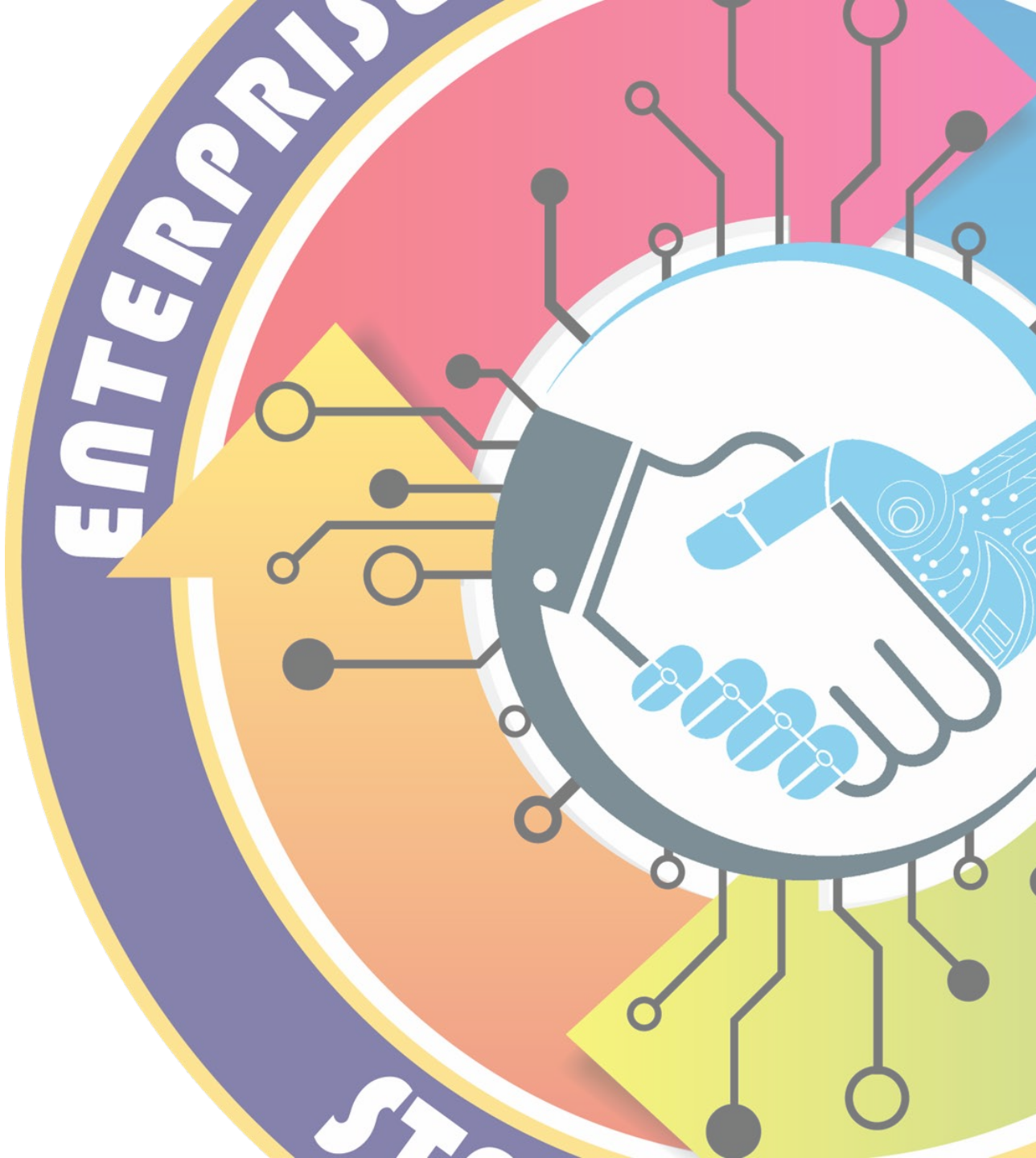
Hawaii Data Task Force Quarterly Meeting

