tapestry NETWORKS

EACLN SUMMARY OF THEMES

AI, cybersecurity, workforce dynamics, corporate regulation, and investor relations

December 2025

On December 3-4, the European Audit Committee Leadership Network met in London for the following sessions:

- **Navigating AI governance** with Tim Hickman, partner, White & Case
- **The impact of AI on the workforce** with Jim Moore, senior operating adviser, TDR Capital
- **Cybersecurity: maintaining preparedness** (members-only)
- **The European corporation in the 21st century** with John Kay, Fellow, St John's College, University of Oxford
- **Europe's regulatory balancing act** (members-only)
- **Dialogue with Jen Sisson,** CEO, International Corporate Governance Network

For a list of meeting participants, see Appendix 1 (page 12).

This *Summary of Themes*[1] provides an overview of the following discussions:

Navigating AI governance

"Governance is always evolving. It's not a one and done exercise," said a member. AI activities, regulation, risk, and technology are evolving faster than governance frameworks can adapt. Members met with Tim Hickman to explore practical approaches and good practices on oversight of AI in a shifting landscape. Key themes emerged:

- **Strong foundations are the key to responsible AI use.** Effective oversight is rooted in clear principles, disciplined processes, and a shared view of where AI creates value and where it introduces risk. Mr. Hickman emphasized *"progress over perfection.*" The group surfaced elements critical to a strong foundation:
  - **Developing an inventory of the company's AI tools.** Mr. Hickman noted that one of the greatest challenges of governance over AI is understanding what AI tools are being used in the company. "Shadow AI," or informal and often unauthorized use, makes creating an inventory difficult. And because there is no clear definition of "regulated AI," drawing boundaries can be challenging.
  - **Embed AI into existing control frameworks.** Fragmented, narrow regulations make effective oversight difficult and risk a siloed approach. UK members highlighted new requirements in Provision 29 of the revised UK Corporate Governance Code requiring an annual declaration over the effectiveness of internal controls. They noted that this will be complicated if controls associated with AI are included.
  - **Ownership and accountability must be unambiguous.** As systems grow more autonomous and complex, boards and management must ensure that responsibility for decisions, oversight, and outcomes are clearly defined. *"Especially now with agentic AI, it is becoming harder to assign 'owners' to the agents*," said a member.
  - **Understand risk tolerances globally.** Trust and usage of AI vary globally, influenced

Definition of AI

Article 2 of the EU AI Act sets out the scope of the Act and explains which providers, deployers, and other regulated roles fall under its rules. Article 3 defines core terms, including "AI systems." Very broadly, such systems must:

- Be machine-based
- Be designed to operate with some level of autonomy
- Infer from inputs to generate outputs (e.g., predictions, content, or recommendations)
- Impact physical or virtual environments

Mr. Hickman explained that this broad and principles-based definition of "AI systems" could include unintended technologies and tools—for example, the spelling checker in a word processing application.

by culture, regulations and media. Understanding where the risks are, and tailoring deployment strategies that focus on regions where the use of AI is more advanced (and accepted) will help build trust.

- **The complexities of evolving regulations add challenges.** *"Regulation is not driving harmonization,"* said a member. Several implications surfaced:
  - **A moving regulatory target.** Enforcement of the main provisions of the EU AI Act that deal with AI systems begins in August 2026, though a new Digital Omnibus Package could simplify some of its provisions. *"It's too hard to get on top of all the reporting obligations, especially as they are changing—doing business in Europe is getting too hard*," said a member. Other jurisdictions remain in "wait-and-see" mode, adding uncertainty for multinational governance.

Deciphering the EU AI Act

Mr. Hickman pointed to White & Case's *EU AI Act Handbook*[2] for a detailed breakdown of the regulation, including commentary and practical examples.

  - **Data provenance is becoming a core compliance obligation.** The EU AI Act raises expectations for traceability and lawful sourcing of training data. Audit committees should insist on documentation that clearly demonstrates where data comes from and how it is used, especially for systems built with or deployed on EU-origin data.
  - **Managing the privacy of data can be arduous.** When external AI models are used, such as in software-as-a-service applications, it is critical to know how vendors who run the models will use the data, since they may be subject to different laws and regulations. Even terms such as "training" AI models using corporate data may create unknown risks: smaller companies supplying these tools may have inadequate governance and oversight. *"Indemnities don't automatically mean you are protected*,' noted Mr. Hickman. *"This is still a new area and everyone is looking to push liability elsewhere*," he added. Employees using "shadow" AI can further expose a company's data.
  - **Assurance for AI models is a developing art.** *"AI does something different every time so it's hard to audit*," said a member. One member encouraged the use of internal audit when deploying AI, but another said that it is very difficult to sign off on an algorithm.
  - **Contradictory regulations can create unavoidable sovereignty conflicts.** Laws such as the CLOUD Act allow US authorities to access data held by US cloud providers even when that data is stored in the EU, creating tension with EU data protection and sovereignty rules. With few practical solutions available today, audit committees should understand their exposure and risk tolerance, scrutinize hosting and provider ownership choices, and ensure viable exit or mitigation strategies are in place.
  - **Penalties are headline-grabbing, but early enforcement will be slow.** As with GDPR,

