Technology, Innovation and Transformation in internal audit

10 October 2024

Ask a question

To ask a question

Click on the **Q&A** button in the bottom toolbar to open the submit question prompt.

Type your question and click send

NOTE: If you wish to ask your question anonymously check the **send anonymously** box shown on the illustration.

Did you know?

From 1 November 2023, ICAEW's revised Continuing Professional Development (CPD) Regulations brought in new CPD requirements, including a minimum number of hours and an ethics requirement.

This webinar could contribute to up to 1 hour of verifiable CPD, so long as you can demonstrate that the content is relevant to your role.

Find out more about how these changes affect you at icaew.com/cpdchanges.

Today's presenters

Carolyn Clarke
BRAVE.

Steven Brown
BRAVE.

Steve Evenden
Nationwide

Steven Yates
PwC

Agenda

- Innovation and the role of Internal Audit

- Technology-enabled innovation

- Responding to the challenges and addressing emerging risks

- Technology, tools and AI in Internal Audit

Innovation and the role of Internal Audit

What is innovation?

➤ Enabling and empowering risk taking – within parameters

➤ Business innovation **and** Internal Audit innovation – working seamlessly together

Code of Practice for Internal Audit 2024

➢ Para 7: Prioritise emerging risks in planning

➢ Para 8: Scope must include emerging risks

➢ Para 8a: Focus on priorities impacting the business model

➢ Para 8e: Key corporate events include significant business process changes

➢ Para 8j: Internal audit must include in plan technology risk and AI

➢ Para 28: Ensure the function has access to appropriate tools and technology

Technology-enabled innovation.

A business perspective.
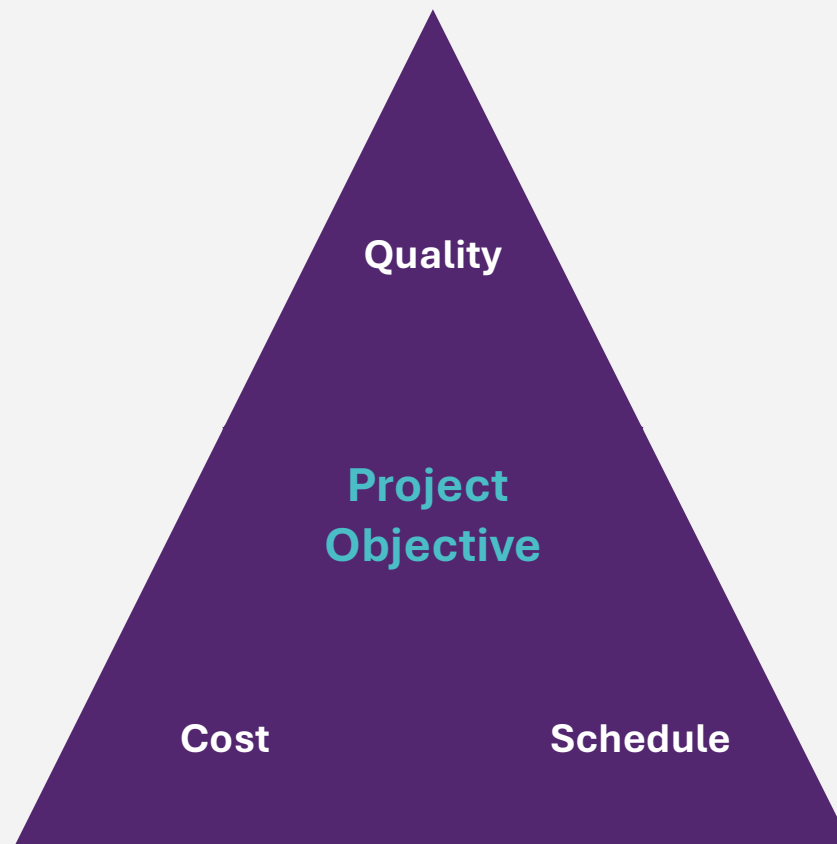
Balanced priorities: the key to enduring transformation.

