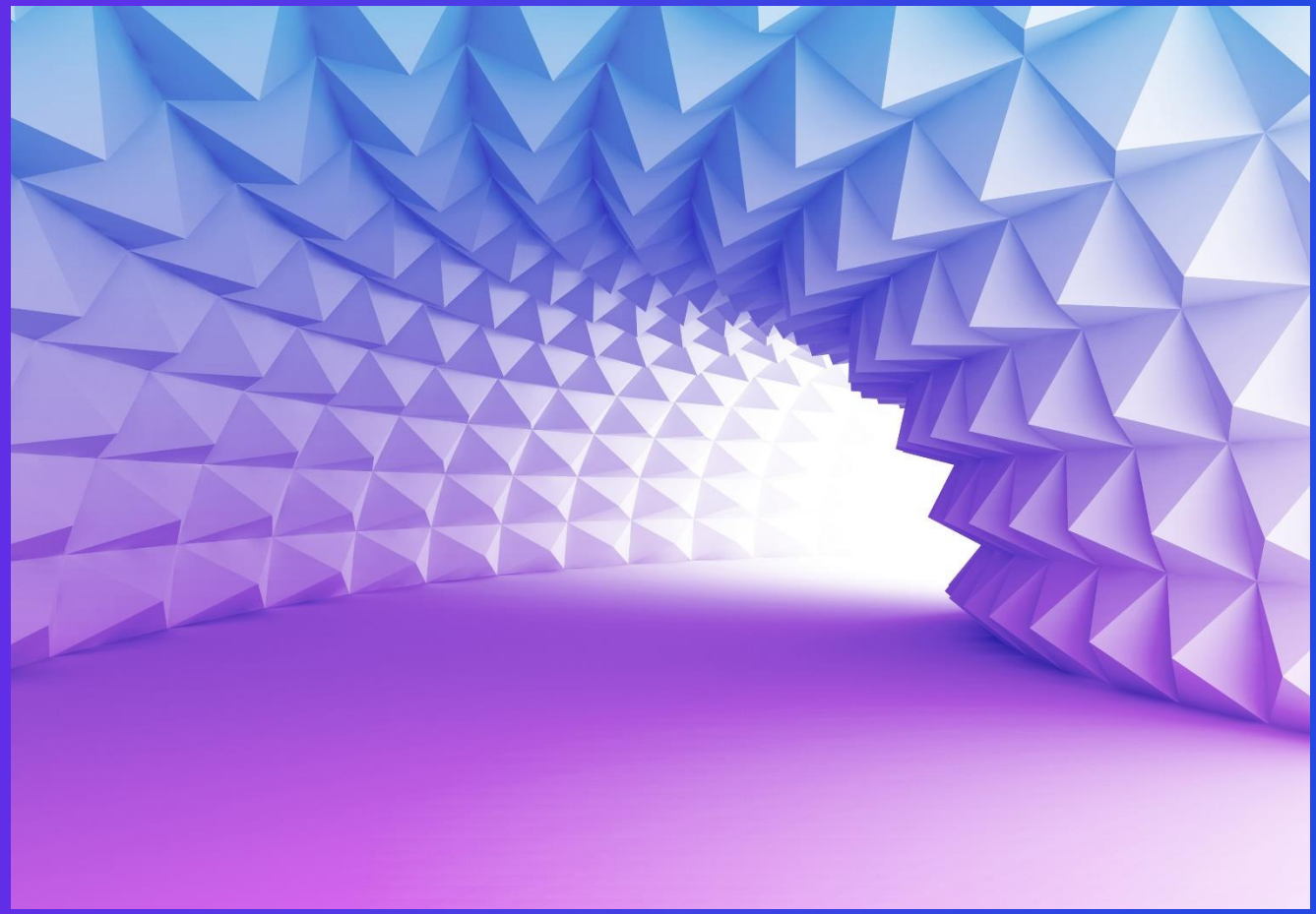
KPMG

IT Assurance Summit 2023



Tuesday 4th July 2023

IT Assurance Summit 2023: Agenda

08:45-09:50	**Registration and refreshments**
09:50-10:15	Welcome and introduction
10:15-10:30	Future of Internal Audit
10:30-11:15	Cyber resilience
11:15-12:00	Change Transformation
12:00-13:00	**Lunch and networking**
13:00-14:00	Three Lines of Defence (client panellist)
14:00-14:45	Enterprise Automation
14:45-15:30	UK controls reform
15:30–15.50	**Coffee Break**
15:50–16:50	Key Note speaker (Alliance partner – Microsoft)
16:50-17:00	Wrap up
17:00- 19:00	**Networking and Drinks**

KPMG representatives

Jamie Thompson

Partner,
UK Head of Technology Risk

Tejas Mehta

Director
Head of UK & FS
IT Internal Audit

Sharon Wiesemann

Director,
Co-Lead Sectors
IT Internal Audit

Alex Fasting

Director,
Co-Lead Sectors
IT Internal Audit

Andrew North

Director,
Head of IGH
IT Internal audit

Ian Arnold

Director,

Head of Sectors
IT Internal Audit

01

Future of Internal Audit

Katie Clinton
Partner and UK Head of Governance, Risk & Compliance Services
KPMG in the UK

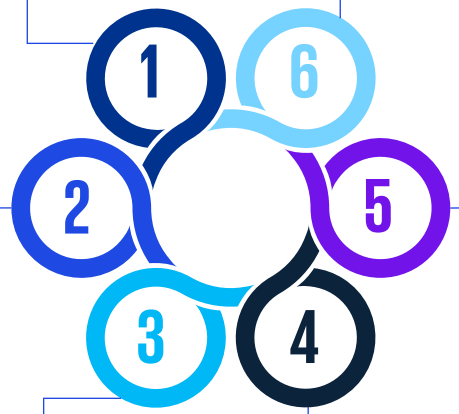
Forces shaping internal audit

Global & Regional - multiple interdependent, and dynamic, forces…

1. Political
- Economy vs COVID Crisis
- De-globalisation
- Nation 1st Policies
- Stimulus to Stabilise & Restart
- Climate & ESG
- State Aid & Ownership overhang on Markets
- Trade Agreements Disputes
- Tax
- Political Instability

2. Regulatory and Legal
- Regulatory Easement to create capacity for Lending, Investment and Losses post Crisis
- Re-calibration of Regulation
- Data Flows & Digital Competition
- Corporate Governance re-framed for State as a Shareholder

