Workflow Based Agentic AI, Automation Support, and a Comprehensive E-Permitting System for Underground Injection Control (UIC) Class 1 and Class 6 Permitting

West Virginia Department of Environmental Protection
Division of Water and Waste Management (DWWM)

Technical Proposal Response - Master Copy

June 10, 2026

BUYER: Joseph (Josh) E Hager III

SOLICITATION NO:
CRFP 0313 DEP2600000003

BID OPENING DATE: 6/10/2026

BID OPENING TIME: 1:30 pm ET

Bid Delivery Address:
Department of Administration,
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

VENDOR NAME:

Infocap Networks, LLC

Vendor Code:VS0000046534

Nathaniel Palmer, CEO
6901 Professional Parkway E, Suite 200
Sarasota, FL 34240
Email: nathaniel@infocap.ai
Phone: 781-534-3868 (direct)

SBA-Qualified Small Business

infocap.ai
Human-Centric Automation

June 10, 2026

Joseph (Josh) E Hager III
Department of Administration,
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Dear Josh,

It is our honor to submit Infocap's proposal to the State of West Virginia for CCRFP 0313 DEP2600000003, Workflow Based Agentic AI, Automation, and E-Permitting System. Our proposal is designed to meet or exceed these requirements, while helping the Agency accelerate permit review, reduce manual workload, improve consistency, and preserve final decision-making authority with agency staff.

Infocap is an SBA-qualified small business founded to help government agencies modernize operations through practical, human-centered automation. Although our billing address is in Florida, our delivery leadership is based in Virginia, and our team is positioned to provide responsive support to the State of West Virginia through both remote collaboration and regional resources within a few hours' drive of Charleston. We are committed to a smooth, well-governed implementation and to providing WVDEP with a secure, explainable, and auditable solution that aligns with the CRFP's requirements for FedRAMP-bound operation, data protection, HITL review, and long-term support. Additional details regarding our approach, qualifications, staffing, and solution capabilities are included in the attached proposal materials.

Supporting the mission of the Agency and its service to the people of West Virginia would be an honor for the Infocap team. It is also of great personal importance to me. I have deep love for West Virginia, and have many family members across Kanawha, Ohio, and Mason County. My great grandad started Palmer's Shoe Store on Capital Street, which my family continued for many years until it finally closed a few decades ago. I enjoy every opportunity I get to visit Charleston and West Virginia. Recently, my son also performed home repairs for a family on the East End, as part of a service project with our church.

With Infocap as your partner of choice for this groundbreaking initiative, you have my personal commitment and guarantee of the greatest value to the people of West Virginia.

Respectfully,

Nathaniel Palmer
CEO, Infocap

Executive Summary

Infocap appreciates the Agency's mission to protect, preserve, and enhance West Virginia's watersheds, while helping modernize permitting workflows through secure, auditable automation that supports faster, more consistent review without compromising regulatory oversight.

As a company whose primary focus for over a decade has been delivering complex document processing and application adjudication within highly-regulated environments, Infocap understands that Class I and Class VI UIC permitting maybe a comparatively low-volume workstream, yet is nonetheless a very high-consequence process where accuracy, repeatability, and the defensibility determinations are all imperatives which cannot be compromised.

Our approach is built on a clear principle: delivering the workflow, evidence, and review-orchestration layer which compliments the One Stop Shop Permitting Portal by converting submissions into governed electronic cases, trusted AI-ready data, source-grounded AI outputs, reviewer work queues, auditable decision records, and enforceable human approval gates.

Why TotalAgility is the Right Platform for the Agency's Workflow-Based Agentic AI UIC E-Permitting Solution

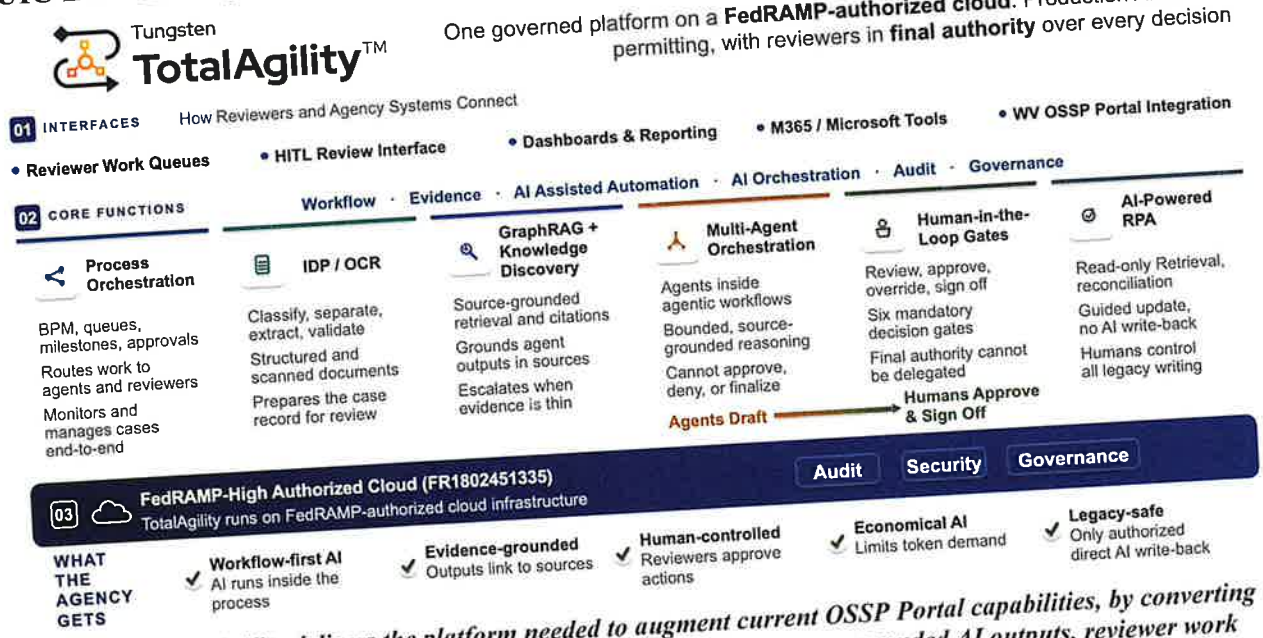


Figure 1 – TotalAgility delivers the platform needed to augment current OSSP Portal capabilities, by converting submissions into governed electronic cases, trusted AI-ready data, source-grounded AI outputs, reviewer work queues, auditable decision records, and enforceable human approval gates.

Infocap has over a decade of experience in cloud-native, full-stack development, as a partner to Google, Microsoft, and Amazon AWS. As a premier AWS partner holding multiple certifications, credentials, and competencies, our own AWS Marketplace offering (*Infocap Intelligent Document Automation*) offers a proven, scalable AI-native solution for Agentic Workflow and OCR. Yet, it is based on our **extensive cloud and AI-native development experience, combined with many years of experience with complex document-driven application adjudication, which leads us to choose Tungsten Automation's TotalAgility as the foundation for the proposed solution.**

The Operating Layer the Agency Needs

TotalAgility is the foundation that turns the Agency's UIC permitting ambition into an operational system. It is not merely a chatbot, OCR engine, RPA tool, or document repository. It is the workflow, evidence, and review-orchestration layer that receives permit packages from the One Stop Shop Permitting Portal, creates the governed UIC case, transforms documents into trusted AI-ready data, routes work to reviewers and agents, grounds AI outputs in source evidence, enforces mandatory human approval gates, and preserves the audit-ready permitting record.

What the Agency Gets with TotalAgility

- ✓ AI Explainability and Traceability
- ✓ Scalable Mult-Agent Orchestration
- ✓ Agentic Automation with HITL
- ✓ Trusted AI-Ready Case Data
- ✓ Human-Governed Permit Decisions
- ✓ Lower-Token Operating Economics
- ✓ FedRAMP Cloud Hosting

For the Agency, this means every Class I and Class VI application moves through a controlled lifecycle: intake, completeness review, technical review, GIS/AoR coordination, deficiency drafting, public notice, response-to-comments, draft permit, final decision package, and closeout. TotalAgility provides the case structure, workflow rules, reviewer queues, milestones, exceptions, approvals, and decision trace that make AI usable in a regulated permitting environment.

Trusted Data Before AI

The central risk in enterprise AI is not model quality; it is untrusted data. Agentic workflows require structured, validated, contextual information before they can act with accountability. TotalAgility addresses this by applying Document Intelligence before GenAI, leveraging IDP/OCR, process automation, Retrieval-Augmented Generation (RAG) and GraphRAG to accurately classify and transform unstructured documents into trusted, AI-ready data and actionable insights.

That matters for UIC permitting. EPA Form 7520-6, maps, AoR materials, geologic data, well construction details, operating parameters, financial responsibility documents, public comments, certification statements, and technical appendices must be classified, separated, extracted, validated, and tied to the case before AI can reliably reason over them. Bad OCR, weak document separation, and poor table extraction create bad AI. TotalAgility prevents that failure mode by making document intelligence the foundation of the review process.

Agentic Automation Under Regulatory Control

The Agency needs agentic AI, but not uncontrolled autonomy. TotalAgility delivers agentic automation inside deterministic governance. Purpose-built worker agents support intake, completeness review, Knowledge Discovery, technical evidence organization, drafting, validation, public participation, and final package assembly. Managing/case agents coordinate those worker agents, invoke approved tools, use Knowledge Discovery, launch workflows, call APIs or MCP tools, trigger RPA, and route exceptions to human queues.

This gives the Agency the benefit of multi-agent orchestration without letting AI become the decision-maker. TotalAgility's agentic design materials describe retrieval agents, worker/micro agents, and managing/case agents, plus tool use, planning, reflection, and multi-agent patterns within guardrails. The result is a digital workforce that accelerates review while remaining governed by rules, evidence, roles, and Human-in-the-Loop (HITL) approvals.

Source-Grounded Review, Not Chatbot Guesswork

TotalAgility replaces free-form chatbotting with source-grounded review. AI Knowledge Bases and the Knowledge Discovery Agent allow the solution to retrieve from approved case documents, the Agency SOPs, regulatory references, public comments, historical records, and external evidence. The Knowledge Discovery pattern uses question embedding, permissioned knowledge base search, result reranking, AI analysis of source document references, and source highlighting in the document viewer.

Analyst Rankings of TotalAgility

- ✓ **Gartner**: Leader, 2025 Magic Quadrant for Intelligent Document Processing.
- ✓ **IDC MarketScape**: Leader, 2024 Worldwide Unstructured Intelligent Document Processing.
- ✓ **Everest Group**: Leader, 2025 Process Orchestration PEAK Matrix.

For the Agency, this means an AI-generated summary, deficiency recommendation, permit condition, or response-to-comments draft is not a floating answer. It is tied to the application record, retrieved evidence, source references, and reviewer validation. Advanced Chunk Enrichment further improves retrieval relevance so RAG results are more complete, contextual, and accurate. Where the Agency requires relationship-aware retrieval, Infocap will map applicants, wells, injection zones, confining zones, USDWs, AoR features, faults, receptors, permit conditions, comments, and historical decisions. Where true graph traversal is required, Infocap will integrate a GraphRAG service through TotalAgility's workflow, Knowledge Discovery, MCP/API, and evidence layer.

Human Authority and Defensible Decisions

TotalAgility preserves the Agency's regulatory authority. AI outputs remain recommendations, summaries, evidence packets, or drafts until the Agency staff approve them. Mandatory human approval gates will stop workflow progression before deficiency notices, administrative compliance approval, Area-of-Review (AoR) validation, technical analysis approval, draft permit approval, and final issue/deny decisions.

Each action is recorded. TotalAgility preserves the agent action trace, source evidence, rules applied, tool outputs, confidence and validation signals, reviewer identity, timestamp, decision, override, rationale summary, and final disposition. The Agency receives an audit-ready permitting record that explains what happened, what evidence was used, and who approved it.

Lower Token Consumption, Predictable Economics

TotalAgility is computationally economical because it avoids the most expensive mistake in AI: sending entire document packages repeatedly through LLMs. The platform performs OCR, classification, separation, extraction, validation, rules, workflow routing, RPA retrieval, and structured case reuse before GenAI is invoked. RAG retrieves targeted evidence instead of stuffing large documents into prompts. GenAI is reserved for high-value tasks such as summarization, drafting, regulatory Q&A, response support, and complex review assistance.

This is the "Right AI for the right task" model: deterministic rules where the answer is known, document intelligence where data must be extracted, RAG where evidence must be retrieved, GenAI where language reasoning adds value, RPA where legacy systems must be accommodated, and human review where regulatory judgment is required.

A Production Platform, Not an AI Prototype

A custom full-stack AI build would force the Agency to assemble separate components for OCR, IDP, RAG, workflow, RPA, agent orchestration, HITL UI, GIS integration, audit logging, security, testing, rollback, reporting, monitoring, and token governance. That creates tool sprawl, integration risk, cost uncertainty, and audit gaps.

In contrast, TotalAgility provides a single point of control with one governed automation foundation. It supports package promotion, testing, rollback, monitoring, dashboards, exception handling, AI Performance & Usage Controls, knowledge discovery, workflow governance, RPA integration, and secure cloud deployment. TotalAgility Cloud securely supports government agencies with document intake, classification, routing, task automation, workflow orchestration, AI-driven knowledge discovery, human-in-the-loop processing, and audit-ready evidence.

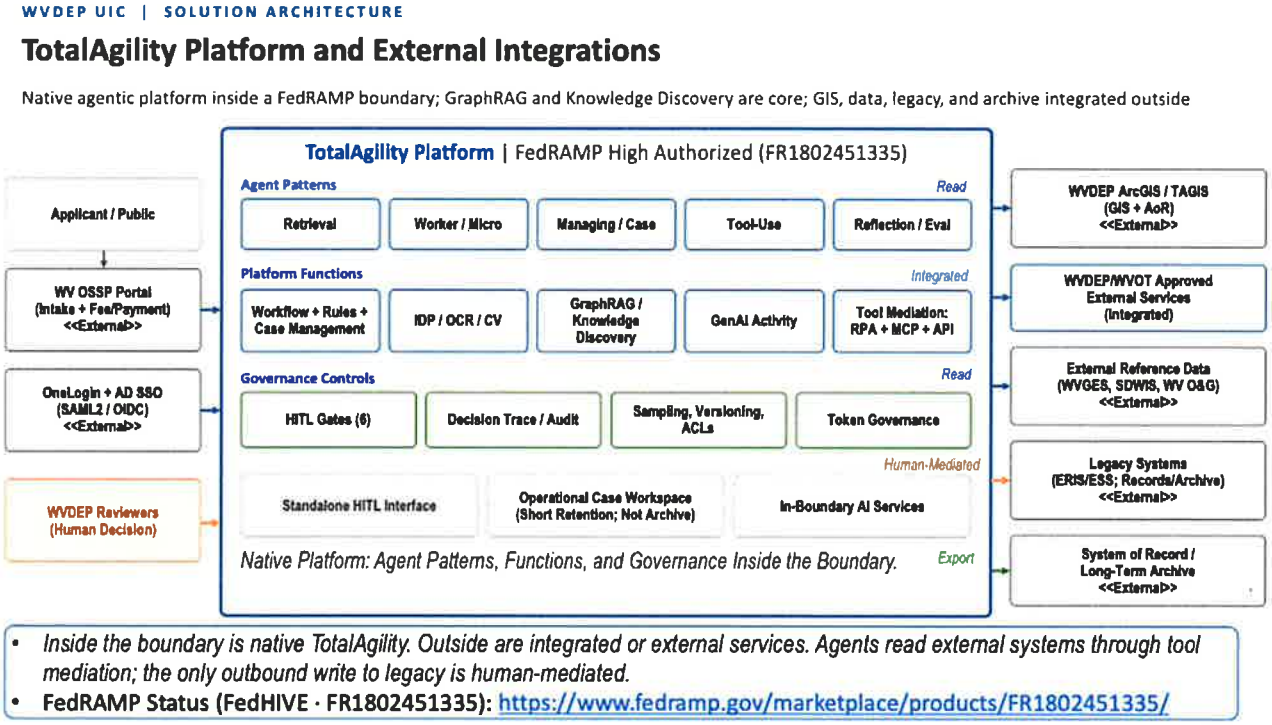


Figure 2 - TotalAgility Platform and External Integrations - native agentic platform inside a FedRAMP High Authorized boundary; GraphRAG and Knowledge Discovery are core; GIS, data, legacy, and archive integrated externally

This is why Tungsten Automation's TotalAgility is the right foundation. Integrated GIS, CAD, and scientific modeling services will perform spatial analysis, topology validation, normalization, visualization, and AoR modeling. TotalAgility will orchestrate those services, pass approved case inputs, receive results, record source layers and assumptions, create reviewer tasks, preserve the evidence packet, and enforce the Agency's human technical validation before findings advance.

It makes the Agency's AI ambition production-ready: governed, explainable, secure, cost-controlled, reviewer-centered, source-grounded, and legacy-safe. It gives the Agency a

comprehensive UIC permitting operating layer, not an AI experiment, and positions the Agency to modernize with confidence from day one.

NOTE: as instructed, the rest of the document follows the structure of Section 4 in the CRFP.

4.2. Software as a Service (SaaS)

Infocap will deliver our proposed solution as a fully managed cloud-based Software as a Service (SaaS) platform hosted within FedRAMP High Authorized boundary and security controls consistent with applicable NIST SP 800-53 requirements. Our proposed solution satisfies the Agency's required FedRAMP Moderate security requirements for secure processing, storage, workflow orchestration, audit logging, monitoring, and AI-assisted permitting operations. End users will securely access the platform through encrypted web-browser sessions, federated authentication services, and authorized application interfaces over the internet.

Secure SaaS AI Platform

- ✓ Centralized platform management, automated maintenance, infrastructure monitoring, backup replication, Disaster Recovery and resiliency
- ✓ All production services, including document storage, logging, monitoring, AI-assisted processing, workflow orchestration, and operational support functions remain within the controlled FedRAMP Authorized boundary hosting environment

The TotalAgility platform provides a secure, scalable, and highly available SaaS environment designed to support the Agency operational, security, compliance, and AI-governance requirements. Our proposed solution will include continuous monitoring, vulnerability management, audit logging, incident response, identity federation, role-based access controls, Multi-Factor Authentication (MFA), and operational-security controls supporting applicable FedRAMP and NIST SP 800-53 security requirements.

With this approach Infocap will ensure the Agency receives:

- Subscription-based licensing with flat year-over-year annual operating costs
- 99.9% platform availability excluding scheduled maintenance windows
- Vendor-managed platform updates, security patches, and approved AI-service enhancements governed through formal change-management processes
- High availability, regional resiliency, and elastic scalability
- Data sovereignty and storage within the continental United States
- Service Level Agreements (SLAs) covering platform availability, performance, incident response, restoration targets, support services, and operational escalation procedures
- Section 508 compliance for user-facing interfaces and workflow components

4.3. Project Goals and Mandatory Requirements

Infocap's proposed solution will support the full permitting lifecycle including permit intake, application classification, OCR and document extraction, administrative completeness review, technical-review workflows, GIS and Area-of-Review (AoR) coordination, AI-assisted drafting, public-notice preparation, response-to-comments support, reviewer collaboration, final-decision

routing, audit logging, records retention, reporting, and mandatory human review before any regulatory action is finalized.

TotalAgility's core platform capabilities align directly with the Agency operational and compliance requirements through integrated:

- Document Intelligence services supporting OCR, document classification, separation, extraction, Natural Language Processing (NLP), computer vision, and metadata generation
- Workflow and Process Orchestration supporting reviewer queues, routing rules, escalations, approvals, exception handling, and dashboard visibility
- Connected Systems integration supporting secure interoperability with the Agency's systems, GIS services, databases, OSSP integrations, email platforms, storage services, and external data sources
- Human-in-the-Loop (HITL) governance controls supporting reviewer validation, confidence scoring, overrides, adjudication workflows, and operational transparency
- AI-assisted processing services supporting controlled orchestration of AI, OCR, computer-vision, and generative-AI workflows under customer-governed policies and audit controls
- Adversarial validation through FedRAMP-required and 3PAO-attested security testing, annual penetration testing/red-team evidence, monthly vulnerability scanning and continuous monitoring, plus AI-specific adversarial testing such as prompt-injection testing, negative testing, RAG Q&A benchmarks, and Azure Prompt Shields.

All AI-assisted processing, OCR services, workflow orchestration, databases, document storage services, audit logging, token metering, monitoring services, and integrated AI capabilities supporting the Agency's solution will operate within controlled FedRAMP Authorized boundary cloud services. The Agency's data, workflow content, permit records, prompts, and AI-processing activities will not be routed to public consumer AI platforms or non-authorized cloud services.

TotalAgility incorporates centralized audit logging, SIEM integration, vulnerability management, incident-response governance, adversarial testing support, continuous monitoring, and operational security controls based on applicable FedRAMP and NIST SP 800-53 security practices. Security and AI-governance controls include role-based access control (RBAC), Multi-Factor Authentication (MFA), federated identity integration, encryption, prompt governance, reviewer approvals, AI auditability, model-change governance, and mandatory human override capabilities at all regulatory decision points.

The TotalAgility Cloud provides adversarial validation through FedRAMP-required and 3PAO-attested security testing, annual penetration testing/red-team evidence, monthly vulnerability scanning and continuous monitoring, plus AI-specific adversarial testing such as prompt-injection testing, negative testing, RAG Q&A benchmarks, and *Azure Prompt Shields*. For the Agency's custom agents, prompts, knowledge bases, and workflows, adversarial validation will be expanded by leveraging TotalAgility's tooling for testing, benchmarks, performance-monitoring. These support automated test scripts/plans/suites, deployment/package

management, version control, sampling, as well as running configured test plans before deployment and terminating deployment if those tests fail.

Consistent with FedRAMP's requirements and guidelines, Tungsten performs TotalAgility Cloud penetration testing annually, as well as monthly vulnerability scans using a third-party scanning service, Web Application Firewall (WAF), anti-malware/threat intelligence, 24/7 log monitoring/alerting by *Trusec*, and static/dynamic code scanning using *Veracode*, *Burp Suite*, and *Qualys*. Microsoft's built-in assessment engines evaluate policy assignments automatically once every 24 hours, and continuously monitor for active threats in real-time.

TotalAgility Provides Adversarial Validation in its Core Design

- ✓ Regular Pentesting, vulnerability scanning and continuous monitoring
- ✓ Prompt-injection testing, negative testing, and prompt shield services
- ✓ Third-party scanning service, WAF, anti-malware/threat intelligence, 24/7 log monitoring/alerting
- ✓ Built-in tooling for testing, benchmarks, and performance monitoring

The TotalAgility FedRAMP package contains its System Security Plan (SSP), Security Assessment Plan (SAP), and Security Assessment Report (SAR) as well as related artifacts such as red-team test plan/reports, penetration test reports, vulnerability-scan artifacts, POA&M (Plan of Action and Milestones) and AI validation test results.

At the AI layer, Tungsten provides prompt-injection testing and adversarial techniques, including human evaluation, negative testing, prompt injection testing, automated testing, and question/answer benchmarks for Document and Knowledge Base RAG using validated correct answers and source references. These methods map to NIST's generative-AI risk guidance for systems to undergo regular adversarial testing to identify vulnerabilities, manipulation, or misuse. NIST also recommends adversarial testing at a regular cadence to identify vulnerabilities, misuse scenarios, and unintended outputs. Further, prompts and completions are evaluated in real time for harmful content, Azure guardrails/content filtering are enabled, and Prompt Shields are configured to prevent jailbreak or indirect attacks.

4.3.1. Goals and Objectives

TotalAgility brings together the three capabilities the Agency needs for AI-assisted permitting: Document Automation, Knowledge Discovery, and Process Automation. Document Automation ingests, classifies, extracts, and validates information from incoming documents so that UIC submissions become trusted, AI-ready data. Knowledge Discovery turns unstructured case content into source-grounded insights that reviewers and agents can use.

Our proposed solution will not replace the Agency regulatory judgment: AI services will classify, extract, summarize, recommend, draft, flag risks, and route work across documents and geospatial data, while authorized the Agency personnel approve deficiencies, compliance determinations, technical findings, draft permits, and final issue/deny decisions. The AI value of TotalAgility begins before generative AI is invoked. UIC applications contain forms, scanned documents, engineering drawings, maps, tables, geologic reports, financial responsibility materials, public comments, signatures, and technical appendices. If these materials are not properly ingested, classified, extracted, validated, and associated with the correct case, any downstream AI result becomes unreliable. TotalAgility reduces that risk by applying Document

and Content AI first, using OCR, classification, separation, extraction, validation, table handling, document review, and business rules to transform unstructured submissions into review-ready evidence.

AI-Accelerated Review, Human-Controlled Decisions

- ✓ Automates intake, extraction, routing, and review of applications and complex document packages
- ✓ Unifies GIS, AoR, and document evidence within a single framework
- ✓ Accelerates and automates notices, permits, and comment responses
- ✓ Preserves regulatory authority, processing observability and application auditability

Infocap's solution for the Agency will significantly reduce manual intake and administrative-processing burdens through automated document ingestion, OCR and metadata extraction, intelligent document classification, completeness verification, workflow routing, reviewer task management, and AI-assisted analysis. Geospatial and AoR inputs (e.g., well locations, plume/pressure extents, receptors, and protected resources) flow into the same workflow, where AI applies configured spatial and rules-based checks, reviewers validate findings in a map-centric interface, and all actions are captured as auditable records that drive standardized technical review, integrated GIS/document evidence, and the automated generation of notices, draft permits, public notices, and response-to-comments documents. This integrated operating model directly fulfills the CRFP's requirements for AI-enabled RPA, document processing, advanced GIS/AoR integration, and mandatory human-in-the-loop decision gates that protect the Agency's regulatory authority and ensure end-to-end auditability.

We will leverage source-grounded AI-generated recommendations, document summarization, extraction validation, risk identification, draft-document preparation, public-notice generation, response-to-comments support, and workflow prioritization using HITL governance controls requiring reviewer validation, adjudication, and approval before regulatory actions are finalized. AI-generated outputs, reviewer actions, workflow events, extracted data, prompts, confidence scores, and operational activities will be logged and auditable to support regulatory oversight, explainability, forensic review, and compliance validation. The system will automate or otherwise accelerate preparation of notices of deficiency, draft permits, public notices, technical-review summaries, response-to-comments packages, and final decision-support documentation while improving workflow consistency, reducing manual administrative effort, and supporting more efficient permit-review operations.

TotalAgility is purpose-built to assist and support (not replace) the Agency's regulatory judgment and decision-making authority. AI-assisted services will support document classification, extraction, summarization, recommendation generation, risk flagging, workflow routing, and draft-document preparation, while authorized the Agency personnel will retain full authority over completeness determinations, technical findings, compliance decisions, permit conditions, deficiency notices, draft approvals, and final issue or deny determinations.

This approach directly supports the CRFP requirements for AI-enabled RPA, document intelligence, OCR processing, workflow orchestration, advanced GIS integration, secure dashboard reporting, auditability, and mandatory HITL decision gates designed to maintain regulatory accountability, operational transparency, and responsible AI governance. All workflow orchestration, document processing, AI-assisted services, audit logging, monitoring,

and operational support functions will remain within the controlled hosting environment, and the Agency's data will not be routed to public consumer AI platforms or non-authorized cloud services. GIS and AoR evidence will be preserved in the electronic case file, routed through AoR HITL validation, and included in approved evidence/export packages.

A Dashboard the Agency Controls

- ✓ Web-based HTML dashboard interfaces with the Agency's existing website
- ✓ Controls automation execution and displays job logs in real time
- ✓ Secure login and password protection on every view
- ✓ Editing and updates limited to authorized personnel only

4.3.2. Terms of Service and Renewal

Infocap confirms compliance with the requested service-term structure. Our proposed solution will support an initial five (5) year term of service with the option for the Agency to renew the contract for one (1) additional year, subject to final contract terms, funding authorization, and renewal approval.

Infocap will align the SaaS subscription, hosting, support, maintenance, monitoring, updates, AI services, licensing, and implementation services with the Agency's requested five-year initial term and optional one-year renewal period.

The subscription will include access to production and non-production environments, workflow orchestration services, document-intelligence capabilities, AI-assisted processing, support services, patching, upgrades, monitoring, backups, and applicable AI-service configuration as defined within the final statement of work, subscription order, and licensing schedule.

Infocap's proposed approach will ensure long-term operational continuity, scalability, maintainability, and regulatory-review operations throughout the base term and renewal periods.

4.3.2.1 General Automation and Dashboard Integration

As part of TotalAgility as the centralized AI-enabled RPA, workflow orchestration, document-intelligence, integration, and operational dashboard platform supporting the Agency's UIC Class I and Class VI permitting lifecycle. Our proposed solution will provide a unified operational environment for permit intake, workflow routing, document processing, AI-assisted review, Human-in-the-Loop (HITL) validation, reporting, audit logging, operational monitoring, regulatory oversight, and secure integration with existing the Agency's systems and approved external data sources.

The system will provide centralized visibility into workflow status, reviewer assignments, task queues, AI-generated recommendations, document-processing results, extracted metadata, exception handling, public-notice activities, response-to-comments workflows, operational metrics, audit events, and final decision routing. Configurable dashboards and reporting services will support reviewer productivity monitoring, SLA tracking, management oversight, compliance reporting, and operational analytics throughout all stages of the permitting process.

GIS/AoR workflow visibility will include submitted-layer status, map-review task status, coordinate-reference-system status, topology-validation status, AoR buffer or model-evidence status, external-source cross-check status, risk-feature flags, GIS reviewer assignment, AoR approval status, and GIS-related override history. This visibility will allow the Agency's

personnel to monitor the status of spatial data validation, AoR review, GIS exception handling, and reviewer-approved GIS findings within the broader UIC case workflow.

TotalAgility will serve as the centralized process and integration hub coordinating the movement of data, documents, tasks, approvals, notifications, and workflow activities across the permitting lifecycle. This architecture minimizes the need for multiple point-to-point integrations, simplifies maintenance, improves auditability, and provides a scalable framework for future enhancements and integrations. The platform supports native integration capabilities including REST and SOAP web services, database connectivity, secure file transfer (SFTP), XML, JSON, CSV, email and event-driven processing, authentication services, custom APIs, and integration services. These capabilities support integration with modern cloud-based applications and existing agency systems without requiring significant modification to underlying platforms. Supporting the requirements listed in the solicitation and associated addenda, our proposed solution will support integration with WV One Stop Shop Permitting (OSSP), OneLogin, Active Directory, ESRI ArcGIS platforms, EPA SDWIS, WVGES, approved state and federal regulatory data sources, and existing the Agency's databases and information repositories supporting permitting operations.

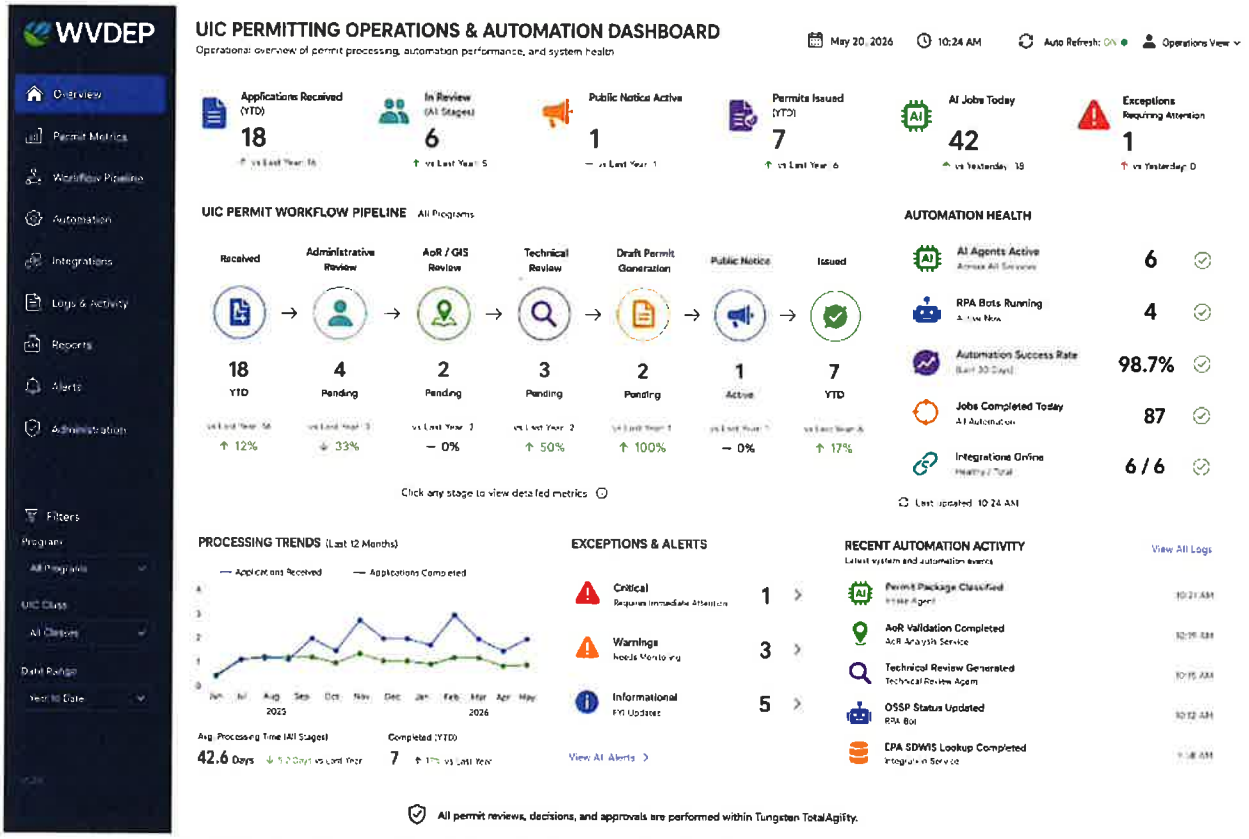


Figure 3 - Sample UIC Permitting Operations & Automation Dashboard Mockup - permit pipeline, automation health, processing trends, exceptions and alerts, and recent automation activity

Infocap's proposed solution will automate the retrieval, validation, routing, and presentation of information supporting administrative completeness reviews, technical compliance evaluations, GIS validation activities, permit drafting, public-notice generation, regulatory reporting, and

final decision support. Where supported APIs or standard integration methods are unavailable, RPA will be utilized to support repetitive digital tasks such as information retrieval, validation, status checks, and system lookups under the same governance, security, exception handling, and audit requirements as other automated processes.

TotalAgility's workflow orchestration services, agent roles, reporting services, transformation services, and document-intelligence capabilities will support OCR processing, document classification, extraction, scheduling, monitoring, automated workflow activities, AI-assisted processing, reporting, and job archiving within a centralized and auditable operational environment. The proposed architecture supports secure, scalable, and operationally resilient workflow automation while maintaining centralized governance, auditability, AI oversight, compliance visibility, and integration integrity throughout the permit-review lifecycle. All integrations will utilize approved interfaces, secured service endpoints, encrypted communications, federated authentication, and centralized audit logging to support secure and traceable permitting operations.

One Platform, One Dashboard, Every Job and Log

- ✓ AI-enabled RPA platform with a central dashboard for all jobs and logs
- ✓ Integrates with the Agency's existing operational software
- ✓ Web-based dashboard posts to the Agency website to control execution and show logs
- ✓ Secure login restricts access, editing, and updates to authorized personnel=

4.3.2.1.1 System Automation/Integration

Infocap will integrate TotalAgility with the Agency's operational software applications, systems of record, repositories, and external data sources through approved APIs, secure connectors, web services, encrypted file exchanges, database views, scheduled imports and exports, and controlled human-mediated workflows where direct integration is not authorized or technically appropriate. The architecture will support secure interoperability between cloud-based and on-premise systems while maintaining operational integrity, auditability, and security controls. TotalAgility includes Connected Systems integration capabilities and Integration Server services supporting secure communications, workflow triggering, document retrieval, metadata synchronization, reporting, and operational data exchange without requiring local storage of regulated data outside controlled hosting environments. Where legacy systems are not suitable for direct AI interaction or automated write-back operations, our proposed solution will support controlled human-mediated workflows through generated export packages, reviewer task queues, operational summaries, and structured update processes designed to preserve legacy system integrity while still enabling workflow automation and AI-assisted review capabilities.

All integration services, workflow orchestration, document processing, audit logging, monitoring services, AI-assisted workflows, and operational data exchanges supporting our proposed solution will operate within FedRAMP boundary cloud services and security controls consistent with FedRAMP operational standards. Operational integrations will align with WVDEP/WVOT-approved systems and access methods confirmed during discovery, including WV One Stop Shop Permitting, OneLogin, Active Directory, approved ArcGIS/ESRI services, and authorized Agency data sources. GIS data-source access will be handled separately through approved ArcGIS services, public data exports, APIs where available, secure file import, scheduled file exchange, reviewer upload, or manual reference. The proposed workflow will not

assume that every GIS, property, well, or regulatory source exposes a direct API or automated write-back capability. Where direct integration is not available or not authorized, TotalAgility will route data-access exceptions, reviewer-uploaded outputs, and manual validation steps through governed HITL workflows with audit logging.

4.3.2.1.2 Dashboard Development

As illustrated in *Figure 3* in Infocap will develop browser-based HTML dashboards that can be linked from or accessed through the Agency's existing website or internal portal. The dashboard will provide a centralized operational view of permit processing activities, AI-enabled automation services, RPA operations, workflow performance, system health, and integration status.

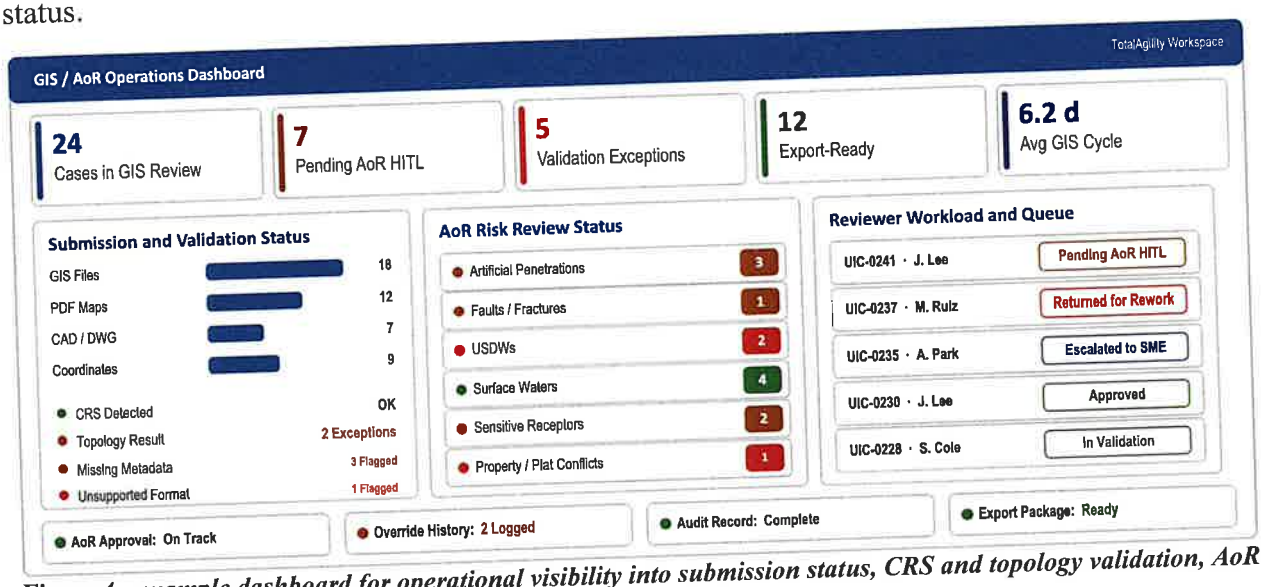


Figure 4 - example dashboard for operational visibility into submission status, CRS and topology validation, AoR risk flags, reviewer workload, approvals, and audit evidence

The dashboard is intended to serve as the operational monitoring and reporting interface for the permitting solution, providing authorized users with visibility into permit processing metrics, automation performance, workload trends, system activity, and audit information. Permit reviews, Human-in-the-Loop (HITL) approvals, document validation activities, and final permit decisions will continue to occur within the TotalAgility platform, where workflow controls, security policies, and audit requirements are enforced. Because the permitting platform will operate within a FedRAMP-authorized cloud environment, the dashboard will not directly access the TotalAgility application or underlying databases. Instead, dashboard information will be provided through a secure integration layer and controlled service endpoints operating within the approved cloud boundary. This approach maintains security while providing users with near real-time visibility into permitting operations and automation activity.

The dashboards will provide visibility into multiple operational metrics, such as:

Permit intake and application volumes	Workflow execution and throughput metrics
Administrative and technical review workload metrics	AI agent activity and processing statistics

HITL workload and processing statistics	RPA execution status and transaction volumes
GIS and Area of Review (AoR) processing status	Exception and error management
Public notice and comment activity	Integration health and connectivity status
Automation, workflow, and system logs	Operational performance and reporting metrics

GIS/AoR dashboard fields will include submitted-layer status, layer validation status, coordinate-system status, topology-validation result, AoR buffer/model-evidence status, external-data cross-check status, risk-feature counts, low-confidence spatial findings, GIS reviewer assignment, AoR approval status, reviewer override history, and GIS evidence export status.

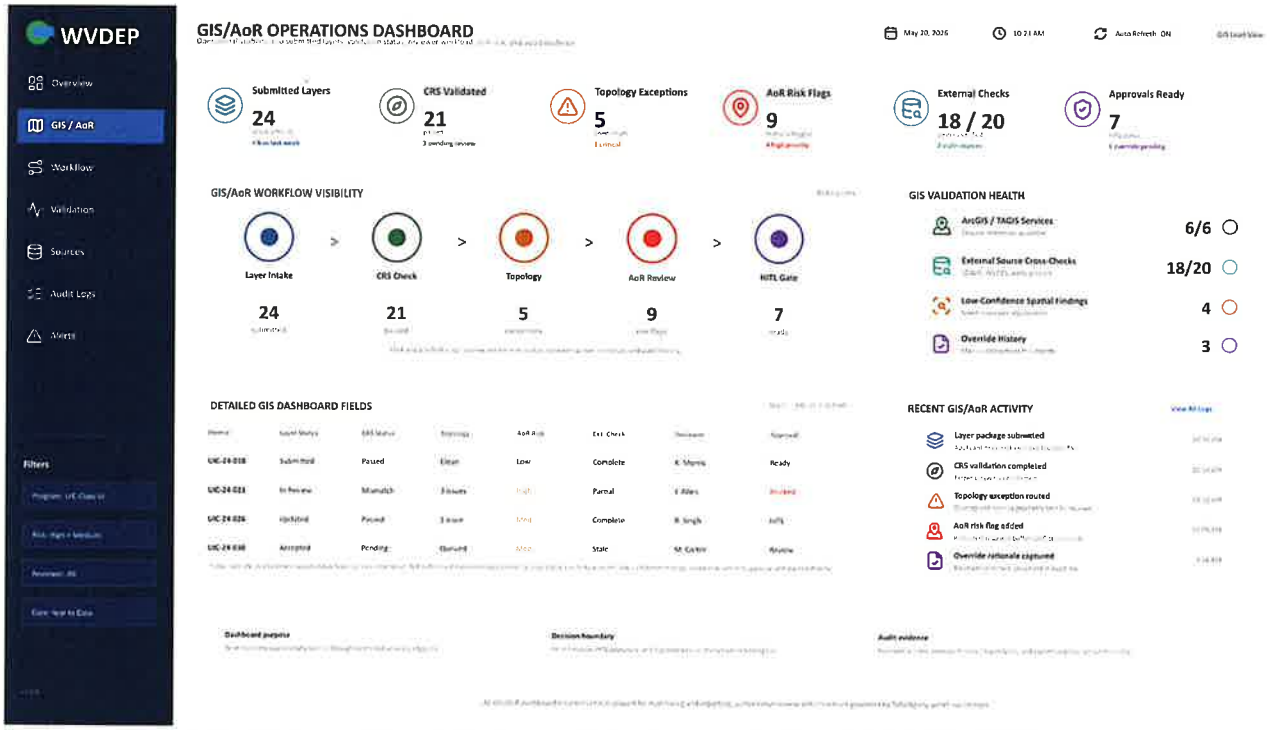


Figure 5 - Sample GIS/AoR Dashboard Mockup - The dashboard provides operational visibility into submitted-layer status, CRS/topology validation, AoR risk flags, external-source checks, GIS reviewer assignment, approval status, override history, and audit evidence

In addition to permit processing metrics, the dashboard will provide centralized monitoring of AI-enabled automation activities supporting the permitting process. Users will be able to view AI processing volumes, agent activity, confidence score trends, exception conditions, document processing statistics, and automation performance metrics. This visibility allows the Agency personnel to monitor the effectiveness of AI-assisted permit processing while maintaining appropriate human oversight.

The dashboard will also provide operational visibility into RPA activities used to support data retrieval, validation, reporting, and integration functions. Users will be able to monitor bot status, transaction volumes, execution history, processing exceptions, and overall automation health through a single interface.

Authorized users may perform approved operational actions, such as monitoring automation execution, reviewing job status, accessing logs, viewing system alerts, and reprocessing failed automation transactions based on assigned permissions. Permit review, approval, and decision-making activities will remain within the permitting platform and are not performed through the dashboard.

Security and Access Control

The dashboard will include secure authentication, role-based access controls, and audit logging to ensure information is available only to authorized personnel. Access permissions will govern the information, workflows, reports, and administrative functions available to each user based on their assigned role. The solution will support integration with Agency approved identity and access management services and security standards, including multi-factor authentication and single sign-on capabilities required by the Agency's security policies.

Logging, Monitoring, and Reporting

The dashboard will provide centralized access to workflow logs, AI activity logs, RPA execution logs, integration events, system alerts, and audit records. Users will be able to monitor permit processing progress, review automation exceptions, analyze operational performance, evaluate AI and RPA effectiveness, and track system health through configurable reports and dashboards.

