



AI: The Evolving Frontier of Opportunities and Risks

20 June 2024

Ask a question



The screenshot shows a Q&A interface. At the top, it says "Q&A". Below that, there is a section for a question and answer. The question is "What happens when I raise my hand?" with a timestamp of 18:03. The answer is "Molly Parker answered: I can take you off of mute." with a timestamp of 18:04. Below the answer, there is a large empty text input field. At the bottom of the input field, it says "Please input your question". At the very bottom, there is a checkbox labeled "Send Anonymously" and a blue "Send" button.

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](https://www.icaew.com/cpdchanges).



Today's speakers



Carolyn Clark
Founding Partner
Brave Within LLP



Carrie Stephenson, Former
General Counsel and Founding
Partner at Brave Within LLP



Radhika Modha Group
Business Information Security
Officer, Spectris plc



Matthew Howard,
IT Audit Director, Unilever



Annabel Gillard
International Advisory Council
Member for Institute of Business Ethics



B.

AI Legal and Regulatory Landscape

Prepared by Carrie Stephenson,
BRAVE Within LLP

20 June 2024



UK vs EU

From One
Extreme to
Another

	EU	UK
Legislation	EU AI Act – publication expected imminently	Non-statutory at this stage.
Timeframe	<p>EU AI Act becomes applicable after 24 months with regard to most parts of the regulation.</p> <p>Shorter deadlines (6 months) will apply for prohibited AI or GPAI (12 months).</p> <p>Longer deadlines (36 months) for AI systems embedded into regulated products.</p>	<p>Temporary pause because of General Election; however, Government's 2024 AI Roadmap remains active.</p> <p>Individual regulators expected to continue implementing the AI framework in respective sectors.</p>
Approach	Traditional - prescriptive and risk-based approach	Agile - principles and context-based approach
Implementation	Central European AI Board	By existing regulators
Sectoral Scope	<p>Horizontal cross-sector regulation</p> <p>Global reach</p>	Vertical sector-specific guidance
Liability	AI Liability Directive	No changes to existing liability regime.
Penalties	Fines – from 7.5 million euros (\$8.2 million) or 1.5% of turnover to 35 million euros or 7% of global turnover	None at this stage.

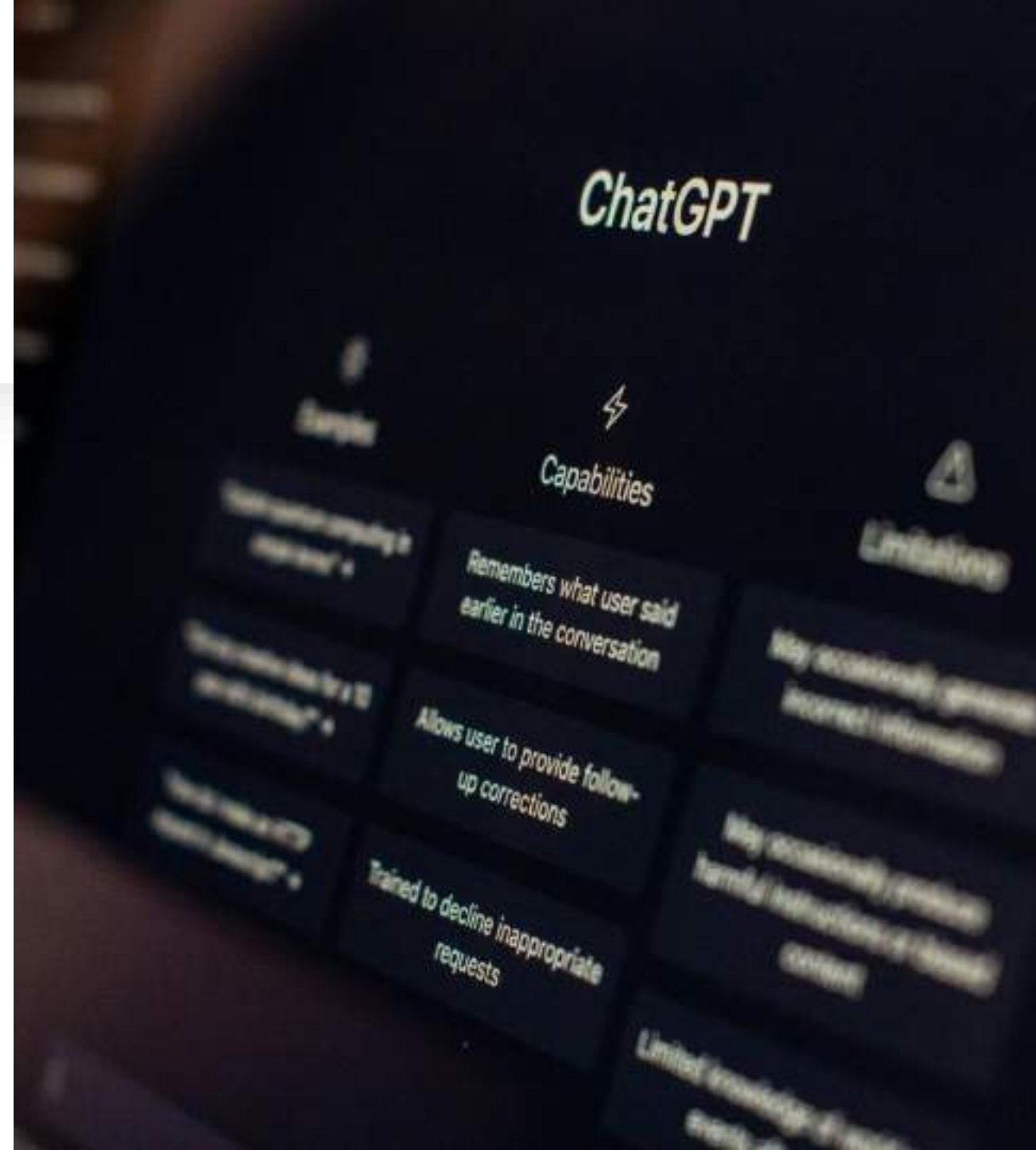
Business risk management considerations – the view of a BISO / CISO



