

AI Technology Stack Assessment Framework

Type: Assessment Framework

Target Audience: Enterprise Architects, AI Program Leads, Compliance

This framework helps document your full AI technology stack to identify concentration risks, data flows, and regulatory touchpoints across all layers of your AI infrastructure.

Layer 1: Hardware / Infrastructure

Component	Details	Regulatory Touchpoints
Data Centers	Location: _____	Data residency requirements
Compute Provider	<input type="checkbox"/> AWS <input type="checkbox"/> Azure <input type="checkbox"/> GCP <input type="checkbox"/> On-prem	Export controls
GPUs/TPUs	Type: _____	Chip restrictions
Key Vendors		Concentration risk

Layer 2: Platforms

Component	Details	Regulatory Touchpoints
Cloud Platform	Provider: _____	Terms of service, data handling
ML Platforms	Tools: _____	Vendor lock-in exposure
API Dependencies		Third-party risk

Layer 3: Models

Component	Details	Regulatory Touchpoints
Foundation Models	Models: _____	Licensing terms
Fine-tuned Models	Custom: _____	IP ownership
Training Data	Sources: _____	Data provenance

Layer 4: Applications

Component	Details	Regulatory Touchpoints
User-facing Apps	Applications: _____	Disclosure requirements
Data Flows	Where data travels: _____	Cross-border transfer

User Populations	Jurisdictions: _____	Extraterritorial reach
------------------	----------------------	------------------------

Regulatory Touchpoint Summary

Layer	EU AI Act	US Requirements	Other
Infrastructure	Data residency (GDPR)	Export controls	Data localization
Platform	Provider accountability	Vendor due diligence	Approved providers
Model	High-risk classification	Sector rules	Algorithm registration
Application	User disclosure	State laws (NYC, CO)	Content compliance

Key Assessment Questions

- ☐ Where is data physically stored and processed?
- ☐ Which jurisdictions does compute cross?
- ☐ Are there single points of failure?
- ☐ What are the data handling policies of vendors?
- ☐ Can we migrate if a provider changes terms?
- ☐ What are the licensing terms for each model?
- ☐ Do we own fine-tuned derivatives?
- ☐ Which jurisdictions do users reside in?

Organization: _____

Assessed By: _____ **Date:** _____