Balanced priorities: innovation vs. risk

Major innovation may introduce unknown risks.
e.g. cryptocurrency

Risk-aversity may stifle innovation.
e.g. Blockbusters

Innovation

Strategic Objective

Risk/ Security
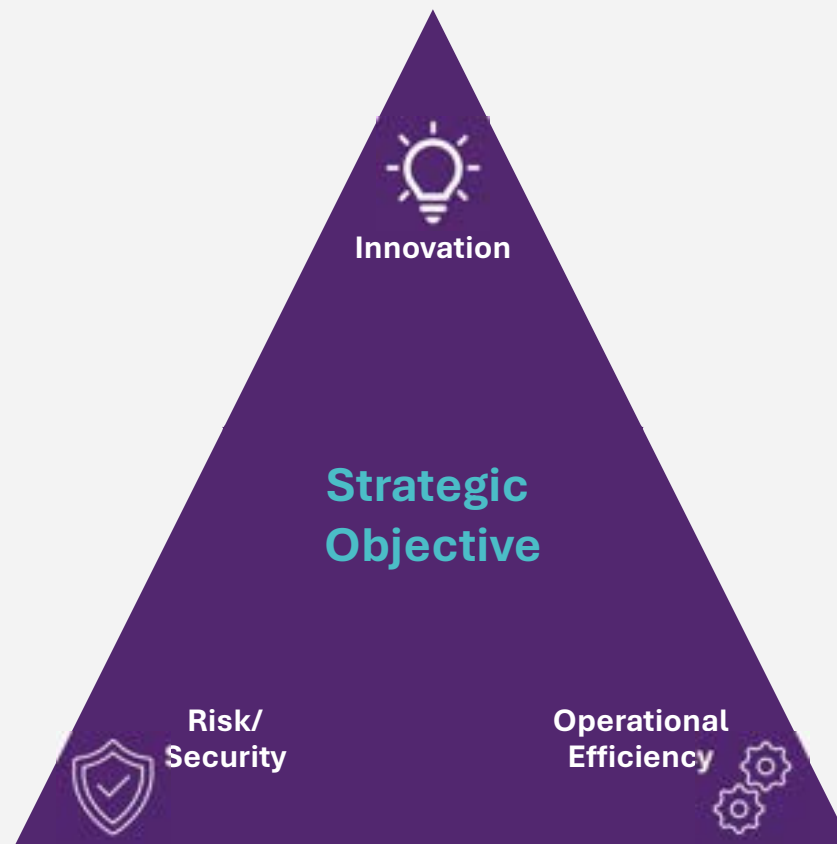
Operational Efficiency
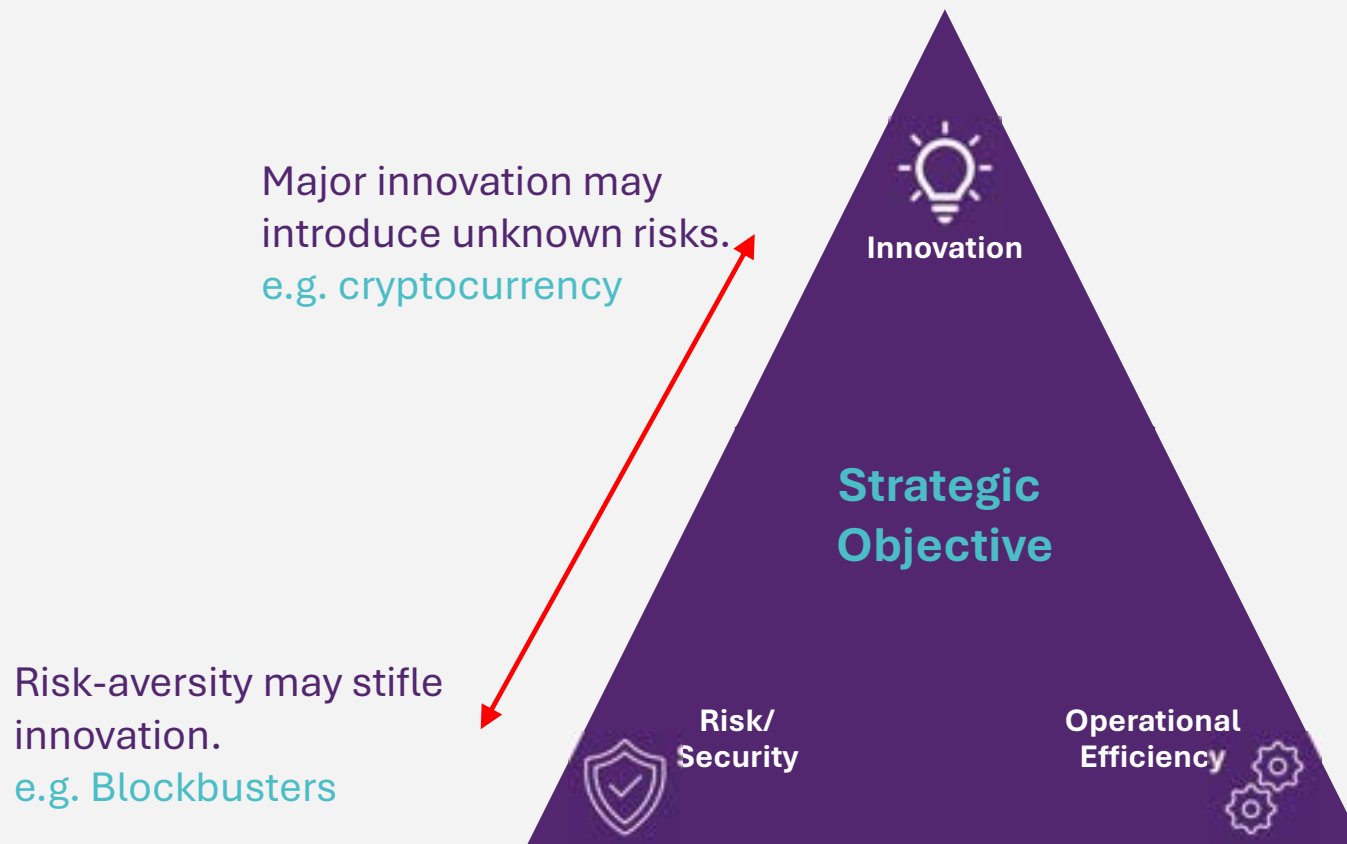
Balanced priorities: innovation vs. operational efficiency

