Redefining Cyber Readiness: Best Practices for Effective Governance

As cyber threats grow more complex and interconnected, the UK Government's new Cyber Governance Code of Practice reinforces that cyber risk is no longer just an IT issue, it's business imperative. This session, led by Ashurst's legal and cyber risk experts, broke down the Code's implications for boards and business leaders, highlighting actionable ways to integrate cyber risk into enterprise governance, enhance organizational readiness, and build resilient incident response frameworks.

Key Takeaways

1. **Cyber Risk Governance Must Start at the Top**

   Boards must align cyber risk with enterprise risk strategy, assigning clear ownership at the senior level and regularly revisiting risk appetite. Effective governance includes mapping critical assets, managing third-party risks, and embedding cyber discussions into business oversight.

2. **Avoid "Zero Tolerance" Pitfalls by Setting Realistic Risk Parameters**

   Many organizations fall into the trap of vague or overly rigid cyber risk postures. Instead, define practical thresholds (e.g., maximum system downtime) and update controls continuously to reflect evolving threat environments.

3. **Build a Cyber-Aware Culture Across the Organization**

   Governance depends on company-wide awareness and accountability. Tailored, measurable training, based on roles and reinforced with feedback loops, helps elevate cyber literacy beyond the IT function and supports compliance with the NCSC toolkit.

4. **Test, Review, and Evolve Your Incident Response Plans**

   A strong response strategy includes flexible playbooks, clear authority lines, and regular simulations. Pre-approved third-party vendors, post-incident reviews, and ongoing board to CISO engagement ensures readiness when incidents occur, not just on paper, but in practice.