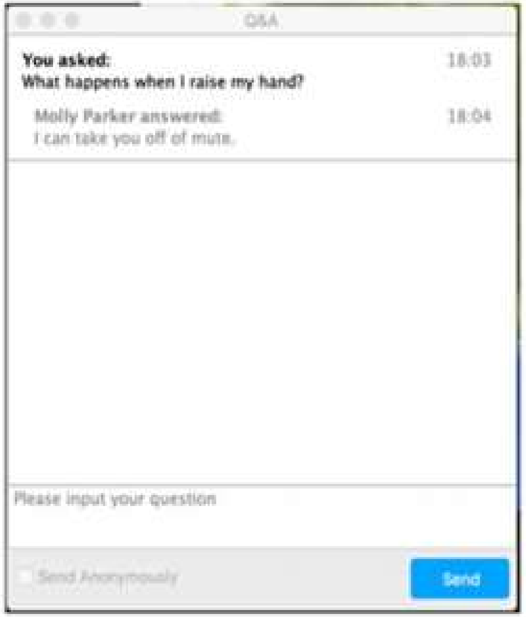
The new frontier for internal assurance: sustainability, AI, and Geopolitics

11 September 2025

Michael Lucas, Chris Tall, Ian Swain, Tracy Woods, Moya Hayhurst

Ask a question



You asked: 18:03
What happens when I raise my hand?

Molly Parker answered: 18:04
I can take you off of mute.

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?

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 speakers

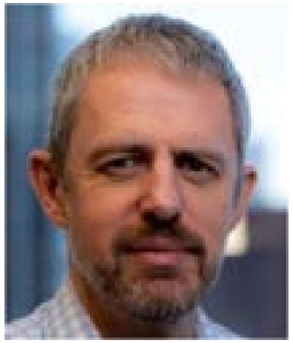
Michael Lucas

Founding Partner

Brave Within LLP

Moya Hayhurst,
Experienced Co-Sec and
Researcher for Centre for AI in
Board Effectiveness

Tracy Woods, Co-founder of
Conversations on AI



Ian Swain,
Brave Within

Chris Tall, CAE,

Deliveroo Plc,

The New Frontier for Assurance

Aligning assurance with the pressures and priorities of today's directors.

Company directors must meet growing expectations while navigating a world like this…

Tariffs, geopolitics, AI governance, cyber threats, new regulation, disruptive competition, ESG obligations, workforce transformation, supply chain fragility.

With financial and non-financial information which is organised like this…

Financial performance reports, ESG reports, risk reports, compliance reports, safety reports, whistleblowing reports, internal audit reports, regulatory reviews, management letters from external auditors….

…and reported like this.

Risk reporting, for example, often occurs quarterly and can be weeks or months after risks have materialised.

So, directors do this.

"63% of directors use AI personally in their work"
(UK IoD survey, May 2025)

And this:

BRAVE.
Changing governance. From within. For good.

The World is Changing: Implications and Opportunities for Our Stakeholders

"In a world in flux, stability is no longer about standing still — it's about adapting with purpose and integrity." Unknown.

Moya Hayhurst

Where Are We Now?

Rising Complexity

Interconnected risks, accelerating technology, and shifting regulation mean governance decisions now demand fluency across legal, digital, and ethical domains — all at once.

Deeper Accountability

Under heightened regulatory scrutiny, Boards expect clear, evidence-based assurance on financial and AI-driven non-financial data — with Internal Audit providing the independent lens on accuracy, integrity, and oversight.

Resilience and Agility

Organisations must absorb shocks and adapt at speed, embedding ethical AI and robust governance into everyday decision-making without losing strategic focus.

How Is the Game Changing? Opportunities and Challenges of AI

Transformative Opportunities

AI and emerging technologies are enabling faster, deeper insight — shifting governance and audit from reactive oversight to proactive value creation.

Risk Management Challenges

Opaque AI decision-making, heightened regulatory scrutiny, and assurance gaps in non-financial data demand sharper oversight and stronger controls.

Evolving Landscape

Rapid regulatory change, rising stakeholder expectations, and shifting assurance roles require governance that adapts with integrity and agility.

Our Role: What now

Lead with Insight
Use our unique vantage point to connect the dots across risk, regulation, and technology — giving Boards the clarity to act decisively in a fast-moving environment.

Embed Assurance by Design
Build governance, ethics, and explainability into AI and data processes from the start — so assurance is continuous, not an afterthought.

Champion Adaptability with Integrity
Lead by example — show how you personally use AI alongside other technologies, demonstrating curiosity, critical thinking, and ethical guardrails in action. Address the three big concerns head-on: test outputs for bias or hallucinations, know where your data is going, and avoid over-reliance by keeping human judgment central. You can't build trust in what you don't practise yourself.