Innovation

Strategic Objective

Risk/ Security

Operational Efficiency
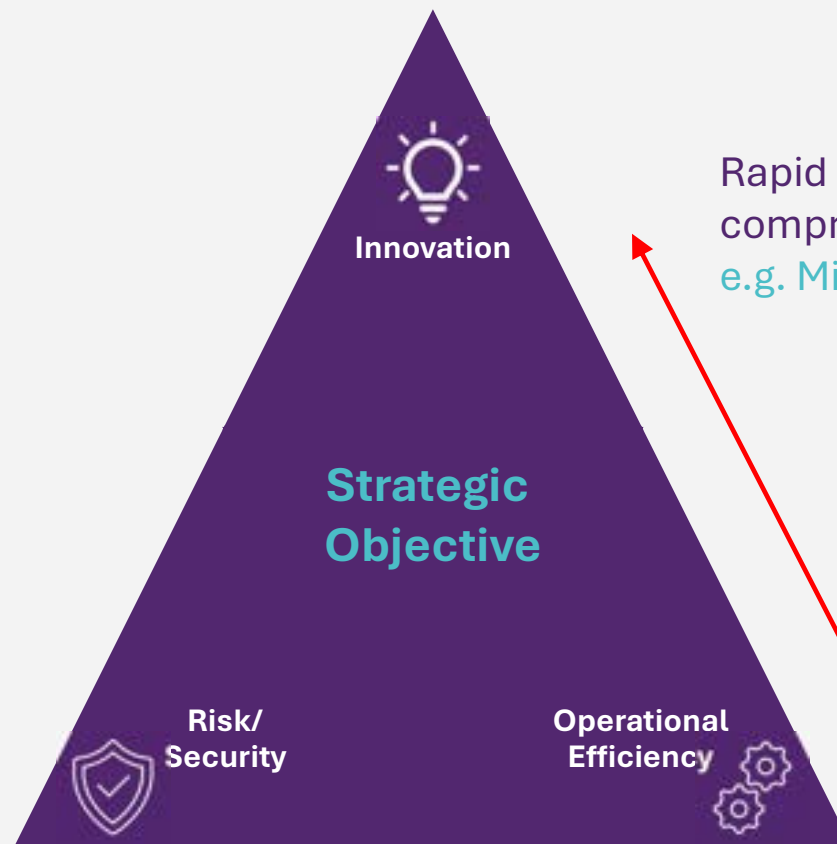
Rapid innovation may compromise efficiency.
e.g. Microsoft software updates

Over-emphasis on efficiency may slow innovation.
e.g. Volkswagen diesel testing

Balanced priorities: risk vs. operational efficiency.

