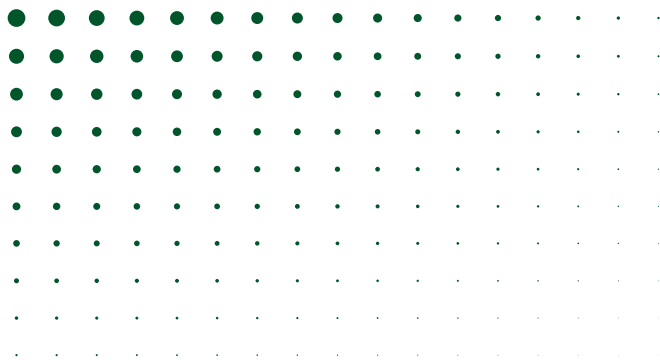




# IDAHO'S AI ADVANTAGE A Framework for Responsible Innovation

# Table of Contents



## 01

Introduction  
& Vision

## 02

Governance  
Framework

## 03

Responsible  
Implementation

## 04

Strategic  
Roadmap

## 05

Strategic  
Governance &  
the Road Ahead

## 06

Appendix A:  
Case Studies

## 07

Appendix B:  
AI Literacy  
Program

## 08

Appendix C: AI  
Concept Brief



# 1 Introduction & Vision

This paper presents a comprehensive framework designed to position Idaho at the forefront of responsible artificial intelligence (AI) innovation in state government. Grounded in eight core principles, the framework balances ethical rigor with practical implementation. It places human needs at the center of AI adoption and ensures transparency, fairness, and proportionate oversight throughout development.

Idaho's tiered governance model applies rigorous scrutiny to high-risk systems and streamlines review for low-risk applications. This structure empowers the state to capture immediate value from early implementations and build institutional capacity systematically. Through this balanced approach, Idaho is poised to transform its citizen services, operational workflows, and decision-making culture, anchoring it in data-driven insights and public accountability.

By embracing this framework, agencies and departments will deliver more responsive, accessible services tailored to the diverse needs of Idahoans. Automation of routine processes will free state employees to focus on complex, human-centered challenges. AI analytics will unlock previously untapped patterns in data, informing smarter policymaking and more efficient resource allocation. These benefits will not come at the expense of public trust. Instead, the framework embeds transparency, privacy protections, and ethical standards as essential prerequisites for system development and use.

More importantly, this vision places Idahoans at the center, with AI serving as a tool to enhance human potential rather than replace it. By thoughtfully implementing AI across state government, agencies and departments can deliver services that are more responsive, efficient, and accessible for all citizens.



---

## Executive Takeaway

*Idaho's risk-based AI framework establishes the state as a national leader in government innovation. Targeted oversight ensures high-impact systems meet rigorous standards. Low-risk applications deploy rapidly to transform citizen services and operational efficiency. This citizen-centered approach builds public trust through transparency and ethical guardrails, positioning Idaho to tackle complex challenges with data-driven solutions.*

# Strategic Vision



## *Transforming Government Through Responsible AI*

AI presents a transformative opportunity to reimagine how state government delivers services, engages citizens, and makes decisions. Idaho's strategic vision for AI extends far beyond achieving efficiency gains. It seeks to fundamentally reshape the relationship between the government and the people it serves, making it more intuitive, accessible, and human-centered.

This framework aligns directly with Idaho's broader IT Modernization Initiative by establishing a comprehensive governance structure for the ethical and effective deployment of emerging technologies. The Modernization Initiative emphasizes citizen-centered design and accessible digital interfaces. This AI framework expands that foundation to ensure systems driving these experiences adhere to the highest standards of transparency, privacy, and fairness.

Idaho envisions a state where citizens interact with government services through streamlined digital interfaces that eliminate unnecessary complexity. Staff will focus on high-impact, judgment-based tasks as AI efficiently manages repetitive, rules-based processes in the background. Government leaders will access timely, actionable insights to support more informed decisions. These enhancements will extend across the entire state, reaching rural communities and underserved populations.

This vision aligns closely with the mission of the Idaho Office of Information Technology Services (ITS), which seeks to "connect citizens with their government." The AI Governance Framework extends this mission by improving both the means of connection and its quality and responsiveness. As a foundational component of the ITS FY2024-2027 Strategic Plan, the framework structures how agencies and departments adopt, evaluate, and manage AI. It ensures Idaho's investments in AI technologies remain strategically aligned, ethically guided, and operationally sound.

*Smarter Systems*  
**Stronger  
Communities**



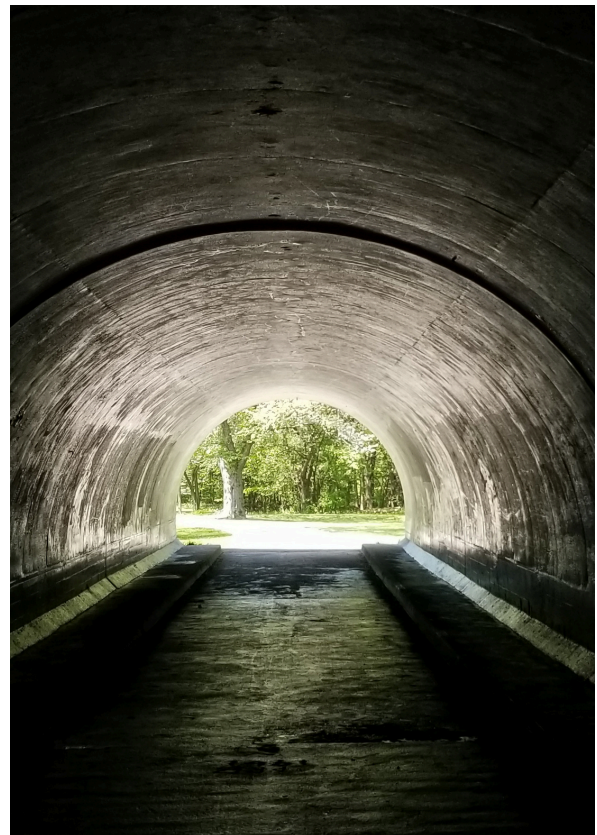
To translate this vision into action, Idaho has identified four strategic objectives that define where AI will deliver the greatest value for the state. Each objective includes specific measures of success to track progress and demonstrate value over time.

**Enhance The Citizen Experience:** AI will create more intuitive, responsive, and personalized public services. Virtual assistants will provide around-the-clock access to government information. Recommendation engines will guide users to the services most relevant to their needs. The effectiveness of these improvements will be measured through citizen satisfaction surveys, reduced processing times, and expanded access to services.

**Drive Operational Excellence:** By automating manual, repetitive tasks, AI will allow state employees to focus on work that demands human judgment, creativity, and empathy. Operational performance will be tracked through metrics such as time savings, error reduction rates, and faster service delivery. These efficiencies will improve internal workflows and enhance service delivery to the public.

**Establish Data-Driven Governance:** AI-powered analytics will support more informed decision-making at all levels of government. By identifying trends, anticipating needs, and revealing areas for improvement, these tools will shift Idaho's governance model from reactive to proactive. Success will be reflected in increased use of evidence-based decisions, more effective allocation of public resources, and stronger cross-agency and department collaboration.

**Build Trust and Accountability:** Trust is essential in government leadership, particularly when introducing technologies that impact public decision-making. This framework includes transparency requirements, audit mechanisms, and ethical standards to ensure AI systems are understandable, explainable, and used responsibly. Public trust will be measured through engagement metrics, feedback channels, and external review processes.



# Strategic Alignment with ITS

This AI Governance Framework serves as a strategic enabler for Idaho's broader technology goals. It supports the ITS Strategic Plan in four key dimensions:

**Technology Infrastructure Integration:** The framework builds on the robust, secure infrastructure established by ITS' Modernization efforts. It introduces AI-specific design patterns and requirements that align with enterprise architecture, allowing agencies to innovate within a shared and secure foundation.

**Shared Services Model:** By offering centralized governance capabilities and shared tools, the framework enables agencies and departments of all sizes to implement AI solutions without duplicating effort. This approach increases consistency, reduces costs, and accelerates time to value, particularly for smaller agencies and departments with limited resources.

**Customer-Centered Design:** In harmony with ITS existing design standards, this framework ensures AI adoption is driven by citizen needs and user experience outcomes. Rather than pursuing AI for its own sake, agencies and departments are encouraged to adopt technologies that improve public-facing services and operational efficiency.

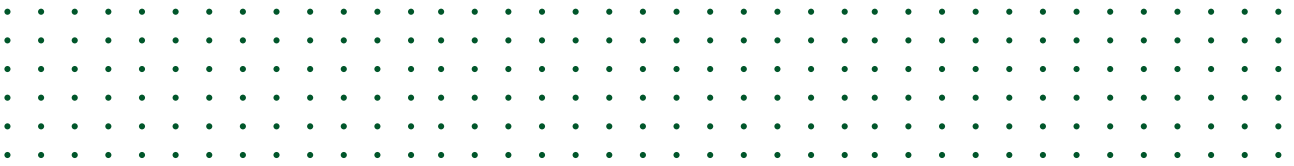
**Security Integration:** The AI-specific security tools defined in this framework extend Idaho's broader enterprise cybersecurity strategy. These controls address the unique vulnerabilities associated with machine learning models, data pipelines, and automated decision-making and maintain alignment with ITS overall security architecture.



By embedding the AI Governance Framework within the existing ITS roadmap, Idaho ensures that AI adoption supports ongoing modernization efforts. The result is a cohesive, forward-looking digital government strategy that balances innovation with oversight, and agility with accountability.



# Core Principles



Eight foundational principles guide Idaho’s approach to responsible AI implementation. These principles serve as both ethical guardrails and operational anchors, ensuring that the state advances innovation in a thoughtful, transparent, and beneficial way for all citizens. Together, they form the philosophical and procedural backbone of the AI Governance Framework, evolving alongside technologies, regulations, and public expectations.

## *Human-Centered Design*

Technology exists to serve people, not the other way around. Idaho’s AI systems must be designed with a clear focus on enhancing human capability, not simply replacing it. This means engaging with the people who use public services, like residents, workers, and government employees, to understand their needs and build solutions that truly support them. The human-centered approach begins in the earliest stages of development.

Agencies and departments must conduct research with a diverse range of users to understand actual pain points, rather than assumed ones. Prototypes must be tested with representative populations to refine interactions and identify usability barriers. After deployment, ongoing evaluation must focus not only on technical performance, but on the system’s ability to serve human outcomes effectively and without bias.



Consider a virtual assistant designed to answer tax-related questions. The system’s technical accuracy matters, but it will ultimately be evaluated based on how clearly and confidently it helps citizens navigate complex issues. By placing people at the center of every decision, Idaho ensures its AI efforts deliver real public value.

# *Transparency and Explainability*

For AI systems to be trusted, they must be understood. Idahoans have a right to know when AI is influencing decisions that affect them and to understand, at an appropriate level, how and why those decisions were made.

Transparency begins with visibility. A comprehensive inventory of AI systems ensures relevant stakeholders can understand where and how these technologies are being used. Each system must include a plain-language explanation of its purpose, functionality, and limitations. More impactful systems must offer detailed, traceable logic that allows agency and department staff and other relevant stakeholders to examine how decisions are made.

For example, an AI tool used to determine eligibility for public benefits must provide an explanation of the key factors that contribute to each determination. This ensures decisions can be reviewed, challenged, and ultimately approved, building trust through openness and accountability.

## *Appropriate Oversight*

Even the most advanced systems cannot replace the importance of human judgment and institutional accountability. Idaho's framework mandates oversight proportional to each system's potential impact, ensuring high-risk applications receive rigorous review and low-risk systems benefit from streamlined governance.

All AI implementations must be supervised by individuals or teams with the appropriate authority and subject-matter expertise. Agencies and departments must define clear lines of responsibility for system outcomes and maintain review processes scaled to each use case's sensitivity and complexity.

For example, a system used to analyze public documents may require only lightweight supervision. An AI tool influencing benefit eligibility or public safety decisions must be reviewed by human staff before outcomes are finalized. This tiered approach ensures limited oversight resources focus where they're most needed without slowing beneficial innovation.





# *Fairness and Accessibility*

AI must serve all Idahoans, without bias. To achieve this, the state's approach to fairness extends beyond technical performance metrics to include issues that impact underserved communities.

Agencies and departments must build fairness into every phase of the AI lifecycle. During development, datasets must be scrutinized for representation and balance. Prior to deployment, systems must undergo assessments to identify any disproportionate impacts across demographic groups. After launch, outcomes must be continuously monitored for emerging disparities and when disparities or accessibility issues are identified, agencies and departments must take swift, documented corrective action.

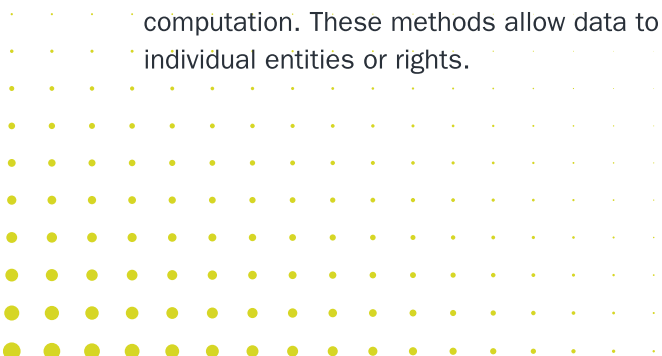
For instance, if an AI system used to review applications for a state assistance program produces different outcomes based on geography, race, income level, or any other federally protected class, the agency or department must investigate and remediate the root causes. Fairness is not a one-time checkpoint, but a continuous obligation embedded in both design and practice.

# *Security and Privacy by Design*

Security and privacy form the foundation of every AI system developed and deployed under Idaho's framework. From the earliest stages of planning, agencies and departments must implement safeguards to protect sensitive data and ensure system integrity.

Key practices include data minimization (collecting only what is necessary), consent mechanisms—in accordance with ITS Information Security Policies (PT-04)—that clearly inform users how their data will be used, and robust access controls and authentication to prevent misuse. For systems processing sensitive information, such as health, financial, or legal data, additional layers of protection are required, including encryption, access auditing, and frequent security assessments. In accordance with ITS Information Security Policies (MP-04(c) and SA-04(j)7), information systems that receive, process, store, access, protect and/or transmit Idaho state data must be located, operated, and accessed within the United States.

Where appropriate, agencies and departments are encouraged to adopt advanced privacy-preserving technologies such as differential privacy, federated learning, and secure multi-party computation. These methods allow data to be used for insight generation without compromising individual entities or rights.

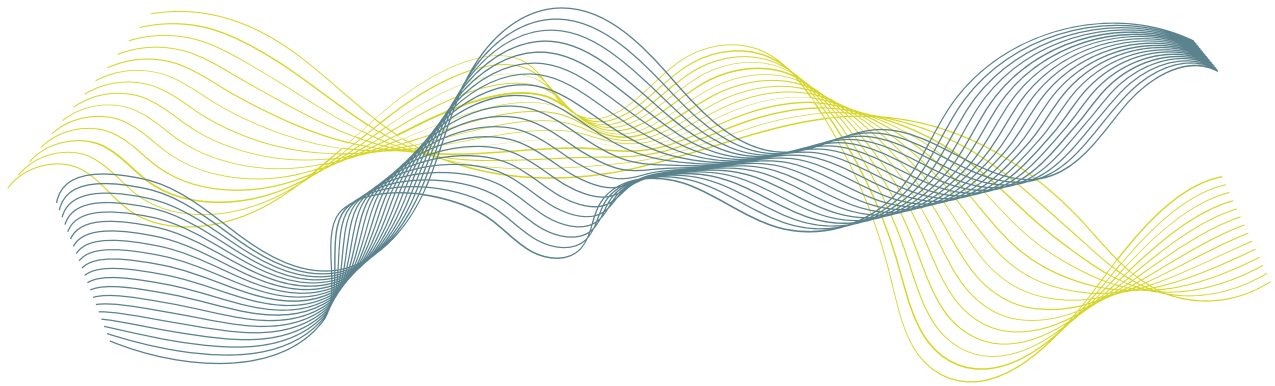


# *Risk-Based Governance*

Not all AI systems carry the same level of risk. Idaho's governance model reflects this reality. The risk-based approach allows agencies and departments to scale review and oversight mechanisms according to the system's potential impact on people, data, and public trust.

A formal risk classification model considers factors such as data sensitivity, decision impact, autonomy, transparency, scope, and complexity. Systems identified as high-risk undergo comprehensive review, and those with low risk may follow expedited pathways. This ensures governance efforts focus where they matter most without impeding useful innovation.

For example, a chatbot that helps users find park hours requires minimal oversight. An AI-driven system that influences criminal justice or public benefits must undergo rigorous ethical and technical evaluation. The framework's flexibility allows Idaho to manage risk without slowing progress.



# *Continuous Improvement*

AI systems must evolve in response to performance feedback, stakeholder input, and shifts in best practices. Idaho's framework incorporates continuous improvement as a formal requirement of responsible AI use.

Each implementation includes mechanisms for performance monitoring, user feedback collection, and adaptive learning. Agencies and departments must routinely evaluate systems against defined metrics, investigate unexpected outcomes, and update models or processes as needed.

This commitment to iteration ensures that AI systems remain responsive to changing needs and avoid becoming outdated or misaligned with public expectations. The result is a culture of learning and refinement, not just deployment.



# Shared Responsibility

Successful AI governance depends on clearly defined roles and responsibilities. ITS establishes standards and provides oversight, while agencies and departments implement and operate systems. This partnership ensures both consistent governance and operational flexibility across state government.

## FOUNDATION AND IMPLEMENTATION PARTNERSHIP

Idaho adopts a shared responsibility model that clearly delineates roles between ITS and individual agencies and departments.