Things to think about

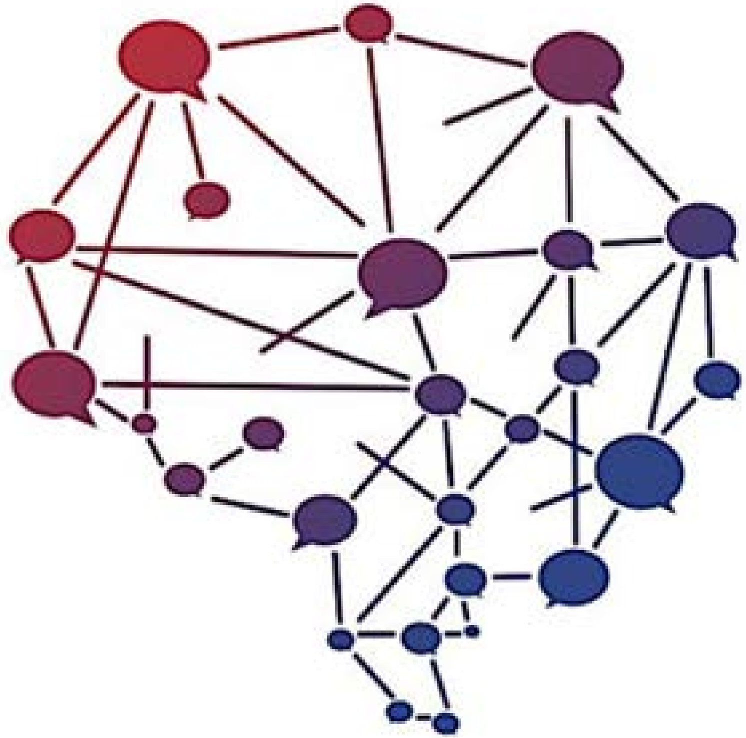
You can't build trust in what you don't practise yourself.

What this means for Internal Audit: your assurance narrative must now cover board fluency, technology governance, and the strength of internal control attestations—not just policy presence.

What is your legacy!

Digital transformations and conversations on AI

1. *101 of recent AI journey – explaining the reality behind some of the terms*
2. *Dispelling a few myths*
3. *Why auditors are so important*
4. *Why projects go wrong and why conversations on AI are so necessary*
5. *Broadening your view on who the stakeholders might be*
6. *My top 6 things to look out for…*