Innovation

Strategic Objective

Risk/ Security

Operational Efficiency

Over-emphasis on risk may reduce efficiency.
e.g. NHS Digital Transformation

Efficiency without safeguards adds risks.
e.g. Boeing 737 MAX

Balanced priorities: Netflix transformation.

Innovation

Pioneered streaming technology.
Recommendations algorithm.
Original content.

Strategic Objective

Networks for secure streaming.
Adaptive streaming to maintain quality.
Digital rights and licensing.

Risk/ Security

Operational Efficiency

Cloud computing infrastructure.
Data analytics for content acquisition.
Streamlined user interface.

Internal Audit can support balanced priorities.

Clarify strategic objective.

Be clear what the innovation and transformation is in service of.

Encourage innovation.

Risk-based approach – don't outpace control.

Integrate controls.

Establish security early in the innovation process…
…without stifling new ideas.

Streamline and automate.

Optimise operations without weakening controls.
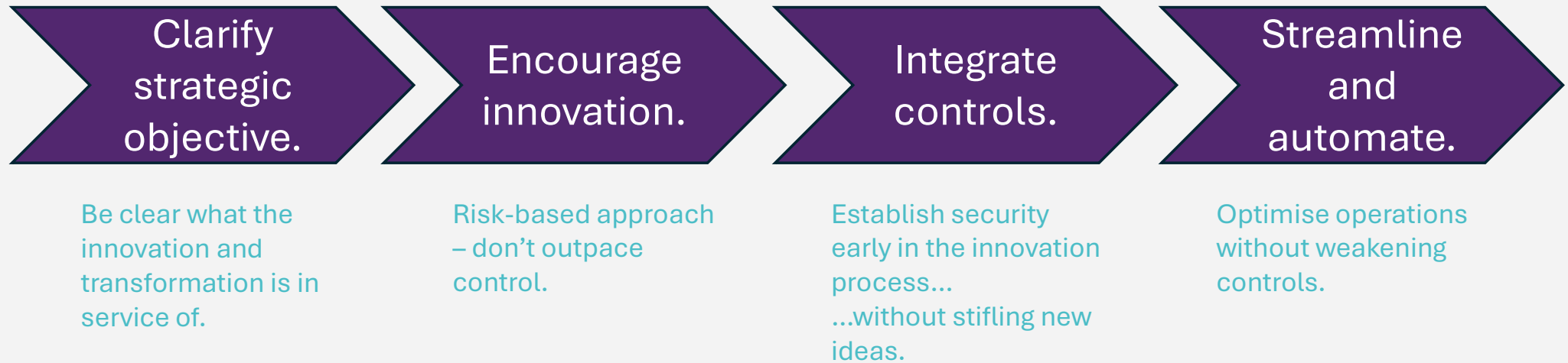
Assurance over Technology & Innovation

Flexibility in assurance approach, including:

- Business Monitoring

- Real-Time Assurance

- Programme/Change Audits

Considerations

- Timely and relevant – speed of assurance more important

- Promote "Eyes-Open" risk taking

- Short shelf-life

- Choosing right time for raising issues and using ratings

Rethink Risk

AI in Internal Audit

pwc

Today's Agenda

1. Overview of AI

2. Trends in AI Adoption

3. Risks & Opportunities for Internal Audit

Ste Yates
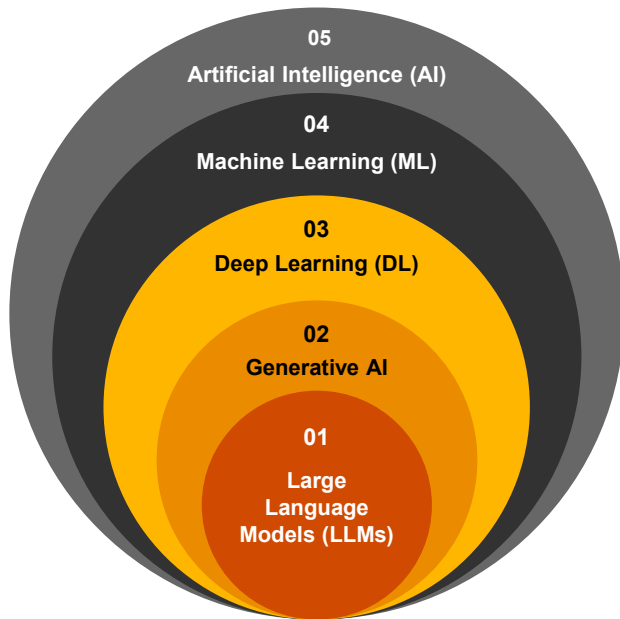Internal Audit Digital Lead - Senior Manager

M: +44 7841 785342
E: steven.j.yates@pwc.com

What is artificial intelligence?