By combining permit operations metrics with AI, RPA, workflow, and integration monitoring, the dashboard provides the Agency with a single operational view of both the permitting program and the automation technologies supporting it.

4.3.2.2 UIC Class I and Class VI Agentic AI Processing

Infocap's solution will streamline the Agency Class I and Class VI UIC application review through a workflow-based agentic AI operating model built on TotalAgility, serving as the workflow, evidence, and review-orchestration layer for the Agency's UIC e-permitting program. The platform augments the Agency's One Stop Shop Permitting Portal by converting submissions into governed electronic cases, trusted data, source-grounded AI outputs, reviewer work queues, auditable decision records, and enforceable human approval gates.

Infocap's proposed solution will not operate as a generic chatbot or a free-form AI system that autonomously issues, denies, or legally approves permits. TotalAgility will establish an electronic UIC case, transform submitted documents into trusted AI-ready data, create source-grounded knowledge bases, launch specialized worker agents, coordinate managing/case agents, trigger deterministic workflows, integrate external data sources, and enforce mandatory human review gates throughout the UIC review lifecycle.

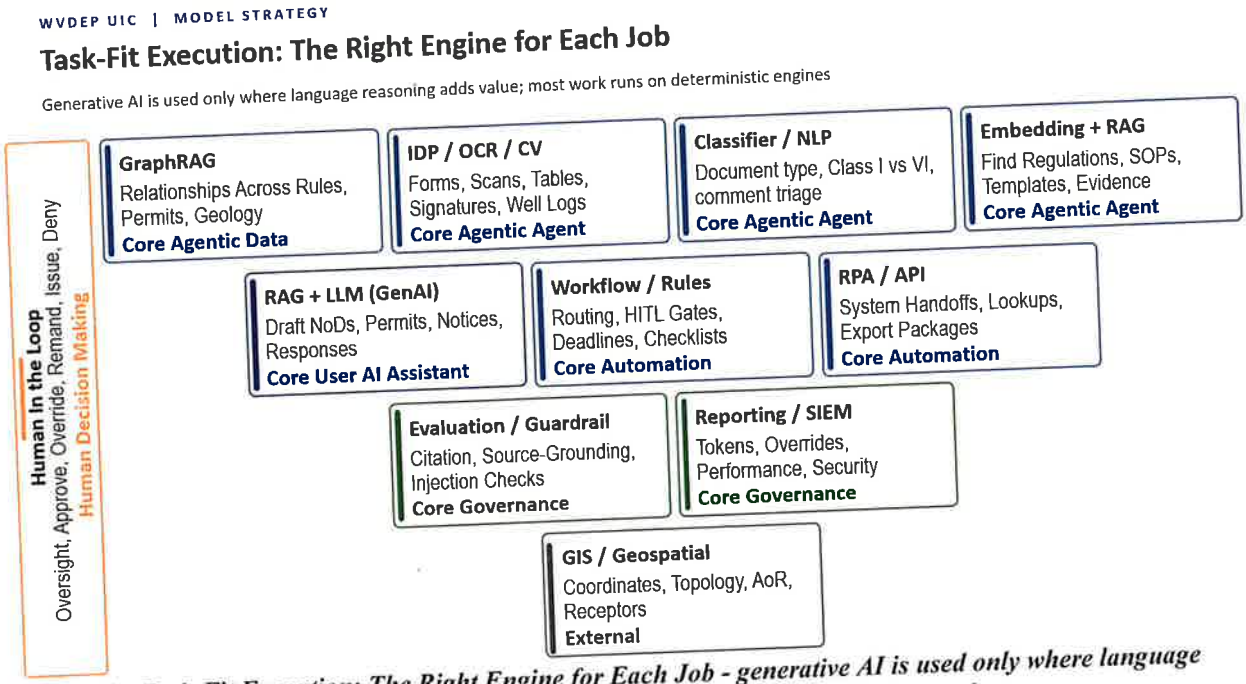


Figure 6 - Task-Fit Execution: The Right Engine for Each Job - generative AI is used only where language reasoning adds value; most work runs on deterministic engines, IDP/OCR, RPA, or rules

Infocap will implement a blended automation model that applies the right automation method to each task. Deterministic workflows and business rules will control known regulatory process steps, routing, required review stages, work queues, approvals, SLAs, and case state changes. TotalAgility Document Intelligence will perform intake, OCR, ICR, classification, separation, extraction, table extraction, image processing, validation, and verification. TotalAgility Knowledge Discovery and AI Knowledge Bases will provide source-grounded RAG review support. Quick AI Agents and worker agents will perform defined review, extraction, drafting, classification, research, and validation tasks. Managing/case agents will orchestrate multi-step UIC review activities, coordinate worker agents, call approved tools, and route exceptions to the Agency staff. MCP, API, RPA, data access, and secure connector integrations will connect external GIS, technical, regulatory, and Agency systems. Human-in-the-loop controls will govern all regulatory decisions.

4.3.2.2.1 Digital Intake Specialist Functionality

The TotalAgility-powered Digital Intake Specialist will serve as the first agentic layer in the UIC permitting process. It will receive or retrieve applications submitted through the Agency's One Stop Shop Permitting Portal, the Agency's UIC public-facing web page, or a secure agency-controlled gateway. Upon receipt, TotalAgility will generate a unique application tracking number, create the electronic UIC case file, normalize the submitted files, classify document types, extract structured case data, identify whether the application requires Class I or Class VI processing, detect required sub-workflows, build the case knowledge base, and route the work to the appropriate the Agency queues and agent teams.

The Digital Intake Specialist will use TotalAgility capture, OCR, classification, trainable separation, document sets, extraction groups, field validators, field formatters, business rules, and AI-supported extraction to normalize the application record before downstream agentic review begins. The intake process will identify and structure key UIC materials, including EPA Form 7520-6, facility location and legal description, operator identification, site maps, AoR calculations, well construction details, injection zone information, confining zone characterization, proposed injection rates, proposed injection volumes, proposed injection pressures, injection fluid characterization, Class VI geologic characterization, Testing and Monitoring Plan, Injection Well Plugging Plan, Post-Injection Site Care Plan, Emergency and Remedial Response Plan, Financial Responsibility documentation, Responsible Corporate Officer signatures, and required certification statements.

Agentic Intake Orchestrates Review-Ready Evidence

- ✓ Converts submission packets into review-ready electronic cases
- ✓ Extracts structured data from complex UIC documents
- ✓ Routes Class I/VI applications to correct workflows
- ✓ Turns missing items into reviewer-ready tasks
- ✓ Builds case knowledge for source-grounded review

TotalAgility will convert intake from a document drop-off process into a governed review-ready case. Submitted documents will become classified case evidence, extracted values will become structured fields, missing or low-confidence items will become reviewer tasks, and the full submission record will be available for workflow routing, RAG retrieval, administrative completeness review, technical review, drafting, public participation, and final decision package assembly.

4.3.2.2.1.1 Agentic Routing and Sub-Workflow Orchestration

TotalAgility will classify and route Class I and Class VI applications using extracted fields, document classifications, permit-type indicators, applicant-supplied form data, business rules, and agentic routing logic. The managing/case agent will observe the case data and submission package, consult document classifications, extracted fields, knowledge base results, GIS outputs, external-system responses, and applicable business rules, and then select the approved worker agents, workflows, APIs, RPA bots, MCP tools, or human review queues needed for the case.

TotalAgility's process orchestration engine will use BPMN-type workflows, branching rules, preconditions, milestones, states, dynamic resource assignment, roles, work queues, alerts, SLAs, business rules, and event triggers to ensure that each application follows the correct review path. Class I applications will be routed to Class I administrative review, fixed-radius AoR screening, well construction review, injection zone/confining zone review, USDW protection review, public notice workflow, draft permit workflow, and final decision workflow. Class VI applications will be routed to Class VI administrative review, computational AoR review, geologic characterization review, corrective action planning, financial responsibility verification, Testing and Monitoring Plan review, Injection Well Plugging Plan review, PISC review, Emergency and Remedial Response Plan review, CO2 stream and operating-parameter review, public notice workflow, response-to-comments workflow, draft permit workflow, and final decision workflow.

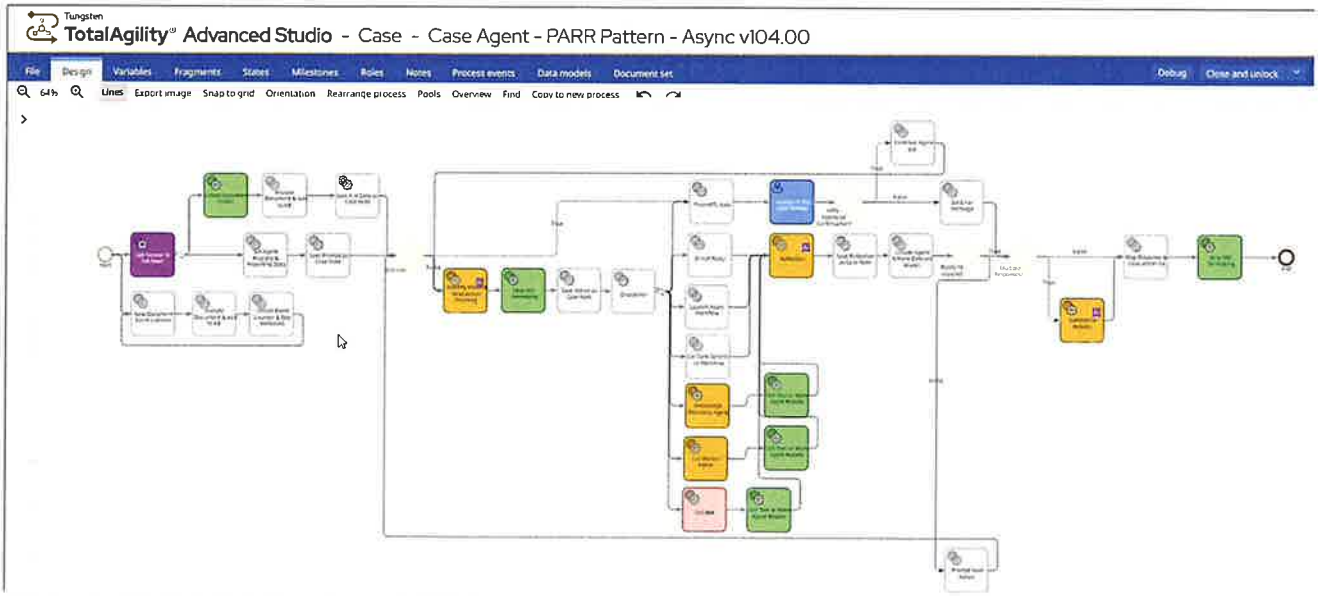


Figure 7 - TotalAgility Case Agent PARR Pattern workflow - Plan, Act, Reflect, Revise agentic orchestration design shown in Advanced Studio

Agentic routing will provide more than simple document classification. The managing/case agent will determine which sub-workflows are required based on the actual contents of the application. For example, detection of Class VI AoR modeling materials will trigger a model-evidence review workflow that routes submitted model inputs, assumptions, outputs, pressure/plume evidence, and AoR delineation materials to the appropriate the Agency's technical reviewers for validation. All Class VI model-related outputs will remain advisory evidence until reviewed and approved through the AoR & Risk Validation and Technical Analysis Approval HITL gates; detection of corrective action commitments will trigger corrective action planning review; detection of financial assurance materials will trigger financial responsibility verification; detection of well construction diagrams will trigger the Blueprint Vision Agent family and technical reviewer queue; and detection of public comment activity will trigger comment categorization and response-to-comments workflows.

Each routing action will be recorded in the TotalAgility decision trace. The trace will include the observed trigger, the case data or source evidence used, the worker agent or tool selected, the workflow launched, the routing rationale, the reviewer queue assigned, and the resulting case state. The case agent will not bypass required human gates. TotalAgility will enforce stop points before deficiency notices, administrative compliance approval, AoR validation, technical analysis approval, draft permit approval, and final issue/deny decisions. GIS/AoR sub-workflows will be triggered based on application class, well location, well type, submitted maps or GIS files, legal description, facility coordinates, geologic attachments, AoR calculations, Class VI model-evidence materials, and reviewer-confirmed metadata. Triggered GIS/AoR workflows will include format validation, CRS review, topology exception handling, Class I fixed-radius AoR review, Class VI model-evidence review, external-source correlation, risk-feature identification, GIS reviewer assignment, and AoR & Risk Validation HITL routing.

4.3.2.2.1.2 Administrative Completeness Review

TotalAgility will perform administrative completeness review using document sets, checklist variables, document rules, extracted fields, extraction confidence, business rules, RAG-supported checklists, and human validation. The system will confirm whether required application materials are present, properly classified, readable, signed where required, and associated with the correct case.

For Class I and Class VI intake, TotalAgility will verify the presence and status of project plans, site maps, AoR calculations, EPA Form 7520-6, facility location and legal description, operator identification, well construction details including casing and cementing programs, injection zone identification, confining zone characterization, proposed injection rates, proposed injection volumes, proposed injection pressures, and injection fluid characterization. For Class VI applications, TotalAgility will also verify detailed geologic characterization, Testing and Monitoring Plan, Injection Well Plugging Plan, Post-Injection Site Care Plan, Emergency and Remedial Response Plan, and Financial Responsibility documentation.

The completeness workflow will compare required document types against permit class, application type, extracted metadata, the Agency-defined checklists, and applicable workflow rules. Missing materials will be captured as structured deficiencies. Low-confidence extraction results will be routed to validation. Conflicting data between forms, attachments, maps, tables, diagrams, and supporting narratives will be flagged for reviewer attention.

Responsible Corporate Officer signatures and mandatory certification statements will be checked through TotalAgility document intelligence, OCR/NLP, signature/certification detection patterns, text extraction, and human validation. Where signature verification requires an external e-signature validation or identity verification service, Infocap will integrate the appropriate validation service and capture the service result, timestamp, reviewer action, and supporting evidence in the TotalAgility case record.

4.3.2.2.1.3 Technical Compliance Review

TotalAgility will orchestrate technical compliance review by extracting, normalizing, comparing, presenting, and routing technical evidence to qualified Agency reviewers. The platform will not replace the Agency technical experts. It will provide the workflow, evidence, RAG, agentic review, external tool integration, and approval controls required to make technical review faster, more consistent, and more defensible.

The technical review workflow will organize evidence related to injection zone depth, thickness, lithology, porosity, permeability, formation pressure, confining zone integrity, USDW identification and protection, well construction design, casing materials, cementing programs, operating parameters, injection pressure, injection rate, injection volume, injection fluid characterization, corrective action needs, AoR technical screening, Class VI computational

model inputs, boundary conditions, assumptions, reevaluation schedules, financial responsibility, plugging, PISC, testing and monitoring, and emergency response.

Specialized worker agents will prepare evidence packets for each technical discipline. The Injection Zone Review Agent will extract and summarize injection zone data; the Confining Zone Review Agent will organize confining zone evidence; the Well Construction Review Agent will compare casing, cementing, tubing, and packer information against required criteria; the USDW Protection Review Agent will gather aquifer and SDWIS-related evidence; the Operating Parameters Agent will organize pressure, rate, volume, and fluid information; and the Corrective Action, Plugging, PISC, Testing and Monitoring, Emergency Response, and Financial Responsibility agents will prepare structured findings for reviewer validation.

Automated Validation, Reviewer-Approved Findings

- ✓ Advanced extraction and geological validation against regulatory standards
- ✓ Evaluates injection zone depth, thickness, lithology, porosity, permeability, and pressure
- ✓ Assesses confining zone integrity and USDW identification and protection
- ✓ Senior technical reviewers validate all findings before they become official

Where hydrogeologic, geologic, AoR modeling, or engineering validation requires specialized tools or SME-authored models, Infocap will integrate those tools and orchestrate their use through TotalAgility. TotalAgility will preserve the request, input data, source documents, external model output, model version, assumptions, confidence or quality indicators, reviewer decision, override rationale, and downstream workflow action. This creates a defensible technical review record while maintaining human decision authority. Applications under technical review will be locked from applicant amendment until the Agency issues an official correction/deficiency letter.

4.3.2.2.2 RAG and Source Grounding

TotalAgility Knowledge Discovery and AI Knowledge Bases will ground AI outputs in the permit record, the Agency policies, SOPs, regulatory references, historical permit records, and approved external sources. TotalAgility serves as the workflow, evidence, and review-orchestration layer for the Agency's UIC e-permitting program. The platform augments the Agency's One Stop Shop Permitting Portal by converting submissions into governed electronic cases, trusted data, source-grounded AI outputs, reviewer work queues, auditable decision records, and enforceable human approval gates.

Infocap will configure the RAG workflow to add submitted documents, extracted application data, reviewer notes, approved reference materials, regulatory materials, SOPs, templates, and historical permit artifacts to governed knowledge bases. Security permissions, filters, case context, source status, and confidentiality controls will limit the retrieval scope. When an agent or reviewer asks a question, TotalAgility will embed the question or prompt, search by semantic/vector similarity, apply filters and permissions, re-rank results using case context and question intent, and generate an answer from source document references. Where available, the answer will include source highlighting and links back to the originating document, page, section, table, figure, field, or chunk.

Ensuring that Every Automated Outcome is Observable, Explainable, Auditable, and Accountable

- ✓ Infocap leverages hierarchical RAG and GraphRAG to make the work done by humans more consistent, predictable, and less reliant upon subjective interpretation of policies and rules
- ✓ The same techniques and capabilities simultaneously expand the aperture for what is automatable
- ✓ The result is that both AI agents and human workers use the same systems, follow the same rules, as well as are equally observable and accountable

Our solution will prevent reliance on irrelevant or outdated information through source governance, knowledge base curation, versioning, permissions, effective-date metadata, superseded-source controls, and workflow review of knowledge base updates. Outdated or incorrect materials will be removed or excluded from retrieval through controlled knowledge base management. Regulatory, SOP, and permit-template changes will be routed through a governance workflow before use in production review.

Infocap will implement relationship-aware retrieval for by creating and maintaining relationships among applicant, facility, well, injection zone, confining zone, USDW, AoR, artificial penetrations, faults, receptors, regulatory citations, permit conditions, public comments, and historical decisions. This relationship layer will allow agents and reviewers to ask questions across the permit record and receive answers that connect the relevant application facts, technical evidence, regulatory requirements, and case history. Where true graph traversal or GraphRAG is required, Infocap will integrate a knowledge graph or graph database service and orchestrate it through TotalAgility's Knowledge Discovery, MCP/API, and workflow layer. This approach is stronger than basic document search or prompting because it retrieves relevant, governed, current material and targeted evidence rather than entire documents, improves explainability, reduces hallucination risk, allows the Agency to validate and version the knowledge base; and preserves source links for audit, public record, appeal, and defensible regulatory decision-making.

4.3.2.2.3 Hallucination Mitigation

Infocap will implement hallucination mitigation through deterministic governance around probabilistic AI. This is enforced through a *defense-in-depth* control framework that prevents unsupported, uncited, outdated, or unvalidated AI content from advancing the UIC permitting workflow. AI may assist the Agency's reviewers with analysis, summarization, drafting, and recommendation support, but workflow rules, document rules, approved knowledge sources, structured validation, compliance checks, and mandatory Human-in-the-Loop approvals will control whether any output can progress. This approach does not rely on a single "magic bullet." It combines trusted data, governed retrieval, deterministic rules, validation agents, auditability, and human authority to prevent ungrounded AI content from becoming a regulatory action.

The first hallucination-control layer is trusted AI-ready data. For example, TotalAgility will apply Document Intelligence before RAG or GenAI, because poor OCR, weak document separation, missed tables, or inaccurate extraction creates poor AI results. EPA Form 7520-6, AoR evidence, GIS/model outputs, Class VI geologic characterization, Testing and Monitoring Plans, Financial Responsibility documentation, public comments, maps, attachments, and certification statements will be classified, separated, extracted, validated, and tied to the electronic case before they are used by AI agents. Low-confidence fields, missing documents, inconsistent values, and unreadable materials will be routed to validation rather than passed forward as reliable evidence.

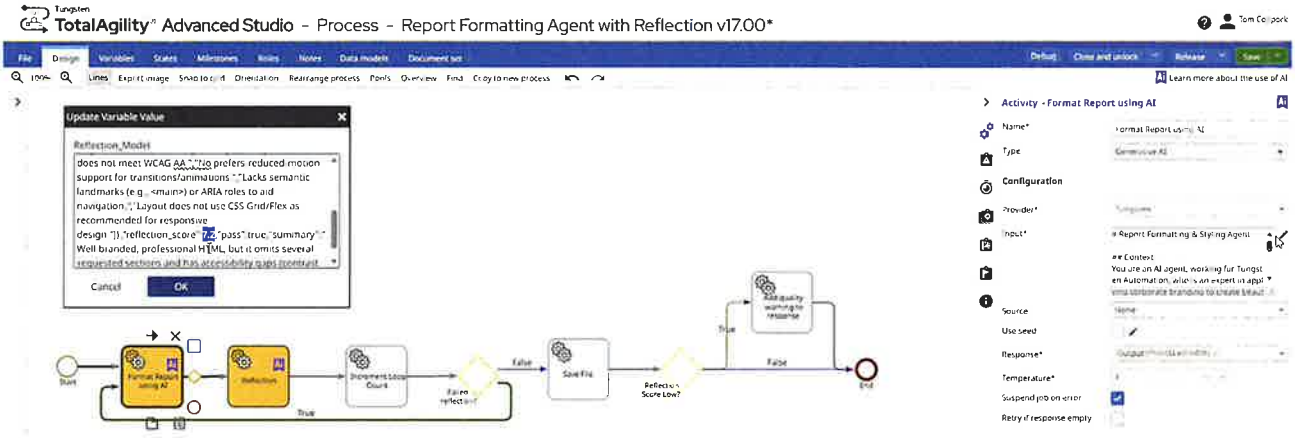


Figure 8 - TotalAgility Report Formatting Agent with Reflection - reflection loop workflow and variable inspection dialog showing reflection_score and pass:true validation result

The second layer is source-grounded RAG using approved TotalAgility AI Knowledge Bases. Agents will retrieve only from governed permit records, approved regulatory sources, Agency SOPs, case-specific evidence, external-system outputs recorded in the case, and current approved reference materials. Retrieval filters, permissions, source version controls, effective-date controls, and approved-source governance will prevent reliance on irrelevant, unauthorized, or superseded content. Knowledge Discovery will use case context, source references, reranking, and source highlighting so reviewers can see where the information originated. Prompt templates will require citations, prohibit unsupported claims, and instruct agents to return a no-answer or insufficient-evidence response when support is missing.

The third layer is structured output validation. AI-generated outputs will use response schemas requiring each material claim, finding, deficiency, recommendation, or draft statement to include source support, confidence or relevance indicators, and review status. Known regulatory logic will be implemented as deterministic business rules wherever possible, including completeness checks, required-document rules, routing criteria, validation requirements, escalation rules, and approval paths. Watchdog and compliance agents will monitor for outdated or superseded regulatory content and route potential regulatory changes for Agency review before any rule, workflow, checklist, or template update is implemented.

High-risk outputs will receive additional reflection and validation. Separate validator agents will review draft Notices of Deficiency, technical findings, draft permit conditions, public notice language, response-to-comments drafts, and final decision-support summaries. These validators

will check source support, completeness, citation accuracy, currentness of evidence, template compliance, conflict with the case record, missing materials, and need for human escalation. Figure 9 illustrates this control pattern using a TotalAgility Report Formatting Agent with a reflection loop, where the system records reflection_score and pass:true validation status before allowing the output to proceed.

4.3.2.2.4 Automated and Continuous AI Validation

Infocap will implement automated and continuous AI validation as part of the TotalAgility governance model. Infocap's proposed solution will provide continuous AI security, validation, and operational control for the permit review system by combining platform security, workflow governance, AI usage/performance controls, benchmark testing, human validation, and deployment controls.

The validation program will include benchmarks for document classification, document separation, field extraction, table extraction, knowledge base retrieval, RAG answer quality, citation accuracy, drafting quality, reflection scoring, and agent outputs. Infocap will configure test sets for Class I and Class VI administrative review, technical review, AoR review, public notice generation, response-to-comments drafting, and final decision package preparation. Q&A benchmark sets will include expected answers, required source references, and acceptable citation ranges.

Before production release, agent workflows, prompts, knowledge base configurations, extraction models, routing rules, and templates will be tested through Dev/UAT/Production promotion. Regression testing will be performed before deployment of material changes. Prompt-injection and negative testing will validate that the system resists malicious requests, instructions embedded in applicant documents, unsafe public comments, unauthorized approvals, unauthorized access, and unintended tool actions.

Sampling/checking ratios will route selected outputs to human review based on risk, confidence, permit class, reviewer override rates, document type, and workflow stage. Human validation feedback will be captured for continuous improvement. Reviewer overrides will be tracked and analyzed to identify model drift, prompt issues, retrieval gaps, training needs, or workflow rule changes.

Security will be enforced through role-based access, federated identity, least-privilege permissions, ACLs, data segregation, encryption in transit and at rest, audit logging, SIEM/SOC integration, vulnerability management, and FedRAMP cloud controls where applicable. AI-generated recommendations will not approve, deny, or finalize permits. TotalAgility will enforce mandatory human decision gates before any regulatory action is taken.

4.3.2.2.5 Citations and Explainability

Infocap's proposed solution will provide citations and explainability for AI-generated interactions used in the review record. Each AI-supported review output will include source references showing where the information originated in supplied documents, approved knowledge bases, external system outputs, or the case record. Where available, references will include document name, page, section, table, figure, field, or chunk, with links back to the TotalAgility document viewer or source record.

TotalAgility will capture confidence and validation indicators where available, including extracted field confidence, retrieval relevance, validation results, source-grounding details, and reviewer actions. The system will provide a plain-language rationale summary explaining the observable basis for the recommendation, including the facts extracted, sources consulted, rules applied, evidence produced, exceptions identified, and reviewer action taken. These citation, confidence, and rationale records will support reviewer validation, quality control, auditability, appeal support, and regulatory defensibility. Detailed AgentOps observability and decision-trace controls are addressed in §4.3.2.5.3.

4.3.2.3 Geospatial Analysis and Geographic Information System (GIS) Integration

Infocap will implement geospatial analysis and GIS integration as part of the TotalAgility-orchestrated UIC e-permitting workflow. TotalAgility will serve as the case, workflow, evidence, and review-orchestration layer for geospatial validation. Agency-approved GIS, CAD, geospatial, ArcGIS/TAGIS, and geoscience tools will perform spatial analysis, topology checks, projection standardization, 2D/3D visualization, and reviewer-led model-evidence validation. TotalAgility will not replace the Agency's authoritative GIS or geoscience modeling environments. TotalAgility will orchestrate GIS intake, tasking, evidence capture, reviewer validation, exception routing, audit logging, and workflow progression based on outputs produced by approved GIS tools, applicant submissions, and Agency technical reviewers.

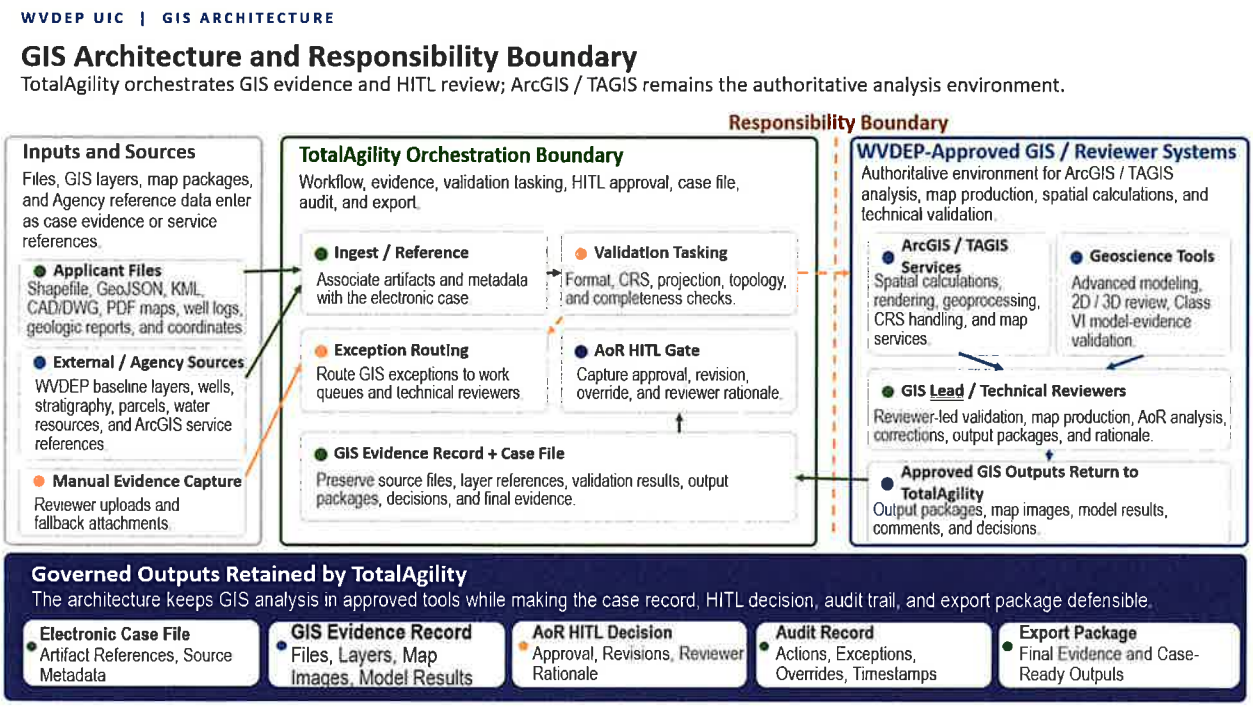


Figure 9 GIS Architecture and Responsibility Boundary - TotalAgility provides GIS workflow orchestration, evidence capture, HITL routing, audit, and export, while WVDEP-approved ArcGIS/TAGIS and reviewer systems remain authoritative for analysis and validation

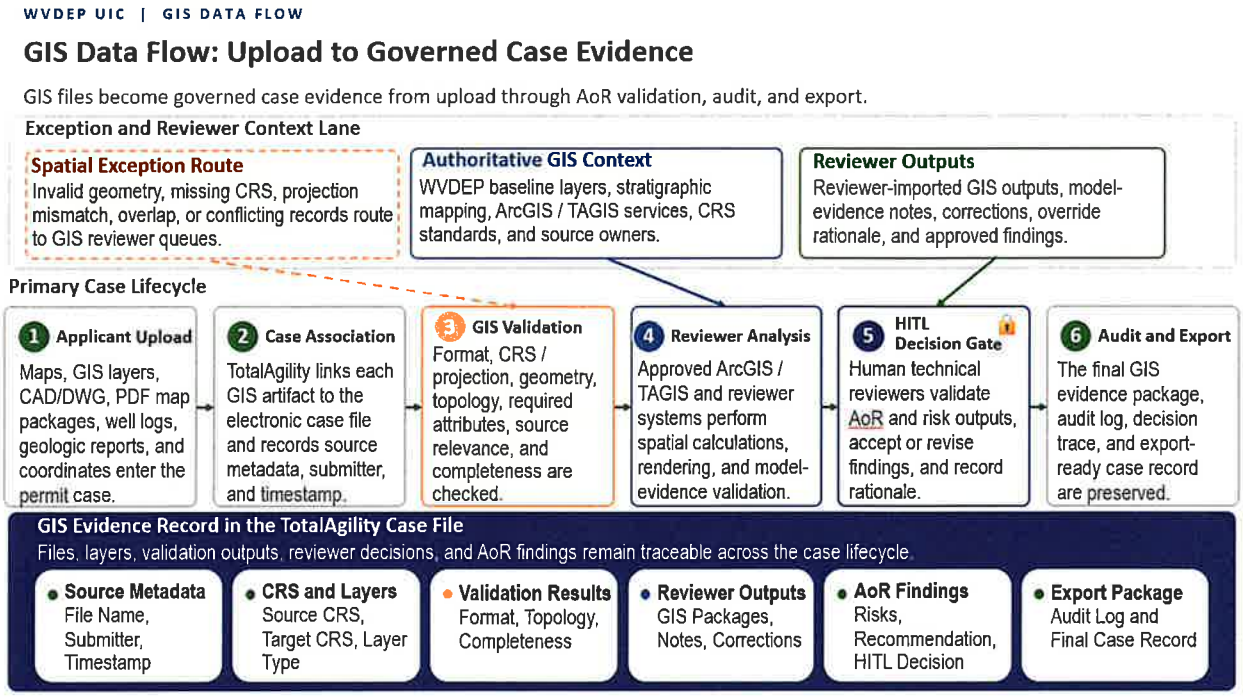


Figure 10 - GIS Data Flow Through the Case Lifecycle-Applicant GIS files, layers, reviewer outputs, and AoR findings move through intake, validation, ArcGIS/reviewer analysis, HITL approval, audit preservation, and export

The system will ingest or reference applicant-submitted geospatial materials, including Shapefile, GeoJSON, KML, CAD, DWG, map images, well schematics, and related technical drawings through integrated GIS/CAD services orchestrated by TotalAgility. The integrated geospatial services will normalize coordinate-system outputs, including auto-projection to NAD83/UTM Zone 17N where required by the final design. TotalAgility will record metadata, source file references, processing status, validation results, projection information, topology-check outputs, map images, model results, and reviewer decisions in the case record.

During discovery and implementation, Infocap will work with the Agency to inventory and validate the baseline GIS, stratigraphic, geologic, and related reference datasets that the Agency will provide for UIC permitting operations, including authoritative layers, map services, subsurface mapping products, and associated metadata used to support AoR review, risk screening, stratigraphic interpretation, and technical evaluation, as described in Addendum Q19. Our proposed solution will be configured to use those Agency-provided baseline datasets and services as the authoritative reference context for geospatial review workflows, while identifying any gaps, format issues, access constraints, or data-preparation steps requiring coordinated resolution during implementation.

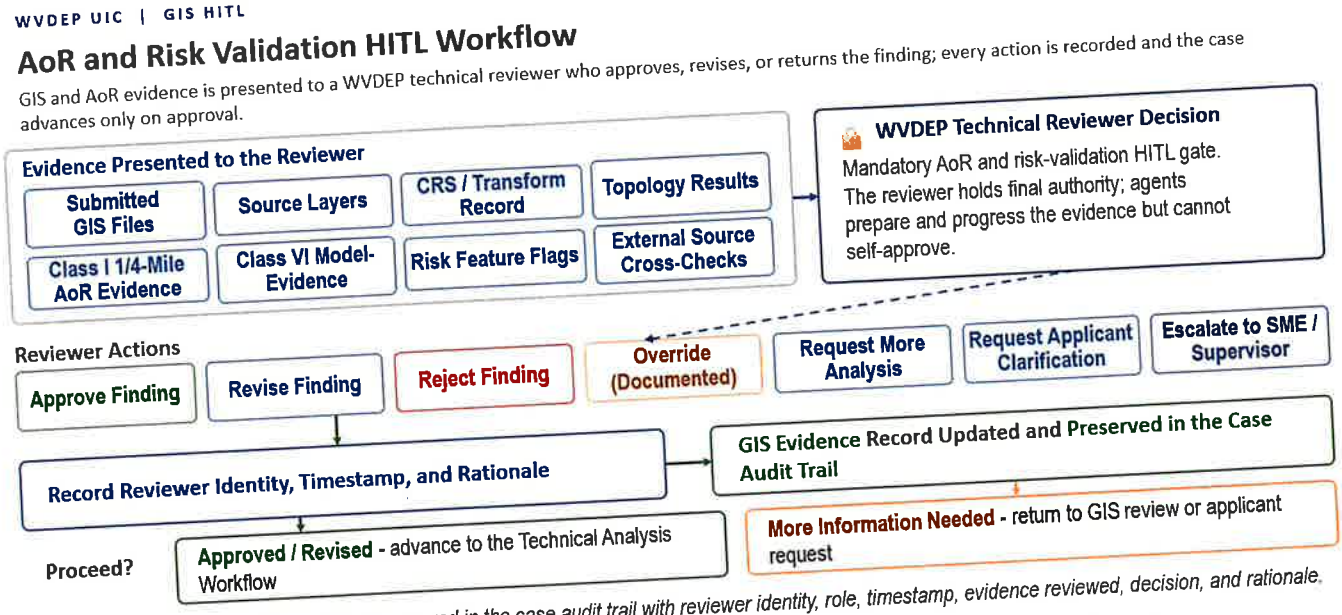


Figure 11 - AoR and Risk Validation HITL Workflow - GIS and AoR evidence is presented to an Agency technical reviewer who approves, revises, or returns the finding; every action is recorded and the case advances only on approval

TotalAgility will route spatial exceptions to appropriate the Agency reviewers and work queues. Examples include invalid geometry, missing coordinate reference system, projection mismatch, overlapping polygons, malformed GIS submissions, inconsistent legal descriptions, proximity to risk features, conflicts with external records, and Class VI model input discrepancies. The platform will present these results as evidence packets and reviewer tasks, not as final determinations.

The table below summarizes how the proposed leverages TotalAgility and its extended AI services to support the Agency's GIS operating model, including supported formats, CRS handling, validation rules, and fallback approaches when native GIS files are not available.

Aspect	Capabilities, Benefits, and Outcomes
Supported Formats	ESRI Shapefile, GeoJSON, KML, CAD, DWG, and related the WVDEP/WVOT-approved geospatial/map layers, ingested via integrations with the Agency's ArcGIS Enterprise 11.5 services, ArcGIS Portal, and ArcGIS Online/Open Data Hub.
Version Support	Supports industry-standard and currently supported versions of ESRI Shapefile and ArcGIS feature services published from the Agency's ArcGIS Enterprise 11.5 environment, as well as common GeoJSON, KML, and CAD/DWG variants; legacy or proprietary formats may require pre-processing through the Agency's TAGIS environment.
Coordinate Reference Systems (CRS)	Native support for the Agency and state-approved CRS and projections, including NAD83 in decimal degrees and NAD83 / UTM Zone 17N, consistent with existing the Agency's county boundary and statewide datasets.
CRS and Metadata Requirements	All geospatial submissions must include explicit CRS definitions and basic layer metadata (e.g., layer type, intended use, date/source, and scale or resolution) aligned with the Agency/TAGIS data-publishing practices to support consistent AoR and geologic-model review.

Maximum Data Size	Optimized for typical UIC project-level datasets and services; extremely large regional models, dense LiDAR/3D grids, or multi-gigabyte engineering files may be staged or tiled via the Agency's ArcGIS Enterprise and LiDAR services rather than loaded as single monolithic files.
Validation Rules	Automated checks flag invalid geometries, topology errors, overlapping or missing boundaries, inconsistent or missing CRS, projection mismatches, incomplete required attributes, and gaps relative to the Agency required reference layers (e.g., county boundaries, wells, water resources) for HITL review.
HITL Exception Handling	Any format, topology, or CRS exceptions that cannot be auto-corrected are routed to designated Agency reviewers in a map-centric interface (leveraging ArcGIS services) for confirmation, correction, or rejection, with all actions captured in the centralized audit log.
Fallback When Native GIS Files Are Unavailable	When native GIS formats are missing or unusable, the workflow supports ingestion of alternate evidence (e.g., PDFs, images, tabular coordinates) and creation of provisional GIS layers via the Agency's ArcGIS environment for manual georeferencing and reviewer validation.
Integration Boundaries	TotalAgility provides workflow orchestration, document intelligence, case management, AI analysis, and HITL routing, while ArcGIS Enterprise/Portal/Online and related the Agency GIS infrastructure remain the authoritative engines for spatial calculations, rendering, and advanced geoprocessing.

Table 1 - Summary of TotalAgility GIS Operating Model Support - supported formats, CRS handling, validation rules, HITL exception handling, and fallback approaches

Note: References to ArcGIS Enterprise "11.5" reflect the Agency's current TAGIS documentation and are provided for illustrative alignment only; the final supported ArcGIS Enterprise/Portal/Online versions and configurations will be confirmed with the Agency during discovery and used as the authoritative basis for integration and validation design.

The proposed GIS architecture is based on a clear responsibility boundary. TotalAgility will orchestrate intake, tasking, evidence capture, reviewer validation, audit logging, dashboard visibility, workflow routing, and export packaging. Agency-approved GIS tools, ArcGIS services, TAGIS resources where applicable, reviewer GIS workstations, and approved geoscience tools will remain the authoritative environments for advanced spatial analysis, map rendering, geoprocessing, stratigraphic visualization, and technical validation. This approach gives the Agency a governed AI-assisted workflow while preserving reviewer control over GIS analysis and regulatory determinations. GIS data will enter the workflow through applicant-submitted maps, GIS layers, CAD-derived files, PDF map packages, well logs, geologic reports, tabular coordinates, and reviewer-imported GIS outputs.

TotalAgility will associate each GIS artifact with the electronic case file, record source metadata, validate format and coordinate-system information, route exceptions to GIS reviewers, capture approved GIS/AoR findings, and preserve the final GIS evidence record for audit and export. Where authoritative analysis occurs outside TotalAgility in Agency-approved GIS tools, the resulting map PDFs, layer exports, validation reports, reviewer notes, screenshots, and sign-off records will be returned to the case as controlled GIS Reviewer Output Packages.

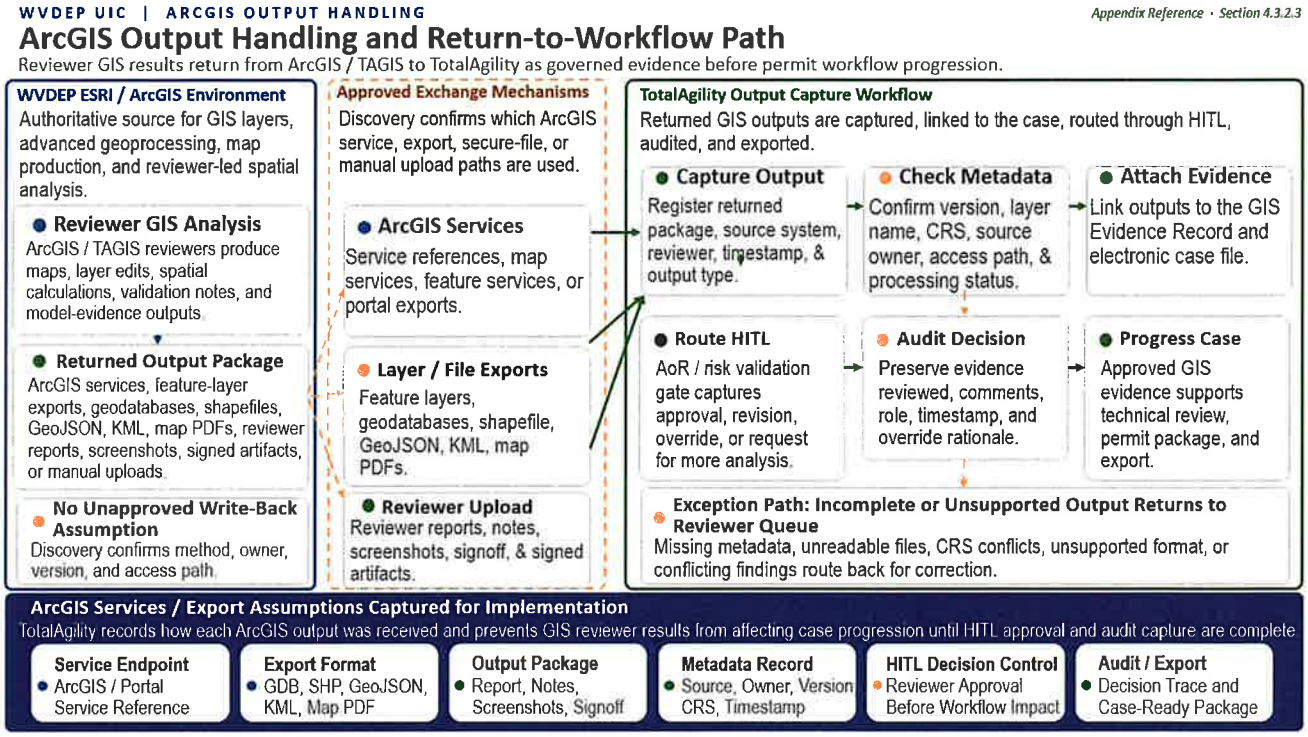


Figure 12 - ArcGIS Output Handling and Return-to-Workflow Path - reviewer GIS results return from ArcGIS/TAGIS to TotalAgility as governed evidence before permit workflow progression

Specific ArcGIS version, TAGIS access, ArcGIS service availability, baseline layer inventory, and integration details will be confirmed during discovery with the Agency. The solution will align to Agency-approved ESRI/ArcGIS environments and exchange mechanisms rather than assuming a specific unverified version or direct-access method. During discovery, Infocap will inventory baseline GIS layers, stratigraphic mapping resources, reference datasets, data dictionaries, coordinate-system standards, metadata requirements, reviewer output formats, and GIS quality-control rules. The solution will not assume that Infocap must recreate authoritative stratigraphic or GIS data from scratch. Instead, TotalAgility will reference, ingest, or capture Agency-approved baseline GIS outputs and reviewer-generated evidence as part of the governed UIC case record.

This GIS operating model strengthens the Agency's control by ensuring that TotalAgility manages workflow orchestration, evidence capture, reviewer tasking, audit logging, dashboard visibility, and export packaging, while Agency-approved GIS and geoscience tools remain authoritative for spatial analysis, map production, advanced geoprocessing, and technical validation. The result is a defensible GIS/AoR review process in which spatial findings are source-linked, reviewer-controlled, auditable, and available for technical review, draft permit support, public record development, and final decision support.