ITS provides the foundation, establishing the statewide AI governance framework, policies, and standards that all agencies and departments build upon. ITS is responsible for developing risk assessment methodologies and assigning risk scores (see page 16 in Section 2), approving high-risk implementations through the AI Executive Committee, maintaining the state's AI system inventory, and providing technical consultation services. As the central hub, ITS coordinates enterprise-wide activity initiatives, develops standardized templates and tools, and monitors compliance with established policies. Consistent with existing statutory authorities and responsibilities, ITS retains the authority to reject high risk AI implementations.



Agencies and departments serve as implementers, responsible for partnering with ITS to support risk assessments for their proposed AI systems, developing agency- and department-specific use cases and implementation plans, and ensuring compliance with ITS policies. Agencies and departments manage their own vendor relationships, implement required security and privacy controls, conduct ongoing monitoring of their systems, and ensure proper training of their personnel on responsible AI use.

Idaho's shared responsibility model includes technology vendors providing AI services and solutions, with specific considerations unique to AI systems. This model acknowledges that AI implementations require robust governance approaches that meet or exceed traditional IT services:

**Vendor Responsibilities for AI Systems:**

- Providing secure AI platforms with appropriate safety systems for filtering harmful inputs and outputs
- Maintaining model quality, reliability, and performance standards
- Implementing foundational protections against AI-specific threats and vulnerabilities
- Offering transparency about model capabilities, limitations, and appropriate use cases
- Supporting responsible AI principles through platform controls and safeguards

**State of Idaho Responsibilities for AI Systems:**

- ITS: Ensuring appropriate use cases align with Idaho's principles and risk tolerance
- Agency or Department: Verifying AI outputs for accuracy, fairness, and alignment with state values
- Agency or Department: Implementing proper human oversight and review processes
- Agency or Department: Maintaining prompt management and content validation procedures
- Agency or Department: Appropriately disclosing AI use to constituents and stakeholders

This AI responsibility model varies based on deployment type (software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), with responsibility shifting based on the level of control. With SaaS AI tools like AI-powered assistants, vendors maintain primary responsibility for the AI platform while Idaho ensures appropriate use. For PaaS offerings like cloud-based AI platforms, Idaho may take greater responsibility for application development and prompt engineering while vendors maintain the underlying models. Custom AI implementations require the most comprehensive state oversight.

This approach maintains clear responsibilities and recognizes the collaborative nature of AI implementation. Joint accountability ensures AI systems operate ethically, safely, and effectively in service of Idaho's citizens.

## **Executive Takeaway**

*These eight principles provide the foundation for how Idaho will govern AI as a public responsibility. They shape every aspect of this framework, from project intake to policy review, and guide the state's long-term approach to AI in service of public trust.*

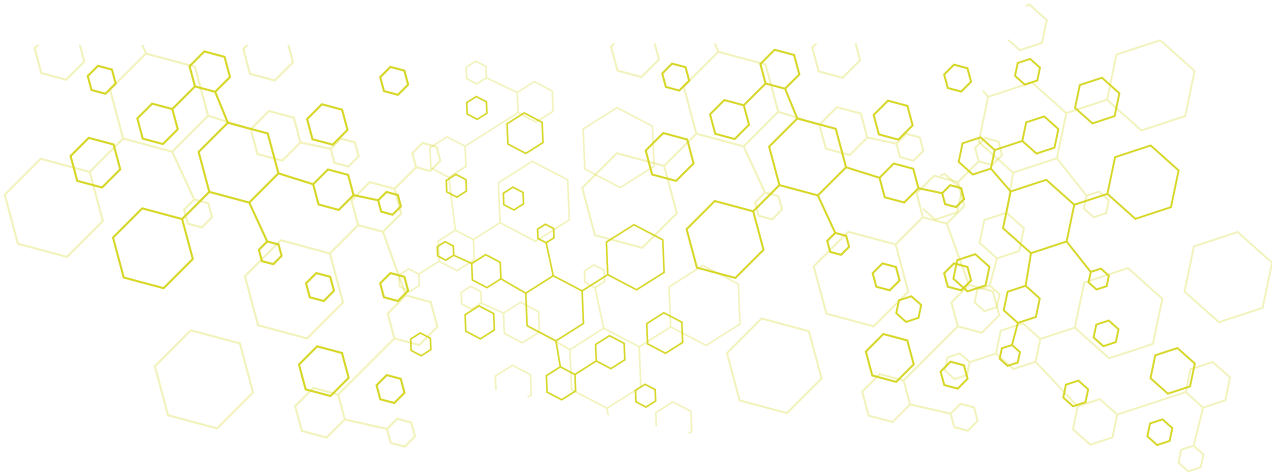


# 2 Governance Framework

Effective AI governance requires clear ownership, cross-functional collaboration, and consistent processes. This section defines the structures that enable Idaho to govern AI implementation reliably across varying system complexities, agency and department sizes, and use cases. The model balances comprehensive oversight with operational flexibility, allowing agencies and departments to fulfill their missions according to established governance principles.



# Governance Structure



The framework establishes five primary governance bodies with distinct responsibilities:

- **AI Executive Committee:** Established within the Idaho Technology Authority, this committee sets statewide AI priorities, reviews high-risk implementations, allocates resources, and ensures alignment with broader technology strategy. It includes representatives from state agencies and departments, technical experts, and policy advisors who meet regularly to make strategic and operational decisions.
- **Ethics Advisory Committee:** Established within the IT Leadership Council, this committee advises on ethical risks, fairness considerations, and demographic impacts, particularly for high-risk use cases. It comprises representatives from government, academia, civil society and the private sector, where appropriate.
- **AI Innovation Team:** Led by the ITS Chief Technology Officer, this team serves as the central hub for Idaho's AI strategy and includes dotted-lined representatives across ITS from relevant governance, risk, compliance, privacy, and security teams. It provides implementation support, facilitate communities of practice, develops documentation standards, and maintains the state's AI system inventory.
- **Technical Review Board:** Led by the ITS Chief Technology Officer, this Board brings together enterprise architects, machine learning experts, security professionals, and data specialists. It provides technical guidance on AI proposals and implementations, including model development, platform standards, risk assessments, and infrastructure requirements.
- **Agency and Department Implementation Teams:** Embedded within individual agencies and departments, these teams execute the practical work of implementation. They include business analysts, subject-matter experts, data leads, and change management professionals who adapt enterprise policies to agency and department needs but maintain consistency and compliance.



These governance bodies operate as an integrated system, deriving value from coordinated actions, shared accountability, and aligned priorities.

- The **Executive Committee** establishes overarching policies and priorities.
- The **Ethics Committee** and **Technical Board** translate these priorities into specific guidance and review criteria.
- The **AI Innovation Team** bridges governance and implementation, equipping agency and department teams with tools, templates, and technical assistance.
- **Agency and Department Implementation Teams** provide frontline feedback, identifying challenges and contributing to continuous improvement.



When new policies emerge—such as updated privacy requirements—the Ethics Committee develops review frameworks, the Technical Board creates implementation patterns, and the AI Innovation Team distributes practical guidance to agencies and departments.

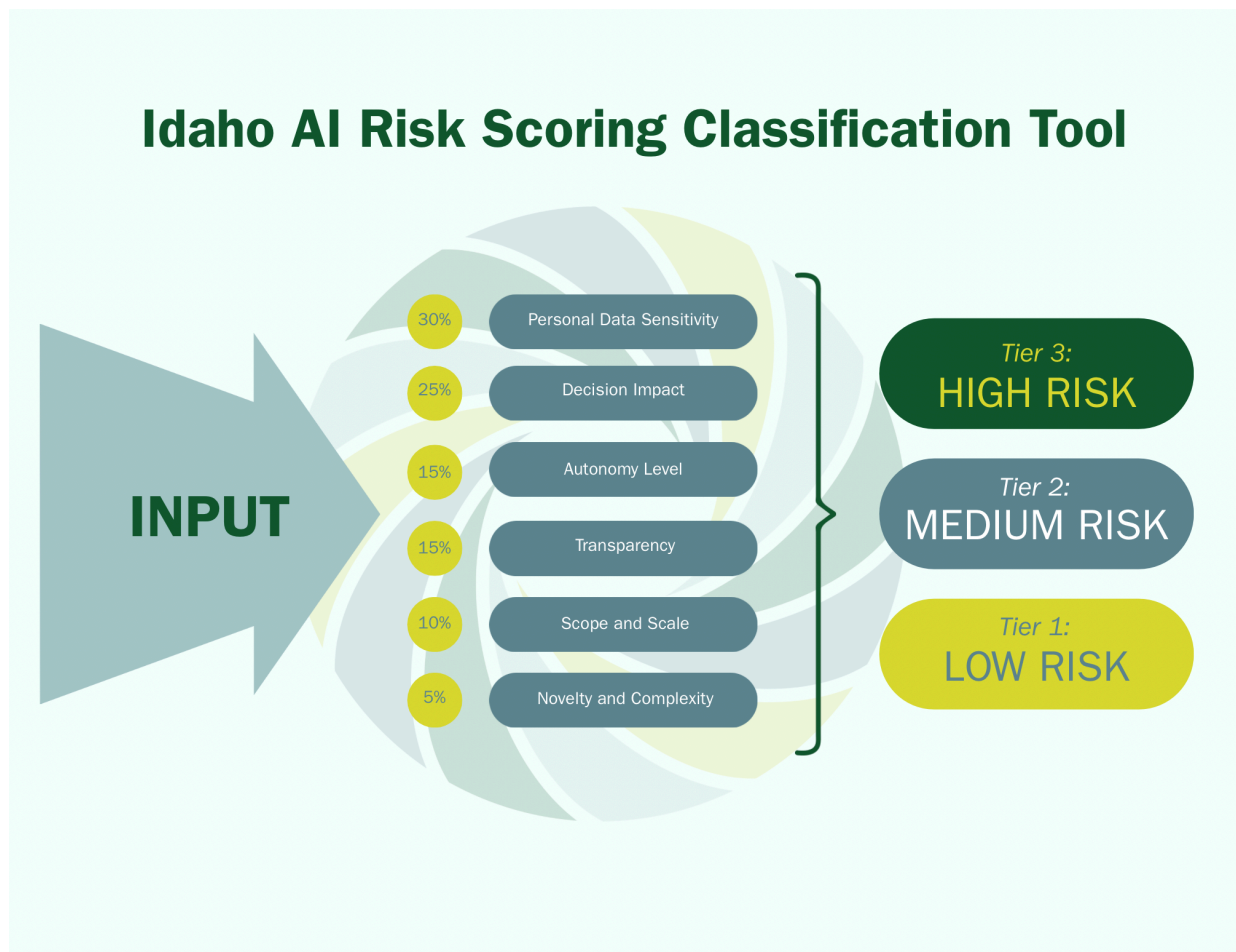
This coordinated approach ensures governance remains relevant, adaptive, and consistently applied statewide.

## *Executive Takeaway*

*Idaho's AI governance structure enables responsible oversight without impeding innovation. It establishes clear authorities yet fosters collaboration and maintains operational flexibility.*

# Risk-Based Oversight

AI systems present varying levels of risk. Idaho's oversight model applies proportional review requirements that scale with system impact, leveraging established solution vetting processes and ITS Information Systems Classification Policies (RA-02). This approach directs governance resources toward higher-risk systems that could affect citizens' rights, access, or privacy. It simultaneously streamlines oversight for lower-risk implementations to accelerate innovation. The result balances innovation and accountability in alignment with both the National Institute of Standards and Technology AI Risk Management Framework (NIST AI RMF) and Idaho's established data classification standards.



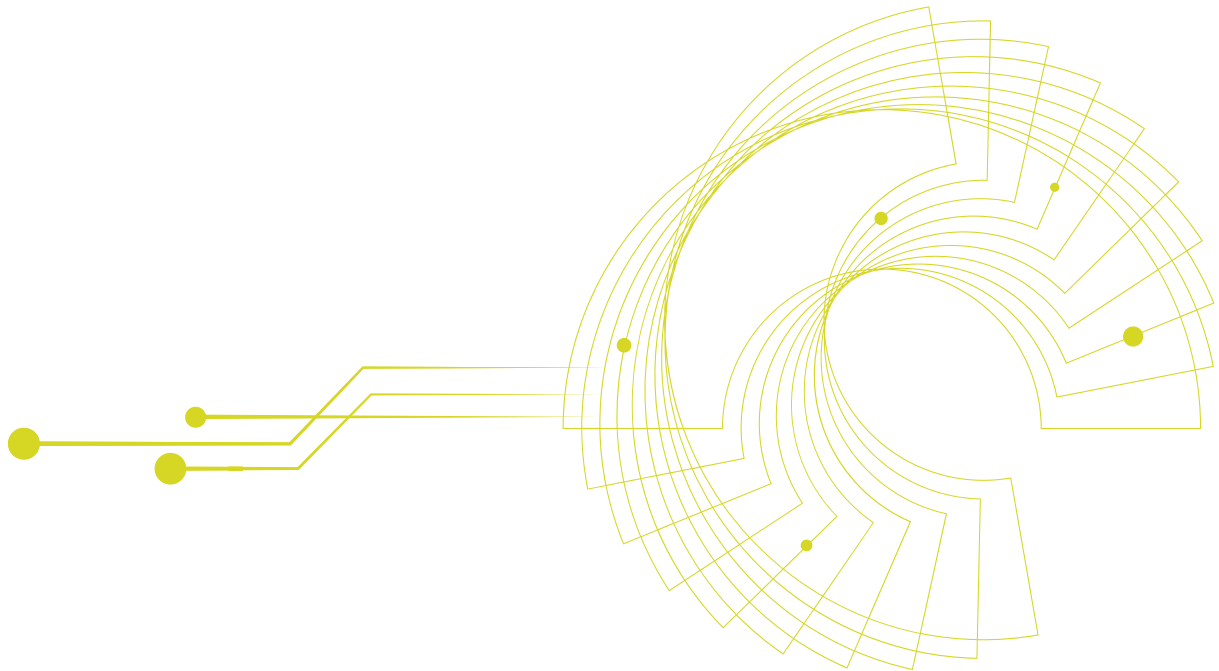
Idaho's oversight strategy centers on a multi-factor risk classification model that aligns with existing ITS Information Security Policies (RA-02). This model evaluates AI systems across six dimensions and rates each dimension based on a four-point scale ("Low", "Medium", "High", and "Very High."). The Personal Data Sensitivity dimension maps directly to Idaho's existing Information Classification levels:

- **Personal Data Sensitivity (30%):** Assesses the nature of the data the system uses and corresponds directly to Information Classification levels:
  - Low: Level 1 (Unrestricted) data
  - Medium: Level 2 (Limited) data
  - High: Level 3 (Restricted) data
  - Very High: Level 4 (Critical) data
- **Decision Impact (25%):** Assesses how system outputs affect individuals, considering Federal Information Processing Standards (FIPS) 199 impact levels (low, medium, high) as referenced in RA-02.
- **Autonomy Level (15%):** Evaluates human oversight involvement, with fully autonomous systems carrying higher risk than those with human validation.
- **Transparency (15%):** Measures how understandable the system's logic and outcomes are to non-technical stakeholders, with "black box" models scoring higher.
- **Scope and Scale (10%):** Considers system reach, from limited pilots to enterprise-wide deployments impacting thousands.
- **Novelty and Complexity (5%):** Evaluates whether the system uses well-established methods or introduces untested approaches with potential unforeseen risks.

These individual dimension ratings are weighted and combined to produce a total risk score. Consistent with the process outlined on page 16 in this section, ITS uses an internal, automated tool to score the system. This score places systems into one of three governance tiers aligned with Information Classification levels:

- **Tier 1: Low Risk (0-25%):** Corresponds to systems processing Level 1-2 data with low FIPS 199 impact. These systems follow standard governance processes with ITS enterprise architecture (EA), governance, and security operations teams' review. The AI Innovation Team receives notification for inventory purposes.
- **Tier 2: Medium Risk (26-50%):** Corresponds to systems processing Level 3 data with medium FIPS 199 impact. These systems follow standard governance processes with additional consultation from the AI Innovation Team and Technical Review Board.
- **Tier 3: High Risk (51-100%):** Corresponds to systems processing Level 4 data with high FIPS 199 impact. These systems follow standard governance processes with mandatory consultation from the Ethics Committee, Technical Review Board, and Executive Committee, and implement the most rigorous security controls.

These risk tiers determine how AI systems integrate into Idaho’s solution vetting and governance processes, as detailed in the following sections.



In accordance with ITS Information Security Policies (P.ITS-03 and S.ITS-02), Idaho integrates AI assessment directly into the existing solution vetting workflow rather than creating parallel processes. This integration emphasizes information classification alignment through five key components:

- Enhanced Intake Questions: Solution vetting requests indicating AI capabilities trigger targeted questions that help gather risk classification information and populate the AI Concept Brief, including Information Classification levels of all data involved.
- Automated Documentation: The intake process generates a supplementary AI Concept Brief that becomes part of the standard documentation package. This brief documents key elements like:
  - Use case, business need, and success metrics
  - Information Owner responsibilities and Information Classification levels
  - Explainability, human oversight and security requirements



- **Risk Assessment:** During standard intake, agency and department IT teams consult with the Information Owner to conduct preliminary risk screening. For systems identified as AI-enabled, governance and EA teams collaborate with security personnel to conduct comprehensive assessments using the six-factor model. This assessment follows the “high water mark” principle from RA-02, incorporates subject matter expertise, and determines the appropriate governance tier. The governance team validates risk classification, with appropriate advisory consultation from specialized teams based on risk level.
- **Unified Approval Path:** The AI Concept Brief and risk assessment flow through the standard governance process. Existing authorities receive enhanced information for informed decision-making and assign security controls based on appropriate classification levels. See pages 20-21 in this section for more information on decision authorities.
- **Lifecycle Documentation:** The AI Concept Brief serves as a living document updated throughout the system lifecycle, maintaining current classification and handling procedures. See pages 20-21 in this section for more information on lifecycle governance.