3. Economic
- Inflation & Supply vs Demand
- Central Banking & Gov't Interventions
- Developed vs Emerging Markets & speed of recovery
- Foreign direct investment (FDI) and organic investment slowdowns
- Supply Chains & Labour Shortages



6. Organisational
- Organisational Migration
- Physical organisation vs Virtual Organisation
- M&A & Alliances
- Culture & Purpose
- People & Access to Talent
- Tax and Regulatory regimes

5. Technology & Data
- Cyber
- Privacy, Digital, AI "backlash"
- Digitisation of Business and Supply Chain
- Data Transfers & Regulation
- Social behaviours fundamentally changed
- Generational shifts and schisms accentuated
- Technology Resilience
- Tech & chip Supply Chains

4. Social
- COVID recovery
- Immigration Controls
- Labour Shortages
- Consumer Consumption models and behaviours change
- Ways of Working Change & Labour Mobility
- Climate & ESG

Dealing with disruption: The CAE's strategic agenda

Leading organisations have developed an agenda to help deal with disruption across their internal audit functions

Stakeholder engagement and trust

Internal audit knows its top stakeholders and takes the time to foster a relationship of trust attuned to their needs

Digital acceleration

Leverage technology with organizational goals in mind, and use it to enable program and project level work

Data, analytics and insights

Enterprise data is available and used, and new data is curated by internal audit. This data is used to provide risk insights and enhanced assurance through broader audit coverage

Strategy and value management

Internal audit strategy considers a mix of enhanced assurance, risk insights and business improvements attuned to stakeholder needs. Strategically important and future-focused emerging risks are prioritized

New ways of working

Where services are delivered, the competencies that enable that delivery, and the way audit teams want to work has to be revisited to help retain the right talent

Operating model agility

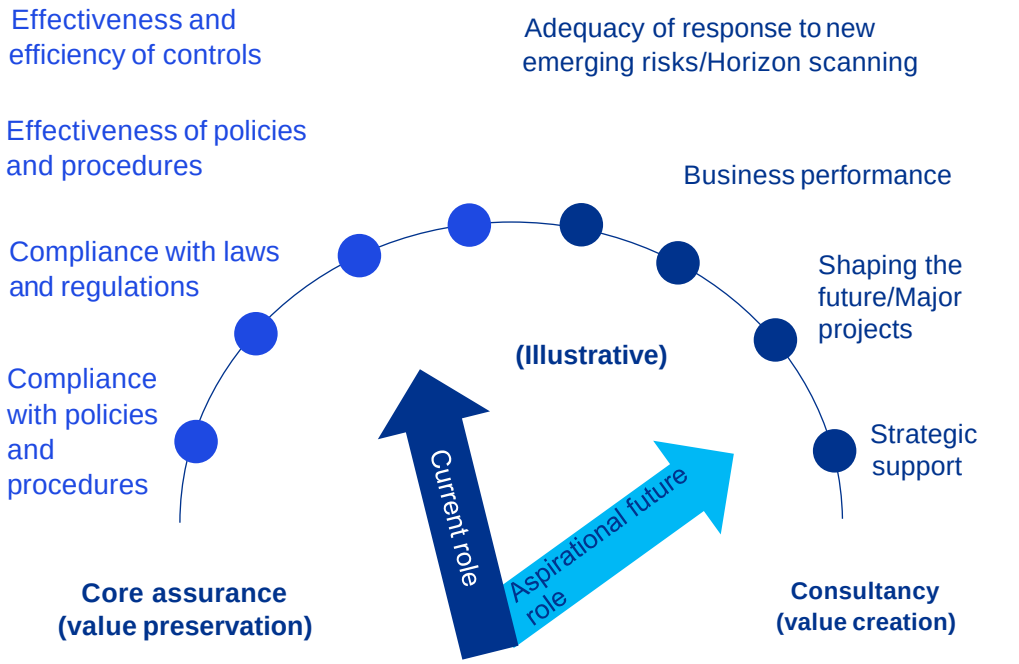
Audit activities are responsive to disruption, flex with the business strategy throughout the year, and consider coordination with other lines of defense

Positioning internal audit for success

Internal audit's core responsibility is to evaluate the effectiveness of internal control, including compliance with policies, procedures, laws and regulations. This is the baseline.

However, a progressive audit function will do more than provide the baseline – it will add value to the organisation aligned to the Vision and Purpose of the organisation; it will seek to continuously improve and it will regularly assess how the function compares to industry peers.

Potential roles for Internal Audit (illustrative)



What does good look like?

Demonstrate executive presence by linking IA to the C-Suite agenda	Act as a trusted, credible advisor to the Board/Audit Committee	Create and deliver a vision that aligns with the Society's strategic direction and stakeholders' expectations	Be the strategic and innovative voice of risk management, control and governance
Rebrand IA as a collaborative leadership function that partners with the business	Operate a function that is perceived positively as value adding by key stakeholders	Partner with the business to develop/coordinate integrated risk & assurance strategies across functions	Be the custodian of a strong control culture and challenge behaviours
Understand regulatory context and business challenges	Source, develop, mentor and retain the right talent	Proactively identify emerging risks	Demonstrate agility and relevance in a changing environment