4.3.2.3.1 Automated Risk Assessment & AoR

TotalAgility will trigger AoR and risk assessment workflows based on permit class, extracted case data, GIS inputs, and document classifications. For Class I applications, the workflow will calculate or validate the fixed-radius 1/4-mile review requirement through integrated GIS

services and will identify artificial penetrations and relevant spatial risk features within the calculated AoR. For Class I applications, the fixed-radius AoR review will be based on validated well coordinates, documented coordinate-reference-system handling, recorded source-layer metadata, and reviewer-approved buffer evidence. If source coordinates, CRS information, or location evidence are incomplete or inconsistent, TotalAgility will route the item to a GIS reviewer before the AoR finding is used in technical review.

For Class VI applications, TotalAgility will trigger model-evidence review workflows and route applicant-provided or reviewer-generated model inputs, boundary conditions, assumptions, outputs, pressure/plume evidence, AoR delineation materials, and reevaluation triggers to the Agency's reviewers and approved GIS/geoscience tools for validation. The solution perform reservoir simulation or CO2 plume modeling specifically when scoped and approved by the Agency. The AoR workflow will identify, record, and route potential risks within the AoR, including wells, mines, boreholes, other artificial penetrations, faults, fractures, Underground Sources of Drinking Water, sensitive receptors, and surface water bodies. For Class VI applications, the workflow will validate that computational model inputs, boundary conditions, assumptions, and delineation outputs are present, documented, and ready for technical review.

AI and GIS outputs will be assembled as recommendations and evidence packets. TotalAgility will store the GIS source layers, model outputs, risk notes, extracted parameters, map references, confidence or quality indicators, exceptions, and reviewer comments in the electronic case file. Human technical reviewers will validate the AoR and risk outputs at the mandatory HITL gate and will determine the appropriate review track. All GIS/AoR findings remain reviewer-validated evidence; no GIS output is a final determination until approved the Agency.

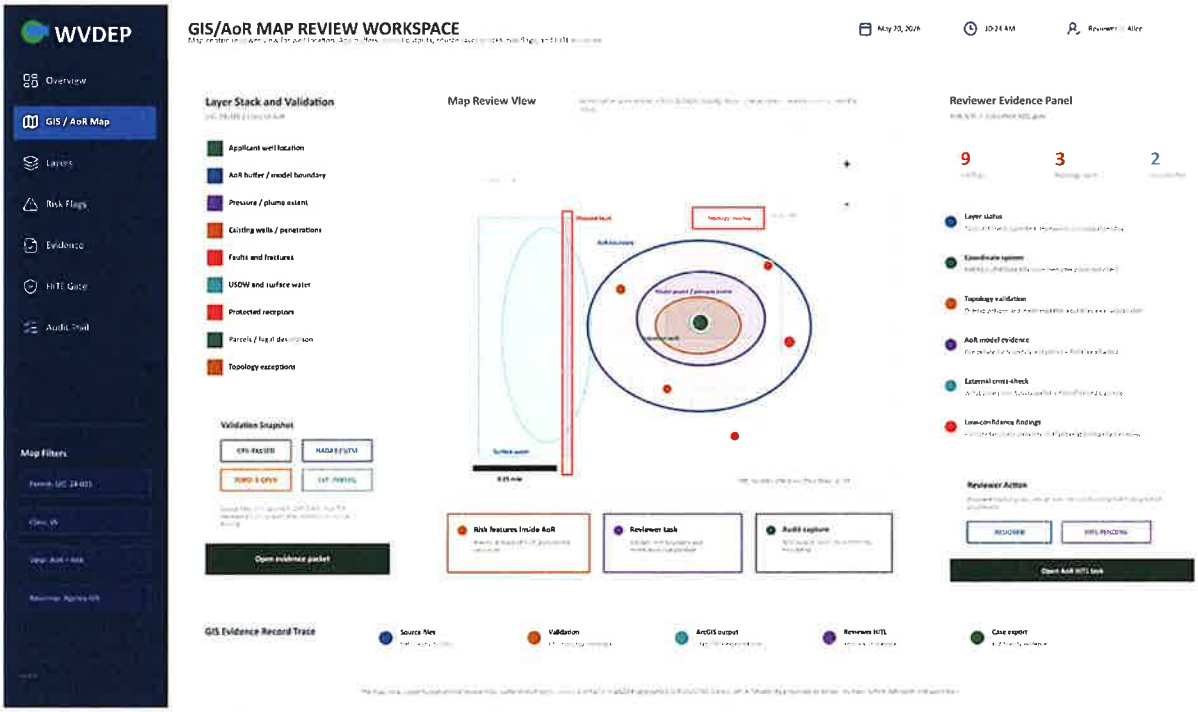


Figure 13 - Sample GIS/AoR Map Review Workspace - mockup illustrating the map-centric reviewer view showing AoR boundaries, model and plume evidence, wells and risk features, topology exceptions, validation status, external-source checks, and HITL reviewer action

4.3.2.3.2 Data Integration & Correlation

Infocap will configure TotalAgility to correlate applicant-submitted information with external and Agency data sources using access methods that reflect how each source is realistically available to the Agency (for example, public web access, approved APIs and web services where exposed, secure file exchange, scheduled imports from Agency systems, downloads from public web portals, and manual upload or discovery where only human-driven access is permitted). The table below summarizes anticipated data sources, primary access modes, and how the platform will use each source for external-data validation, AoR and risk assessment, and technical review.

For each spatial or regulatory data source, the access mode will be confirmed during discovery and documented as API, ArcGIS service, database view, scheduled file export, public portal download, secure file import, reviewer upload, or manual reference. TotalAgility will not assume that every source exposes a direct API or automated data feed. Where direct access is unavailable, incomplete, or not authorized, the system will record the access limitation, route the item for reviewer validation, and preserve the fallback method in the GIS evidence record. It will support property, plat, and pore-space review by linking applicant-provided legal descriptions, surface ownership tracts, courthouse plats, parcel records, and related GIS layers to the case file. Potential property, plat, pore-space, mineral rights, or legal-rights conflicts will be flagged for the Agency's reviewer or legal validation and will not constitute automated legal determinations.

Where a listed source does not expose an approved API, data feed, or direct system connection, Infocap's solution will rely on the next authorized access mode identified in the matrix (such as public-portal retrieval, secure file exchange, scheduled imports, or reviewer upload), and TotalAgility will flag the source, capture the exception path, and route the case for HITL validation under the same audit and security controls as other data-correlation activities. All property, plat, pore-space, mineral rights, and legal-rights checks performed by the platform are advisory screening and evidence-organization functions only. TotalAgility will identify potential inconsistencies, missing documentation, overlapping records, or conflict indicators and route them to the Agency's reviewers or legal reviewers for validation. The system will not make automated ownership, legal-rights, pore-space, mineral rights, or permit-conflict determinations.

Where a listed source does not expose an approved API, data feed, or direct system connection, TotalAgility will use the next authorized access method identified in the matrix, such as secure file exchange, public portal retrieval, batch import, reviewer upload, or manual evidence capture. The solution will not assume direct automated access to every source. Each source usage, exception path, reviewer validation, and resulting decision will be captured in the electronic case file and audit record. No GIS, AI, or TotalAgility workflow output will be automatically written back to ESS or any other legacy permitting system. GIS findings, reviewer outputs, spatial validation results, and audit records will be preserved in the electronic case file and included in approved evidence or export packages. Legacy system updates based on GIS or AoR evidence will occur only through authorized human-mediated processes, governed RPA assistance where approved, and applicable reviewer approval and audit controls described in §4.3.2.7.

Existing or historical permit records will be used only where provided by the Agency or publicly available and applicable to the review context. Our proposed solution does not assume the existence of WV Class I or Class VI historical UIC records unless such records are supplied, identified, or authorized by the Agency during discovery.

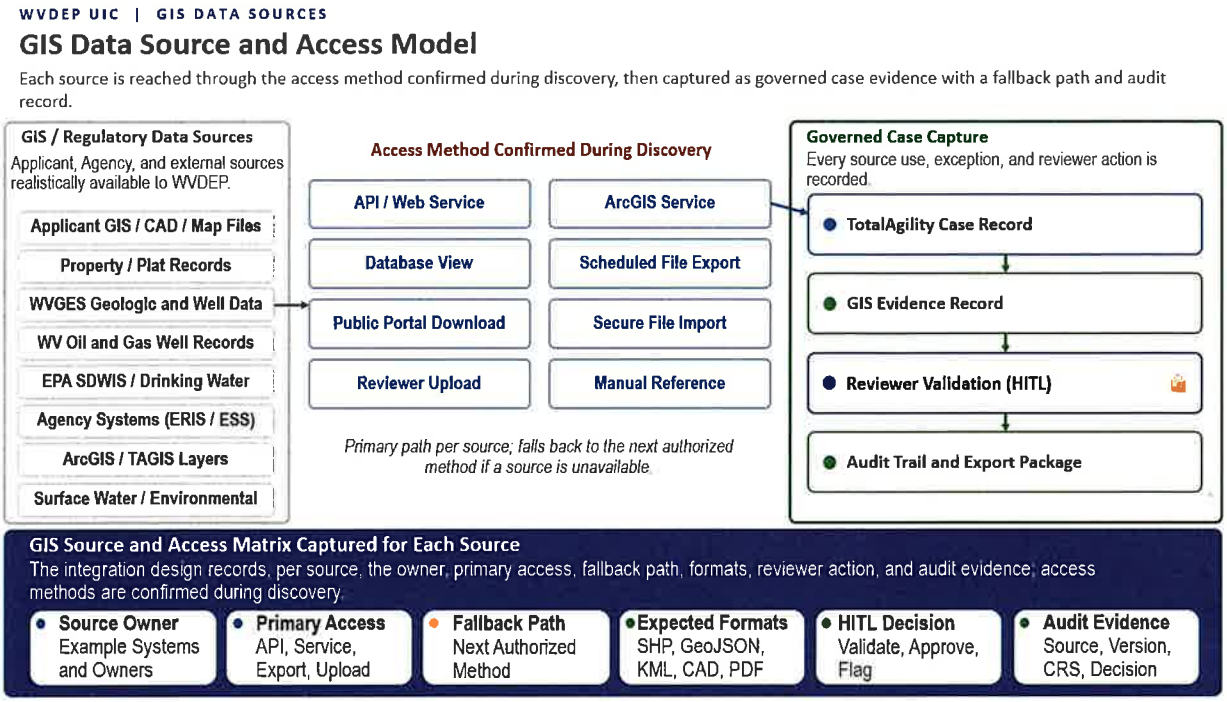


Figure 14 - GIS Data Source and Access Model - anticipated data sources, primary access modes, and how TotalAgility uses each source for external-data validation, AoR and risk assessment, and technical review

4.3.2.3.3 GIS Evidence Record and AoR HITL Review

TotalAgility will maintain a GIS Evidence Record for each UIC case to preserve the source, processing history, reviewer validation, and audit trail for GIS and AoR-related findings. The GIS Evidence Record will link applicant-submitted GIS materials, Agency-approved GIS outputs, external source checks, reviewer-generated maps, validation results, and AoR findings to the electronic case file.

Each GIS/AoR finding will preserve the source file or layer, source system, upload or import date, coordinate system, transformation method, feature ID, extracted attributes, spatial operation, validation checks, risk flag, confidence or quality indicator where applicable, reviewer action, reviewer comments, override rationale, timestamp, version, and final disposition. This evidence record will support technical review, draft permit preparation, public record development, audit review, and export package generation.

The AoR and Risk Validation HITL gate will require the Agency's technical review of GIS files, source layers, map outputs, topology exceptions, coordinate-system transformations, external-source matches, risk-feature flags, and Class I/Class VI AoR evidence before the workflow proceeds to technical analysis approval. AI/GIS-generated findings will remain recommendations and evidence packets until reviewed and approved, revised, rejected, or returned for additional analysis by authorized Agency personnel.

GIS reviewer tasks will display the submitted spatial files, detected format, detected CRS, target CRS, transformation result, topology checks, source-layer references, external-source cross-checks, mapped risk features, Class I buffer evidence, Class VI model-evidence materials, reviewer notes, confidence or quality indicators where available, and recommended next actions.

Reviewers will be able to approve the finding, revise the finding, reject the finding, override the AI/GIS recommendation, request additional applicant information, route the case to a technical SME, or return the case for additional GIS analysis.

Each reviewer action will be recorded with reviewer identity, timestamp, decision, comments, rationale, related source evidence, and workflow disposition. Reviewer overrides will be preserved as part of the case audit record and will be available for supervisory review, quality control, legal defensibility, and future process improvement.

4.3.2.4 Document Processing and AI Drafting

TotalAgility will provide the document processing and AI-assisted drafting foundation for the UIC e-permitting solution. The platform will convert submitted permit materials into structured, review-ready case evidence through intelligent document processing, OCR, image processing, classification, trainable document separation, unstructured extraction, table extraction, key-value extraction, NLP, Knowledge Discovery, GenAI activities, document generation, templates, workflows, review gates, and audit trails.

Infocap's solution will use AI to accelerate (but not replace) regulated drafting and review. AI-assisted services will support summarization, issue identification, comment categorization, evidence-backed narrative development, and preparation of draft Notices of Deficiency, permit language, public notices, response-to-comments materials, technical-review summaries, and final decision-support documents. Where applicable, TotalAgility will also support template-driven document creation and Tungsten Communications Manager integration.

Every AI-generated document will remain a draft work product until approved by authorized Agency staff. TotalAgility workflow will route each draft through the appropriate human review, validation, approval, and audit steps, ensuring that regulatory communications and final documents remain under Agency control. This approach gives reviewers faster, source-grounded drafting support while preserving human judgment, regulatory accountability, and a complete decision record.

4.3.2.4.1 Engineering "Blueprint" Vision Agents

Infocap will implement a specialized Blueprint Vision Agent family for engineering schematics, well construction diagrams, CAD drawings, shapefile/GIS overlays, maps, and technical drawing materials. This agent family will combine TotalAgility imaging, OCR, table extraction, unstructured extraction, computer-vision locators, Azure Document Intelligence/Computer Vision where configured, and integrated CAD/GIS/engineering drawing services.

The Blueprint Vision Agent family will extract or validate technical data such as casing depths, cement thickness, tubing and packer placement, well construction diagrams, wellbore schematics, drawing metadata, shapefile/GIS overlay metadata, map annotations, compliance-relevant dimensions, and construction-related labels. Extracted data will be normalized into structured fields, compared against application forms, technical narratives, tables, and regulatory criteria, flagged for exceptions, and routed to the Agency technical reviewers.

When specialized interpretation or engineering drawing validation requires an external tool or SME-authored model, TotalAgility will orchestrate the external service call and preserve the inputs, outputs, source files, model/service version, extracted values, exception notes, and reviewer actions in the UIC case file.

Extracted maps, CAD-derived PDFs, well diagrams, GIS-related drawings, cross-sections, stratigraphic diagrams, and well-location exhibits will be linked to the GIS Evidence Record described in §4.3.2.3.3 so that each reviewer-visible spatial finding retains its source document or layer reference, validation result, reviewer action, and audit trail before it is used in technical findings, AoR conclusions, draft permit conditions, or final decision-support materials.

Vision Agents That Read the Drawings

- ✓ Computer Vision agents trained on engineering schematics and CAD drawings
- ✓ Extracts casing depths, cement thickness, and tubing packer placement from diagrams
- ✓ Verifies construction and design details against regulatory standards
- ✓ Extracted findings remain advisory pending engineering review

4.3.2.4.2 AI Draft Generation

TotalAgility will support AI draft generation using the WVDEP/WVOT-approved templates, standard clauses, structured case data, reviewer-approved findings, RAG-grounded source references, and approved permit language. The draft generation workflow will use GenAI activities and worker agents to assemble formatted draft materials while preserving source grounding and human review requirements.

Draft permits will follow the Agency standard templates and include Facility Information, Well Construction Requirements, Operating Requirements, maximum injection pressure, rate and volume limitations, Monitoring and Reporting Requirements, Plugging and Abandonment Requirements, and General Conditions. For Class VI permits, the drafting workflow will include approved AoR with reevaluation schedule, corrective action requirements, CO2 stream specifications, Testing and Monitoring Plan conditions, Emergency Response requirements, and Post-Injection Site Care requirements. Reflection and validation agents will review draft outputs for consistency, completeness, source support, template compliance, terminology, missing conditions, and internal contradictions. TotalAgility will route drafts through the Draft Permit Approval HITL gate before documents are locked for public comment, distribution, or issuance.

4.3.2.4.3 Completeness Determination

TotalAgility will determine application completeness using document sets, document rules, checklist variables, extracted fields, validation workflows, RAG-supported checklists, and human review gates. The system will evaluate documents submitted via e-form and attachment-based application sections against Class I and Class VI regulatory checklists.

For Class I applications, the completeness workflow will check EPA Form 7520-6, geologic data, well construction details, casing and cementing programs, injection zone information, confining zone information, AoR calculations, operating parameters, injection fluid characterization, maps, legal descriptions, operator information, and required certifications. For Class VI applications, the workflow will check site characterization, detailed geologic characterization, AoR modeling, operational plans, Testing and Monitoring Plan, Injection Well Plugging Plan, PISC Plan, Emergency and Remedial Response Plan, Financial Responsibility

documentation, corrective action information, public notice materials, and required signatures and certification statements.

Completeness determinations will be structured as review-ready findings, not final autonomous actions. Missing, inconsistent, unreadable, unsigned, or low-confidence items will be routed to the appropriate the Agency reviewer queue. The Pre-NoD HITL gate will ensure the Agency staff verify missing or insufficient items before a Notice of Deficiency is finalized or sent.

4.3.2.4.4 Notice of Deficiency Generation

When deficiencies are identified, TotalAgility will generate a draft Notice of Deficiency email or letter for the Agency review and approval. The draft NoD will specify exactly which items are missing, incomplete, inconsistent, unreadable, unsigned, unsupported, or insufficient. Each deficiency item will include the related checklist item, regulatory/SOP basis where available, source document reference, extracted field or document-status evidence, and recommended applicant response.

The NoD drafting workflow will use structured case data, checklist results, Knowledge Discovery source references, standard the Agency language, and approved templates. A reflection/validation agent will check the draft for completeness, clarity, source support, and consistency with the case record. The NoD will be held at the Pre-NoD Review HITL gate. After a Notice of Deficiency, the system will ingest corrected versions and cover sheets, identify changed sections, and route changes for reviewer validation. TotalAgility will not transmit or finalize the NoD until authorized the Agency staff approve it.

4.3.2.4.5 Public Notice Document Generation

TotalAgility will generate draft public notice documents and fact sheets compliant with 40 CFR 124 and applicable state requirements. The workflow will use the Agency templates, structured case data, permit conditions, RAG-grounded source material, recipient lists, publication rules, and calendar/deadline logic. The system will calculate comment period deadlines, including a 30-day minimum and 45 days for Class VI where required by the CRFP.

Draft public notice packages will include fact sheets summarizing the permit application, proposed activity, facility and well information, review status, public comment instructions, recipient lists, deadlines, and relevant permit information. TotalAgility will route draft notices through human review before publication, distribution, or posting. Publication and distribution will occur only after the Agency approval, and the final notice package, approval record, publication status, and deadline calculations will be preserved in the case record.

4.3.2.4.6 Response to Comments

TotalAgility will ingest, classify, categorize, and route public comments. The platform will detect duplicate, related, or campaign-style comments; identify substantive technical comments; extract key themes; identify the relevant permit condition, technical issue, or regulatory topic; and route complex comments to SMEs.

Knowledge Discovery and a regulatory response library will support draft response generation. Response agents will use the public comment text, permit record, technical findings, regulatory sources, the WVDEP/WVOT-approved standard language, and reviewer instructions to prepare

draft response support. Technical comments requiring detailed analysis will be flagged and routed to the appropriate the Agency technical reviewer.

The platform will compile a Response to Comments document formatted for public release. The response package will include comment categories, substantive issue summaries, draft responses, source references, reviewer edits, approval history, and final disposition. The response document will remain a draft until the Agency staff approve it through the workflow.

4.3.2.5 Workflow Integration

TotalAgility will provide the end-to-end workflow integration layer for the Agency's UIC e-permitting solution. TotalAgility serves as the workflow, evidence, and review-orchestration layer for the Agency's UIC e-permitting program. The platform augments the Agency's One Stop Shop Permitting Portal by converting submissions into governed electronic cases, trusted data, source-grounded AI outputs, reviewer work queues, auditable decision records, and enforceable human approval gates. The system will connect portal submissions, secure intake, document processing, case management, review queues, agentic review support, Knowledge Discovery, external GIS/scientific systems, public notice activities, response-to-comments workflows, records management, and final decision package generation. TotalAgility will coordinate automated steps, human review tasks, external service calls, RPA bots, API integrations, case notes, workflow milestones, and audit records in a single governed process.

4.3.2.5.1 Secure Submission Handling

Applications submitted through the Agency's One Stop Shop Permitting Portal, the Agency's UIC web page, or a secure agency-controlled gateway will be received or retrieved by Infocap's proposed solution and processed through TotalAgility. TotalAgility will create a unique application tracking number and electronic case file immediately upon submission. Submitted documents will be stored, normalized, classified, indexed, extracted, and tied to the case.

Security will be enforced through the proposed FedRAMP cloud controls where applicable, tenant isolation, TLS, encryption at rest, federated identity, RBAC/ACLs, secure integration patterns, and audit logging. Role-based access will control which the Agency staff, reviewers, supervisors, administrators, and integration services can view, modify, approve, or export case data. Submission status will be available to authorized by Agency users and integrated systems through controlled dashboards, work queues, case views, and system interfaces.

4.3.2.5.2 Agency Logs & Deep Observability

TotalAgility will create an agency case log and evidence record for quality control, audit, monitoring, and defensibility. The log will capture AI actions, automation actions, workflow state changes, extracted fields, source references, tool calls, reviewer comments, human approvals, overrides, errors, exceptions, escalations, retry actions, and final dispositions.

Infocap's proposed solution will use TotalAgility audit logs, job history, notes, reporting worker roles, business events, dashboards, case notes, performance statistics, package/version records, and SIEM/logging integration as the foundation for deep observability. Each electronic UIC case will maintain a traceable record of what was submitted, what was extracted, what was classified, what workflows were launched, what agents or tools were invoked, what evidence was retrieved, what drafts were generated, what reviewers changed, and approvals granted.

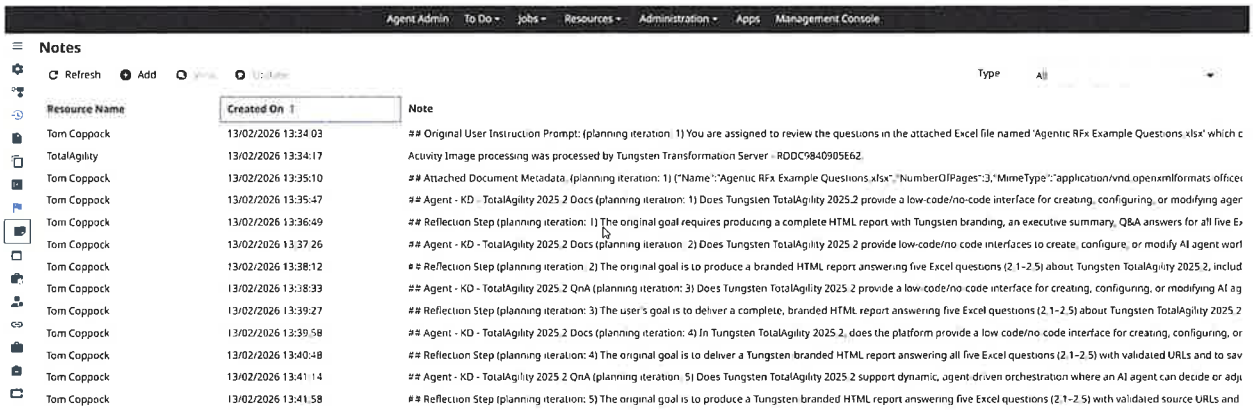


Figure 15 - TotalAgility Case Notes audit trail - full record of a multi-iteration agentic review session including original user prompt, planning iterations, Knowledge Discovery queries, reflection steps, and decision trace

All automation directions and actions will be recorded for the period meeting the Agency's retention policy, or for five years if a specific the Agency retention period is not defined. Retention configuration will be aligned with the Agency records, public information, litigation hold, appeal, and administrative record requirements.

4.3.2.5.3 AgentOps Observability

Shown in *Figure 15* above, every step by an agent will be captured, persisted, and reportable. Infocap will implement AgentOps observability through a decision trace that records observable system actions while protecting model-internal reasoning. For each AI-supported review action, TotalAgility will preserve the agent or workflow invoked, trigger, input evidence, tool or data source used, result returned, rule applied, RAG citation, confidence or relevance signal, reflection or validation outcome, exception condition, reviewer action, and final disposition.

Key HITL checkpoints, including AoR & Risk Validation, will create decision-trace records for each UIC case. For example, when an integrated GIS service identifies a mapped fault within a preliminary AoR, TotalAgility will record the GIS output, source layer, timestamp, and case association; Knowledge Discovery will retrieve the applicable rule and Agency SOP reference; the AoR Screening Agent will generate an evidence-backed risk note; and TotalAgility will route the task to the AoR & Risk Validation gate for the Agency's technical review. The reviewer's approval, revision, return for further analysis, rationale, identity, and timestamp will be recorded. AgentOps observability will also track prompt versions, model versions where applicable, tool registry version, knowledge base version, source documents, external service responses, workflow states, loop counts, escalations, failed tool calls, retry attempts, abnormal usage patterns, reflection scores, and human overrides. This provides the Agency with an audit-ready operating record for legal defensibility, regulatory oversight, quality review, and operational troubleshooting.

4.3.2.5.4 Mandatory Human-in-the-Loop (HITL) Decision Gates

TotalAgility will enforce mandatory stop points at critical regulatory milestones. At each HITL gate, TotalAgility will suspend workflow progression, notify assigned the Agency's staff through dashboards and work queues, require digital sign-off, record reviewer identity, timestamp, action, comments, and rationale, and prevent AI from autonomously issuing, denying, or finalizing a permit.

AoR and Risk Validation HITL tasks will include related GIS Evidence Records, source layers, CRS/topology validation results, AoR calculations, risk-feature flags, reviewer-imported GIS outputs, AI-generated summaries, reviewer decision fields, and override-rationale fields. GIS services will produce evidence; the Agency's reviewers will validate the findings.

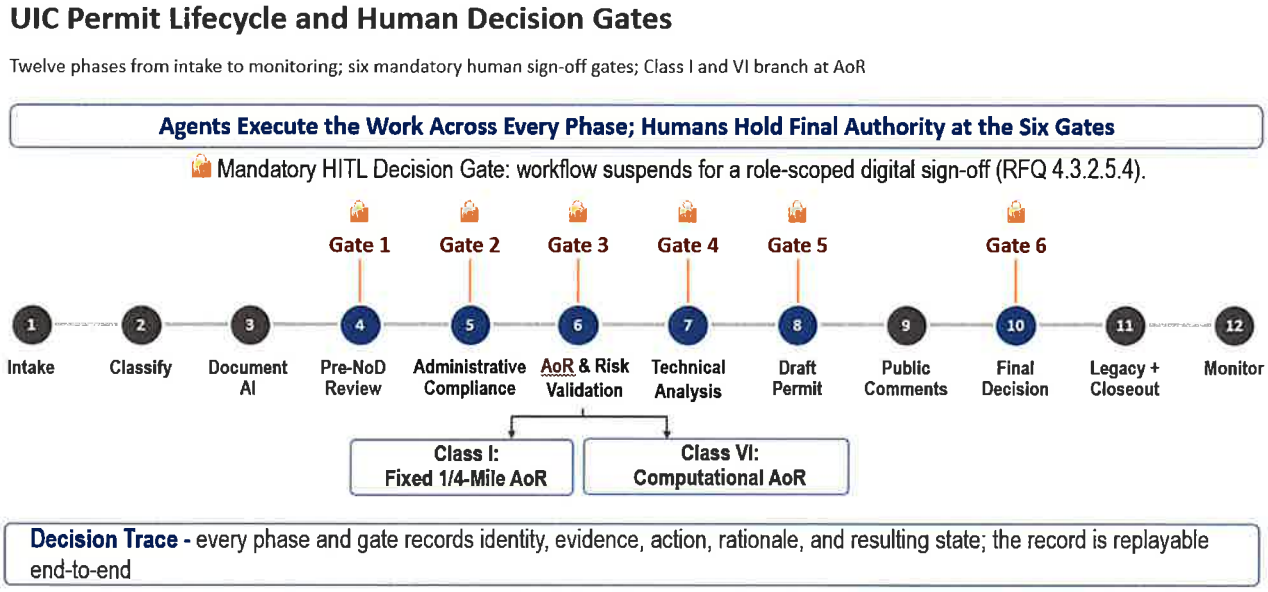


Figure 16 - UIC Permit Lifecycle and Human Decision Gates - twelve phases from intake to monitoring; six mandatory human sign-off gates; Class I and Class VI branch at AoR

HITL Milestone	Trigger Conditions	TotalAgility Actions/Outcomes
1. Pre-NoD Review (Administrative Completeness)	Application intake complete; all required documents checked; missing or insufficient items identified by the Digital Intake Specialist and completeness workflow	Records reviewer identity, timestamp, action, and rationale
2. Administrative Compliance Approval	Fees verified; ownership, pore-space, plat, and legal-description evidence cross-checked and routed for reviewer/legal validation where required; public notice requirements identified; administrative checklist completed	Suspends progression until digital sign-off is recorded
3. AoR & Risk Validation (Technical Screening)	Initial technical parameters extracted; AoR delineated; spatial risk assessment complete; GIS/model outputs attached to case	Records the evidence packet, reviewer decision, and required follow-up actions
4. Technical Analysis Approval	Full technical review complete; corrective action needs identified; proposed permit conditions and technical findings prepared	Preserves all findings, source references, reviewer edits, and approvals
5. Draft Permit Approval	Draft permit document generated with all applicable conditions, source references, and reviewer-approved findings	Records approval, revision, rejection, or return-for-rework decisions
6. Final Decision	Public comment period complete; response to comments prepared; final decision package assembled	Records the final decision action, administrator identity, timestamp, supporting record, and final package disposition

Table 2 - Mandatory Human-in-the-Loop Decision Gates - trigger conditions and required reviewer actions for each of the six HITL milestones governing the UIC permit review lifecycle

4.3.2.6 AI Token Usage and Cost Management

Infocap will make AI token consumption transparent, predictable, and controlled by using TotalAgility's workflow, document intelligence, business rules, RAG/Knowledge Discovery, HITL gates, and governance controls before invoking GenAI. Our proposed solution will not use a generic "LLM does everything" architecture. Instead, TotalAgility will serve as the workflow-based agentic AI and automation platform that orchestrates document processing, case management, deterministic routing, knowledge retrieval, governed agents, human review, and auditability. TotalAgility's Case Agents view will report tokens used for each case and agent run, giving the Agency per-case visibility into consumption alongside the model, iteration count, status, and output.

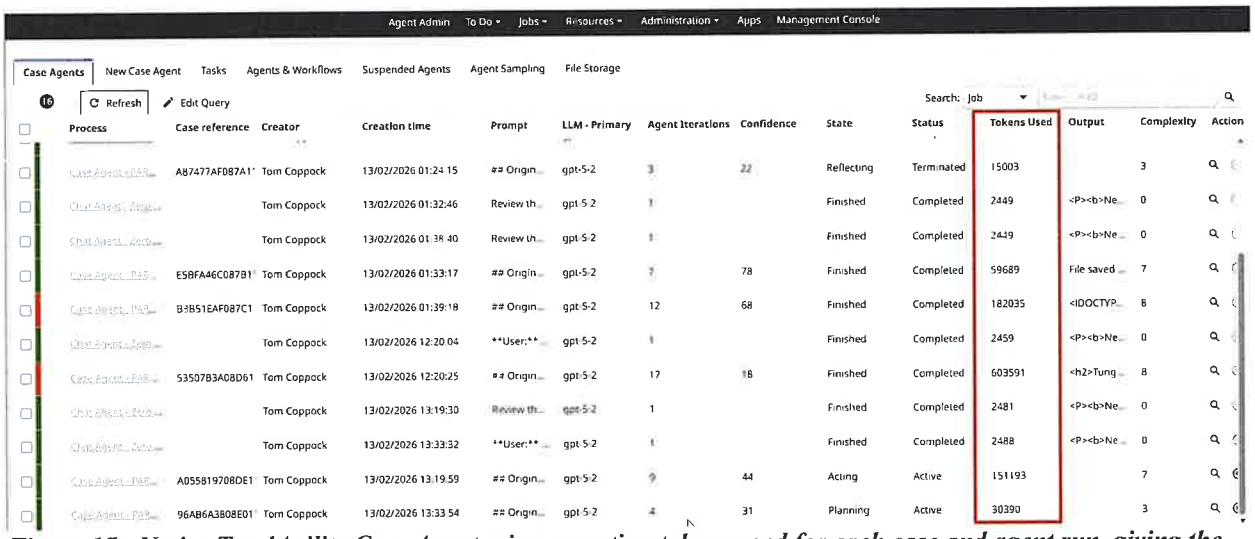


Figure 17 - Native TotalAgility Case Agents view reporting tokens used for each case and agent run, giving the Agency per-case visibility into consumption alongside model, iteration count, status, and output

This approach reduces token exposure because the system does not repeatedly send entire permit packages, maps, technical plans, public comments, or correspondence into a foundation model. TotalAgility performs high-volume processing through purpose-built platform capabilities, including OCR, ICR, document classification, document separation, field and table extraction, validation, HITL review, sampling/checking, audit trails, and model governance. GenAI is reserved for bounded tasks where reasoning, summarization, explanation, or drafting adds value.

For the Agency, known permitting logic such as intake routing, case creation, review assignment, completeness status, approval gates, public notice workflow, review handoffs, and case closeout will be handled through deterministic workflows and configured review processes. LLM use will be applied selectively for high-value tasks such as targeted Q&A, evidence-grounded summaries, deficiency draft assistance, public comment response support, and technical or administrative review drafting. This balances cost, quality, auditability, operational efficiency, and regulatory control. All token-consuming AI services, model endpoints, prompt processing, retrieval services, logging, and token reporting will operate within a FedRAMP Moderate-or-better authorized boundary accepted by the Agency. Model flexibility will be limited to models, endpoints, and providers approved by the Agency and operating within the required authorized boundary.

CRFP Requirement	Infocap Response	Response Reference
"AI Token Usage (1 EA = 1 Million Tokens/MTOK)" with quantity "250.00000" EA.	TotalAgility Enterprise includes 6.25B annual Tungsten-managed LLM tokens. This satisfies the CRFP-evaluated 250 MTOK allocation.	4.3.2.6.1; Cost Proposal, Attachment A, Item 11
"The Vendor shall clearly describe how token costs are structured within their pricing proposal."	The response separates platform subscription, implementation services, included token capacity, and metered MTOK pricing. The required unit price and extended cost are provided in Attachment A.	4.3.2.6.1; Cost Proposal, Attachment A, Item 11
"The unit price per token (per million tokens/EA) established in the vendor's proposal shall remain firm-fixed for the entire life of the contract, including any optional renewal periods."	Infocap's MTOK unit rate remains firm-fixed for the contract term, optional renewal periods, and approved token-capacity increases.	4.3.2.6.7; Cost Proposal, Attachment A, Item 11
"The Vendor shall describe mechanisms to ensure cost predictability for the Agency."	Our proposed solution provides token monitoring, near-real-time visibility, threshold alerts, configurable caps, role-based permissions, and approval gates.	4.3.2.6.2
"The Vendor shall describe technical approaches used to minimize token consumption while maintaining output quality."	Infocap minimizes token use through workflow-first routing, IDP/OCR before GenAI, deterministic rules, targeted RAG, model routing, structured data reuse, selective reflection, and HITL escalation.	4.3.2.6.3
"Based on the estimated volumetrics provided in Section 1.3, the Vendor shall provide estimated token consumption. See Attachment B."	Infocap estimates token usage using CRFP volumetrics, CRFP Attachment B, the 250 MTOK evaluated allocation, RAG query patterns, drafting events, reflection passes, and implementation benchmarks.	4.3.2.6.4; Cost Proposal, Attachment B
"The Vendor shall provide robust token usage monitoring and reporting capabilities."	Our proposed solution provides token and AI usage reporting by case, workflow, user, document, document type, AI model, knowledge base, and reporting period where supported.	4.3.2.6.5
"The Vendor shall describe how the solution accommodates evolving AI capabilities and cost structures."	Our proposed solution will include WVDEP/WVOT-approved models, endpoints, and providers within the required authorized boundary. External, BYOK, custom, or out-of-bundle AI services require Agency approval.	4.3.2.6.6
"The Vendor shall describe contractual commitments regarding token costs over the life of the contract."	Infocap provides firm-fixed MTOK pricing, approval controls for token-capacity increases, and governance controls to prevent uncontrolled token overages.	4.3.2.6.7; Cost Proposal, Attachment A, Item 11

Table 3 - Token Requirements Compliance Summary - CRFP and Addendum #1 token requirements mapped to our proposed solution response and applicable proposal section

4.3.2.6.1 Token Cost Pricing Model

The Cost Proposal will price the CRFP-required AI Token Usage line item of 250 MTOK, where each MTOK equals one million tokens. Infocap will provide the firm-fixed MTOK unit rate in

the Cost Proposal and will use that rate for the CRFP-evaluated 250 MTOK and any approved token capacity increases, subject to final commercial terms.

The proposed TotalAgility Enterprise configuration includes an annual LLM token allocation of 6.25 billion tokens for Tungsten-managed AI capabilities. Because the CRFP-evaluated AI Token Usage line item is 250 MTOK, or 250 million tokens, the evaluated quantity is expected to be well within the included annual allocation under the proposed usage pattern. This provides the Agency with substantial token headroom while preserving cost predictability for bounded GenAI, Knowledge Discovery, drafting, summarization, and review-support use cases.

This included-token model supports predictable AI economics by allowing Infocap to reserve token-consuming activities for high-value tasks while relying on TotalAgility workflow, document intelligence, business rules, RPA, and HITL controls for functions that do not require GenAI. If the Agency elects to use external providers, customer-provided endpoints, BYOK model access, custom LLMs, or out-of-bundle AI services, those costs will be governed by the applicable approved pricing model and will not be enabled without the Agency approval.

4.3.2.6.2 Cost Predictability and Budget Controls

Infocap's approach is to make token consumption governed by process design, not ad hoc user prompting. The Agency's users will interact with guided workflows, role-based queues, structured review tasks, controlled agents, and approved forms rather than manually constructing prompts against large permit records.

Cost predictability will be supported through a workflow-first architecture. TotalAgility will use deterministic workflows and configurable business rules to determine when an LLM call is allowed, when a document-intelligence or workflow step is sufficient, and when human escalation is more efficient or required.

Token Optimization By Design

- ✓ Leverage platform capabilities before calling GenAI services
- ✓ Apply rules before reasoning
- ✓ Limit loops; escalate to humans

The solution will support token monitoring, near-real-time usage visibility, threshold alerts, and configurable caps to prevent unapproved overages. Token usage will be managed through workflow controls, model routing, RAG targeting, prompt templates, output limits, role-based permissions, and approval gates. Administrators will be able to monitor consumption against the contracted allocation and establish alert thresholds before usage reaches defined limits. If the contracted token allocation is exhausted, token-consuming AI functions will pause and notify the administrator, while non-token workflow, IDP, OCR, RPA, HITL, case management, and export functions will continue where technically supported.

Agentic workflows will also include loop limits and escalation conditions. Planning, reflection, and tool-use patterns will be configured so agents cannot continue consuming tokens without control. When a task is ambiguous, repeatedly failing, low-confidence, legally significant, or better handled by an Agency reviewer, the system will escalate to HITL review rather than continuing to spend tokens in an uncontrolled attempt to resolve the issue autonomously.

4.3.2.6.3 Token Optimization Strategies

Infocap will minimize token consumption while maintaining review quality through the following strategies.

Workflow-first routing. Known review logic will be handled through TotalAgility workflows, business rules, work queues, and HITL gates. LLMs will not be used for deterministic workflow state changes, approvals, deadlines, case routing, or basic checklist progression.

IDP/OCR before GenAI. Document intelligence services will perform high-volume intake work before any GenAI call is made. Incoming forms, technical plans, maps, reports, certifications, public comments, et al., will be classified, separated, OCRed, extracted, validated, and routed through TotalAgility. This reduces the need to send full documents into prompts.

Deterministic rules for known permitting logic. UIC permitting contains repeatable process steps that do not require an LLM. Intake routing, case creation, required attachment tracking, review assignments, deficiency workflow, public notice workflow, notifications, escalations, and case closeout will be handled through configured rules and workflows.

Targeted RAG/Knowledge Discovery. Enforced by hierarchical RAG, only the most relevant regulations, SOPs, templates, or source references will be retrieved for a given task. This avoids sending entire permit packages, regulations, and technical appendices into each prompt.

Case-specific knowledge access. Case-specific knowledge will be available to support active review and decision support, decision records, and final artifacts will be persisted through the approved archive architecture and made available to the active workflow as needed.

Tool and semantic intent routing. TotalAgility agentic design patterns support worker agents, managing/case agents, tool-use patterns, tool registries, semantic intent routing, and MCP-enabled tool access. This allows the workflow to route a request to the appropriate deterministic process, extraction model, knowledge base, RPA bot, API, GIS integration, reviewer queue, or drafting agent without presenting every possible tool to the model in every prompt.

Right model for the task. Infocap will use the smallest reliable model, rule system, or execution component for each task. Traditional machine learning, deterministic rules, OCR, table extraction, computer vision, RPA, APIs, and human review will be used when no LLM is required. Lower-cost models may support simple formatting or summarization where appropriate, while higher-capability models will be reserved for complex regulatory reasoning, high-risk drafting support, or multi-step analysis.

Selective reflection. Reflection will be used selectively for high-risk, public-facing, or legally significant outputs, such as deficiency notices, draft permit conditions, public notices, response-to-comments drafts, and final decision summaries. Reflection will not be used for routine extraction, routing, or checklist updates unless there is a defined business justification.

Human-in-the-loop escalation. HITL escalation is both a regulatory safeguard and a token-control mechanism. The system will escalate to the Agency's reviewers when further model calls are unlikely to add value, when confidence is low, when evidence conflicts, when a task is legally significant, or when the workflow reaches a mandatory approval gate.

Reuse of structured data and prior work products. Once TotalAgility has extracted applicant details, well information, permit type, form fields, required attachments, checklist status, reviewer notes, and public-comment categories, those structured data elements will be reused throughout the case lifecycle. The system will not regenerate the same information through repeated prompts unless the underlying source data changes.

Prompt and output controls. Infocap will use concise prompt templates, output schemas, output length limits, citation requirements, retrieval limits, and controlled session memory. Agents will be instructed to use retrieved evidence, structured fields, and approved case data rather than re-reading full source documents.

Periodic optimization reviews. Token optimization will include workflow-first routing, IDP/OCR before GenAI, deterministic rules for known logic, targeted RAG retrieval, prompt and output size controls, model tiering, reusable structured data, selective reflection, HITL escalation, and periodic usage reviews.

4.3.2.6.4 Estimated Token Usage

Infocap is pricing the CRFP-required 250 MTOK allocation and will manage actual consumption through reporting, caps, workflow controls, model routing, RAG targeting, and optimization reviews. The proposed TotalAgility Enterprise configuration includes an annual Tungsten-managed LLM token allocation currently understood to be 6.25 billion tokens, which is expected to provide substantial headroom above the CRFP-evaluated 250 MTOK quantity when the Agency operates within the proposed Tungsten-managed AI usage model.

The CRFP-required AI Token Usage line item is 250 MTOK, where each MTOK equals one million tokens. Infocap will estimate usage using Section 1.3 volumetrics, Attachment B, and the CRFP-evaluated 250 MTOK allocation, then refine actual usage through implementation benchmarks for RAG queries, drafting events, reflection passes, public comment volume, and case-specific retrieval.

The estimated token usage methodology will consider the following factors:

Estimate Driver	Token Impact
Number of UIC applications per year	Drives total annual AI-assisted review activity.
Average pages per application package	Drives document processing and potential RAG/query volume.
Technical attachments, maps, figures, and appendices	Drives targeted retrieval, summarization, and evidence packaging.
Administrative review tasks	Drives completeness review, deficiency analysis, and staff support.
Technical review tasks	Drives source-grounded summaries, issue spotting, and draft findings.
Public comment volume	Drives comment categorization, summarization, and draft response support.
Deficiency cycles	Drives NoD drafting and applicant-response review.
Drafting events	Drives draft permit, notice, response-to-comments, and decision package support.
Reflection passes	Drives additional token consumption for high-risk or public-facing outputs.

Case-specific retrieval	Drives Knowledge Discovery query volume.

Table 4 - Estimated Token Consumption Drivers - activities and corresponding token usage factors for the WVDEP UIC permit review workflow

Knowledge Discovery token estimates will use Tungsten-confirmed query consumption assumptions and will be refined through configuration benchmarks during implementation. Any working assumption regarding tokens per Knowledge Discovery query will be treated as an estimation input unless confirmed by Tungsten as a fixed billing unit.

The TotalAgility-based estimate is expected to be substantially lower than a native full-stack AI estimate because OCR, classification, separation, extraction, workflow routing, deterministic rules, validation, and case management consume little or no LLM tokens. In a full-stack AI architecture, each page or large document section may be repeatedly represented in prompts for classification, extraction, routing, quality assurance, drafting, and review. In the Infocap approach, TotalAgility converts content into structured fields and indexed knowledge first; Knowledge Discovery retrieves targeted context; deterministic rules govern known workflow decisions; and human escalation stops runaway loops when continued model calls are not justified.

4.3.2.6.5 Usage Transparency and Reporting

Infocap will provide the Agency with usage transparency and reporting designed to connect AI consumption to permit outcomes, not merely count tokens. Reporting will support management review of token usage, AI performance, case throughput, review cycle time, quality, risk, and human override rates.