This approach provides a single-entry point for all solution vetting requests and ensures thorough evaluation of AI-specific risks. The risk framework extends existing criteria, complementing rather than replacing standard technical, security, and privacy reviews. The risk variance process (described on page 22 in this section) also reinforces integration with existing ITS processes and maintains operational flexibility for exceptional circumstances without compromising governance integrity.

ONE PATH  
**FULL  
VISIBILITY**



## *Executive Takeaway*

*Idaho’s risk-based oversight model delivers the best of both worlds: streamlined paths for low-risk AI and deep scrutiny for high-impact systems. It provides a scalable, adaptable governance approach that protects the public yet enables meaningful progress.*

# AI System Lifecycle Governance

Idaho's AI governance extends beyond risk classification to encompass the entire system lifecycle. This approach assigns specific decision authorities at each stage, integrates governance into existing ITS technology management processes, and provides structured variance handling when needed. While the sections above establish how systems are classified into risk tiers and what consultation they receive, this section focuses specifically on which governance bodies have decision authority for each tier and how this authority functions throughout the system lifecycle.



## *Decision Authority Framework*

In accordance with ITS Information Security Policies (SA-03), Idaho designates specific approval authorities that align with the appropriate level of oversight for each risk tier:

- Tier 1 (Low Risk): ITS and Agency (or Department) IT leaders make approval decisions following standard governance processes. The AI Innovation Team receives notification for inventory purposes only.
- Tier 2 (Medium Risk): ITS and Agency (or Department) leadership make approval decisions with advisory input from the AI Innovation Team and Technical Review Board. Information Owners manage information sharing agreements and security controls as required by RA-02.
- Tier 3 (High Risk): ITS and Agency (or Department) leadership make approval decisions with mandatory consultation from the Ethics Committee, Technical Review Board, and Executive Committee. Information Owners maintain enhanced oversight of classification and security controls for critical data.

These authorities exercise responsibility across key lifecycle activities aligned with the NIST AI RMF functions of GOVERN, MAP, MEASURE, and MANAGE. Idaho implements these functions through:

1. Initial Planning and Design (GOVERN, MAP): ITS and Agency sponsors with Information Owner classification guidance.
2. Development and Testing (MAP, MEASURE): Risk-appropriate authority approves resources with security validation.
3. Technical Evaluation (MEASURE): Technical Review Board verifies integration and proper data separation.
4. Deployment Decision (MANAGE): Risk-appropriate authority approves launch with security verification.
5. Monitoring and Evaluation (MANAGE): Implementation teams oversee performance with periodic reviews.

This framework establishes accountability through clear governance roles and ensures appropriate oversight scaled to risk.

## *Lifecycle Integration Points*

Idaho integrates AI oversight into existing technology management processes at key points:

- Ideation and Concept Development: Agencies and departments submit solution vetting requests through standard intake processes. For AI capabilities, the system gathers additional information for the AI Concept Brief. The Information Owner validates classification decisions and governance teams conduct preliminary risk screening.
- Project Proposal and Risk Assessment: Governance, EA, and security teams conduct a formal risk assessment in collaboration with the Information Owner, documenting classification levels, security controls, and data separation methods.
- Implementation and Deployment: Standard deployment processes incorporate additional verification of AI-specific controls. Governance and security teams validate privacy, fairness, and transparency requirements alongside classification-appropriate security controls.
- Monitoring and Continuous Improvement: Standard monitoring processes incorporate AI-specific metrics from the AI Concept Brief. Information Owners conduct periodic classification reviews as required by RA-02, with regular reassessment of risk classifications.

This lifecycle approach ensures appropriate governance at each stage without creating parallel processes or unnecessary administrative burden. It forms part of a continuous process that reflects the evolving nature of AI technologies and their real-world impacts.

# Risk Variance Process

Innovation doesn't always follow a template. Unique use cases, time-sensitive needs, or emerging technologies may require deviations from standard approval paths. Idaho's governance model incorporates ITS's existing risk variance process to accommodate these situations without compromising oversight.

When agencies or departments identify a legitimate need to deviate from established procedures, they initiate the variance process by submitting a formal request. This documentation captures essential information including system information, risk descriptions, justification for the variance, current controls and proposed mitigations, risk management strategy, and plans for ongoing monitoring and review.

Upon receiving this request, ITS conducts a targeted assessment. They evaluate the probability and potential impact of risks, identify any gaps introduced by the proposed deviation, and recommend compensating controls. Depending on the nature and complexity of the variance, the request may require review by the Technical Review Board, Ethics Advisory Committee, or both.

Consistent with the decision framework outlined on page 20 in this section, approval authority aligns with the system's risk tier. All variance decisions must be documented and signed by both ITS and the requesting agency or department's leadership.

Approved variances may include specific conditions such as time-bound authorization periods, required compensating controls, and scheduled review points. For example, during a natural disaster, an agency or department might receive approval for expedited AI deployment with abbreviated testing requirements, provided they implement enhanced monitoring and conduct a full compliance review once the crisis passes.

This structured approach promotes innovation and addresses potential urgent operational needs without compromising governance integrity or public trust. For hypothetical examples on how to walk through the governance process, see Appendix A.

## Executive Takeaway

*Idaho's variance process transforms potential governance roadblocks into structured pathways for innovation. By requiring rigorous documentation, appropriate review, and time-bound authorizations, the framework enables agencies and departments to pursue novel approaches and respond to urgent needs without sacrificing accountability or public trust.*



# Stakeholder Engagement

Responsible implementation requires building and maintaining trust across diverse stakeholders, both inside and outside of government. Idaho's stakeholder engagement strategy builds on the principle that broad participation leads to better outcomes, stronger accountability, and greater public legitimacy.



## *Internal Engagement*

Internally, Idaho leverages a collaborative model to ensure that AI initiatives reflect the full spectrum of agency and department priorities, operational realities, and workforce needs. At the executive level, strategic briefings and planning workshops give agency and department leaders visibility into ongoing AI efforts and invite their participation in shaping future priorities. These leaders help integrate AI with broader transformation initiatives, allocate resources, and sponsor high-value pilots.

IT teams engage through working groups, technical training programs, and communities of practice that build collective capacity and foster cross-agency and department knowledge sharing. These venues provide opportunities to solve shared challenges, develop reusable patterns, and build familiarity with emerging technologies.

Operational staff—those closest to the work—play a key role in identifying pain points, refining system requirements, and ensuring implementations support real-world needs. Through user testing, change management workshops, and structured feedback sessions, frontline employees become co-creators of AI-enabled services, not just recipients.

This internal collaboration ensures AI implementations are practical, effective, and aligned with Idaho's public service mission.

# External Engagement

AI systems can affect the public in visible and invisible ways. Idaho prioritizes external engagement as a central pillar of responsible governance.

Legislative partners are engaged through annual reports, committee briefings, and collaborative policy development sessions that ensure elected leaders understand the trajectory of AI adoption, its benefits, and its risks. These touchpoints help maintain alignment with state priorities and ensure appropriate oversight and support.

Public engagement is grounded in transparency and access. Citizens are informed when they interact with AI systems and are invited to provide input through structured comment periods, community outreach, and educational materials. Agencies and departments are encouraged to translate technical capabilities into plain language, helping citizens understand how AI supports their experience, and where human judgment remains central.

Idaho also engages with industry and academia through forums, research partnerships, and co-development efforts. These external stakeholders bring vital expertise and fresh perspectives to implementation challenges and help shape the talent pipeline and advance the state's innovation ecosystem.

## Transparency Mechanisms

Transparency builds and sustains trust. Idaho's framework includes a suite of mechanisms that provide visibility into where AI is being used, how it performs, and how citizens can engage with it.

- **AI System Inventory** serves as an internal record of all AI systems deployed by the state. Each entry includes the system's purpose, capabilities, limitations, and risk classification.
- The **Performance Dashboard** (developed once pilots and projects mature) tracks metrics such as accuracy, response times, and service quality, connecting system operation to public value.
- The **Annual AI Report** summarizes major initiatives, lessons learned, upcoming plans, and cross-agency and department efforts, and is shared with both internal and public audiences.

These tools help demystify AI, invite public dialogue, and ensure accountability across all levels of implementation.



# Citizen Communication Strategy



Communication must make information meaningful, not just available. When communicating about AI systems, agencies and departments are encouraged to follow four principles:



**Be Transparent:** Clearly identify when and where AI is used, and what its role is in the citizen experience.



**Provide Context:** Explain the capabilities and limitations of AI tools to set realistic expectations.



**Make It Understandable:** Offer explanations at varying levels of detail depending on the impact of the system and the user's preferences.



**Create Feedback Loops:** Empower citizens to share concerns, ask questions, and influence improvements through structured feedback channels.

Clear, timely communication is essential to maintaining trust in public institutions as AI becomes a more visible part of government service delivery.

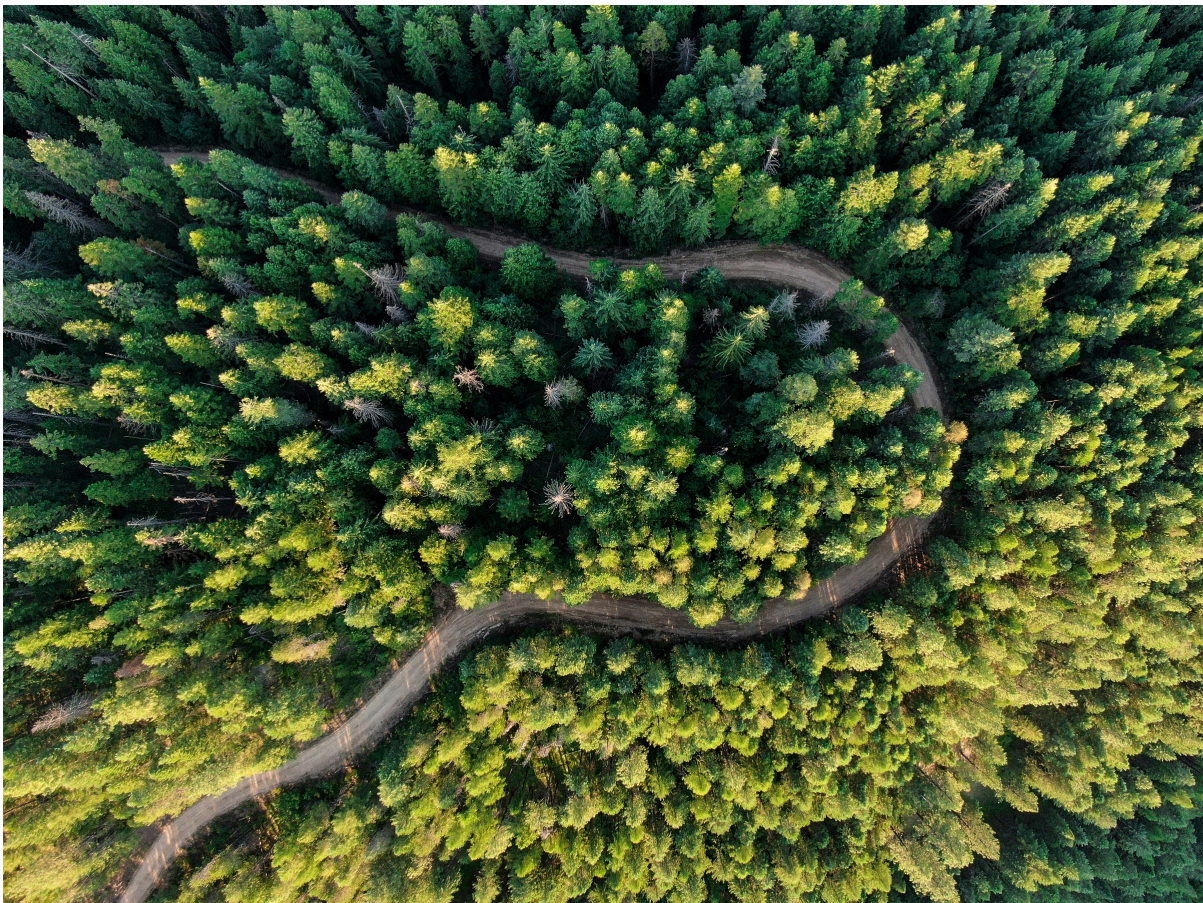
## Executive Takeaway

*Engaging stakeholders early and often, through structured participation, transparency mechanisms, and citizen feedback, builds the foundation for growing public trust in AI. This approach moves beyond compliance to create an environment where technology serves shared public goals defined through robust dialogue.*



# 3 Responsible Implementation

*Where governance defines the rules and transparency builds trust, responsible implementation brings those commitments to life.*



*This section details how Idaho ensures that AI systems are not only well-designed, but secure, ethical, and continuously improving. From protecting personal privacy to securing digital infrastructure, every aspect of implementation is grounded in operational rigor and public responsibility.*



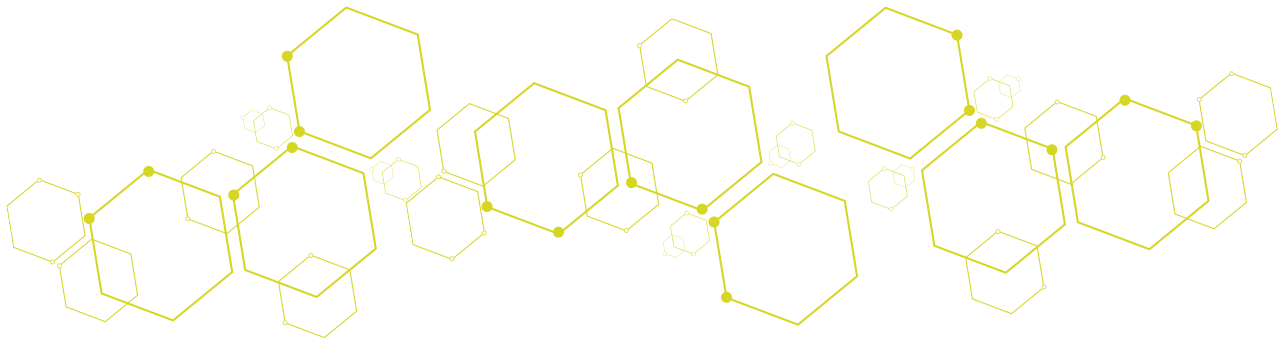


# Ethics and Privacy

## *Privacy Protection Framework*


AI systems introduce new considerations for data protection that extend beyond conventional privacy controls. In accordance with ITS Information Security Policies (PM-25), these systems often rely on large volumes of training data, including personal and sensitive information, and produce outputs that may inadvertently reveal characteristics of the original data. As a result, privacy must be addressed not only at the point of data collection, but across the full lifecycle of model development and use.

In accordance with ITS Information Security Policies (PM-18), Idaho's privacy framework ensures that AI systems handle personal data responsibly and with transparency. It applies privacy requirements at each phase of system design, from dataset curation and model training through deployment, inference, and system retirement. These requirements include data minimization, access controls, purpose limitation, retention management, and transparency, all tailored to the nature and sensitivity of the data involved.



Oversight is coordinated through ITS. The privacy officer works with agencies and departments to conduct privacy impact assessments for new implementations, advise on technical design decisions, and establish consistent evaluation criteria for data use across contexts. For high-risk systems, the privacy officer and designated personnel provide additional review to ensure privacy protections meet state standards and align with statutory obligations.

The framework emphasizes the risks posed by model inference. Based on the existing solution vetting process, agencies and departments work with ITS to assess whether trained models could reveal information about individual records through outputs or model behavior. Mitigation measures must be documented and integrated into deployment plans where such risks are present.



To align privacy oversight with the actual level of risk introduced by AI systems, Idaho applies a structured classification model that integrates relevant ITS Information Security Policies (RA-02 and S.MP-01c). This model accounts for the sensitivity of the data being used, the nature of the outputs produced, and the degree to which decisions informed by the system affect individuals or groups.

### **Privacy Risk Classification Levels**

**Level 1 (Unrestricted):** AI systems that process public, non-sensitive information, where a breach is considered low impact and systems are typically classified as low risk. These systems use readily available public data, produce informational outputs, and do not influence user access to services, benefits, or obligations. Oversight includes baseline privacy controls and periodic documentation reviews.

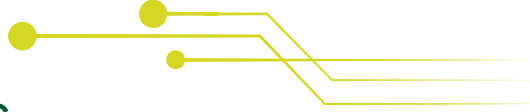
**Level 2 (Limited):** AI systems that process sensitive information that may be protected from public disclosure but could jeopardize privacy if easily accessible, where a breach is considered low impact and systems are typically classified as low to medium risk. These systems use identifiable information or support decisions that indirectly impact services and require moderate privacy controls, including purpose limitation documentation and regular privacy reviews.

**Level 3 (Restricted):** AI systems that process protected personal information, such as personally identifiable information, financial or health records, or federal data, or other information exempt from public disclosure, where a breach is considered medium impact and systems are typically classified as medium to high risk. These systems use this information to make or inform decisions about eligibility, enforcement, or public resource allocation and require comprehensive privacy impact assessments, detailed consent mechanisms, and structured retention policies.

**Level 4 (Critical):** AI systems that process extremely sensitive information where disclosure could potentially cause major damage or injury. A breach is considered high impact and systems are typically classified as high risk. These systems require the highest level of privacy protection, including advanced technical safeguards, explicit review schedules, and stringent data handling procedures.

The classification assigned to a system informs the scope of governance applied to it and must be reviewed if the system is retrained, significantly modified, or used in a new operational context. This classification framework ensures consistent implementation of Idaho's data protection principles across the full lifecycle of model development and use.

# Key Privacy Protection Mechanisms



The state implements privacy requirements through core technical and administrative controls applied in proportion to system risk. These controls support adherence with Idaho's data protection principles and create enforceable boundaries around the use of personal information in AI systems.

In accordance with ITS Information Security Policies (PT-04), consent mechanisms must be specific, understandable, and scalable to the system's function. For systems using sensitive data, agencies and departments must provide clear information about how data will be used, what choices are available to individuals, and how those choices will be respected during system operation.