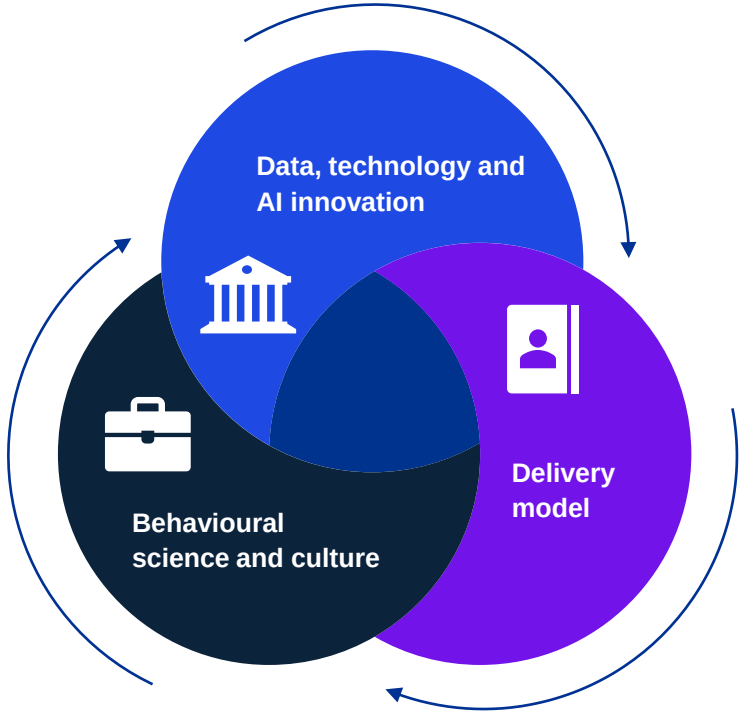
The future of Internal Audit

Data, technology and AI innovation

- Technology and generative AI led scenario reviews to forecast potential outcomes and predicting areas of risk.
- Automated continuous assurance (including the use of AI / RPA) to monitor control exceptions to identify non-conformance.
- Default use of process mining to support ongoing assessment of future control changes and audit planning.
- Capturing qualitative 'risk perspectives' from stakeholders (Executives, Regulators and External Audit) and use of tooling (e.g. Alteryx) to highlight common themes / managements perspective on focus areas.

Behavioural science and culture

- Incorporating behavioural science into GIA methodology, including consideration of Behavioural Risk and behavioural root cause.
- Horizon scanning: leveraging behavioural data science to generate unique insights and identify potential hot spots for a targeted audit.
- Targeted audits leveraging econometric approaches to assess impact of activity, product or service at scale.



Enhancement through the delivery model

- Monitoring of audit efficiency, to identify areas of potential over-auditing. E.g. use of data to identify the ratio of key/non-key controls identified and tested.
- Digitalisation / automation of repetitive tasks – data collection / documentation analysis through AI.
- AI and technology to generate first-drafts of audit reports, based on working paper data and other supplementary evidence.
- Increasing the breadth of scope for IQA to focus and report on audit efficiency.
- Continuing investment in Change professionals who can deliver real-time assurance and challenge over large transformation programmes.
- Increased off-shoring / outsourcing of low-risk, repetitive activities, to increase flexibility and agility of resource model.

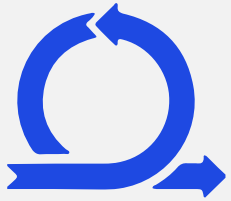
02

Building Cyber resilience and the 3LoD - Challenges & Strategic Priorities

Indy Dhami
Partner, FS Cyber
KPMG in the UK

What is cyber resilience ?

Withstand



Recover

Adapt

Challenges organisations face

Disparate views & ownership

Lack of visibility

Growing vulnerabilities

Increasing regulations

Sophisticated attackers

What are the mature organisations doing?

- Strategic Alignment
- Clarity of Risk
- Stress Test
- Agile Metrics
- Estate Visibility
- External Visibility
- Continuous Testing
- Quantifying Risk
- Regulatory Focus
- Build Relationships

Enhancing cyber resilience in 3LoD – key takeaways

1st Line – Cyber teams

Data

Education

Agility

2nd Line – Risk Managers

Team

Define

Report

3rd Line – Internal Audit

Expertise

Improve

Take me away

Cyber security is no longer enough: businesses need cyber resilience

To do this, businesses must defend against attacks and recover quickly after a major disruption by leveraging data and expertise

Cyber resilience can be an enabler of business outcomes – only if it is governed by top leadership and embedded in the business operating model

