



From data disorder to Data Confidence™

The Public Sector **unified governance** workbook

Table of contents

Command your data: For public sector leaders in the age of AI	3
Public sector data challenges	4
Unified governance: The solution for governance fragmentation	5
The critical capabilities you need	7
Data governance - Mission alignment checklist	8
AI governance - AI readiness assessment	11
Data quality & observability - Six steps to data observability	15
Data catalog - Data catalog checklist	19
Data lineage - Map your critical data flows	22
Data privacy - Privacy impact worksheet	25
Policy control - Create an access control strategy	28
Get started in 3 steps	32
Step 1 Trust: Ensure data is reliable	32
Step 2 Comply: Enable unified governance	33
Step 3 Consume: Get the right data in the right hands	34
Case study	35
The Office of the Secretary of Defense	35
Unifying governance for mission success	36



Command your data

You're a public sector leader staring down federal mandates. And trying to turn mountains of data into mission success. Sound familiar? You're in the right place. What you're reading isn't just another compliance checklist — it's your field guide to unified governance in an era where data is your agency's most strategic asset and possibly its biggest headache.

What you'll get in these pages

- A practical roadmap for turning data chaos into confidence
- A foundation that satisfies both today's mandates and tomorrow's AI or other data-driven ambitions
- Critical capabilities to nail compliance with federal data strategy, and the OPEN Government Data Act
- A battle-tested framework for implementing unified governance
- A real story from a federal leader who has already navigated these "waters"

Public sector data challenges

Why now?

Three forces are converging. Each one demands action. Together, they're making unified governance an urgent priority for public agencies.

1. More and more data

Petabytes of data across scattered systems. Legacy environments that won't die. Modern cloud platforms that won't wait. And somewhere in this complexity, you need to find, protect and use data.

2. Rapidly evolving legal and regulatory landscape

The Federal Data Strategy demands evidence-based everything. AI governance requirements are here. State-specific AI regulations are multiplying. And you need to respond. Fast.

3. The mission can't wait

Citizens need government support at digital speed. Leadership needs data-driven decisions. Yesterday. Cross-agency collaboration isn't optional now. And every new technology — from AI to whatever comes next — needs governed, reliable data to deliver value.

The root of it all? Fragmented governance

These challenges feel dispersed. But there's one root cause: governance fragmentation. When your data governance (if it exists) is tethered to specific systems or platforms, you get:

- Over-budget projects
- Compliance blind spots
- Collaboration dead ends
- Legacy system lock-ins
- Innovation bottlenecks

But there's a better way.

The path forward: Unified governance

Imagine data and AI governance that works like your best teams. Breaking down silos. Adapting to new challenges. Getting the job done without sacrificing security. It's not just aspirational language. It's the foundation for modern government data strategy: data and AI governance. And it's unified.

For every data asset, every system, every user

Unified governance frees your agency's data from the constraints of silos by untethering governance from individual systems and sources. This approach delivers visibility, context and control throughout the full data lifecycle—from every data producer to every consumer, from input through output.

Across your data ecosystem, unified governance works:

- **For every bit of data:** Whether your data resides in public clouds, private clouds, legacy applications or self-hosted systems, unified governance brings it all under one consistent framework. This comprehensive approach ensures no data asset operates outside your governance structure
- **Across every system:** True unified governance is system- and platform-agnostic, allowing you to compute where and how you need without being locked into specific vendors or platforms. This flexibility is crucial for agencies managing complex hybrid environments while preparing for future modernization
- **For every user:** From data scientists to policy analysts, program managers to senior leadership—unified governance brings everyone into the data stewardship fold through smart workflows, intuitive interfaces and automated access controls that maintain security while enabling appropriate data use
- **With rich semantics:** The enterprise metadata graph underpinning unified governance goes beyond technical documentation. It captures essential business context, regulatory requirements and ethical considerations—critical for traditional data usage and AI development. The semantic layer ensures everyone understands not just what data exists, but how it can be used in conventional and AI-powered applications

Building Data Confidence™

When governance is unified, agencies gain what we call “Data Confidence”—the ability to accelerate mission-critical initiatives while maintaining security and compliance.