In accordance with ITS Information Security Policies (S.ITS-02b), data minimization is a default requirement. Agencies and departments must demonstrate that each attribute used in training, inference, or decision logic is necessary to system function. Where attributes are included for optional features or analytic purposes, those uses must be clearly documented and reviewed separately.

In accordance with ITS Information Security Policies (SI-12), purpose limitation and retention controls ensure that data is used only for its declared purpose and not held longer than necessary. Systems must include documentation on how purpose boundaries are enforced, how long data will be retained, what procedures exist for reviewing exceptions, and what procedures will be used for data sanitization.

Access to personal data, including during model development and testing, must be governed by role-based access policies and logged for review. Model outputs that incorporate or reflect personal data must be subject to the same controls as the source data.

These protections should be implemented in proportion to system risk, as determined by the state's classification model.

# *Ethical Implementation*

In accordance with ITS Information Security Policies (P.ITS-01), ethical AI implementation requires systems to align with the values of fairness, accountability, and transparency throughout the lifecycle of development and use. Idaho's framework embeds these principles in concrete expectations for design, evaluation, and oversight.

Transparency is required at both the system and user interaction level. Citizens must be informed when interacting with AI systems, and the system's purpose, decision logic, and limitations must be available in accessible language. Internally, agencies and departments must maintain documentation and explain how outputs are generated and how those outputs are used in decision making.

Fairness is evaluated through pre-deployment testing and post-deployment monitoring. Agencies and departments must assess whether systems produce disparate outcomes across demographic or geographic groups and must document corrective actions when disparities or accessibility issues are identified. These evaluations are required for all medium and high-risk systems and must be updated whenever a model is retrained or repurposed.



Human oversight remains necessary, particularly for systems that inform decisions affecting access to services or benefits. Oversight responsibilities must be clearly assigned, and reviewers must have the authority and tools necessary to intervene, override, or review outcomes.

Finally, all systems must define and document the public value they're intended to create. ITS, agencies and departments must work together to establish metrics to measure that value and evaluate whether it is being delivered over time. Ethical implementation includes a commitment to purposeful, measurable impact beyond risk avoidance.



# Security Controls

AI systems introduce security risks that differ from those associated with conventional information systems. Models can be misled through adversarial inputs, trained on compromised data, or probed to extract sensitive information. Inference endpoints and generative interfaces may become vectors for manipulation or misuse, especially when exposed to external users or integrated with decision making workflows.

Idaho's AI Governance Framework embeds security requirements into each stage of system implementation. These requirements are proportional to system risk, consistent with enterprise cybersecurity best practices, and designed to evolve as agencies and departments build operational maturity and as tools for model protection continue to advance.

## *AI-Specific Security Approach*

AI systems require safeguards that address both their technical architecture and operational behavior. In accordance with ITS Information Security Policies (RA-02 and S.MP-01c), Idaho mandates a set of baseline controls for all AI implementations, with additional requirements for systems operating at medium-or high-risk. Over time, these controls will evolve to include protection against emerging threats such as model poisoning, prompt injection, and inference manipulation—security considerations unique to contemporary AI implementations.

At a minimum, agencies and departments must secure model artifacts using version control, integrity checks, and access restrictions. This applies to training data pipelines, serialized models, inference engines, and associated APIs. In accordance with ITS Information Security Policies (AC-06), access to any of these components must be traceable, auditable, and governed through role-based permissions.

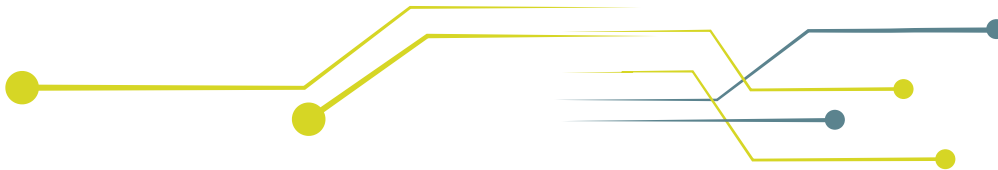
For systems with elevated risk, such as those supporting automated decision-making, generating public-facing content, or operating without human review, security controls must include input validation, query rate limiting, and behavioral monitoring. These measures help detect and prevent adversarial inputs, prompt injection attacks, or reverse engineering through output patterns.

Security requirements scale with Information Systems Classification Levels:

- **Level 1 (Unrestricted):** Basic security controls including authentication, version control, and audit logging.
- **Level 2 (Limited):** Enhanced controls including input validation, output monitoring, and automated security scanning.
- **Level 3 (Restricted):** Comprehensive protections including strict access controls, advanced monitoring, and detailed audit trails for all system interactions.
- **Level 4 (Critical):** Maximum security measures including sophisticated input/output controls, continuous monitoring, adversarial testing, and formal verification where feasible.

Agencies and departments are also responsible for securing their training environment. In accordance with ITS Information Security Policies (PM-14 and P.ITS-01), this includes validating the provenance of training data, using isolated development environments for model experimentation, and restricting code execution in environments that connect to production systems.

Where existing controls are insufficient, agencies and departments must identify gaps in implementation plans and consult with the **AI Innovation Team** and agency and department security leads to define compensating controls or adoption timelines for advanced capabilities.



## *Enterprise Security Integration*

AI systems must operate within the broader enterprise cybersecurity infrastructure. Security expectations for AI systems are embedded within Idaho's established security operations, identity and access controls, monitoring platforms, and incident response plans. All AI-related services, whether internal, cloud-hosted, or vendor-supplied, must be monitored alongside other enterprise applications. In accordance with ITS Information Security Policies (AU-02), logs from inference endpoints, access control events, model versioning, and output anomalies must be routed to the agencies or departments existing security monitoring stack for aggregation and alerting.

Identity and access governance must extend to all users and systems interacting with model APIs, training data, and deployment environments. Where agencies and departments use federated identity or privileged access management, AI assets must be integrated into those same platforms and enforcement policies.

In accordance with ITS Information Security Policies (IR-07), AI-specific events must be reflected in incident response playbooks. For example, prompt abuse in a generative interface, unexpected shifts in model behavior, or indicators of model extraction must trigger escalation and remediation workflows. These updates must be coordinated by the agency or department Chief Information Security Officer (CISO), or equivalent role.

This integration ensures that AI systems are governed by the same institutional safeguards that protect the broader digital environment, preventing them from becoming a separate source of unmanaged risk.

# Comprehensive Accountability

Security is not the responsibility of a single team or role. Idaho's framework assigns clear accountability across the AI lifecycle to ensure that risks are understood and mitigated at every stage.

Implementation teams are responsible for embedding security controls into model architecture, preprocessing workflows, and system interfaces. This includes preparing documentation on model limitations, threat exposure, and operational constraints.

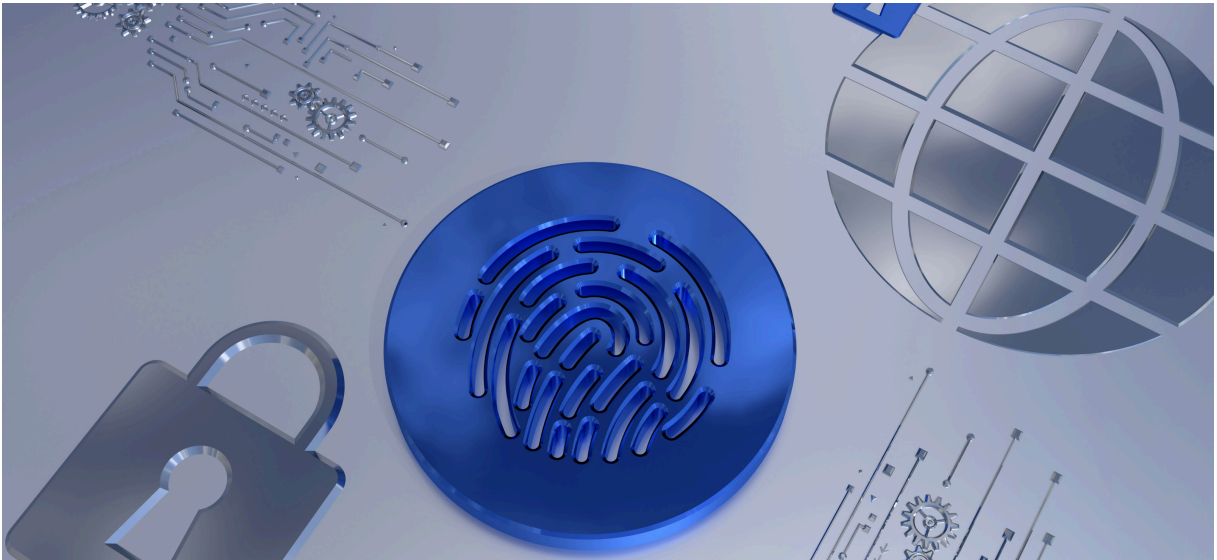
Agency and department IT staff are responsible for validating system security posture prior to deployment and ensuring alignment with existing cybersecurity programs. In accordance with ITS Information Security Policies (SA-03), they are expected to review test results, risk assessments, and any deviation requests prior to production use.

The **AI Innovation Team** maintains oversight for emerging risks, supports interagency coordination on advanced security patterns, and contributes to the continuous improvement of statewide practices. In cases of system failure or public impact, this team helps inform post incident evaluations and recommend governance adjustments.

Security accountability is tracked through formal documentation and periodic audits. Agencies and departments must maintain system-level risk registers and demonstrate that responsibilities have been assigned, executed, and reviewed throughout implementation.



# Advanced Security Controls



Certain use cases demand more sophisticated defenses beyond baseline protections. These include systems that serve external users, generate high-stakes outputs, or operate in partially autonomous settings.

In accordance with ITS Information Security Policies (PL-02 and PL-11), agencies and departments deploying such systems must begin planning for advanced capabilities, including:

- Adversarial robustness testing to evaluate susceptibility to input manipulation.
- Model fingerprinting to detect unauthorized reuse or exfiltration.
- Drift detection to identify shifts in model behavior that may indicate data or system changes.
- Output filtering for generative systems to block disallowed or risky content.

These controls may not be readily available for all use cases, and Idaho does not require immediate implementation. However, agencies and departments must evaluate the relevance of these techniques during system design and maintain a roadmap for phased adoption as capabilities mature.

The AI Innovation Team will continue to support the development and piloting of advanced controls and may issue implementation guidance for specific tools or frameworks as they reach operational maturity.



# Vendor Security Management

When AI capabilities are sourced through third-party vendors, whether as pre-built models, APIs, or platform integrations, agencies and departments remain accountable for system security. Idaho requires that vendor-supplied systems undergo the same level of review and governance as those developed internally.

In accordance with ITS Information Security Policies (SA-05), agencies and departments must obtain documentation from vendors describing the model's architecture, training data practices, security testing, and compliance with Idaho's privacy and security standards. For high-risk systems, agencies and departments may require additional information regarding model validation, third-party audits, or the presence of embedded controls to mitigate inference risk, output abuse, or data leakage.

In accordance with ITS Information Security Policies (SA-04), security expectations must be defined contractually. These include notification obligations for security events, audit access, data handling procedures, and software change control processes. Where vendors cannot meet these expectations directly, agencies and departments must implement compensating controls to reduce exposure.

In accordance with ITS Information Security Policies (RA-03), vendor risk assessments must be conducted during procurement and reassessed upon major product updates or scope expansions. Systems provided by vendors must be tracked within the AI System Inventory and subject to the same classification and monitoring requirements as in-house solutions.

Approval requirements scale based on potential impact, with higher-risk changes requiring more extensive review. Implementation verification includes comprehensive testing, phased deployment for high-impact changes, post-implementation verification, and enhanced monitoring following significant modifications. Agencies and departments must conduct regular audits of vendor-supplied systems against established state standards, with results incorporated into the implementation matrix (see pages 47 and 48 in this section).

## Executive Takeaway

*Idaho's security approach extends beyond traditional information security to address AI-specifics within existing enterprise security infrastructure. By working to implement specialized protections for models, training data, and inference operations, the framework safeguards AI systems throughout their lifecycle. This balanced approach combines technical controls with clear accountability, ensuring appropriate protection without impeding innovation.*

# Risk Management



AI systems introduce a dynamic and evolving risk landscape. Unlike conventional software, AI models learn from data, adapt to shifting inputs, and often operate in probabilistic ways. These characteristics create novel technical, operational, and ethical risks that may not be fully understood at the time of deployment and can evolve significantly during real-world use.

Idaho's framework treats risk management as an integrated continuous process that spans the AI system lifecycle and emphasizes early identification, clear accountability, ongoing monitoring, and structured mitigation. Agencies and departments are expected to manage risk as an evolving practice—one that adapts to each system's behavior, user interactions, and service context, rather than relying on a static checklist.

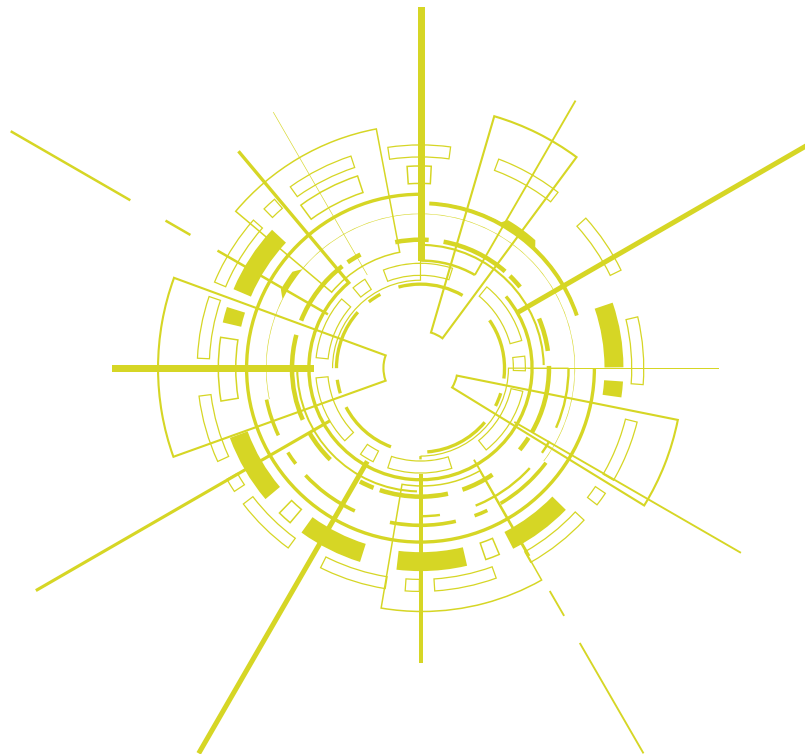
# Risk Management Lifecycle

Risk awareness must begin at the design stage. Implementation teams are required to document potential risks during system planning and keep this record updated throughout development, deployment, and long-term operation. These risk registers should include technical concerns, such as data quality issues, inference variability, or architectural limitations, as well as fairness, privacy, and operational dependencies.

In accordance with ITS Information Security Policies (RA-03), each system's risk register should be reviewed at key decision points, including project intake, classification, and deployment approval. Risk profiles are expected to evolve over time. When a model is retrained, repurposed, or integrated into a new workflow, agencies and departments should reassess its classification and oversight requirements accordingly.

In accordance with ITS Information Security Policies (RA-02), risk registers must explicitly document the Information Systems Classification Level of all data being processed by the AI system:

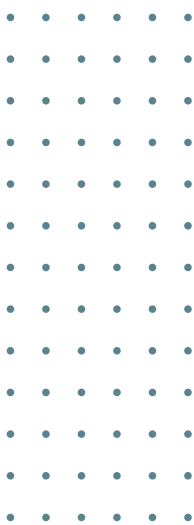
- **Level 1 (Unrestricted):** Public information with minimal privacy or security concerns.
- **Level 2 (Limited):** Sensitive information requiring basic safeguards.
- **Level 3 (Restricted):** Protected information requiring comprehensive controls.
- **Level 4 (Critical):** Extremely sensitive information requiring maximum protection.





Once deployed, systems must be actively monitored for indicators of drift, degradation, or unanticipated effects. Monitoring should track both system performance metrics (e.g., accuracy, latency, and prediction quality) and governance indicators (e.g., override frequency, stakeholder complaints, or fairness imbalances across population groups). In accordance with ITS Information Security Policies (RA-07), where meaningful deviation from expected behavior occurs, mitigation planning should begin promptly.

Risk mitigation should be targeted and proportionate. In some cases, adjustments to model parameters or retraining may suffice. In others, rollback procedures, workflow changes, or policy interventions may be needed. High-risk or high-impact systems require response plans defined in advance, with clear triggers, escalation paths, and authority for intervention.



**Mitigate**  
what  
matters

The learning function of risk management is equally important. Each implementation team is expected to reflect on what risks materialized, how they were handled, and what could be improved. These lessons should inform future risk assessments, refine design practices, and contribute to a more mature and resilient statewide AI capability.

The **AI Innovation Team** coordinates this cycle according to the defined escalation pathways outlined on pages 14-15 in Section 2. It maintains shared risk scenarios, supports the dissemination of mitigation patterns, and convenes working groups to address cross-agency and department challenges or emerging concerns. For high-severity incidents, the **AI Innovation Team** coordinates with the **AI Executive Committee** following the governance structure interactions defined in Section 2 (see pages 14-15).

# *AI Incident Response and Recovery Framework*

Even with strong oversight, AI systems may fail in unexpected ways. Idaho's AI incident response framework provides a pathway for managing errors, service disruptions, fairness failures, and other significant anomalies in production systems when they occur.

In accordance with ITS Information Security Policies (IR-08), AI-specific incident types, such as hallucinated outputs, misclassification of inputs, inference bias, or inappropriate content generation, must be formally recognized within agency and department response plans. These incidents may not always resemble conventional IT failures, but they demand the same level of discipline and accountability in response.