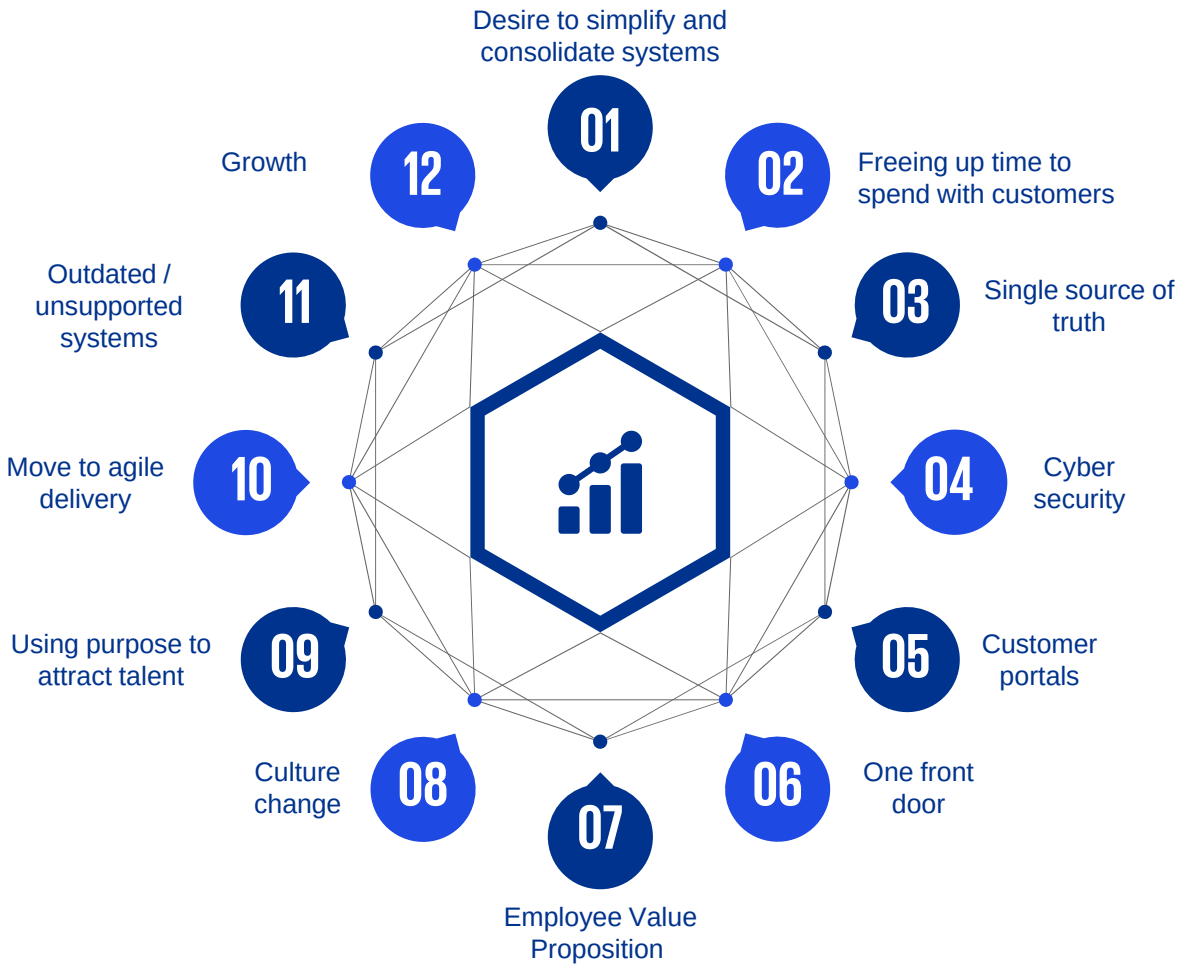
03

Transformational Change

Alison Dent
Director of Program Assurance
KPMG in the UK

Andy North
Director, Head of IGH IT Internal Audit
KPMG in the UK

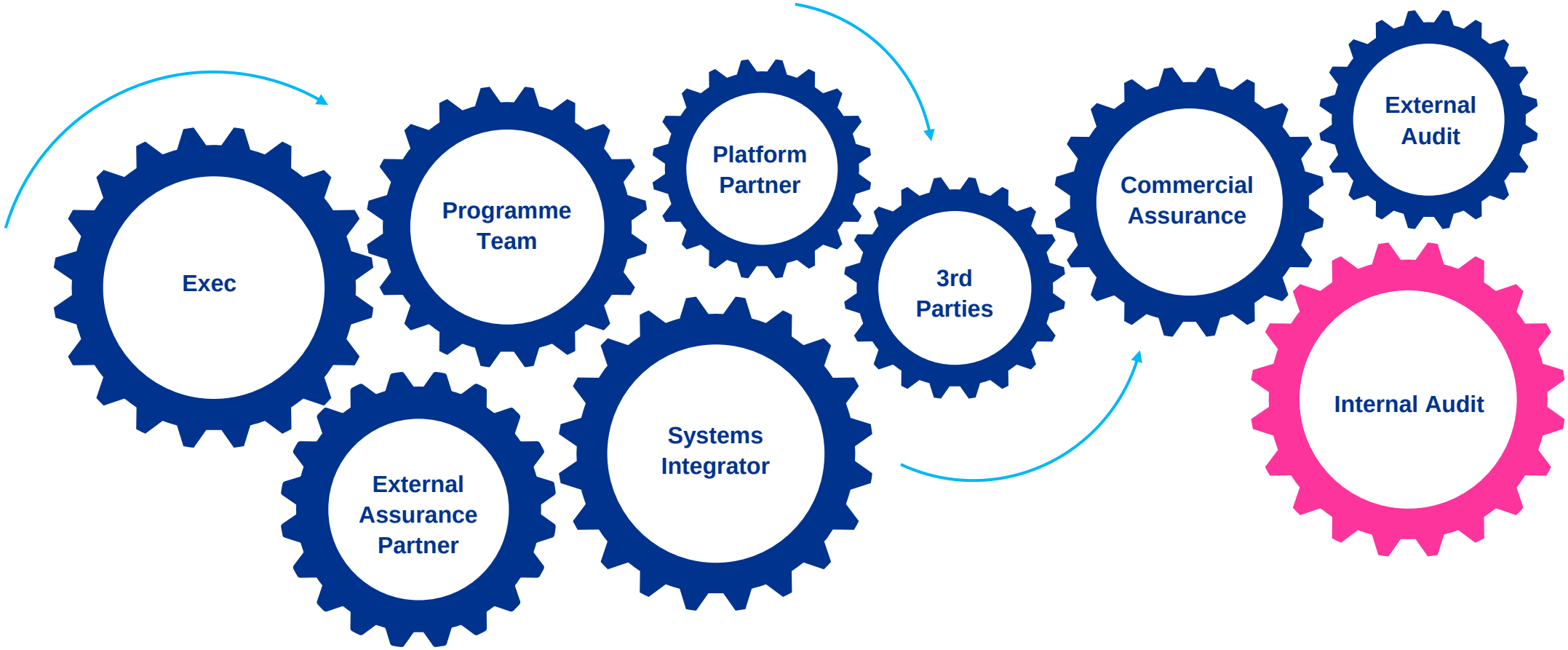
Organisational drivers of change



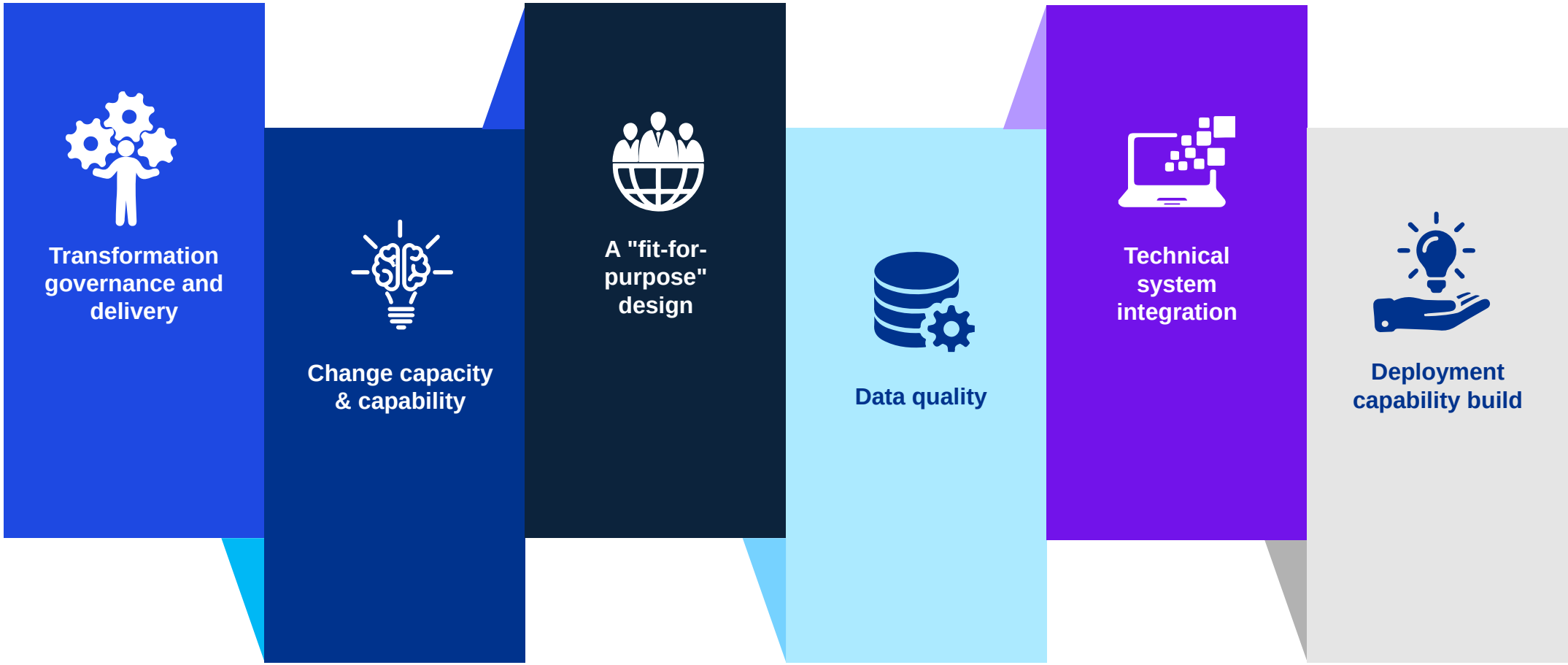
Question 01

what is driving your change agenda and

Delivering change successfully needs support from a range of risk and assurance partners



Key risks we typically see in transformation programmes



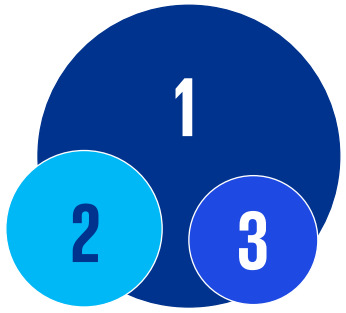
Question 02

Where are you getting most of your assurance from?

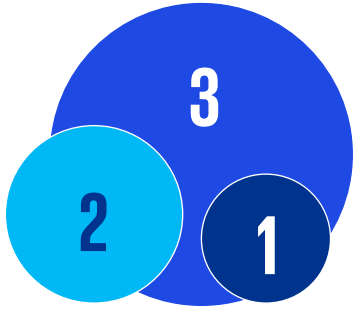
Assuring change across the 3LoD

Line of defence	What	Challenges
Delivery team Programme Management Office (PMO) 1	Strong **Business Case / Mandate** Design and implement effective **Governance** Strong **RAID** (Risk, Assumptions, Issues, Dependencies) management Maintain strong **open culture, reporting and escalation**	**Business case not robust** **Tendency to green** reporting Staff **motivation** vs issue recognition **Change inertia** **RAID is an afterthought**
Internal change risk assurance function Third party assurer 2	**Regular challenge** / deep dive assurance on critical areas. **Learn lessons** from other programmes Ensure specific change **risks are understood** Ensure suitable level of **assurance to protect the Board** Ensure **effective RAID** process	Limited **resources and capability** **Focus** on business case / go-live **Access** to suppliers
Internal Audit Regulator 3	Focus on ensuring **1st / 2nd LOD are effective** **Targeted reviews** in high risk areas as directed by Audit Committee **Thematic coverage** e.g. testing, security, IAAPs **Focus on Governance** - Risks understood and addressed?	Provision of **over assurance** vs coverage i.e. beyond governance Needs **digital change and IA skills**