How AI is reshaping the Security & Risk environment

Traditional AI has been around a long time, but Generative AI has exploded recently.

Across the Information Security landscape, this creates both opportunity and risk.



From a security risk perspective:

- Attackers have an increasingly sophisticated set of tools to use.
- The same way Generative AI can make our tasks easier; it can make an attackers easier too.
- Methods humans have used in the past to identify malicious items are less likely to be effective (for example, spotting spelling and punctuation mistakes in a phishing email).

Opportunities



From a security risk perspective:

- Security tooling and risk management techniques are being bolstered through use of AI, whether this be built into tooling, or by making complicated security practices and knowledge more accessible through generative AI

how can I spot a phishing email that was made with generative AI



Spotting a phishing email created using generative AI can be challenging, as these emails may have fewer spelling and grammatical errors and can appear more convincing than traditional phishing attempts. However, there are still several indicators you can look for to identify AI-generated phishing emails:

1. Unusual Sender Email Address:

- Even with AI, phishing emails often come from email addresses that don't match the official domain of the organization they claim to be from. Check the sender's email address carefully for any discrepancies.

2. Generic Greetings and Lack of Personalization:

- AI-generated phishing emails might still use generic greetings like "Dear Customer" or "Dear User" instead of your actual name, especially if they lack specific personal information.

3. Requests for Personal or Financial Information:

- Legitimate organizations rarely ask for sensitive information (e.g., passwords, credit card details, Social Security numbers) via email. Be wary of any email requesting such information.

4. Urgent or Threatening Language:

- Phishing emails often create a sense of urgency or fear to prompt immediate action. Be

Strategic Implications of AI in the broader technology landscape



Considerations:

- How far do we take use of AI, and will it change how we work?
- How fast could AI change the broader technology landscape?
- How will governance and regulation impact this?



Challenges & Responses: First hand examples

Common themes:

- Terminology & shared understanding
- Data governance, classification & exposure
- Hallucinations & reliance
- User access implications
- IP Infringement
- Change management & process change
- Understanding & auditing AI models

400+ Uses of AI within our business



How are we auditing?



AI to support Internal Auditing Activities

I asked Copilot:

What are the top 3 most exciting uses or opportunities for using AI in Internal Auditing?

Copilot responded:

Certainly! Artificial intelligence (AI) offers exciting opportunities for internal auditing. Here are three key areas where AI can make a significant impact:

Risk Assessment and Planning:

GenAI can help auditors research and understand industry-specific risks.

Leaders can leverage GenAI to suggest scheduling, resource allocations, and engagement planning based on constraints like staff availability and skills.

AI-driven risk assessments enhance efficiency and accuracy in identifying potential risks¹².

Audit Fieldwork and Efficiency:

AI enables data analytics, allowing auditors to analyze large volumes of financial transactions and identify patterns or anomalies.

Continuous monitoring using AI can improve risk detection and audit quality.

Automation streamlines audit processes, increasing efficiency and coverage²³.

Enhanced Audit Quality and Insights:

AI can simplify language, generate summaries, and improve report quality.

By covering 100% of the population (rather than sampling), AI helps identify potential fraud and irregularities more efficiently.