Each agency and department must maintain an AI incident response protocol that defines categories of severity, roles and responsibilities, communication requirements, and remediation procedures. Low-severity issues may be resolved by the implementation team. Moderate or recurring issues should involve data governance, privacy, or security staff. High-severity incidents, particularly those involving public trust, rights, or legal risk, must be escalated to the **AI Innovation Team** and, where warranted at the discretion of the **Innovation Team**, escalated to the **AI Executive Committee**.

Response workflows include four key stages: identification, containment, resolution, and recovery. In accordance with ITS Information Security Policies ((IR) Incident Response Family), agencies and departments must be able to detect the incident, assess its implications, contain further risk or harm, restore service functionality, and document the entire process. This includes not only technical resolution but updates to training, workflows, or oversight policies where needed.

In accordance with ITS Information Security Policies (IR-04), every major incident must result in a formal post-event review. These reviews should identify root causes, assess whether original risk mitigation strategies were adequate, and recommend adjustments. Findings may also be shared across agencies and departments to support cross-learning and continuous improvement.

The goal is not to eliminate all failures; such a standard is neither realistic nor productive in dynamic systems. Instead, the state responds consistently through its established governance bodies, improves over time according to the processes outlined in Section 2 (see pages 14-15), and sustains public confidence through visible accountability and transparent oversight when failures occur.

# Cross-Agency and Department Collaboration

AI systems increasingly touch multiple agencies and departments, shared populations, and interdependent services. As a result, risk management cannot be conducted in isolation. Idaho's framework establishes formal structures for cross-agency and department collaboration in risk identification, mitigation, and learning.

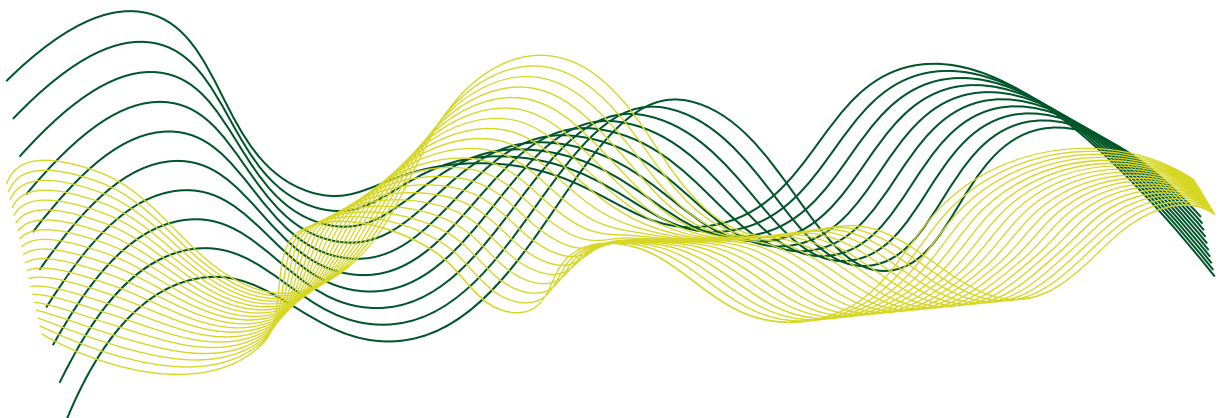
The AI Innovation Team coordinates periodic working sessions with risk, privacy, and technical leads from across the enterprise. These forums are used to review common risk scenarios, align classification decisions, and discuss early indicators of systemic issues.

Agencies and departments that operate shared models, use federated datasets, or participate in integrated workflows must coordinate risk classification, deployment review, and model governance. Shared systems require joint ownership of documentation, post-deployment monitoring, and escalation protocols.

To support transparency and coordination and in accordance with ITS Information Security Policies (RA-03), Idaho maintains a shared repository of risk mitigation strategies, incident summaries, and evaluation tools. Agencies and departments are encouraged to contribute implementation experiences to this repository, particularly in high-risk domains or novel use cases.

Collaboration is not limited to known risks. When new vulnerabilities, patterns of failure, or policy questions arise, the state will use cross-agency and department coordination mechanisms to evaluate response options and update governance expectations.

Effective AI risk management requires a networked response. By working across organizational boundaries, Idaho ensures that risk knowledge is diffused, remediation is shared, and oversight remains consistent across programs, agencies and departments, and services.





# Standards Alignment

## *NIST AI Risk Management Framework Integration*



In accordance with ITS Information Security Policies (P-ITS-01), Idaho's AI Governance Framework fully integrates with the NIST AI RMF, the federal standard for responsible AI implementation, and the associated AI RMF Playbook. This alignment ensures compatibility with federal systems and maintains flexibility to address state-specific requirements.

The AI RMF provides a structured approach to managing AI risks through four core functions: GOVERN, MAP, MEASURE, and MANAGE. Each function addresses distinct aspects of risk management throughout the AI lifecycle, creating a comprehensive approach to responsible implementation. Idaho's framework implements each function through specific mechanisms tailored to our state context.

Our implementation of the **GOVERN function** establishes clear authority and direction through interconnected governance bodies. The AI Executive Committee, Ethics Advisory Committee, and AI Innovation Team create the organizational structure needed for effective oversight, with clearly defined responsibilities and interaction patterns. The governance structure ensures appropriate leadership and direction for AI activities throughout state government.

The **MAP function** identifies potential issues early in the AI lifecycle through structured risk assessment processes. Our approach implements multi-dimensional risk evaluation across domains including privacy, security, and fairness, creating comprehensive understanding of potential impacts. The risk assessment methodology incorporates diverse stakeholder input, addresses supply chain risks from external dependencies, and provides clear system categorization driving appropriate oversight requirements.

For the **MEASURE function**, we've established comprehensive performance testing methodologies and evaluation approaches. These verification mechanisms ensure AI systems work as intended and remain safe and fair throughout operation. Our approaches include explainability assessment, fairness evaluation across demographic groups, control effectiveness verification, real-time metric tracking, and citizen experience evaluation.

The **MANAGE function** implements appropriate controls and response mechanisms throughout the AI lifecycle. Our approach includes technical safeguard deployment proportional to risk, AI-specific incident response procedures, regular control effectiveness reviews, and process refinement based on operational experience.

Idaho's framework fully aligns with the NIST AI RMF principles, promoting AI systems that are valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with potential harmful impact managed.

This alignment creates several strategic advantages for Idaho's AI implementation. The state can readily leverage federal guidance as it emerges, applying best practices to state challenges. Idaho can adapt more efficiently to evolving regulatory requirements as national policy develops. The framework's structured approach also facilitates reporting and compliance activities when interacting with federal agencies or pursuing federal funding opportunities.

## *Generative AI Considerations*

Generative AI (GenAI) systems, including large language models, image synthesis engines, and multimodal content generators, introduce operational and policy changes that differ in nature from those associated with traditional AI systems. These technologies generate new content in response to prompts and can produce output that is probabilistic, unpredictable, and occasionally unverifiable. This presents novel risks in areas such as content integrity, attribution, privacy, intellectual property, and the public perception of automation.

To guide agencies and departments in assessing and managing these risks, Idaho references the NIST AI RMF and its companion Generative AI Profile, which together provide structured guidance for identifying and mitigating risks unique to generative systems. Agencies and departments must:

1. Establish comprehensive prompt libraries with security controls and review processes.
2. Implement robust content filtering mechanisms aligned with state guidelines.
3. Maintain human review protocols calibrated to the system's risk tier.
4. Deploy output monitoring to detect hallucinations, bias, or inappropriate content.
5. Implement content attribution standards for transparency.

To operationalize these expectations, the state recommends the adoption of a **standardized use policy** for GenAI, tailored to public sector service delivery and grounded in existing information security principles. The use policy, located in Appendix D, is intended to be incorporated directly into agency and department level information security and governance manuals.

For Idaho agencies and departments, this alignment supports several goals. It enables risk classification to account for generative capabilities, ensures that content-producing systems are integrated into privacy and security oversight processes, and prepares the state to advance an emerging federal AI compliance ecosystem. At the agency and department level, it encourages early examination of whether generative features are appropriate for a given service context and, if so, how they should be governed during implementation and use.

## *Interoperability and Data Standards*

As AI capabilities expand across Idaho's public sector, the ability to integrate these systems into a cohesive digital environment becomes increasingly important. Interoperability serves as a foundation for delivering coordinated public services, ensuring data consistency, and enabling oversight across decentralized implementations. Idaho's framework defines interoperability goals and reference practices to support the integration of AI systems into the state's broader information technology ecosystem, recognizing that agency and department maturity in this area may vary.

In accordance with ITS Information Security Policies (PL-02, PL-08 and PM-07), the framework encourages alignment with Idaho's existing enterprise architecture strategy, including shared services for identity, data cataloging, and cross-platform integration. AI systems should be designed to operate within these environments when feasible, leveraging common metadata conventions, schema definitions, and governance structures already in use or under development. Where enterprise services are not yet available or adopted by an agency or department, implementations should demonstrate forward compatibility and define transitional integration strategies as part of their technical planning.

Agencies and departments are expected to use documented interface specifications when developing or integrating AI systems that exchange data with external services or other state systems. These specifications include guidance on authentication, request-response formatting, error handling, and documentation. For systems that support real-time integration, such as decision support models embedded in service portals or call center tools, agencies and departments should work with technical leads to evaluate performance requirements and test for reliability under typical operational conditions.

Semantic interoperability represents a long-term objective. As AI systems begin to produce structured classifications, recommendations, or prioritizations that inform downstream processes, the ability to ensure consistent interpretation across systems will become increasingly important. Agencies and departments are encouraged to contribute to cross-agency and department efforts that define controlled vocabularies and aligned data definitions in domains where shared models are anticipated.



To support implementation, the framework includes reference architectures for common AI use cases, such as document classification, language-based search and summarization, and predictive resource allocation. These templates are intended as starting points, not mandates, and should be adapted to agency- and department-specific contexts. Where possible, agencies and departments are encouraged to reuse tested patterns, promote modularity, and participate in knowledge sharing to accelerate adoption and reduce duplication of effort.

Interoperability testing is recommended prior to deployment of systems operating in environments where data exchange, shared services, or user-facing integrations are expected. Testing should evaluate adherence to interface specifications, confirm compatibility with role-based access models, and ensure that outputs can be reliably consumed by receiving systems. For higher-risk systems or those intended for shared use, technical reviews may be coordinated with the **AI Innovation Team**.

Idaho's approach to interoperability recognizes that technical alignment is a process, not a fixed condition. The framework establishes expectations for system compatibility, promotes consistency in interface and data design, and supports the gradual development of shared infrastructure that enables AI implementation efficiently and responsibly across state agencies and departments.



# *Additional Standards Alignment*

Idaho's AI governance framework integrates with a broader ecosystem of national and international standards that provide recognized best practices for privacy, security, and risk management. This alignment enables consistency across state agencies and departments, supports compatibility with federal systems, and ensures that the state remains well-positioned to comply with emerging regulatory requirements and policy expectations.

The framework draws directly from the **NIST Privacy Framework**, which provides a structured model for managing privacy risk in data-driven systems. The core principles of the NIST Privacy Framework, such as data minimization, purpose specification, role-based access, and transparency, are applied throughout Idaho's governance processes. These principles are also reflected in the **Fair Information Privacy Principles**, which have long served as the foundation for federal privacy policy and are widely adopted by U.S. states. Idaho's privacy posture, particularly as it relates to AI-enabled data use, is grounded in these frameworks and adapted to the operational and legal context of public sector service delivery.

For information security and operational resilience, the framework references NIST 800-53, which establishes internationally recognized standards for information security management systems. Idaho incorporates key components of NIST 800-53, including structured risk assessment, asset classification, access control, cryptographic protection, and incident response, into the design and operation of AI systems classified as medium- or high-risk. These controls are applied in conjunction with Idaho's own enterprise cybersecurity policies and provide a consistent foundation for agency implementation.

In addition, the framework incorporates elements of the NIST Cybersecurity Framework, particularly in the areas of identify, protect, detect, respond, and recover. These categories extend to cover model-level concerns such as training data provenance, inference behavior monitoring, and generative content safeguards, when applicable. This extension allows AI-specific security risks to be addressed within the same architectural and operational systems used to protect the state's broader digital infrastructure.

By treating these standards as operational guides rather than passive references, Idaho ensures that AI systems are developed, deployed, and maintained in alignment with both industry best practices and the unique responsibilities of public service. This approach facilitates smoother intergovernmental collaboration, reduces administrative friction in procurement and oversight, and strengthens public confidence in the state's use of AI technologies.

# National AI Policy Alignment

As national policy on AI continues to evolve, Idaho's governance framework has been developed to remain compatible with emerging federal guidance and allow for gradual, locally informed implementation. Executive Orders, guidance from the Office of Management and Budget (OMB), and federal initiatives such as the NIST AI RMF are shaping the expectations for trustworthy AI across public sector domains. Idaho's framework enables state agencies and departments to participate in this broader policy landscape and focus on pragmatic, mission-aligned use of AI within state operations.

Idaho draws from these policy developments to inform principles, risk structures, and implementation priorities rather than replicate federal mandates in full. For example, the emphasis on regulatory barrier reduction, economic competitiveness, and national security considerations found in Executive Order 14179 (Removing Barriers to American Leadership in Artificial Intelligence) aligns with Idaho's efforts to prioritize value delivery and operational efficiency metrics to quantify economic benefits and establish strong security requirements to protect sensitive systems and data.

Idaho's alignment also positions the state to participate in federally supported initiatives, such as intergovernmental pilot programs, shared infrastructure platforms, and grant opportunities that may prioritize frameworks compatible with national guidelines. Agencies and departments that work with federally regulated data, such as Medicaid claims, workforce data, or criminal justice records, must be prepared to demonstrate adherence to evolving federal expectations around AI risk and model auditing, among others.

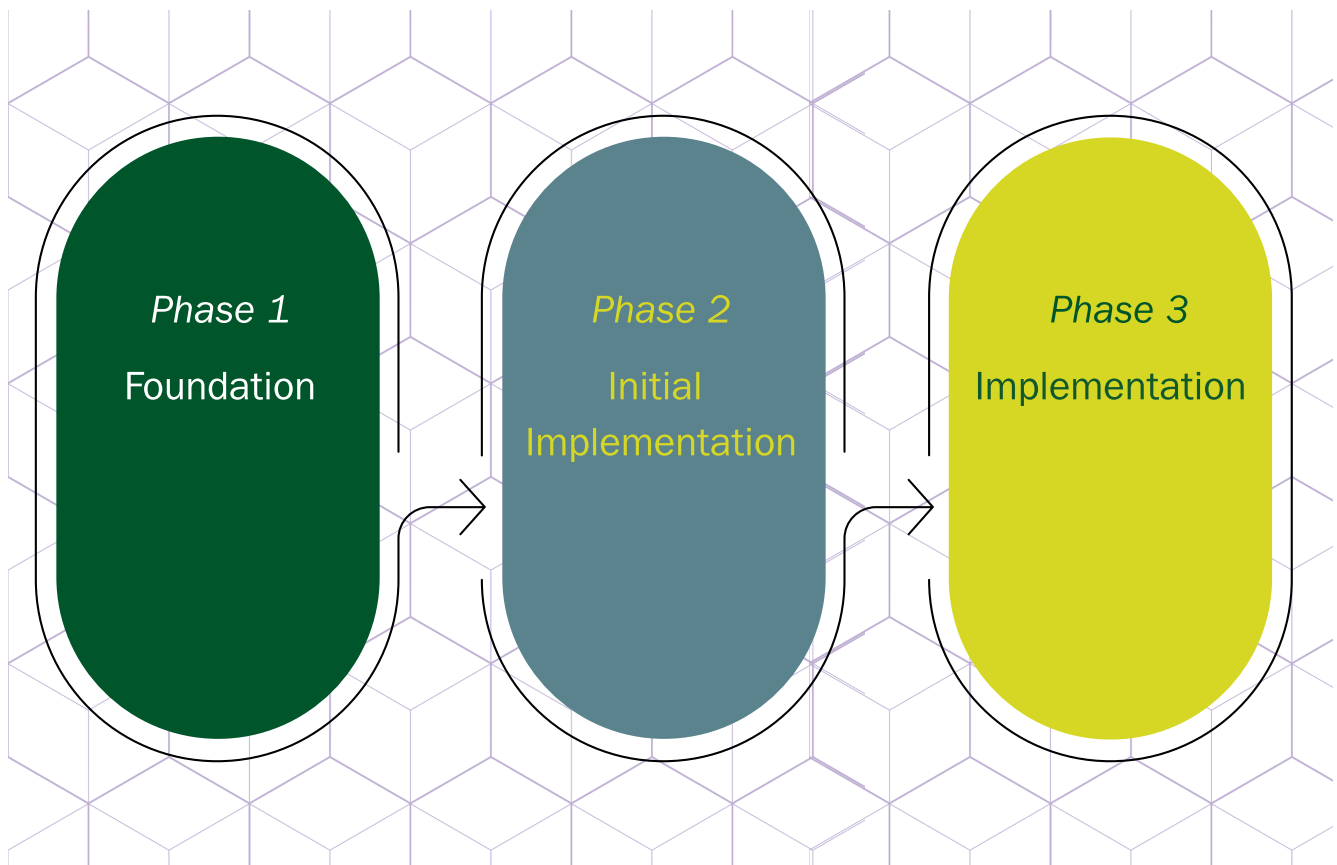
Because federal policy is still in development, Idaho's framework remains adaptable. The **AI Innovation Team** is responsible for monitoring changes to federal AI requirements and issuing interpretive guidance as needed. Agencies and departments are not expected to implement every element of national frameworks immediately, but they are encouraged to assess how their systems align with emerging federal standards and identify areas where future readiness may be necessary.

This forward-compatible approach allows Idaho to remain aligned with national direction without compromising the autonomy, budgetary constraints, or domain-specific needs of individual agencies and departments. It also supports interoperability and collaboration with federal partners by ensuring that state-level AI systems are built on comparable governance principles.