Resources available across 3LoD …



Assurance expectations …



Having a robust framework to assess risk is key…

Our digital GETT Framework…

Global Enterprise Transformation Tool						
Governance	Programme management	Change	Performance	People	Process	Technology
Strategic Alignment	Scope & Change control management	Change Approach & Strategy	Business cases	People Strategy & Approach	Target Operating model	Enterprise Architecture
Leadership	Plan Resource & Programme	Case for change	KPIs metrics	Organisations Design	Process Design	System Design
Delivery Principles & policies	Risks, Assumptions, Issues & Dependencies	Change Leadership	Benefits Planning & Management	Culture and Behaviours	Requirements management	System & Infrastructure Build
Accountability & Responsibility	Cost Management	Change Capacity & Capability	Incentives to Deliver	Skills & Competencies	Data Management	Data Conversion& Migration
Structure &capability	Vendor Management	Stakeholder Engagement & Comms	Performance Improvement	Role and Job Design	Process Controls	Interfaces & Legacy Systems
Monitoring & controls	Quality Standards & Management	Change Impact Assessment	Independent Assurance	Training & Development	Functional Testing	Non-functional Testing
Portfolio Management	Lifecycle & Release management	Business Readiness	High Performing Culture	People Performance Management	Compliance Security	Transition & Support

Take a look at our framework during the breaks!

Take me away

Understand the drivers of your change transformation – we should be assuring the delivery of business outcomes, not just milestones and spend.

Be clear about what assurance you're not providing given limitations in your scope and technical capabilities

Never trust a green report!