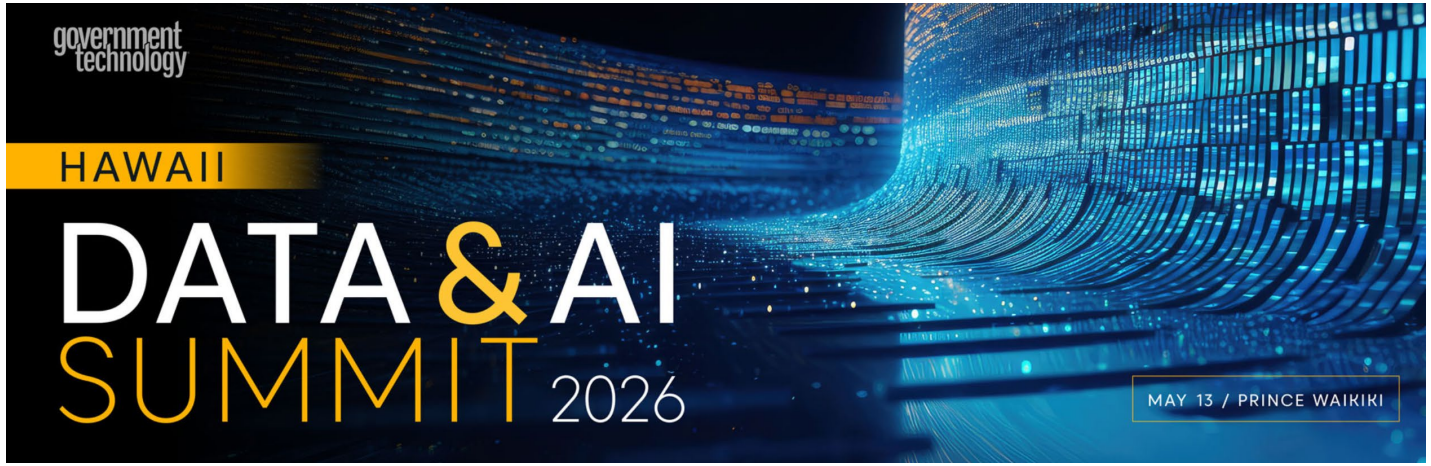
June 22nd, 2026



Agenda

- Meeting minute approval for March 16th, 2026 DTF meeting
- Data & AI Summit update
- Update from the State Chief Data/AI Officers Summit
- The new White House Executive Order on AI
- Responsible Data/AI Approach
- Update on AI Acceptable Use Guidelines
- Update on Data/AI projects
- Next meeting

The third Hawaii Data & AI Summit wrapped out successfully on May 13th, 2026, with



10:00 am
Hawaii

General Session – Conversations with the State Data Task Force: Opportunities and Challenges in Data and AI

Pi'inaio Ballroom

Join members of the State Data Task Force for a candid conversation on the opportunities and challenges of data and AI in the public sector. Panelists will share current realities, lessons learned, and what comes next.

Moderator: Rebecca Cai, Chief Data Officer, Office of Enterprise Technology Services, State of Hawaii

