

EPMA

FORCE

12 NON-NEGOTIABLE REQUIREMENTS

The FORCE Executive Checklist for Enterprise AI
Procurement

**A board-ready summary of the controls every organization
should demand before allowing an outside AI provider to
learn how it thinks.**

No FORCE. No deal.

Version 1.0 | September 2026 | epmainc.com/FORCE

The board-level premise

	The risk Once an AI system begins learning an organization's decisions, customers, processes, communications, failures, and strategy, it becomes part of the organization's cognitive infrastructure. The procurement question is no longer only what the AI can do. It is whether the organization can inspect, preserve, govern, move, and operate without it.
--	--



GATE 1	GATE 2	GATE 3
Who controls the intelligence?	Can we keep operating?	Can we leave?

If the provider cannot satisfy all five pillars, treat the failure as the risk assessment.

The 12 requirements at a glance

#	Requirement	FORCE pillar	Minimum outcome
1	Defined Ownership and Control of Enterprise-Created State	F - Fiduciary Custody	The contract must identify every category of enterprise-created or enterprise-funded state and explicitly assign ownership, control, export, reuse, retention, and deletion rights.
2	No Secondary Use Without Explicit Authorization	F - Fiduciary Custody	Customer information must not be reused for training, model improvement, product development, benchmarking, advertising, or unrelated human review without specific and revocable authorization.
3	Sovereign Custody and Cryptographic Control	F - Fiduciary Custody	Sensitive AI workloads require control that is physical, operational, jurisdictional, and cryptographic - not data residency alone.
4	Model Version Pinning and Validated Baselines	O - Operational Continuity	A validated model performing consequential work must not be silently replaced by a materially different model.
5	Governed Change, Notice, Testing, and Rollback	O - Operational Continuity	Material behavioral, policy, alignment, capability, or safety changes are operational continuity events - not routine background updates.
6	Retirement, Service Continuity, and Provider-Failure Protection	O - Operational Continuity	The organization must have a continuity path if a model, service, provider, or contractual relationship ends.
7	Resilience Against Monoculture and Single-Provider Failure	R - Resilience Against Monoculture	Critical cognition must not depend on one provider, model family, identity plane, cloud, alignment policy, or inference path.
8	Least Privilege and Customer-Controlled System Boundaries	C - Control and Organizational Autonomy	AI systems should receive only the data, credentials, tools, network paths, and authority required for the approved task.

#	Requirement	FORCE pillar	Minimum outcome
9	Independent Audit, Incident Disclosure, and Evidence Preservation	C - Control and Organizational Autonomy	The customer must be able to investigate material incidents from preserved evidence rather than relying solely on the provider's characterization.
10	Nondelegable Responsibility and Contractual Liability Allocation	C - Control and Organizational Autonomy	"The AI acted autonomously" must not operate as a blanket defense against negligent design, integration, permissions, monitoring, or deployment.
11	Complete Cognitive Export and Functional Migration	E - Egress and Exit	Egress is the retrieval of assets. Exit is the ability to continue operating elsewhere. A data dump is not an exit plan.
12	No Punitive Exit and a Tested Exit Capability	E - Egress and Exit	The right to leave must be economically, technically, and operationally real - and proven before dependence becomes irreversible.



Architecture must match consequence

Workload category	Preferred architecture	Minimum governance posture
Public, reversible, low sensitivity	Controlled hosted AI	Standard access controls, logging, vendor due diligence, and data-use restrictions.
Internal productivity, limited sensitivity	Private enterprise tenant	Strong identity governance, least privilege, retention controls, monitoring, and tested fallback.
Trade secrets, regulated data, strategic decision support	Sovereign private cloud or on-premises	Customer-controlled keys, restricted networking, pinned versions, local evidence retention, and tested migration.
National security, critical infrastructure, crown-jewel IP	Customer-controlled on-premises; no external inference path; air-gapping where justified	Physical, operational, cryptographic, and legal sovereignty; independent continuity capability.

FORCE quick score

Score	Control maturity	Meaning	Board disposition
0	Unknown	No verified control or evidence.	Do not deploy.
1	Provider assertion	Policy statement or sales assurance only.	Treat as unmanaged.
2	Contracted	Contract language exists but has not been operationally tested.	Conditional; require testing.
3	Implemented and tested	Control works in the customer environment.	Deploy within defined risk tier.
4	Independently verified	Control is tested and independently reviewed.	Preferred for critical workloads.

Score each of the five FORCE pillars from 0 to 4. A critical workload should not proceed with any pillar below 3. A total score does not cure a zero in custody, control, or exit.

Decision rule

No workload should enter production until the organization can answer the relevant FORCE questions with evidence. Low-risk hosted use may be acceptable. Crown-jewel knowledge, regulated decisions, critical infrastructure, and national-security workloads require customer-controlled infrastructure, including on-premises or isolated operation where justified.

Legal and use notice

The FORCE Framework is an independent enterprise risk-management framework developed by EPMA. It is not an ISO certification, regulatory standard, legal opinion, or substitute for advice from qualified legal, cybersecurity, procurement, privacy, insurance, or regulatory professionals. Organizations should adapt the framework to applicable law, contractual obligations, sector requirements, and workload risk.