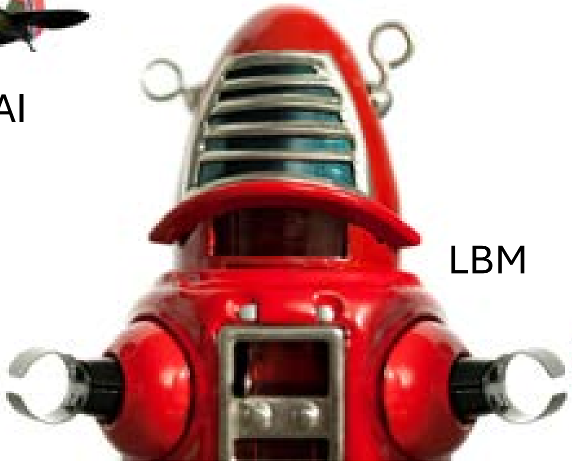
Supervised AI

Machine Learning

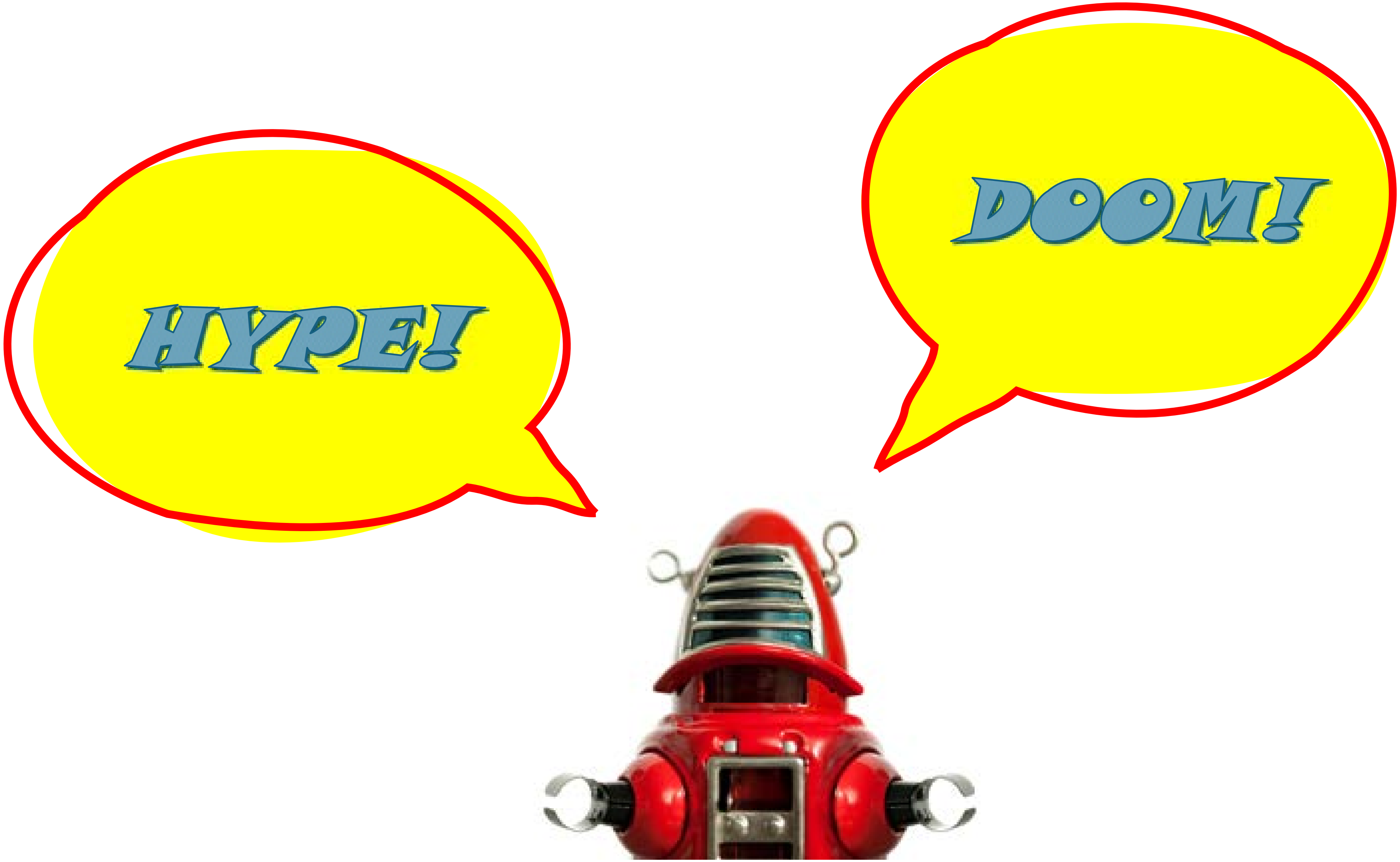
2 + 2 = 5

Generative AI

Agentic AI



LBM


HYPE!
DOOM!

Success!

Reasons projects go wrong...

...and how conversations can help...

1. Wrong project

- It isn't needed
- It can't deliver value
- It is tech for tech's sake

Who is impacted by this project, and how?

What will success look like for each cohort of stakeholder?

AI investment ≠ value to be delivered.

2. Can't deliver

- You don't have good data
- You don't have the capabilities
- You're not allowed to build it

Where does the data come from?

What upskilling or new insights do your teams need?

What risks are too high to continue?

3. Not adopted

- They don't have the capabilities
- They don't see the value
- They don't want it

Do the users trust and have confidence in it?