# Framework Implementation Matrix

To ensure internal alignment and transparency, Idaho maintains a structured implementation matrix that maps elements of the AI governance framework to relevant standards, policy objectives, and agency and department operational goals. This matrix functions as both a planning tool and a documentation resource, allowing agencies and departments to understand how governance requirements correspond to enterprise IT strategy, risk management obligations, and external standards such as the NIST AI RMF or NIST 800-53.



The implementation matrix connects directly to the risk classification model (outlined on pages 16-17 in Section 2) by mapping framework components to appropriate governance tiers. This creates a direct relationship between a system's risk score and the governance requirements it must meet, ensuring proportional oversight. When risk classifications change following the variance process (outlined on page 22 in Section 2), the matrix provides clear guidance on which additional governance components activate or may be streamlined. For more information on implementation phases, see Section 4.

# AI Framework Implementation Overview

## Risk-Aligned Governance and Implementation Timeline

<u>Idaho Framework Component</u>	<u>NIST AI RMF Function</u>	<u>Tier 1 Requirements</u>	<u>Tier 2 Requirements</u>	<u>Tier 3 Requirements</u>	<u>Primary Responsibility</u>	<u>Implementation Plan Timeline</u>
Governance Structure	GOVERN	Standard ITS vetting + AI Innovation Team notification	AI Innovation Team + Technical Review Board	Executive Committee + Ethics review	Agency and Department IT leaders + ITS, AI Innovation Team	Phase 1
Risk Assessment	GOVERN, MAP	Standard ITS vetting	AI Innovation Team validation	Technical Review Board + Ethics review	ITS + Agency and Department Implementation Teams	Phase 1
Data Management	MAP, MEASURE	Standard documentation	Enhanced protections	Comprehensive controls	Information Owner, Privacy Officer	Phase 2
Model Documentation	MAP	Concept Brief	Technical Documentation	Full model cards	ITS + Agency and Department Implementation Teams, Technical Review Board	Phase 2
Security Controls	MEASURE, MANAGE	Basic controls	Enhanced monitoring	Comprehensive protection	ITS (CISO), Agency and Department security teams	Phase 2
Transparency	GOVERN	System labeling	Basic explanation	Full explainability	ITS + Agency and Department Implementation Teams	Phase 3
Monitoring	MANAGE	Periodic review	Routine monitoring	Continuous oversight	ITS + Agency and Department Implementation Teams + AI Innovation Team	Phase 3
Incident Response	MANAGE	Standard protocols	Enhanced procedures	Specialized playbooks	ITS + AI Innovation Team	Phase 3



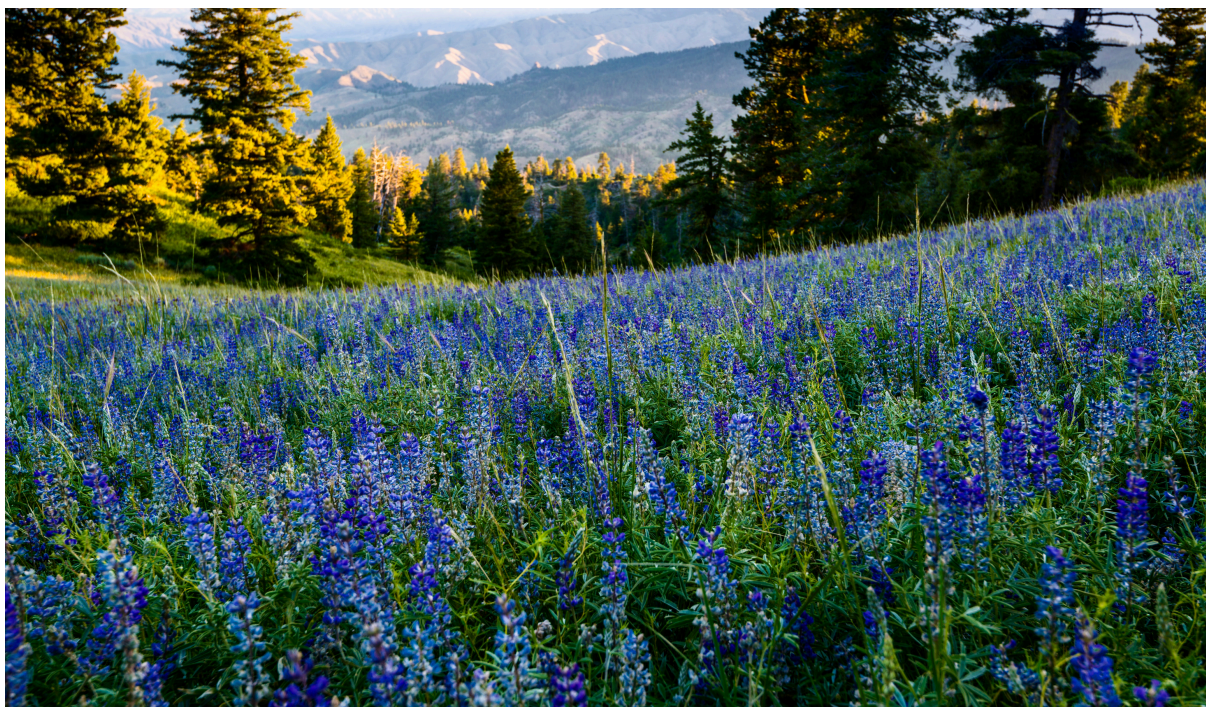
Agencies and departments should use this matrix to assess current governance maturity and plan implementation activities. Each component includes specific deliverables and documentation requirements detailed in corresponding framework sections. The matrix follows RACI (Responsible, Accountable, Consulted, Informed) principles, with primary responsibility assigned recognizing cross-functional input. Implementation timelines align with the phase approach in Section 4, with flexibility for agency- and department-specific prioritization based on existing AI activity and resource availability.

The **AI Innovation Team** updates the matrix annually, or as major policy updates require. Changes are informed by implementation, feedback, federal policy updates, and new tools or standards that affect the applicability of governance components.

The matrix remains lightweight and actionable. It does not impose additional requirements beyond what is already defined in the framework, but it does provide traceability and structure for agencies and departments working to implement AI responsibly and consistently within the enterprise environment.

## *Executive Takeaway*

*The successful implementation of responsible AI depends on sound technical approaches and well-designed operational models. By grounding deployment in strong data protection practices, aligning to establish standards, and measuring success through impact, Idaho ensures that AI delivers valuable outcomes consistently across state government.*





# 4 Strategic Roadmap



This section outlines Idaho’s phased approach to AI governance implementation, balancing immediate capability development with long-term institutional maturity. By structuring adoption across four deliberate phases, the roadmap enables agencies and departments to build governance expertise incrementally and deliver early value from lower risk use cases. This strategic sequencing creates a foundation of experience, shared resources, and organizational readiness that supports the responsible scaling of AI across state government.

# Implementation Phases

The implementation of Idaho's AI governance framework follows a strategic roadmap designed to build governance capacity, technical maturity, and operational consistency over time. Each phase includes specific deliverables and organizational milestones enabling agencies and departments to scale AI adoption and align with state standards for privacy, security, ethics, and oversight. The implementation plan will evolve and adapt based on ongoing feedback and operational iteration over time.

## *Phase 1: Foundation (Months 0-6)*

**Objective:** Establish statewide governance structures, agency and department roles, and foundational capabilities necessary to initiate AI oversight and support early-stage project planning.

**Key Activities:**

Governance bodies are formally established, including the AI Executive Committee, Ethics Advisory Committee, Technical Review Board, and the AI Innovation Team as described in Section 2. These structures provide centralized policy direction, risk oversight, and technical advisory functions.

Each executive branch agency and department identifies internal AI leads responsible for implementation coordination. This includes designating points of contact for privacy, information security, procurement, and data governance.

The AI Innovation Team partners with agencies and departments to begin populating an initial AI System Inventory and conduct Privacy Impact Assessments for known or anticipated use cases (see page 24 in Section 2 and pages 27-28 in Section 3). This documentation helps establish a statewide view of AI activity and inform capacity planning for subsequent phases.

Baseline training is deployed to all participating agencies and departments, covering risk classification methodology (see page 16 in Section 2), governance processes (see pages 20-21 in Section 2), and ethical implementation expectations (see page 30 in Section 3).

The AI Concept Brief template is incorporated into the standard solution vetting process. During intake, this brief is automatically generated to document proposed use cases, data sources, system purpose, and anticipated decision impact (see pages 20-21 in Section 2).

Integration planning begins to align AI governance with existing cybersecurity, procurement, and data management frameworks (reference pages 32 in Section 3 and pages 41-43 in Section 3 for guidance).

**Deliverables:**

- Governance body charter and meeting cadence are established.
- Agency and department AI implementation leads and points of contact assigned.
- Initial system inventories completed and submitted to the AI Innovation Team.
- AI Concept Brief is fully integrated into existing solution vetting process and generates automated template based on sample submissions.
- Completion of foundational training programs in risk classification and oversight procedures.

**Outcome:** Governance capacity is established across the enterprise. Agencies and departments are equipped to identify AI-related activity, document use cases and prepare for project intake and initial classification.

## *Phase 2: Initial Implementation (Months 7-12)*



**Objective:** Pilot AI governance processes across selected use cases, validate oversight mechanisms, and deploy initial systems with risk classification and lifecycle monitoring in place.

**Key Activities:**

In accordance with ITS Information Security Policies (P.ITS-03), agencies and departments begin submitting AI project proposals through the existing solutions vetting process. Tier 1 and Tier 2 systems are classified using the risk model outlined in Section 2 (see pages 16-17) and reviewed under the appropriate approval pathway referenced in Section 2 (see page 20).

Pilot implementations are selected across a variety of functional domains such as citizen information assistants, document summarizers, or internal analytics or productivity tools. These use cases are subject to privacy review, security controls validation, and transparency planning (see page 24 in Section 2 and pages 28 and 31 in Section 3).



Each system is launched with a documented governance plan, including reviewer roles, escalation paths, and reporting procedures aligned with the lifecycle oversight model (see page 20 in Section 2).

Early feedback mechanisms are implemented to gather insights from system users, reviewers, and affected stakeholders. Agencies and departments begin tracking performance indicators, override frequency, and system stability (see pages 30 and 37 in Section 3).

Findings from pilot projects are collected and synthesized to improve training, refine vetting procedures, and update technical documentation requirements.

**Deliverables:**

- Approved AI Concept Briefs and classification records for pilot systems.
- System deployment packages with documented privacy, fairness, and security mitigations.
- Post-deployment reviews and stakeholder feedback summaries for each pilot.

**Outcome:** Governance processes are exercised and refined through pilot deployments. Agencies and departments develop capacity to apply oversight in practice, and the state validates its core governance model in operational settings.

## *Phase 3: Implementation (Months 13-24)*

**Objective:** Expand governance maturity, implement oversight for higher-risk systems and deepen integration across data, security, and lifecycle management domains.

**Key Activities:**

Agencies and departments begin onboarding higher-risk systems that require Ethics Advisory Committee and Executive Committee review in accordance with the Tier 3 governance process outlined in Section 2 (see page 20).

AI systems developed during this phase are built and validated with documented data sources, clear operational intent, and defined performance thresholds. Agencies and departments are responsible for demonstrating how models support intended outcomes and how outputs will be reviewed, interpreted, or challenged.

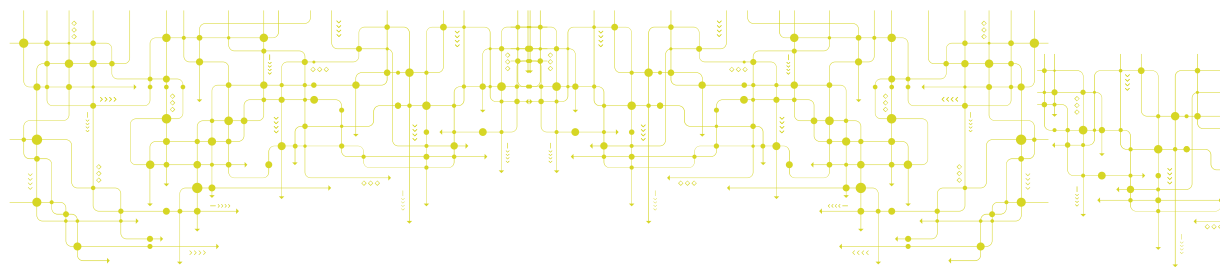
Security controls are integrated directly into the system architecture. This includes input validation, access management, and monitoring for abnormal inference behavior, aligned with Section 3 (see page 34) and commensurate with risk classification.

Structured risk assessments are conducted prior to deployment. These assessments evaluate privacy impact, fairness considerations, and operational risks using Idaho's classification and review procedures (see pages 27, 30, and 36 in Section 3). The appropriate governance bodies must review and approve mitigation plans before system launch.

Documentation of system behavior becomes an essential requirement. Agencies and departments must describe how the model produces its outputs, how those outputs will be used in decision-making, and where human oversight is maintained (see page 20 in Section 2 and page 30 in Section 3).

Agencies and departments prepare systems for deployment by finalizing mechanisms for performance monitoring, confirming data retention and access protocols, and establishing escalation channels for feedback, error correction, or citizen concerns.

Cross-agency and department collaboration structures are launched for shared use cases, enabling the reuse of evaluation templates, audit protocols, and pre-approved infrastructure deployments (see page 40 in Section 3).



### **Deliverables:**

- Reviewed and approved Tier 3 project documentation, including model design, risk assessments, privacy and security reviews.
- Operational deployment packages with audit-ready documentation of system behavior, reviewer roles, and monitoring indicators.
- Cross-agency and department working group charters and shared model evaluation resources.

**Outcome:** Idaho agencies and departments demonstrate capacity to deploy and govern high-risk AI systems using documented, repeatable practices. Technical controls, review structures, and transparency mechanisms are fully engaged, and the state has begun to institutionalize cross-agency and department collaboration and lifecycle monitoring for AI systems in production.

## *Phase 4: Optimization (Months 25-36)*

**Objective:** Institutionalize AI governance across state enterprise functions, expand technical oversight capabilities, and formalize integration of governance procedures into procurement, planning, and policy.

### **Key Activities:**

Agency and department procurement and IT planning processes are updated to include AI risk classification and review checkpoints. Model documentation, oversight requirements, and transparency expectations are included in standard vendor onboarding and evaluation workflows (see page 35 in Section 3).

The GenAI Use Policy becomes a standing operational requirement for all systems involving content synthesis. Agencies and departments implement prompt controls, validation workflows, and disclosure protocols consistent with Section 3 (see pages 41-44).

The framework implementation matrix (see page 48 in Section 3) is used to support agency and department planning, internal audits, and cross-agency and department reporting. This matrix allows executive leadership to track governance adoption, risk management posture, and alignment with ITS strategic goals.

Monitoring infrastructure is matured to potentially include anomaly detection, fairness evaluations, and model drift tracking. These capabilities are coordinated through technical working groups and supported by shared tools (see page in Section 3 and page in 4.2.2).

Governance policies and documentation are reviewed and updated to reflect changes in federal direction, including guidance from NIST, OMB, and executive orders related to AI use in government (see pages 45-46 in Section 3).

Agency and department training is updated to reflect emerging practices, including dynamic consent, adaptive oversight, and AI security trends. Communications and documentation tools are scaled to support ongoing transparency, staff awareness, and accountability.

### **Deliverables:**

- Updated procurement and project planning materials embedding AI governance checkpoints.
- Full integration of the GenAI Use Policy into operational guidance and system documentation.
- Statewide rollout of the implementation matrix with agency- and department specific targets and timelines.
- Updated AI Governance Framework, published for internal use, with policy revisions and performance data.

**Outcome:** AI governance is embedded in the institutional operations of Idaho State government. Systems are developed, deployed, and managed with consistent review, transparency, and performance accountability, supported by shared tools and documented procedures across the enterprise.

## *Scaling for Agency Size and Resources*

Idaho's AI Governance Framework is designed to be both rigorous and adaptable. Agencies and departments vary widely in mission, staffing, technical maturity, and implementation capacity. The governance principles outlined in Sections 2 and 3 apply uniformly across state government, but the application of those principles must scale appropriately to the size and complexity of each agency and department's operations.

Smaller or resource-constrained agencies and departments are not exempt from oversight requirements, but they are not expected to replicate the internal governance structures of larger departments and agencies. Instead, the framework enables shared support, streamlined documentation, and targeted engagement with centralized governance bodies to ensure that oversight remains feasible, proportional, and effective.

### **Tailoring Expectations**

Each phase of the implementation roadmap (see page 51 in this section) includes deliverables and activities that can be scaled in scope or staffing intensity based on the agency or department capacity. For example:

- In Phase 1, smaller agencies or departments may adopt governance templates and policies developed by the **AI Innovation Team** rather than creating them independently.
- In Phase 2, project teams may coordinate directly with ITS and the **AI Innovation Team** for risk assessment and documentation support rather than convening full internal review boards.
- In Phases 3 and 4, shared resources, such as model evaluation tools, technical assistance, or transparency reporting infrastructure, can reduce duplication and increase consistency across agencies and departments.

Agencies are encouraged to document how they are scaling oversight activities and to consult with the **AI Innovation Team** if deviations from standard roles, formats, or timelines are needed. These adjustments must maintain the intent and integrity of the governance model, particularly for medium- and high-risk systems.





## Shared Resources and Support

To support participation across the state enterprise, Idaho offers shared governance infrastructure coordinated through the **AI Innovation Team**. These include:

- Common solution vetting processes and classification tools.
- Optional access to shared privacy or security review resources.
- Training and onboarding pathways tailored for smaller agencies and departments.

For agencies and departments that are unable to sustain a full cross-functional governance team, escalation procedures are defined that route high-risk decisions to centralized governance bodies (see page 14 in Section 2) with support from agency and department leadership.