AI is…

05 Artificial Intelligence (AI)
Computer systems designed to simulate human intelligence, perception and processes.

04 Machine Learning (ML)
A subfield of AI focused on the use of data and algorithms in machines to imitate the way that humans learn, gradually improving its accuracy.

03 Deep Learning (DL)
An ML technique that imitates the way humans gain certain types of knowledge, uses statistics and predictive modeling to process data and make decisions.

02 Generative AI
Algorithms that use prompts or existing data to create new content - e.g. written (text, code), visual (images, videos), auditory.

01 Large Language Models (LLMs)
A subset of Generative AI which is trained on high volume data-sets to generate, summarise and translate human-like text and other multimedia content.

Deep learning models are trained on massive volumes of input data.
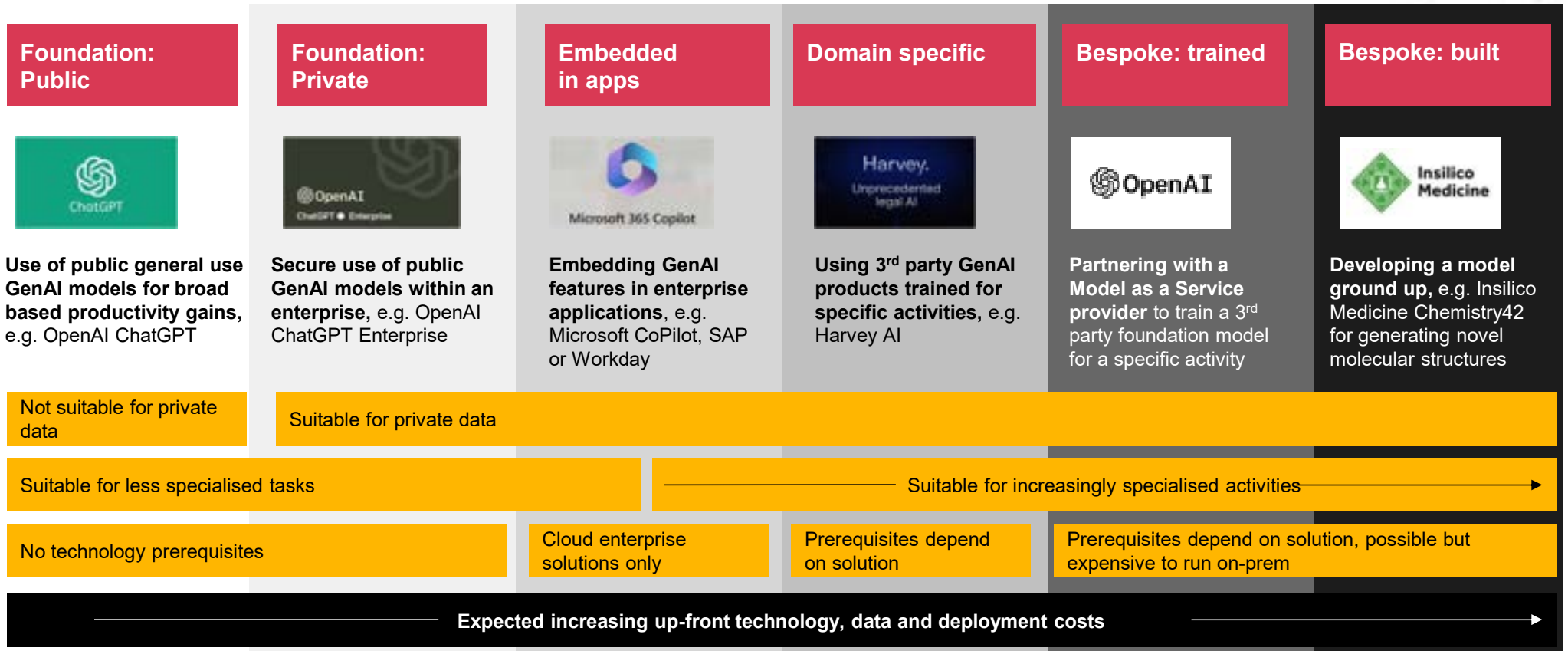
Human prompts in natural language are then used to query the generative AI models – taking any prompt/question without specific training.