Data Confidence offers tangible benefits:

- Expedited time to data value, allowing faster response to mission needs
- De-risked data initiatives through consistent policy enforcement
- Streamlined compliance with Federal Data Strategy, OPEN Government Data Act and emerging AI regulations
- Enhanced ability to share data securely across organizational boundaries
- Accelerated modernization through a solid data foundation

Most importantly, unified governance positions agencies to tackle tomorrow's challenges, whether they involve artificial intelligence, cross-agency collaboration or evidence-based policymaking. It creates the foundation for innovation while maintaining the strict security and compliance requirements unique to public sector organizations.

Through unified governance, agencies can move beyond fragmented, system-specific approaches to achieve true data confidence—knowing that their data is trusted, protected and ready to drive mission success.

Critical capabilities for unified governance

While individual tools might address specific needs, true data confidence emerges from a complete unified governance platform that brings these capabilities together.

For agencies navigating everything from Federal Data Strategy compliance to AI readiness, understanding these core capabilities is essential. Each one plays a vital role in transforming fragmented data practices into a unified governance platform that accelerates mission outcomes while maintaining security and compliance.

Let's explore the seven critical capabilities that form the foundation of unified governance, and how they work together to deliver data confidence for your agency:

Critical capabilities

- **Data governance:** The establishment and management of policies, processes and roles for data handling, decision-making and regulatory compliance
- **AI governance:** The application of rules, processes and responsibilities to drive maximum value by ensuring streamlined, ethical AI practices that mitigate risk and protect privacy
- **Data quality & observability:** A methodology (and a purpose-built software solution) for achieving high-quality, accurate and consistent data as well as insights into data health
- **Data catalog:** An organized inventory of data assets that empowers stakeholders to find and use the right data
- **Data lineage:** A visual representation of data flow, helping to manage the origin, transformation and consumption of data
- **Data privacy:** A process and a goal to ensure sensitive data is protected and in compliance with data protection regulations is maintained
- **Policy control center:** A centralized location to define, enforce and monitor data access and usage policies across the organization

By understanding the components of a unified governance platform and aligning your organization's needs with what's available in the market, you can make an informed decision on the right solution.

Data governance: Ensure collaboration and compliance

Data governance is the practice of managing and organizing data and processes to enable collaboration and compliant access to data. Data governance allows your data citizens — and that's everyone in your organization — to create value from data assets. Leveraging a business glossary and a data dictionary as well as stewardship management and reference data management, enterprise data governance provides a single location to find, understand and create a shared language around data.

Why data governance is important

Unfortunately, when data governance goes badly, it can lead to consequences that could jeopardize your mission, including:

- **Misinformation:** Incorrect decisions based on inaccurate data
- **Security breaches:** Vulnerabilities due to improper data handling
- **Regulatory violations:** Potential legal consequences and hefty fines
- **Wasted resources:** Time and money spent rectifying data errors

The regulatory landscape is evolving on two fronts. Data protection regulations like CCPA in California and similar laws in 20 other states set strict requirements for handling data. Meanwhile, new AI-specific regulations are emerging with states like Colorado and Nevada establishing frameworks for algorithmic accountability and model auditing. This dual regulatory challenge makes robust data governance critical for public sector organizations.