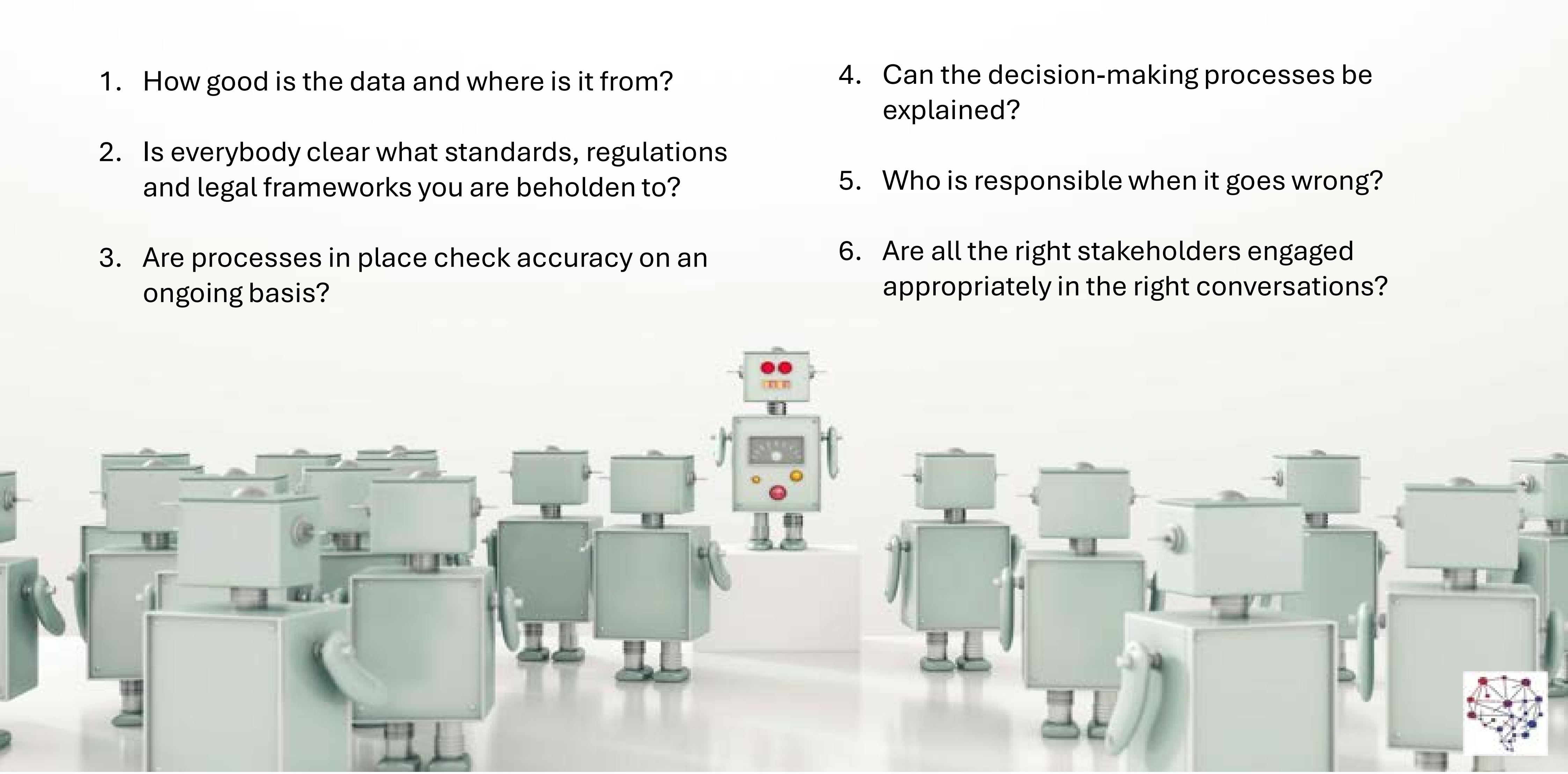
Do they have the rights skills to use it?

Their perception is your reality.

Who is impacted by self driving cars?

As an auditor, things to look out for…

1. How good is the data and where is it from?
2. Is everybody clear what standards, regulations and legal frameworks you are beholden to?
3. Are processes in place check accuracy on an ongoing basis?
4. Can the decision-making processes be explained?
5. Who is responsible when it goes wrong?
6. Are all the right stakeholders engaged appropriately in the right conversations?