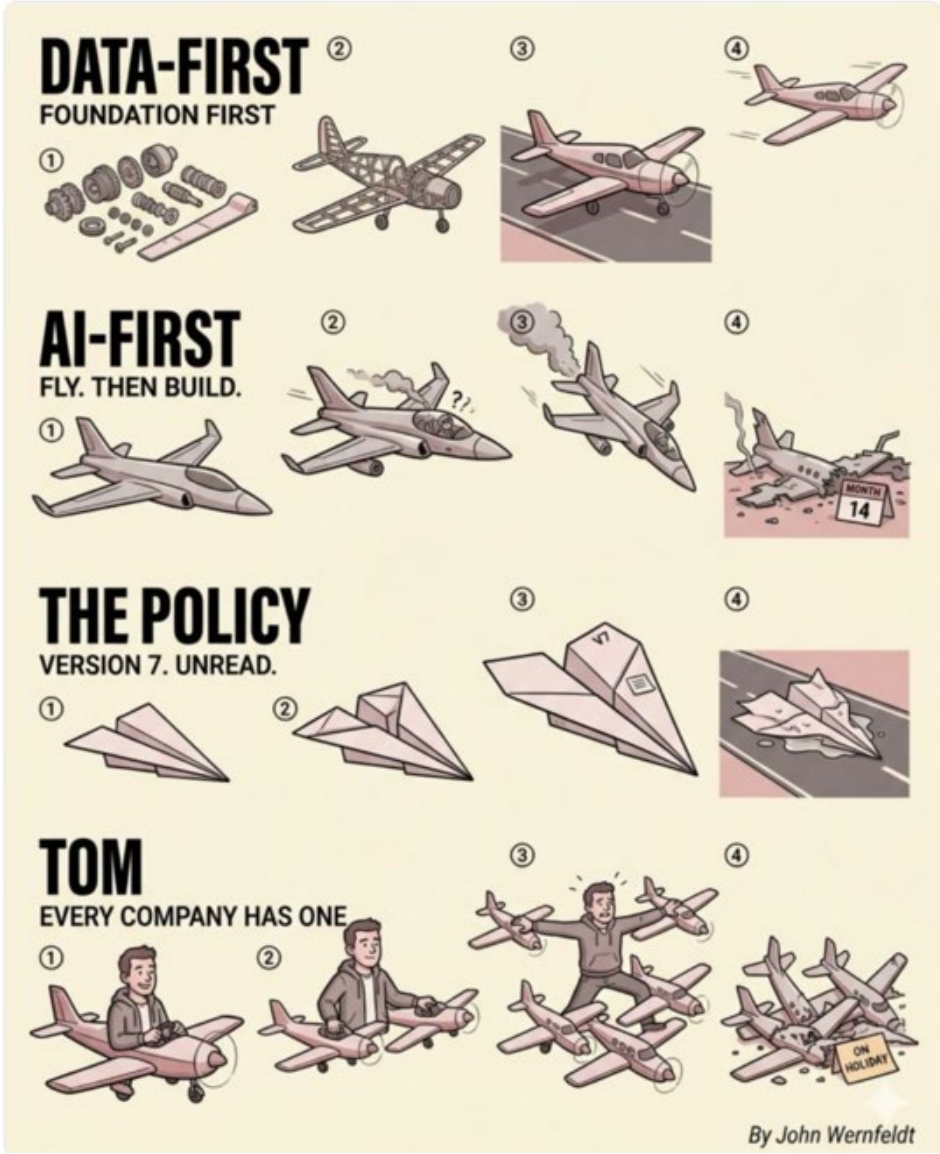
Torrie Inouye, State of Hawaii Data Task Force Member

Derek Vale, Chief Data Officer & Data Modernization Director, Health Data & Informatics Office, Department of Health, State of Hawaii

- **260 government employees registered, compared to** 230 in 2025.
- **23 event sponsors,** compared to 19 in 2025.
- We will move to a bigger hosting space in 2027 to accommodate more people.

2026 State Data/AI Officers Summit update and the data-first AI approach

- The summit focused on how governments can move from AI experimentation to responsible implementation, with discussions centered on governance, workforce readiness, procurement, evaluation, and the future of AI in public service.
- Fireside chat with OpenAI CEO Sam Altman.
- Anthropic offers $100k to states to identify our own cyber security vulnerabilities using Claude Security.
- Rebecca participates in AI Evaluation working group.
- Session on vision of future government service empowered by data and AI:
  - Rebecca: proactive and personalized service with government in our neighborhood and on the road.



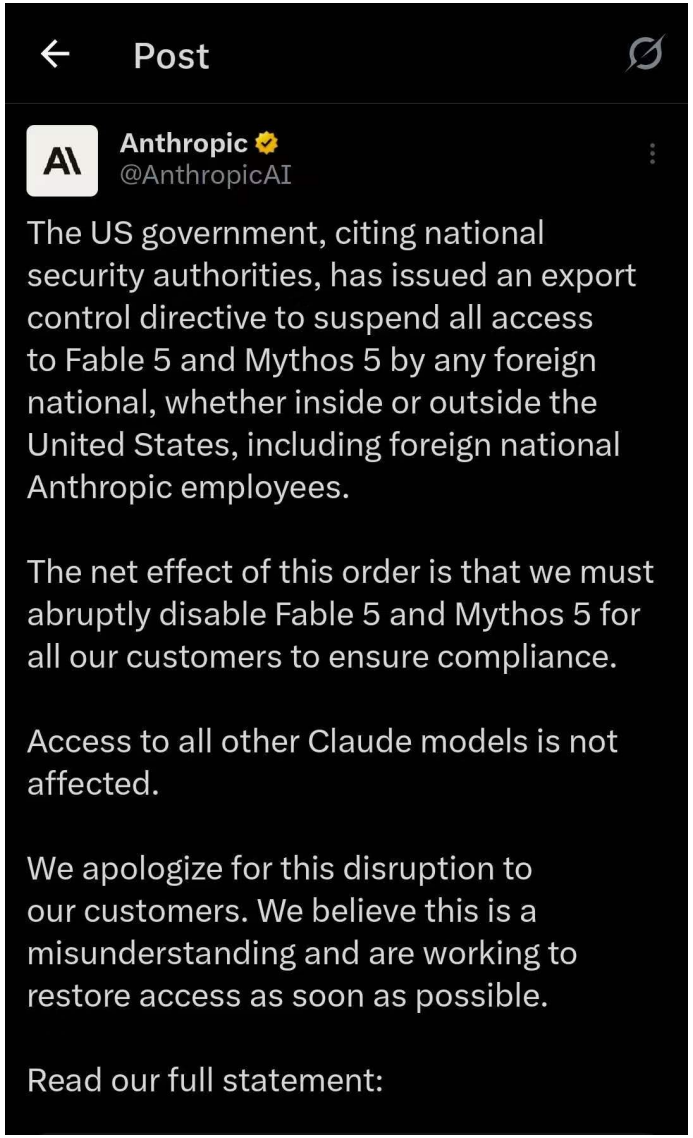
The White House EO 14409: Promoting advanced artificial intelligence innovation and security