Key features to look for

- **Comprehensive business glossary:** A centralized location for all data-related terminologies ensuring consistency in understanding and usage
- **Stewardship management:** Identifying owners for the data who ensure data quality and usage adheres to organizational policies
- **Reference data management:** Managing standard data assets that are repeatedly used across the organization
- **Centralized policy management:** A singular point to define, manage and monitor data-related policies
- **Workflows:** Automated processes for data approval, quality checks and updates
- **Flexible operating model:** A flexible model allows you to design your environment to meet your specific needs



Use case

Here are some key areas where data governance plays a critical role in the public sector:

- **Regulatory compliance/Reporting:** Ensuring data accuracy and consistency for regulatory reporting (e.g., FOIA, GDPR, CCPA, AI Act) and audits, reducing risks of non-compliance and penalties
 - **Public sector data sharing:** Establishing clear governance frameworks to enable secure, standardized data exchange between agencies (e.g., health departments, law enforcement, social services) while protecting sensitive citizen information
 - **Fraud detection/risk management:** Leveraging high-quality, well-governed data to identify fraud patterns in public benefits programs (e.g., unemployment insurance, tax compliance) and improve risk mitigation strategies
 - **Citizen services/digital transformation:** Enhancing service delivery by ensuring citizen data is accurate, secure and accessible across digital government platforms, reducing redundancy and improving user experience
- 

Data governance assessment worksheet

Mission alignment checklist

Map your data governance initiatives to agency missions:

Strategic mission support

How will data governance enhance mission delivery?

What specific mission objectives will be supported?

Which stakeholders need to be involved?

Compliance requirements mapping

Federal Data Strategy milestones

OPEN Government Data Act requirements

Privacy Act considerations

Agency-specific mandates

AI governance:

Accelerating data and AI use cases

To ensure mission success—and launch AI use cases and applications that leverage the capabilities of large language models (LLMs)—you should be thinking about your holistic AI strategy. However, successfully integrating AI initiatives into your roadmap will require a rigorous approach. To ensure AI is used responsibly, government agencies are leveraging AI governance.

AI governance is the application of rules, processes and responsibilities to drive maximum value from your automated data products by ensuring applicable, streamlined and ethical AI practices that mitigate risk and protect privacy.

Why AI governance is so important

The truth is data is the backbone of AI, and if the data is bad, the AI models trained on it will produce results that look good but are fundamentally flawed. The implications for the public sector agencies building AI applications are profound. And as AI's impact grows, so does the scrutiny. While regulation around AI varies, we're already starting to see some US states (including California, Nevada, Colorado and New York) pass laws that will require state agencies to monitor the use of generative AI.

It's why AI governance is mission-critical and non-compliance can lead to:

- **Regulatory violations/Legal risks:** Agencies face increasing AI regulations, such as bias audits for automated decision-making tools used in hiring, law enforcement and public benefits programs
- **Public trust erosion:** Misuse of AI in government services—such as faulty algorithms in social services eligibility assessments—can decrease public confidence in government
- **Policy/Ethical concerns:** AI-driven systems in areas like policing, fraud detection and social assistance must ensure fairness, accountability and transparency to avoid discrimination and systemic bias
- **Operational failures:** Poorly governed AI can lead to inaccurate risk assessments in areas like public health response, cybersecurity and disaster preparedness, undermining mission-critical decisionsdata-driven, AI-powered world

Key features to look for

A well-defined AI governance solution should encompass:

- Out-of-the-box, industry- standard frameworks, like the NIST AI Risk Management Framework
- Clear AI objectives and principles
- Data quality and integrity checks
- Model transparency and interpretability measures
- Regular audits and updates
- Ethical considerations, including fairness and bias checks
- Legal and data compliance

As data becomes increasingly critical to organizational decision-making, the emphasis on data governance becomes more and more mission-critical. Whether you're looking at traditional data governance or the emerging practice of AI governance, the presence of a clear, comprehensive framework is essential in our data-driven, AI-powered world.



