ORIGINAL

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) John Redfern

(Address) 19 Fulton St. Suite 408 NY, NY 10048

(Phone Number) / (Fax Number) 310-266-0243

(email address) john.redfern@advancedgrc.com

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contained herein; that this bid, offer or proposal constitutes a binding offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise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.

Advanced GRC
(Company)

john redfern
(Signature of Authorized Representative)

John Redfern
(Printed Name and Title of Authorized Representative) (Date)

Government Account Manager
(Phone Number) (Fax Number)

3102660243
(Email Address)

CRFP SEC2600000001 – One-Stop-Shop Portal
TECHNICAL PROPOSAL

Submitted by:
Advanced GRC (AGRC)

Business Address: 19 Fulton Street, Suite 408, New York, NY 10038
Telephone: 212-725-7646

Fax: 212-725-7647
Contact Person: John Redfern
Email: John.Redfern@advancedgrc.com
Phone: 310-266-0243

Authorized Signature: John Redfern
Date: 11/20/2025

Table of Contents

4.2.1. Goals and Objectives

4.2.1.1 Vendors should provide a methodology and explain in details how they would develop and create a user-friendly dashboard interface with public-facing, and internal agency components as a One-Stop-Shop Permitting Portal.

The proposed **ALiS platform** provides an enterprise framework for creating both citizen-facing and internal dashboards that unify information across programs. State administrators can configure each dashboard through the low-code designer to display live metrics such as permit volumes, processing times, inspection outcomes, and renewal trends. Widgets, filters, and drill-downs can be added or modified by authorized staff without code changes, ensuring that every agency maintains its own performance view while contributing to a single statewide picture. Additionally, granular roles and user access allow each user/role view to be customized or limited to ensure they see only what they need to in order to keep their adoption and use of the solution easy and efficient.

Behind each dashboard, ALiS aggregates data from licensing, inspection, and financial modules in real time through its reporting API. Decision-makers gain visibility into workload distribution and compliance statistics, while public users can track application status and receive transparent progress updates. This design was proven in Vermont DOE's educator licensing portal and Colorado DPHE's inspection environment, where configurable dashboards improved transparency and shortened processing time by allowing management to act on real-time metrics.

4.2.1.2 Vendors should describe how they would implement a flexible and secure Role-Based Access Control system.

ALiS includes an extensive User Management subsystem that supports multi-agency role hierarchies and least-privilege access. Each user may hold roles across multiple business units, enabling inter-agency collaboration while keeping data boundaries intact. Administrators can define roles such as Intake Clerk, Reviewer, Inspector, Finance Officer, or Supervisor and assign permissions to screens, workflow actions, and data sets through configuration rather than code.

The platform integrates with the State's identity provider through SAML 2.0 Single Sign-On,

letting staff authenticate with their government credentials while external applicants use secure portal accounts. All authentication events and role changes are logged for auditability, aligning with NIST 800-53 and FIPS 140-3 controls. This configuration model successfully implemented in Nevada DPBH and Colorado DPHE has demonstrated both ease of administration and strong compliance posture.

4.2.1.3 Vendors should explain how they will design a user-friendly, and responsive interface that tracks applications through the approval process and the ability to apply for additional permits or other licenses as needed.

At the core of ALiS is a configurable application lifecycle engine that guides users from initial submission to final approval. Applicants interact through an intuitive portal that presents required questions, attachments, and attestation statements specific to the license type. Statuses such as Submitted, Under Review, Approved, or Returned for Revision are displayed visually in the applicant dashboard, providing transparent, self-service tracking.

User-Friendly, AI-Enabled, and Accessible Resident Portal

Advanced GRC will deliver a resident portal that is WCAG 2.1 AA compliant, intuitive, and designed to serve all users equitably — regardless of age, device, language preference, or accessibility needs. To lead this effort, we will assign a dedicated **User Experience (UX) Analyst** who will collaborate with County stakeholders and accessibility experts to ensure the portal is easy to navigate, visually clear, and optimized for all residents. This UX Analyst will guide wireframing, usability testing, and interface design to ensure every step — from login to permit submission — is streamlined and frictionless.