Token and AI usage reporting will be designed to show consumption by case, permit type, workflow, agent, task, user role, document, document type, AI model, knowledge base, and reporting period, where supported by the deployed platform and governance layer. Reports will support cost governance, workload analysis, anomaly detection, optimization reviews, contract administration, and auditability.

The solution will also use workflow logs, case notes, audit trails, source references, prompt/version tracking, model/version tracking, Knowledge Discovery references, human review outcomes, sampling/checking results, and operational dashboards. Governance dashboards will monitor extraction confidence, validation exceptions, reviewer overrides, RAG failures, reflection scores, human escalations, failed tools, abnormal usage patterns, excessive planning loops, high-cost cases, and token/cost trends.

Monthly or quarterly cost-governance reviews with the Agency will evaluate whether token consumption remains within expected bands, whether model tiering is appropriate, and whether prompts, retrieval settings, workflows, or agent policies should be tuned.

4.3.2.6.6 Model Flexibility and Future-Proofing

Infocap's architecture is designed to avoid lock-in to a single foundation model, single token pricing structure, or custom full-stack AI codebase. TotalAgility separates workflow/process logic from the underlying model, enabling the Agency to use the right AI capability for each task and adapt over time as models, pricing, security requirements, and agency policies evolve.

Model flexibility will be limited to models, endpoints, and providers approved by WVDEP/WVOT and operating within the required authorized boundary. Infocap will not use public, unapproved, or out-of-boundary AI services for Agency data or workflow execution.

TotalAgility supports multiple AI configuration patterns, including Tungsten-managed AI services, Azure-hosted model services, approved OpenAI/Azure OpenAI configurations, custom LLMs, fine-tuned models, smaller language models, and custom RAG/chat implementations where approved and configured. This allows Infocap to use deterministic or traditional ML approaches when no LLM is required, smaller or lower-cost models for lower-risk tasks, and higher-capability models only for complex regulatory, technical, or public-facing drafting support.

Before production changes are made, prompts, workflows, extraction models, RAG configurations, knowledge bases, decision rules, and model routing policies will be tested, versioned, reviewed, and approved through the governance process.

4.3.2.6.7 Cost Guarantees and Contractual Protections

Infocap will define token-related costs in the pricing schedule and tie them to agreed volumetric assumptions, the selected TotalAgility licensing model, the selected LLM hosting option, included usage allowances, and mutually agreed contract terms. Actual pricing will be provided only in the separately sealed Cost Proposal.

Infocap will require the Agency approval before enabling new high-token workflows, new models, new external providers, new agents, or overage-producing features. Infocap will also establish alert thresholds and escalation procedures for abnormal usage, including unusual token spikes, excessive planning loops, repeated failed reflection, unexpectedly high-cost cases, or unapproved model usage.

Infocap will provide a governance process for periodic optimization of prompt templates, retrieval settings, model tiers, context limits, reflection thresholds, and workflow routing. Where commercially agreed, Infocap may offer capped usage bands, not-to-exceed token budgets, included token pools, pre-approved overage rates, or fixed-price bundles for defined volumes.

Governed AI, Protected Systems

- ✓ Governs prompts, models, retrieval, and routing
- ✓ Creates auditable decision traces, not black boxes
- ✓ Minimizes GenAI use and token spend
- ✓ Protects legacy systems with human-mediated updates

TotalAgility will serve as the active workflow, document processing, AI orchestration, and HITL case workspace. Long-term permit records, source documents, generated documents, decision traces, audit exports, and knowledge artifacts will be persisted to the Agency's designated system of record or approved archive/data layer. Infocap will maintain structured decision trace records rather than hidden model chain-of-thought. Decision traces will include prompt template IDs, model metadata, retrieved sources, extracted fields, confidence scores, validation results, reviewer actions, overrides, approvals, timestamps, and generated outputs.

Infocap's commitment is to design the Agency UIC e-permitting solution to avoid uncontrolled token consumption. By using TotalAgility's platform capabilities for document intelligence, deterministic workflow, RAG, case management, governance, human review, and model

flexibility, Infocap will minimize GenAI use while maintaining review quality, auditability, operational efficiency, and user value.

4.3.2.7 HITL Workflow Interface and Legacy System Independence

Infocap's solution preserves the Agency's existing legacy permitting systems while enabling AI-assisted UIC permit review through a standalone, governed TotalAgility workflow environment. The Agency's legacy systems remain protected from direct AI interaction because TotalAgility operates as the independent workflow, evidence, case, agentic AI, document intelligence, RPA-enabled automation, and review-orchestration layer between AI-assisted processing and systems of record.

TotalAgility serves as the workflow, evidence, and review-orchestration layer for the Agency's UIC e-permitting program. The platform augments the Agency's One Stop Shop Permitting Portal by converting submissions into governed electronic cases, trusted data, source-grounded AI outputs, reviewer work queues, auditable decision records, and enforceable human approval gates. This architecture recognizes that the Agency currently operates multiple independent, pre-AI legacy systems for permit management. These systems were developed before modern AI integration patterns, operate on independent architectures, and are not designed for direct AI interaction or autonomous automation. Infocap's solution protects those systems by ensuring that AI-generated review activity occurs inside TotalAgility, while official legacy record updates remain human-mediated, governed, and auditable.

TotalAgility will receive or retrieve UIC application submissions from the Agency's One Stop Shop Permitting Portal, the Agency's UIC web submission channel, or a secure agency-controlled gateway. It will create the electronic case record, perform document intelligence, classify and extract submission content, create AI Knowledge Bases, generate agentic review outputs, route AI-generated tasks to human reviewers, generate export packages and reviewer instructions, support human-mediated synchronization with legacy permit systems, and record the complete audit trail. The AI platform will not directly modify the Agency legacy systems or issue final agency actions.

The solution augments the One Stop Shop Portal and the Agency legacy systems rather than replacing them. This design allows the Agency to modernize UIC permit review, introduce workflow-based agentic AI, and improve reviewer productivity without destabilizing existing systems of record.

4.3.2.7.1 Standalone HITL Workflow Interface

Infocap will provide a standalone, browser-based TotalAgility HITL Workflow Interface where all AI-to-human and human-to-AI review interactions occur. The interface shall serve as the primary workspace where the Agency reviewers receive, process, validate, approve, reject, revise, escalate, and complete AI-generated requests.

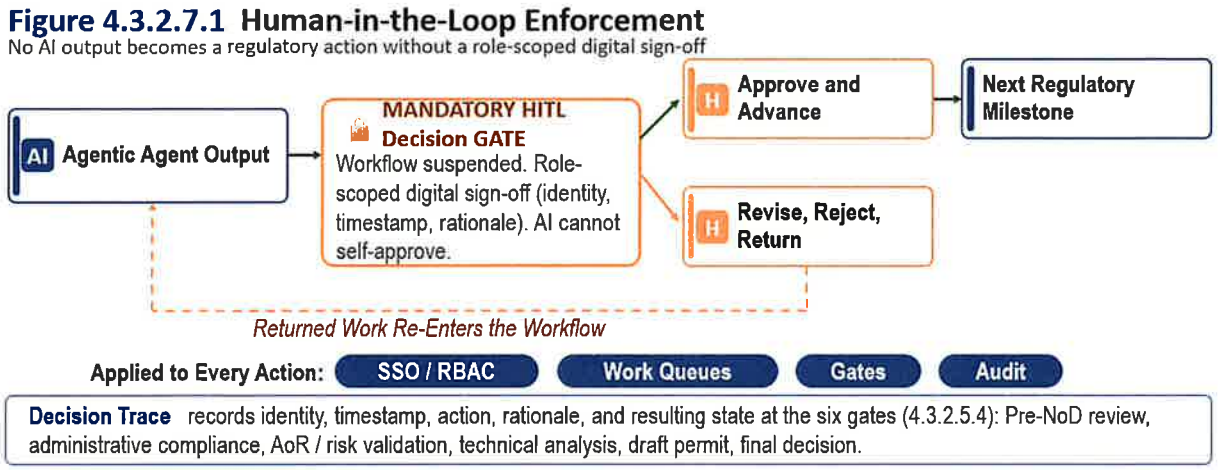


Figure 18 -Human-in-the-Loop Enforcement - no AI output becomes a regulatory action without a role-scoped digital sign-off; workflow is suspended at the gate until a human reviewer acts

The HITL Workflow Interface will be delivered through TotalAgility Workspace and configured TotalAgility forms. It will provide role-based dashboards for intake staff, administrative reviewers, technical reviewers, supervisors, public participation staff, and final decision administrators. Each role will see the tasks, cases, review queues, due dates, evidence packages, and pending decisions relevant to that user's authority and assigned responsibilities.

The interface will provide dedicated work queues for AI-generated requests, document validation tasks, administrative completeness review, deficiency review, AoR and risk validation, technical review, public notice review, response-to-comments review, draft permit review, legacy update confirmation, reconciliation exceptions, and final decision package review. TotalAgility's workflow rules, roles, milestones, SLAs, alerts, business events, and dynamic work allocation will route each task to the correct reviewer queue.

Each UIC case view will display applicant information, permit class, application tracking number, submission status, submitted documents, extracted fields, document classifications, administrative checklists, technical review checklists, milestones, deadlines, source references, Knowledge Discovery results, agent outputs, RPA retrieval results, reviewer notes, pending approvals, export packages, legacy synchronization status, and audit history.

HITL activity screens will show the reviewer the AI-generated recommendation, source evidence, document references, extracted values, relevant case data, confidence or validation indicators, RAG-grounded citations, workflow context, prior reviewer comments, available decision options, approval controls, and required rationale fields. Reviewers will approve, revise, reject, return for rework, escalate, or complete the task directly in TotalAgility. The platform will capture reviewer identity, timestamp, action, rationale, and resulting workflow state.

Digital sign-off and role-based approval gates will be enforced for regulatory milestones, including administrative deficiency review, administrative compliance approval, AoR/risk validation, technical analysis approval, draft permit approval, public notice release, response-to-comments approval, final decision package approval, and legacy update confirmation. AI-

generated content will be visibly identified as AI-assisted draft material until the Agency reviewer approves it.

The interface preserves separation from legacy systems. The Agency reviewers complete AI review activities in TotalAgility, while legacy permitting systems remain external systems of record updated through human-mediated processes. This allows the Agency reviewers to work from one governed review cockpit without requiring the AI platform to log into, traverse, directly operate, modify, or control existing legacy permitting systems.

4.3.2.7.2 AI-Generated Request Workflow

AI-generated requests will be created and routed as TotalAgility workflow objects, not as legacy system transactions. They will not directly update a legacy permit record. They will create controlled review tasks inside TotalAgility, supported by source evidence, reviewer options, audit logging, and mandatory human decision authority.

Figure 4.3.2.7.2 AI-Generated Request Lifecycle

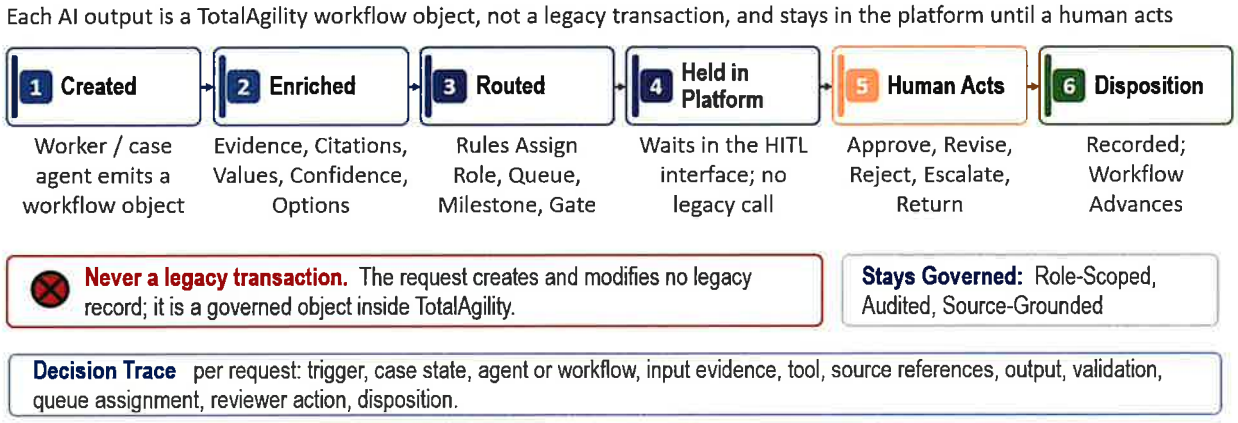


Figure 19 - AI-Generated Request Lifecycle - each AI output is a TotalAgility workflow object, not a legacy transaction, and stays in the platform until a human acts

The AI-generated request workflow will operate as follows:

1. Application intake occurs through the Agency's One Stop Shop Permitting Portal, the Agency's UIC web page, or a secure agency-controlled gateway.
2. TotalAgility receives or retrieves the submission package and creates an electronic UIC case with a unique application tracking number.
3. TotalAgility Document Intelligence classifies, separates, OCRs, extracts, validates, and normalizes submitted materials, including e-form data, PDFs, scans, attachments, tables, maps, certifications, plans, public comments, and supporting documentation.
4. TotalAgility creates or updates the case knowledge base and indexes approved case evidence, application materials, extracted data, reviewer notes, and approved reference materials.
5. Managing/case agents evaluate the case state, extracted data, document set status, RAG results, workflow milestones, business rules, and required review gates.

6. Worker agents generate task-specific outputs, including administrative completeness findings, deficiency recommendations, technical evidence summaries, RAG-supported regulatory notes, AoR evidence packets, public notice drafts, response-to-comments drafts, legacy reconciliation notes, and draft permit sections.
7. TotalAgility workflow rules convert those outputs into HITL requests assigned to the proper the Agency role, work queue, milestone, or approval gate.
8. The Agency reviewers receive those requests in the standalone HITL Workflow Interface.
9. Each AI-generated request includes source evidence, citations, document references, extracted values, workflow context, recommended action, confidence or validation indicators, required reviewer decision options, and required rationale fields.
10. The request remains inside TotalAgility until a human reviewer completes, revises, approves, rejects, escalates, or returns it for additional analysis.

TotalAgility's agentic capabilities will support this workflow through Quick AI Agents, worker/micro agents, managing/case agents, multi-agent orchestration, tool-use patterns, semantic intent routing, MCP activities, API services, RPA bots, and long-running workflows. Quick AI Agents and worker agents will perform defined tasks. Managing/case agents will coordinate multi-step reviews. Tool registries and semantic intent routing will select approved workflows, knowledge bases, tools, RPA bots, APIs, or human queues. Knowledge Discovery will ground recommendations in source evidence. MCP, API, RPA, and secure connector integrations will retrieve or prepare supporting data where authorized. Workflow rules and HITL gates will determine what happens next.

Every AI-generated request will be captured in the TotalAgility decision trace. The trace will record the trigger, case state, agent or workflow used, input evidence, tool selected, source references, output generated, validation result, reviewer queue assignment, reviewer action, and final disposition. This provides the Agency with a defensible record of how AI-assisted review tasks were created, routed, reviewed, and resolved.

4.3.2.7.3 Human-Mediated Legacy System Updates

The Agency legacy permitting systems will remain systems of record for their designated permit records unless the Agency directs otherwise. TotalAgility will maintain the AI-assisted review workspace, electronic case file, evidence record, task history, document repository, agentic review outputs, reviewer decisions, export packages, reconciliation tasks, and audit trail.

Figure 4.3.2.7.3 Legacy Update Boundary

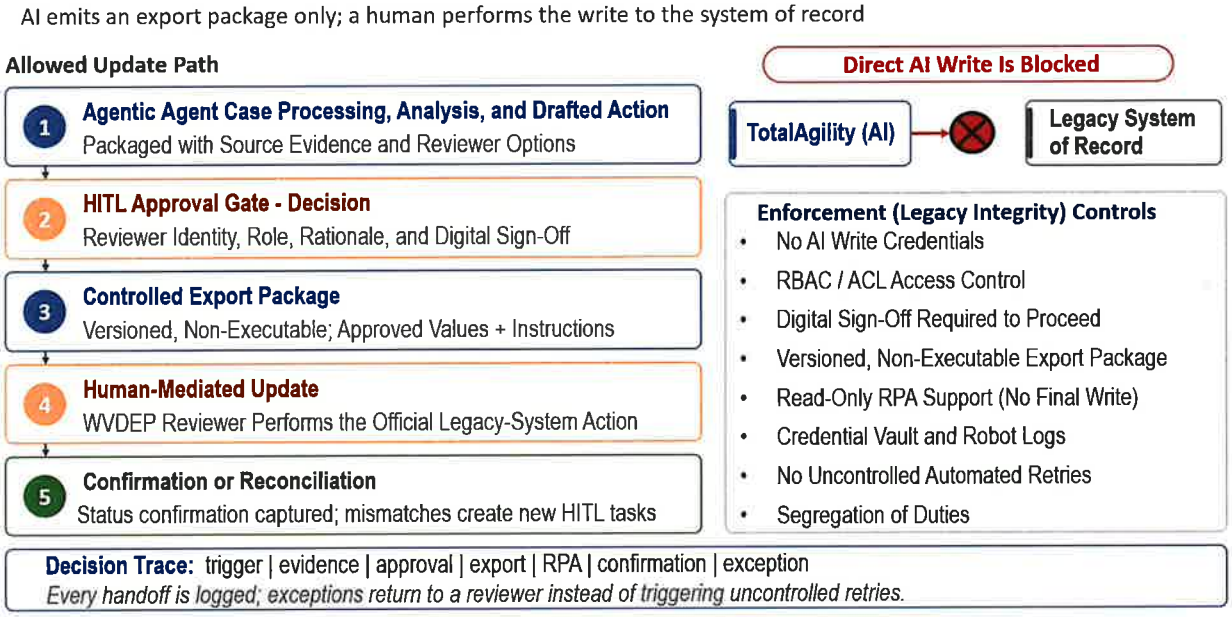


Figure 20 - Legacy Update Boundary - AI emits an export package only; a human performs the write to the system of record; five-step governed process with enforcement controls

AI-generated recommendations will not directly update legacy systems. The Agency reviewers will review and complete HITL tasks in TotalAgility first. After human approval, TotalAgility will generate an export package containing approved status updates, structured data summaries, source references, reviewer-approved findings, documents, draft or final communications, update instructions, and legacy record identifiers where available. The Agency reviewer will use the export package to manually update the associated legacy permit system and permit record.

Where the Agency approves RPA assistance, Tungsten RPA will support the human-mediated process without bypassing reviewer control. RPA bots will be orchestrated by TotalAgility as a controlled automation layer, not as uncontrolled AI agents. RPA bots will retrieve read-only reference data from legacy systems, capture screen or record information, gather status information, prepare reconciliation data, open the correct legacy screens, generate guided update aids, prefill non-final fields, prepare data-entry packets, provide screen-navigation assistance, and validate that user-entered legacy data matches the reviewer-approved TotalAgility export package.

Figure 4.3.2.7.3 Legacy Update Boundary

The only thing that crosses to the system of record is a human-carried export package

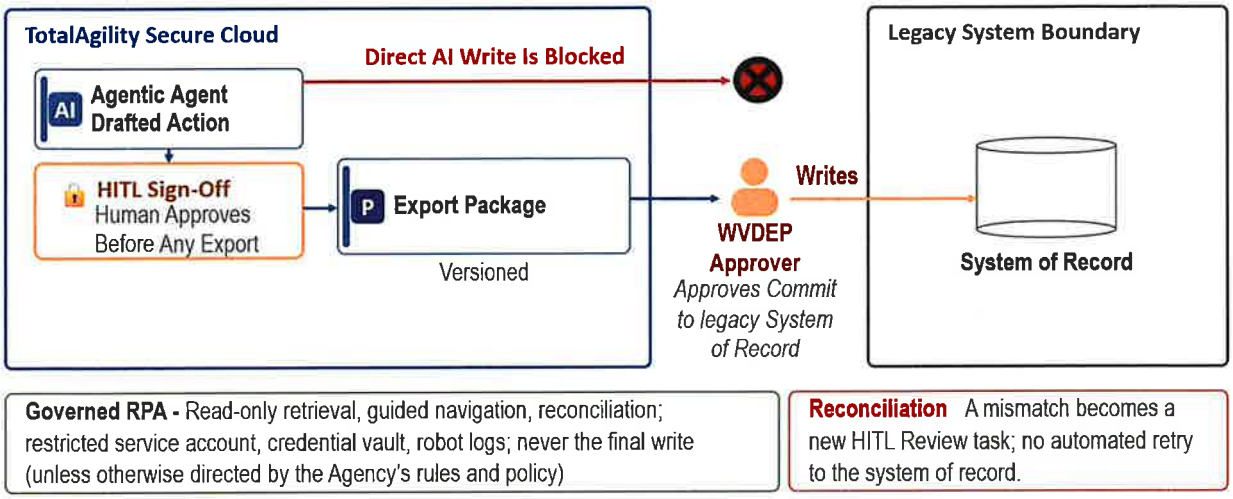


Figure 21 - Legacy Update Boundary - the only thing that crosses to the system of record is a human-carried export package; direct AI write is blocked; governed RPA provides read-only retrieval support

Final submission, save, issue, deny, or record-changing actions will remain human-controlled unless the Agency expressly authorizes a specific RPA-assisted step through governance, role permissions, credential controls, approval gates, and audit requirements. AI-generated recommendations will not directly write to, alter, or finalize legacy permitting records.

Every RPA action will be governed through TotalAgility workflow control, role-based access, restricted service accounts, credential vaulting/password store, centralized AI deployment and management, AI logs, audit trails, and workflow approval gates. TotalAgility will record the request, input, RPA action, output, reviewer approval, export package, legacy update confirmation, and synchronization status.

After a legacy system update is completed, TotalAgility will capture confirmation of the update, including reviewer identity, update date/time, legacy system name, legacy record identifier, status change, documents uploaded or referenced, data fields updated, and any exceptions. Failed, incomplete, or inconsistent updates will generate reconciliation tasks in the HITL interface rather than uncontrolled automated retries.

This model reduces risk by ensuring there no direct AI write path to legacy systems, no requirement to refactor legacy systems for AI, no disruption to existing permit records, and no uncontrolled agent access to systems of record. Human reviewers remain accountable for official permit record updates. RPA reduces reviewer burden while preserving legacy system integrity. TotalAgility provides the workflow, evidence record, reconciliation controls, and audit trail that legacy systems often lack.

4.3.2.7.4 Data Flow Architecture

A. Separation Principles

The data flow architecture is built on a clear separation model that protects the Agency's legacy systems while enabling AI-assisted review inside TotalAgility.

The Agency's One Stop Shop Permitting Portal remains the applicant-facing intake channel. TotalAgility operates as the AI-assisted workflow, evidence, and review-orchestration layer. The Agency legacy systems remain independent systems of record. AI-generated processing occurs inside TotalAgility. Legacy systems are not directly controlled by AI agents. Human reviewers mediate outbound updates. RPA is governed by TotalAgility and used for controlled retrieval, reconciliation, guided navigation, package preparation, and human-supervised legacy assistance. Every inbound and outbound handoff is logged.

Figure 4.3.2.7.4A Trust Boundaries

Layered boundaries isolate the public, WVDEP portal, the FedRAMP High cloud, controlled integration, and legacy systems

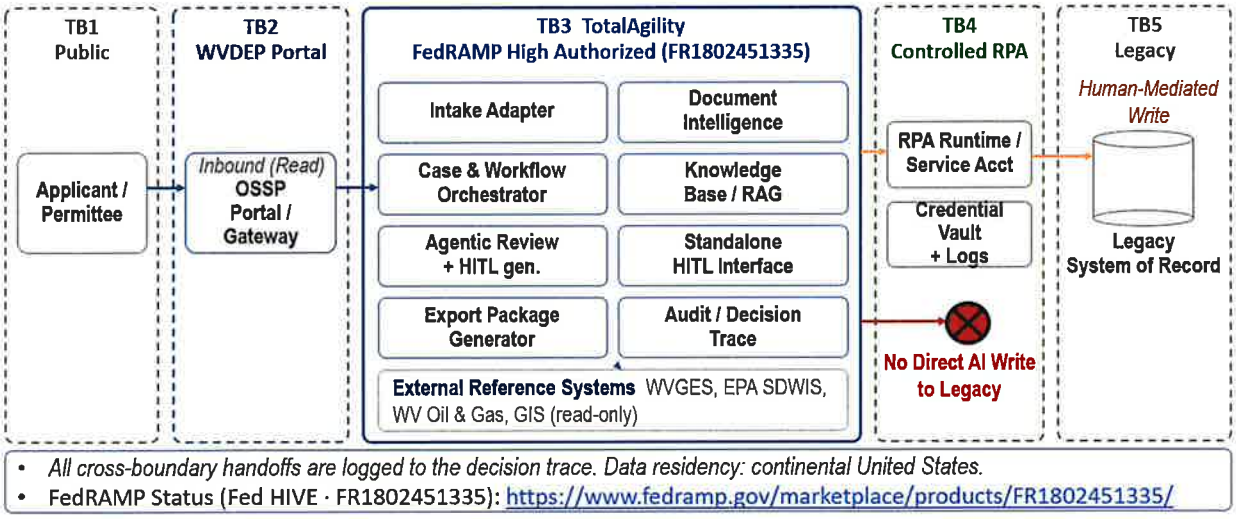


Figure 22 - Trust Boundaries (4.3.2.7.4A) - layered boundaries isolating the public, WVDEP portal, the FedRAMP High Authorized cloud (FR1802451335), controlled integration, and legacy systems; data residency: Continental United States (CONUS)

This architecture establishes a separation boundary between AI-assisted review and legacy permit systems. TotalAgility receives submissions (using a listen, event trigger, or through RPA) then creates an electronic case, processes documents, generates AI-assisted review requests, presents those requests to the Agency reviewers, creates export packages, and records synchronization outcomes. Legacy systems receive updates through human-mediated action, supported by approved export packages and governed RPA assistance where authorized.

There is no direct AI write path from the agentic AI platform to the Agency legacy permit systems. The official update path is human-mediated and audit-controlled.

B. Inbound Data Flow: Application Intake

Figure 4.3.2.7.4B Inbound Application Intake Data Flow

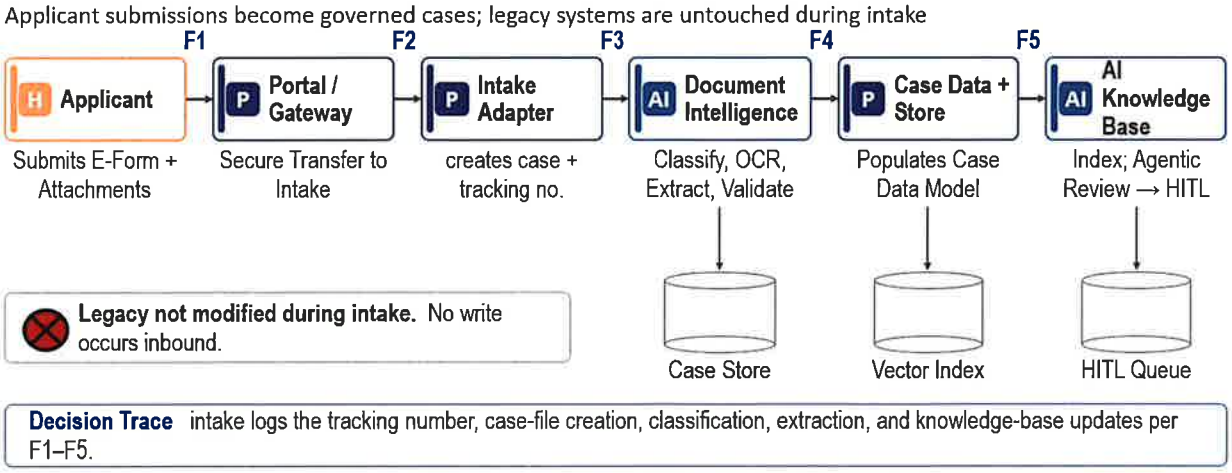


Figure 23 - Inbound Application Intake Data Flow (4.3.2.7.4B) - applicant submissions become governed cases; legacy systems are untouched during intake; flows F1 through F5

1. The applicant submits the UIC permit application through a web-based application portal, the Agency's One Stop Shop Permitting Portal, the Agency's UIC web page, or a secure agency-controlled gateway.
2. The portal or gateway transfers the e-form data, metadata, application package, and attachments to the TotalAgility intake layer through an approved secure exchange method.
3. TotalAgility assigns a unique tracking number and creates the electronic UIC case file.
4. TotalAgility stores the submission in the case document repository and applies document conversion, image processing, OCR, classification, separation, extraction, table extraction, validation, and document review workflows.
5. Extracted fields and document classifications populate the case data model, document sets, checklists, permit-type indicators, workflow variables, and reviewer task context.
6. TotalAgility creates or updates the case knowledge base with submitted materials, approved reference material, extracted case evidence, and applicable review content.
7. Managing/case agents and agent agents generate HITL requests as intake, administrative completeness, technical review, AoR, GIS screening, public notice, drafting, response-to-comments, final decision, and synchronization milestones are reached.
8. Legacy systems are not modified during inbound AI processing.
9. Where legacy reference data is required, TotalAgility retrieves it through approved read-only API, scheduled synchronization, secure connector, or RPA read operation. TotalAgility records the source, timestamp, user or service identity, retrieved values, and associated case context.

Figure 4.3.2.7.4C Outbound Update Flow

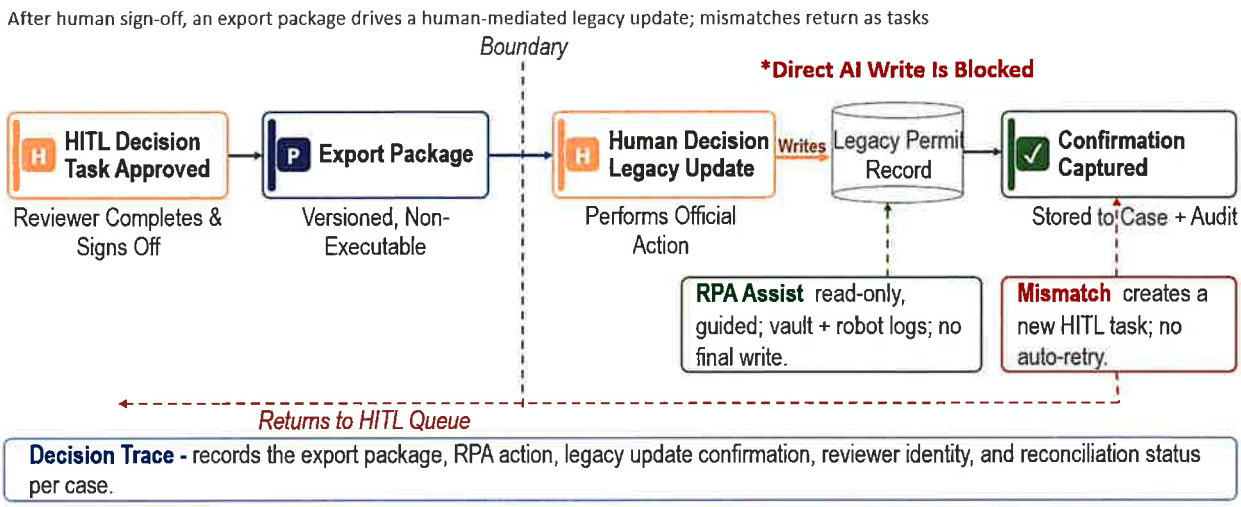


Figure 24 - Outbound Update Flow (4.3.2.7.4C) - after human sign-off, an export package drives a human-mediated legacy update; mismatches return as new HITL tasks; direct AI write is blocked

1. An Agency human reviewer receives and completes the HITL task in the TotalAgility HITL Workflow Interface.
2. The reviewer approves, revises, rejects, escalates, or returns the AI-generated request.
3. TotalAgility records the decision, reviewer identity, timestamp, comments, supporting evidence, rationale, and resulting workflow status.
4. TotalAgility generates an export package containing approved status updates, structured data summaries, documents, source references, draft or final communications, reviewer-approved findings, and legacy update instructions.
5. The reviewer manually updates the associated legacy system and permit record with the approved information from the export package.
6. Where authorized, RPA assists the reviewer by retrieving relevant legacy screens, comparing fields, pre-populating update aids, preparing data-entry packets, guiding navigation, or confirming that the legacy record matches the approved export package.
7. The reviewer records the legacy system update confirmation in TotalAgility, including legacy record identifier, update status, date/time, fields updated, documents uploaded, and exceptions.
8. TotalAgility stores the export package, update confirmation, synchronization status, and reconciliation status in the UIC case record.
9. Any mismatch between TotalAgility and the legacy record creates a reconciliation task in the HITL interface. Reconciliation exceptions require human review and do not trigger uncontrolled AI-driven legacy changes.

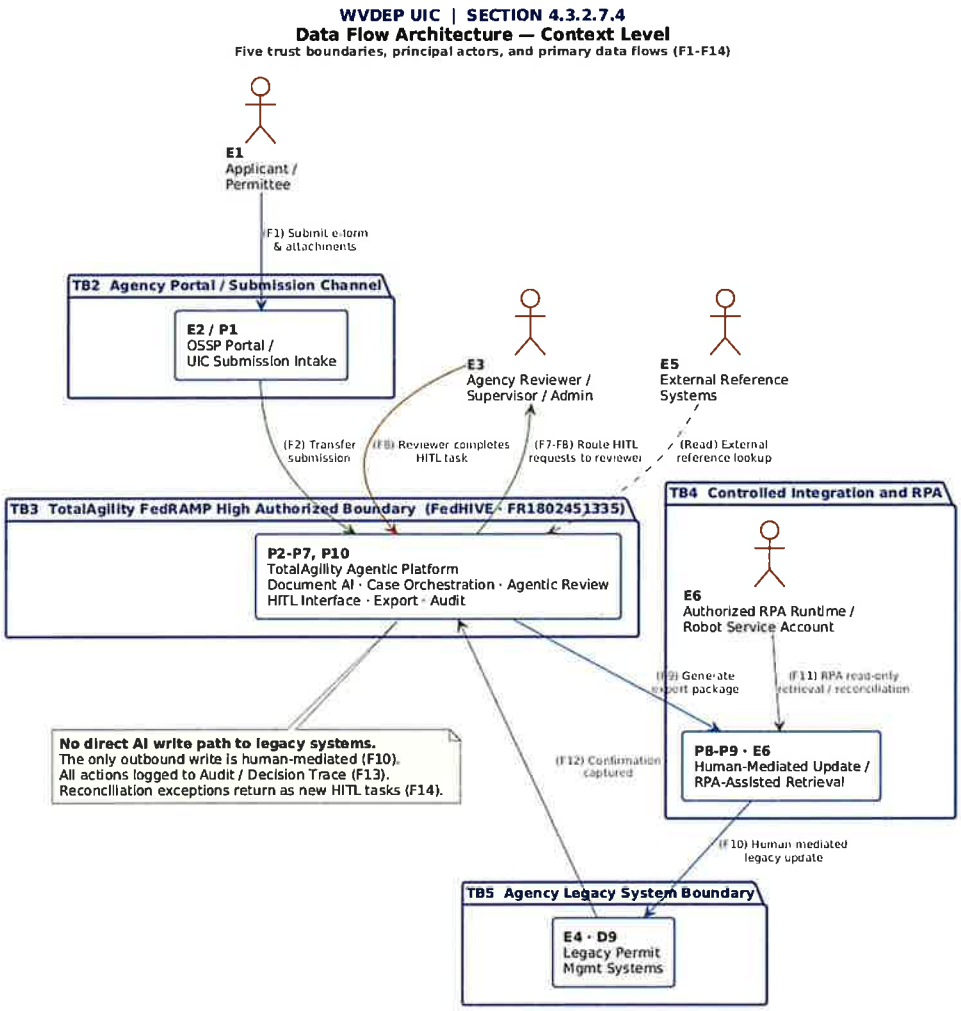


Figure 25 - Data Flow Architecture - Context Level showing trust boundaries, principal actors, and primary data flows; no direct AI write path from TotalAgility to Agency legacy systems

Infocap will implement **legacy integrity controls** that preserve the Agency's systems of record while allowing AI-assisted review to occur in TotalAgility. The solution will provide no direct AI write credentials to legacy systems. The Agency reviewer access will be role-based and governed through assigned responsibilities, work queues, approval gates, and digital sign-off. RPA service accounts will be restricted, centrally managed, and governed through credential vaulting/password store controls. Read-only retrieval will be the preferred pattern for legacy reference data. Human approval will be required before outbound packages are used for legacy updates. Each export package will include a version ID, package timestamp, case identifier, approved status updates, data summaries, document list, reviewer-approved findings, and legacy update instructions. Where implemented, checksum or equivalent package-control mechanisms will preserve package integrity. Legacy update confirmation will be captured in TotalAgility after the reviewer completes the update. Any mismatch, missing field, failed upload, inconsistent status, or unresolved discrepancy will create a reconciliation task rather than allowing uncontrolled automated retries.

The audit trail will span the complete lifecycle: intake, AI-assisted processing, document extraction, knowledge base update, HITL task generation, reviewer action, export package creation, RPA retrieval or reconciliation, legacy update confirmation, exception handling, and final disposition. Segregation of duties will be maintained between AI recommendation, human approval, and legacy record update. All synchronization activity will be retained in accordance with the Agency retention requirements, or for five years if a specific retention period is not defined. This approach preserves legacy system integrity, protects the Agency's official records, and provides a defensible operating model for AI-assisted UIC permitting.

4.3.2.7.5 Unified User Experience Across Microsoft Tools

Agency staff work through a unified experience that spans the governed TotalAgility environment and the Microsoft tools they already use every day. The platform's capabilities reach directly into those tools: a reviewer can complete HITL tasks from Microsoft Outlook, interact with agentic agents through Microsoft Teams, and exchange documents with the case file through SharePoint, with every action recording back to the TotalAgility decision trace. All review, approval, and decision activity remains governed within the standalone HITL Workflow Interface described in §4.3.2.7.1, and the final issue or deny authority is exercised there, with the complete case record and audit trail in view. The figure below shows this in operation. A user submits a complex natural-language request from within Microsoft Teams; the TotalAgility Agent acknowledges it, creates a governed electronic case with a unique case identifier, and generates a refined, structured prompt that drives the downstream review workflow. The case is created as a TotalAgility workflow object, not a legacy system transaction.

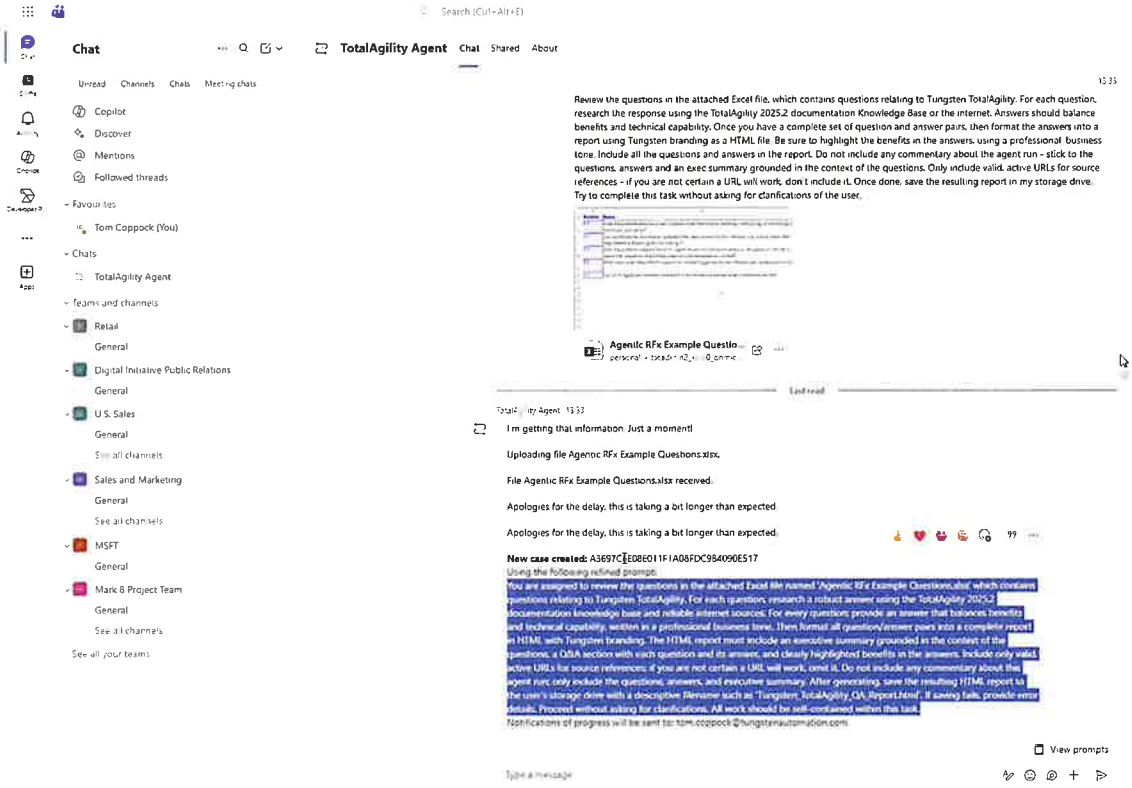


Figure 26 - Illustrative agentic request-to-case workflow through Microsoft Team Integration

Outlook task completion and SharePoint document exchange are native or natively configurable connectors that operate within the Agency's existing Microsoft 365 environment; enabling them requires no new integration beyond the Agency's existing Microsoft 365 footprint.

4.3.2.8 Agentic Agent Design: Organizational Development and Human-Centered Design Approach

Infocap's approach to designing, developing, and implementing agentic AI agents begins with the organization, not the technology. Each AI agent deployed in the Agency's UIC permitting system is treated as a governed participant in a human-AI work system: defined by a role, bounded by a scope of authority, evaluated against measurable performance criteria, and assigned to a human accountable owner before it operates in any workflow. The role is designed first. The technical configuration follows. This design discipline prevents the most common failure mode in AI implementations: deploying a capable model into an undefined role and discovering its limits through production errors. Agentic AI agents interact with people, policies, data, workflows, and consequential regulatory decisions. The design process must be structured accordingly. Infocap applies a combined Organizational Development and Human-Centered Design lifecycle to ensure that every AI agent deployed in the UIC review system is role-defined, workflow-integrated, SME-validated, and governed from initial design through steady-state operations.

4.3.2.8.1 Work System Discovery and Diagnosis

The design lifecycle begins with the work system, not the platform. Before selecting models, defining agents, or configuring workflows, Infocap conducts a structured analysis of the current operating environment to identify the business purpose, stakeholder map, workflow structure, decision rights, pain points, compliance constraints, and performance expectations that the AI agents must support. For the Agency's UIC permitting program, this discovery surfaces the twelve-phase permit review lifecycle described in §4.3.2.5.4, covering Class I injection well review and Class VI CO2 sequestration permit review as parallel but distinct tracks. The stakeholder map includes permit intake staff, administrative compliance reviewers, technical geoscience reviewers, AoR and risk validation specialists, supervisors, final decision authorities, and permit applicants. The system and data inventory covers the Agency's One Stop Shop Permitting Portal, ArcGIS and TAGIS, Agency-designated legacy systems used for reference, export, reconciliation, or human-mediated update support, EPA SDWIS, WVGES, and the WV Oil and Gas database.

Discovery identifies the six mandatory human decision gates described in §4.3.2.5.4 as the structural anchor points for human accountability in the workflow. These gates define where agentic execution must pause and human judgment must act. The AI agent design is organized around these gates, not around what the platform can execute autonomously. Pain points identified through this discovery include manual document handling at intake, inconsistent completeness review, AoR boundary validation complexity, the coordination burden of multi-step technical review, and the friction of updating legacy permit systems after human approval. These inform the AI agent opportunity list that the role definition stage converts into specific, bounded agent roles.

4.3.2.8.2 Agentic Agent Role Definitions

The second stage of the design lifecycle defines each AI agent as an organizational role. Rather than specifying a model or configuring a workflow node, Infocap first defines what the agent does, what it cannot decide, what human review it requires, and what performance standard it must meet. This role definition precedes any technical implementation decision. The Agency's named agents describe objectives, not individual pieces of software. Each one, the Digital Intake Specialist, the Engineering "Blueprint" Vision Agents, the Professional Engineering Specialist, and the Regulatory Monitoring "Watchdog" Agent, is delivered by a Multi-Agent system: a fleet of agents and Sub-Agents that work together to meet that objective. An agentic agent is not a fixed routine but a coordinated set of specialized workers, so a single named agent is carried out by several agents and Sub-Agents acting in concert.

The fleet works under a managing agent, the Case Orchestrator, which routes each case, triggers the right Sub-Agents, sequences their work, and monitors milestone state across the case lifecycle. Specialized Sub-Agents handle discrete functions such as document classification, administrative completeness, technical analysis, and Area of Review evaluation, while shared and cross-cutting Sub-Agents support the fleet across the case lifecycle: the Knowledge Discovery Sub-Agent grounds every output in approved sources, the Reflection and Validation Sub-Agent checks each output before it reaches a reviewer, the Draft Generation Sub-Agent assembles the resulting drafts, the Public Comment Analysis Sub-Agent prepares comment responses during the public phase, and the Legacy Export and RPA Reconciliation Sub-Agent packages approved results for legacy update. For an intake, for example, the Case Orchestrator routes the application, the Document Classification and Administrative Completeness Sub-Agents prepare the case record, the Knowledge Discovery Sub-Agent grounds the findings, and the Reflection and Validation Sub-Agent checks them before the package reaches the reviewer queue. Working together this way, the fleet assembles the evidence and drafts that each named agent's objective requires.