Overall, AI-driven insights enhance audit quality and provide deeper insights into organizational processes²³.

Remember that integrating AI requires careful planning, governance, and controls to maximize its benefits while managing risks¹. If you'd like more details or have additional questions, feel free to ask! 😊



AI to support Internal Auditing Activities

What Unilever is doing:

- Advanced Analytics and Analysis tools for auditors
 - Control performance
 - Risk Analysis
 - Anomaly/Fraud Detection
- Language Translation
- Document Summarisation

Areas that we are actively exploring:

- Document query
 - Ask the engine questions about documentation
 - Ask questions about previous audits
- Proof-reading and correction
- Suggested wording for Issues and Recommendations
- Suggested wording for Audit Summaries and reports
- Suggested Test Plans
- Advanced Statistical Code Query generation

All within a private and secure AI environment

Building trust and human connection in a digitalising world

- **Ethics through a behavioural lens**
- **AI and ethics**
- **Decision-making framework**
- **Monitoring and assurance**

Behavioural insights for ethics

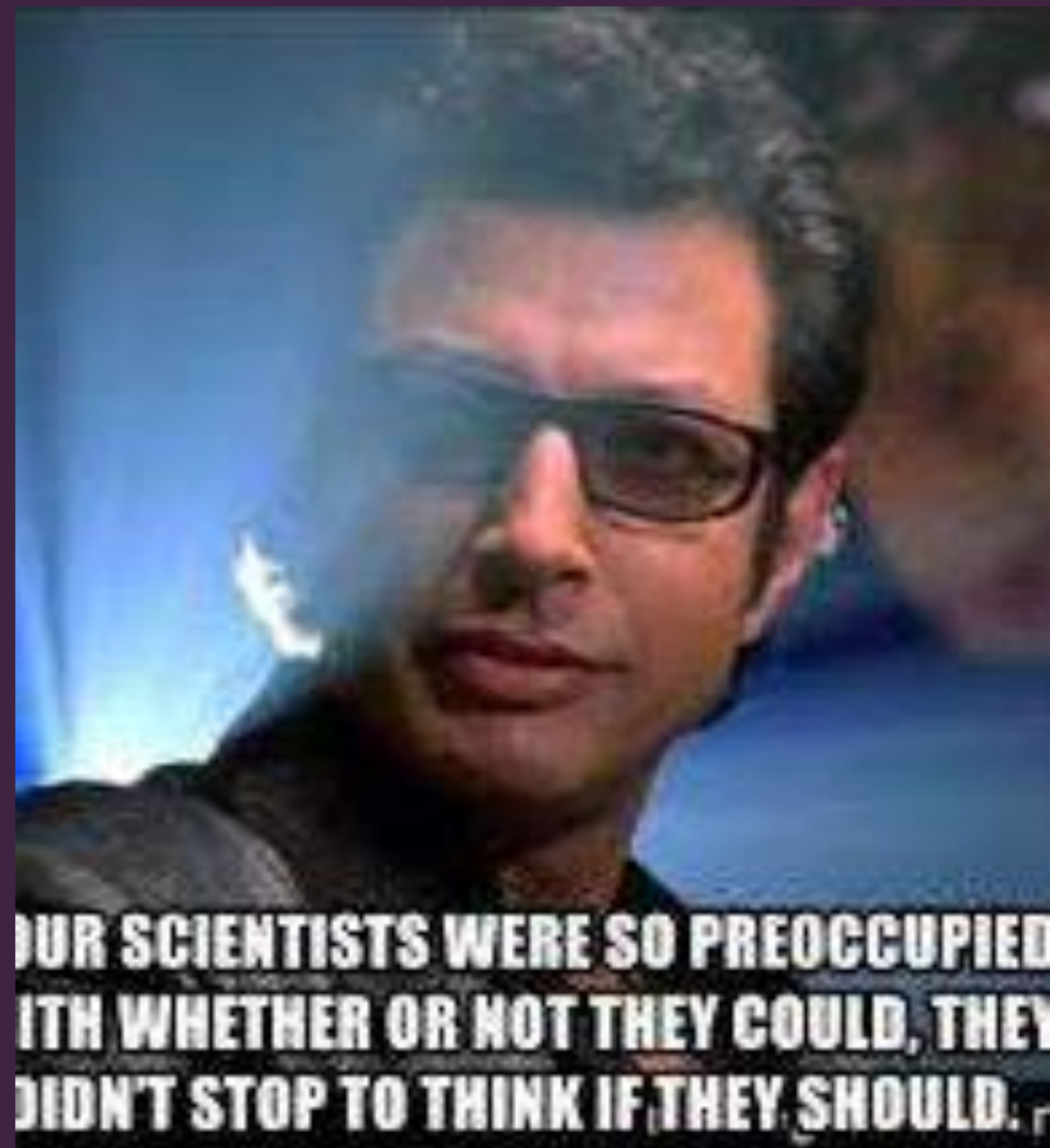
The value of ethics

- It's the 'how' of what we do – not staking a moral claim
 - Sets identity – what to expect from your organisation
 - Alignment of what's said & what's done = integrity = authenticity
- Builds trust with employees, customers, shareholders, regulators