04

Client Panel Discussion

Client panel discussion

Jon Measures

Partner, Facilitator for the session
KPMG in the UK

Nayab Kohli

Partner, IT External
KPMG in the UK

Paul Howard

Technology Audit Director
Lloyds Banking Group

Lele Ly

Head of Cybersecurity Governance, Risk and Compliance at UK Civil Service

Denis Ontiveros

Director of security platforms BP

05

Enterprise Automation

Richard Walters
Risk Analytics Manager
KPMG in the UK

Enterprise Automation Maturity

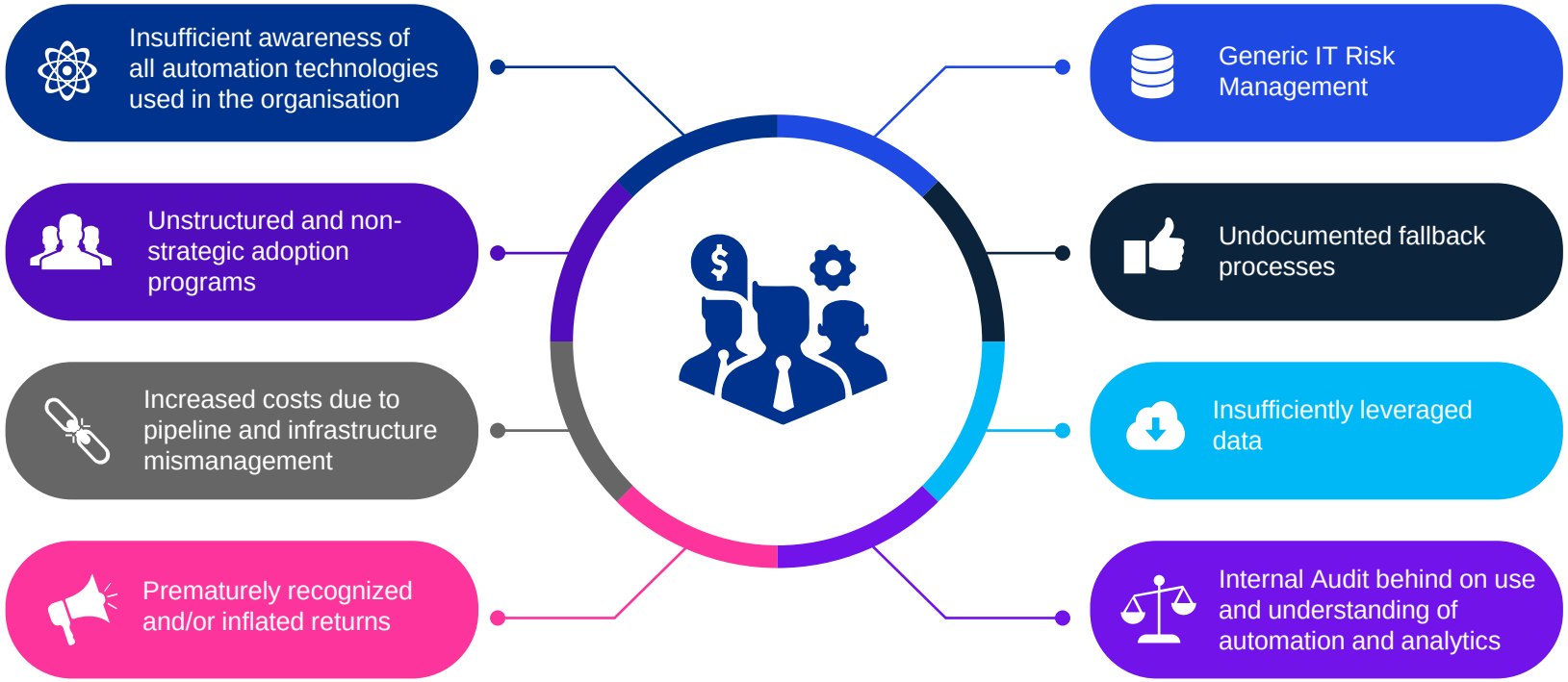
Maturity Levels

1	2	3	4	5
Ad Hoc	Developing	Defined	Optimized	Leading

Dimensions

- Strategy and Governance
- Automation Delivery
- People / Change Management
- COE Operating Model
- Continuous Improvement
- Technology Management
- Value Management

Analytics, Automation and Internal Audit: Challenges



Roles of the 3 Lines of Defence in Automation

1st Line of Defence

- Log every activity
- Automate processes
- Rethink processes - easily auditable by design

2nd Line of Defence

- Strive for full population oversight
- Define automation risk appetites
- Maintain the risk register