EO summary:

- Focus on AI and cybersecurity and directs federal agencies to take coordinated, rapid action to strengthen cyber defenses, establish a voluntary framework for secure frontier AI model deployment, and prioritize enforcement of criminal activity involving the use of AI.
- Voluntary framework for secure frontier model deployment with two main components:
  - Classified benchmarking
  - Voluntary developer engagement
- Enforcement against criminal misuse of AI
  - Section 4 of the order directs the U.S. attorney general to prioritize enforcement of federal criminal laws, such as the Computer Fraud and Abuse Act (18 U.S.C. § 1030), against anyone who uses AI to engage in cybercrime.
  - Notably, the order specifically calls out the use of **AI agents** to unlawfully access data or compromise IT systems, consistent with growing concern among policymakers about autonomous or semi-autonomous AI systems that could conduct cyberattacks or facilitate unauthorized access.

Implications to us:

- Frontier AI models can be used to attack our infrastructure and systems.
- How we can be prepared:
  - For our own custom developed codes: We use AI models to detect our own vulnerability points and patch them.
  - Vendor codes (not available to us): Vendors need to be held accountable for identifying and patching their vulnerable points as they do not share their codes with us. → Discussion points: any policy recommendation to make this mandatory? What are the required actions for different risk levels? Any policy to allow/ban certain models and/or to require who can use what models?



In a responsible data/AI approach, we balance innovation and risk not only to better serve our residents, but also to promote trust alongside service excellence.

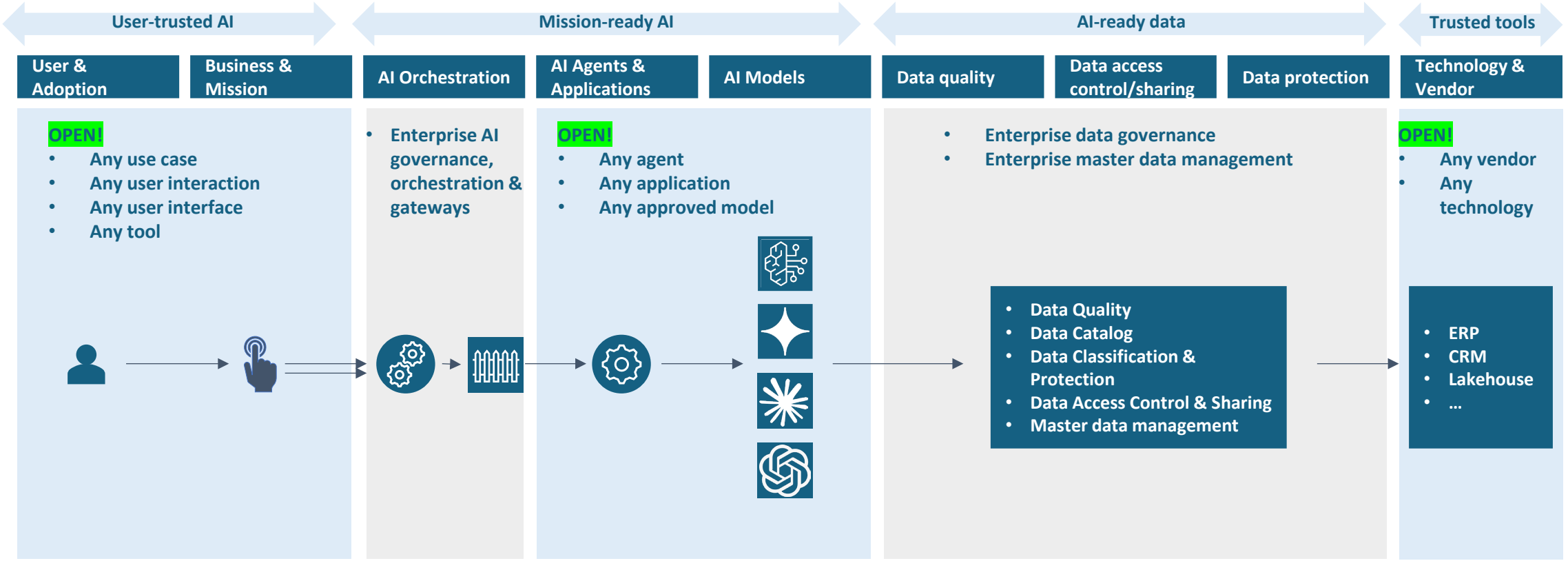
A responsible data/AI approach ensures proactive risk management from end users to AI models with clear guardrails and accountability.