Use case

Here are some key areas where AI governance plays a critical role in the public sector:

- **Automated citizen services/Chatbots:** Governing AI-powered virtual assistants for public inquiries (e.g. DMV services, tax filings) to ensure accuracy, transparency and compliance with privacy regulations
 - **Fraud detection:** Implementing responsible AI-driven risk assessment models in unemployment insurance, tax compliance and social benefits programs to detect fraudulent activities while maintaining fairness and due process
 - **Cybersecurity/Threat detection:** Establishing governance frameworks for AI systems used in government cybersecurity to detect threats while ensuring transparency and accountability in automated decision-making
 - **Regulatory compliance/AI risk management:** Implementing AI governance policies to meet evolving federal and state-level AI regulations, ensuring agencies maintain transparency in algorithmic decision-making
- 

AI readiness assessment

Rate your agency (1-5)

Data quality standardization

Metadata management maturity

Cross-domain data sharing capability

Model documentation processes

AI use case | Evaluation template

For each potential AI initiative

Mission impact

Primary mission supported

Expected outcomes

Success metrics

Data requirements

Data sources needed

Data quality status

Data sharing agreements required

Risk assessment

Privacy implications

Bias concerns

Security considerations

Data quality & observability: Ensure value and transparency

Modern stacks are complicated. While amassing vast amounts of data is an achievement, it doesn't automatically translate to value. And data without quality is like a recipe without any good ingredients — there's potentially a meal at the end of the process, but if it's not going to taste good, the recipe isn't very useful.

Data quality refers to the ability of data to fit its intended purpose, ensuring it is accurate, complete and reliable for decision-making. Observability in the context of data is the ability to fully understand the health, status, and performance of data systems and pipelines through monitoring, logging and tracing. Together, data quality and observability give government data leaders and their colleagues the confidence that everyone is using trusted, high-quality data, and, as a result, you can accelerate every data and AI use case.

\$15M

The average annual financial repercussions of poor data quality.

Source: Gartner Data Quality Market Survey

Why data quality & observability is so important

You rely on data to drive policy decisions, allocate resources and deliver public services effectively. But poor data quality causes costly mistakes, compliance risks and, ultimately, erodes the public's trust in government. A data quality & observability solution ensures your agency can monitor data in real time, catching issues before they escalate.

- **Regulatory compliance:** Accurate, auditable data is essential for FOIA requests, public records management and meeting federal reporting requirements
- **Operational efficiency:** Reliable data improves decision-making for staffing, budgeting and service delivery, reducing waste
- **Fraud prevention/Risk management:** Clean, well-monitored data helps detect fraudulent claims

Key features to look for

- **Data profiling:** Understand your data's structure, content and quality. This is the preliminary step in identifying areas that need attention
- **Data cleansing:** Clean or remove corrupt, inaccurate or erroneous data to maintain data integrity and reliability
- **Data enrichment:** Enhance the data's value by appending related information from external sources to add depth and context
- **Data monitoring:** Continuously track data streams to detect anomalies, inconsistencies or any deviation from the defined quality standards
- **Data pushdown:** Address data quality issues at the source to improve security, reduce costs and enhance efficiency across agency systems



Use case

Here are some key areas where data quality & observability plays a critical role in the public sector:

- **Interagency data sharing:** Maintaining data consistency across government agencies to improve collaboration on initiatives such as housing, transportation and public safety
 - **Citizen services optimization:** Improving the accuracy of public records, reducing errors in benefits processing and streamlining government digital services
 - **Infrastructure/Resource planning:** Using high-quality data to make informed decisions on public works projects, energy distribution and environmental initiatives
- 

Six steps to data observability

Profile your data

Discover and classify all data sources

Identify sensitive data types and understand data structures

Define data policies and quality rules

Establish clear data policies and quality rules

Implement continuous testing and validation to maintain data integrity

Detect anomalies

Use machine learning to establish baselines and detect deviations

Identify potential data quality issues early

Monitor for impact

Correlate anomalies with business events to assess their impact

Prioritize remediation efforts based on severity

Notify key experts

Alert relevant stakeholders about data issues

Initiate and manage remediation processes effectively

Optimize continuously

Evolve data policies and practices based on insights from monitoring

Implement continuous improvement loops for ongoing optimization

These steps will guide you in building a reliable data infrastructure, ensuring high data quality and supporting informed decision-making.

