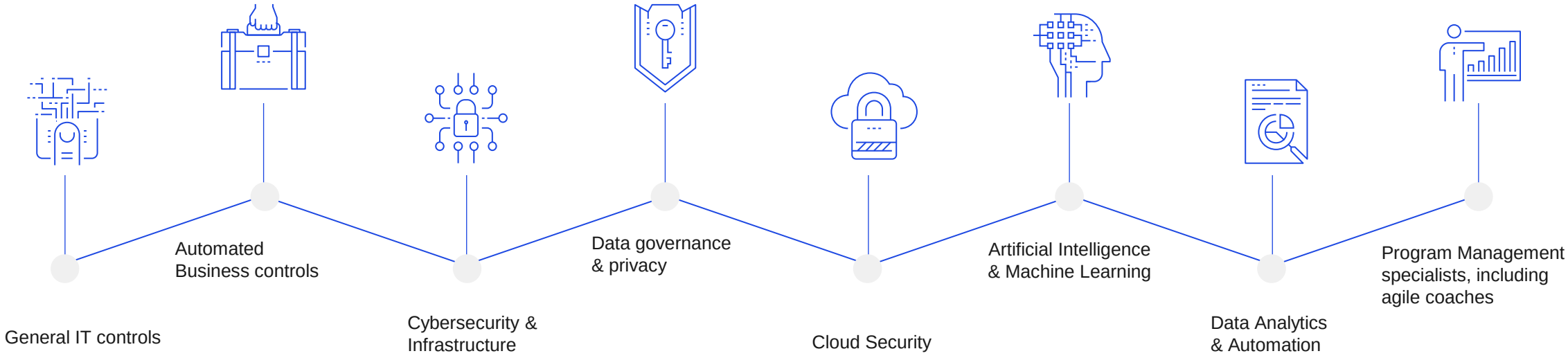
— **Automation of testing** – Technology internal audit teams need to leverage data analytics, process mining, and RPA as well as existing organizational tools to balance resource constraints and auditing high risk areas.

— **Continuous Auditing & Monitoring** - Developing & implementing advanced analytics that can be used to assess routine business transactions in systems and presenting insights in dashboards for continuous review, monitoring and remediation.

KPMG © 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Where should IT internal audit focus?

Desired Capabilities of Today's Internal Auditors



© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Challenge or opportunity ahead

IT Internal Auditors should drive opportunities out of the challenges by:

Keeping up with the transformation activities in the organization

IT Internal Auditors must stay aware of, and align themselves to, the IT transformation activities across the organization to stay relevant.

Building an IT Internal Audit team that can address new technology and emerging risks

IT Internal Audit departments should rethink the recruitment approach to keep pace with emerging technology, challenging though, given the pace of IT change.

Rethinking how they report findings and make recommendations

IT Internal Audit should make their recommendations more impactful. Internal audits are also building predictive risk sensing capabilities to help businesses understand on impending risks and report them.

Transforming how they work

IT Internal Auditors are not only providing assurance but are also increasingly acting as trusted advisers to business. IA functions continue to revamp their risk assessment and audit execution capabilities by utilizing automation.

KPMG

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Abhisek Bhattacharyya

Partner | KPMG
abhattacharyya1@kpmg.com

Dimitrios Petropoulos

Partner | KPMG
dpetropoulos1@kpmg.com

Suleiman Gammoh

Associate Director | KPMG
sgammoh1@kpmg.com

www.kpmg.com/ae
www.kpmg.com/om

Follow us on:

@kpmg_lowergulf

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.