	User-trusted AI		Mission-ready AI			AI-ready data			Trusted tools
	User & Adoption	**Business & Mission**	**AI Orchestration**	**AI Agents & Applications**	**AI Models**	**Data quality**	**Data access control/sharing**	**Data protection**	**Technology & Vendor**
Key risks	• Over-reliance • Misuse • Policy violation • Shadow AI	• Wrong decisions • Compliance violation • Citizen harm	• Wrong context & tools • Prompt injection	• Incorrect autonomy • Unauthorized actions • Agent conflicts	• Hallucinations • Bias & toxicity • Poor reasoning • Inconsistent answers	• Inaccurate data • Incomplete data • Stale data	• Unauthorized access • Compliance violation	• Data poisoning • PII leakage	• Vendor lock-in • Explainability & transparency • Vendor viability
Guardrails: policies & procedures	• AI acceptable use policy • AI training	• AI risk classification • Impacts assessment • Approval requirements	• Multi-agent coordination standards • Human-in-the-loop	• Agent identity management • Agent authorization	• Model approval process • Responsible AI approach	• Data quality for AI usage • Data stewardship	• Data sharing policy • Data classification policy	• Data privacy policy • Data classification standards	• Procurement rules • Monitoring & reporting requirements
Guardrails: technologies & tools	• Usage monitoring • Role-based access control • User warnings	• Audit trail • Compliance reviews • Outcome monitoring	• Agent control plane • Policy enforcement • Audit logging & tracing	• Role-based permissions • Human override capability • Agent observability	• Comprehensive testing • Ongoing auditing • Safety filters • Red-teaming	• Data quality score & monitoring • Metadata and master data management	• Data lineage • Data cataloging • Data sharing approvals • Master data management	• PII detection and masking • Encryption in transit and at rest	• Multi-vendor resilience • SLA monitoring • Platform observability

Guardrails align with NIST AI RMF 1.0.
Collaborated with Department of Transportation using their AI use case as example

We adopt an OPEN data and AI architecture to promote flexible and scalable innovation while providing consistent data and AI governance and orchestration to manage risks.

An OPEN enterprise data & AI architecture promoting scalable and flexible innovation with consistent governance



ETS procured tools for consistent data and AI governance.

Departmental use case specific tools for optimized user experience and adoption.