New human–like content is created in response to the prompts – based on predictions from the GPT model.
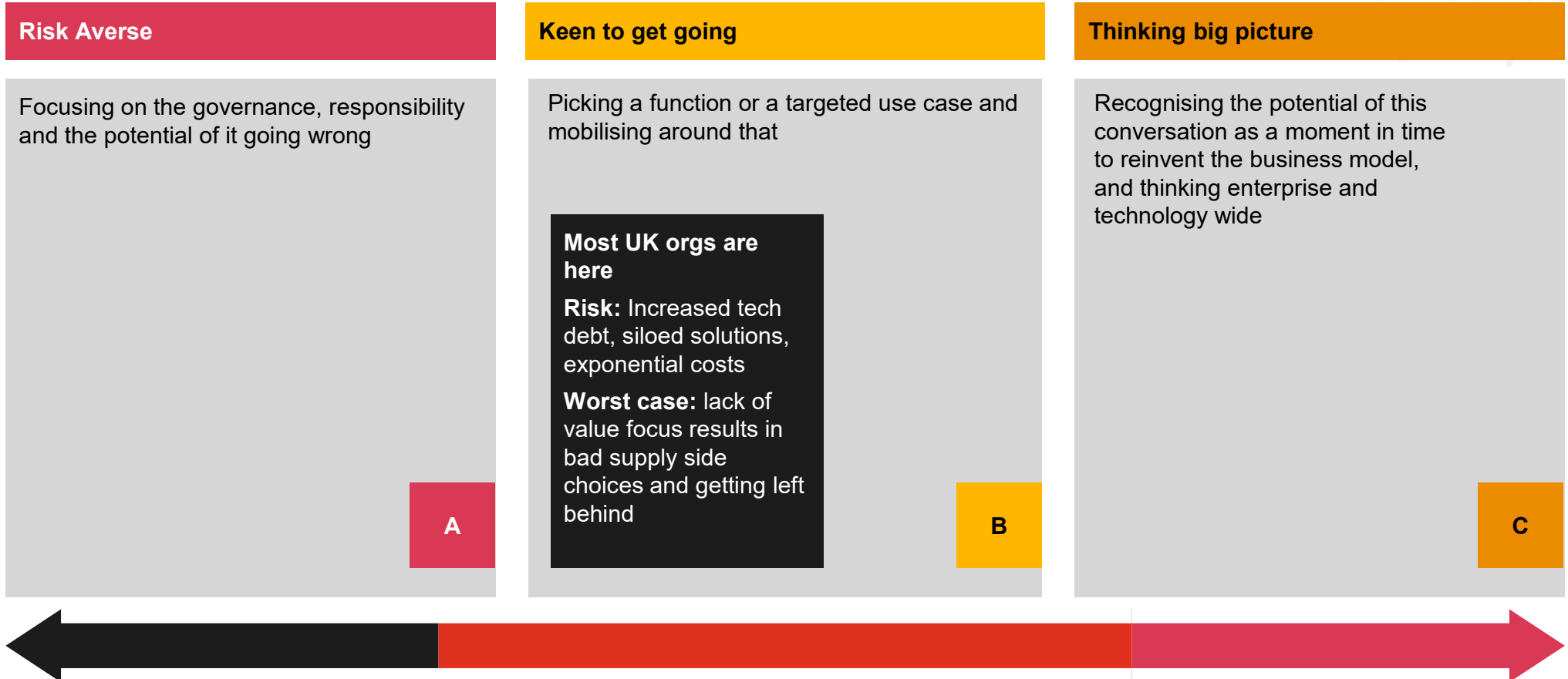
Modes of adoption: the use, buy or build consideration

There are five potential modes of adoption; from public models, embedded and productised solutions to highly bespoke models