Figure 27 - Specialized Sub-Agents are managed by Managing Agents and bounded by HITL gates; example is Class I Technical Analysis Agent also supporting intake technical compliance review under the Digital Intake Specialist

Every agent and Sub-Agent in the Multi-Agent system is a worker that produces advisory evidence and drafts. The Agency's reviewers hold final authority at the six mandatory HITL gates, and no agent or Sub-Agent can approve, deny, or advance a case past a gate, override a reviewer, or write to a legacy system. The table below lists each agent and Sub-Agent in the fleet, the Agency agent name or RFP function it serves, and its authority boundary.

Agent / Sub-Agent	Agency Agent Name	RFP Section	Authority Boundary
Case Orchestrator / Managing Agent	Managing agent for the fleet: routing and sub-workflow orchestration (Digital Intake Specialist); enforces the six HITL gates	4.3.2.2.1.1, 4.3.2.5.4	Cannot approve, deny, or advance past any HITL gate; cannot override reviewer decisions or update legacy systems.
Document Classification Agent	Digital Intake Specialist (document classification)	4.3.2.2.1	Classification is advisory; cannot reject submissions or determine incompleteness without reviewer confirmation.
Administrative Completeness Agent	Digital Intake Specialist (Administrative Completeness Review)	4.3.2.2.1.2	Cannot issue a Notice of Deficiency, waive deficiencies, or grant extensions; the reviewer approves and signs all NoDs.
Engineering Blueprint Vision Agent	Engineering "Blueprint" Vision Agents	4.3.2.4.1	Extracted findings are advisory evidence; cannot approve construction design or technical compliance.
AoR Screening Agent	Professional Engineering Specialist; GIS and Area of Review analysis	Q.20, 4.3.2.3	Advisory; cannot approve findings, waive risk features, or determine AoR compliance without reviewer sign-off.
GIS Evidence Agent	Professional Engineering Specialist; GIS evidence assembly	Q.20, 4.3.2.3	Advisory pending reviewer validation; cannot make final AoR findings or waive identified risk features.
Class I Technical Analysis Agent	Professional Engineering Specialist (Class I); intake technical compliance review	Q.20, 4.3.2.2.1.3	Outputs are draft findings only; the senior technical reviewer validates before they become official findings.
Class VI Technical Analysis Agent	Professional Engineering Specialist (Class VI)	Q.20	Cannot approve findings or set permit conditions; contested and computational AoR conclusions escalate to a senior geoscientist.
Knowledge Discovery Agent	RAG and Source Grounding	4.3.2.2.2	Retrieval only; cannot modify the knowledge base; escalates rather than substituting general model knowledge when evidence is insufficient.
Reflection and Validation Agent	Hallucination Mitigation; Citations and Explainability	4.3.2.2.3, 4.3.2.2.5	Cannot approve its own results; failed reflection returns output for revision; reflection scores are written to the case audit trail.
Draft Generation Agent	AI Draft Generation; Notice of Deficiency; Public Notice; Response to Comments	4.3.2.4.2, 4.3.2.4.4, 4.3.2.4.5, 4.3.2.4.6	All drafts are advisory; nothing is issued or transmitted without reviewer editing and formal approval.
Public Comment Analysis Agent	Response to Comments (public comment	4.3.2.4.6	Cannot determine comment disposition or issue Agency responses; substantive

	categorization and response preparation)		and legally significant comments require senior or legal review.
Legacy Export and RPA Reconciliation Agent	HITL Workflow Interface and Legacy System Independence	4.3.2.7	Cannot write to legacy systems or perform uncontrolled retries; the human reviewer performs all legacy writes using the export package, and mismatches create new HITL tasks.
Regulatory Watchdog Agent	Regulatory Monitoring "Watchdog" Agent	4.3.3.1.2	Cannot update compliance logic, workflows, or knowledge base content; all identified changes require Agency review and formal change-control approval.

Table 5. Proposed Agentic Agent Role Catalog. The Multi-Agent system fleet of agents and Sub-Agents, the Agency agent name or RFP function each serves, and its authority boundary under HITL governance.

4.3.2.8.3 Work Allocation: Humans, Automation, and Agentic Execution

The third design stage determines which tasks within the UIC review workflow remain human-led, which are AI-assisted, which run through deterministic automation, and which are appropriate for agentic execution. This is not a binary human-versus-AI question. It is a structured analysis of task complexity, reversibility, regulatory stakes, data sensitivity, and the degree to which human judgment is required for legal and operational accountability.

For the Agency's UIC system, known routing decisions, intake completeness checks, document classification, and workflow milestone triggers operate through deterministic business rules and do not require language model reasoning. AoR boundary screening, technical data extraction, regulatory citation retrieval, and draft document preparation require bounded agentic reasoning within governed knowledge bases and approved source materials. All permit decisions, technical finding approvals, deficiency notice issuance, and final permit actions remain human-led and may not be delegated to the AI system under any configuration. The Task-Fit Execution model presented in §4.3.2.2 captures this allocation in full. The allocation is enforced through TotalAgility workflow gate logic, role-scoped access controls, and the digital sign-off requirements described in §4.3.2.7.1.

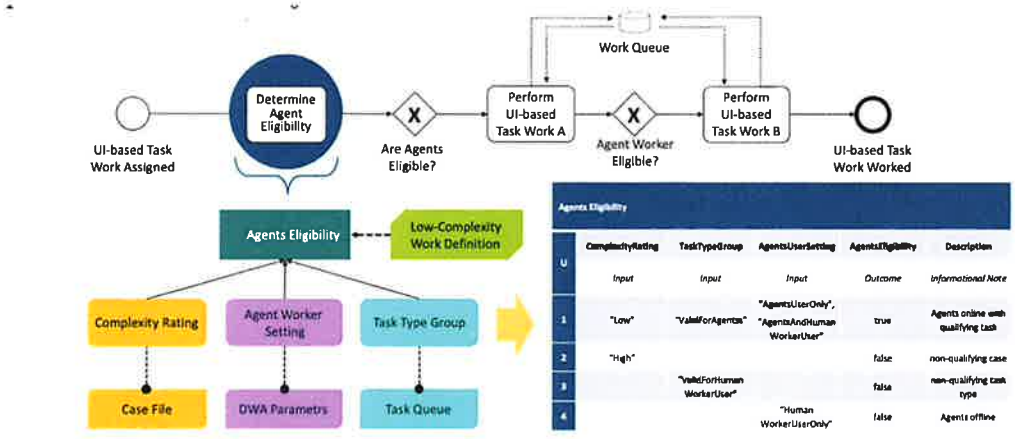


Figure 28 - Agent Eligibility Decision Service evaluates each task to determine whether to perform agentically or route for human reviewer

4.3.2.8.4 Human-AI Workflow Design

The fourth stage translates the role definitions and work allocation model into a designed workflow showing how agents and reviewers interact, how handoffs are structured, how exceptions are routed, and how every action is recorded across the full case lifecycle.

For the Agency's UIC system, the human-AI workflow is anchored to the twelve-phase permit lifecycle and six mandatory HITL decision gates described in §4.3.2.5.4. At each gate, the workflow suspends. The assigned agent presents its evidence package and draft output to the reviewer in the Standalone HITL Workflow Interface described in §4.3.2.7.1. The reviewer exercises independent judgment before the case advances. Human-Centered Design methods inform the reviewer interface design, work queue structure, and evidence presentation format. Reviewers see the agent's work product alongside source citations, confidence indicators, and Reflection Agent validation results in a format shaped by how the Agency's technical reviewers evaluate permit materials, not by how the platform stores data. Handoff design, exception routing, and audit trail requirements are described in Sections 4.3.2.7.2 through 4.3.2.7.4.

4.3.2.8.5 Development, Validation, and Pilot Approach

Each agent in the role catalog is built and validated against acceptance criteria defined before development begins. Acceptance criteria are derived directly from the role definition established in §4.3.2.8.2: the tasks the agent must perform, the authority limits it must respect, the outputs it must produce, and the quality standard it must meet. Criteria are developed in collaboration with the Agency's technical staff and supervisors who hold the regulatory knowledge required to evaluate whether an output is correct, incomplete, or unsuitable for reviewer presentation.

Agent development follows the PARR orchestration pattern described in §4.3.2.2.1.1: each agent plans its approach, acts within its defined tool-access boundaries, reflects on its output through the Reflection and Validation Agent, and revises before routing to the reviewer queue. Reflection scoring thresholds are calibrated against SME-validated examples drawn from real Agency case types. Golden task sets cover the representative cases within the Class I and Class VI permit tracks, including edge cases and exception scenarios identified during work system discovery. No agent advances to the live permitting workflow until it meets the performance threshold defined for its role. Prior to full deployment, Infocap will conduct a structured pilot with a controlled set of UIC cases and a defined group of the Agency's reviewers to validate workflow fit, adoption readiness, reviewer experience, governance operation, and performance against production-representative permit materials.

4.3.2.8.6 Operational Governance and Continuous Improvement

Each agent in the role catalog is assigned a governance owner: an Agency or Infocap role responsible for monitoring the agent's performance, reviewing its outputs on a defined cadence, and initiating a role revision, prompt or configuration update, knowledge base update, workflow change, or retraining where applicable when performance degrades, scope changes, or regulatory requirements are updated. Governance ownership is substantive, not nominal. The owner reviews the agent performance scorecard, participates in periodic quality reviews, and holds accountability for the agent's behavior in the permitting workflow.

The operational governance infrastructure supporting each agent runs across the observability and monitoring architecture described in Sections 4.3.2.5.2 through 4.3.2.7. The TotalAgility case notes and audit trail (§4.3.2.5.2) capture every agent action, tool call, Knowledge Discovery query, Reflection result, reviewer interaction, and workflow state change to a replayable decision record. The Case Agents monitoring view (§4.3.2.6) reports per-case token consumption, model version, iteration count, and output status, giving governance owners visibility into cost, usage patterns, and early signs of behavioral drift. The governance operating rhythm runs at three levels: continuous automated monitoring through the observability infrastructure; periodic quality reviews conducted by governance owners on a defined schedule; and triggered reviews initiated when a performance threshold is crossed, an escalation pattern emerges, or an incident condition is met. When a review identifies a performance gap, scope change, or regulatory update requiring agent modification, changes follow the same SME-validated design and testing process used in the initial build. No agent role is modified in production without review against the acceptance criteria defined in §4.3.2.8.2.

4.3.3. Mandatory Project Requirements

Our solution will support AI-enabled RPA, document processing, workflow orchestration, HITL governance, centralized dashboards, audit logging, GIS and AoR integration, regulatory-review workflows, operational reporting, and secure interoperability with approved the Agency's systems and data sources. TotalAgility Cloud capabilities including document classification, data extraction, workflow automation, task routing, queue management, reporting, and AI-assisted review will be configured to support the Agency's permitting operations.

Where capabilities are confirmed through TotalAgility platform functionality, Infocap identifies and maps those capabilities directly within the proposal response. Where requirements are operational, contractual, deployment-specific, or dependent upon the WVDEP/WVOT-approved configurations, Infocap provides implementation commitments, governance controls, deployment methodology, or supporting compliance artifacts consistent with the final system architecture and approved hosting environment.

TotalAgility incorporates centralized security controls including federated SSO, MFA, RBAC, ACLs, tenant segregation, encryption, vulnerability management, SIEM logging, continuous monitoring, incident-response governance, penetration testing, audit logging, and operational-security monitoring consistent with FedRAMP and applicable NIST SP 800-53 requirements.

All workflow orchestration services, AI-assisted processing, document-intelligence services, audit logging, monitoring functions, reporting services, integration activities, operational dashboards, and supporting infrastructure will operate within controlled cloud services. The Agency's data and AI-processing activities will not be routed to public consumer AI platforms or non-authorized cloud services.

Infocap's implementation approach emphasizes configurable workflow automation, centralized governance, operational transparency, source-grounded AI-assisted analysis, regulatory oversight, secure interoperability, and mandatory Human-in-the-Loop (HITL) approvals to support secure, auditable, and operationally sustainable permitting and compliance-review operations for the Agency.

4.3.3.1 Data Integration and Regulatory Compliance

Mandatory Integration and Compliance, Met by Design

- ✓ Ingests XML, CSV, PDF, GIS layers, well logs, and standard permit forms
- ✓ Compliance engine encodes Class I and Class VI requirements for automated checks
- ✓ Watchdog Agent monitors regulatory sources 24/7 and alerts Agency staff
- ✓ Cross-checks validation data from other agency and department systems

Infocap will support the Agency UIC Class I and Class VI regulatory-review operations through centralized data integration, document intelligence, configurable compliance workflows, AI-assisted analysis, Retrieval-Augmented Generation (RAG) grounding, knowledge base search, Human-in-the-Loop (HITL) approvals, audit logging, operational dashboards, and policy-driven workflow orchestration. Our proposed solution will integrate structured, semi-structured, unstructured, geospatial, and operational data sources to support permit intake, completeness review, technical-review workflows, Area-of-Review (AoR) coordination, compliance validation, reporting, public-notice preparation, and final regulatory decision support. TotalAgility document-intelligence services will support OCR processing, document classification, metadata extraction, indexing, workflow routing, validation checks, and AI-assisted document analysis across permit applications, supporting records, engineering documentation, GIS-related information, and regulatory-review materials.

The compliance framework will utilize configurable business rules, validation logic, workflow routing, reviewer tasks, exception handling, escalation workflows, and approval controls consistent with applicable UIC Class I and Class VI regulatory requirements, the Agency procedures, operational policies, and reviewer governance processes. Infocap's proposed solution will support configurable updates to forms, workflows, review criteria, routing logic, and compliance controls as regulations, guidance, templates, and operational requirements evolve.

Retrieval-Augmented Generation (RAG) services and knowledge-discovery capabilities will provide source-grounded regulatory context, document search, evidence retrieval, policy-reference support, and AI-assisted summarization using approved the Agency content repositories, operational records, regulatory references, guidance documents, and authorized data sources. AI-assisted outputs will be grounded in retrieved source content and operational data to support explainability, reviewer transparency, and traceable decision-support workflows.

Our proposed solution will support centralized audit logging, compliance dashboards, workflow telemetry, reviewer approvals, confidence scoring, operational metrics, and records tracking across the permitting lifecycle. All AI-assisted actions, reviewer decisions, workflow activities, extracted data, prompts, generated outputs, regulatory references, and operational events will be logged and auditable to support regulatory oversight, forensic review, operational transparency, and compliance validation.

Human-in-the-Loop (HITL) governance controls will ensure that all compliance determinations, workflow approvals, permit decisions, deficiency notices, technical findings, and final regulatory actions remain under authorized the Agency personnel oversight and approval. AI-assisted services will support analysis, extraction, summarization, recommendation generation, and

workflow prioritization but will not replace the Agency regulatory judgment or decision-making authority.

The Agency's data and AI-processing activities will not be routed to public consumer AI platforms or non-authorized cloud services. The proposed architecture provides centralized governance, improved regulatory consistency, enhanced auditability, source-grounded AI-assisted analysis, reduced manual review effort, and more efficient permitting and compliance-review operations across the Agency's regulatory environment.

4.3.3.1.1 Formats

Our proposed solution will support ingestion, validation, processing, workflow routing, and management of a broad range of structured, semi-structured, unstructured, document, image, geospatial, and engineering data formats required to support the Agency's UIC Class I and Class VI permitting workflows.

Supported formats include XML, CSV, PDF, TIFF, JPEG, PNG, scanned documents, standard permit forms, well logs, image-based records, GIS layers, ESRI Shapefiles, GeoJSON, KML, CAD drawings, DWG files, spreadsheets, text documents, metadata records, exported reports, and other WVDEP/WVOT-approved supporting documentation and operational records.

TotalAgility document-intelligence capabilities will support OCR processing, document classification, metadata extraction, form recognition, content separation, workflow routing, indexing, validation, and AI-assisted document analysis for structured and unstructured permit-review materials. Workflow orchestration services will support automated intake, completeness verification, reviewer assignments, exception handling, audit logging, records tracking, and Human-in-the-Loop (HITL) review activities across supported document and workflow types.

GIS, mapping, geospatial-analysis, and CAD-related formats will be integrated through the WVDEP/WVOT-approved GIS platforms, geospatial repositories, mapping services, engineering-review tools, secure APIs, and authorized external systems supporting Area-of-Review (AoR) analysis, geospatial validation, spatial-reference workflows, and environmental-review activities. Integration services will support secure retrieval, synchronization, display, and validation of geospatial and engineering information required for regulatory-review operations.

Where unsupported, incomplete, corrupted, or inconsistent formats are encountered, the system will generate configurable exception notifications, reviewer tasks, workflow flags, and validation alerts for manual review and adjudication by authorized the Agency personnel. See "*Appendix B: GIS/CAD Format Support Matrix*" for details supported versions, CRS expectations, metadata requirements, validation checks, size limits, fallback handling, exception-routing rules, and reviewer-validation requirements for common geospatial, engineering, document, and map-based submission types. Unsupported, incomplete, corrupted, missing-CRS, or inconsistent files will

generate reviewer-visible exceptions and tasks rather than unsupported automated conclusions, ensuring that geospatial evidence is always subject to human review before it influences AoR, technical findings, permit conditions, or decision-support materials.

Regulatory Compliance & Watchdog Agent

- ✓ Evergreen rules govern every agent action and workflow outcome
- ✓ Watchdogs immediately detect regulatory drift
- ✓ No compliance changes deploy unapproved
- ✓ No agent outruns the law: Watchdogs keep every workflow current, controlled, evidenced, and approval-ready

4.3.3.1.2 Compliance Engine & Watchdog Agents

As described in the CRFP as well as cited in Table 5 (*Proposed Agentic Agent Role Catalog*) the solution will include both a centralized compliance engine as well as specifically built *Watchdog Agents*. The compliance engine will leverage combination of business rules and GraphRAG to maintain an evergreen knowledge base of applicable regulatory requirements, business rules, permit-review procedures, completeness checks, workflow routing rules, permit-condition logic, validation requirements, reviewer tasks, exception handling, escalation criteria, and approval workflows to support standardized and repeatable regulatory-review operations.

The compliance framework will support configurable updates to workflows, templates, checklists, decision logic, routing rules, review criteria, forms, notifications, and operational policies as Federal regulations, EPA guidance, the Agency procedures, permit conditions, or agency business requirements evolve. Authorized Agency administrators and compliance personnel will be able to manage rule updates, workflow configurations, approval paths, and operational policies through controlled administrative interfaces and governed change-management processes.

The regulatory monitoring Watchdog Agent will monitor the WVDEP/WVOT-approved regulatory, legislative, policy, and compliance information sources for changes potentially impacting permitting workflows or regulatory-review requirements. Approved monitoring sources are understood to include Federal Register notices, EPA publications, State legislative feeds, the Agency-designated policy repositories, guidance documents, compliance bulletins, and authorized internal legal or operational content repositories. Regulatory-change alerts will be routed to named reviewer roles within configured service targets; no compliance logic changes deploy without approval.

The Watchdog Agent will support change detection, document summarization, policy-difference analysis, workflow-impact identification, and reviewer notification activities. Potentially relevant regulatory or policy changes may be summarized and routed to authorized Agency personnel with suggested impacts to workflows, compliance logic, forms, checklists, or operational procedures for further review and adjudication.

All proposed compliance updates, workflow changes, AI-generated recommendations, or regulatory-rule modifications will remain subject to mandatory Human-in-the-Loop (HITL) governance controls requiring authorized the Agency review, validation, approval, and change-management authorization prior to implementation within the operational environment. No

automated compliance-rule change, workflow modification, or policy update will be deployed without human review and approval.

Compared to static checklist-driven processes or manually maintained compliance workflows, the proposed compliance-engine and Watchdog architecture provides centralized governance, improved regulatory responsiveness, configurable workflow management, enhanced auditability, reduced manual policy-tracking effort, and more consistent regulatory-review operations across the permitting lifecycle.

Every Required Format, One Case Record

- ✓ XML, CSV, and PDF ingestion out of the box
- ✓ GIS layers: Shapefile, GeoJSON, KML, CAD, and DWG
- ✓ Well logs and standard permit forms
- ✓ Originals preserved unaltered for audit

4.3.3.1.3 External System Integration

Infocap will integrate our proposed solution with approved external systems, operational data sources, GIS repositories, regulatory databases, and supporting government applications through secure APIs, encrypted connectors, web services, Integration Server capabilities, scheduled synchronization, approved data feeds, database views, secure file exchange, and controlled human-mediated workflows where direct system integration is not authorized or technically appropriate.

The proposed integration architecture will support retrieval, validation, synchronization, enrichment, and cross-checking of permitting, geospatial, operational, environmental, and regulatory data required to support the Agency's UIC Class I and Class VI permitting workflows. Anticipated integration sources to include WVGES data repositories, EPA SDWIS, West Virginia Office of Oil and Gas records, the Agency operational databases, ERIS, ESS, GIS and Area-of-Review (AoR) services, property and plat systems, public-notice repositories, document-management systems, and other approved Federal, State, or agency-authorized information sources.

Base-scope integrations are limited to WV One Stop Shop Permitting (OSSP) for reporting and payment, OneLogin for external user access, and Active Directory for internal user access, together with WVDEP/WVOT-approved GIS/reference-data access needed for review workflows. ERIS, ESS, and other legacy or records systems will not be modified or written to by AI. Any reference, export, manual-update, read-only, or future integration pattern for those systems will be subject to the Agency's approval during discovery.

Final integration scope, access methods, and write-back permissions will be confirmed during discovery and aligned with WVDEP/WVOT-approved systems and addendum guidance. Where systems are read-only, out of scope, unavailable, or not suitable for direct integration, TotalAgility will support controlled export packages, reviewer-mediated updates, secure file exchange, reviewer upload, or manual reference workflows with audit logging.

TotalAgility's capabilities support interoperability with both cloud-based and on-premise systems while maintaining centralized workflow orchestration, auditability, operational visibility, and secure information exchange. Integration workflows may support automated document retrieval, metadata synchronization, workflow triggering, validation checks, status updates, reporting, GIS coordination, reviewer task generation, and operational analytics based on the Agency business processes and security requirements.

Where external data is unavailable, incomplete, inconsistent, stale, or determined not to be authoritative, Infocap's proposed solution will automatically flag exceptions, generate reviewer notifications, apply configurable business rules, and route the item to the authorized Agency personnel for manual review, adjudication, or corrective action. Human-in-the-Loop (HITL) governance controls will ensure that regulatory decisions, data validation activities, and final workflow approvals remain under authorized Agency oversight. Integration communications will utilize encrypted transport mechanisms, federated authentication, role-based access controls, audit logging, and continuous monitoring consistent with FedRAMP High security practices. TotalAgility enables centralized orchestration, improved operational consistency, reduced manual reconciliation effort, enhanced auditability, secure interoperability, and more efficient regulatory-review workflows across the permitting lifecycle.

4.3.3.2 Security and Deployment

Infocap will implement a comprehensive full security and deployment architecture to protect the Agency's permitting data, workflow operations, AI-assisted processing activities, and regulatory-review functions. TotalAgility is hosted within the FedRAMP Authorized boundary (Package ID FR1802451335 - https://www.fedramp.gov/marketplace/products/FR1802451335), operated under security controls consistent with applicable NIST SP 800-53 requirements.

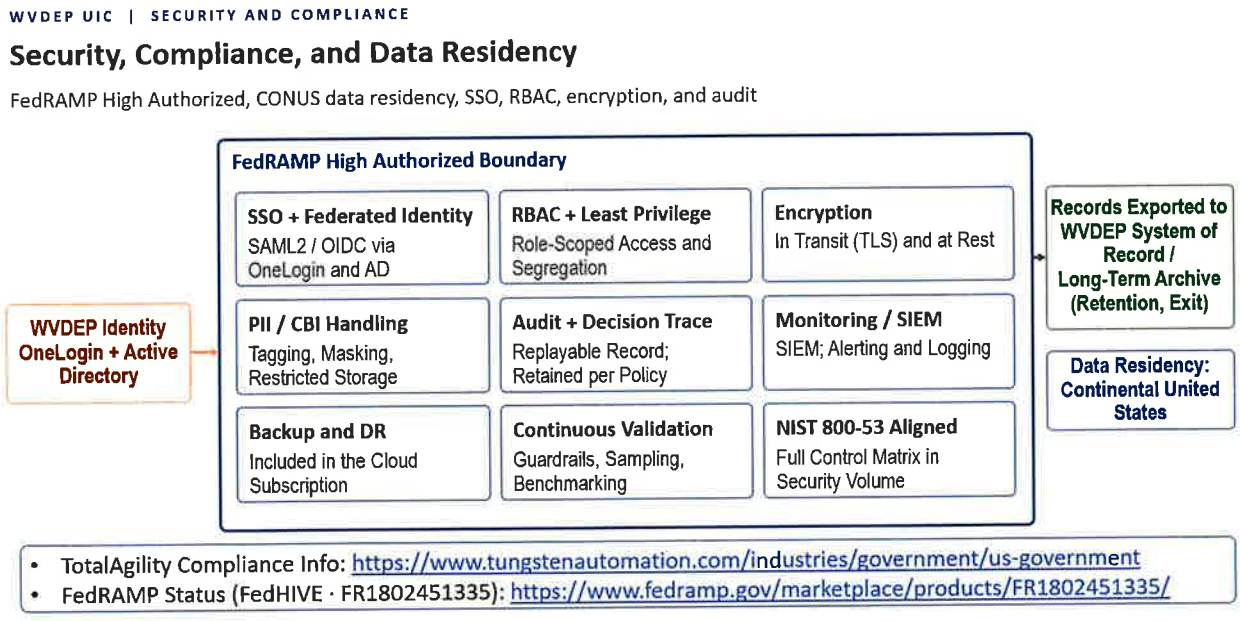


Figure 29 - Security, Compliance, and Data Residency - FedRAMP High Authorized boundary (FedHIVE FR1802451335); CONUS data residency; SSO, RBAC, encryption, audit, and continuous monitoring

Within the secure Azure-hosted infrastructure, the solution architect will include logical tenant segregation, optional dedicated-instance deployment models, Web Application Firewall (WAF) protection, network firewalls, secure virtual-network architecture, encrypted communications, centralized identity management, federated authentication, role-based access controls (RBAC), Access Control Lists (ACLs), Multi-Factor Authentication (MFA), and least-privilege authorization controls to protect access to applications, workflow services, operational dashboards, APIs, documents, audit records, and administrative functions.

Infocap will ensure that all production workflow orchestration, document processing, OCR, RAG/Knowledge Discovery, prompt processing, model calls, token metering, audit logging, monitoring, storage, and third-party AI API activity used for the Agency's solution operate entirely within a WVDEP/WVOT-approved FedRAMP Moderate-or-better boundary. No permit data, prompts, extracted data, generated outputs, reviewer activity, or AI-processing tasks will be routed to public consumer AI services or to standard/non-authorized cloud environments.

As stated in the CRFP addendum, authentication and access-management services will leverage OneLogin for external user access, and with ActiveDirectory for internal user access enabled by federated Single Sign-On (SSO), SAML 2.0, OpenID Connect (OIDC), and claims-based authentication services. MFA enforcement will be supported through the WVDEP/WVOT-approved identity providers and conditional-access policies. Administrative access, workflow permissions, API access, reviewer assignments, and operational-security functions will be centrally managed, logged, and auditable.

The TotalAgility security architecture includes Azure Web Application Firewall services, virtual firewalls, endpoint protection, antivirus and anti-malware controls, vulnerability scanning, security telemetry collection, centralized SIEM logging, Azure Sentinel monitoring services, and 24x7 Security Operations Center (SOC) monitoring designed to support continuous monitoring, operational visibility, threat detection, and incident-response activities.

Infocap and Tungsten Automation maintain formal security-governance processes including vulnerability management, secure software development lifecycle (SSDLC) practices, configuration management, change management, annual third-party penetration testing, incident-response procedures, audit logging, patch management, operational monitoring, and security-event escalation processes. Vulnerabilities will be prioritized and remediated in accordance with established severity classifications, risk-management procedures, and operational-security policies.

4.3.3.2.1 Encryption

All data is encrypted in transit using TLS 1.3 and encrypted at rest using AES-256. TotalAgility utilizes FIPS-compliant cryptographic controls and Azure Key Vault for secure key management, key rotation, and secret storage. Databases, file attachments, logs, backups, exported data, and storage repositories are encrypted by default. Encrypted backup data is replicated across FedRAMP Authorized boundary regions to support disaster recovery, backup resiliency, and continuity-of-operations requirements. Encryption controls align with FedRAMP High and applicable NIST SP 800-53 security requirements, including protection of data at rest, secure key management, and encrypted backup and recovery operations.

Requirement	How Compliance is Enforced
Encryption in Transit	TotalAgility Cloud uses TLS 1.3 over HTTPS port 443. Infocap will meet the CRFP's TLS 1.3 requirement for applicable user-facing and integration endpoints or provide an WVDEP/WVOT-approved compensating control/architecture if any component remains TLS 1.3.
Search Traffic	Azure AI Search network traffic is encrypted using TLS 1.3.

Encryption at Rest	All data at rest is encrypted using AES-256 at the database level, and Azure AI Search data is encrypted at rest with AES-256 managed keys.
Key Management	Azure Key Vault is used for encryption keys in the TotalAgility Cloud environment.

Table 6 - Encryption Compliance Summary - TLS and AES-256 controls mapped to CRFP encryption requirements

4.3.3.2.2 Access Control

Access permissions are managed through roles, groups, Access Control Lists (ACLs), functional access rights, administrative security, hierarchy-based security, supervisor review workflows, and dynamic work allocation based on configurable business rules. Administrative access, workflow permissions, API access, document access, and runtime privileges are centrally managed and fully auditable. The system will not permit unauthenticated public submission or access; external users must register and authenticate through OneLogin or another WVDEP/WVOT-approved identity process.

Multi-Factor Authentication (MFA) is enforced through the Agency's identity provider, and can include authenticator applications, FIDO2 tokens, Smart Card/PIV authentication, certificate-based authentication, and conditional-access policies. User provisioning, authorization, and deprovisioning can be synchronized with the Agency enterprise identity-management systems to support centralized lifecycle management and organizational role alignment.

The platform supports segregation of duties, Zero Trust security principles, secure work queues, role-based workflow routing, and granular authorization controls to restrict access to sensitive functions and data. Authentication events, user activity, workflow transactions, administrative actions, and security events are centrally logged and monitored through SIEM and Azure monitoring services to support compliance, operational monitoring, auditability, and incident-response activities.

4.3.3.2.3 Privacy and PII Handling

Infocap's proposed solution protects Personally Identifiable Information (PII) and Confidential Business Information (CBI) through encryption, metadata tagging, tenant isolation, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), audit logging, retention policies, secure workflow controls, and logical data segregation. The Agency's data is stored within dedicated databases and storage repositories located within the continental United States and protected through least-privilege access policies, federated authentication, and secure routing controls.

The platform supports configurable retention schedules, redaction, records-management controls, auditability, and Human-in-the-Loop (HITL) review workflows to support responsible AI governance and operational oversight. Access to sensitive data is restricted to authorized users and monitored through centralized logging and audit controls. The Agency's data will not be used to train proprietary or shared AI models without explicit written consent. All data and processing results are deleted within 24 hours and are not used for model training, and Tungsten-hosted LLM services are configured for no data retention or reuse for model training purposes. Provider-level non-retention for model training does not limit TotalAgility's retention of AI audit records for at least five years.

AI-assisted workflows operate under HITL governance controls requiring reviewer validation, approval, or adjudication before regulatory decisions are finalized. AI-generated outputs, workflow actions, prompts, model interactions, and processing events are logged and auditable to support operational transparency, explainability, forensic review, and regulatory oversight. The Agency's data, prompts, workflow content, permit records, reviewer activity, and AI-processing operations are not routed to public consumer AI platforms, unmanaged AI services, or non-authorized cloud environments. AI orchestration, document processing, token metering, audit logging, and workflow services remain within the controlled FedRAMP boundary.

4.3.3.2.4 Deployment Environment & Hosting Options

All production, backup, disaster recovery, logging, monitoring, AI-assisted processing, workflow orchestration, and operational support services remain within the FedRAMP Authorized boundary and continental United States. TotalAgility satisfies the Agency's required FedRAMP Moderate security requirements for secure processing, storage, workflow automation, audit logging, monitoring, and regulatory-review operations. The platform supports dedicated logical tenants with isolated databases, storage repositories, authentication contexts, and tenant-specific URLs. Optional dedicated infrastructure deployments are available for enhanced isolation requirements. The architecture supports high availability, automated failover, regional replication, disaster recovery, and continuity-of-operations capabilities through Azure Availability Zones and paired-region replication. Disaster-recovery capabilities include encrypted backups, geographically redundant replication, restoration procedures, operational recovery validation, and failover processes designed to maintain service availability and protect the Agency's data during infrastructure disruptions or security events.

Backup operations, recovery activities, failover procedures, and restoration processes are governed through established operational-security and infrastructure-management practices to support ongoing resiliency, data protection, and operational continuity. TotalAgility operates under a shared-responsibility security model in which foundational cloud infrastructure controls are inherited from the underlying FedRAMP High Authorized environment, while Infocap and TotalAgility manage application-layer security, workflow orchestration, AI-processing controls, identity integration, document-processing services, logging, monitoring, tenant isolation, auditability, and operational security services. The Agency retains responsibility for customer-managed administrative policies, user governance, business-process approvals, and organizational access-management decisions.

The authorization boundary leverages inherited FedRAMP security controls provided by the cloud service provider, including physical security, infrastructure protection, regional resiliency, and foundational platform services. All application services, workflow orchestration, OCR/document processing, AI-assisted review workflows, storage repositories, databases, logging, monitoring, audit services, token metering, and operational dashboards remain within the controlled FedRAMP Authorized boundary. External integrations, including Agency identity-management systems, GIS services, OneLogin, Active Directory, and OSSP integrations, connect through secured APIs, encrypted communications, and federated identity controls. The Agency's data and AI-processing activities are not routed to public consumer AI platforms, unmanaged SaaS services, or non-authorized cloud environments. Administrative users may manage customer-specific workflow policies, reviewer assignments, retention settings,

and organizational authorization structures through delegated administrative controls consistent with least-privilege governance practices.

4.3.3.2.5 Single Sign-On Integration

Infocap will integrate Infocap's proposed solution with the Agency identity-management systems using federated Single Sign-On (SSO). TotalAgility supports SAML 2.0, OpenID Connect (OIDC), WS-Federation, and claims-based authentication for integration with enterprise identity providers including Microsoft Entra ID, ADFS, Okta, OneLogin, Ping Identity, and other standards-based identity platforms. User provisioning, authorization, and deprovisioning are centrally managed through the federated identity provider to support lifecycle management, least-privilege access enforcement, and organizational role alignment. Multi-Factor Authentication (MFA) enforcement is supported through the Agency conditional-access policies and enterprise authentication controls. Supported authentication methods include authenticator applications, FIDO2 tokens, Smart Card/PIV authentication, certificate-based authentication, and adaptive conditional-access policies. SSO implementation activities include exchange of federation metadata, certificates, claims mappings, callback URLs, and identity-provider configuration settings during onboarding and deployment. Infocap's proposed solution will support SAML 2.0 integration with the Agency identity-management systems, and OpenID Connect compatibility will be validated during solution design.

4.3.3.2.6 Security Assessments

Tungsten Automation maintains a comprehensive security program that includes third-party penetration testing, vulnerability management, cloud-security monitoring, secure software development lifecycle (SSDLC) practices, continuous monitoring, incident-response governance, and ongoing security operations consistent with FedRAMP High and applicable NIST SP 800-53 security requirements. The TotalAgility security program includes Web Application Firewall (WAF) protection, anti-malware controls, code review, infrastructure monitoring, and application-security testing using industry-standard tools including Veracode, Burp Suite, and Qualys. Annual TotalAgility Cloud penetration testing is performed to assess application, API, authentication, infrastructure, and configuration security controls. Customer-authorized third-party penetration testing is supported through established review and approval processes.

The platform operates under a formal Incident Response (IR) program based on FedRAMP and NIST incident-handling guidance. Incident-response procedures include detection, analysis, containment, eradication, recovery, escalation, forensic support, and customer notification processes. Security incidents and suspicious activities are monitored through centralized SIEM and 24x7 SOC operations to support rapid detection and coordinated response activities. Incident severity classifications, escalation procedures, breach-notification timelines, remediation tracking, and post-incident review activities are governed through established operational-security and incident-management processes.

Vulnerabilities are prioritized using CVSS severity ratings and managed through formal vulnerability-management and change-management procedures. Critical vulnerabilities are patched, mitigated, or addressed through compensating controls within established remediation timelines and emergency change procedures. Major vulnerabilities are mitigated through patching, removal, or enhanced monitoring within defined operational timelines, while medium-

and low-severity vulnerabilities are managed according to risk-based remediation priorities. Security findings, vulnerabilities, configuration deviations, and remediation activities are formally tracked through structured remediation-governance processes consistent with FedRAMP and NIST vulnerability-management practices. Findings are prioritized using risk-based severity scoring, assigned to responsible personnel, monitored through remediation closure, and documented within centralized tracking workflows. Compensating controls, risk acceptances, remediation exceptions, and emergency changes are governed through established review and approval procedures.

Security events, infrastructure telemetry, authentication activity, audit logs, vulnerability scans, configuration changes, and operational metrics are continuously collected, correlated, retained, and monitored through centralized SIEM and 24x7 SOC operations to support threat detection, incident response, compliance validation, forensic analysis, operational visibility, and ongoing risk management. Continuous-monitoring activities include ongoing vulnerability scanning, log analysis, configuration monitoring, security-alert correlation, remediation tracking, and periodic operational-security reviews designed to maintain security posture and compliance alignment. Assessment activities include application, API, authentication, infrastructure, and configuration testing, with findings documented, prioritized, tracked, and remediated through formal governance processes. Security artifacts and any required updates will be tracked through a POA&M and finalized before go-live.

Severity	Critical	Major	Minor
Common Vulnerability Scoring System	**Critical CVS Score 9.0-10.0**	**High CVS Score 7.0-8.9**	**Medium, Low CVS Score 0.1-6.9**
Impact	Critical business impact on business operations.	Considerable Major business impact on business operations.	Minor business impact on business operations if the risk occurs.
Timeframe for Remediation	For critical vulnerabilities systems/services must be patched or removed within 72 hours during workdays, outside office hours for a consecutive period 7 days. If a critical vulnerability has such a high risk that a crisis can occur, it can be handled as an emergency change and be introduced as soon as possible.	Major vulnerabilities must be mitigated by patching, removal, or increased monitoring within 30 days.	Minor vulnerabilities Medium vulnerabilities must be mitigated by patching, removal, or increased monitoring within 90 days. Low vulnerabilities must be mitigated by patching, removal or increased monitoring as deemed necessary from case to case.

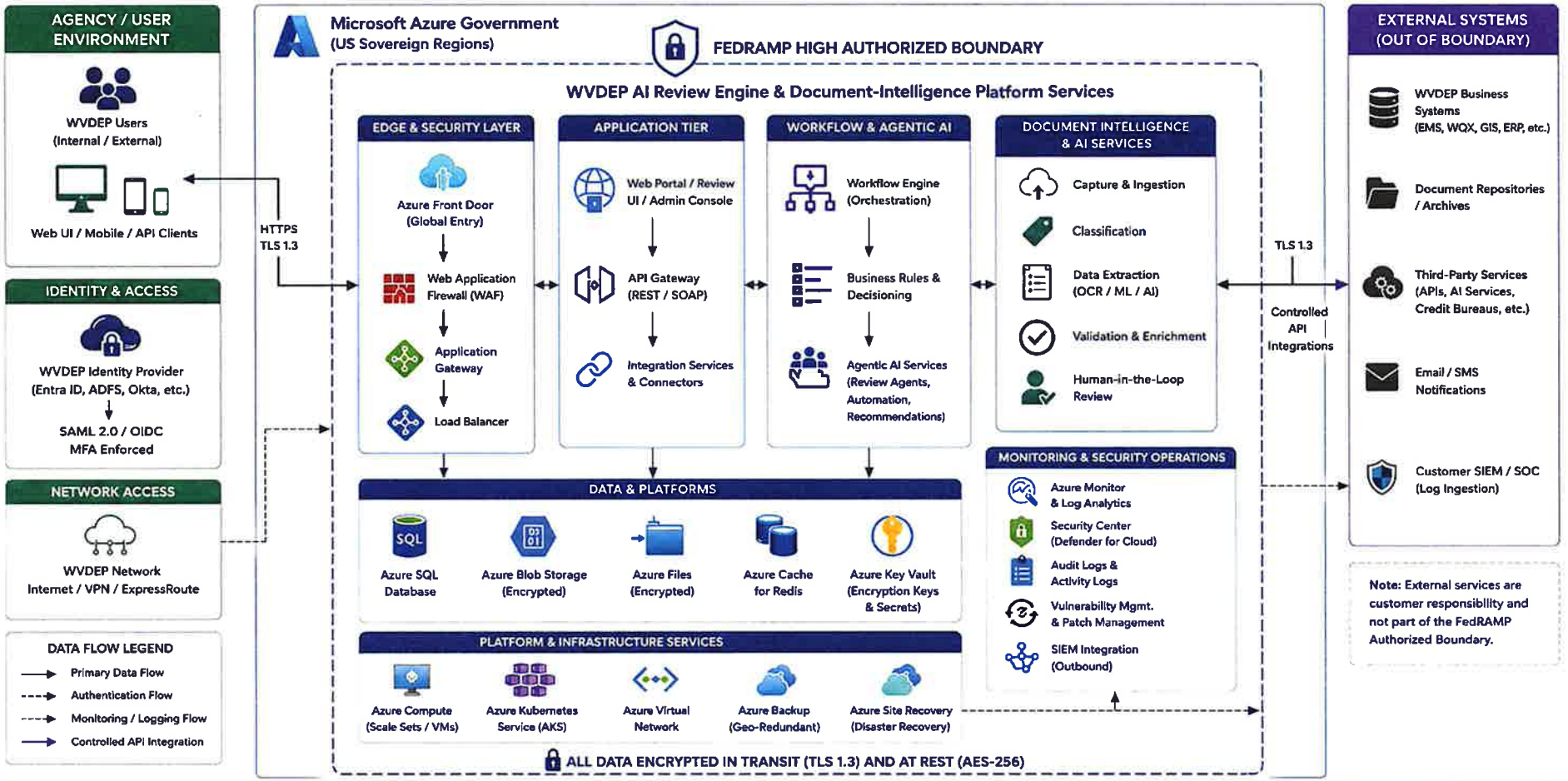
Table 7 - Vulnerability Management Prioritization and Remediation Timelines - severity classification, CVSS scoring thresholds, and remediation timeframe requirements

WVDEP AI Review Engine and Document-Intelligence Platform

Workflow Based Agentic AI, Automation, and Review

TUNGSTEN AUTOMATION

FedRAMP HIGH



FEDRAMP HIGH SECURITY CONTROLS (NIST 800-53 REV. 5)

- **ACCESS CONTROL** — AC-2, AC-3, AC-6, AC-17 — RBAC, Least Privilege, MFA, Session Mgmt.
- **IDENTIFICATION & AUTHENTICATION** — IA-2, IA-5, IA-12 — SSO, MFA, Strong Auth, Federated Identity
- **DATA PROTECTION & ENCRYPTION** — SC-13, SC-28, SC-12 — Encryption at Rest/In Transit, Key Mgmt., Data Masking
- **AUDIT & ACCOUNTABILITY** — AU-2, AU-6, AU-12 — Comprehensive Logging, Audit Trails, Non-Repudiation
- **SYSTEM & COMMUNICATIONS PROTECTION** — SC-7, SC-18, SC-20, SC-23 — WAF, Network Segmentation, Secure Configurations
- **CONTINUOUS MONITORING** — CA-7, CA-2, SI-2 — Continuous Monitoring, Vuln Scanning, CM
- **INCIDENT RESPONSE & RESILIENCY** — IR-2, IR-4, CP-2, CP-10 — IR Plan, BCP, DR, Backups, RTO/RPO Defined

ATO PACKAGE INFORMATION

- ✓ FedRAMP High Authorized Service
- ✓ Boundary: WVDEP AI Review Engine and Document-Intelligence Platform
- ✓ Hosting: Microsoft Azure Government
- ✓ Impact Level: High
- ✓ Authorization Documentation Available in FedRAMP Repository to Authorized Parties

4.3.3.2.7 Testing, User Acceptance Testing, and Production Readiness

Infocap will conduct structured testing and User Acceptance Testing (UAT) before production deployment. The UAT process will validate configured workflows, document intake, AI-assisted extraction, reviewer routing, Human-in-the-Loop (HITL) decision gates, GIS/AoR evidence handling, audit logging, security controls, reporting, and export package generation. UAT results, defects, corrections, retesting outcomes, and final acceptance signoff will be documented before production release.

4.3.3.2.7.1 GIS User Acceptance Testing

GIS-specific UAT scenarios will be included in the acceptance process to validate that applicant-submitted spatial materials, reviewer-generated GIS outputs, ArcGIS/TAGIS outputs, CRS transformations, topology checks, AoR screening results, Human-in-the-Loop (HITL) decision reviewer actions, and audit records are correctly captured within the TotalAgility case lifecycle. GIS UAT will confirm that TotalAgility acts as the workflow, evidence, HITL routing, and audit layer, while Agency-approved GIS tools and reviewer workflows remain authoritative for technical GIS analysis and validation.

4.3.3.3 Support and Maintenance

Infocap will provide support and maintenance services for the proposed SaaS environment, workflow automation platform, document-processing services, AI-assisted processing capabilities, dashboards, integrations, reporting services, and regulatory-review workflows supporting the Agency's UIC permitting operations.

Support and maintenance services will include operational monitoring, incident management, workflow support, integration support, vulnerability-management coordination, patch management, platform upgrades, backup coordination, disaster-recovery support, AI-service monitoring, usage reporting, user-support services, and training assistance.

Infocap will also support workflow configuration updates, business-rule modifications, dashboard enhancements, reviewer queue management, exception handling, and operational optimization activities consistent with the Agency operational and regulatory requirements.

