EPIC
Insurance Brokers
& Consultants

GOVERNANCE AND RISK IMPACTS

AI, HR–IT Convergence and Governance Risk: What Boards and Executives Need to Know

Organizations across industries are increasingly blending HR and IT functions or formalizing Chief Human Resource Officer (CHRO) and Chief Technology Officer (CTO) "AI partnerships" to accelerate automation, workforce analytics, and talent-related AI use cases. This trend can enhance speed and innovation, but it also concentrates operational, cyber, and human capital risk in a small set of interconnected systems and leaders.

Boards, executives, and risk managers should evaluate the impact of this convergence on corporate governance, civil liability/regulatory risk, and risk transfer under traditional Cyber, EPL, D&O, and Commercial Crime policies as insurers attempt to adapt to these interconnected exposures.

Governance and Risk Impacts

AI use in HR and workforce management (e.g., hiring, promotions, performance management, insider threats, and internal mobility) introduces several governance challenges:

- Cyber and data privacy risk
  Unified HR–IT architectures often mean sensitive employee data, behavioral metrics, and performance information flow through AI-enabled tools, increasing the stakes of a cyber incident, data leak, or misuse. Inadequate governance over AI-model access, data retention, or third-party vendors can lead to privacy violations, regulatory investigations, and class action lawsuits.
- Employment practices liability (EPL) risk
  AI-driven recruitment, screening, and promotion tools can unintentionally create or amplify discrimination, bias, or disparate impact claims if not properly designed and monitored. Allegations of discriminatory algorithms, unfair hiring processes, or automated adverse actions may trigger employment practices liability exposure, e.g., applicants' discrimination claims against employers' improper use of AI hiring tools under federal and/or state civil rights law. However, it is important to note that EPL policies often limit or exclude coverage for regulatory claims, as well as civil and criminal fines and penalties.
- D&O and corporate governance risk
  Directors and officers may face scrutiny if they underinvest in controls, adopt AI strategies without appropriate oversight, ignore findings showing vulnerabilities involving technology platforms, do not safeguard employee access rights strictly aligned with job roles and revoked promptly upon departure, or fail to ensure the supervision of known model weaknesses, bias issues, cyber vulnerabilities, or regulatory non-compliance. Prevention increasingly supports the collaboration of officers charged with managing the workforce that uses the technology with officers charged with its implementation as it is increasingly embedded in day-to-day business operations. Given their interdependence, we expect plaintiffs will soon argue breach of fiduciary duty, misrepresentation of AI capabilities, or failure to implement adequate governance against those directors and officers who fail to govern human and technology risk holistically.
- Over- or under- governance of AI
  Too little governance elevates regulatory, cyber, and conduct risk, and excessive controls can drive "shadow AI" as employees adopt unsanctioned tools, creating unmanaged exposure. Effective governance balances innovation and control, with clear accountability between HR, IT, legal, and risk.

Implications for Risk Transfer and Insurance Markets

Carriers are starting to ask questions about AI primarily focused on governance. We have not seen questions focused specifically on HR-IT convergence yet, but we expect increased scrutiny around controls, governance, privacy, and oversight as adoption expands. Certain clients are beginning to anticipatorily address their coordination of HR-IT initiatives, particularly as it relates to research, testing, and implementation of AI tools because they see its importance to mitigate firm risks and manage its resources.

AI-related laws, claims, regulations, and private litigation theories are still evolving. As a result, liability standards (and loss scenarios) are not yet consistent or well established. The convergence of HR-IT, while potentially streamlining processes and improving efficiencies, has yet to be evaluated for the full risk.

Insurance follows established liability, so expect continued carrier questions and scrutiny as more organizations converge departments and as various claims and laws work through our legal systems.

Practical Steps for Boards and Executives

To manage governance risk and position your organization favorably with insurers, consider the following:

- Formalize AI governance across HR and IT
  Establish a cross functional AI governance structure (e.g., CHRO–CTO-led committee) that includes legal, compliance, information security, and risk management. Clearly allocate responsibility for model approval, monitoring, incident handling, and regulatory compliance.
- Map AI use cases and data flows
  Inventory AI use in HR and related systems (recruiting, performance, learning, internal mobility) and document data sources, vendors, and access rights. This helps identify concentrations of cyber risk, privacy issues, internal controls to mitigate improper fund diversion, and potential EPL exposure.
- Implement controls for bias, explainability, and human oversight
  Adopt documented processes to test for bias, maintain explainability where feasible, and ensure humans retain meaningful oversight of high-impact employment decisions. Periodic audits and clear escalation paths are critical.
- Align disclosures and board reporting with AI reality
  Ensure public or client-facing statements about AI capabilities and risk management are accurate and supported by internal controls, reducing the risk of D&O claims alleging misrepresentation or inadequate oversight.

Carriers are starting to ask questions about AI, primarily focused on governance.

- Review and update insurance risk transfer strategy
  Work with internal risk management and external advisors to review Cyber, EPL, D&O, Commercial Crime, and related insurance policies for AI-related gaps, exclusions, and limitations. Consider whether endorsements, enhanced wording, or additional insurance products are needed to address AI-specific exposures.
- Engage proactively with your insurance broker or advisor
  A knowledgeable broker or insurance advisor can help assess how AI-driven HR–IT convergence affects your risk profile, advise on insurer expectations, and negotiate appropriate coverage, limits, and terms in a rapidly evolving market. Early engagement is especially important for organizations where AI is central to strategy or operations.

Ready to be EPIC***?***

For more information about how EPIC can help your business, visit us at **epicbrokers.com**.