Definition of Terms

Note: We are expanding the use of the 'Stack' label to keep the simple analogy for common understanding, but the word could be replaced with 'Pillars', 'Layers', or other descriptors.

We have learned that AI Sovereignty must look across four dimensions, each having a 'stack'. The dimensions are:

1. *Organization metric in the AI Ecosystem - the Business Sovereignty Stack*
2. *The AI and its supply chain - the Tech Sovereignty Stack*
3. *The AI pre or post deployment path, or Lifecycle - the Lifecycle Sovereignty Stack*
4. *The Controls and Mitigations to foreign dependencies - the Governance stack*

Business Sovereignty Stack

Definition: The degree to which an AI ecosystem participant operates independently from foreign influence across its organizational layers.

Configurable Metrics Layers:

Ownership & Funding: Is the company majority-owned and funded domestically?
Leadership & Governance: Are decision-makers based in Canada or the country of the assessing organization aligned with national interests?
Strategic Autonomy: Can the organization set its own AI roadmap without external constraints?
Legal Jurisdiction: Is the company subject to Canadian laws and oversight?
Operational Autonomy: Is there a contingency plan (i.e. technology alternative) in the event of vendor insolvency or new policy constraints?

Tech Sovereignty Stack

Definition: The extent to which the technical components of AI systems are developed, hosted, and controlled within national boundaries.

Configurable Metrics Layers:

Infrastructure: Are compute resources (e.g., cloud, servers) located in Canada?
Frameworks & Tools: Are core development tools open-source or locally governed?
Model Architecture: Are models built using transparent, auditable methods?
Deployment Pipelines: Is the deployment stack free from foreign control?
Security Protocols: Are cybersecurity measures aligned with national standards?

Lifecycle Sovereignty Stack

Definition: The control and transparency over the entire AI lifecycle—from data sourcing to model updates.

Configurable Metrics Layers:

Training & Testing Data: Is the data sourced ethically and stored within Canada?
Model Development: Are models built and tuned by Canadian teams or partners?
Usage & Monitoring: Is model usage tracked and governed locally?
Drift & Updates: Are updates managed in a sovereign, auditable way?
National Strategies: Is the deployed usage within relevant national interests (eg. Energy, dual-use)?

Governance Sovereignty and Mitigation Stack

Definition: The robustness of governance mechanisms that ensure AI strategy aligns with national values and mitigates external risks.

Configurable Metrics Layers:

Legislative Alignment: Are AI practices aligned with Canadian laws and directives?
Policy Framework: Are Internal policies designed to reinforce AI sovereignty by minimizing foreign dependencies and embedding national values.
Organization Governance: Are decision-making bodies, oversight mechanisms, and escalation paths in place to ensure sovereign control over AI strategy and operations.

Use Case Transparency & Reporting: Do AI use case include built-in sovereignty controls, such as data localization, ethical safeguards, and jurisdictional governance and are trust assessment scores and metrics publicly available?

Strategic Enablement: Does governance support long-term national AI competitiveness?