Tungsten Automation will provide core TotalAgility Cloud platform hosting, infrastructure monitoring, backup operations, security monitoring, centralized logging, platform patching, maintenance activities, and SaaS platform upgrades within the managed hosting environment. Infocap will provide implementation support, workflow configuration, integration support, AI-governance support, operational oversight, and customer coordination services.

The Agency will retain control over agency-specific workflow policies, reviewer assignments, organizational structures, and user-governance decisions through federated authentication and role-based access controls.

4.3.3.3.1 The Support and Maintenance period, including the warranty, shall officially commence only upon written System Acceptance by the Agency.

Infocap confirms that the support and maintenance period, including all applicable warranty services, will officially commence upon written System Acceptance by the Agency unless

otherwise defined within the final contract, statement of work, or mutually approved implementation schedule.

System Acceptance activities will include completion of implementation milestones, configuration validation, integration testing, User Acceptance Testing (UAT), security validation, workflow verification, operational testing, and confirmation that Infocap's proposed solution satisfies agreed functional, operational, security, and performance requirements. Upon written acceptance, Infocap will transition Infocap's proposed solution into full operational support and maintenance status.

Following System Acceptance, Infocap will provide ongoing support and maintenance services including operational monitoring, incident management, vulnerability management, patch coordination, workflow support, integration support, audit-log monitoring, backup coordination, upgrade management, and security operations based on the approved support model and service-level commitments.

4.3.3.3.1.1 Acceptance shall be defined as successful demonstration and testing of all system requirements including training, with the ability for all users to navigate and utilize the system to perform their roles.

Infocap will support acceptance through a requirements traceability matrix, configuration review, system integration testing, UAT, role-based test scripts, training completion, defect remediation, security review, accessibility review, and production readiness review. Acceptance will require successful demonstration and testing of all system requirements, including the ability for administrators, reviewers, technical staff, GIS reviewers, managers, and HITL approvers to navigate and use the system for their assigned roles.

Acceptance will be defined as successful demonstration and testing of all system requirements, including completion of training and validation that all authorized users can navigate and utilize the system to perform their assigned roles and responsibilities. Infocap will support System Acceptance through requirements traceability, configuration review, system integration testing, User Acceptance Testing (UAT), workflow validation, role-based testing, training completion, defect remediation, security validation, and production-readiness review activities.

Acceptance testing will validate workflow automation, document processing, dashboards, integrations, reporting functions, Human-in-the-Loop (HITL) approval workflows, role-based access controls, and operational support capabilities for administrators, reviewers, technical staff, GIS reviewers, managers, and HITL approvers.

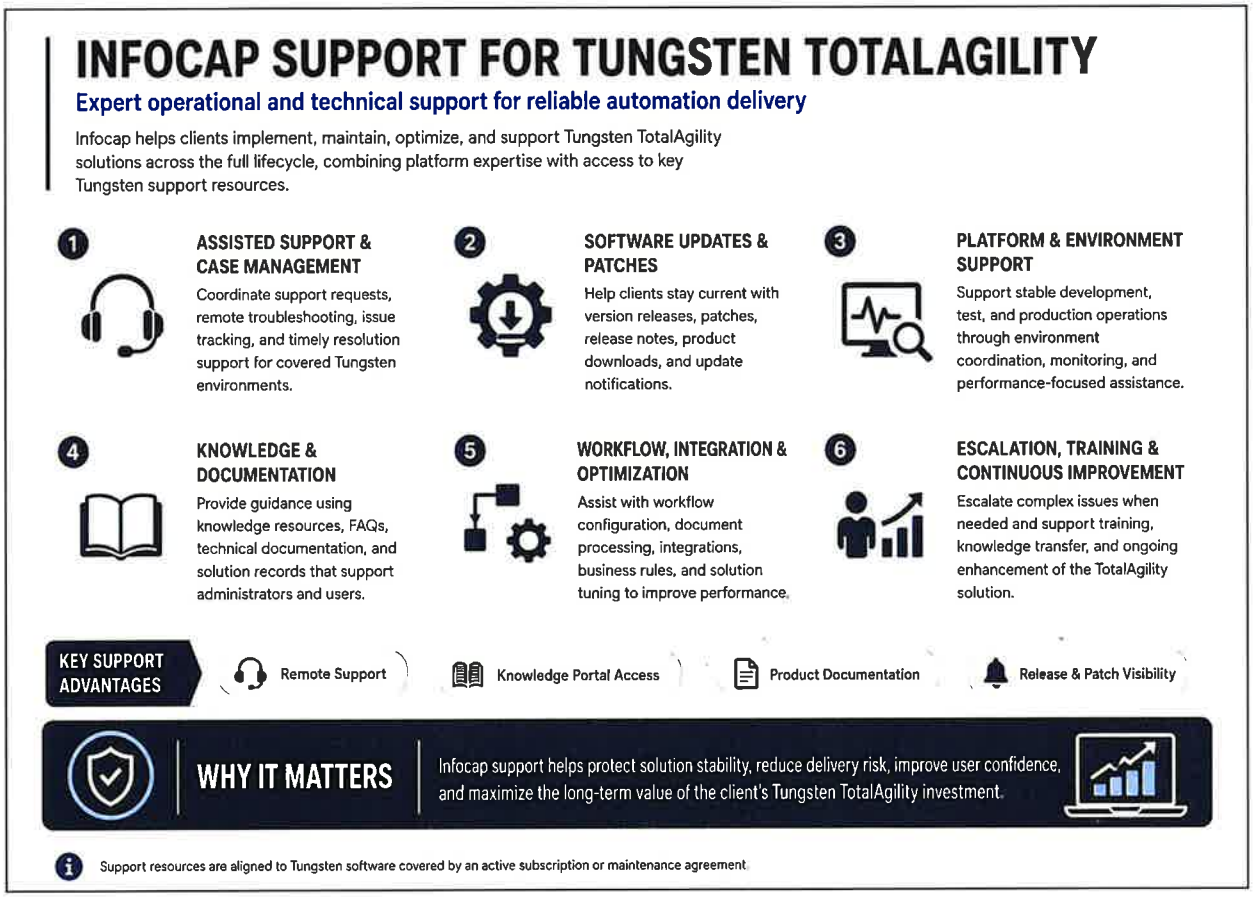
4.3.3.3.2 Support Access & Availability

Infocap will provide technical support, operational support, and maintenance services for TotalAgility during standard business operating hours at a minimum, with 24x7 cloud operations, infrastructure monitoring, security monitoring, SIEM alerting, incident-response coverage, and Security Operations Center (SOC) monitoring supporting the hosted environment.

Support services will include user support, troubleshooting, incident management, integration support, workflow support, dashboard support, reporting support, vulnerability-management coordination, patch-management coordination, and escalation management for issues impacting system availability, security, or workflow operations.

Support access will be available through approved support channels including email, ticketing systems, support portals, and authorized support contacts. Response procedures, escalation paths, severity classifications, response-time objectives, and service-level commitments will be defined in the final Service Level Agreement (SLA).

4.3.3.3.2.1 The Vendor shall provide technical support at minimum, during standard business operations hours



Infocap confirms that technical support will be provided, at a minimum, during standard business operating hours. Support services will include ticket intake, troubleshooting, issue triage, escalation management, operational-status updates, and coordination with Tungsten Cloud Services and authorized the Agency personnel to support timely resolution of operational and technical issues. Support requests may be submitted through approved support channels including email, ticketing systems, and authorized support contacts. Response procedures, escalation paths, and support metrics will be defined in the final Service Level Agreement.

4.3.3.3.3 Scope of Support

Infocap will provide implementation support services and reseller-coordinated support for the proposed permitting environment, including software configuration, workflow setup, dashboard configuration, integration assistance, operational troubleshooting, secure-connectivity troubleshooting, reporting support, and escalation coordination.

During implementation, Infocap will support workflow configuration, OCR and extraction setup, metadata validation, Retrieval-Augmented Generation (RAG) configuration, Human-in-the-Loop (HITL) workflow implementation, testing support, operational-readiness activities, administrator guidance, reviewer training, documentation support, and knowledge-transfer activities associated with the deployed solution configuration.

Following production deployment, Infocap will provide Tier 1 support coordination through a designated support portal and ticketing process supporting issue intake, ticket tracking, status visibility, user guidance, basic troubleshooting, and escalation management.

Support services will include;

- User Support
- Troubleshooting
- Incident Management
- Workflow Support
- Dashboard Support
- Reporting Support
- Integration Support
- Vulnerability-Management Coordination
- Provide Fix Packs, Service Packs and Software Major / Minor Version Updates
- Escalation Management for Issues Impacting
    - System Availability
    - Security Remediation
    - Workflow Operations

Platform-managed operational services including cloud hosting, infrastructure monitoring, platform patching, backup operations, vulnerability management, and core SaaS operational maintenance remain the responsibility of Tungsten TotalAgility Cloud managed services under the shared-responsibility operating model.

4.3.3.3.3.1 Assistance with software configuration and cloud environment optimization for efficiency and cost control.

During implementation, Infocap will complete software configuration, workflow optimization, and cloud-environment tuning to support operational efficiency, system performance, scalability, and cost control for the Agency's permitting environment. Other activities will include workflow tuning, business-rule configuration, reviewer queue optimization, dashboard configuration, storage-retention management, integration-performance tuning, and document-processing optimization based on the Agency operational requirements. Infocap will also support optimization of AI-assisted processing through prompt tuning, token-usage controls, workflow prioritization, and Human-in-the-Loop (HITL) workflow configuration to improve efficiency and manage operational costs.

Cloud-environment optimization services will include performance monitoring, utilization analysis, storage management, capacity planning, and operational telemetry review to support efficient resource utilization and reliable platform operations. Infocap's configuration and optimization services will include focus on optimizing operational efficiency, scalability,

performance, and cost control for the Agency's permitting environment. Activities will be performed in collaboration with Agency stakeholders and aligned with approved business requirements, workflow objectives, and governance processes. The implementation timeline, phase durations, milestones, and level of effort are further defined within the project schedule and implementation plan sections of the proposal.

During the initial implementation phase, Infocap will configure workflows, business rules, reviewer work queues, dashboards, integrations, document-processing services, retention settings, role and permission structures, AI-service configurations, and Human-in-the-Loop (HITL) approval workflows. Initial optimization activities will include OCR and extraction tuning, prompt configuration, token-usage controls, workflow prioritization, and baseline cloud-environment configuration. This phase will conclude following Agency review and approval of the configured workflows and business processes. Deliverables will include configuration documentation, workflow diagrams, role matrices, integration specifications, dashboard configurations, and implementation-status reports.

During system testing and User Acceptance Testing (UAT), Infocap will support workflow validation, extraction validation, performance tuning, telemetry review, exception handling, dashboard refinement, and business-rule adjustments based on Agency feedback and test outcomes. the Agency's reviewers and administrators will participate in configuration validation, workflow sign-off, UAT execution, and operational-readiness review activities. This phase will conclude upon successful completion of UAT and Agency acceptance of production-readiness activities. Deliverables will include UAT support materials, issue-resolution logs, updated configuration documentation, optimization recommendations, test-result summaries, and UAT sign-off records.

During production rollout and transition to operations, Infocap will provide limited reseller-coordinated support for issue intake, configuration troubleshooting, workflow guidance, and escalation coordination through the designated support and ticketing process. Post-production activities will focus on stabilization, operational guidance, knowledge transfer, and coordination with Tungsten Automation support services for platform-managed issues. This phase will conclude following production stabilization and transition to normal support operations. Deliverables will include operational runbooks, support procedures, escalation matrices, production-readiness documentation, knowledge-transfer summaries, and transition-to-operations documentation.

Platform-managed operational services including cloud hosting, infrastructure monitoring, patch management, backup operations, vulnerability management, and core SaaS operational maintenance remain the responsibility of Tungsten TotalAgility Cloud managed services under the shared-responsibility operating model.

4.3.3.3.3.2 Troubleshooting and establishing secure remote connections.

Infocap will provide support for troubleshooting, establishing, validating, and maintaining secure remote connections supporting integrations, APIs, encrypted web services, secure file transfers, and authorized external-system communications within the Agency's permitting environment. Operational issues can be supported via remote system access if allowable by customer security posture. Support activities will include connectivity troubleshooting, certificate coordination, authentication support, firewall and network-configuration review, Integration Server

configuration, connection validation, and escalation management consistent with approved security procedures. TotalAgility Integration Server supports secure communication between cloud-hosted services and approved on-premise or external systems without persistent storage of the Agency's data. Troubleshooting and support activities will utilize secure logging, audit records, and monitoring processes based on FedRAMP High and applicable NIST SP 800-53 requirements.

4.3.3.3.3.3 Dedicated Technical Account Manager assigned to the Agency.

Infocap has assigned Ken Zink to serve as the Agency's Technical Account Manager (TAM) to the Agency as the primary point of contact for support coordination, issue escalation, operational reporting, and ongoing service management. The TAM will coordinate support activities, incident escalation, service reviews, usage reporting, workflow optimization discussions, roadmap updates, and communication between the Agency, Infocap, and Tungsten Cloud Services. The TAM will also support monthly service reviews, quarterly business reviews, operational-status reporting, and continuous-improvement activities associated with the Agency's permitting environment.

4.3.3.3.3.4 Monthly service review meetings and quarterly business reviews

Infocap will conduct monthly service review meetings and quarterly business reviews with the Agency to support operational oversight, service transparency, and continuous improvement. Monthly service reviews will include SLA performance, support-ticket status, incident trends, open risks, maintenance activities, workflow performance, integration status, security events, and operational support metrics. Quarterly business reviews will include usage trends, workflow analytics, token consumption, AI-assisted processing performance, model updates, roadmap planning, training needs, operational improvements, and governance updates.

4.3.3.3.3.5 Additional AI system training

Infocap will provide AI system training activities focused on machine learning model refinement, document intelligence optimization, extraction-model improvement, and AI-processing accuracy enhancement within the Agency's permitting environment. Training activities will include supervised model training, validation-set creation, extraction tuning, classification refinement, prompt optimization, GraphRAG/RAG refinement, confidence-threshold tuning, exception-pattern analysis, feedback-loop incorporation, and Human-in-the-Loop (HITL) validation workflows designed to improve AI-assisted processing accuracy, consistency, explainability, and operational performance.

AI training may utilize reviewer feedback, corrected extraction results, benchmark datasets, workflow outcomes, approved permit records, reviewer-approved classifications, GIS validation findings, and operational analytics to improve document classification, OCR accuracy, metadata extraction, technical-review assistance, and workflow-routing performance. Training and refinement activities will operate within controlled governance processes including model validation, testing, sampling, approval workflows, audit logging, rollback procedures, and operational monitoring to support secure and regulatorily defensible AI-assisted permitting operations. All AI-model training, tuning, validation, monitoring, and optimization activities will remain subject to the Agency's governance controls, reviewer oversight, and approved operational procedures prior to deployment into production workflows.

4.3.3.3.4 Stabilization Warranty: The Vendor shall provide a stabilization warranty beginning immediately after system acceptance. During this period, the Vendor will remediate any automation breakages or system failures caused by minor updates or environment changes at no additional cost.

Infocap will provide a stabilization warranty beginning immediately following written System Acceptance by the Agency. During the stabilization period, Infocap will remediate automation breakages, workflow failures, integration issues, and system disruptions caused by minor updates, approved configuration changes, platform maintenance activities, or environment changes at no additional cost, subject to final warranty terms. Stabilization services will include monitoring, issue tracking, regression testing, defect remediation, rollback support, and prioritized resolution of production-impacting issues to support stable and reliable system operations.

4.3.3.4 Licensing

Infocap will provide all software licenses, subscriptions, and access rights required to support deployment, administration, workflow execution, document processing, AI-assisted services, dashboards, reporting, integrations, monitoring, and ongoing operation of the Agency's permitting solution. Licensing will include access for administrators, automation creators, permit applicants, reviewers, GIS/AoR reviewers, managers, Human-in-the-Loop (HITL) approvers, support personnel, and monitoring/reporting users as defined in the final licensing schedule and implementation scope.

The proposed access model supports approximately 4–7 internal full-access users, an additional 3–5 internal read-only users, and registered external users authenticated through OneLogin or another WVDEP/WVOT-approved identity process. The system will not permit unauthenticated public submission or access. Role-based access controls will restrict dashboards, reviewer queues, HITL approvals, administrative functions, audit logs, and external-user functions according to Agency-approved roles.

All licensed services, dashboard services, reporting functions, automation management capabilities, audit logging, monitoring activities, workflow telemetry, and operational support functions supporting the Agency's solution will operate within controlled FedRAMP Authorized boundary, leveraging FedRAMP High authorized cloud services and security controls consistent with applicable NIST SP 800-53 requirements.

4.3.3.4.1 Licenses for 4 administrative staff to utilize the monitoring/reporting dashboard.

Infocap confirms that our proposed solution will include the required licenses, subscriptions, or authorized access rights for four the Agency administrative personnel to utilize the monitoring and reporting dashboard environment.

Administrative dashboard access will support authorized operational oversight, workflow monitoring, audit-log review, reporting analytics, operational metrics visibility, workflow-status tracking, integration monitoring, SLA reporting, AI-assisted processing oversight, token-usage reporting, and system-health visibility associated with the Agency's permitting environment.

Administrative users will be able to securely access dashboard capabilities through federated authentication, role-based access controls (RBAC), Multi-Factor Authentication (MFA), and

least-privilege authorization policies consistent with the Agency security and operational-governance requirements. Access permissions, reporting visibility, and administrative functions will be centrally managed and auditable through the platform's identity and authorization framework.

4.3.3.4.2 Licenses for 4 staff members to adjust/create automation via web interface.

Infocap confirms that our proposed solution will include licenses or authorized access rights for four the Agency staff members to create, configure, and adjust workflow automation through secure web-based administration interfaces.

Authorized users will be able to manage workflows, business rules, routing logic, forms, dashboards, notifications, integrations, and Human-in-the-Loop (HITL) approval workflows based on assigned permissions and approved change-management procedures.

Access to automation-management functions will be governed through federated authentication, role-based access controls (RBAC), Multi-Factor Authentication (MFA), and least-privilege authorization policies. All configuration changes and automation updates performed through the web interface will be logged and auditable.

4.3.3.4.3 Appropriate access for permit applicants, reviewers, and managers as needed for HITL approval workflows.

Infocap will provide role-based access for permit applicants, reviewers, technical reviewers, GIS/AoR reviewers, supervisors, managers, administrators, and Human-in-the-Loop (HITL) approvers as required to support secure and auditable workflow execution throughout the permitting lifecycle. Access will be controlled through federated authentication, Multi-Factor Authentication (MFA), role-based access controls (RBAC), Access Control Lists (ACLs), and least-privilege authorization policies based on the Agency's security requirements.

Permit applicants will be limited to authorized submission, document-upload, notification, and status-tracking functions. Reviewers, managers, and HITL approvers will have access to assigned work queues, workflow tasks, source documents, AI-assisted recommendations, dashboards, reports, and approval workflows based on assigned permissions and operational responsibilities. All user access, workflow actions, reviewer approvals, AI-assisted processing events, and administrative activities will be logged and auditable to support operational transparency, compliance validation, and regulatory oversight.

4.3.3.5 Regulatory Compliance

Infocap will support the Agency regulatory and security compliance requirements through a secure SaaS deployment hosted within FedRAMP Authorized boundary and security controls consistent with applicable NIST SP 800-53 requirements. Our proposed solution satisfies the Agency's required FedRAMP Moderate security requirements and supports secure processing, workflow orchestration, AI-assisted review, audit logging, monitoring, and operational resiliency for sensitive government permitting and regulatory-review workloads.

Infocap's proposed solution supports compliance alignment through NIST SP 800-53 security-control mapping, centralized audit logging, continuous monitoring, vulnerability management, incident-response governance, Section 508 accessibility conformance, and comprehensive operational-security controls. The platform also supports responsible AI governance through

Human-in-the-Loop (HITL) review workflows, AI auditability, customer-governed AI policies, and human override capabilities at all regulatory decision points.

TotalAgility maintains SOC 2 Type II and ISO 27001 certifications supporting enterprise security, operational governance, confidentiality, availability, and risk-management controls. Infocap will provide applicable compliance documentation, audit-support artifacts, and security evidence under appropriate non-disclosure protections.

Our proposed solution further supports privacy, data ownership, retention governance, right-to-audit provisions, tenant isolation, encryption, role-based access controls, and secure handling of Personally Identifiable Information (PII) and Confidential Business Information (CBI) in accordance with applicable Federal and State regulatory requirements.

4.3.3.5.1 FedRAMP Authorized Environment

Infocap will host our proposed solution within Microsoft FedRAMP Authorized boundary authorized cloud services and security controls consistent with applicable NIST SP 800-53 requirements. Our proposed solution satisfies the Agency's required FedRAMP Moderate security requirements with the entire system, including all components of the agentic workflow, data processing tasks, Azure APIs as well as any third-party AI APIs should the deemed necessary, will reside and operate entirely within the FedRAMP Authorized boundary. The FedRAMP environment supports secure RPA uploads and document processing within the authorized security boundary using encrypted transport, controlled access, audit logging, malware protection, workflow governance, and AI-assisted processing services operating under applicable NIST SP 800-53 security controls.

The TotalAgility platform incorporates enterprise-grade security controls including tenant isolation, Web Application Firewall (WAF) protection, network-security controls, vulnerability scanning, SIEM and SOC monitoring, encryption, federated identity management, role-based access controls, annual penetration testing, and continuous security monitoring. The platform additionally maintains SOC 2 Type II and ISO 27001 certifications supporting operational governance, confidentiality, availability, and risk-management controls.

All production systems, backup repositories, logging services, monitoring systems, AI-assisted processing services, and operational support functions remain within controlled FedRAMP Authorized boundary located within the continental United States. The Agency's data and AI-processing activities are not routed to public consumer AI platforms or non-authorized cloud services. Third-party AI and document processing services will be limited to approved services operating within the authorized hosting environment and governed through contractual, technical, and operational security controls.

4.3.3.5.2 NIST Compliance

Our proposed solution leverages TotalAgility operating within a FedRAMP High authorization boundary, with an Authority to Operate (ATO) issued on March 12, 2026, through the FedRAMP Program Authorization process (formerly JAB P-ATO). The solution supports security, auditability, and operational-governance objectives aligned with applicable NIST SP 800-53 control families. The security architecture uses a shared-responsibility model combining Tungsten-managed SaaS platform controls, Microsoft Azure-hosted infrastructure protections, and customer-configured governance controls. Platform capabilities include RBAC, ACLs,

MFA, federated authentication, SIEM logging, vulnerability scanning, WAF protection, encryption in transit and at rest, audit logging, backups, regional failover, continuous monitoring, and 24x7 SOC operations. TotalAgility maintains SOC 2 Type II and ISO 27001 certifications and supports continuous monitoring, penetration testing, vulnerability management, incident response, and secure software-development practices consistent with FedRAMP-aligned cloud operations. Please see "*Appendix D: NIST 800 Details*" for the NIST 800-53 control matrix.

4.3.3.5.3 Auditability

All workflow, automation, AI-assisted processing, and regulatory-review activities within our proposed solution will be fully auditable. The platform supports centralized audit logging and traceability for workflow transactions, AI-assisted actions, user activity, reviewer decisions, administrative actions, and system events to support operational oversight, compliance validation, forensic analysis, and regulatory accountability.

Audit records will include workflow steps, source documents, retrieved evidence, extracted values, prompts and outputs where appropriate, model responses, confidence scores, reviewer approvals, overrides, generated documents, task assignments, timestamps, exports, routing actions, authentication activity, and final regulatory decisions. Human-in-the-Loop (HITL) validation and override actions are captured to support explainability, reviewer accountability, and responsible AI governance.

The platform supports configurable retention schedules consistent with the Agency records-management and retention policies. Audit logs and operational records may be retained in accordance with the Agency-defined retention requirements or a default five-year retention period subject to the final hosting, storage, and records-management agreement.

TotalAgility supports centralized log management, SIEM integration, Azure Sentinel transmission, SOC monitoring, audit reporting, and configurable log-retention controls. Security events, authentication activity, workflow telemetry, administrative actions, and operational metrics are continuously monitored through centralized monitoring and security operations processes based on FedRAMP and NIST operational-security practices.

4.3.3.5.4 Section 508 Compliance

Infocap will ensure that all user-facing interfaces, workflow components, dashboards, forms, and generated outputs conform to applicable Section 508 accessibility requirements and support accessible user interaction across supported devices and browsers. Our proposed solution is designed to support accessibility, usability, and inclusive access for the Agency personnel, reviewers, administrators, and authorized external users.

The implementation will include accessible forms, keyboard navigation, screen-reader compatibility, semantic HTML, sufficient color contrast, accessible error messaging, focus management, alt text for applicable images and controls, captions or transcripts where applicable, and support for assistive technologies. Accessibility considerations will be incorporated throughout workflow design, user-interface configuration, testing, and deployment activities.

Accessibility validation activities will include automated accessibility scanning, manual accessibility testing, user-interface review, and remediation processes consistent with Section

508 and applicable WCAG accessibility standards. Infocap will support accessibility-related issue resolution and usability improvements identified during testing or operational use.

A current Voluntary Product Accessibility Template (VPAT) and Accessibility Conformance Report (ACR) for applicable platform components will be provided to the Agency upon request.

4.3.3.5.5 AI Governance

Infocap will implement AI governance controls that support secure, transparent, auditable, and responsible use of AI-assisted workflows within the Agency's permitting and regulatory-review environment. The governance framework will address AI model documentation, model configuration management, Agency-controlled data use, prevention of unauthorized model training, bias and error testing, model performance monitoring, drift detection, human override, and model-change governance.

Infocap will document the AI models and AI-enabled components used in the solution, including model/provider, approved use, deployment boundary, model version where available, configuration settings, retrieval sources, prompts or prompt-template identifiers, and any customer-trained or customer-configured training data sources. For third-party foundation models, Infocap will provide available provider documentation, model cards, training-data summaries, and security documentation to the extent made available by the model or platform provider. For customer-trained extraction, classification, computer-vision, or workflow-specific models, Infocap will document the Agency's approved source materials, configuration method, validation approach, and change history.

Infocap will not use the Agency's data, prompts, outputs, permit records, reviewer feedback, or workflow content to train, fine-tune, or improve models for other customers or shared services without the Agency's explicit written authorization. The Agency's data and AI-processing activities will remain within the approved FedRAMP Moderate-or-better authorized boundary and will not be routed to public consumer AI platforms or unauthorized cloud services.

The solution will include ongoing AI quality controls for extraction, classification, retrieval, drafting, recommendation, and routing functions. These controls include benchmark testing, negative testing, prompt-injection testing, source-grounding checks, citation checks, sampling, checking ratios, reviewer override analysis, performance monitoring, and drift detection. Infocap will provide annual AI governance reporting covering model inventory, material model/configuration changes, validation activities, identified issues, mitigation actions, reviewer override trends, and recommended improvements.

The proposed workflow will enforce Human-in-the-Loop review at all consequential decision points. AI-generated outputs may classify, extract, retrieve, summarize, compare, draft, flag, recommend, and route. The Agency's staff will approve, edit, reject, override, remand, issue, or deny. No AI-generated output will become a final regulatory action without authorized the Agency's review and approval.

The system will maintain structured, auditable decision records rather than relying on hidden model chain-of-thought as the official record. The official record will consist of observable decision records, not hidden model chain-of-thought. These records will include, as applicable, prompts or prompt-template identifiers, model identifiers and versions, retrieved source documents, extracted data, confidence scores, validation results, business-rule results, tool calls,

reviewer actions, comments, overrides, approvals, timestamps, and final disposition. These records will support operational transparency, quality assurance, forensic review, appeal support, and regulatory accountability.

TotalAgility will support this governance approach through workflow controls, case management, HITL gates, access controls, audit trails, sampling, benchmarking, versioning, automated deployment, customer-trained model monitoring, and configurable testing and validation processes. Infocap will supplement these platform controls with the Agency's specific AI governance procedures, model-risk review, change control, and operational reporting.

4.3.3.5.6 Annual SOC 2 Type II audit report provided to the Agency with right to audit clause allowing the Agency or designated third party to conduct security assessments.

Infocap will provide applicable annual SOC 2 Type II audit reports to the Agency under appropriate non-disclosure agreement (NDA) protections to support security-review, compliance, and operational-governance activities. The TotalAgility platform maintains SOC 2 Type I and SOC 2 Type II certifications, as well as ISO 27001 certification, supporting enterprise security, availability, confidentiality, operational governance, and risk-management controls.

Infocap will support contractual right-to-audit provisions permitting the Agency or its designated third-party representatives to conduct security assessments, compliance reviews, or operational-security evaluations subject to mutually agreed procedures, scope limitations, scheduling, confidentiality protections, and applicable security-review requirements.

Supporting audit and compliance activities will include review of applicable security documentation, architecture diagrams, operational procedures, vulnerability-management processes, incident-response procedures, audit evidence, penetration-testing summaries, continuous-monitoring evidence, and compliance attestations associated with the final hosting configuration and operational environment.

4.3.3.6 Data Ownership and Exit Strategy

Infocap recognizes the Agency as the sole owner of all the Agency's data, records, documents, metadata, workflow content, audit logs, AI-generated outputs, configuration data, and system-generated information processed or stored within our proposed solution environment. The Agency ownership rights will be contractually protected throughout the operational lifecycle of Infocap's proposed solution and during any transition, termination, or contract closeout activities.

Infocap will provide contractually defined data-export, transition-support, secure-transfer, and system-transition assistance services to support orderly migration of the Agency's data and operational workflows at the conclusion of the contract term or upon authorized termination. Export capabilities will include permit applications, supporting documentation, metadata, audit records, workflow history, AI-generated drafts and outputs, reviewer actions, generated correspondence, reporting data, configuration documentation, and other operational records defined within the final contract and data-retention agreement.

All the Agency's data will remain within the FedRAMP boundary and protected through encryption, access controls, audit logging, retention governance, and secure-transfer mechanisms throughout the transition process. Upon completion of transition activities and the Agency

authorization, Infocap will perform secure data deletion and provide certification of destruction in accordance with applicable Federal and State data-protection, records-management, and media-sanitization requirements.

The exit strategy will support continuity of operations, preservation of regulatory records, protection of sensitive information, and maintenance of auditability throughout transition and decommissioning activities. Transition procedures, retention schedules, export formats, destruction timelines, and operational responsibilities will be finalized during contract negotiation and implementation planning activities.

4.3.3.6.1 All the Agency's data, including application materials, permit documents, and system-generated content, shall remain the sole property of the State of West Virginia.

Infocap acknowledges and contractually recognizes that all the Agency's data processed, transmitted, generated, or stored within our proposed solution environment shall remain the sole and exclusive property of the State of West Virginia. This includes, but is not limited to, application materials, permit documents, metadata, extracted fields, workflow records, audit logs, reviewer actions, public comments, generated correspondence, AI-generated drafts and outputs, system-generated content, reporting data, and final regulatory documents.

No Agency data, workflow content, prompts, AI-generated outputs, or operational records will be sold, shared, reused, or utilized for proprietary model training, commercial purposes, or third-party benefit without explicit written authorization from the Agency. The Agency's data ownership rights will remain protected throughout the operational lifecycle of Infocap's proposed solution, including during backup, disaster recovery, retention, export, transition, and secure-deletion activities.

Infocap will maintain administrative, technical, and contractual safeguards to ensure the Agency retains full ownership, control, and authorized access to all the Agency's data in accordance with applicable Federal and State privacy, records-management, and regulatory requirements.

4.3.3.6.2 Infocap shall not use the Agency's data for any purpose other than providing the contracted services without explicit written authorization.

Infocap confirms that all the Agency's data will be used solely for the purpose of providing contracted services and supporting authorized Agency operational, regulatory, and administrative activities. The Agency's data will not be sold, shared, disclosed, mined, reused, or utilized for any secondary purpose without explicit written authorization from the State of West Virginia.

The Agency's data, workflow content, prompts, permit records, AI-generated outputs, and operational information will not be used to train proprietary, shared, or third-party AI models that benefit other customers without explicit written consent from the Agency. All the Agency's data will remain within the FedRAMP Authorized boundary located within the continental United States and will not be transmitted to public consumer AI platforms, unmanaged AI services, or non-authorized cloud environments.

Infocap will comply with applicable West Virginia artificial intelligence policies, data-governance requirements, and prohibited software or model restrictions associated with the final contract and hosting environment. The TotalAgility platform supports customer-governed control over what data is transmitted to AI-assisted services and model-processing workflows.

Azure Document Intelligence services do not retain customer input data or use customer content for model training purposes. Tungsten-hosted LLM services are configured for no data retention or reuse for model training. Optional AI-related services and configurations will be reviewed and configured in accordance with the Agency security and governance requirements to prevent unauthorized data retention, model training, or information disclosure.

Administrative, technical, and operational safeguards including encryption, access controls, audit logging, retention governance, federated authentication, and Human-in-the-Loop (HITL) review controls will be implemented to support secure, authorized, and auditable use of the Agency's data throughout the lifecycle of Infocap's proposed solution.

4.3.3.6.3 Upon contract termination, Infocap shall provide complete data export within 30 days in open, non-proprietary formats (PDF, CSV, JSON, XML, standard document formats) at no additional cost.

Infocap confirms that, upon contract termination or authorized transition request, the Agency will receive a complete export of the Agency's data within thirty (30) days at no additional cost. Data exports will be provided in open, non-proprietary, and industry-standard formats including PDF, CSV, JSON, XML, and standard document formats to support transition, migration, records retention, and operational continuity requirements. Export packages will include application records, uploaded documents, generated correspondence, extracted fields, metadata, audit logs, workflow history, reviewer actions, AI-generated drafts and outputs, decisions, source references, reporting data, configuration documentation, and other operational records defined within the final contract, retention policy, and exit strategy agreement. Infocap will provide reasonable transition-support assistance to facilitate secure transfer, validation, and migration of the Agency's data and operational records to a successor environment or customer-managed repository. Data exports will be transmitted through secure, encrypted transfer mechanisms and protected through access controls, audit logging, and chain-of-custody procedures during transition activities. All the Agency's data will remain the sole property of the State of West Virginia throughout the transition process. Upon completion of authorized export and transition activities, Infocap will perform secure data deletion and provide certification of destruction in accordance with applicable Federal and State records-management, privacy, and media-sanitization requirements.

4.3.3.6.4 Infocap shall provide transition assistance for up to 90 days following termination to support migration to a replacement system.

Infocap confirms that it will provide transition assistance for up to ninety (90) days following contract termination or authorized transition activities to support orderly migration to a replacement system or customer-managed environment. Transition-support services will be coordinated with the Agency and any authorized successor vendor to help ensure continuity of operations, preservation of regulatory records, and secure transfer of the Agency's data. Transition assistance will include data-export validation, secure data transfer, data mapping, knowledge transfer sessions, operational documentation, workflow and configuration reviews, migration-support activities, interface coordination, and technical consultation related to the existing solution environment. Infocap will also provide reasonable support for configuration explanation, audit-log interpretation, retention-policy review, and workflow transition activities associated with the final exit plan. All transition activities will be conducted using secure

transfer mechanisms, access controls, audit logging, and confidentiality protections meeting applicable Federal and State security and privacy requirements. Operational responsibilities, transition timelines, support scope, and final deliverables will be coordinated and documented as part of the contract closeout and transition-planning process.

4.3.3.6.5 All the Agency's data shall be securely deleted from vendor systems within 60 days of confirmed data transfer, with written certification of destruction.

Infocap confirms that all the Agency's data will be securely deleted from vendor-managed systems and controlled hosting environments within sixty (60) days following confirmed data transfer and completion of authorized transition activities, subject to applicable legal-hold requirements, backup-retention obligations, regulatory requirements, and contractual provisions. Secure deletion procedures will be performed in accordance with applicable Federal and State records-management, media-sanitization, privacy, and information-security requirements. Deletion activities will ensure removal of the Agency's data from production systems, storage repositories, workflow services, AI-processing environments, temporary processing locations, and associated operational support environments in accordance with approved retention and destruction procedures. Upon completion of authorized deletion activities, Infocap will provide the Agency with written certification of destruction identifying the scope of deleted data, applicable deletion procedures, and completion status. Retention schedules, backup-handling procedures, destruction timelines, and secure-deletion responsibilities will be documented within the final data-processing agreement, records-retention policy, and contract exit plan.

4.4. Qualifications and Experience

Infocap brings more than a decade of production Agentic AI experience, at scale demonstrated through with 2013-era RPA-based modernization and evolving into governed digital workforces combining decision automation, machine learning, human workers, and AI as across millions of adjudications and tens of millions of documents. Infocap has purposefully organized a delivery team that combines the exact disciplines the Agency needs for this program: agentic AI, geospatial analysis, construction and permitting modernization, complex document processing, workflow automation, and implementation in highly regulated environments.

In addition, Genus adds highly relevant experience with TotalAgility and permitting-related document modernization, including current work supporting a building-permitting environment involving legacy system access, document intake, classification, extraction, engineering and planning documents, human validation, and enterprise content management integration. Infocap adds deep experience building governed digital workforces in regulated environments where human and digital workers follow the same policies, rules, controls, and audit expectations. Together, Infocap and Genus provide a differentiated team uniquely aligned to the Agency's challenge: combining agentic workflow, GIS-aware evidence handling, complex document understanding, policy-driven automation, and regulated case adjudication into a practical, production-ready UIC permitting solution.

4.4.1. Qualification and Experience Information

Infocap's expertise in Agentic AI is grounded in production experience building human-centered digital workforces, not in generic chatbot demonstrations or isolated automation scripts. We understand that digital transformation requires rethinking work around outcomes rather than discrete tasks. In complex public-sector operations, the problem is not simply how to automate one step, but how to coordinate intake, research, decision support, exception handling, escalation, quality assurance, reporting, and auditability across a full lifecycle. Infocap designs agentic systems so that human workers, AI agents, and robots use the same systems, follow the same rules, and are subject to the same reporting, quality, and accountability expectations. This is the foundation for reliable automation in regulated environments.

Infocap distinguishes deterministic RPA from agentic automation. Robots are valuable because they execute defined tasks consistently, but they do not independently interpret ambiguous business events. Agentic automation adds the missing layer: context, knowledge retrieval, rules, workflow orchestration, collaboration, and escalation. Infocap has designed specialized Agentic AI Design patterns which capture not only what action occurred, but why it occurred, preserving action history, context, causality, auditability, and defensibility.

Infocap's approach combines Retrieval-Augmented Generation with directed workflow structures such as DAGs to make agentic work safer and more transparent. RAG provides contextual knowledge from permitted data sources; DAGs structure task progression, reduce ambiguity, prevent infinite loops, enable parallelization, and improve decision transparency. Infocap also understands that effective AI requires behavioral context, situational context, and semantic context, so agents operate with the right rules, case history, domain boundaries, and business meaning.

This expertise has produced measurable results in regulated adjudication environments: compound efficiency gains exceeding 500%, year-over-year positive ROI, automation of 30%–70% of complex manual work, more than one-third of casework volume completed without human case worker intervention, and complex casework performed 2-4 times faster with greater accuracy and consistency. That experience is directly relevant to the Agency's need for workflow-based agentic AI, document-heavy permitting, policy-driven review, RAG/source grounding, human-in-the-loop governance, GIS-aware evidence handling, legacy system accommodation, and auditable regulatory decisions.

4.4.1.1. Company Background and Years of Experience

Founded in 2012, Infocap offers over a decade of proven experience designing and supporting digital workforces for highly regulated government adjudication environments. Its relevant experience includes intelligent document processing, OCR/classification, robotic process automation, decision automation, dynamic work assignment, operational analytics, auditability, and human/digital worker orchestration at federal scale. The strongest proof point is Infocap's on-going role with the CMS Eligibility Support, where the operating model combined intake and ingestion, verification, research and resolution, consumer outreach, eligibility determination, final status notification, notices, call-center interactions, business operations, IDP, RPA, BPM, decision automation, machine learning, and operational intelligence.

That experience is directly relevant to the Agency's Agentic workflow ambitions and inevitable challenges. While CMS Eligibility Support was not an environmental permitting program, it required the same core disciplines the Agency needs: document-heavy intake, policy-driven adjudication, secure legacy system interaction, dynamic work routing, repeatable rules-based outcomes, human oversight, SLA management, audit trails, and scalable automation. The same operating pattern applies to UIC permitting: transform documents into trusted data; apply deterministic rules; route work to the right human or digital agent; preserve auditability; automate repeatable steps; and escalate complex matters to human experts.

For the Agency, this translates into Digital Intake Specialist agents, completeness-review agents, RAG/source-grounding agents, GIS/AoR evidence agents, drafting agents, HITL decision gates, RPA-supported legacy access, and auditable workflow-state management.

4.4.1.2. Relevant experience with agentic AI or autonomous systems (References)

Project Name	**CMS ACA Eligibility Support**
Client	Centers for Medicare & Medicaid Services
Scope	Since 2016 (in partnership with prime contractor Serco) Infocap built a digital workforce and Agentic Workflows on top of TotalAgility (running within AWS) operating within a highly regulated environment, performing end-to-end application adjudication spanning intake and ingestion, verification, research and resolution, consumer outreach, eligibility determination, notice generation, consumer interactions, and final determination. The Agentic Workflows leverage AI services which act on multiple external data feeds as well as leveraging AI-powered RPA to securing access to government systems.
Dates	2016-Present
Contact	Paul Coviello, Program Director, pcoviello@serco-na.com
Relevance to the Agency	The CMS ACA Eligibility Support program demonstrates Infocap's ability to design and support digital workforces for highly regulated, document-intensive adjudication environments where outcomes must be consistent, auditable, policy-driven, and supported by human oversight. Although the CMS program was not an environmental permitting program, its operating pattern is directly relevant to the Agency's UIC e-permitting requirements: ingest complex document packages, classify and extract data, apply deterministic rules, route work to the right human or digital agent, preserve auditability, automate low-complexity repeatable steps, and escalate complex matters to human experts. Infocap built digital agents operating under the same program rules, controls, reporting, and quality expectations as human workers, including secure access to government systems through APIs and legacy web-based user interfaces. It also demonstrated dynamic work assignment, decision automation using thousands of explicit business rules, operational intelligence, audit trails, SLA management, and automation during burst periods. Source materials report compound efficiency gains exceeding 500%, positive year-over-year ROI on intelligent automation investments, 30%–70% or more of previously manual work automated end-to-end, more than one-third of casework volume completed without human intervention, and complex casework performed 2–4 times faster with greater accuracy and consistency. For the Agency, the same proven pattern translates into Digital Intake Specialist agents, completeness-review agents, RAG/source-grounding agents, GIS/AoR evidence agents, drafting agents, HITL decision gates, RPA-supported legacy access, auditable workflow-state management, and repeatable policy-driven permitting outcomes.

This reference below for Los Angeles Department of Building and Safety is included as a highly relevant example TotalAgility-based modernization of a public-sector e-permitting environment involving multi-channel permit intake. The same proven pattern applies directly to UIC permitting: receive complex technical submissions, process forms, maps, plans, drawings, and supporting documents, route exceptions to reviewers, preserve auditability, and integrate approved records with downstream systems without disrupting existing applicant-facing services.

Project Name	**Los Angeles Department of Building and Safety E-Permitting**
Client	City of Los Angeles
Scope	Genus Technologies is performing modernization of a document intake, capture, and workflow processing environment supporting Los Angeles Department of Building and Safety permitting operations. The project includes migration of legacy Kofax Capture and IDIS-based workflows to Tungsten TotalAgility, consolidation of approximately six capture configurations, automation of document classification and extraction, and integration with IBM ECM. The scope supports permit processing workflows, planning documents, and engineering drawings, with multi-channel ingestion through scan, email, portal, and API channels, plus human-in-the-loop validation. This work aligns with LADBS's broader e-permitting and plan-review environment: LADBS identifies ePlanLA as a secure electronic plan-review method for submitting plans and construction project documents, with plan check performed electronically through verification and permit issuance, and LADBS PermitLA supports online express permitting, fee calculation, and e-permit payment status.
Dates	Currently in progress
Contact	Dinh Trinh, Systems Analyst, Technology Services Bureau, LADBS; Greg Wilcox, Director of Systems, Technology Service Bureau, 213-274-3449 Greg.wilcox@lacity.org
Relevance to the Agency	This reference is directly relevant to the Agency because it demonstrates TotalAgility-based modernization in a public-sector e-permitting context involving document-heavy regulatory intake, plan review, engineering drawings, workflow processing, human validation, and enterprise content management integration. LADBS permitting supports construction, alteration, and repair work on buildings within Los Angeles, and its public plan-review environment includes ePlanLA for electronic submission of plans, drawings, and construction project documents, as well as PermitLA for express permit services. While the LADBS project is not a UIC or environmental permitting engagement, the operating pattern is highly transferable to the Agency: receive permit-related submissions from multiple channels, migrate legacy capture configurations, classify and extract document content, support review of technical and engineering materials, route exceptions for human validation, and export approved records and metadata to an enterprise ECM repository. Genus's role as a systems integrator with more than 25 years of experience in document automation, content services, process transformation, intelligent automation, AI, and cloud solutions strengthens the relevance of this reference. Genus also publicly positions its Tungsten Automation practice around AI-powered workflow and document automation, TotalAgility, Tungsten RPA, Transformation, Import Connector, and related Tungsten technologies. For the Agency, this experience supports the proposed approach of using TotalAgility as the workflow, evidence, and review-orchestration layer for e-permitting: modernizing legacy Kofax-style capture processes, automating document classification and extraction, supporting complex drawings and plans, enforcing human-in-the-loop validation, preserving auditability, and integrating approved records with enterprise repositories and downstream systems without disrupting existing applicant-facing services.

The U.S. Army HRC reference demonstrates Infocap's ability to modernize secure, mission-critical, document-driven workflows using TotalAgility, including complex document ingestion, classification, extraction, validation, work queues, export to downstream systems, controlled deployment, testing, defect resolution, and sustainment in hardened government environments.