Data catalog: Deliver trusted data

A data catalog does more than inventory your agency's information assets—it creates a single source of truth across your entire data ecosystem. And it streamlines the discovery, description and organization of data. By leveraging metadata intelligently, a data catalog connects stakeholders, ensures compliance and enables evidence-based decision-making. Agencies use data catalogs to meet Federal Data Strategy requirements and OPEN Government Data Act mandates while improving efficiency and transparency.

Why data catalogs are important

Government agencies can't afford scattered data silos and disconnected systems—you need your data to work harder. A modern data catalog transforms how your agency operates by:

- **Delivering end-to-end visibility:** Get a comprehensive view of your data assets, showing where they come from, how they transform and where they're used
- **Maximizing the value of your data:** Eliminate scattered data silos and establish a clear path to trusted data—for day-to-day operations to strategic initiatives
- **Breaking down silos:** Unify scattered data assets so you can get the most out of your data and support agency initiatives




Use case

Here are some key areas where a data catalog plays a critical role in the public sector:

- **Regulatory compliance:** Simplifying data access for audits, FOIA requests and transparency mandates
- **Interagency collaboration:** Enabling secure data sharing across departments for improved coordination
- **Evidence-based policymaking:** Ensuring decision-makers have accurate, trusted data for public initiatives

Public services improvement: Enhancing service delivery by making high-quality data more accessible.



Choosing a data catalog | Checklist

Look for these capabilities when considering a data catalog:

- ❑ **Connectors:** Make sure your data catalog offers a centralized repository of connectors to your most widely and actively used data sources. This ensures your catalog is as comprehensive as possible
- ❑ **Duration:** Make sure your data catalog offers tagging, grouping and documentation to improve data discoverability and understanding. Tagging can help users quickly find related datasets, grouping can categorize data and documentation provides context and clarity
- ❑ **Automated classification:** Automation accelerates and drives efficiencies in classifying ingested data, eliminating error-prone manual efforts and enhancing accuracy
- ❑ **Collaboration tools:** An important element for operationalizing your data catalog is the capacity for users to communicate and interact with each other within the data context by sharing comments, annotations and shared insights. This can foster a more collaborative data culture, which is key for adoption
- ❑ **Data marketplace:** A distinguishing capability for enterprise data catalogs, a data marketplace is a platform where allowing users at all levels can 'shop' for datasets easily, helping them discover, share and collaborate around data

Data lineage:

Map the data journey

Data lineage is about understanding. As data moves through multiple systems, it transforms. Understanding its journey—where it comes from, how it changes and where it's used—is critical for managing your complex data environment. Data lineage provides transparency, accuracy and compliance support with evolving regulations.

Why data lineage is important

Data doesn't exist in isolation; it flows, transforms, gets consumed and influences decisions.

- **Trust and accuracy:** Just as you'd trust a news story more if you knew its source, tracing data's lineage boosts confidence in its accuracy
- **Data quality:** If data seems incorrect or inconsistent, lineage helps pinpoint the stage where the discrepancy occurred
- **Compliance and audits:** Regulations often require businesses to explain their data sources and transformations. Data lineage offers a clear map for compliance teams and auditors

Key features to look for

- **Automated lineage discovery:** Eliminates manual tracking and ensures accuracy
- **Visualization capabilities:** Graphical views make data flows easier to understand
- **Integration with diverse data sources:** Connects with cloud, databases and third-party systems
- **Technical and business lineage:** Supports both detailed data tracking and high-level impact analysis
- **Scalability:** Handles large datasets without performance issues



Use case

Here are some key areas where data lineage plays a critical role in the public sector:

- **Regulatory compliance:** Demonstrate compliance — for example, to CCPA — by mapping the journey of personal data through various systems and processes
 - **Data migration:** Assess the potential impact of planned data changes to business units across the organization, minimizing disruptions
 - **Data lineage:** Track and document the lineage of input, training and output data of AI models, ensuring transparency and accountability
- 

