CITMA The Chartered Institute of Trade Mark Attorneys

Part A – Trust & partnership assessment

Part A of this Top 5 series focuses on the foundational considerations that Trade Mark Attorneys and related IP professionals should evaluate when selecting and working with AI vendors. Trust is the cornerstone of any successful AI deployment, particularly in a profession where accuracy, confidentiality, and regulatory compliance are critical. As firms increasingly rely on AI tools to support decision-making, efficiency, and client service, ensuring that suppliers can demonstrate robust governance, transparent practices, and alignment with professional standards becomes essential.

This section provides a detailed framework for assessing whether an AI vendor can be regarded as a trusted and reliable partner. It expands upon several key themes:

- **Vendor credibility and transparency**
  Firms must be able to understand how an AI system functions, the data it relies upon, and the safeguards that govern its behaviour. Vendors should provide clear, accessible documentation covering training data sources, accuracy levels, performance testing, predictive limitations, and update procedures. Transparent vendors empower legal professionals to make informed decisions about how and when an AI tool should be used.

- **Long-term partnership potential**
  AI procurement should not be viewed as a transactional purchase. A sustainable relationship with the vendor requires ongoing dialogue, shared expectations, and responsiveness to regulatory and operational developments. Signals of a strong partnership include proactive communication, flexible support arrangements, and a willingness to adapt the system to sector-specific needs and risk appetites.

- **Data handling, confidentiality, and privacy**
  Given the sensitivity of client and matter data, firms must closely examine how vendors store, process, and protect information. This includes evaluating data isolation across clients and regions, reviewing whether inputs are used for model training, and ensuring that data retention and deletion procedures align with professional confidentiality obligations. A trustworthy supplier should be able to demonstrate compliance with all relevant data-protection requirements through verifiable policies and controls.

- **Governance, control, and monitoring**
  Robust governance structures underpin a reliable AI deployment. Vendors should provide systems that allow firms to monitor usage, access audit logs, assess risks, and review incident-response procedures. Certifications, technical documentation, and risk assessments further demonstrate that a vendor takes governance seriously and is committed to responsible AI practice. These elements give firms the visibility and assurance needed to deploy AI tools with confidence.

- **Sector familiarity and user-focused behaviour**
  A vendor's understanding of trade mark practice, professional duties, and regulatory nuances significantly influences the suitability of their product. Suppliers who recognise the importance of accuracy, confidentiality, and ethical practice within IP sectors are better equipped to support safe and effective AI adoption. A clear understanding of what IP practitioners need from a vendor; including responsiveness, clarity of communication, and a certain degree of flexibility, serves as an important indicator of whether a vendor will remain a reliable partner over time.

Together, these areas provide a holistic view of what makes an AI vendor trustworthy and suitable for long-term collaboration. This section aims to help firms conduct thorough, structured evaluations that go beyond technical features, ensuring that any AI solution is implemented within a relationship grounded in transparency, accountability, and shared professional values.

Top 5 tips for trust and partnership assessment

1. **Prioritise vendors who demonstrate a "trust-first" approach**
   Select AI suppliers who place governance, professional ethics, and risk management at the centre of their product development and client engagement. Trust-first vendors provide clear information about system limitations, maintain strong internal controls, and proactively address concerns around data handling and model behaviour. This mindset is often a more reliable indicator of long-term suitability than technical features or marketing claims.

2. **Assess the vendor's commitment to long-term partnership**
   Look for indicators that the supplier intends to build a collaborative, sustained relationship rather than completing a transactional sale. Strong partnership qualities include: willingness to understand your workflows and risk requirements; regular communication and review cycles; dedicated account support; and openness to adjusting or updating the tool as legal, regulatory, or operational needs evolve.

3. **Evaluate credibility and transparency through the "trust equation"**
   Apply a structured evaluation across four dimensions:

   - **Credibility** – clear documentation of data sources, training methods, performance metrics, and system limitations.
   - **Reliability** – proven stability, consistency of outputs, and transparent update processes.
   - **Sector familiarity** – understanding of trade mark and IP-specific considerations, including risk appetite, regulatory constraints, and professional duties.
   - **User-focused** – evidence that the vendor prioritises user safety, confidentiality, and control over commercial self-interest. This framework helps firms make an objective assessment of whether a supplier can be trusted with professional workflows.

4. **Verify data privacy, confidentiality, and isolation standards**
   Ensure the vendor (and any sub-processors) can demonstrate robust and compliant data-handling practices. Key questions include:

   - Will client or matter data be used to train shared models?
   - How is data isolated across clients, offices, and jurisdictions?
   - What encryption, retention, and deletion policies apply?
   - Is the supplier transparent about any third-party integrations? A trustworthy vendor should be able to provide detailed, verifiable information that aligns with your firm's confidentiality obligations and professional standards.

5. **Require evidence of transparent governance and oversight**
   A credible AI partner should support full visibility into how their system operates and how your use of it can be monitored. Look for:

   - audit logs and usage reporting
   - model cards or technical documentation explaining how outputs are generated
   - risk assessments, incident-response procedures, and regulatory statements
   - independently verified security or quality certifications Transparency enables firms to understand risks, maintain compliance, and demonstrate effective oversight to clients, regulators, and internal stakeholders.