For the Agency, the same disciplined approach applies to UIC permitting: secure intake of complex application packages, Digital Intake Specialist processing, administrative completeness review, technical evidence routing, HITL validation, legacy-system synchronization, audit-ready evidence records, and a governed TotalAgility workflow, evidence, and review-orchestration layer.

Project Name	**U.S. Army HRC Secure Evaluation Workflow Modernization & TotalAgility Customization**
Client	U.S. Army Human Resources Command (HRC)
Scope	Infocap supports the U.S. Army Human Resources Command's Soldier Evaluations Program at Fort Knox, KY with secure enterprise workflow modernization, TotalAgility customization, document processing, and operational sustainment across NIPRNet and SIPRNet, including secure installation, process migration, extraction/validation rebuilds, automated ingestion/export, testing, defect resolution, and training.
Dates	July 2019-Present
Contact	Stephen Chevalier, HRC CoE Director, stephen.c.chevalier.civ@army.mil
Relevance to the Agency	Demonstrates Infocap's ability to modernize highly-sensitive, mission-critical document-driven workflows in controlled government environments while preserving mission continuity, compliance, data quality, and operational sustainment. Our work involves secure intake of complex document packages, classification, extraction, validation, quality control, work queue management, controlled reviewer workflows, export to downstream systems of record, testing, defect resolution, and production sustainment. Infocap's HRC work includes migration to TotalAgility, secure deployment across the Secret Internet Protocol Router Network, is the U.S. Department of Defense's and Department of State's private, classified intranet, STIG-compliant deployment on hardened Army systems, and configuration of server prerequisites, SQL databases, service accounts, user groups, resources, Active Directory synchronization, environment-specific variables, field validation rules, formatters, work queues, and versioned deployment artifacts. The engagement also included safeguards to prevent PII or sensitive data from moving to inappropriate environments, lower-environment testing before production replication, end-to-end testing, UAT, defect handling, corrective action, production promotion, administrator/user training, architecture documentation, solution design documentation, delivered-solution documentation, and knowledge transfer. For the Agency, the same disciplined approach translates into secure UIC intake workflows, document-heavy application processing, Digital Intake Specialist functions, administrative completeness review, technical evidence routing, human-in-the-loop validation, legacy system export or synchronization, audit-ready evidence records, secure configuration, controlled deployment, operational visibility, and sustainment. This experience is directly relevant to the Agency's need for a governed TotalAgility-based workflow, evidence, and review-orchestration layer.

4.4.1.3. Relevant Key Personnel and Roles

This is not an assembled-at-bid team. The core Infocap personnel have worked together for many years on the company's most advanced digital workforce and agentic automation initiatives, including the regulated adjudication, document intelligence, RPA, decision automation, and workflow modernization projects included as references in this proposal. Those projects demonstrate the team's ability to transform complex document packages into trusted data, apply rules consistently, coordinate human and digital workers, preserve auditability, and deliver repeatable outcomes in mission-critical government operations.

For this opportunity, Infocap has also included its longtime partner, Genus Technologies, to strengthen the team's geospatial, permitting, construction-document, and Tungsten platform expertise. Infocap and Genus have collaborated for nearly a decade, and we are bringing that partnership forward because the Agency's UIC requirements demand more than AI, more than OCR, and more than workflow alone. The solution requires the combined ability to process complex permit packages, interpret engineering and map-based evidence, integrate GIS outputs into regulated review workflows, orchestrate agentic review steps, and maintain defensible Human-in-the-Loop decision controls.

Role	Responsibility	Staff
Project Executive	Executive oversight, contract accountability	Nathaniel Palmer
Project Manager	Schedule, budget, scope, risks, communications	Joe Caplinger
Business Analyst Lead & Delivery Manager	Leads requirements, aligns stakeholders, coordinates delivery, ensures outcomes	Wanda Matthews
Solution Architect	Overall TotalAgility architecture and integration design	Ray Reaux
TotalAgility Workflow Lead	Workflow configuration, work queues, dashboards, HITL gates	Robert Coop
AI/RAG Lead	RAG, prompts, LLM configuration, hallucination controls, AI governance	Michael Torres
GIS Integration Lead	GIS integration, AoR workflow, spatial validation coordination	Ben Cole
Security & Compliance Lead	FedRAMP/NIST/SOC 2/ISO/security controls and ATO artifacts	Jason Hall
Data Migration & Integration Lead	ERIS/ESS/external data integration and exports	Mary-Ann Erskine-Pourier
QA/Test Lead	Test plans, UAT, regression testing, acceptance criteria	Patrick Koch
Training Lead	Role-based training, materials, adoption support	Theresa Resek
Technical Account Manager	Ongoing service reviews, support escalation, continuous improvement	Ken Zink

Role	Project Executive
Resource	Nathaniel Palmer, CEO, Infocap
Qualifications	Best-selling author and globally recognized authority in the field of AI 30+ years in systems architecture and Digital Transformation; provides executive-level technology strategy, innovation roadmaps, and program oversight. Proven contract and program accountability — Chief Architect on the CMS Eligibility Support program since 2015, with delivery responsibility across thousands of users and 100M+ records; introduced Intelligent Automation that reduced ODCs and lowered FUPs on a major federal program. Led intelligent automation using AI, machine learning, RPA, and decision automation, delivering a 200% productivity gain across a workforce of more than 4,000 support workers. Established Agile practices while achieving CMMI Level III; industry-recognized with the WfMC Marvin L. Manheim Award (2019), Innovation Pulse Award for Intelligent Automation (2019), and WfMC Global Excellence in Case Management (2017).
Degree/ Certifications	Postgraduate study, Babson College, Wellesley, MA Postgraduate study, University of Oxford Saïd Business School, Oxford, UK B.S., Computer Information Systems, Bentley University, Waltham, MA
Relevant Experience	Served as Chief Architect for CMS Eligibility Support, delivering digital transformation strategy and business analysis for a major regulated federal adjudication program. Managed architecture and delivery of highly complex applications supporting millions of customers, thousands of users, and 100+ million data records. Led migration of 1,000+ on-premise servers across three data centers into a secure commercial cloud environment with FISMA controls, FIPS 140-2, encryption, and petabytes of sensitive data. Modernized CMS Eligibility Support systems by introducing Agile, document automation, AI/ML, decision automation, advanced analytics, and RPA. Served as lead architect for a $100M FDA modernization effort responding to the Food Safety Modernization Act, demonstrating relevant regulated-government modernization experience. Program Chief Architect & Practice Lead, SRA International: integrated $2B in systems modernizing FDA, CDC, and VA; lead architect on a $100M FDA modernization following the 2011 Food Safety Modernization Act.

Role	Project Manager
Resource	Joe Caplinger
Qualifications	25+ years of project and program management across commercial and federal agencies, focused on BPM, Electronic Document Capture, and ECM; direct accountability for schedule, budget, scope, risk, and customer communications. Owned full-SDLC delivery (planning, requirements, design, development, testing, installation, evaluation) on federal contracts including USCIS and CMS Eligibility Support; serves as liaison between technical and business teams and manages JIRA across IFP, FRD, DOCINGSTN, QA, IT Request, and DBA workstreams. Demonstrated financial and contract accountability, including ownership of a $16M annual budget with monthly/quarterly/annual forecasting and reporting to senior leadership and the customer.
Degree/ Certifications	Certified SAFe 5 Agilist
Relevant Experience	Project Lead, Infocap (Jan 2018–Present): full oversight of MIDPS — project/maintenance monitoring, release management, resource and JIRA board management, team status reporting, production environment monitoring, and PWS conformance across all SDLC phases. Service Delivery Manager, ACA, Exela Technologies/Novitex (Sep 2013–Dec 2017): managed mail receipt and digitization for the Federally Facilitated Marketplace — 9M+ consumer transactions and 40M+ images/year, up to 440 staff across KY and OK, $16M annual budget. Program Manager, USCIS IDDMP, Datatrac (May 2005–Jun 2007): built out and ran A-File digitization in a NARA 36 CFR 1234 Level 3 facility, processing ~1M A-Files and 250M+ images annually.

Role	Business Analyst Lead & Delivery Manager
Resource	Wanda Y. Matthews, PMP
Qualifications	Program leader with a track record directing $25M+ federal programs and multi-site initiatives on time and within budget, spanning workforce management, operational transformation, and business analysis in public and private sectors. Established and led a business analysis practice that standardized requirements, documentation, and QA across the SDLC — meeting compliance standards and cutting costly rework; hands-on with workflow logic and business-rule translation between operations and technical teams. Strong change-management and adoption discipline — designed enterprise training and stakeholder communications that drove sustained tool adoption and reduced development time by 40%.
Degree/ Certifications	M.S., Project Management, Walden University B.A., Broadcast Management, Clark Atlanta University Advanced Leadership Program, University of Oxford, Saïd Business School McKinsey Management Accelerator, McKinsey & Company Project Management Professional (PMP)
Relevant Experience	Senior Manager, Workforce Management (2019–2023): directed a multi-year workforce optimization and analytics portfolio; led cross-functional delivery for AI-enabled operational improvements across North America; implemented an AI-enabled WFM solution (geofencing, mobile time capture, advanced scheduling) achieving 95% compliance and reduced labor-charge risk. Manager, Workforce Management (2019–2021): established and led the BA practice ensuring compliance-aligned requirements, documentation, and workflows; directed system implementations, feasibility studies, and process improvements that strengthened compliance while lowering cost; standardized documentation and QA across the SDLC. Manager, Business Analysis Practice & Program Manager (2010–2019): introduced AI to a federal benefits program serving 20M+ consumers; ran global rollout of a Workforce Optimization framework using predictive analytics and rules-based automation for explainable, auditable decision support; transformed tens of thousands of SOP pages into business-owned decision models.

Role	Solution Architect
Resource	Ray Reaux
Qualifications	30+ years in software/database/network architecture; recognized SME in document imaging and intelligent automation, architects, designs, implements, and manages complex KTM/KTA-based document imaging and process orchestration solutions, including RPA integrations. Hands-on integration designer and developer (Java, .NET, Kofax RPA) with deep experience integrating OOTB and open-source document management products. Cloud and security-focused, leading the migration of multiple on-prem applications to AWS, currently architecting KTA MIDPS and RPA into AWS with cost/performance optimization; ensures sensitive-data access and transmission comply with Federal IAM/PII policies and PKI authentication.
Degree/ Certifications	AWS Certified Solutions Architect
Relevant Experience	Developer II, Infocap (Feb 2016–Present): architects/designs/implements complex document imaging and process orchestration; on MIDPS serves as Sr. Cloud Engineer, Sr. KTA/RPA Engineer, and Solution Ops Analyst — architecting KTA MIDPS/RPA into AWS and designing mailroom enhancements (name-variance matching, Spanish translation, FFM EBP integration). Chief Technology Officer, Servient, Inc. (Aug 2005–Jan 2016): set tech direction; chief architect/designer for proprietary platform built on JBoss, Struts, PostgreSQL, Linux, SOLR, Hadoop/HBase; led migration of server systems from co-located facility to Rackspace and ultimately AWS. Senior Software Consultant, Virginia Supreme Court, Java/J2EE developer on the eMagistrate system; unit/integration/performance testing (Apache JMeter) and WebSphere deployment/security configuration.

Role	TotalAgility Workflow Lead
Resource	Robert Coop
Qualifications	30+ years in enterprise software with the last 19 dedicated to architecting, deploying, and supporting Kofax, including stable, highly available, scalable KTA environments following vendor best practices he helped author while at Kofax. Hands-on KTA workflow configuration on MIDPS — process, UI, and business-rule development (scripting and coding) directly applicable to workflow configuration, work queues, dashboards, and human-in-the-loop (HITL) gates. Specializes in Intelligent Document Recognition (IDR), distributed capture, and advanced ML-driven classification/extraction models supporting validation and HITL review experiences inside TotalAgility.
Degree/ Certifications	Tungsten Automation (formerly Kofax) TotalAgility Master Class Certification Achieved KC3/KCCC (Certified Capture Consultant) - multi-certification title from Tungsten Automation (formerly Kofax) AWS Accredited Business Professional AWS Accredited Technical Professional AWS Accredited Cloud Economics
Relevant Experience	Developer II, Infocap (Jan 2013–Present): designs and manages complex document imaging and process orchestration; on MIDPS serves as Infrastructure Maintenance/Monitoring, Sr. App QA, Sr. Solution Engineer, and Cloud Engineer — KTA process/UI/business-rule development, advanced ML transformation, and integration of BasisTech, AWS services, Kodak, and RPA. Professional Services Architect, Kofax, Inc. (Oct 2004–Dec 2012): one of two Americas Capture Architects; delivered advanced solution designs, customer health checks, and infrastructure audits with best-practice recommendations to increase throughput and reliability. Senior Professional Services Consultant, Kofax: technical lead on Kofax's largest and most complex deployments — Wells Fargo Home Mortgage (7 production environments, 128+ servers, 400+ workstations), Coca-Cola worldwide AP (5 regions), and the State of Texas Vital Statistics solution with custom VB/C# validation and QC modules.

Role	AI/RAG Lead
Resource	Michael Torres
Qualifications	Focused on scaling customer AI operations and moving organizations from scattered AI activity into governed, measurable, secure, operationally useful AI operating models. Federal AI, data, cybersecurity, and governance leader with senior experience across the Department of the Air Force CIO and U.S. Space Force, led Departmentwide IT/AI/data/cybersecurity governance and compliance analytics. Deep expertise in AI strategy and governance, workforce enablement, human-AI work systems, human-in-the-loop design, AI risk and oversight, and AI-enabled systems design anchored by secure cloud architecture, cybersecurity, and federal acquisition experience.
Degree/ Certifications	Doctor of Education, Human and Organizational Learning (Doctoral Candidate), The George Washington University Master's Degree, Management Information Systems, Florida International University Claude Certified Architect – Foundations, Anthropic (exp. Jun 2029) AWS Certified Solutions Architect – Professional, Amazon (exp. Jun 2028) AWS Academy Accredited Educator (exp. Jun 2028) Certified Ethical Hacker, EC-Council (exp. Jun 2028) Certified EC-Council Instructor, EC-Council (exp. Jun 2028) Certified Scrum Product Owner & Certified Scrum Master, Scrum Alliance (exp. Mar 2029)
Relevant Experience	Leads AI strategy, governance, workforce enablement, human-AI work systems, AI risk oversight, and AI-enabled systems design; develops governed AI operating models that support measurable, secure, and scalable AI adoption. Department of the Air Force CIO: led Departmentwide IT, AI, data, and cybersecurity governance and compliance analytics, supporting enterprise governance across the U.S. Air Force and U.S. Space Force. SpaceVerse Architect & Digital Infrastructure Division Chief, U.S. Space Force CTIO: architected and led SpaceVerse while supporting agency-wide IT strategy and portfolio leadership; designs human-AI work systems with HITL controls, role clarity, oversight, accountability, and measurable outcomes.

Role	GIS Integration Lead
Resource	Ben Cole
Qualifications	15+ years as a Technical GIS Solutions Architect integrating complex geospatial workflows into core IT infrastructure; proven record establishing spatial-data validation pipelines, regulatory evidence records, and auditable GIS deliverables for decision-support systems. Coordinates GIS deliverables across engineering, hydrogeology, AI/RAG, and legal review on high-stakes infrastructure and regulatory programs — directly applicable to AoR workflow coordination and cross-team spatial review; expert in multi-source cross-checks, topology correction, and zero-error delivery on UIC permitting workflows. Hands-on enterprise GIS integration (ArcGIS REST/FeatureServer, HIFLD, Cloudflare R2, Supabase, Netlify) with strong Python automation (arcpy, geopandas, GDAL/ogr2ogr) — builds ArcGIS Pro layout automation and arcpy batch exports producing 80–100+ map products per engagement.
Degree/ Certifications	B.S., Geography / Geographic Information Systems, University of Alabama
Relevant Experience	Technical GIS Solutions Architect / Geospatial Consultant, BC Mapping & Analytics (2020–Present): designs spatial-data validation pipelines including CAD-to-GIS integration and georeferencing; leads cross-functional GIS coordination as the technical bridge between spatial workflows, enterprise IT, and non-technical stakeholders; deploys interactive Mapbox/MapLibre GL JS web maps with layered filtering and secure admin controls. GIS Analyst, Geospatial Services Division (2015–2020): managed end-to-end GIS data acquisition, multi-source cross-checks, and cleanup for multi-jurisdictional infrastructure and environmental projects; created automated topology-validation workflows ensuring zero-error delivery to backend mapping systems and electronic record preservation. Regulatory Accreditation GIS Framework & Federal Safety Grant Parcel Audit (430 parcels): produced 80–100+ ArcGIS Pro regulatory maps with Closest Facility / Location-Allocation models, arcpy batch export across 13 call categories, spatial-statistics package, and review-board dashboard; led a 430-parcel audit integrating zoning, future land use, transit, and appraisal records into a federal-grant-compliant evidence package.

Role	Security/Compliance Lead
Resource	Jason Hall
Qualifications	30+ years on mission-critical federal civilian and defense programs (DHS, CMS, HHS, DoD, DOE, DISA, USAF Space Command, Army, Navy); known for stabilizing high-risk initiatives and leading modernization in regulated environments. Cybersecurity and cloud executive with deep expertise in governance, Zero Trust, cloud transformation, IAM, DevSecOps, and operational resiliency across AWS and large-scale distributed systems. Aligns security, compliance, and enterprise architecture with mission objectives; leads cross-functional teams and partners with executives to deliver secure, scalable Federal solutions.
Degree/ Certifications	AWS Cloud Practitioner Essentials Splunk Accreditation JNCIP-ENT JNCIS-ENT JNCIA-Junos
Relevant Experience	Chief Information Security Officer, Infocap (Jul 2024–Present): leads compliance and security engineering aligned with FedRAMP, FISMA, NIST 800-53/171, CMMC, TIC 3.0, and VA RMF; oversees cloud security modernization, DevSecOps, ATO support, POA&M remediation, vendor reviews, DR/BCP, and security architecture for contact center, AI/ML, automation, and IDP platforms. Led the Authority to Operate (ATO) process with CMS OIT for TotalAgility running within a FedRAMP AWS cloud enclave, and continued to maintain the ATO through multiple recertifications. Senior Architect, Citizant (Oct 2022–Jul 2024): supported the DHS CTO Directorate (HQTGD) on enterprise IT governance, modernization, and innovation across DHS HQ and Components — Program Health Assessments, TechStat evaluations, EAB facilitation, and SELC tailoring aligned with Agile, SecDevOps, ITAR, and Federal IT standards. Solution Architect, Serco North America (Jul 2008–Dec 2021): led enterprise architecture, cloud modernization, and cybersecurity for CMS, DHS, DISA, and DoD — deployed AWS WorkSpaces/AppStream/Connect/Chime, Appian BPM, Zscaler Zero Trust, DLP, and NGFW; transitioned 2,400 employees to secure remote operations during COVID-19 using cloud-native and Zero Trust architectures.

Role	Data Migration / Integration Lead
Resource	Mary-Ann Erskine-Pourier
Qualifications	20+ years across Health, Banking, and Energy specializing in ECM — has worked from the vendor, partner, and customer sides on ECM design, integration, upgrade, and implementation. Hands-on across the full implementation lifecycle (analysis, scanning/fax, records management, HA/BC, support) using Agile and Waterfall; translates business needs into technical solutions and drives software quality through completion. Deep integration stack: IBM Content Manager, FileNet P8, Content Navigator, WebSphere; SQL Server, Oracle; VB/.NET, Java/JavaScript; OpenText Documentum D2/Extended ECM, Capture/InputAccel, RightFax; scanning (IBML Fusion, Kodak i5650, Kofax/Tungsten).
Degree/ Certifications	IBM FileNet Image Services Administration and Support Professional v1 Agile Product Owner IBM SVP Primary Support Provider Mastery Professional v1 Oracle SQL DBA HP Advanced System Administration
Relevant Experience	Customer IBM P8 Software Upgrades & IBM ECM DR/HA Design (2024): planned and documented IBM P8 upgrades aligned to customer OS/database environments, led phased non-prod-to-prod rollouts, and designed IBM FileNet DR/HA strategies (backup, restore, failover) and migration plans from Image Services to P8. ECM Records Management Framework (2023) & IBM P8 Agile Product Owner (2017–2019): built a framework integrating project knowledge, vendor best practices, and RM/ECM team input; delivered training on retention and deletion strategies; as PO/Team Lead, migrated legacy systems to an IBM P8 EDMS with .NET, REST, JavaScript, and SQL, leading UAT and performance tuning. IBM FileNet International Support Team Lead — Implementation & Upgrades (1992–2001) and Large Document Scanner Conversion (2005, PCI Removal 2010): led global onsite FileNet installations/upgrades and 'Follow the Sun' support from Ireland; integrated Capture/Fax/Print/SAP with ECM; replaced Kodak with IBML scanners for Healthcare/Medicare Part D volume, with 2010 PCI removal for compliance.

Role	QA/Test Lead
Resource	Patrick Koch
Qualifications	Process Automation Consultant with 20+ years of software engineering on intelligent document management and business processing — directly applicable to authoring test plans, defining acceptance criteria, and executing regression testing on TotalAgility/KTA solutions. Enterprise Kofax experience since 2010 (Kofax Capture and Transformation Modules) supporting test design for OCR/IDR accuracy, classification/extraction validation, and end-to-end workflow verification; produces strong UAT scripts, acceptance criteria, and user-facing artifacts thanks to a non-technical user perspective. Decade-plus cleared experience on highly confidential and classified defense projects with deep understanding of secure environments; hands-on test-automation stack including .NET (ASP.NET, C#, VB.NET, ADO, VBScript, XML), Visual Studio, relational databases, Windows server admin, Remedy, SharePoint, and TFS.
Degree/ Certifications	B.S., Computer Information Systems, Bellevue University, NE AWS Certified Solutions Architect
Relevant Experience	Developer, Infocap Networks, LLC (Sep 2018–Present): drives successful implementation and support of CMS-ES process orchestration through defined system design, testing, and implementation plans; applies .NET and Visual Studio expertise to translate business and technical requirements into validated outcomes. IT Specialist, US Army Human Resource Command (Oct 2010–Sep 2018): introduced automated intelligent scanning using Kofax Capture and Transformation Modules saving thousands of man-hours on the HRC evaluations team; upgraded the Unemployment for Ex-Servicemembers app to a .NET web app integrated with Kofax, saving millions in incorrect/false claims; implemented thin-client modules and administered Kofax server, TFS, OpenText, CollabNet, and Subversion Edge. IT Specialist (security/compliance) & Information Engineer, CACI Federal Inc., Naval Warfare Center (Jun 2007–Sep 2010): neutralized security threats using Fortify, applied fixes from STIG/IAVA findings, and reported trends — directly relevant to regression and compliance-oriented test coverage; earlier roles at Dairyland Healthcare Solutions and Charter Communications built end-user troubleshooting and issue-replication fundamentals.

Role	Training Lead
Resource	Theresa Resek
Qualifications	15+ years of project management and 20+ years in Information Management; Certified Information Professional (CIP) with an MBA. Deep training and adoption-program leadership — directed the full project lifecycle for AIIM's Certification Program, including a 100-item certification exam update and 20+ monthly learning lessons; hands-on with LMS, webinar/virtual event platforms, content management, and digital content delivery for role-based training. Strong stakeholder engagement and adoption expertise; multimedia content production (webinars, podcasts, ebooks, infographics) that aligns technical specs to audience needs and continuously improves content from user feedback.
Degree/ Certifications	MBA Certified Information Professional (CIP)
Relevant Experience	Director, Education & Research, Infocap (Oct 2024–Present): leads content management and end-to-end project lifecycles delivering technical, SEO-optimized content across platforms; coordinates cross-functional teams and tracks deadlines, aligning technical initiatives with growth objectives and customer needs. Vice President, Education & Research, AIIM International (Jan 2023–Apr 2024): directed the full Certification Program lifecycle using Agile; managed a 40-person global task force; delivered a 100-item certification exam update on time and on budget; evaluated and optimized LMS and content delivery platforms supporting 20+ monthly learning lessons. Vice President, Content Development & Market Intelligence, AIIM International (Feb 2019–Jan 2023): orchestrated planning and execution of dozens of events and media projects annually; used content management and analytics tools to develop editorial roadmaps and adjust strategy based on lead-generation and engagement metrics.

Role	Technical Account Manager
Resource	Ken Zink
Qualifications	Two decades in automation, consulting, and technical leadership with deep hands-on Kofax expertise (including Kofax TotalAgility), business process optimization, and solution architecture — well-suited to ongoing technical account stewardship. Continuous-improvement leader with collaborative, relationship-driven style and strong escalation and stakeholder-management orientation; translates complex business needs into actionable strategies and resolves customer issues. Governance background — established and refined governance processes, policies, and reporting for a global technology portfolio; direct experience with service reviews, CRFP responses, and ongoing optimization of TotalAgility environments.
Degree/ Certifications	Certified in Robotic Process Automation (RPA) Kofax Technical Solutions Specialist
Relevant Experience	Director, Business Transformation, Infocap (Aug 2024–Present): leads strategic initiatives driving innovation, streamlining operations, and elevating organizational efficiency; guides cross-functional teams in designing and executing solutions that align with company vision and deliver measurable impact. Manager, Transformation Engineering Group & Senior Intelligent Automation Architect, Canon Business Process Services (Dec 2020–Jul 2024): led cross-functional teams across multiple locations; spearheaded adoption of Kofax TotalAgility to improve efficiency and reduce costs; defined the organization's automation roadmap and established global governance processes, policies, and reporting. Senior Solutions Consultant, Infocap (May 2020–Oct 2020) & Senior Sales Engineer, Kofax (Mar 2016–May 2020): conducted technical discovery and designed tailored TotalAgility integration strategies; served as technical expert in the sales cycle; engineered TotalAgility adaptations for RPA, BPM, and intelligent automation, and led process-improvement workshops.

4.4.2. Mandatory Qualification/Experience Requirements

Infocap will meet the mandatory qualification and experience requirements through documented certifications, security controls, confidentiality commitments, AI governance procedures, and compliance documentation.

4.4.2.1. Vendor shall ensure compliance with all applicable data privacy, cybersecurity, and AI governance procedures.

Infocap confirms compliance with all applicable data privacy, cybersecurity, and AI-governance requirements associated with the proposed Agency solution.

Our proposed solution will implement encryption, SSO, MFA, RBAC, ACLs, least-privilege access controls, audit logging, SIEM integration, 24x7 SOC monitoring, vulnerability scanning, annual penetration testing, incident-response procedures, and continuous monitoring within the FedRAMP Authorized boundary services and security controls consistent with applicable NIST SP 800-53 requirements.

Infocap's proposed solution will also implement responsible AI-governance controls including Human-in-the-Loop (HITL) approvals, AI auditability, workflow traceability, model monitoring, controlled AI orchestration, and restrictions preventing unauthorized AI-model training or use of the Agency's data outside the authorized environment. The Agency's data and AI-processing activities will not be routed to public consumer AI platforms or non-authorized cloud services.

4.4.2.2. Vendors must sign a confidentiality agreement upon contract award.

Infocap confirms its willingness to execute all required confidentiality and non-disclosure agreements upon contract award and to comply with all the Agency confidentiality, data-handling, and information-protection requirements.

4.4.2.3. Vendors must hold current FedRAMP, StateRAMP, or SOC 2 Type II certification.

Infocap's proposed satisfies this requirement through the Tungsten Automation security and compliance credentials for the TotalAgility FedRAMP Cloud, which includes current SOC 2 Type II certification and ISO 27001 certification as documented within the TotalAgility security primer. The SOC 2 Type II assessment validates the effectiveness of security, availability, confidentiality, and operational controls supporting the TotalAgility FedRAMP Cloud platform. Applicable SOC 2 Type II reports and supporting compliance documentation will be made available to the Agency under appropriate non-disclosure agreement (NDA) protections.

Our proposed solution is hosted within the FedRAMP Authorized boundary cloud services and security controls consistent with applicable NIST SP 800-53 requirements. Infocap's proposed solution supports secure processing, workflow orchestration, AI-assisted review, audit logging, continuous monitoring, and operational resiliency for sensitive government permitting and regulatory-review workloads while satisfying the Agency's required FedRAMP Moderate security requirements.

4.5. Oral Presentations

Infocap is ready to participate in oral presentations and demonstrations when the Agency exercises this option. The presentation will clarify the submitted proposal without altering it.

4.6 Implementation Approach, Schedule, and Deployment Strategy

Infocap delivers the solution in five governed phases that mirror the structure of Attachment C, executed with a phase-gated Agile method on the configured Tungsten TotalAgility low-code platform. The phases run in offset parallel, so work that can proceed concurrently does, while each phase still closes at a controlled stage gate. Infocap commits to a go-live on or before the Agency's July 1, 2027 target. Delivery is expressed as approximately 47 weeks from Notice to Proceed (NTP), with all phase scheduling baselined to the actual NTP date once issued.

Three delivery methods carry this schedule. Phase-gated Agile organizes each phase into short, iterative sprints with continuous validation, while the five phase gates preserve formal control. Low-code configuration means TotalAgility supplies workflow, intelligent document processing, retrieval, robotic process automation, human-in-the-loop review, and observability as configured capabilities rather than custom code, which lowers delivery risk. Parallel execution overlaps Discovery, Integration, and Testing on the shared platform foundation, so the expanded per-phase durations still complete within the fixed window. The full system is operable at go-live through a single production cutover. Sprint increments are build and validation steps, not partial production releases, so the Agency receives one complete, accepted system rather than a sequence of live partial deployments. Consistent with the Agency's guidance, Infocap commits to the target go-live and expresses the schedule as an estimate from NTP, conditioned on the actual NTP date and timely completion of Agency dependencies identified below.

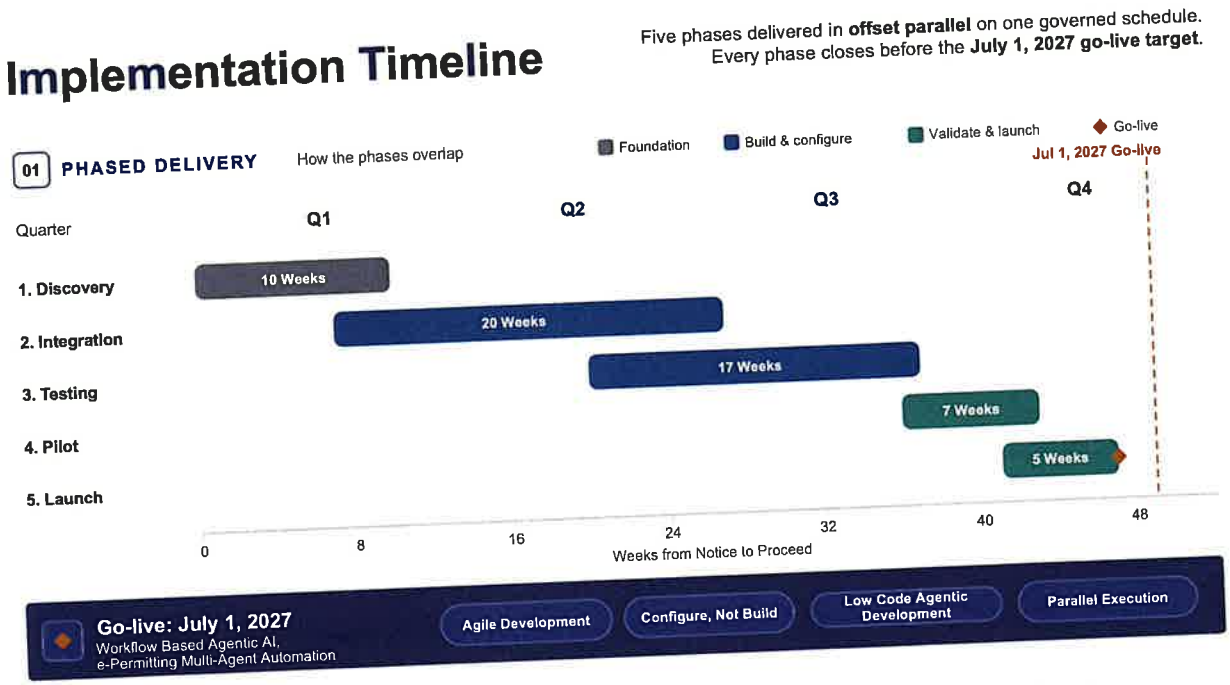


Figure 31- Five phases delivered in offset parallel, baselined to the Notice to Proceed date, with go-live on or before the July 1, 2027 ceiling. The Production Launch bar extends past go-live to reflect the 30-day hypercare and stabilization period

Table 4.6.1. Implementation Phases, Key Activities, and Key Deliverables

Phase	Duration	Key Activities	Key Deliverable
Phase 1: Discovery & Configuration	10 weeks	Requirements validation, tenant setup, SSO integration, and ERIS/ESS system assessment.	Approved requirements baseline and a configured tenant within the FedRAMP-authorized boundary, with single sign-on, role-based access control, and multifactor authentication operational.
Phase 2: Integration Development	20 weeks	API integration with Agency systems, WV-specific regulatory rule configuration, and AI model training.	Configured end-to-end system, with integrations, named agents, GraphRAG, GIS and Area of Review validation, and the standalone HITL Workflow Interface proven in a first full-case dry run.
Phase 3: Data Migration & Testing	17 weeks	Historical data migration, User Acceptance Testing (UAT), security testing, and HITL workflow validation.	Agency-accepted User Acceptance Testing, with security and adversarial testing complete and all six HITL decision gates validated.
Phase 4: Pilot Deployment	7 weeks	Pilot launch with limited applications, user training, and system refinement based on feedback.	Completed Class I and Class VI pilot and user training, with token and cost-governance reporting validated and the full system demonstrated to the Agency.
Phase 5: Production Launch	5 weeks	Full production deployment, go-live support, and 30-day "hypercare" stabilization period.	Written System Acceptance and go-live with the full system operable on or before July 1, 2027, followed by completed 30-day hypercare and an active stabilization warranty.

Table 4.6.1 consolidates the Agency's Attachment C phase structure and Key Activities with Infocap's anticipated durations and the key deliverable that closes each phase; the Key Deliverable entries are the key development milestones for their phases. The same phase structure, durations, and Key Activities are submitted in the Agency's prescribed Attachment C format. The phases run in offset parallel as shown in Figure 4.6-1, so the durations overlap and total elapsed time is shorter than their sum; go-live falls on or before July 1, 2027, and the 30-day hypercare and stabilization period runs after go-live.

Assumptions and Shared Responsibilities

- The schedule is baselined to the Notice to Proceed date. All phase scheduling adjusts to the actual NTP date once issued.
- The Agency provides timely access to business, technical, geoscience, GIS, and permitting subject matter experts for requirements validation, design reviews, and User Acceptance Testing within the agreed governance cadence.

- The Agency provides standard operating procedures, regulatory content, document templates, and representative training data needed to configure the platform and ground the agents.
- WV OSSP, OneLogin, and Active Directory access and readiness are available to support integration on the planned schedule.
- The Agency participates in periodic demonstrations and in the phase-gate review at the close of each phase.
- Security authorization activities proceed concurrently with configuration so that authorization artifacts are finalized in advance of go-live.

Schedule Risk and Buffer

July 1, 2027 is a not-to-exceed commitment. Each phase carries margin added to its baseline duration, and offset parallel execution absorbs that margin so go-live still lands on or before the date. The 30-day hypercare and stabilization period runs afterward and does not move it. The principal schedule risks are the timing of Agency dependencies, the integration readiness of connected systems, and source data quality. Infocap manages these by sequencing shared platform components first, validating each increment before integration, and applying centralized integration governance across the parallel workstreams.

Governance and Progress Tracking

Infocap leverages Agile governance methods to keep delivery on time while building the solution iteratively. Configured capabilities are developed in increments, with periodic demonstrations that keep the Agency engaged in validation and refinement as the solution takes shape. Each phase closes with a phase-gate review against the deliverables in Table 4.6.1, giving the Agency a formal checkpoint before the next phase advances. Regular, two-way communication between the Agency and Infocap, including the review cadence defined in §4.3.3.3.3.4, keeps progress, risks, and decisions visible to both parties throughout delivery.

Appendix A: GIS Artifacts

Proof Artifact	Purpose	CRFP/Proposal Section	Owner / Contributor
GIS Architecture Diagram	Shows role split between TotalAgility and WVDEP/ESRI GIS tools	§4.3.2.3	GIS Lead / Solution Architect
GIS Data-Flow Diagram	Shows lifecycle of GIS files, reviewer outputs, AoR findings, audit records, and exports	§4.3.2.3	GIS Lead
ArcGIS Output-Handling Diagram	Shows how reviewer-generated GIS outputs return to TotalAgility case workflow	§4.3.2.3	GIS Lead
GIS Data-Source/Access Matrix	Clarifies source owners, access modes, fallback methods, and avoids unsupported API assumptions	§4.3.2.3.2	Integration Lead / GIS Lead
GIS/CAD Format-Support Matrix	Demonstrates support for Shapefile, GeoJSON, KML, CAD, DWG, PDF maps, and fallback formats	§4.3.3.1.1	GIS Lead / QA Lead
CRS Normalization Approach	Documents source CRS, target CRS, transformation handling, and reviewer exceptions	§4.3.2.3	GIS Lead
Topology-Check Approach	Documents geometry, topology, overlap/gap, and attribute validation	§4.3.2.3	GIS Lead
Sample GIS/AoR Dashboard Mockup	Shows operational visibility into GIS/AoR workflow status	§4.3.2.1.2	UX Lead / GIS Lead
Sample GIS Validation Exception Queue	Shows reviewer handling of file, CRS, topology, and source-data issues	§4.3.2.3	GIS Lead / UX Lead
Sample AoR & Risk Validation HITL Task	Demonstrates reviewer control and decision options	§4.3.2.5	GIS Lead / UX Lead
GIS Audit/Evidence Record Sample	Shows source layer, CRS, transformation, topology result, reviewer decision, and override rationale	§4.3.2.3.3	AI Governance Lead / GIS Lead
GIS UAT Test Cases	Demonstrates implementation credibility and acceptance readiness	§4.6	QA Lead
GIS/AoR Lead Resume or Role Commitment	Demonstrates GIS capability and accountability	§4.4	Proposal Manager
Hydrogeology/Geoscience SME Resume or Role Commitment	Supports Class VI and technical review credibility	§4.4	Proposal Manager
ESRI/ArcGIS Experience Evidence	Demonstrates ability to work within WVDEP's ESRI environment	§4.4 / Appendix	GIS Lead

Sample GIS Audit

Audit Field	Sample Value
Case ID	UIC-2026-0001
GIS Artifact	Applicant_AoR_Boundary.shp
Artifact Type	ESRI Shapefile
Source	Applicant upload
Upload Date	[Date]
Source CRS	NAD83 geographic coordinates
Target CRS	NAD83 / UTM Zone 17N
Transformation	[Transformation method confirmed during configuration]
Validation Result	CRS passed; topology failed due to overlapping polygon
Risk Feature	Artificial penetration within AoR
Source Layer	WV Office of Oil and Gas well record export
Spatial Operation	Intersect within Class I 1/4-mile AoR
AI/GIS Finding	One well record intersects AoR boundary; reviewer validation required
Reviewer Action	Revised and approved
Reviewer Rationale	Reviewer confirmed well ID and corrected distance after ArcGIS review
Timestamp	[Date/time]
Final Disposition	Approved for technical review evidence package

Sample GIS Evidence Record

This sample illustrates how TotalAgility will preserve GIS, CAD, map, AoR, reviewer-generated GIS output, and spatial-risk evidence as part of the electronic UIC case file. The record supports source traceability, CRS/topology validation, AoR review, reviewer decision-making, HITL approval, audit logging, and export.

Table 1 Sample GIS Evidence Record

Field	Example Value
Case ID	UIC-CLASS-I-2026-00017
Permit class	Class I
Evidence record ID	GIS-EVR-00042
Evidence type	AoR risk feature validation
Source material	Applicant-submitted AoR Shapefile
Source file	Proposed_Well_AoR.shp
Source owner	Applicant
External source checked	WV Office of Oil and Gas well records
GIS format	Shapefile
Source CRS	NAD83 geographic coordinates
Target CRS	NAD83 / UTM Zone 17N
Transformation applied	Reprojected to project review CRS
Layer type	AoR boundary
Geometry type	Polygon
Spatial operation	1/4-mile buffer and intersection with well records
Topology result	Passed
CRS result	Passed after reprojection
Validation exception	One intersecting well record missing operator attribute
Risk feature type	Artificial penetration
Risk feature result	3 wells identified inside Class I AoR
Source citation	Applicant file page 14, AoR map; WV Oil and Gas well layer extract
AI-generated summary	Three artificial penetrations were identified within the fixed-radius AoR. One record requires reviewer validation due to missing operator metadata.
Confidence status	High for spatial intersection; Medium for missing attribute record
Reviewer role	GIS reviewer
Reviewer action	Request clarification
Reviewer comment	Confirm ownership/operator details for Well ID WV-OG-18391 before technical approval.
Override rationale	Not applicable
HITL gate	AoR & Risk Validation
Timestamp	2026-06-02 14:35 ET
Workflow action	Returned to applicant clarification queue
Export status	Included in GIS/AoR evidence package

Table 2 Sample Class VI Model Evidence Record

Field	Example Value
Case ID	UIC-CLASS-VI-2026-00004
Evidence record ID	GIS-EVR-00077
Evidence type	Class VI AoR model-evidence review
Source material	Applicant-submitted AoR modeling report
Source file	ClassVI_AoR_Model_Assumptions.pdf
Spatial output	Applicant-provided plume and pressure-front map
Model evidence reviewed	Boundary conditions, assumptions, pressure-front extent, AoR delineation
GIS output imported	Reviewer-generated ArcGIS map PDF and exported GeoJSON layer
Reviewer system	WVDEP-approved GIS/geoscience review environment
TotalAgility role	Capture, route, audit, preserve reviewer output
Reviewer action	Approved with condition
Reviewer comment	Pressure-front map accepted for draft permit support, subject to reevaluation schedule.
HITL gate	AoR & Risk Validation
Audit status	Complete
Export status	Included in final technical review package

Appendix B: GIS/CAD Format Support Matrix

This appendix supports §4.3.3.1.1 by defining expected handling for GIS, CAD, map, and engineering submissions. It identifies supported or expected formats, version assumptions, CRS and metadata requirements, validation checks, size handling, fallback paths, exception routing, reviewer validation, and audit evidence. Final accepted versions, service endpoints, size thresholds, CRS transformations, and authoritative source rules will be confirmed with the Agency during discovery and documented in the final integration design.

Format / Material Type	Supported Input and Version Expectation	CRS and Metadata Requirements	Validation Checks	Size Handling, Fallback, and Exception Routing	Reviewer Validation and Audit Evidence
Applicant GIS Vector Layers	ESRI Shapefile, GeoJSON, KML/KMZ, feature exports, and layer packages if approved. Industry-standard variants and specific versions will be confirmed during discovery.	Source CRS required. Target CRS recorded, including NAD83 geographic coordinates and NAD83 / UTM Zone 17N where required by final design. Metadata includes layer name, intended use, source date, feature IDs, scale or resolution, and submitter.	Completeness, required sidecar files, readable geometry, CRS presence, projection mismatch, invalid geometry, duplicate features, overlaps, gaps, missing attributes, AoR boundary consistency, and reference-layer checks.	Project-level datasets are processed directly. Large regional layers are staged, tiled, referenced through ArcGIS services, or handled through approved bulk import. Missing CRS, corrupt files, malformed attributes, unsupported variants, or excessive size create GIS exception tasks and correction workflows.	GIS reviewer approves, rejects, revises, overrides, or requests correction. Audit captures file name, upload time, source CRS, target CRS, transformation, validation result, exception status, reviewer comments, timestamp, and export status.
ArcGIS Feature Services, Map Services, and TAGIS Layers	WVDEP/TAGIS ArcGIS Enterprise, ArcGIS Portal, ArcGIS Online/Open Data Hub, state GIS repositories, and approved feature or map services. The proposal does not assume a fixed ArcGIS version unless confirmed by the Agency.	Service CRS, layer CRS, transformation method, layer ID, service owner, service version, refresh date, layer purpose, and authoritative status recorded.	Service reachability, permission check, layer availability, CRS alignment, schema compatibility, layer currency, spatial relationship checks, and match against applicant materials.	Large or authoritative layers are referenced through ArcGIS services rather than copied into TotalAgility as monolithic files. If service access is unavailable, TotalAgility uses approved layer export, PDF map, screenshot, manual service reference, reviewer upload, or controlled file import.	Reviewer validates layer relevance, CRS alignment, data currency, spatial output, and final GIS evidence status. Audit captures service name, layer ID, version, CRS, access method, reviewer signoff, and case linkage.