Foundation: Public	Foundation: Private	Embedded in apps	Domain specific	Bespoke: trained	Bespoke: built
ChatGPT	OpenAI ChatGPT Enterprise	Microsoft 365 Copilot	Harvey. Unprecedented legal AI	OpenAI	Insilico Medicine
Use of public general use GenAI models for broad based productivity gains, e.g. OpenAI ChatGPT	**Secure use of public GenAI models within an enterprise,** e.g. OpenAI ChatGPT Enterprise	**Embedding GenAI features in enterprise applications**, e.g. Microsoft CoPilot, SAP or Workday	**Using 3rd party GenAI products trained for specific activities,** e.g. Harvey AI	**Partnering with a Model as a Service provider** to train a 3rd party foundation model for a specific activity	**Developing a model ground up,** e.g. Insilico Medicine Chemistry42 for generating novel molecular structures

Not suitable for private data	Suitable for private data				
Suitable for less specialised tasks			Suitable for increasingly specialised activities →		
No technology prerequisites		Cloud enterprise solutions only	Prerequisites depend on solution	Prerequisites depend on solution, possible but expensive to run on-prem	

Expected increasing up-front technology, data and deployment costs →

Many businesses are keen to get going, but there are risks

Risk Averse

Focusing on the governance, responsibility and the potential of it going wrong

A

Keen to get going

Picking a function or a targeted use case and mobilising around that

Most UK orgs are here

Risk: Increased tech debt, siloed solutions, exponential costs

Worst case: lack of value focus results in bad supply side choices and getting left behind

B

Thinking big picture

Recognising the potential of this conversation as a moment in time to reinvent the business model, and thinking enterprise and technology wide

C

Artificial intelligence – risks and opportunities

Key industry trends we are seeing from our **Global CEO Survey** are as follows:

Gen AI	AI Regulation	Responsible AI	Accountability

70%

of CEOs said GenAI will significantly change their business in the next 3 years[1].

1 August 2024

EU AI Act came into force.

Many emerging AI use cases may now be subject to additional governance requirements.

Ethics

Use of AI within organisations introduces ethical challenges. Furthermore, AI-related incidents attract negative media coverage which highlights public concern.

SM&CR

Within the Financial Services sector, the Senior Managers & Certification Regime stresses Senior Management's accountability, including AI use.

Other organisations should take note and implement policies, processes, and controls, owned by accountable individuals, so that their use of AI stands up to scrutiny.

[1] | **PwC Global 27th Annual CEO Survey**

Artificial intelligence – risks and opportunities

What's on the risk agenda?

Potential threats and risks associated with GenAI

While enabling new opportunities, the ever-growing capabilities and impact of AI introduces and exacerbates a number of risks that need to be managed:

Transparency

A lack of transparency around how and when AI is used can lead to lack of accountability and customer mistrust.

Misinformation

Most GenAI solutions are unaware of, and will exclude, events, cases or developments that post-date its training data.

Data protection and security

Data leakage risks can be heightened if GenAI tools are granted inappropriate access.

Hallucination

AI models could 'make up' information which is plausible but incorrect.

Discrimination

If AI models can 'learn' discrimination and if this is based on protected characteristics, it could pose a significant regulatory and/or reputational risk.

Cyber security

AI could introduce new threat vectors, such as prompt injection attacks.

Copyright and intellectual property

GenAI models which are trained on copyright data may pose liability risks.

Accountability

Many organisations lack clarity around roles and responsibilities to manage GenAI risks. Further, the ease of access to GenAI solutions, increases the risk of misuse – whether intended or accidental.

Misuse

GenAI could be used for malicious purposes, which could result in misalignment against the intended/approved purposes.

AI incidents in the press

Professor Flunks All His Students After ChatGPT Falsely Claims It Wrote Their Papers

Error-prone facial recognition leads to another wrongful arrest

Australian mayor prepares world's first defamation lawsuit over ChatGPT content

AI-Detectors Biased Against Non-Native English Writers

OpenAI, Microsoft want court to toss lawsuit accusing them of abusing open-source code

How I Broke Into a Bank Account With an AI-Generated Voice

ChatGPT resumes service in Italy after adding privacy disclosures and controls

NY regulator investigating Apple Card for possible gender bias

The probe follows a series of viral tweets about algorithms used for the credit card, which Goldman Sachs manages with Apple.