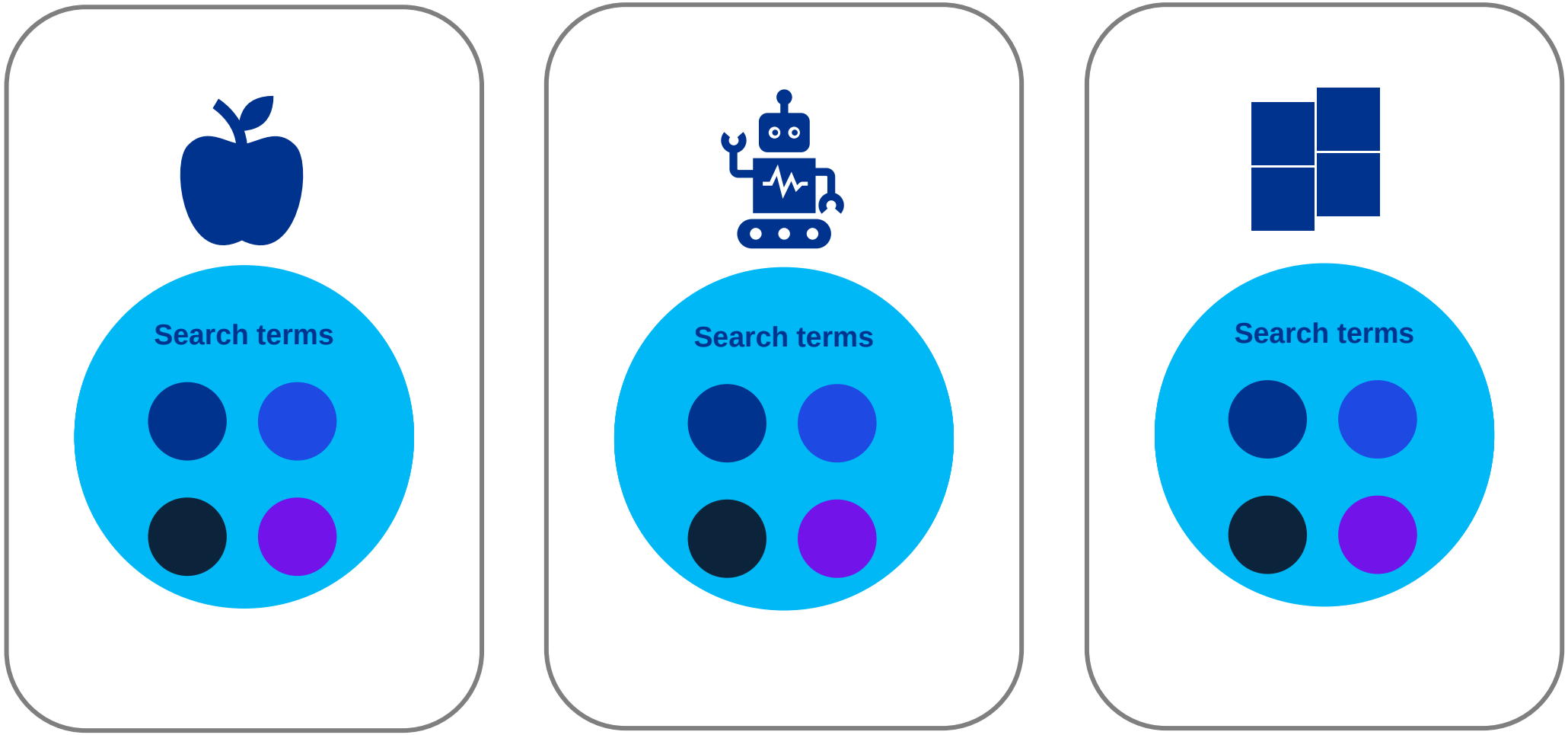
3rd Line of Defence

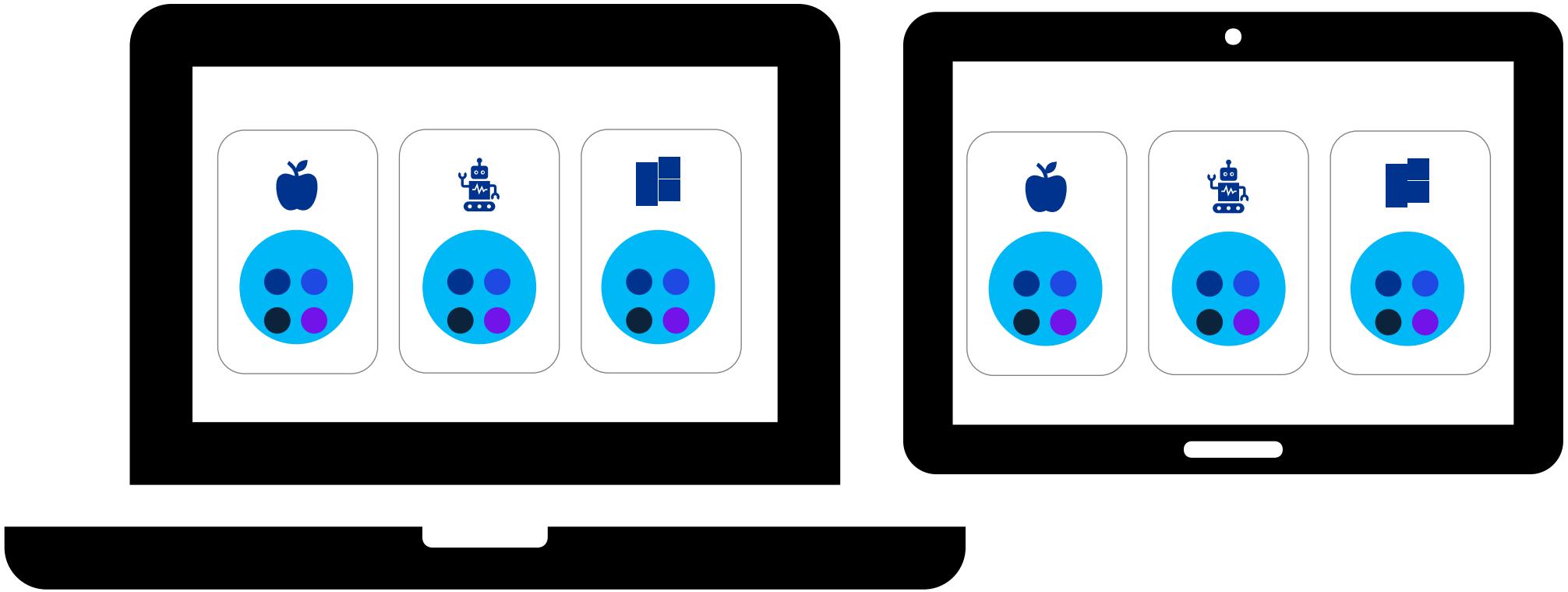
- Set the tone and expectations
- Expect process automation
- Expect data quality and aggregation
- Monitor regulatory environment

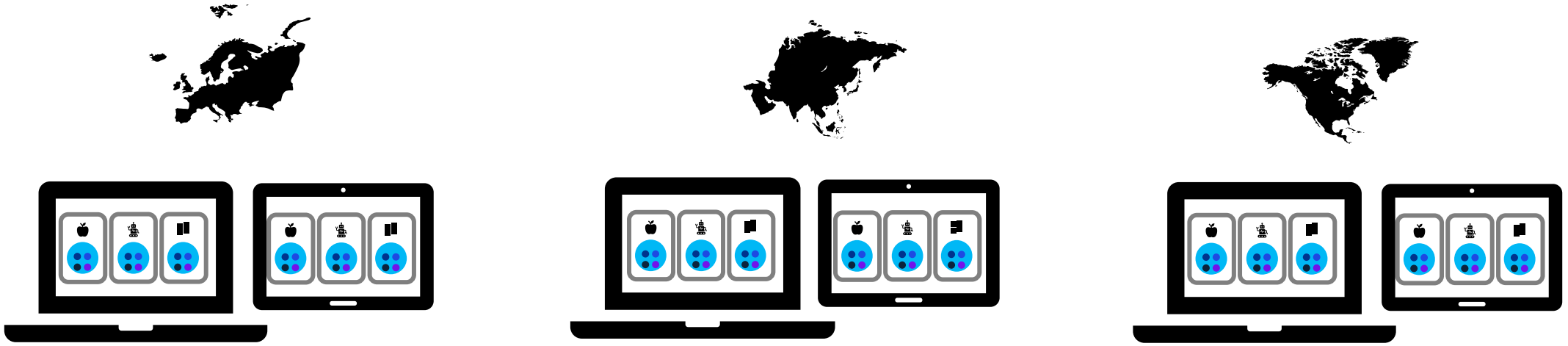
Case study

Client Ask:

