CITMA The Chartered Institute of Trade Mark Attorneys

Part C – Liability and compliance

Part C of this series explores the legal, contractual, and organisational responsibilities that arise when Trade Mark Attorneys and IP professionals adopt AI-based tools. Unlike technical or operational risks, liability and compliance concerns directly affect the firm's regulatory standing, professional duties, and exposure to legal claims. This section therefore provides a structured overview of the safeguards firms should implement to ensure that AI solutions are deployed in a controlled, responsible, and legally compliant manner.

The guidance covers five core areas:

- **Defined liability framework**
  A clear contractual allocation of responsibility is essential when procuring or deploying AI systems. Vendors should articulate, in unambiguous terms, which party is liable for errors, system failures, misinformation, data breaches, or other AI-related harms. This includes indemnification clauses, limitations of liability, service-level commitments, and obligations regarding system performance. Establishing these boundaries at the outset protects firms from unforeseen exposure and ensures that both parties understand their respective obligations.

- **Professional accountability**
  Although AI tools may support legal research, analysis, or decision-making, the responsibility for professional advice always remains with the qualified practitioner. Firms must ensure that internal policies, contracts, and training reinforce the principle that AI outputs are assistive rather than authoritative. This section emphasises the continuing need for human oversight, independent verification, and the safe integration of AI tools into regulated professional workflows.

- **Insurance requirements and verification**
  AI-related risks may not always be covered under standard indemnity insurance. Firms should verify that vendors hold adequate insurance that explicitly covers AI functionalities, including system errors, operational failures, cybersecurity incidents, and professional liability exposures. Reviewing the vendor's insurance protects the firm from assuming liabilities that the vendor is better placed to manage and demonstrates responsible procurement practices.

- **Compliance with legal, regulatory, and standards frameworks**
  AI outsourcing and usage must align with relevant laws, data-protection requirements, professional conduct rules, and emerging AI governance standards across all jurisdictions in which the firm operates. Vendors should be able to demonstrate compliance through documentation, certifications (such as ISO 27001 or ISO 42001), and routine regulatory updates. This section highlights the importance of assessing how a vendor monitors regulatory changes and maintains compliance over time, particularly given the rapid evolution of AI-related legislation.

- **Internal stakeholder engagement and firm-wide readiness**
  Liability and compliance are not purely legal considerations; they require collaboration across IT, Risk Management, Data Protection, Information Security, and Innovation Teams. Successful AI adoption depends on ensuring that internal stakeholders understand the risks, controls, and responsibilities associated with the tool they are using. This part of the document addresses the need for governance frameworks, internal approval processes, and ongoing monitoring to support safe and compliant use of AI across the firm.

Top 5 tips for liability and compliance

1. **Establish a clear and enforceable liability framework**
   Question whether AI vendors provide explicit contractual clarity on responsibility for system performance, errors, outages, or inaccurate outputs. Your Firm should ensure that contracts clearly define the allocation of risks, including indemnities for AI-related failures, breach of confidentiality, or misinformation generated by the system. A well-structured liability framework will protect both the firm and its clients by ensuring accountability is understood from the outset.

2. **Reinforce ongoing professional accountability for legal practitioners**
   Despite the increasing sophistication of AI tools, legal professionals remain fully responsible for the advice they provide. Firms should ensure that practitioners understand AI outputs as supportive aids, not substitutes for legal judgement. Contracts and internal policies should reflect that responsibility ultimately sits with the human professional, and that AI-assisted decisions must always be independently reviewed and validated.

3. **Verify vendor insurance coverage for ai-related risks**
   Vendors should maintain appropriate insurance that expressly covers the deployment and use of AI technologies, including errors, omissions, operational failures, cybersecurity incidents, and data breaches. Firms should request evidence of this insurance and confirm that coverage is adequate for the scale and nature of their intended use. The absence of relevant insurance can significantly heighten exposure to liability.

4. **Confirm ongoing regulatory and standards compliance across jurisdictions**
   AI vendors must demonstrate that they comply with relevant laws, professional standards, and emerging AI governance frameworks in all jurisdictions where the firm operates. This includes data protection regulations, sector-specific guidance, and internationally recognised standards such as ISO 27001 and ISO 42001. Ongoing compliance monitoring is essential, particularly as AI regulation evolves rapidly across different regions.

5. **Engage internal stakeholders early to ensure organisational readiness**
   Successful and compliant AI adoption requires input from IT Security, Risk Management, Data Protection, Innovation, and senior leadership teams. Early engagement ensures that legal, technical, and operational risks are properly

assessed and that appropriate controls, oversight mechanisms, and usage policies are in place. A coordinated approach strengthens compliance, reduces implementation risk, and supports responsible firm-wide deployment of AI tools.