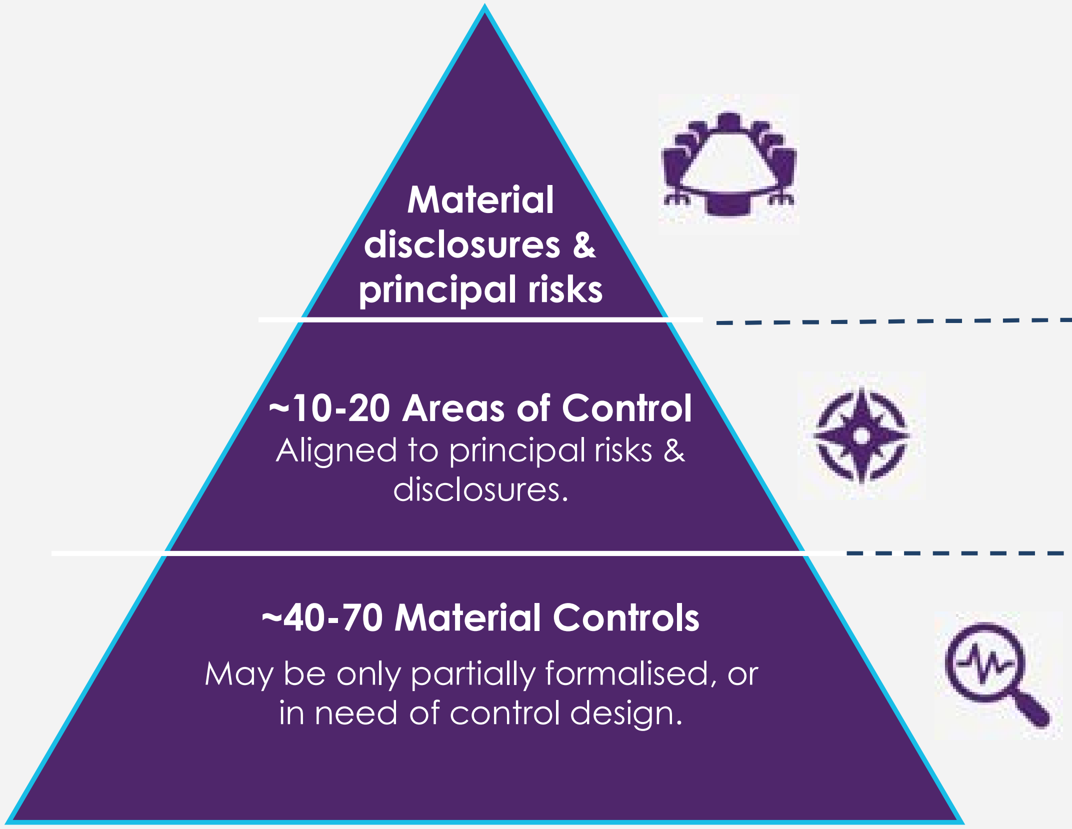
Thank you

Tracy Woods
Conversations on AI
https://conversationsonai.org

The last 2-years; the next 18-months

- What have we learned (or surmised)?
  - Not UK SOX, it's P29!
  - Not Bottom-up, it's Top-Down
  - Not process detail, it's frameworks and cluster controls
  - Not external but (probably) internal assurance
  - Not regulation but good practice

A hierarchy of disclosures, risks and controls.



Material disclosures & principal risks

~10-20 Areas of Control
Aligned to principal risks & disclosures.

~40-70 Material Controls
May be only partially formalised, or in need of control design.

Comment

Informed by Board levels of materiality and risk appetite

- *Non-financial disclosures*
- *Principal and possibly emerging risks (Principal Risk+)*

- *Circa 10-20 Control Areas for Reporting*
- *Includes Entity Level Controls*

May be entity level or specific operational or process controls to specific high-risk exposures. Monitoring may allow grouping (if comprehensive).

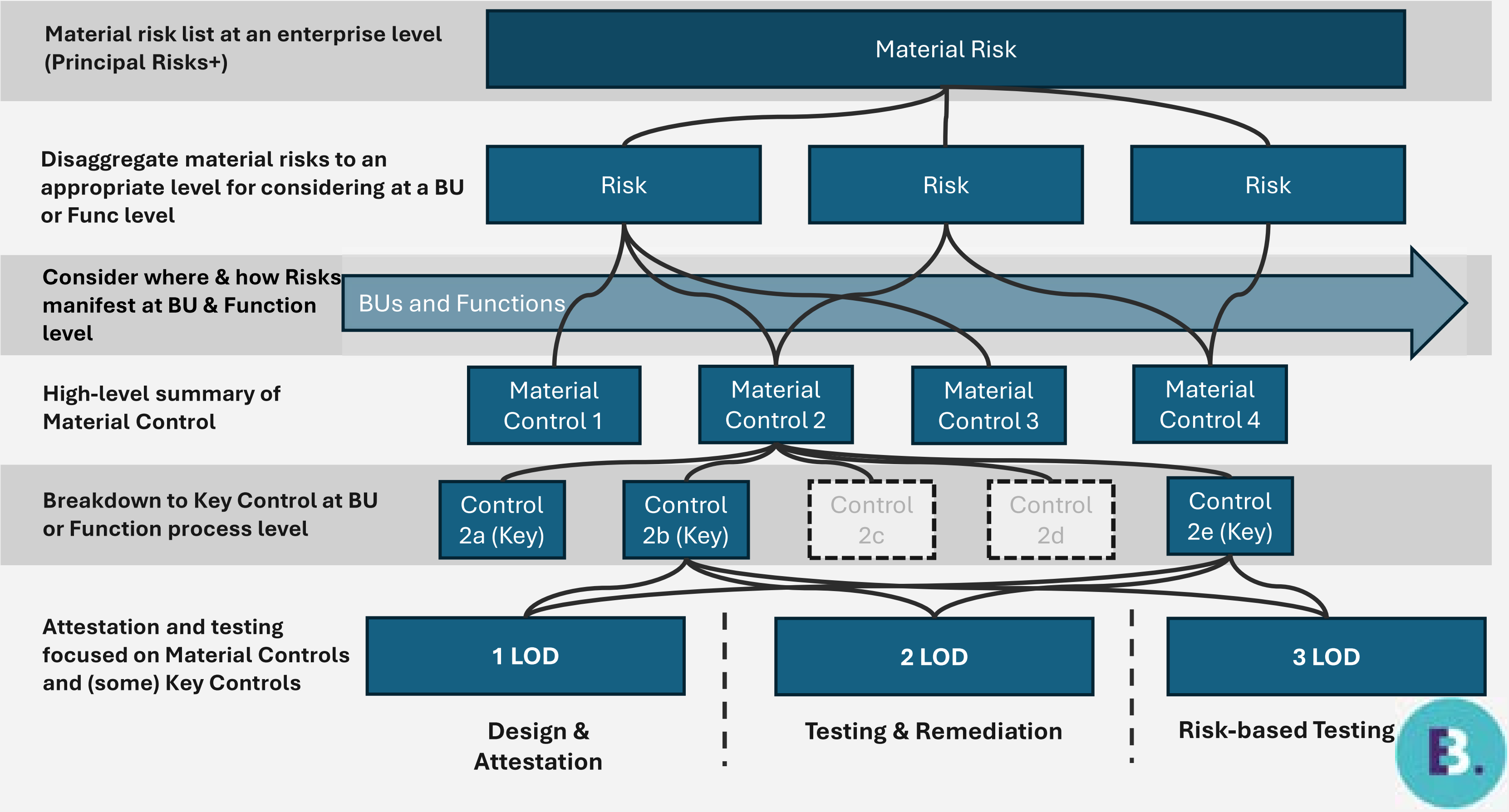
What will constitute material controls?