large fines will likely take years as regulators develop theories of harm. *"Approaches to enforcement are also inconsistent, even within countries*," noted Mr. Hickman. Boards should focus on avoiding press exposure, settling complaints where appropriate, and developing defensible, risk-appropriate compliance strategies.

- **Operational discipline will help contain real-world AI risks.** Discussions highlighted:
  - **Shadow AI is a growing and under-recognized exposure.** *"Studies on the extent of shadow AI in companies are frightening,"* said an EY leader. Without sanctioned tools, employees turn to unsupervised ones. Boards should pair policies with enablement, monitoring, and controls to reduce unauthorized use and data leakage.
  - **Dependence on hyperscalers creates concentration risk.** European alternatives are still maturing. Audit committees should oversee resilience testing, multi-region hosting, and exit strategies from specific providers.

The impact of AI on the workforce

One of the most debated aspects of AI—and among the most consequential for society—is its workforce impact. Boards are grappling with how automation, augmentation, and new operating models will reshape jobs, skills, and communities. Members met with Mr. Moore to explore these questions, examine emerging evidence, and consider how audit committees should weigh the risks and opportunities of increasing AI adoption. *"One thing is clear – nothing is certain. There is a spectrum of plausible outcomes. There will be some short-term pain, and the benefits will come, but only later*," said Mr. Moore. Several observations were made:

- **AI job displacement is a short-term risk.** Mr. Moore advised members to think about what is possible with today's technology, and use that to identify the risks. Members debated whether AI-driven job loss should be treated as a systemic risk akin to pandemics or cyberattacks. The consensus: workforce scenarios need to be built directly into enterprise risk planning, not treated as a HR issue alone.
- **Near-term workforce disruption is already underway.** AI is rapidly automating repeatable tasks and shrinking call-center, software, and back-office roles. Mr. Moore provided an example where a small booking center deployed an off-the-shelf AI assistant: *"On day one it handled 70% of calls, providing service with a higher Net Promoter Score. The team went from 40 people to 10 almost overnight."*
- **Societal impacts may be severe.** Job loss concentrated in specific hubs—such as call center or outsourcing regions—may have cascading economic effects. As Mr. Moore noted, *"Imagine a town where 10% of the residents work in call centers—think what a big cut means for the restaurants and local economy."* He stressed the importance of considering the community impact, reputational exposure, and social footprint of large-scale automation. Members discussed how companies needed to establish reskilling and retraining programs;

employees may need to reciprocate with greater adaptability and a stronger work ethic.

- **Reskilling and education must evolve without delay.** *"You can't stop the jobs going away, but the right answer is transitioning the workforce in a way that moves people on quicker*," said Mr. Moore. As an EY leader put it, *"The best protection against AI is AI."* Members also discussed challenging management on readiness and measurable progress.
- **Ethical and cultural risks rise as AI reshapes work.** Bias, fairness, and cultural adaptation were flagged as material concerns. Members encouraged embedding ethical guardrails in governance and people processes—and ensuring that accountability for responsible use is clearly understood as more people are upskilled in this area.
- **Regulation will also shape the pace and boundaries of workforce change.** Global AI rules remain fragmented, and enforcement is uneven. Members noted the need to stay alert to regulatory developments and ensure the company's AI strategy can adapt as legal expectations evolve.

Cybersecurity: maintaining preparedness

"It's going to happen; how can you minimize impact?" said a member. Recent incidents at Jaguar Land Rover, Marks & Spencer, and Asahi underscored the destructive potential of attacks on operations. Even well-established companies can face shutdowns, data compromise, and real-time tests of board readiness.