Map your critical data flows

Use this template to document your highest-priority data flows:

Critical system inventory

List your mission-critical systems

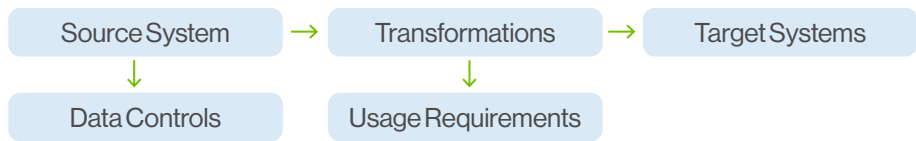
System Name:

Data Owner:

Primary Purpose:

Key Stakeholders:

Draw your data flow



Assess impact

Data flow	Mission impact	Compliance requirements	Dependencies
Flow 1			
Flow 2			

Data privacy:

Handle data properly

Data privacy is about protection. As sensitive information moves through government systems, it requires careful handling to safeguard citizen privacy, maintain public trust and ensure compliance with federal regulations. Privacy management provides the controls, visibility and governance needed to protect sensitive data while enabling agencies to fulfill their missions.

Why data privacy is important

Data privacy isn't just about compliance—it's fundamental to maintaining public trust and enabling secure government operations.

- **Public trust:** Citizens share sensitive information with government agencies with the expectation it will be protected and used appropriately
- **Mission enablement:** Strong privacy controls allow agencies to safely leverage data for improved public services while protecting individual rights
- **Regulatory compliance:** Federal agencies must comply with various privacy laws including the Privacy Act of 1974, FISMA, and FERPA, among others

What features to look for

- **Automated sensitive data discovery:** Automatically identifies and classifies sensitive information across systems
- **Granular access controls:** Ensures users can only access information necessary for their roles
- **Audit trails:** Tracks and documents all data access and usage




Use case

Here are some key areas where data privacy plays a critical role in the public sector:

- **Benefits administration:** Protect sensitive citizen information while processing benefits applications and managing program eligibility
- **Cross-agency collaboration:** Enable secure data sharing between agencies while maintaining privacy controls and tracking data usage
- **Law enforcement:** Safeguard sensitive investigation data while enabling appropriate information sharing across jurisdictions

Data privacy is not just a legal necessity but also a marker of trust and reputation for organizations. As individuals, understanding and controlling our data footprint is the first step in ensuring our privacy in an increasingly interconnected world.



Privacy impact worksheet

Data inventory assessment

Complete for each major system:

PII Identification

- ☐ Direct identifiers
- ☐ Indirect identifiers
- ☐ Derived data
- ☐ Metadata

Usage matrix

Purpose of Collection:

Legal Authority:

Sharing Requirements:

Retention Period:

Policy control:

Define and control data access

Policy control is about protection through permissions. As government agencies manage vast amounts of sensitive data, they need robust controls to enforce who can access what information and under what circumstances. Policy control provides the framework for implementing “need to know” principles while enabling mission-critical data sharing and use.

Why is policy control is important

Policy control isn't just about restricting access—it's about enabling secure and appropriate data use across government operations.

- **Mission enablement:** Ensures personnel can access the information they need while protecting sensitive data from unauthorized access
- **Regulatory compliance:** Helps agencies meet federal requirements including FISMA, FedRAMP and agency-specific security directives

What features to look for

- **Centralized policy management:** Single interface to create and manage access policies across all systems
- **No-code policy creation:** Enables subject matter experts to define policies without technical expertise
- **Automated enforcement:** Consistently applies policies across systems without manual intervention
- **Data masking capabilities:** Protects sensitive information while maintaining data utility



Use case

Here are some key areas where policy control plays a critical role in the public sector:

- **Classified information:** Manage access to sensitive government information based on security clearance levels and need-to-know requirements
 - **Interagency collaboration:** Enable secure data sharing between agencies while maintaining appropriate access restrictions and tracking
 - **Personnel records:** Control access to federal employee information while enabling necessary HR functions and oversight
- 

Create an access control strategy

Document domains

Complete this matrix for your key data domains:

Data domain	Classification	Access levels	Approval chain
Mission data			
Personnel records			
Financial data			
Citizen services			

Define the roles

Role mapping template

Role name:

Business purpose:

Access levels:

- ☐ View only
- ☐ Edit
- ☐ Approve
- ☐ Admin

Systems access:

System one:

System two:

System three:

Required clearances:

- ☐ Public trust
- ☐ Secret
- ☐ Top Secret
- ☐ Compartmented

The power of active metadata

Active metadata is a dynamic, interconnected representation of data that can span a wide range of asset types, weaving together information about each asset. It's a key component that brings together every component of a data governance platform across your organization.

The integrated view provides rich content and context to data, ensuring it can be both trusted and acted upon. Unlike static metadata which offers a snapshot, active metadata is constantly evolving, reflecting real-time changes and integrations.

Key benefits of active metadata

- **Generate greater visibility into the data landscape:** With automatic data classification and auto-linking of data sets, business terms, policies, processes and more, data curators and data consumers can collaborate on business semantics for trusted data
- **Evaluate the right data for your needs:** Data profiling, data scoring and crowdsourced ratings and reviews strengthen data context and allow business analysts and data scientists to evaluate and choose the best data for their purposes
- **Enhance data shopping experience:** With highly relevant and rich business context around data, users have a more intuitive and simplified data shopping experience, which provides the right data with the right context to the right users
- **Deliver faster insights:** Automated discovery, understanding and collaborative data access for business analysts and data scientists reduce time to insights

Active metadata isn't just another buzzword. It represents a shift toward a more interconnected, dynamic and actionable data environment. As data continues to grow both in volume and complexity, tools and methodologies like these will be instrumental in ensuring that data remains an asset, not a challenge.

Three steps to getting started: Trust, comply, consume

Step 1 | Trust: Ensure data is reliable

The foundation for trusting data isn't just about policies and procedures—it's about reliably supporting your agency's mission. Instead of adopting another agency's framework, map your specific mission requirements.

- What decisions do your leaders make?
- What evidence do they need?
- How does data flow through your organization?

These questions will help shape a framework that works for you.

Take stock of your data landscape

Think of your agency's data like city infrastructure—you need to know what you have before you can effectively manage it. Look beyond obvious databases to legacy systems, shared services, unstructured data and external feeds. Your goal is understanding your entire data ecosystem—from ownership to usage to mission urgency.

Build quality into the process

You know data quality isn't optional—that citizens and agencies rely on high-quality data. So define what “good” data looks like. Monitor it actively. And create clear processes for addressing challenges before they become issues.

How to get started

Begin with a single mission-critical dataset. Document where you are and where you need to be. Map out who creates and uses the data, define what quality means in this context and create a focused plan for improvement.

Remember, trust isn't built overnight—start small, demonstrate value, and expand thoughtfully.

Step 2 | Comply: Enable unified governance

Compliance isn't a checkbox

It's a fundamental mission responsibility. While everyone shares responsibility for privacy, your risk, legal and privacy teams need to be woven into the fabric of your data operations. They aren't gatekeepers but enablers, helping shape how data serves the mission while protecting citizen trust. The goal is embedding privacy into your agency's DNA, making it part of how you think about and use data, not an afterthought.

As your agency explores AI, remember that algorithms are only as good as the data they learn from. AI governance isn't separate from data governance—it's an extension of it and organizations like NIST have developed frameworks to make it easy for you to ensure you're on the right track. The same teams that help govern your data should help shape your AI strategy. Start by understanding what AI projects are already happening across your agency.

- Which models are approved
- Which are experimental

Creating this baseline helps you govern AI initiatives properly from the start.