- Potential categories of material control
  - Elevated ‘Key’ Controls - ‘Dip down’ into individual key process-level controls
  - Entity Level Controls - Organisation-wide controls that establish a pervasive control environment
  - Cluster Controls - Groupings of controls (prevent, detect, compensating) monitored by an executive committee or risk owner
  - Frameworks - A specialised subset focused on a specific principal risk (likely to be a mature control area)

Who provides the assurance?

- What's Internal Audit's role?
  - Oversight and advice; not the arbiter
  - Optimising the 1st-Line; Organising the 2nd-Line (Assurance Maps)
  - As much focus on how the business effectively enables monitoring and review as on the year-end declaration

Identifying material controls through ‘Elevated Key Controls’ approach



Material risk list at an enterprise level (Principal Risks+)

Material Risk

Disaggregate material risks to an appropriate level for considering at a BU or Func level

Risk

Risk

Risk

Consider where & how Risks manifest at BU & Function level

BUs and Functions

High-level summary of Material Control

Material Control 1

Material Control 2

Material Control 3

Material Control 4

Breakdown to Key Control at BU or Function process level

Control 2a (Key)

Control 2b (Key)

Control 2c

Control 2d

Control 2e (Key)

Attestation and testing focused on Material Controls and (some) Key Controls

1 LOD

2 LOD

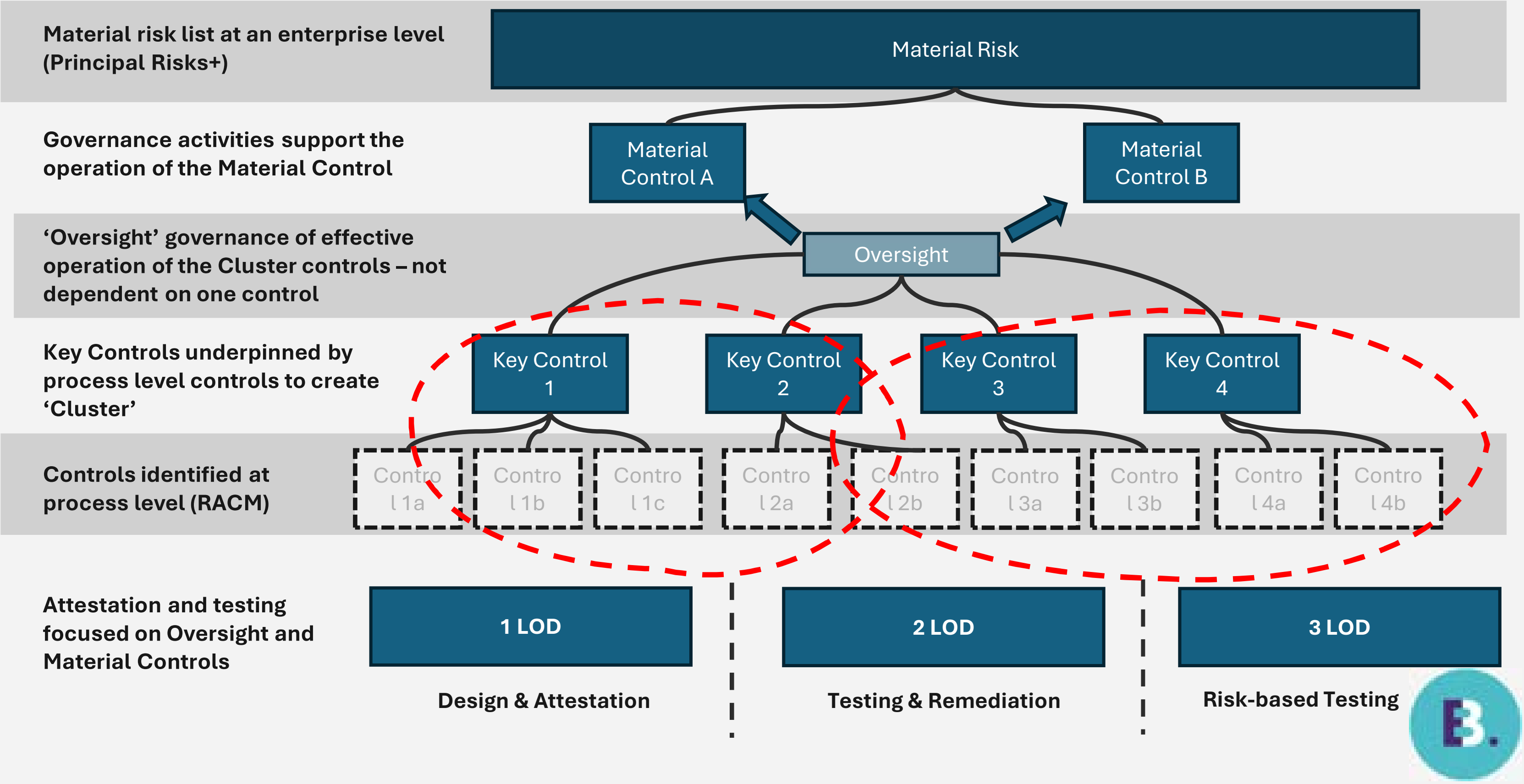
3 LOD

Design & Attestation

Testing & Remediation

Risk-based Testing

Identifying material controls through 'Cluster Controls' approach



Material risk list at an enterprise level (Principal Risks+)

Governance activities support the operation of the Material Control

'Oversight' governance of effective operation of the Cluster controls – not dependent on one control

Key Controls underpinned by process level controls to create 'Cluster'

Controls identified at process level (RACM)

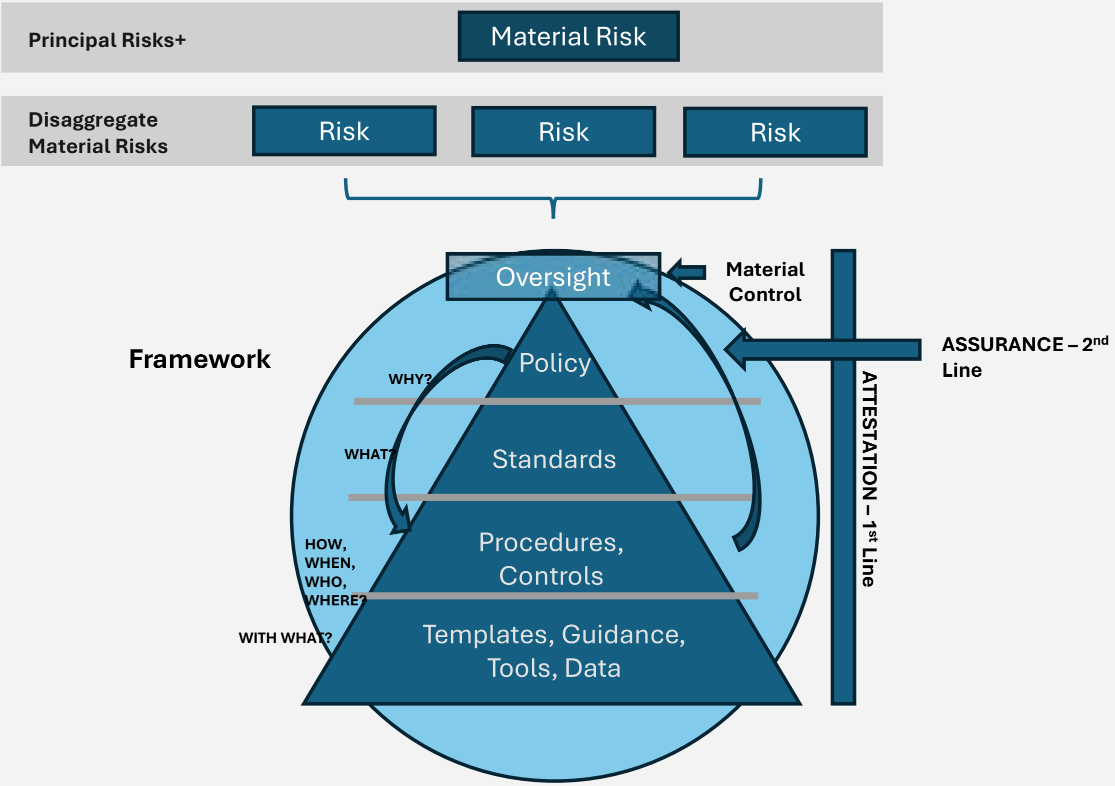
Attestation and testing focused on Oversight and Material Controls