CAD and Engineering Drawings	DWG, DXF, CAD exports, well schematics, construction drawings, site plans, engineering drawings, and related reviewer output packages. Accepted CAD/DWG variants and engineering-review tools will be confirmed during discovery.	Drawing units, scale, coordinate basis, layer names, sheet title, revision, author, date, and relationship to GIS layers or permit documents required where available.	Readability, unit consistency, layer availability, drawing scale, coordinate reference, title block consistency, well location consistency, and relationship to site maps, forms, and AoR materials.	Large or complex CAD files may be staged, reduced to required layers, exported as GIS layers, or reviewed in approved CAD/GIS tools. Unsupported, corrupt, oversized, missing-unit, or unreferenced CAD files are routed to GIS/CAD reviewer tasks.	Reviewer validates drawing relevance, technical acceptability, and relationship to permit evidence. Audit captures source file, version, reviewer output, notes, exceptions, decision, timestamp, and linked HITL task.
PDF Maps, Scanned Maps, and Map Images	PDF, TIFF, JPEG, PNG, scanned plats, map exports, screenshots, and image-based map evidence supported through document intelligence, OCR, reviewer upload, and GIS reviewer workflows.	Required where available: scale, north arrow, coordinate grid or coordinates, map date, source, legend, author, page reference, and relationship to GIS layer or permit evidence.	Readability, map presence, scale, legend, coordinate clues, OCR text, required map elements, consistency with legal descriptions, site locations, AoR calculations, and applicant forms.	Large images or multi-page PDFs are indexed and linked to the case. Georeferencing is handled in Agency-approved GIS tools when needed. Unreadable, missing, low-resolution, unreferenced, or conflicting maps create reviewer tasks and may trigger deficiency workflow.	Reviewer validates whether the map is acceptable evidence, requests correction, or attaches a georeferenced reviewer output. Audit captures document name, page, map reference, reviewer action, rationale, and export inclusion.
CSV and Tabular Coordinate Files	CSV, Excel extracts, tabular coordinates, well lists, receptor lists, parcel lists, and coordinate tables embedded in documents where fields can be mapped to the case model.	Required fields: coordinate values, coordinate order, units, datum or CRS, feature ID, source, date, and intended use. Decimal degrees, projected coordinates, and NAD83-based values are normalized according to final design.	Column mapping, missing values, coordinate range, coordinate order, numeric format, duplicate IDs, datum mismatch, out-of-bounds locations, and consistency with GIS layers and forms.	Large tables may be processed in batches or staged through secure import. Missing datum, ambiguous coordinate order, invalid values, duplicate identifiers, or inconsistent source records create data validation and GIS reviewer tasks.	Reviewer confirms field mapping, CRS interpretation, accepted values, correction need, or override. Audit captures original table, mapped fields, validation results, reviewer decision, and case linkage.
Raster, Imagery, and	GeoTIFF, TIFF, JPEG, PNG, scanned imagery, map	Required where available: raster CRS,	CRS presence, extent, resolution, pixel size, no-	Large rasters and grids are tiled, staged, or referenced	Reviewer validates applicability, data quality,

Reference Grids	rasters, DEM/DSM, grids, and reference image products where approved. Raster and geospatial grid handling will align with Agency GIS and geoscience tools.	pixel size, extent, acquisition date, source, band description, vertical datum where relevant, and intended use.	data values, registration quality, layer currency, overlap with project area, and relationship to surface-water, environmental, or AoR evidence.	through ArcGIS or approved data services rather than copied as single monolithic files. Missing georeference, excessive size, unclear source, or poor quality creates GIS reviewer tasks.	and whether the raster supports review. Audit captures source, CRS, extent, version/date, validation result, reviewer comments, and final evidence status.
LiDAR, point Cloud, 3D Grids, and 2D/3D Visualization Outputs	LAS, LAZ, 3D grids, terrain surfaces, structure surfaces, cross sections, screenshots, map PDFs, and reviewer-generated 2D/3D outputs. Advanced rendering and spatial computation remain in Agency-approved GIS/geoscience tools.	Required where available: horizontal CRS, vertical datum, units, acquisition date, source, classification, resolution or point density, and intended technical use.	CRS and vertical datum, unit consistency, extent, density or resolution, classification status, model/source date, and relationship to AoR or geologic evidence.	Dense LiDAR, 3D grids, and multi-gigabyte engineering files are staged, tiled, summarized, or referenced through approved ArcGIS/LiDAR/geoscience services. Oversized files, missing datum, unclear vertical reference, unsupported point-cloud variants, or visualization-only outputs create reviewer tasks.	Reviewer validates the output package and its technical use. Audit captures source, processing system, map/layer version, reviewer decision, override rationale, and linked GIS Evidence Record.
Class VI Model evidence and Geoscience Outputs	AoR delineation layers, pressure/plume extents, model inputs, boundary conditions, assumptions, outputs, reevaluation schedules, geologic maps, stratigraphic evidence, and technical memos. TotalAgility captures and routes model evidence but does not independently perform reservoir simulation or CO2 plume modeling unless separately scoped and approved by WVDEP.	Required: model source, version, date, author, assumptions, input references, output CRS, extent, unit conventions, model scenario, and relationship to applicant materials.	Completeness of model package, required inputs, boundary condition documentation, CRS alignment, output availability, AoR relationship, risk feature intersections, and reviewer evidence consistency.	Large model files remain in approved geoscience or GIS systems. TotalAgility stores evidence summaries, references, reviewer outputs, reports, maps, and final approved packages. Missing inputs, undocumented assumptions, conflicting outputs, unsupported model files, or unclear source packages create Class VI model-evidence review tasks.	Agency technical reviewers approve, reject, revise, request additional analysis, or override. Audit captures reviewer name, timestamp, model version, assumptions, decision, rationale, HITL gate, and export status.

Reviewer-Generated ArcGIS/TAGIS Outputs	Reviewer map PDFs, exported layers, feature exports, validation reports, screenshots, technical notes, signed memos, and final GIS evidence packages produced in Agency-approved GIS, ArcGIS/TAGIS, geoscience, or reviewer systems.	Required where available: source system, reviewer name, output date, layer or map version, CRS, transformation, scope of review, and final evidence status.	Completeness, source linkage, CRS documentation, decision consistency, exception closure, relationship to AoR/risk findings, and presence of reviewer rationale.	Reviewer outputs are attached to the electronic case file and GIS Evidence Record. Large files may be referenced or packaged through approved export methods. Incomplete, conflicting, or unclear reviewer outputs return to the reviewer queue.	Reviewer action controls whether the output becomes final GIS evidence. Audit captures reviewer decision, comments, override rationale, timestamp, linked HITL gate, and export package inclusion.

Use note: This matrix is a proof artifact and configuration baseline. It does not make TotalAgility the authoritative GIS/CAD engine. TotalAgility orchestrates intake, routing, evidence capture, HITL review, audit logging, and export packaging. Agency-approved GIS, CAD, ArcGIS/TAGIS, geoscience, and reviewer systems remain authoritative for spatial calculation, rendering, model review, and technical validation.

Appendix C: Example and Anticipated UAT Test Cases

Each UAT case will include pass/fail criteria, test data, expected reviewer action, audit evidence, and acceptance signoff. Failed tests will be tracked through the implementation issue log and retested before production release. UAT results will be included in the acceptance package together with configuration notes, sample audit records, and reviewer validation evidence.

Test Case	Input / Scenario	Test Objective	Expected Result	HITL And Audit Result
Shapefile Ingestion	Applicant ESRI Shapefile with projection file and required attributes	Confirm Shapefile upload, file completeness, metadata capture, CRS detection, and case association	File is ingested; layer metadata is captured; CRS is detected; geometry is displayed or referenced in the case; missing files, missing CRS, or invalid geometry create reviewer-visible exceptions	Source file, CRS, timestamp, validation status, and reviewer task are logged; reviewer may approve, request correction, or reject file
GeoJSON Ingestion	Applicant GeoJSON AoR boundary or feature layer	Confirm GeoJSON feature ingestion and attribute capture	GeoJSON is parsed; geometry is validated; attributes are mapped to case fields; invalid geometry routes to GIS reviewer	Reviewer sees layer status and approves, requests correction, or rejects; all actions and exceptions are logged
KML/KMZ Ingestion	Applicant KML/KMZ site boundary, well location, or overlay	Confirm map-overlay handling and coordinate interpretation	KML/KMZ is imported or referenced; coordinates are normalized; CRS/coordinate assumptions are documented; missing metadata is flagged	Exceptions for incomplete CRS or attributes are routed to GIS reviewer; reviewer decisions and any conversion outputs are recorded
CAD/DWG Handling	CAD/DWG site map, well diagram, or engineering plan	Confirm CAD/DWG file routing through approved CAD/GIS review process	File is accepted, linked to case, and routed for GIS/CAD review; CAD/DWG file is captured and, where needed, converted or summarized	Reviewer task is created; reviewer output, converted files, and notes are stored as case evidence with timestamp and identity
PDF Map Package Review	Permit PDF with site maps, AoR calculation pages, or other map exhibits	Confirm OCR/vision extraction and manual map-review workflow	System detects required map materials and links them to the completeness checklist; key map evidence is extracted	Missing or unreadable maps trigger Pre-NoD reviewer validation; reviewer decisions and

			where possible; low-confidence items route to reviewer	comments are logged in the GIS Evidence Record
Missing CRS Exception	GIS layer without CRS metadata	Confirm that missing CRS generates exception and blocks automated spatial use	System flags missing CRS and prevents automatic spatial acceptance	Reviewer assigns correction, override, or manual CRS validation; rationale, identity, date, and outcome are logged
CRS Detection and Transformation	Input layer in one CRS (e.g., NAD83 decimal degrees) requiring target CRS (e.g., NAD83/UTM Zone 17N)	Validate capture of source CRS, target CRS, and transformation method	System records source CRS, target CRS, transformation method, and validation result in the GIS Evidence Record	Transformation decision and reviewer approval (or exception) are logged, including any issues or overrides
Topology Failure Routing	Polygon layer with overlaps, gaps, invalid geometry, or malformed boundary	Confirm invalid geometries and topology issues generate exceptions	System flags topology exceptions (overlaps, gaps, invalid geometry, missing attributes) and creates a GIS-review task with issue details	Reviewer approves fix, rejects file, or requests applicant correction; resolution and disposition are recorded in the audit trail
Class I Fixed-Radius AoR	Valid Class I well coordinate	Confirm 1/4-mile AoR evidence workflow using validated well coordinates	System creates or references 1/4-mile AoR screening result and risk-feature list; buffer output, source coordinate, CRS, and query parameters are recorded	AoR and Risk Validation HITL gate requires reviewer signoff; reviewer approval, edits, or rejection are tracked for audit/export
Risk Feature Overlay	AoR with wells, mines, boreholes, faults, USDWs, receptors, property/plat records, or surface-water features	Confirm risk-feature overlay and reviewer validation workflow	System produces reviewer-visible risk-feature list with source references and spatial context	Reviewer validates, edits, overrides, or requests additional analysis; actions, sources, and downstream workflow decisions are logged
Class VI Model-Evidence Review	Applicant or reviewer-generated Class VI model inputs, assumptions, boundary conditions, pressure/plume evidence,	Confirm routing and organization of model evidence without performing independent simulation	System extracts and organizes model evidence and links it to the case and AoR record; no independent reservoir/plume simulation is performed unless separately scoped	Agency technical reviewer validates model evidence and records decision, comments, and disposition in the GIS Evidence Record

	and AoR delineation materials			
External-Source Cross-Check	WVGES, SDWIS, Oil and Gas, property/plat, WVDEP, or similar external data sources	Confirm source checks and fallback paths for external data	Source-access method, query parameters, and results or limitations are recorded; unavailable or inconsistent data generate exceptions	Reviewer validation status, decisions on use/limitations, and any manual substitutions are captured for audit purposes
ArcGIS/TAGIS Reviewer Output Import	Reviewer map PDFs, layer exports, notes, validation reports, or signoffs	Confirm that reviewer outputs return to TotalAgility case record	Output package is attached to the case and linked to the relevant AoR/GIS review task; GIS Reviewer Output Package is recorded	Reviewer output, version, timestamp, decision, and audit record are preserved and included in the HITL decision chain
Reviewer Override	GIS finding with low confidence, ambiguous inputs, or conflicting source data	Confirm reviewer can revise, reject, or override GIS/AoR finding	System allows reviewer override with required rationale and disposition options	Override reason, reviewer identity, timestamp, affected source data, and downstream workflow actions are logged in the audit trail
GIS Audit Export	Completed GIS/AoR review record for a given case	Confirm GIS Evidence Record is included in case audit/export package	System exports GIS Evidence Record with source layers, CRS, transformations, validation results, risk flags, reviewer actions, overrides, and final disposition	Export package supports final record retention and audit review; export event, user, and timestamp are logged

Appendix D: NIST 800 Details

NIST 800-53 Control Ownership Summary

Control Area	Primary Owner	Notes
TotalAgility Deployment	Tungsten Automation	Responsibility matrix assigns deployment to Tungsten.
Monitoring, Logs, Performance	Tungsten Automation	Logs/SIEM/SOC are Tungsten-managed; solution-level reporting is customer-configured.
Backups	Tungsten Automation	Azure point-in-time restore and optional geographically redundant backups are documented.
Security and Logging	Tungsten Automation	Shared for solution-level audit configuration and customer policy.
Patching and Upgrades	Tungsten Automation	Customer tests updates in Dev/UAT where applicable.
Solution Configuration	Customer / Infocap implementation team	Workflows, roles, rules, HITL gates, AI prompts, knowledge bases, and agency-specific controls must be configured.
User Setup	Customer	Customer controls agency users, groups, access policy, and identity-provider governance.

NIST SP 800-53 Control Matrix - TotalAgility Cloud

NIST 800-53 Family / Control	Control Objective	TotalAgility Cloud Alignment	Responsibility	Evidence / Notes
AC-1 - Access Control Policy and Procedures	Establish access-control governance	TotalAgility supports role-based access, ACLs, federated security, and customer-configured user governance.	Shared: Tungsten provides platform controls; customer configures policies, roles, and users.	The responsibility matrix assigns TotalAgility deployment, monitoring, backups, security/logging, patching, and upgrades to Tungsten, while solution configuration and user setup are customer responsibilities.
AC-2 - Account Management	Manage user accounts and access lifecycle	TotalAgility supports user setup, federated authentication, resource roles, work queues, and access permissions.	Customer for business-user setup; Tungsten for cloud administrative controls.	TotalAgility Feature Guide documents federated security and access-control settings; the InfoSec Primer assigns user setup to the customer.
AC-3 - Access Enforcement	Enforce approved authorizations	TotalAgility enforces role-based application access, ACLs, functional access, case/process access, and security permissions.	Shared	InfoSec Primer table of contents identifies authentication/authorization, federated security, user privileges, ACLs, functional access, and case/process access as documented security areas.

AC-5 - Separation of Duties	Separate conflicting roles and responsibilities	TotalAgility supports role-based assignment, manual/dynamic work allocation, HITL approval queues, and reviewer/supervisor roles.	Customer-configured; platform-supported	Feature Guide documents roles, work allocation, manual/dynamic assignment, supervisors, and security levels.
AC-6 - Least Privilege	Limit access to authorized functions	TotalAgility supports ACLs, role-based access, functional permissions, case/process permissions, and restricted administrative access.	Shared	InfoSec Primer identifies user privileges, ACLs, functional application-level access, and case/process access.
AC-17 - Remote Access	Control remote access to cloud environments	TotalAgility Cloud administrative access is remote, requires approval, and is limited to authorized Cloud Services personnel.	Tungsten	The primer states access to the Azure-hosted environment requires Director, Cloud Services approval and is limited to TotalAgility Cloud Services personnel.
AC-20 - Use of External Systems	Control external-system connections	TotalAgility supports Integration Server, REST/SOAP services, secure sessions, SSO, and TLS-secured connections to customer systems.	Shared	Integration Server supports communication to/from the Agency's data centers, import/export, systems of record, scaling, and load-balancing; REST/SOAP access is secured with TLS 1.3, SSO, secure sessions, and network controls.
AT-2 / AT-3 - Security Awareness and Role-Based Training	Ensure users and privileged personnel are trained	Tungsten administrative access requires security training; access is revoked if annual training is not completed.	Tungsten for cloud staff; customer for agency users	The primer states administrative access requires username, password, rotating MFA key, initial security training, and annual training.
AU-2 - Event Logging	Identify events to be logged	TotalAgility Cloud transmits access and system logs to Azure Sentinel SIEM; web logs are routed to SOC tooling.	Tungsten; customer configures solution-level events	Log management section says all access and system logs are transmitted to Azure Sentinel for analysis and long-term storage.
AU-3 - Content of Audit Records	Capture useful event details	Platform logs support access/system/security events; TotalAgility workflows and cases also support case history, notes, job history, and audit logs.	Shared	Feature Guide documents Workspace audit log, job/case management, history, reporting, execution, notes, and performance statistics.
AU-6 - Audit Review, Analysis, and Reporting	Review and analyze audit logs	Logs are monitored by a 24/7 SOC; valid threats are escalated	Tungsten	The primer states SOC operates 24/7, reviews logs, and notifies network

		to the Tungsten network operations center.		operations by email and phone if a valid threat is suspected.
AU-9 - Protection of Audit Information	Protect audit records from unauthorized modification	SIEM-based log storage and restricted administrative access support protection of audit data.	Tungsten; customer for solution audit retention/config	Logs are sent to Azure Sentinel for long-term storage and monitored by SOC; access to cloud environments is restricted and approval-based.
AU-11 - Audit Record Retention	Retain audit logs for required period	TotalAgility Cloud stores logs for at least 12 months; customer solution may require additional case-record retention.	Shared	The primer states logs are stored for at least 12 months.
CA-2 - Control Assessments	Assess controls periodically	Tungsten performs annual TotalAgility Cloud penetration testing; customers may engage third-party penetration tests.	Shared	Primer FAQ states Tungsten performs annual penetration testing and that customer-engaged third-party penetration testing can be performed.
CA-3 - Information Exchange	Secure interconnections and data exchanges	TotalAgility supports Integration Server, REST/SOAP, TLS 1.3, SSO, secure sessions, source IP restriction options, and network controls.	Shared	Integration Server provides secure communication to/from the Agency's data centers; customer applications can connect using REST/SOAP secured via TLS 1.3, SSO, and secure sessions.
CA-7 - Continuous Monitoring	Maintain ongoing control monitoring	TotalAgility Cloud uses SIEM, SOC, monitoring tools, vulnerability scanning, WAF, IDS, and anomaly detection.	Tungsten	InfoSec Primer documents 24/7 SOC monitoring, Azure Sentinel SIEM, WAF, IDS, network anomaly detection, monthly vulnerability scans, and Trusec 24/7 monitoring.
CA-8 - Penetration Testing	Conduct penetration testing	Tungsten performs annual TotalAgility Cloud penetration testing; customer third-party tests can be supported.	Tungsten / Shared	Primer FAQ confirms annual penetration testing and customer third-party penetration test options.
CM-2 - Baseline Configuration	Establish and manage system baselines	TotalAgility packages, environments, deployment servers, schedules, and rollback support controlled deployment baselines.	Shared	Primer states packages can be created for Development, UAT, or Production; test plans can run before deployment; failed tests terminate deployment; rollback can occur if configured.
CM-3 - Configuration Change Control	Control configuration changes	Major versions and patches are communicated before production updates; Dev is	Tungsten / Shared	Primer states major versions/patches are applied after release cycles, customers are

		upgraded before test/production to allow customer testing.		notified, and development environments are upgraded before test/production.
CM-6 - Configuration Settings	Establish secure configuration settings	Azure VNet rules, WAF, firewalls, tenant separation, and application settings support secure configuration.	Shared	InfoSec Primer documents virtual firewall rules, WAF, Azure AD roles, tenant isolation, and secure cloud settings.
CM-8 - System Component Inventory	Maintain inventory of system components	TotalAgility Cloud architecture defines web roles, agent roles, Azure SQL, table/blob storage, Azure Document Intelligence, Azure OpenAI, and Azure AI Search.	Tungsten	Architecture section identifies Azure web roles, agent roles, Azure SQL, Azure table/blob storage, Azure Document Intelligence, Azure OpenAI, and Azure AI Search.
CP-2 - Contingency Plan	Plan for continuity and recovery	TotalAgility Cloud includes business continuity, availability zones, region failover, and high availability/scaling.	Tungsten; customer confirms mission RTO/RPO	InfoSec Primer documents business continuity, availability zones, ZRS, paired regions, region failover, high availability, and scaling.
CP-6 / CP-7 - Alternate Storage / Alternate Processing Site	Provide alternate processing/storage capability	Region failover provisions SQL Server, restores databases, deploys VNet/subnets/WAF/DNS/load balancer/public IPs, and deploys Live/Dev cloud services in the paired region.	Tungsten	Region failover steps are documented in the primer, with paired-region architecture shown on page 32.
CP-9 - System Backup	Backup system data	Local database backups use Azure point-in-time restore; near-real-time backups are kept up to 35 days; geographically redundant backups are available if a secondary site is chosen.	Tungsten / Customer-specific for geo backup schedule	Primer FAQ documents point-in-time restore, near-real-time backups, 35-day retention, and customer-specific geographically redundant backup schedule.
CP-10 - System Recovery and Reconstitution	Recover system after disruption	TotalAgility Cloud supports region failover, database restoration, infrastructure redeployment, and live/dev service deployment.	Tungsten	Paired-region failover steps include restoring databases and deploying the infrastructure and cloud services.

IA-2 - Identification and Authentication	Identify and authenticate users	TotalAgility supports federated security, Azure AD integration, SSO, user authentication, and MFA for cloud administrative access.	Shared	Primer identifies Authentication and Authorization, Federated Security, ACLs, and Azure AD roles; administrative access uses username, password, and rotating MFA key.
IA-5 - Authenticator Management	Manage authenticators	Rotating MFA keys are required for privileged access; customer identity-provider controls govern agency users.	Shared	The primer states username, password, and rotating multi-factor key are required for access.
IR-4 - Incident Handling	Detect, analyze, and respond to incidents	SOC monitors logs 24/7; suspected valid threats are escalated to Tungsten network operations, which is staffed 24/7.	Tungsten	Log management section describes SOC monitoring and escalation to Tungsten network operations by email and phone.
IR-5 - Incident Monitoring	Track and monitor incidents	Azure Sentinel SIEM, SOC monitoring, WAF, IDS, and anomaly detection support incident monitoring.	Tungsten	SIEM/SOC, IDS, network anomaly detection, and full 24/7 monitoring are documented.
IR-6 - Incident Reporting	Report security incidents	SOC escalation process to Tungsten network operations is documented; customer notification procedures should be confirmed contractually.	Tungsten / Contract-dependent	The primer documents SOC-to-network-operations escalation but does not fully define customer notification SLAs in the retrieved text.
MA-2 - Controlled Maintenance	Control system maintenance	Maintenance windows, emergency patch windows, patch notices, and update notifications are documented.	Tungsten	Primer FAQ documents monthly maintenance windows, nightly emergency patch windows, 36-hour notice for maintenance, and 30-day notice for major version updates.
MA-4 - Nonlocal Maintenance	Control remote maintenance	Administrative access is remote, approval-based, and restricted to Cloud Services personnel.	Tungsten	Remote access requires approval from Director, Cloud Services and is limited to TotalAgility Cloud Services personnel.
PE Family - Physical and Environmental Protection	Protect physical facilities and infrastructure	Physical infrastructure protection is primarily inherited from Microsoft Azure / Tungsten Cloud hosting.	Inherited from cloud provider / Tungsten	TotalAgility Cloud runs on Tungsten Cloud using Microsoft Azure as underlying infrastructure.

PL-2 - System Security and Privacy Plans	Document system security posture	TotalAgility Cloud InfoSec Primer provides security architecture, data flow, responsibility, AI services, business continuity, and information-security details.	Shared	Primer table of contents covers architecture, AI services, business continuity, information security, FAQs, shared/dedicated instance, and responsibility matrix.
RA-3 - Risk Assessment	Identify and analyze system risks	Tungsten performs vulnerability scanning, code scanning, penetration testing, and SOC monitoring. Customer performs solution-specific risk assessment.	Shared	Primer documents Veracode, Burp Suite, Qualys, monthly vulnerability scans, annual penetration testing, and SOC monitoring.
RA-5 - Vulnerability Monitoring and Scanning	Scan and remediate vulnerabilities	Tungsten performs monthly vulnerability scans on the Azure platform using a third-party service and uses Veracode, Burp Suite, and Qualys in development.	Tungsten	InfoSec Primer documents third-party monthly vulnerability scanning and static/dynamic code scanning with Veracode, Burp Suite, and Qualys.
SA-3 - System Development Life Cycle	Use secure SDLC controls	Tungsten uses agile development with multiple review/approval levels and static/dynamic scanning.	Tungsten	Product development practices section documents agile development, multiple review/approval levels, Veracode, Burp Suite, and Qualys.
SA-10 - Developer Configuration Management	Maintain integrity of system development	Package promotion, Dev/UAT/Production deployment, test plans, failed-test termination, and rollback support solution configuration management.	Shared	Primer FAQ documents packages, environment migration, deployment schedules, test plans, termination on failure, and rollback.
SA-11 - Developer Testing and Evaluation	Test software before deployment	Tungsten performs security scanning and testing; TotalAgility packages support pre-deployment test plans.	Shared	Product development practices and package/deployment testing are documented.
SC-7 - Boundary Protection	Monitor and control communications at boundaries	TotalAgility uses firewalls, virtual firewalls, Azure WAF, VNet rules, load balancing, IDS, and anomaly detection.	Tungsten	Primer documents WAF, virtual firewall rules, inbound/outbound VNet rules, firewalls, IDS, and network-based anomaly detection.

SC-8 - Transmission Confidentiality and Integrity	Protect data in transit	Connectivity to TotalAgility Cloud uses TLS 1.3 over HTTPS port 443; hosted AI services use TLS 1.3 or newer.	Tungsten / Shared for integrations	Primer states TotalAgility Cloud uses TLS 1.3 over HTTPS port 443; AI services use encrypted transport TLS 1.3 or newer.
SC-12 / SC-13 - Cryptographic Key Management and Protection	Manage and use cryptographic mechanisms	Azure Key Vault is identified in the security architecture; each tenant storage has separate encryption key in shared instances.	Tungsten / Azure	Primer lists Key Vault and states each tenant has its own storage with a separate encryption key.
SC-28 - Protection of Information at Rest	Encrypt stored information	All data at rest is encrypted using AES-256 at the database level; tenant storage is logically separated.	Tungsten	Primer states all data at rest is encrypted using AES-256; tenant storage is separate with separate encryption key.
SI-2 - Flaw Remediation	Identify, report, and correct flaws	Microsoft patching, Tungsten patch cycles, emergency patch windows, and security update processes are documented.	Tungsten	FAQ documents Microsoft patching, TotalAgility version/patch timing, hot-patch notice, major version notice, and emergency patches.
SI-3 - Malicious Code Protection	Detect and prevent malicious code	Antivirus/next-generation anti-malware is installed in production; WAF and SOC monitoring support malware/threat detection.	Tungsten	Primer states antivirus protection is installed and acts as next-generation anti-malware with cloud security analytics and threat intelligence.
SI-4 - System Monitoring	Monitor system and network events	Azure Sentinel SIEM, SOC, WAF, IDS, network anomaly detection, alerts, and Trusec 24/7 monitoring support system monitoring.	Tungsten	Primer documents logs to Azure Sentinel, 24/7 SOC, WAF, IDS, network anomaly detection, and Trusec monitoring.
SI-7 - Software, Firmware, and Information Integrity	Protect software and code integrity	Static and dynamic code scanning are performed with Veracode, Burp Suite, and Qualys; deployment packages and rollback support release integrity.	Tungsten / Shared	Product development practices and package deployment controls are documented.
SI-10 - Information Input Validation	Validate information inputs	TotalAgility supports document validation, verification, business rules, field validators,	Customer-configured / platform-supported	Feature Guide documents validation, verification, document review, field

		formatters, extraction confidence, and human review workflows.		validators, field formatters, business rules, and capture workflows.
SR-3 - Supply Chain Controls and Processes	Manage supply-chain risks	TotalAgility Cloud documents third-party subprocessors and Microsoft Azure-hosted services; customer should review contractual subprocessor list and data-flow boundary.	Shared / Contractual	Primer table of contents includes third-party subprocessors and AI service sections for Azure Document Intelligence, Azure OpenAI, Azure AI Search, and Google Vision.
SR-6 - Supplier Assessments and Reviews	Assess suppliers and service providers	TotalAgility Cloud maintains SOC 2 Type 1/2 and ISO 27001 certification; customer should review assurance reports under NDA/procurement process.	Tungsten / Customer review	Primer FAQ states TotalAgility Cloud is SOC 2 Type 1 and Type 2 certified and ISO 27001 certified as of January 2023.
PT-2 / PT-3 - Authority and Purpose for Processing PII	Define and limit PII processing	TotalAgility Cloud supports customer-controlled configuration, data retention timelines, and customer choice of AI service region/provider.	Customer policy / platform-supported	Primer states the Agency's data is deleted from Azure Table/Blob Storage according to timelines and policies defined by the customer, and customers can configure AI service region/provider options.
AI-Specific Governance Overlay - RA, CA, AU, SI, SC	Govern AI-assisted processing	TotalAgility supports AI services, customer-trained model monitoring, sampling/checking, Azure Document Intelligence, OpenAI LLMs, real-time content filtering, and modified abuse monitoring where Microsoft does not store prompts/completions for the TotalAgility Azure subscription.	Shared	Primer documents sampling/checking, AI services, region hosting, TLS 1.3, prompt/completion content filtering, and modified abuse monitoring.

Required Forms

The following forms are included in this section:

- Addenda Acknowledgement Form
- Designated Contact and Signature Page
- Final CRFP 0313 DEP2600000003 1 Form
- Final CRFP 0313 DEP2600000003 2 Form
- Subcontractor Listing
- FedRAMP Marketplace Listing, TotalAgility Cloud, Package ID FR1802451335 (printed from https://marketplace.fedramp.gov/products/FR1802451335)
- **SOC 2 Type II Documentation.** The TotalAgility Cloud platform maintains current SOC 2 Type II certification. The current report, Tungsten Automation Corp. Type II System and Organization Controls Report addresses the Security, Availability, Confidentiality, and Processing Integrity trust services categories and includes the TotalAgility cloud service within its system description. The report is a restricted-use document under standard AICPA distribution terms. Infocap is prepared to provide it to the Agency immediately upon execution of a mutual non-disclosure agreement, including during the evaluation period upon the Agency's request.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP DEP26*03

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Infocap Networks, LLC
Company

Authorized Signature

6/10/2026
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Nathaniel Palmer, CEO

(Address) 6901 Professional Pky E, Suite 200, Sarasota, FL 34240

(Phone Number) / (Fax Number) (phone) 781-534-3868

(email address) nathaniel@infocap.ai

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Infocap Networks LLC
(Company)

(Signature of Authorized Representative)
Nathaniel Palmer, CEO
(Printed Name and Title of Authorized Representative) (Date)
(phone) 781-534-3868
(Phone Number) (Fax Number)
nathaniel@infocap.ai
(Email Address)

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1913510	**Reason for Modification:**
Doc Description: Workflow Based Agentic AI, Automation, and E-Permitting Syst	
Proc Type: Central Contract - Fixed Amt	

Date Issued	Solicitation Closes	Solicitation No	Version
2026-04-29	2026-05-27 13:30	CRFP 0313 DEP2600000003	1

ID RECEIVING LOCATION

ID CLERK
EPARTMENT OF ADMINISTRATION
URCHASING DIVISION
019 WASHINGTON ST E
HARLESTON WV 25305
S

ENDOR

Vendor Customer Code:

Vendor Name : Infocap Networks, LLC

Address : 6901 Professional Parkway, E

Street : Suite 200

City : Sarasota

State : FL **Country :** United States **Zip :** 34240

Principal Contact : Nathaniel Palmer, CEO

Vendor Contact Phone: 781-534-3868 **Extension:**

OR INFORMATION CONTACT THE BUYER

oseph (Josh) E Hager III
304) 558-2306
oseph.e.hageriii@wv.gov

endor
ignature X FEIN# 93-2120968 DATE 6/10/26

ll offers subject to all terms and conditions contained in this solicitation

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder:	1913510
Doc Description:	Workflow Based Agentic AI, Automation, and E-Permitting Syst
Proc Type:	Central Contract - Fixed Amt
Reason for Modification:	Addendum #1 is issued to publish agency respones to all vendor submitted questions, and extend the b..... See Page 2 for complete info

Date Issued	Solicitation Closes	Solicitation No	Version
026-05-19	2026-06-10 13:30	CRFP 0313 DEP2600000003	2

ID RECEIVING LOCATION

ID CLERK
EPARTMENT OF ADMINISTRATION
URCHASING DIVISION
019 WASHINGTON ST E
HARLESTON WV 25305
S

ENDOR

endor Customer Code:

endor Name : Infocap Networks, LLC

ddress : 6901 Professional Parkway, E

treet : Suite 200

ity : Sarasota

tate : FL **Country :** United States **Zip :** 34240

rincipal Contact : Nathaniel Palmer, CEO

endor Contact Phone: 781-534-3868 **Extension:**

OR INFORMATION CONTACT THE BUYER

oseph (Josh) E Hager III
04) 558-2306
seph.e.hageriii@wv.gov

endor ignature X FEIN# 93-2120968 DATE 6/10/26

ll offers subject to all terms and conditions contained in this solicitation

Subcontractor List Submission (Construction Contracts Only)

Bidder's Name: Infocap Networks, LLC

☐ Check this box if no subcontractors will perform more than $25,000.00 of work to complete the project.

Subcontractor Name	License Number if Required by W. Va. Code § 21-11-1 et. seq.
Genus Technologies	

Attach additional pages if necessary

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = Total Cost Score of 27.27273

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

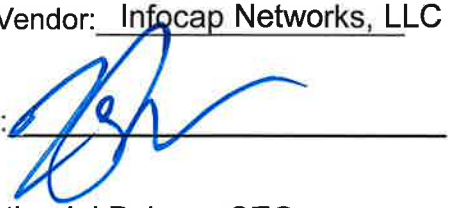
Infocap Networks, LLC
(Company)

Nathaniel Palmer, CEO
(Representative Name, Title)

(phone) 781-534-3868
(Contact Phone/Fax Number)

6/10/2026
(Date)

AGREED:

Name of Agency:_____	Name of Vendor: Infocap Networks, LLC
Signature:_____	Signature: 
Title:_____	Title: Nathaniel Palmer, CEO
Date:_____	Date: 6/10/2026

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: Infocap Networks, LLC

Name of Agency: Department of Environmental Protection

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes [X]
   No [ ]

2. If yes to #1, does the restricted information include personal data?
   Yes [ ]
   No [X]

3. If yes to #1, does the restricted information include non-public data?
   Yes [X]
   No [ ]

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes [ ]
   No [X]

5. Provide name and email address for the Department privacy officer:

   Name: John Nilles

   Email address: John.J.Nilles@wv.gov

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: Jason Hall, CISO

   Email address: jason.hall@infocap.ai

   Phone Number: 202-899-8895

FR MENU

Marketplace **Products** **Federal High Impact Virtualized Environment (FedHIVE)**

Human Resources Technologies, Inc. (HRTec)

Federal High Impact Virtualized Environment (FedHIVE)

Visit their website

Status	Certification Class	Authorizations
FedRAMP Certified *As of 12/7/2020*	Class D (High)	4
Package ID	**Certification Type**	**Reuses**
FR1802451335 Package Request Form	Rev5	3

Overview Agency Authorization Details Dependent Products

Service Description

Give Feedback

Disclaimer: FedRAMP does not review or endorse vendor-submitted content. Vendors are responsible for accuracy of product descriptions, provided services, and contact information.

FedHIVE® is the only FedRAMP High Authorized accelerator platform delivering Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) capabilities within a single High-impact authorization boundary. Originally granted a Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the FedRAMP High baseline, FedHIVE enables broad reuse across Federal and DoD agencies and significantly reduces redundant security assessment efforts. FedHIVE implements and continuously manages over 400 NIST SP 800-53 Rev. 5 High baseline security controls within its boundary, including 24/7 Security Operations Center (SOC) operations, automated continuous monitoring, vulnerability management, patching, incident response, and independent third-party validation activities. The environment is designed to protect Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII) at the FIPS PUB 199 High level and currently supports multiple federal agencies, including DoD, U.S. Space Force, TSA, and the Department of State. FedHIVE also holds a DISA Provisional Authorization at IL4 and IL5, is GovRAMP (StateRAMP) authorized, and meets the Cybersecurity Maturity Model Certification(CMMC) Level 2.

FedHIVE accelerates the authorization process by providing sponsorship and enabling full High baseline control inheritance, allowing SaaS providers to achieve FedRAMP High ATO status significantly faster and at substantially lower total cost than building and sustaining a High environment independently. Unlike models that require containerization or major re-architecture, FedHIVE supports lift-and-shift migration of legacy systems, COTS applications, and complex enterprise stacks with minimal re-

engineering; containers are supported but not required. The platform enables hybrid architectures spanning private GovCloud and hyperscaler environments such as AWS, Google Cloud, and Azure within the same authorized boundary, eliminating the need to re-initiate compliance when scaling. By managing the full security stack—including infrastructure, platform services, data protection, identity, and continuous monitoring—FedHIVE reduces compliance duplication, lowers long-term operational burden, and provides an economically efficient alternative to multi-million-dollar DIY FedRAMP High builds. Its compliance team includes former working-level FedRAMP and DISA personnel who have executed authorization and assessment activities within the federal ecosystem, strengthening implementation rigor and operational readiness.

FedHIVE enables the secure federal deployment of commercial and enterprise solutions and mission applications within its authorized High-impact environment including:
1Kosmos Platform - Powered by biometric verification, government-issued credential validation, and advanced liveness detection, the 1Kosmos Platform ensures the right person accesses the right systems. Purpose-built for high-impact federal systems, it also delivers phishing-resistant authentication and a digital identity wallet. Deploy as a complete identity solution or modular components: identity verification, digital wallet, or passwordless MFA. Zero passwords. Zero shared secrets. Zero trust, verified.

- ACF Customer Experience Platform - ACF Customer Experience Platform is a cloud-based SaaS solution hosted on Microsoft Azure that helps enterprise organizations manage customer interactions through appointment

scheduling, queue management, automated communications, and AI-powered analytics. Serving 500+ clients across healthcare, government, banking, retail, and education sectors.

- Allocore ULP-UGP-UFP Software - Allocore's ULP, UGP, and UFP platforms provide FedRAMP High–authorized, cloud-based lifecycle management for federal loans and grants, delivering advanced origination, workflow automation, servicing, compliance, and auditability aligned with federal program requirements. Together, they integrate AI-driven fraud detection, real-time risk assessment, and cross-program data intelligence to help agencies prevent improper payments and strengthen program integrity across lending and grant operations.

- Archer Risk and Resilience Management (RRM) - Archer Risk and Resilience Management enables organizations to strengthen resilience by identifying critical products, services, and dependencies, defining impact tolerances, and coordinating risk-driven actions across business, IT, operational risk, and cyber teams. It provides integrated visibility into resiliency risks, supports preparation for disruptions such as natural disasters or cyber events, and helps organizations adapt, withstand, and recover through structured scenario analysis and operational resilience workflows.

- Contegix TrueStack (TSX) - a secure, FedRAMP-authorized, and DoD-compliant managed application platform designed to help government and regulated agencies deploy collaborative tools like Atlassian (Jira, Confluence), GitLab, and MatterMost. It focuses on Zero Trust security, handling

compliance, hosting, and maintenance to streamline secure DevSecOps.

- Contegix TrustStack Atlassian Confluence - Delivered on Contegix's FedRAMP High authorized cloud platform, providing secure, compliant hosting of Atlassian Confluence for federal agencies.

- Contegix TrustStack Atlassian JIRA - Hosted within Contegix's FedRAMP High authorized cloud environment to enable secure Jira use and migration for agencies requiring high-impact compliance.

- Contegix TrustStack Mattermost - A secure collaboration platform offered through Contegix's FedRAMP-certified DevSecOps ecosystem, supporting high-impact environments and compliant deployment of Mattermost.

- Dell PowerStore - Dell PowerStore delivers high-performance, all-flash storage with advanced data reduction and automation to support mission-critical government workloads. Its secure, efficient NVMe architecture and always-on protection help agencies modernize infrastructure, improve resilience, and meet evolving demands across hybrid environments.

- Dell PowerSwitch - Dell PowerSwitch provides flexible, high-performance Ethernet switching from edge to core, helping government agencies modernize networks with open architectures, scalable designs, and secure,

reliable connectivity. Its agility and efficiency support mission-ready operations across data centers, campuses, and cloud environments.

- First Due Fire and EMS RMS Software - First Due and E-9 Corporation deliver a FedRAMP HIGH -authorized solution unifying Fire incident reporting, ePCR, fire prevention, scheduling, analytics, and response. Trusted by over 3,000 civilian jurisdictions, every DoW branch, and a growing number of Federal Civilian agencies, the all-in-one suite streamlines operations and protects mission-critical data.

- FormAssembly Gov Cloud Fed – Provides a FedRAMP High–authorized, no-code platform to securely manage and automate sensitive data collection. It modernizes processes from simple paper forms to sophisticated, multi-respondent processes through role-based access controls, encryption, audit trails, and integrations with gov-preferred systems such as Salesforce Government Cloud, Microsoft 365 Government, and Google Workspace FedRAMP.

- Hitachi - Hitachi's government-ready storage platforms deliver mission-focused performance, cyber-resilience, and scalability across core data centers and edge environments. Designed for secure, compliant, and hybrid-cloud operations, they support AI-driven workloads while ensuring high availability and robust data protection for critical agency needs.

- HPE Greenlake - HPE GreenLake for Government delivers a secure,

on-premises, pay-per-use cloud platform that scales with public-sector demand. It provides data sovereignty, strong security, simplified procurement, and hybrid-cloud agility—modernizing IT while preserving control and ensuring resilient, compliant service delivery for agencies.

- Horizon3.ai Node Zero Federal - NodeZero delivers FedRAMP High-authorized autonomous security testing and validation. Continuously hack, fix, and verify exploitable attack paths across your entire infrastructure, from weak credentials and misconfigurations to exposed data, failed controls, and weak policies without disrupting missions. Accelerate ATO readiness, prioritize remediation, and harden defenses beyond CVEs and patchable vulnerabilities.

- OneNet Emergency Management Platform – Platform as a Service (PaaS) cloud-native Emergency Management Platform providing Computer-Aided Dispatch OneNet CAD, ESRI native OneNet MAP, OneNet MOBILE and OneNet Revere (iOS and Android). Purpose-built for federal and DoW force protection and public safety, its microservices architecture ensures high availability, real-time multi-agency coordination, and mission-critical resilience. OneNet was designed for and is FedRAMP HIGH authorized having been deployed for years within DoW components.

- Portworx - Portworx delivers a secure, Kubernetes-native data platform that helps government agencies modernize mission-critical applications with resilient, scalable, and automated container storage. It simplifies operations across hybrid and multi-cloud environments, providing robust data

protection, disaster recovery, and encryption to support compliant, high-availability digital services.

- Red Hat OpenShift - Red Hat OpenShift provides a secure, enterprise-grade Kubernetes platform that helps government agencies modernize applications across on-prem, hybrid, and multi-cloud environments. With built-in automation, CI/CD, and consistent operations, it strengthens mission agility, accelerates modernization, and supports compliant, resilient service delivery.

- RegScale Continuous Controls Monitoring – Streamline your governance, risk, and compliance processes with shift-left security and compliance as code. RegScale's CCM platform delivers constant audit-readiness and continuously self-updating paperwork. Designed as a cloud-native solution, RegScale also delivers hybrid and on-premises options, enabling integration of compliance as code into the CI/CD pipelines, speeding up certification, reducing costs, and future-proofing security posture.

- Tungsten TotalAgility® (formerly Kofax TotalAgility) is an AI-powered automation platform that enables U.S. government agencies to securely process documents, automate workflows, and manage case-driven operations. The platform combines intelligent document processing (IDP), agent-driven automation, and knowledge discovery to help agencies streamline and optimize content-intensive processes. Within the FedRAMP authorization boundary, TotalAgility is implemented as a scalable SaaS solution hosted in a government-authorized Microsoft Azure environment and incorporates security controls aligned with FedRAMP High requirements.

- VMware - VMware enables government agencies to modernize mission-critical IT with secure, scalable virtualization and private-cloud architecture. Its solutions support Zero Trust, application modernization, resilient infrastructure, and seamless workload mobility—helping agencies protect citizen data, improve efficiency, and accelerate digital transformation across hybrid environments.

Certified Services

If there are microservices or applications included within this Cloud Service Offering's (CSO) assessment scope, they are listed below. This may be more applicable to Infrastructure as a Service (IaaS) vendors.

Service(s) added in the last 90 days

- Dell PowerStore
- Dell PowerSwitch
- FileCloud
- HPE Alletra
- HPE Aruba
- HPE GreenLake
- HPE ProLiant Servers
- Red Hat OpenShift
- VMware Cloud Foundation

Other Service(s)

- 1Kosmos BlockID
- Allocore ULP-UGP-UFP Software
- Archer Risk and Resilience Management (RRM)
- Contegix TrustStack Atlassian Confluence
- Contegix TrustStack Atlassian JIRA
- Contegix TrustStack Mattermost
- First Due Fire and EMS RMS Software
- Form Assembly Government Cloud
- Horizon3.ai Node Zero
- OneNet
- RegScale Governance, Risk and Compliance
- Tungsten TotalAgility Cloud®

Vendor Contacts

SALES

info@fedhive.com

SECURITY

Fedramp_security@fedhive.com

PRODUCT WEBSITE
https://www.fedhive.com/

More Info

UEI Number

GJ4HVG535VM9

Business Functions

CUSTOMER SERVICE | CYBERSECURITY & RISK MANAGEMENT | DATA MANAGEMENT | HUMAN RESOURCES | NETWORK MANAGEMENT | OPERATIONS MANAGEMENT | STORAGE | SYSTEM ADMINISTRATION | VIRTUAL PRIVATE NETWORK (VPN)

(Up to 10 tags)

Service Model

IaaS, PaaS, SaaS

Deployment Model

Government Community Cloud

Interact with FedRAMP

LinkedIn

X

YouTube

GitHub

info@FedRAMP.gov
(monitored by real humans who care)

Keep Up To Date

To receive news and updates, join the GSA's subscriber list.

Subscribe

FedRAMP.gov
An official website of the GSA's Technology Transformation Services

About GSA

Accessibility statement

GSA FOIA

No FEAR Act data

Office of the Inspector General

Performance reports

GSA privacy policy

Vulnerability disclosure policy

Looking for U.S. government information and services? **Visit USA.gov**