In this members-only discussion, several themes emerged:

- **Education and awareness remain the most effective defense.** Basic cybersecurity literacy—such as recognizing suspicious emails—is still essential. Continuous training is critical, and contractors and third parties must be held to the same standards.
- **Audit committees must stay skeptical and proactive.** Members emphasized:
    - Seeking assurance beyond dashboard indicators. Cyber reports often offer abstract benchmarks and an abundance of *"green lights"* without clarifying whether the company can genuinely respond when an incident occurs. Boards should dig deeper, pressing for key performance indicators that demonstrate defense and control effectiveness and for reports that indicate practical readiness, not just conceptual performance.
    - **Identifying priority areas.** Audit chairs emphasized the value of selecting a few priority cyber risks for deeper review. One described focusing next year's internal audit on major third-party suppliers—creating a dedicated team to assess their cyber awareness and defenses and determine whether gaps in ERM signal a broader preparedness issue.
    - **Understand the organization's risk tolerance.** Cyber risk can never be fully eliminated, making clarity about acceptable exposure essential. One member noted: *"In the real world you have to think in terms of risk tolerance, because the risk is never*

going away."

- **Using established frameworks to assess cybersecurity maturity.** A range of well-regarded frameworks can help an organization benchmark and strengthen its cybersecurity posture. Members pointed to NIST as a helpful reference point for evaluating controls and guiding improvement.[3]
- **Keeping pace with evolving risks.** Members noted increasing confidence in their cybersecurity understanding and ability to ask the right questions but emphasized the need to refresh knowledge as threats evolve, citing areas like quantum technologies. As one cautioned, *"What we're doing today may not be enough."*

Top cybersecurity concerns

Members identified the threats that are top of mind:

- **Third parties.** Even trusted partners require scrutiny; as one member warned, *"The people we take for granted and automatically trust—we need to be wary of that."*
- **Social engineering.** Attackers exploit human trust—duping or bribing employees to click, share, or improperly grant access. With many functions now offshored, one member noted, *"Life-changing sums are smaller than in big cities."*
- **Unauthorized software**. *"So many people think they're doing the best thing—something cheaper—so they use it. But they create risks they don't see at the local level for the entire enterprise,"* said a member.

- **End-to-end readiness requires a renewed emphasis on resilience, response, and recovery.** Members noted that while companies have historically invested heavily in identification and detection, the real differentiator now lies in how effectively organizations withstand, contain, and rebound from attacks. They highlighted several practices:
  - **Focusing on the "absolute criticals."** Resilience efforts shouldn't attempt to cover everything. Companies should focus on the few assets the business truly cannot function without.
  - **Testing detection through regular red-team exercises.** Members stressed that true capability is revealed only when adversaries are allowed *"inside the system."* Red-team exercises help determine how quickly the organization detects intrusions, exposes blind spots, and builds learning over time.
  - **Defining acceptable downtime and recovery expectations.** Boards need to determine in advance how long critical operations can be offline and how quickly recovery must occur.
- **Preparing for the legal and regulatory realities of a cyber incident.** Members raised several considerations:

- **Early coordination with law enforcement strengthens incident response.** Companies benefit from establishing relationships with police and specialist cyber agencies before an attack—aligning on reporting expectations, investigation processes, and points of contact.
- **Setting a pre-incident ransom policy.** Boards should discuss ransom decisions before an attack occurs: legal constraints across jurisdictions, ethical considerations, risk appetite to pay a ransom, and operational needs – for example, holding cryptocurrency.
- **Using law-enforcement interactions as a signal of cyber maturity.** *"A question I always ask when joining a company is: When did security services last call about an intrusion?"* said a member. *"If they're calling the company, it's a red flag about the organization's capabilities."*

- **The right balance in cybersecurity investment is a critical strategic choice.** Key themes included:
  - **Pushing cyber maturity before an incident becomes a significant investment.** Companies often aim for *"good enough"* until a breach forces rapid escalation. The challenge for boards is how hard to press management to invest earlier.
  - **Mutual insurance models can strengthen collective resilience.** One member described a mutual cyber insurance arrangement that encouraged transparency, information sharing, and aligned incentives across participating companies.
  - **Integrated IT systems can widen the blast radius.** State-of-the-art, tightly integrated IT systems offer efficiency but may give attackers broad access once inside. More fragmented architectures can limit exposure.
  - **Strong cybersecurity leadership is a high-value investment.** Good cybersecurity requires strong, experienced leadership, which is costly. As one member observed, *"You'll never know the value of the CISO because if they're good at their job, you'll never have to pick up the pieces."*

> "You'll never know the value of the CISO because if they're good at their job, you'll never have to pick up the pieces."
>
> —EACLN member

The European corporation in the 21st century

The nature of the corporation has changed more in the past two decades than in the previous century. As John Kay emphasized in *The Corporation in the 21st Century*, today's most successful firms no longer resemble the vertically integrated enterprises around which traditional governance models were built.[4] Instead, they operate as orchestrators of vast, distributed ecosystems—blending owned, outsourced, and digitally enabled capabilities in ways that challenge inherited assumptions about control, responsibility, and value creation.