## Maintaining Governance Integrity

The flexibility provided in this section supports consistency and fairness across agencies and departments operating with different levels of internal capacity. All agencies and departments, regardless of size, remain responsible for ensuring that AI systems are documented, monitored, and reviewed in accordance with their risk classification.

**The AI Innovation Team** will incorporate readiness and capacity perspectives into the AI System Inventory (see page 24 in Section 2) to help inform technical assistance, training outreach, and shared service availability. The inventory will be updated regularly and reviewed alongside statewide implementation progress.

# Capability Development



Effective governance requires more than clear policies; it depends on agency and department capacity to apply them consistently. As Idaho enters the early stages of AI implementation phases described above, building that capability becomes essential. Agencies and departments must be equipped to assess risk, document decisions, monitor system behavior, and make responsible use of AI in operational settings.

This section outlines how the state will prepare its workforce and support consistent implementation through shared tools and infrastructure. It focuses on two essential pillars: ensuring that agencies and departments have the right people in the right roles and providing practical resources that translate governance expectations into executable actions.

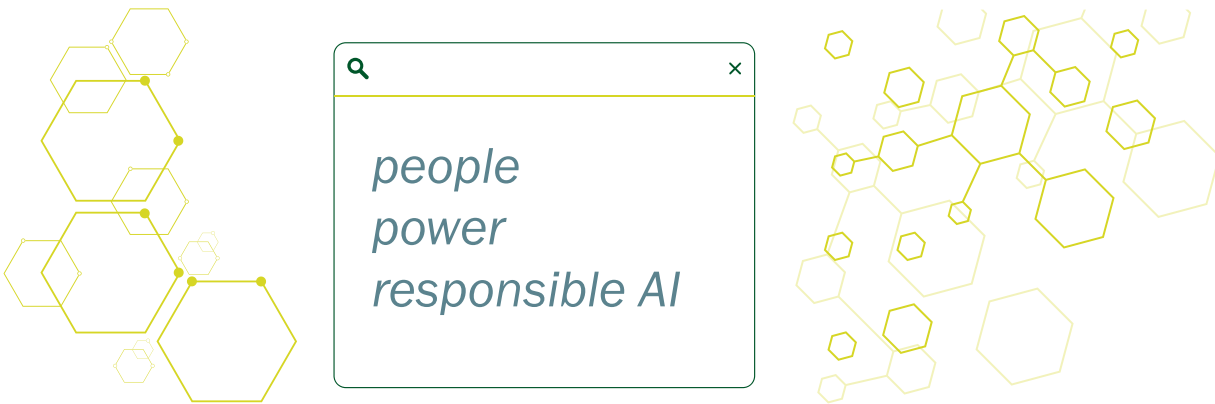
These investments make it possible for oversight to move beyond the policy level to day-to-day operations, where systems are designed, deployed, and used to deliver public value.



# Talent and Organizational Readiness

The successful implementation of AI governance depends on people, who define project goals, assess risk, manage oversight, and ensure that systems deliver successful outcomes. Idaho's approach to talent development focuses on embedding knowledge where it is needed most: inside implementation teams, review bodies, and executive leadership. This means enhancing literacy and structuring roles, training, and staffing models in ways that sustain capability over time.

In accordance with ITS Information Security Policies (AT-02, AT-03), the newly proposed **AI Literacy Program** provides the foundation for this work. All staff participating in AI projects, whether through planning, review, or deployment, are expected to complete training aligned to their responsibilities. Role-specific modules address project intake, documentation, privacy, and system monitoring. Executive tracks focus on strategic oversight and risk governance. Training content is versioned and maintained by the **AI Innovation Team** and delivered through Idaho's enterprise learning systems.



Agencies and departments are building staffing structures that support repeatable governance. Agencies and departments are expected to define internal roles for oversight, integrate privacy and security review into their project workflows, and coordinate staffing for classification, documentation, and post-deployment evaluation. When in-house expertise is limited, agencies and departments may escalate decisions to centralized governance bodies or request support through the **AI Innovation Team**. These processes ensure consistency without imposing one-size-fits-all structures.

To ensure continuity across budget cycles and leadership transitions, Idaho is institutionalizing long term capacity through career path development, targeting recruitment, and strategic partnerships. The **Operation Cyber Idaho** program attracts early and mid-career professionals for cross-agency and department placements. Agency and department partnerships with in-state universities strengthen talent pipelines. These efforts complement Idaho's broader workforce strategy, ensuring that technical knowledge, ethical fluency, and operational discipline are built and retained.

# Tools, Infrastructure, and Implementation Support



Translating AI governance from policy into practice requires access to structured tools and shared infrastructure. Idaho provides implementation teams with a suite of resources designed to guide system planning, standardize documentation, and reduce administrative burden. These tools ensure that oversight expectations are not reinvented on every project but delivered consistently across agencies, departments and use cases.

Core documentation like the **AI Concept Brief**, which is automatically generated during the solution vetting process, is maintained by the **AI Innovation Team** and aligned to the risk-based lifecycle described in Section 2 (see page 20). These resources are accompanied by model examples from past projects, helping teams apply standards with clarity and confidence. Agencies and departments are encouraged to customize tools to reflect local context and preserve required elements.

Technical reference materials support implementation at the infrastructure level. These include security requirements, integration patterns, and model evaluation templates aligned to Idaho's enterprise architecture. Agencies and departments working with large scale or high-risk systems may also access shared resources for inference logging, fairness testing, or model documentation. Where needed, the **AI Innovation Team** can help support system reviews, documentation validation, or architectural alignment.

For innovation and experimentation and in accordance with ITS Information Security Policies (CM-04), Idaho plans to establish a controlled test bed environment where agencies and departments can evaluate new AI technologies before operational deployment. Cross-agency and department implementation groups share lessons, pilot emerging tools, and contribute to the refinement of templates and methods. This collaborative infrastructure ensures that implementation remains practical, scalable, and grounded in Idaho's institutional landscape.





# Success Measurement and Value Realization

Governance alone does not demonstrate success. To justify continued investment and ensure public accountability, Idaho must be able to measure the value and performance of AI systems and the governance structures that support them. This section defines the core principles and structures Idaho will use to evaluate success.

Measurement and evaluation integrate with the implementation lifecycle (see page 20 in Section 2) and connect to the transparency and risk management procedures defined throughout this framework. Success is evaluated across multiple dimensions: operational performance, public impact, governance fidelity, and alignment with state priorities.

## *Operational Metrics and Lifecycle Performance*

Every AI system implemented in Idaho must be measurable in terms of how it functions, how it supports its intended purpose, and how it performs over time. The role of governance is not simply to authorize deployment, but to ensure that systems remain accurate, accountable, and aligned with performance expectations throughout their lifecycle.

System-level metrics are defined early, during the initial solution vetting process and risk classification, and are carried forward through deployment and post-launch evaluation. These metrics vary depending on system function but may include throughput, resolution speed, accuracy, error rates, escalation frequency, or overall impact on service workload. For systems that support or influence decisions, agencies and departments must monitor additional indicators such as consistency of outcomes, reviewer overrides, and variance across population groups.

Monitoring plans must be documented prior to deployment, with clear baselines and escalation thresholds. Medium- and high-risk systems require performance check-ins at specific intervals, typically within the first ninety-day post-launch, followed by scheduled reviews tied to system updates or retraining events. These reviews assess whether system behavior remains stable and whether risk mitigation remains sufficient. Performance assessments should inform, not merely follow, governance decisions.

The **AI Innovation Team** provides measurement templates, oversight checklists, and model documentation guides to help agencies and departments define, collect, and interpret performance data. These tools are not intended to produce uniformity across systems, but to ensure that all implementations, regardless of use case or scale, are reviewed against clearly stated objectives and monitored as living systems, not static deployments.

## *Strategic Alignment and Public Value*

AI systems must serve a purpose that is meaningful, measurable, and aligned with the public mission of government. Idaho's governance model requires agencies and departments to define their purpose explicitly and evaluate whether it is being realized over time.

Each implementation must include a clear articulation of intended value: what problem the system addresses, what public benefit it delivers, and how that benefit will be observed. These definitions must be tied to the agency or department's mission, programmatic goals, or strategic priorities, not just technical optimization. For example, a virtual assistant may reduce call volume, but its value lies in improving citizen access to accurate information. A predictive model may streamline resource allocation, but its benefit depends on transparency and fairness and how those resources are distributed.

Value realization is reviewed periodically alongside performance. Where systems fail to meet their intended outcomes, or introduce trade-offs that outweigh their benefit, agencies and departments must consider redesigning, retraining, or decommissioning. Governance is designed to ensure systems remain justified, not simply to preserve them. In some cases, sunset clauses or usage limits may be appropriate for systems with narrow application windows or emerging risks.

At the enterprise level and in accordance with ITS Information Security Policies (CM-08, PM-05), the **AI Innovation Team** maintains a portfolio view of active systems, identifying implementation patterns, underperforming projects, and opportunities for shared value creation. These insights inform investment planning, training priorities, and updates to the framework itself. Over time, this strategic lens allows Idaho to measure success at the system level and define what a healthy, purpose-aligned AI ecosystem looks like in public service.

### *Executive Takeaway*

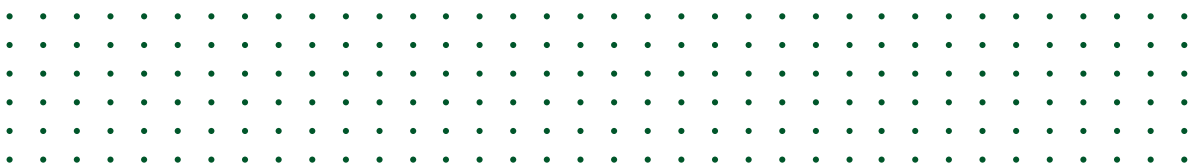
*Success requires more than deployment—it demands measurable value. Idaho's implementation roadmap builds capability incrementally, tracks progress through transparent metrics and ensures every AI system serves a clear public purpose. This strategic approach transforms potential into reality across the state enterprise.*

# 5 Strategic Governance and the Road Ahead



AI is no longer an emerging concept in state government, it is becoming a practical tool for service delivery, decision support, and operational efficiency. As these systems move from concept to deployment, Idaho’s ability to govern them responsibly will rest not only on the strength of this framework, but on the leadership, coordination, and institutional discipline that sustain it over time.

This section defines the path forward. It outlines the responsibilities of state and agency leadership, identifies immediate actions to operationalize governance, and articulates the long-term vision Idaho is pursuing. The objective is not simply to deploy AI responsibly, but to ensure that governance becomes embedded in the state’s operational culture—maintained through clear roles, active oversight, and a shared commitment to public value.







# Leadership Responsibilities

The structures outlined in this framework can only succeed if leadership treats governance as a core operational function, not a one-time launch initiative. Idaho's framework provides structure, but it is leadership at the enterprise, agency, and department level that determines whether governance is institutionalized or remains peripheral. That responsibility does not end with project approval or pilot launch, it extends into budget planning, talent development, risk oversight, and how executive decisions reinforce expectations over time.

At the enterprise level, the **Chief Information Officer (CIO)** and the **AI Executive Committee**, as established in Section 2 (see page 14), are responsible for maintaining strategic alignment, reviewing cross-cutting risks, and ensuring that oversight bodies remain resourced and empowered to meet the state's needs. This includes validating that high-risk systems are reviewed thoroughly, that agencies and departments are supported through implementation challenges, and that policy updates reflect the pace of technological change. The CIO also serves as a central voice in articulating Idaho's governance model externally, as a benchmark for other States and as a point of connection to national initiatives.

Agency and department leaders play a critical role in translating this framework into operational reality. They are expected to ensure that AI governance is not treated as a compliance exercise, but as a management function integrated into day-to-day decision-making. This includes confirming that governance roles are staffed, documentation and oversight cycles are built into delivery timelines, and that the agency and department's AI portfolio is periodically reassessed for alignment with program goals and risk posture.

Leadership in this context also means recognizing when systems no longer serve their intended purpose. Executives must be willing to intervene, whether to adjust oversight, pause deployment, or decommission a system, when performance, fairness, or accountability cannot be sustained. That level of responsibility is not technical, it is institutional. And it is central to making AI work in public service, not just for this year's projects, but for the long-term evolution of state operations.



# Sustaining Governance Through Institutional Practice



Once systems are deployed, the responsibility of governance shifts from design to discipline. Oversight becomes a management function, embedded in operations, informed by data, and accountable to outcomes. This transition, from launching new systems to governing them as part of normal business, is where institutional integrity is either reinforced or lost. The framework anticipates this shift and provides agencies and departments with tools to embed governance into everyday decisions, workflows, and program management.

At the operational level, sustaining governance means building review cycles, documentation checkpoints, and performance assessment into project and program routines. AI risk classification should be revisited as systems are retrained, scaled, or integrated into new workflows. Post-deployment monitoring must be treated as a management input, not a reporting requirement. Oversight bodies must have access to updated system metrics, escalation records, and staff feedback that reflect how systems are functioning in practice, not just on paper.

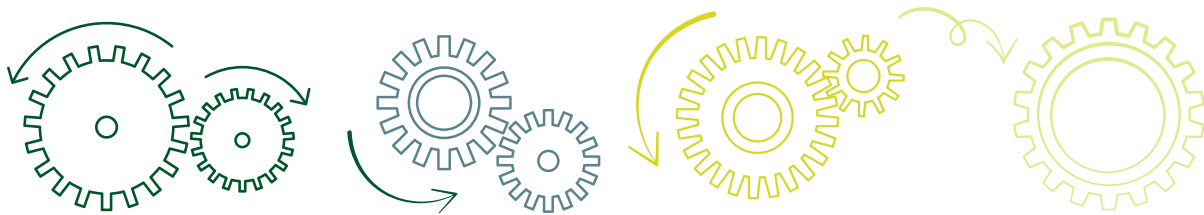
At the administrative level, governance must be reflected in budgeting, hiring, procurement, and planning processes. In accordance with ITS Information Security Policies (PS-09, SR-02), agencies and departments should assess whether AI-related responsibilities are reflected in position descriptions, whether procurement includes vendor accountability for model documentation and risk disclosures, and whether project timelines allow for governance checkpoints. Over time, these practices will become part of how agencies and departments plan and operate.

The **AI Innovation Team**, as defined in Section 2 (see page 14), will support this institutionalization by maintaining implementation tools, reviewing agency and department documentation, coordinating shared learning, and updating guidance based on observed practice. But the shift toward embedded governance depends on agencies and departments owning the work, ensuring that AI systems are not only launched responsibly, but managed that way over time. This is how Idaho builds a governance model that is not episodic, but enduring.

# Adapting Through Learning and Change

The rapid pace of AI development means that no governance framework can remain static. New technologies will challenge existing oversight models, and implementation experience will reveal where policies need to evolve. Idaho's framework is designed to accommodate this reality, through formal review cycles, cross-agency and department learning, and structured mechanisms for change.

Framework updates are managed by the **AI Innovation Team**, in collaboration with the **AI Executive Committee** and relevant review boards. Each year, the team will coordinate a comprehensive review informed by agency and department feedback, implementation data, and emerging policy guidance. This process is not intended to introduce sweeping change annually, but to ensure that the framework remains coherent, consistent, and reflective of lived practice, following the governance structure interactions defined in Section 2 (see page 15).



Feedback is expected at all levels. Agencies and departments are encouraged to document points of friction, suggest clarifications, and share examples of adaptations made during implementation. Where tools or policies require adjustment, the **AI Innovation Team** will work with agency and department leads to pilot new templates or governance models before issuing formal revisions according to the processes in Section 2 (see page 15). Lessons drawn from these adaptations are used not only to improve documentation, but to inform future training and implementation guidance.

Through this iterative approach, Idaho builds a governance system that is both principled and adaptable, able to incorporate change without sacrificing clarity or accountability. This review process is not about reinvention, it is how Idaho ensures the framework matures alongside implementation experience and public needs, in alignment with the implementation matrix in Section 3 (see page 48).

As Idaho's internal governance processes take root, the next opportunity is to model responsible adoption more broadly, demonstrating that principled innovation is possible at the state level.

# Idaho's Leadership Opportunity



AI is reshaping how public institutions operate. As systems become more capable and more embedded in government workflows, the question facing states is not just how to use AI, but how to govern it in a way that preserves trust, protects rights, and delivers real public value securely. With this framework, Idaho has positioned itself to lead on that question.

Idaho's model is grounded in the realities of public administration: uneven capacity, evolving risks, and the need to move incrementally while maintaining institutional control. It offers agencies and departments a practical way to classify risk, structure oversight, and deploy AI systems that align with their mission. It gives policymakers the tools to maintain transparency and accountability across a distributed enterprise. And it demonstrates that governance can keep pace with innovation without slowing it down.

This approach is not just about mitigating risk, it's about setting a standard. By implementing governance that is proportionate, forward-looking, and deeply embedded in institutional operations, Idaho is showing what public sector leadership in AI can look like. Other states, and national partners, will increasingly look to this framework as a model for how to align emerging technologies with public values.

The work of implementation continues. But the foundation is in place. With this framework, Idaho has committed not only to deploying AI responsibly, but to building the capacity, the discipline, and the leadership model needed to govern it overtime. That is how institutional credibility is earned and sustained in a rapidly evolving policy and technology landscape. And it is work Idaho is prepared to lead.

# *Hypothetical Case Studies in Risk-Based Oversight*

This appendix illustrates how Idaho's risk-based AI governance framework applies in practice across different tiers of system risk, directly connecting to the governance approaches specified in Sections 2 and 3. Each case study traces a hypothetical AI implementation through the stages of concept development, risk classification, review, deployment, and monitoring, demonstrating proportional governance in action.