Behavioural influences on ethics

- Behaviourally informed approaches to conduct, culture and compliance are on the rise
 - Align incentives
 - Make it easy
 - Social norms
 - Time to think
- Be aware of contributors to ethical fails: cognitive fatigue, self-interest, drifting norms, pressure
- Ethics as a practice, rather than something that can be coded

AI and Ethics



Why it's not just Business (ethics) as usual

AI:

- Is not ethically neutral
- changes the size and distribution of risk – existing measures may not work
- introduces new issues - privacy, personalised targeting, lack of transparency
- clouds responsibility and accountability
- is not understood or trusted

Training data

Algorithm

Deployment

Undermines fairness, wellbeing and trust

Bias - Open Data Institute case study

Car insurance quote

GoCompare Hi John!

Adjust cover 49 car quotes found, 4 telematics quotes included. Sort: Annually

Provider	Legal Assistance	Breakdown Cover	Personal Accident	Windscreen	Courtesy Car	Price	Total Excess
LLOYD BANK	+£374	+£406	✓	✓	✓	£538.26	£150
M&S BANK	+£374	+£414	✓	✓	✓	£571.66	£150
HALIFAX	+£366	+£439	✓	✓	✓	£573.39	£150
BANK OF SCOTLAND	+£366	+£439	✓	✓	✓	£577.87	£150

GoCompare Hi Mohammed!

Adjust cover 37 car quotes found, 5 telematics quotes included. Sort: Annually

Provider	Legal Assistance	Breakdown Cover	Personal Accident	Windscreen	Courtesy Car	Price	Total Excess
LLOYD BANK	+£389	+£459	✓	✓	✓	£1,446.32	£150
HALIFAX	+£389	+£459	✓	✓	✓	£1,458.04	£150
BANK OF SCOTLAND	+£389	+£459	✓	✓	✓	£1,459.64	£150
M&S BANK	✓	✓	✓	✓	✓	£1,476.70	£150

Car: Ford Fiesta Ghia 2002-2008 1.6
 Profession: Insurance Director
 Address: Milford Haven
 Always resided in the UK
 Date of birth: 01/01/1980
 No claims and license: 16 years
 Car kept on drive

Deep Fakes and deception



Who and what do we trust?

Dependency



Diminishes human capabilities, autonomy and responsibility

Decision-making frameworks

Ethics can help us chart an intentional and humane course



Inclusive growth, sustainable development and well-being >



Human-centred values and fairness >



Robustness, security and safety >

OECD AI Principles



Transparency and explainability >



Accountability >

A universal standard for minimizing harm and building trust

Principles need practical application

- Operational frameworks are emerging
 - Need to be culturally embedded, practical and include a process for managing trade-offs
 - Ethics by design, and during development, and in deployment, and check for drift (4xDs)
- Emerging standards and Independent oversight can do some of the heavy lifting

Don't make promises you can't keep

Monitoring and assurance

Developing rigour in ethical AI use



DETERMINE
ETHICAL
PRINCIPLES



DEVELOP
OPERATIONAL
FRAMEWORK



ALIGN BEHAVIOURAL
INFLUENCES



CULTURALLY
EMBEDDED



ONGOING
OVERSIGHT

Ensuring the technology serves the humans, not the humans serving the tech

WHAT CAN YOU DO NOW?

5 no-regret actions

5 no-regret actions for you to take now:

1. **Prepare for an AI audit** by identifying key stakeholders, defining the scope, and establishing a timeline for assessing, categorising AI systems and their associated risks.
2. **Develop a roadmap** for implementing an AI governance framework, including drafting policies, assigning responsibilities, and setting milestones for progress.
3. **Review current data governance practices**, identify gaps, and plan necessary enhancements to ensure data used in AI is secure, unbiased, and compliant with regulations.
4. **Assess current AI systems** for transparency and explainability, and develop a strategy for improving these aspects and communicating AI use to stakeholders.
5. **Evaluate existing AI knowledge** within the organisation, identify training needs, and develop a comprehensive education plan for employees and stakeholders to promote responsible AI practices and regulatory compliance.





Questions