Members met with Mr. Kay to explore shifts in corporate architecture, competitive positioning, governance, and the future of work. They surfaced the following themes:

- **Modern corporations compete on the quality of the ecosystems they orchestrate.** Mr. Kay emphasized that what now differentiates leading firms is their ability to integrate specialized partners, mobilize knowledge flows, and coordinate novel, hard-to-replicate capabilities at speed. Success, he said, is about combining novel and difficult-to-reproduce collections of capabilities.
- **Europe is not capitalizing on its structural strengths in the modern corporate model.** Despite strong traditions and networks, Europe has lagged in high-growth sectors due to limited focus on high tech, capital market norms that favor quick exits, and restrictive regulations. Talent and investment have shifted toward finance and consulting, weakening the region's innovation base.
- **Human relationships remain central to innovation and corporate resilience.** *"People do better together*," said a member. Breakthrough ideas emerge from informal interactions, shared experiences, and tacit learning; in-person collaboration is uniquely effective, making it essential that hybrid models preserve space for unstructured, face-to-face connection.
- **Cultures that encourage curiosity outperform those fixated on targets.** Mr. Kay advised companies to focus on creating great business rather than shareholder value. History shows that when companies shift from mission-driven strategies to narrow financial targets, resilience and innovation suffer. Drawing on his principle of obliquity, he emphasized that complex outcomes—innovation, adaptability, long-term performance—are often best achieved indirectly through cultures that encourage exploration, curiosity, and purposeful work rather than rigid profit metrics.[5] He noted that profitable companies are not typically the most profit-oriented—they give people the opportunity to innovate.

Europe's regulatory balancing act

The expanding scope and complexity of European Union initiatives aimed at fostering long-term value and embedding sustainability across sectors are significantly increasing demands on audit committees. Evolving regulatory expectations and frequent changes make compliance increasingly challenging. Furthermore, Europe's regulatory framework often conflicts with global regulations in areas such as sustainability and AI.

Top of mind for members currently are their first experiences with the EU Corporate Sustainability Reporting Directive (CSRD). Several themes emerged from the discussions:

- **Compliance is overshadowing strategic value in sustainability reporting.** *"CSRD reporting is counterproductive—so bureaucratic. The compliance focus causes misalignment between what the organization wants to achieve and reporting,"* one audit chair said. Members are pressing management for disclosures that reflect strategic priorities and

deliver value beyond regulatory box-checking.

- **First-year CSRD implementation exposed the need for simplification and automation.** Members described 200+-page reports and labor-intensive data gathering. The priority for the next report is to streamline—automate data collection, clarify accountability, and use clearer formats such as infographics to reduce preparatory burden, improve insights, and make it more readable.
- **Assurance expectations remain unclear and uneven.** *"Nobody has asked for reasonable assurance other than the regulator,"* noted a member. Assurance remains constrained, driven mainly by regulators and remuneration-linked KPIs. Members noted growing pressure from auditors and regulators in some jurisdictions, but voluntary assurance is still rare.
- **Regulatory divergence is draining resources and complicating compliance.** A patchwork of global standards—CSRD in Europe, fragmented US rules, mandatory sustainability reporting in China, Japan, the UK, South Africa, and others, and culturally varied enforcement—creates operational strain for global companies and uncertainty. Strong regulatory scanning and more proactive engagement are essential to avoid misalignment and compliance surprises.
- **Inclusion rules are colliding across jurisdictions.** Europe's mandatory diversity, equity, and inclusion (DEI) reporting sits uneasily alongside US legal restrictions, creating operational and reputational complexities, in particular for dual-listed companies. A principle-based global approach—focused on values over numeric targets with careful articulation of published policies and actions—may help maintain coherence across conflicting regimes.
- **Governance fatigue is mounting as new standards accumulate.** Upcoming mandates—country-by-country tax reporting, IFRS 18 "Presentation and Disclosure in Financial Statements", ISSB standards—add to already stretched teams. Prioritization and clarity on what truly adds value will be essential as regulatory expectations continue to expand.

Dialogue with Jen Sisson, International Corporate Governance Network

The International Corporate Governance Network (ICGN) is an association formed primarily of institutional investors, aimed at promoting better corporate governance. Members met with Jen Sisson, ICGN's recently appointed CEO, for a candid discussion on how investor expectations are reshaping governance practice. In a landscape where scrutiny is rising and trust is increasingly hard-won, Ms. Sisson offered perspectives on how boards can strengthen dialogue, demonstrate good governance, and navigate evolving investor dynamics. Key themes included:

- **Governance must go beyond compliance.** Boards often default to "comply" rather than "explain," hesitant to articulate judgment-based decisions. Ms. Sisson stressed that

governance is a strategic, ongoing responsibility—not a compliance checklist—and that thoughtful explanations can work, as long as your investors agree with the rationale.