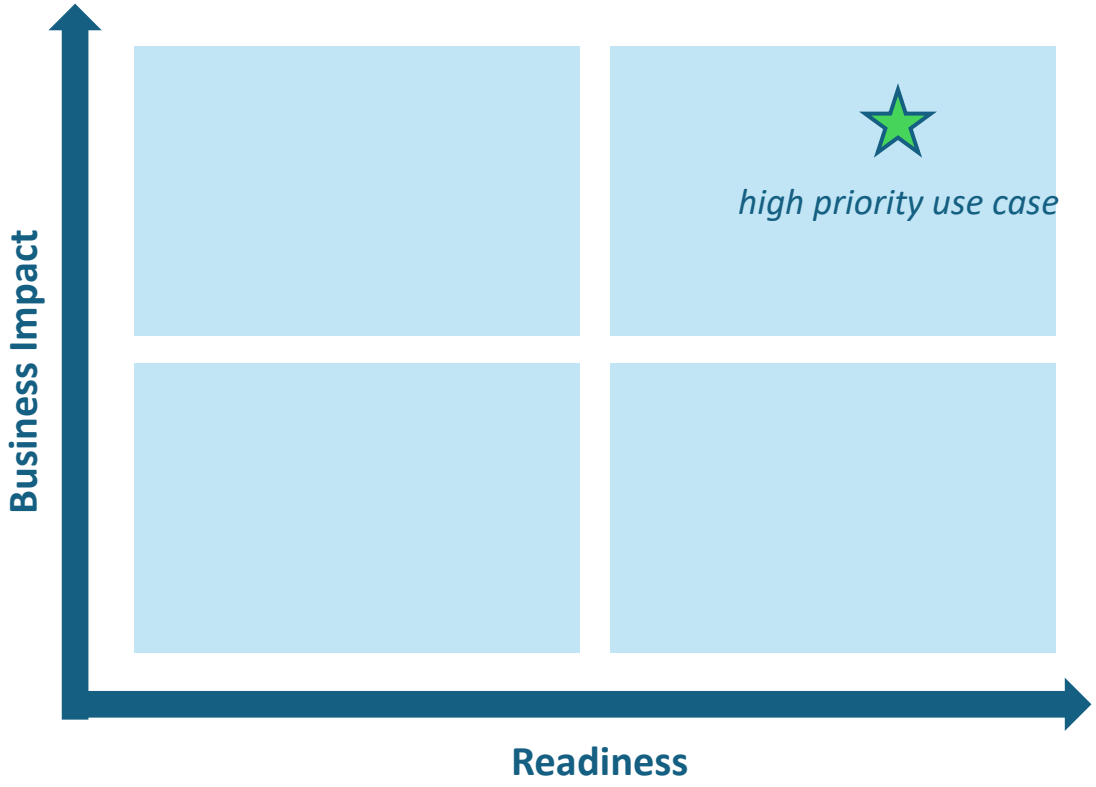
We assess and prioritize data and AI use cases based on business impacts to be created and the readiness of data, process, people, and technology to create immediate and continuous impacts.

Readiness:

- Data readiness: data quality managed, access controlled, classified?
- Process readiness: process well defined?
- People readiness: business owners identified and available?
- Technology readiness: tools available?

Business impact (measurable):

- Operational efficiency: Hours saved? Backlog reduction? Rework reduction?
- Customer experience & satisfaction: Higher customer engagement? Higher satisfaction score? Self-service adoption rate? Wait time reduction? First contact resolution rate improvement? Complaint reduction? Number of people served?
- Cost reduction: Cost reduced? Contractor spend reduction?
- Quality & accuracy improvement: Error rate reduction? Prediction accuracy? Data quality score? Audit findings reduction?
- Risk reduction: fraud losses prevented? Compliance violation reduced? Financial losses avoided?



With advancement in AI and additional risks uncovered, we updated the AI Acceptable Use Guidelines and intend to keep updating it in the future – DRAFT for DTF members to review.

