

AI Compliance in M&A:: Essential Due Diligence Checklist

1. Regulatory & Legal Compliance

- Identify applicable laws (EU AI Act, GDPR, HIPAA, SEC disclosure rules).
- Confirm AI system explainability and auditability.
- Review contracts for AI-related compliance obligations.
- Assess cross-border AI use and jurisdictional risks.

2. Governance & Risk Management

- Evaluate AI governance policies and accountability structures.
- Check for AI ethics frameworks (bias, transparency, fairness).
- Review internal AI risk assessments or audits.
- Verify incident response procedures for AI-related failures.

3. Data Management

- Ensure compliance with data privacy and security standards.
- Confirm data provenance and consent for training datasets.
- Assess data retention and deletion practices.
- Review cross-border data transfer mechanisms.

4. Technical Due Diligence

- Evaluate accuracy, reliability, and robustness of AI models.
- Test explainability tools and outputs.
- Identify use of third-party AI vendors or APIs.
- Confirm compliance with model monitoring and update practices.

5. Industry-Specific Requirements

- Healthcare: HIPAA + medical device AI rules.
- Finance: SEC disclosure + algorithmic trading oversight.
- Consumer/Tech: GDPR + digital services laws.
- Defense/Energy: Export controls + critical infrastructure standards.

6. Deal Impact Considerations

- Assess potential liabilities tied to AI systems.
- Evaluate reputational risks from AI misuse or bias.
- Review IP ownership of AI models and training data.
- Consider future regulatory costs in valuation models.

7. Post-Deal Integration

- Plan for harmonizing AI governance with acquirer's framework.
- Align ongoing compliance monitoring processes.
- Train staff on responsible AI use.
- Schedule periodic AI audits post-acquisition.