To validate accessibility and usability, we will use **heatmapping, clickstream tracking, and accessibility compliance audits** to monitor real-time user behavior and flag potential barriers. These insights will drive continuous refinements based on actual resident usage — not assumptions. This includes tailoring layouts for screen readers, enabling keyboard navigation, simplifying mobile forms, and improving content clarity for non-technical users. Our reporting tools will also give the County visibility into interaction trends, drop-off points, and compliance scores.

In addition, the portal will support **AI-enabled chatbot integration** through one of our technology partners. This chatbot can answer resident questions in real time, walk users

through permitting steps, and surface relevant FAQs based on their inputs — all without requiring human intervention. By combining conversational AI with dynamic, searchable FAQ modules, we help residents find answers faster and reduce call center volume. These features also support multilingual capabilities and 24/7 access, making the portal more inclusive and responsive to community needs.

Staff reviewers see the same application within their task queue, complete with electronic checklists, audit flags, and supporting documents. Multiple permits can be applied for within one submission when business rules permit, and each license type may carry its own fee schedule or workflow.

4.2.1.4 Vendors should describe how the solution assists public users through the application process, the vendor should implement an intelligent, interactive assistant (AI) or automated tool embedded within the public dashboard.

ALiS supports appropriate guidance and dynamic help content throughout its low-code portal. Administrators can configure a **guided help panel** that surfaces FAQs, workflow instructions, or next-step recommendations based on the user's current page or role. Optional integration points allow the State to connect approved AI or chatbot services through secure APIs, providing conversational assistance without altering the core product.

4.2.1.5 Vendors should explain how the solution would implement a dynamic and transparent tracking system within the public dashboard that would provide public users with up-to-date visibility into the status and progress of their applications throughout the approval workflow.

ALiS offers real-time visibility into every submission and workflow stage. Each license or permit record automatically reflects its current status such as *Submitted*, *In Review*, *Awaiting Payment*, or *Approved* which is displayed to both applicants and reviewers. Authorized users can filter, export, and analyze this data through dashboards or ad-hoc reports without technical assistance. The transparency reduces calls to agency offices and builds public trust in the State's review process.

The platform's workflow designer allows West Virginia to configure any number of processing steps or status codes. Once implemented, automated notifications and color-coded progress bars update instantly when a reviewer completes an action.

4.2.1.6 Vendors should explain how the solution will implement a robust session management and draft-saving system for mid-process applications.

The ALiS portal manages user sessions through secure tokens and configurable time-outs, ensuring data protection while supporting a smooth user experience. Applicants can save partially completed applications as *Draft* and return later from any device without losing progress. All saved drafts are encrypted and linked to the authenticated user profile, preventing unauthorized access.

Administrators may adjust session durations or draft-retention periods directly from the configuration console. This low-code flexibility enables the State to align user convenience with cybersecurity policy.

4.2.1.7 Vendors should describe how the solution implements a transparent and dynamic time-tracking module within the public dashboard.

ALiS captures time stamps for every workflow transition and aggregates them into dashboards that measure processing durations by stage, reviewer, and license type. Managers can view average review times, identify bottlenecks, and export results to Excel for analysis. The reporting tool requires no scripting authorized staff build or modify metrics through drag-and-drop fields.

These analytics give the State real-time insight into workload and efficiency.

4.2.1.8 Vendors should explain how the proposed solution implements a mobile-friendly, offline-capable inspection module that allows field

inspectors to work seamlessly without network connectivity, then queue those for automatic upload once connected to a network

ALiS includes a dedicated **Inspections module** designed for both online and offline operation. Inspectors using tablets or laptops can download scheduled inspections, complete electronic forms, capture photos and signatures, and sync results once connectivity is restored. The system automatically reconciles data conflicts and records synchronization history for auditing.