ChatGPT bug temporarily exposes AI chat histories to other users

SECURITY / POLICY / ARTIFICIAL INTELLIGENCE

ChatGPT cooks up fake sexual harassment scandal and names real law professor as accused

OpenAI sued for defamation after ChatGPT allegedly fabricated fake embezzlement claims

Apple Restricts Employee Use of ChatGPT, Joining Other Companies Wary of Leaks

The iPhone maker is concerned workers could release confidential data as it develops its own similar technology

IBM abandons 'biased' facial recognition tech

Welfare surveillance system violates human rights, Dutch court rules

Government told to halt use of AI to detect fraud in decision hailed by privacy campaigners

Lawyer cites fake cases generated by ChatGPT in legal brief

Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak

- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

Artificial intelligence – risks and opportunities

What does this mean for Internal Audit?

Examples of key elements for Internal Audit to consider include:

Auditing organisational AI use

EU AI Act readiness

Many IA teams are working now to:

- Assess the existence and suitability of the organisation-wide AI inventory and classification of AI models as per EU AI Act requirements.
- Assess plans and progress with implementation of necessary governance (determined by the risk classifications) covering: transparency, technical documentation, impact assessments and codes of conduct depending on the use case.
- Ensure alignment with other sectoral regulation. The risks posed by AI may fall under the scope of other regulation, such as breaches/disruption of critical AI-enabled services leading to regulatory fines.

AI risk and controls

- Understand the AI universe including use cases and development status.
- Understand your organisation's AI strategy, risk assessment, governance and policy arrangements and how they are being developed and embedded.
- Build and execute a risk-based AI audit programme (referencing materials such as the PwC AI Readiness Framework).
- Prepare tailored audit programmes for higher risk AI models.

Building AI skills within Internal Audit

AI enabled Internal Audit

- Identify use cases that will drive efficiencies, optimise, automate or enhance Internal Audit processes.
- Collaborate with AI steering committees and/or responsible AI council to ensure that controls and assurance remain high on the agenda.
- Develop or secure access to digital skills to provide confidence in Internal Audit's capacity and capability to use AI effectively and provide assurance over the key and emerging risks associated with AI.

Artificial intelligence - transforming Internal Audit with AI

What does this mean for Internal Audit? (continued)

AI has the potential to revolutionise Internal Audit functions – transforming capabilities, providing opportunities for optimisation of resources and better insight gathering through more detailed analysis. Here are some examples and key benefits of AI use cases that are changing the way organisations conduct Internal Audit.

AI enabled control testing
The capability of AI to process large volumes of unstructured data can be leveraged in controls evaluation and testing to recognise patterns and propose findings. AI is capable of:
- Reviewing documents, emails and summarising evidence submitted,
- Identifying gaps in data,
- Generating test scripts for remediation of identified issues, and
- Evaluating large control databases to identify duplicate controls and incomplete controls description.

Gen AI Internal Audit planning and support
GenAI models can help design Internal Audit plans and provide support on audit engagements, drawing from Internal Audit methodologies, web searches for relevant risk assessments and historic annual reports. Use cases include:
- Automating risk assessments,
- Developing audit plans with tailored domains and risk theming, and
- Drafting audit scope and announcement memorandums (or Terms of Reference).

AI enabled stakeholder engagement
GenAI solutions can enable more effective stakeholder engagement using tools such as Microsoft Copilot, which can improve productivity through:
- Drafting relevant stakeholder questions,
- Transcribing meetings and generating summaries, and
- Identifying next steps based on stakeholder conversations.

Continuous monitoring
AI tools can be used to continuously monitor systems and processes to automatically flag risks and provide an audit trail for review. Examples of continuous monitoring include:
- Identifying of anomalies and potentially fraudulent transactions,
- Automated monitoring to ensure compliance with policies and regulation, and
- Embedding predictive analytics for forecasts and ongoing risk assessments.

Audit practice and quality assurance support
AI can significantly enhance audit quality assurance and enable cost efficiency. Some examples are:
- Using GenAI to review audit reports and completed files to identify quality-related issues, and
- Incorporating interactive chatbots and virtual assistance to provide real time support to auditors on methodologies and audit standards.

Key benefits:

Reduce human error in data analysis and reporting

Improve accuracy of data analysis and verification against regulations

Increase efficiency and cost saving through process automation

Enable ongoing monitoring and real-time risk detection

Enable ongoing quality and continuous improvement

The key to success with GenAI is to keep exploring…

> **"**
>
> In the next 12 months, I think the systems that we use today will be laughably bad.
>
> GPT-4 is the dumbest model any of you will ever have to use again by a lot.
>
> **Sam Altman**
> CEO - OpenAI

Questions?