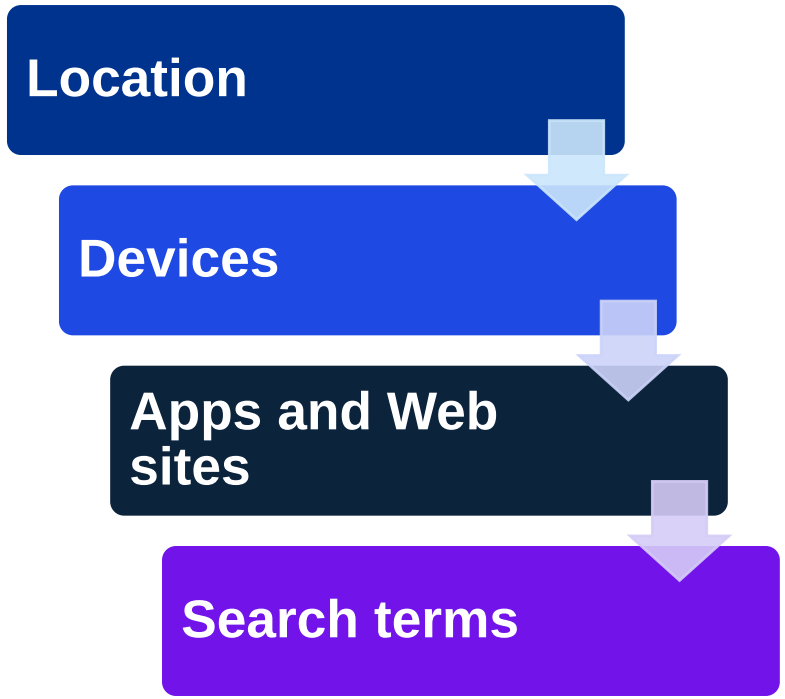
Requirement to comply with **Consumer law** concerning **accuracy and transparency of communication** on product availability and pricing across full suite of online access points (platform × OS × countries)







Understanding complexity



Tech stack	VPN for location simulation
	Device simulators
	Application and browser simulators
	Machine Learning

Take me away

Discover your organisation’s analytical capability and how associated risks are managed.

Develop a detailed RACI matrix across the 3 lines of defence for analytics and automation.

Evolve internal audit plans and approaches to include considerations in pursuit of continuous digital transformation.

06

UK Controls Reform

Sarah Ward
Partner, Risk Assurance
KPMG in the UK

Agenda

01 Reforms overview

- What's new
- Timeline

02 Technology Risk Focus Areas

- Key Technology Risk Drivers
- Impact on the IT Organisation

03 Audit and Assurance Policy

- What is changing here?

Audit and Corporate Governance Reforms Overview

01 Internal Controls Statement

- **Active evaluation** of internal controls effectiveness **publicly reported**
- **Material controls** over **reporting** and **operational and compliance** risk
- Disclosure of **Material Weaknesses**
- First **'through the year'** opinion to reporting date

02 Audit & Assurance Policy

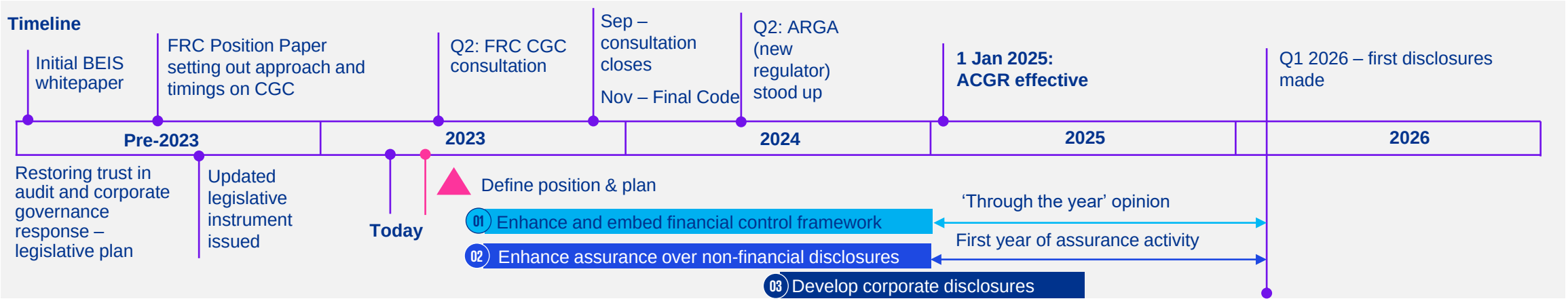
- **Assurance plans** on a three year rolling basis
- **Statutory and voluntary disclosures** in the Annual Report & Accounts (ARA)
- **Summary publicly disclosed** within the ARA
- First disclosures for year ended **31 December 2025**

03 Corporate Disclosures

- **Explicit statement** on **resilience** as part of the Strategic Report
- Disclosure on UK parent company **capital maintenance** and **distributable reserves**
- **Enhanced reporting** around **fraud**
- First disclosures in the ARA for year ended 31 December 2025

Comply or explain requirement through CGC (applicable to listed companies from 1 Jan 2025)

Mandatory requirement through legislative change to UK Companies. Effective for listed companies 1 Jan 2025 and large PIES 1 Jan 2026.



The AAP

Key: 1.5 or 2 LOD External assurance Internal audit

The scope of the AAP is “the Annual Report and Accounts” annually. Key requirements are shown below.

AAP requirements		
An explanation of the company’s **plans** for obtaining **internal audit and assurance** over **financial and non-financial disclosures** reported over the next 3 years;	A **statement** of whether, and if so how, the company is **proposing to strengthen its internal audit and assurance capabilities** over the next 3 years	An explanation of how s**hareholder views have been taken into account** including the views of employees and any other stakeholders
A description of an **organisation’s operation** and **governance** over its **internal auditing and assurance**	The **planned independent assurance**, if any, the company intends to obtain over the next 3 years in addition to the statutory audited accounts	An explanation of the **policies around the tendering of external auditors**
An explanation of how **any management conclusions and judgements,** which are disclosed in the annual report and accounts, may be challenged and verified within the company	Specific information on whether, and if so, how, the **company will obtain independence assurance** over: • the company’s **resilience statement**; • the **effectiveness of the company’s internal controls over financial reporting**	If the organisation has **procured independent assurance**, the clarification of whether it is “limited or reasonable” and the professional standards which applies

Technology Risk – What it means for 3LOD

1LOD

1. Controls evidencing (GITC and application controls)
2. Alignment with in scope programmes
3. Remediation
4. 1.5 line assurance
5. Wider assurance mapping

2LOD

1. Assurance strategy
2. QA over assurance
3. Policies and procedures

3LOD

1. Three year forward view on IT assurance plans?
2. Explanation of methodology
3. Increased focus on disclosure?

Take me away

Think about controls in anything you have in-flight – can they be better articulated, evidenced or assured in readiness for reforms?

Consider if you have any material weaknesses and plan to remediate – are there open audit issues, any known live issues?

Speak to your peers in Risk and Finance to develop an integrated and optimised approach

07

Key note speaker

Glen Robinson
National Technology Officer
Microsoft

08

Wrap up

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk

Document Classification: KPMG Public

CREATE: CRT149453B