Nurturing a culture of compliance

Effective compliance isn't about saying "No"—it's about finding secure, responsible ways to say "Yes" to mission needs. Your governance framework should help teams understand not just what they can't do, but how they can achieve their goals while maintaining public trust. This means creating clear pathways for data and AI initiatives that balance innovation with responsibility.

How to get started

Begin with your current AI initiatives. Map them to your data governance framework. Where are the gaps? What new controls are needed? Build from what works in your data governance program, adapting it for AI's unique challenges. Remember, the goal isn't perfect governance—it's governance that enables mission success while protecting public trust.

Step 3 | Consume: The right data in the right hands

Making data discoverable

Success in the public sector isn't just about collecting data—it's about getting the right information to the right people at the right time. Think of your data as a well-organized library where every book has its place and purpose. Your teams shouldn't have to navigate a maze to find what they need. Instead, create clear pathways to reliable, mission-ready data that's already vetted and validated.

Building a data marketplace

A government data marketplace isn't like a commercial app store. It's a curated environment where approved datasets, AI models and analytics tools come together to serve your agency's mission. It's not about unlimited access—it's about streamlined, secure access to the resources your teams need. When someone needs data for a new initiative or report, they should know exactly where to go and what to expect.

The end goal isn't just making data available—it's enabling better decisions across your agency. Your marketplace should help teams understand not just what data exists, but how to use it effectively. Include context about data quality, lineage, and appropriate use cases. Help your teams make confident decisions with data they can trust.

How to get started

Start by identifying your most frequently used datasets. Make these your first marketplace offerings. Document their context, quality and proper use. Create simple processes for access that balance security with usability. Remember, adoption comes from making things easier—show your teams how the marketplace helps them serve the mission better.

Case study



U.S. Department of Defense

The Office of the Secretary of Defense

The problem:

The Office of the Secretary of Defense (OSD) and its Comptroller Office of the Undersecretary of Defense are responsible for US defense policy, planning, resource management and program evaluation. In carrying out those duties, the OSD's day-to-day decisions impact a wide range of operations, including human resources, weapons acquisition, research, intelligence and fiscal policy across all of the US armed forces (Army, Navy, Marine Corps and Air Force). Steering an organization of that size means data is crucial to its decision-making processes. However, ensuring decision makers have access to the right data, can trust in its accuracy and understand its context is by no means a simple task.

The solution:

Recognizing the challenge, the Director of the CFO Data Transformation Office partnered with Collibra to launch their Advana (Advancing Analytics) Data Catalog to create a centralized platform to support data and analytics across the organization. The Advana program is still relatively nascent, but has already made significant strides in its mission, with the team tracking key performance indicators to ensure they remain on the right path and can measure their progress.

[Learn how the Office of the Secretary of Defense enabled data discovery with Collibra](#)

Conclusion

Unifying governance for mission success

The gap between what agencies need to do with data and what they can accomplish continues to widen, especially as AI adoption accelerates. Traditional fragmented governance, with controls tethered to specific systems and sources, prevents agencies from scaling their data and AI initiatives safely.

Collibra's platform—which provides several deployment models including FedRAMP authorized cloud and self-hosted—offers a different approach through unified governance. By untethering governance from systems and sources, we give agencies true visibility, context and control throughout the full data cycle. Our platform enables automated access control and comprehensive AI governance, creating active links between datasets, policies and AI use cases.

The result? Data Confidence. Now you can accelerate all your data and AI use cases—without the risk—while maintaining the highest standards of security and compliance required in the public sector.

Accelerate all your data and AI use cases

Collibra Platform, a FedRAMP certified solution, accelerates data and AI for government departments and agencies faced with complex data challenges. Collibra unifies governance for data and AI across on-premises, hybrid and multi-cloud environments, engages every user and group, and creates the safety and autonomy needed for scaling data and AI across every use case.



Are you ready to transform how your agency manages data and AI?

Test drive Collibra today collibra.com