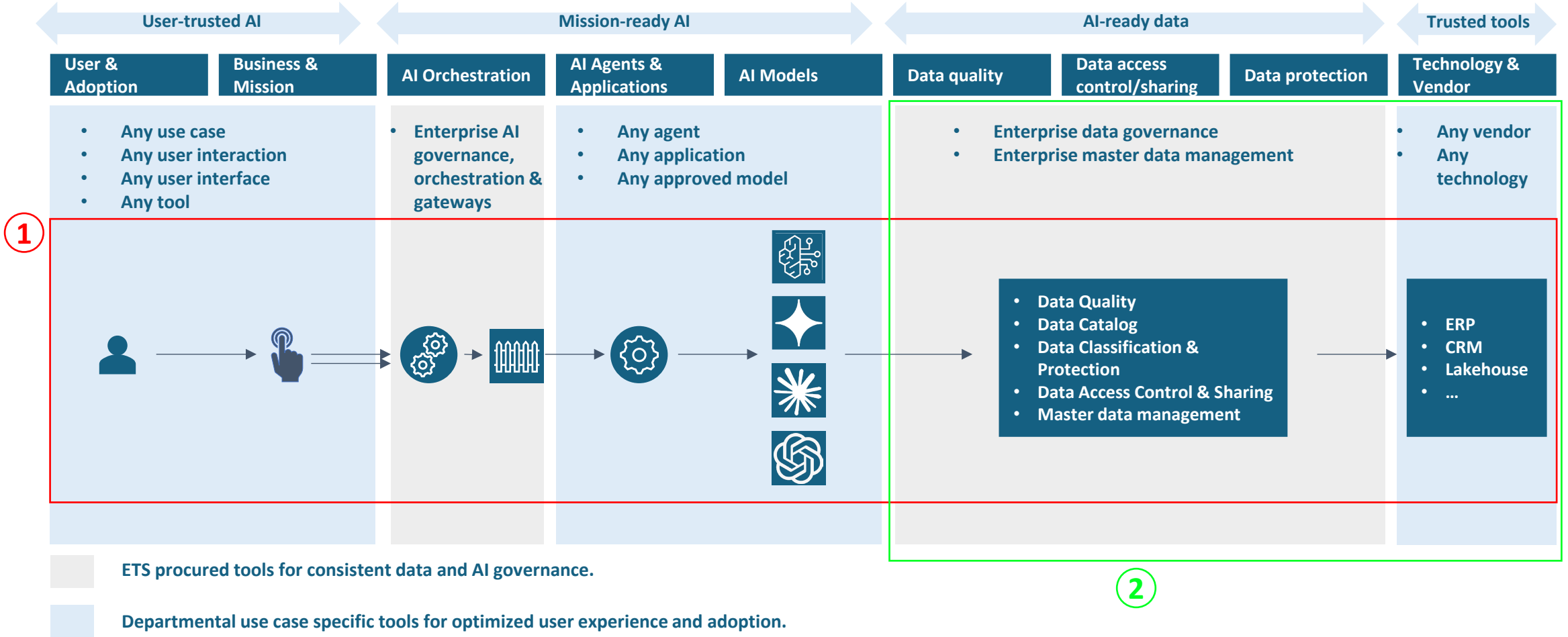
The guideline focuses on statewide standards for ethical, transparent, and secure AI use across Hawai‘i agencies, aligned with NIST AI RMF and ISO/IEC 42001.

- **Key areas addressed include**:
  - Safeguarding PII and maintaining data privacy
  - Human oversight of AI-assisted decisions
  - Transparency and disclosure of AI-generated content
  - Bias mitigation and fairness
  - AI-ready data and retention compliance
  - Centralized AI inventories
  - Standardized tool evaluation criteria (security, explainability, fairness, interoperability, scalability, vendor governance)
  - Use-case-driven implementation with operational, technical, and equity-based success metrics
  - Statewide collaboration through a shared AI use case inventory

Collaborated with Department of Transportation using their AI use case as example

We are making progress on Data/AI projects we are supporting right now, covering both end-to-end AI solution and data governance and sharing initiative.

1. Department of transportation omni-channel virtual agent initiative.
2. Department of Corrections and Rehabilitation, and Department of Human Services data sharing project.



Any data or AI policies or standards to recommend?

- Addition to the existing AI guidelines:
  - Model approval?
  - Mandatory data and AI training?
  - AI risk classification? (use NIST RMF?)
  - Procurement rules?
  - Monitoring and reporting
  - Agent and orchestration standards (agent authority controls)
- AI use case risk management standards
  - Business impact assessment
  - AI risk assessment
  - Privacy impact assessment
  - Civil rights/bias assessment
  - Human-in-the-loop determination and accountability
  - Approval requirements and workflow
- AI agent and orchestration governance standards
  - Agent authority controls (what agents can/cannot do, approval requirements)
  - Multi-agent controls (agent identity, authentication, agent-to-agent authorization, agent provenance/audit trail)
  - Workflow controls (checkpoints, human review gates, rollback capability, escalation paths)
- AI-ready data guidelines:
  - Data quality: published
  - Data sharing: data stewardship and accountability for AI usage
  - Data classification: published
  - Data privacy: published

Thank you!

Next meeting:

- **Date: September 21st, 2026**
- **Any agenda item to propose?**