Scaling Trusted AI Across Defence: From Siloed Pilots to a Multi-Cloud Operating Model

Operating AI at scale in secure environments introduces complexities, particularly in multi-cloud settings. Defence has a unique opportunity to transform early, siloed AI pilots into a scalable, trusted, and responsible AI operating layer.

Key recommendations:

- Adopt a hybrid approach: Centralise governance, federate execution.
- Accept embedded vendor AI: Govern all AI through Responsible AI policies.
- Map all AI use cases to business processes and owners.
- Embed Responsible AI as non-negotiable.
- Invest in open, reusable, and interoperable architecture.
- Scale sustainably through a phased roadmap.

This roadmap aligns with Defence Data Strategy 2.0 and Defence Digital Strategy, prioritising decision advantage, secure data, and digital integration.

Context and challenges

Unifying fragmented AI pilots into a secure, trusted AI operating layer will enable Defence to reduce duplication, strengthen governance, manage embedded vendor AI, and ensure alignment with Defence strategies.

Risks of fragmented AI in a multi-cloud environment:

- Operational duplication
- Inconsistent governance
- Unmanaged embedded AI
- Regulatory and security exposure
- Cost inefficiency

A unified approach is essential for decision advantage and measurable value.

Principles for a unified AI operating layer

By grounding your AI strategy with principles, Defence can ensure that AI is deployed responsibly, efficiently, and sustainably across a complex multi-cloud environment. A unified AI operating layer is a secure, repeatable, and flexible foundation for RPA AI, Agentic AI, and Generative AI with the purpose of benefiting your stakeholders and the communities you serve.

Core principles that should guide the design of your unified AI operating layer:

1.
Centralised governance, federated execution

2.
Respect embedded vendor AI, govern it consistently

3.
Open, interoperable, and reusable

4.
Data-centric AI

5.
Responsible and ethical by design

6.
Align AI to business processes and owners

Balance central governance with federated execution for agility and control.

Considerations for multi-cloud AI platform design

There is no single "best" AI platform design. Success will come from applying a hybrid approach, which requires:

- Centralised governance and policy controls
- Federated design, development, and execution
- Oversight of embedded vendor AI

This will maximise your agility, maintain trust, and ensure your AI investments deliver measurable value for Defence, Ministers, and citizens alike.

Governance and risk management

For a large public sector like Defence, AI governance is not just a compliance task, it is the foundation for responsible, secure, and trusted use of advanced automation, Agentic AI, and Generative AI. As Defence's AI adoption grows, so too will the scrutiny around:

How data is collected, used, and shared across clouds.

How models make decisions that affect citizens, policy, or funding.

Whether Defence can prove it is using AI ethically and responsibly.

Governance must be proactive, practical, and enforceable, evolving as AI maturity grows.

Roadmap to establishing a unified AI operating model for a multi-cloud environment

Phase 1
Establish principles and governance foundations

Phase 2
Catalogue and map use cases

Phase 3
Design the unified AI operating layer

Phase 4
Deliver priority pilots and prove value

Phase 5
Scale and embed AI as a business capability

Each phase builds towards a sustainable, responsible, and scalable AI operating model.

Further Reading:

- DXC Responsible AI Framework
- DXC AI POV
- DXC AI Blueprint
- DXC Generative AI Services
- DXC Cloud and Infrastructure Services
- DXC Data and AI Services
- DXC Thought Leadership and Insights

Authors:

Paul Hyland
Partner, DXC Data & AI Practice
paul.hyland@dxc.com

Mohammad Siddique
DXC CTO for Defence
mohammad.siddique4@dxc.com

Get the insights that matter.
dxc.com/optin

About DXC Technology

DXC Technology (NYSE: DXC) is a leading global provider of information technology services. We're a trusted operating partner to many of the world's most innovative organizations, building solutions that move industries and companies forward. Our engineering, consulting and technology experts help clients simplify, optimize and modernize their systems and processes, manage their most critical workloads, integrate AI-powered intelligence into their operations, and put security and trust at the forefront. Learn more on **dxc.com**.