- **Significant dissent is the real signal—and calls for listening and response.** Boards often interpret anything short of 100% support, such as on a say on pay vote, as a setback. Ms. Sisson emphasized that 90% approval can be a good outcome; unanimity is neither expected nor realistic in all cases. But, she noted, significant dissent should be viewed as a prompt for constructive dialogue: *"It is important to listen and respond to the views of your shareholders."*
- **Investors focus on audit quality more than on fees.** Most investors do not believe audit fees are excessive; in fact, reduced fees can raise concerns that an audit is under-resourced. For sustainability reporting, where processes are less mature, investors care about the credibility, rigor, and transparency of assurance.
- **Engagement remains a priority on both sides.** Several themes emerged:
  - **Mutual inertia hinders dialogue on audit.** Institutional investors rarely initiate conversation with audit chairs unless there is a problem; boards often hesitate unless required to engage. Ms. Sisson said, *"If you want to have a dialogue with investors, you have to proactively reach out to them and invite them in."*
  - **Audit reporting frameworks contribute to a widening trust gap.** Current regimes often create a closed loop: *"The board and management say everything is fine, and the external auditor says everything is fine—so what is there to talk about?"* said Ms. Sisson. This limits insight, leaving investors with few hooks to drive engagement and reinforces skepticism.
  - **Contentious issues require early, proactive engagement.** Too often, boards wait until dissent materializes. *"If boards seek to gain support for contentious issues, they must proactively engage with investors,"* Ms. Sisson said.

What should investors be asking audit chairs?

When Ms. Sisson asked members what questions *they* would expect from investors, several themes emerged:

- Cyber risk and third-party dependencies
- People, culture, and talent resilience
- Confidence in the management team

How investors read board culture

Ms. Sisson noted key signals:

- **Composition and skills mix.** Diversity of gender, geography, and expertise—supported by a transparent skills matrix—helps investors assess whether the board brings balanced perspective.
- **Responsiveness.** Stewardship teams often have only days to make voting decisions; delayed or limited access is a red flag.
- **Access to independent directors.** Reluctance to make them available signals weak board openness and accountability.
- **Combined CEO-chair role.** Investors frequently view this structure as diluting independent oversight.
- **Quality of disclosure and board-effectiveness reviews.** Thoughtful, candid disclosure, versus boilerplate, signals a board willing to reflect honestly on its performance and culture.

Appendix 1: Participants

The following members participated in all or part of the meeting:

Philip Broadley, AstraZeneca

Christine Catasta, Erste Group Bank

Liz Doherty, Novartis and Philips

Byron Grote, IHG

Margarete Haase, ING

Monika Kircher, RWE

Dagmar Kollmann, Deutsche Telekom

Benoît Maes, Bouygues

René Medori, Vinci

David Meline, ABB and HP Inc.

Anne-Françoise Nesmes, Compass Group

Gordon Orr, Meituan

Dessi Temperley, Coca-Cola Europacific Partners

The following members participated virtually in part of the meeting:

Laurence Debroux, Novo Nordisk, Exor, and Randstad

Teresa García-Milá Lloveras, Repsol

Frank Witter, Deutsche Bank and Traton

EY was represented by the following in all or part of the meeting:

Marie-Laure Delarue, Global Vice-Chair, Assurance

Hildur Eir Jónsdóttir, Assurance Managing Partner, Spain

Bridget Walsh, EMEIA Area Managing Partner

The following Tapestry Networks representatives participated in all or part of the meeting:

Beverley Bahlmann, Executive Director

Thomas Crampton, Senior Advisor

Jonathan Day, Chief Executive

Laura Koski, Project and Event Manager

Todd Schwartz, Executive Director

Hannah Skilton, Senior Associate

Endnotes

[1] *Summary of Themes* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from members and guests in connection with the meeting but may be edited for clarity.

[2] White & Case, *EU AI Act Handbook*, 2025.

[3] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST Cybersecurity White Paper (CSWP) No. 29, February 26, 2024.

[4] John Kay, *The Corporation in the 21st Century* (Oxford: Oxford University Press, 2023).

[5] John Kay, *Obliquity: Why Our Goals Are Best Achieved Indirectly* (London: Profile Books, 2010).