Design & Attestation

Testing & Remediation

Risk-based Testing

Identifying material controls through ‘Risk Frameworks’ approach



- Activity can focus initially on areas of the business critical to the delivery of the objective and mitigation of the material areas of risk
- Effectiveness of the Oversight control is dependent on the ability of the control owner to receive data on the framework’s operation
- Framework control operates above other key controls but is not dependent on the effectiveness of any one individual control
- Ideally built on codifying existing practices
- Likely to mature over time
- Oversight should be at an appropriately senior level of management or committee

Assurance at Deliveroo

- Deliveroo was founded in 2013 by Will Shu and Greg Orlowski
- We IPO’d in April 2021, but retain entrepreneurial and growth culture
- We’ve been focusing on developing our control framework for UK Corporate Governance Code Compliance and Provision 29
- Takeover by DoorDash (US listed) likely to complete in October 2025
- Separate Internal Audit and Risk teams combined into the Assurance team in September 2023

Working across 2nd & 3rd lines of defence

- Highly collaborative relationship between Risk and IA team - no barriers or sensitivity about ownership

- Strong "pull" from the business for support. Who is best placed to perform the work? What's right for the business?

- Joint projects where the skillsets are complimentary

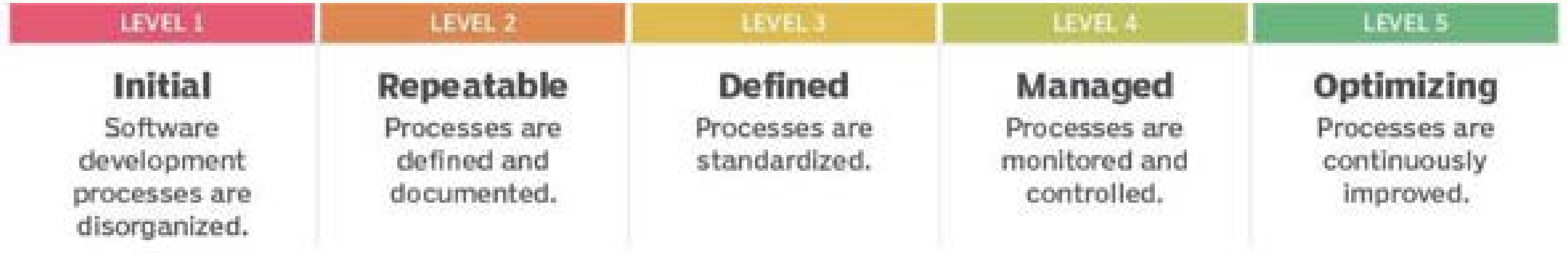
- Maintaining an objective mindset is more important than functional independence

Working with the business

- All work starts with our Principal Risks, risk appetite and target control maturity as set by the Executive
- Highly collaborative/trusted approach with the business, with engagement via key committees/working groups and full transparency both ways expected
- Focus on “framework audits” to help drive increasing control maturity
- Work with agility and pace - we land findings and actions early in our audit process to help get these fixed quickly
- Give credit where it’s due - e.g. where management have already identified improvements or taken prompt action we make sure this is recognised in our reports

Framework audits - NIST

Principal Risk (ARA)	Risk Appetite (ARA)	NIST Domain	Maturity Target	Management Assessment	Internal Audit assessment	
					2024	2025
Cyber Security	Critically Low	Identify	*Numerical target for each domain, aggregated from individual control scores*	*Management's self assessment of maturity across each domain (not shared with IA until post-audit)*	*We track progress across each domain year on year, as well as where controls are ahead/behind management's expectations.* *Regardless of the maturity target, we identify improvement actions for prioritisation by management across each domain and control.*	
		Protect				
		Detect				
		Respond				
		Recover				



LEVEL 1

Initial

Software development processes are disorganized.

LEVEL 2

Repeatable

Processes are defined and documented.

LEVEL 3

Defined

Processes are standardized.

LEVEL 4

Managed

Processes are monitored and controlled.

LEVEL 5

Optimizing

Processes are continuously improved.

QUESTIONS

ICAEW