# Hypothetical Case Study Mapping Table



# Hypothetical Case Study 1: Tier 1 (Low Risk)

## *Department of Parks and Recreation - Virtual Information Assistant/Chatbot*

### SYSTEM OVERVIEW

The Idaho Department of Parks and Recreation (IDPR) proposes a virtual assistant to provide park visitors with automated responses to frequently asked questions, such as hours of operation, amenities, trail closures, and reservation processes. The system is intended to reduce call center volume and improve the online visitor experience.

#### **Phase 1: Concept Brief and Screening**

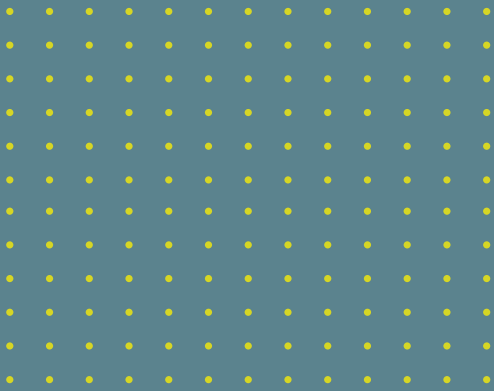
The proposing team submits a standard solution vetting request to ITS outlining the use of a commercial chatbot platform configured with publicly available park data and pre-vetted FAQs. This request automatically generates an **AI Concept Brief**. The Department CIO/IT leader connects with ITS to support an initial risk screen and determines:

- No personal data will be processed.
- The system does not make eligibility or enforcement decisions.
- Outputs are informational and easily auditable.
- The system will be publicly accessible but narrowly scoped.
- The implementation uses well-established commercial tools.

Preliminary Classification: Tier One — Low Risk

#### **Phase 2: Risk Assessment and Proposal**

A streamlined project proposal includes a basic implementation plan, resource estimates, and a lightweight monitoring strategy focused on call volume reduction and response accuracy. Using the risk scoring tool (see page 16 in Section 2), a full risk assessment confirms the low-risk classification:



### **Phase 3: Review and Approval**

Following Tier 1 procedures defined in Section 2 (see page 20):

- The Department CIO/IT leader and ITS review and approve the implementation through standard governance processes.
- The AI Innovation Team receives notification for inventory purposes only.
- A lightweight annual review cycle is established.

Approval is completed within 10 business days.

### **Phase 4: Deployment**

The chatbot is configured, tested for factual accuracy, and deployed to the Department's public website. Staff receive a short training on updating content and monitoring unresolved queries. The system is labeled clearly as AI-driven.

### **Phase 5: Monitoring and Evaluation**

Oversight includes:

- Automated tracking of usage volume and unanswered questions.
- Monthly review of content gaps.
- Quarterly updates aligned with seasonal park activity.
- Annual risk assessment.

After three months, the system shows a thirty-five percent reduction in routine call center volume and high satisfaction scores among website users.

### **Key Insight**

*This Tier 1 case demonstrates that low-risk AI systems can move from concept to deployment quickly under Idaho's governance model. Lightweight documentation, fast-track approval, and streamlined monitoring allow agencies and departments to implement useful tools without sacrificing accountability or oversight.*

# Hypothetical Case Study 2: Tier 2 (Medium Risk)

## *Transportation Department - Road Maintenance Prioritization*

### SYSTEM OVERVIEW

The Idaho Transportation Department (ITD) proposes a system to support road maintenance prioritization by analyzing data from surveys, traffic volumes, safety reports, weather systems, and citizen-reported issues. The system will provide ranked recommendations for human review.

#### ***Phase 1: Concept Brief and Screening***

The proposing team submits a standard solution vetting request to ITS outlining the business need, potential data sources, and a human-in-the-loop deployment model. This request automatically generates an AI Concept Brief. The Department CIO/IT leader connects with ITS to support an initial risk screen and determines:

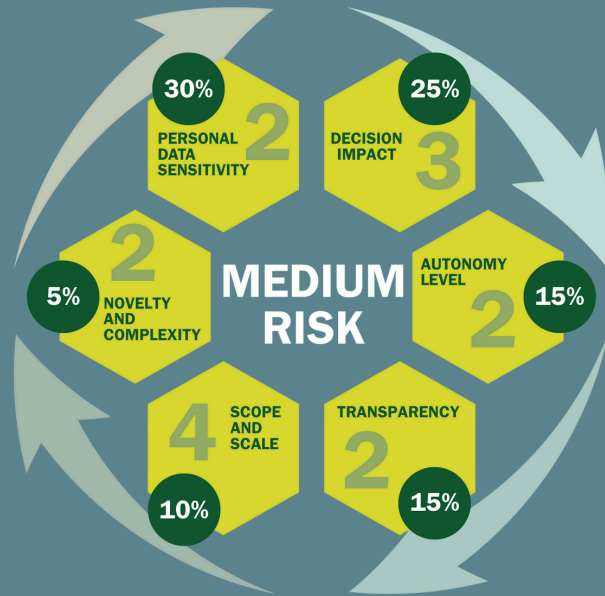
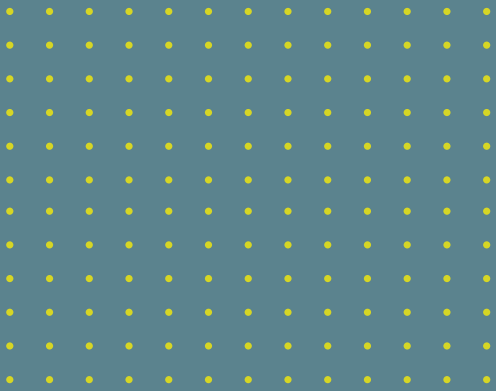
- No sensitive personal data is used.
- The system influences, but does not automate, resource allocation.
- The solution will rely on existing data but incorporate multiple variable types.
- Similar systems exist but are not common in Idaho's infrastructure domain.

Primary Classification: **Tier 2—Medium Risk**

#### ***Phase 2: Risk Assessment and Proposal***

The proposal includes a technical description of data processing methods, integration points, system outputs, and training for maintenance planners. Using the risk scoring tool (see page 16 in Section 2), a full risk assessment confirms the medium-risk classification:





### **Phase 3: Review and Approval**

Following Tier 2 procedures defined in Section 2 (see page 20):

- Department CIO/IT leader review and approval.
- AI Innovation Team review and approval, which recommends improving algorithm documentation, aligned with their responsibilities in Section 2 (see page 14).
- The Technical Review Board is consulted on data integration and architectural alignment questions, consistent with their advisory role described in Section 2 (see page 14).

The proposal is approved with conditions:

- Enhanced documentation of prioritization logic.
- Adjustment to weather data processing strategy.
- Quarterly performance reports.
- Annual reassessment.

### **Phase 4: Deployment**

After technical testing, user validation, and security review, the system is deployed in one district. It includes:

- A phased rollout plan.
- Planners' training materials.
- Logging of model outputs and overrides.
- Help desk protocols.

**Phase 5: Monitoring and Risk Variance Management**

Within six months, the system demonstrates consistent performance and is approved for statewide rollout. During year two, extreme weather necessitates a temporary algorithm adjustment.

Following Idaho's risk variance process detailed in Section 2 (see page 22):

1. The request is submitted using the formal risk variance request form with documented justification and defined time limits.
2. A rapid risk review confirms the adjustment retains human oversight and walks through the information gathering steps specified in the above-referenced process.
3. Subject-matter experts validate the interim method.
4. The Department CIO/IT leader and AI Innovation Team jointly approve the variance.
5. The event is logged and reviewed post-season.

All variances are documented, time-bound, and subject to follow-up review as required by the risk variance process defined in Section 2 (see page 22).

**Key Insight**

*This Tier 2 case illustrates how Idaho's framework balances governance and adaptability. While oversight is more robust than Tier 1, it enables innovation with confidence, ensures traceability, and preserves operational flexibility under exceptional conditions.*

# Hypothetical Case Study 3: Tier 3 (High Risk)

## *Department of Health and Welfare - Benefits Eligibility Assistant*

### SYSTEM OVERVIEW

The Idaho Department of Health and Welfare (IDHW) proposes a machine learning system to assist with benefit eligibility evaluations and identify individuals potentially eligible for unclaimed assistance. The system uses household, demographic, and financial data to recommend program eligibility.

#### ***Phase 1: Concept Brief and Screening***

The proposing team submits a standard solution vetting request to ITS highlighting the system's purpose, data sources, and partial automation model. This request automatically generates an AI Concept Brief. The Department CIO/IT leader connects with ITS to support an initial risk screen and determines:

- The system will process sensitive personal data.
- Recommendations will directly affect benefit eligibility.
- The system will assist, but not replace, human decisions.
- It will serve vulnerable populations.
- It uses a combination of established methods and novel rule integration.

Primary Classification: **Tier 3–High Risk**

#### ***Phase 2: Risk Assessment and Approval***

The proposal includes a detailed data governance strategy, fairness testing plans, and explainability requirements. Using the risk scoring tool (see page 16 in Section 2), a full risk assessment confirms the high-risk classification:



### ***Phase 3: Review and Approval***

The proposal receives comprehensive review from relevant governance bodies (see page 16 in Section 2) and follows the Tier 3 process defined in Section 2 (see page 20):

- Information Owner and Privacy Officer: Adds data minimization and consent refinement as specified in Section 3 (see page 29).
- Ethics Advisory Committee: Recommends demographic fairness testing and monitoring aligned with their ethical oversight role.
- Technical Review Board: Requests clearer explanation templates consistent with transparency requirements in Section 1 (see page 8).
- Executive Committee: Conditionally supports with six required safeguards.

These include human-in-the-loop requirements, monitoring dashboards, and explanation protocols.

### ***Phase 4: Deployment***

The system is launched in two counties under close monitoring. Implementation includes:

- Fairness verification across populations.
- Reviewer training and override mechanisms.
- Comprehensive audit trail and metadata logging.
- Public communications and opt-out options.

*greenlit*  
**with**  
**guardrails**



**Phase 5: Monitoring and Oversight**

Post-deployment monitoring includes:

- Weekly performance analysis.
- Monthly fairness audits.
- Detailed override review.
- Stakeholder surveys.

After ninety days, the Executive Committee reviews and supports a phased statewide rollout. Annual reassessment continues, with findings used to refine model logic and explanation design.

**Key Insight**

*This Tier 3 case shows how Idaho's framework applies the most intensive oversight to systems with high public impact. While governance is resource-intensive, it ensures accuracy, fairness, and transparency, maintaining public trust and advancing access to critical services.*

*These three hypothetical case studies demonstrate how Idaho's risk-based governance framework applies proportional oversight based on system impact. The increasingly rigorous governance requirements from Tier 1 to Tier 3 ensure that governance resources are focused appropriately, with streamlined processes for low-risk systems and comprehensive controls for high-risk implementations.*

# ***AI Literacy Program: Proposed Statewide Curriculum for Responsible Adoption***

## *Purpose*

The **AI Literacy Program** provides a robust curriculum to equip Idaho state government personnel with the knowledge, context, and judgment required to responsibly plan, procure, oversee, and use AI systems. The program supports capability development objectives outlined in Section 4 (see pages 58-59) of the Idaho AI Governance Framework.

The **AI Literacy Program** directly supports the implementation phases described in Section 4 (see pages 58-59), providing the knowledge foundation necessary for successful governance adoption. Learning objectives and delivery formats are calibrated to align with the progressive advancement of governance maturity, with core modules supporting Phase 1, specialized content enabling Phase 2, and advanced material sustaining Phases 3 and 4.

## *Scope and Structure*

The program is modular, role-specific, and designed to scale with agency and department maturity. It includes foundational training for all employees, targeted modules for implementation leads and governance staff, and ongoing learning pathways for specialized roles in policy, procurement, security, privacy, and communications.

# Curriculum Structure

## CORE FOUNDATIONS (ALL STAFF)

*Required for all agency and department personnel interacting with AI systems.*

### **Learning Objectives:**

- Understand what AI is and how it is being used in Idaho government.
- Recognize AI system boundaries and the role of automation and decision support.
- Identify when human judgment, oversight, or escalation is required.

### **Delivery Format:**

- 45-minute eLearning module (industry compliant).
- Printable quick-reference guide: “How to Identify AI-Support Services”.
- Optional live Q&A (quarterly).

## AI GOVERNANCE & ETHICS (IMPLEMENTATION TEAMS, GOVERNANCE LEADS)

*Core training for teams planning and managing AI systems.*

### **Learning Objectives:**

- Apply Idaho’s AI risk classification model (see page 16 in Section 2).
- Use the AI Concept Brief and existing solution vetting process (see page 20 in Section 2).
- Navigate approval pathways and governance checkpoints.
- Understand transparency obligations and public-facing requirements.

### **Content Modules:**

- “Classifying AI Risk: From Concept Brief to Deployment”
- “High-Risk Implementations: What Governance Bodies Evaluate”
- “Documenting Oversight Roles: Why It Matters”

### **Delivery Format:**

- Half-day virtual or in-person workshop.
- Facilitated case study: review and classify a mock use case.
- Post-training knowledge check and certificate.

## PRIVACY AND DATA USE IN AI (PRIVACY AND LEGAL STAFF, PUBLIC INFORMATION OFFICERS)

*Specialized training aligned to Section 3 (see page 27) and privacy impact protocols.*

### **Learning Objectives:**

- Understand how data is used differently in AI versus traditional systems.
- Conduct and review privacy impact assessments for AI systems.
- Advise on consent, data minimization, and retention in model pipelines.
- Communicate clearly with the public about AI data practices.

### **Delivery Format:**

- 60-minute instructor-led session (virtual or in-person).
- Templates and walkthroughs: consent language, retention schedules.
- Sample FAQs and citizen communications scripts.

## SECURITY AND INFRASTRUCTURE (CISOs, DevSecOps, IT ADMINS)

*Specialized training aligned to Section 3 (see page 31) and model-specific threats and migrations.*

### **Learning Objectives:**

- Identify and manage risks related to model storage, inference, and training data pipelines.
- Integrate AI systems into enterprise security logging and incident response.
- Understand emerging risks: prompt injection, model inversion, and adversarial inputs.

### **Content Modules:**

- “AI is Not Just Code: What to Log and Why”
- “Aligning AI Deployments with Idaho’s Security Baseline”
- “Vendor AI Risk Reviews: What to Ask and What to Watch”

### **Delivery Format:**

- Two-hour technical workshop with breakout sessions.
- Optional tabletop exercise (high-risk incident simulation).



## PROCUREMENT AND VENDOR ENGAGEMENT (CONTRACT OFFICERS, PROGRAM MANAGERS)

*Specialized training aligned to Section 3 (see page 35) and connecting AI to procurement processes.*

### **Learning Objectives:**

- Identify AI-specific terms and obligations in vendor contracts.
- Understand transparency, audit, and change control for third-party models.
- Use the GenAI Use Policy in external system onboarding

### **Delivery Format:**

- 60-minute recorded briefing.
- Companion playbook: “Evaluating AI in RFP’s and Vendor Submissions”.
- Model contract clauses and checklist for AI-specific reviews.

## OPTIONAL: EXECUTIVE BRIEFING TRACK (AGENCY DIRECTORS, CABINET-LEVEL OFFICIALS)

*Brief high-level track designed for policy and budgetary leadership.*

### **Learning Objectives:**

- Understand enterprise-wide risk and opportunity positioning for AI.
- Ask the right questions about AI proposals and system performance.
- Interpret public value, economic and national security impact, and governance indicators.

### **Delivery Format:**

- 30-minute recording overview with framework summary.
- One-page dashboard template: “What to Track in Your Agency”.
- Leadership playbook: “AI Governance and Strategic Planning Context”.

## *Program Administration and Evaluation*

The AI Literacy Program is administered by the AI Innovation Team in partnership with other ITS elements and relevant agencies, departments, and third parties, where appropriate. The AI Innovation Team will take steps to ensure:

- Training records, role-based compliance, and completion tracking are managed through the state's existing Learning Management System.
- Program modules are reviewed annually and updated to reflect changes in Idaho’s framework (e.g., see page 41 in Section 3) and federal policy.
- Program outcomes are reported as part of the Framework Implementation Matrix (see page 48 in Section 3) and used in agency and department capability planning.

# AI Concept Brief

This template supports early-stage planning for AI projects by helping agencies articulate key elements of a proposed system—its purpose, data, technical approach, risks, and stakeholders. It ensures alignment with Idaho’s governance framework and prepares projects for responsible development and review.

# AI Concept Brief

**Agency Name:**

**Project Title:**

**Project Owner:**

Agency Name  
Project Title

## Use Case Overview

*Provide a plain language summary of the AI use case, including who it serves and the primary objective.*

## Business Need & Success Metrics

*Describe the business challenge this addresses. How will success be measured?*

## Data Inputs and Ownership

*What data will be used? Who owns the data? What security/privacy classifications apply?*

## Model Type & Technical Architecture

*Briefly describe the kind of AI/Machine learning (ML) being considered (e.g., Large Language Model (LLM), classification model). Include expected input/output format, system.*

### Human-in-the-loop and Explainability

*Will humans review, override, or audit the model's output? How will decisions be explained to end users?*

### Potential Harms, Bias, or Safety Concerns

*What risks (e.g., fairness, misinformation, misclassification, over-reliance) have been identified? How will they be mitigated?*

### Deployment and Monitoring Plan

*Describe how the system will be deployed and how performance, drift (i.e. how model performance declines over time as it process new data that deviates from data it was trained on), and incidents will be monitored?*

### Stakeholder and End-User Involvement

*Which stakeholders or citizen/user groups will be engaged in design, testing, and review?*

Date Submitted: \_\_\_\_\_

Submitted By: \_\_\_\_\_




# Thank you

## Acknowledgements

We extend our sincere gratitude to the Idaho Office of Information Technology Services Administrator/Chief Information Officer Alberto Gonzalez, Executive Leadership team and broader agency. Their leadership and expertise were instrumental in shaping a framework that balances innovation with responsibility, ensuring Idaho's AI initiatives remain secure, ethical, and aligned with public values.



Built by  
**SPOOKWORKS**



Idaho leads.  
AI delivers.