All inspection forms, scoring criteria, and deficiency codes are configurable through the low-code designer. Implementing this will enable inspectors to conduct on-site evaluations efficiently and securely, even in low-connectivity areas.

4.2.1.9 Vendors should explain how the solution is accessible with mobile devices for both public and agency users, the system should be designed with an approach that ensures full functionality, usability, and performance across mobile devices such as smartphones and tablets.

The ALiS interface is responsive by design and optimized for smartphones, tablets, and desktops. All screens, dashboards, and forms automatically adjust to the device's resolution, ensuring accessibility without separate mobile apps. The portal adheres to WCAG 2.1 and Section 508 guidelines, including keyboard navigation and contrast standards.

4.2.1.10 Vendors should describe how the solution implements a flexible and user-controlled notification system. The system should allow users to be able to sign up for an receive workflow notifications throughout the process through email, mobile phone, or both as the individual chooses.

ALiS includes a configurable notification engine that supports email, SMS, and in-portal alerts. Administrators can define when and how each notification is triggered, for example, on status change, upcoming renewal, or payment confirmation. Applicants choose their preferred communication channel, and all templates are editable through a simple

interface.

Messages can include dynamic merge fields (e.g., license number, due date) and are logged for audit tracking. The same automation will let West Virginia agencies maintain proactive, personalized communication with constituents.

4.2.1.11 Vendors should explain how the solution includes a flexible, secure, and user-friendly form and document management module with the ability to upload documents or create fillable forms for certain permits as needed.

ALiS offers comprehensive document and form management across all modules. Agencies can design online forms with rich validation, conditional logic, and file-upload fields. Uploaded documents are stored in the platform's encrypted repository and linked to the relevant record, ensuring chain-of-custody and version control. Reviewers can annotate, approve, or request additional documentation directly within the interface.

The low-code form builder allows administrators to modify questions, attach supporting documentation requirements, or publish new forms instantly, no coding needed.

4.2.1.12 Integrate seamlessly with existing portals and systems to enhance accessibility and functionality

ALiS has a **data-exchange service layer** built on RESTful APIs and secure file interfaces, enabling interoperability with existing state systems such as payment processors, GIS, and document archives. Integration adapters manage inbound and outbound data flows while enforcing schema validation and error logging.

4.2.1.13 – Provide ongoing support and maintenance while ensuring program and data security

ALiS includes a comprehensive **support and maintenance framework** designed for government operations that require continuous uptime and secure change control. The vendor-hosted environment operates under documented SLAs, scheduled maintenance windows, and versioned release management. All enhancements, patches, and hotfixes

are tested first in a sandbox environment before promotion to production, guaranteeing system stability.

Security is embedded throughout the lifecycle: vulnerability scans, role-based access audits, and encryption of data in transit and at rest maintain compliance with NIST 800-53 and FIPS 140-3. The same operations model supports Vermont DOE and Colorado DPHE, where ALiS maintains over 99.9 percent availability while providing quarterly releases aligned with state change-management procedures. West Virginia will benefit from predictable updates, transparent ticketing, and certified security controls that exceed state standards.

4.2.1.14 – Provide a comprehensive, flexible, and interoperable solution minimizing disruption

ALiS's architecture was purposely engineered for **multi-agency interoperability** and phased deployment. Its modular, low-code framework allows the State to onboard one program at a time, map existing processes, and gradually retire legacy systems without service interruption. Each business unit retains autonomy over its data, forms, and workflows while leveraging shared infrastructure such as user authentication, payments, and reporting.

The solution communicates through standardized APIs, supporting data exchange with ERP, GIS, and content-management systems. This flexibility allows the State to modernize incrementally, lowering risk. Similar phased rollouts in Vermont DOE and Nevada DPBH showed that agencies could transition within months rather than years while preserving regulatory continuity and public-facing operations.

4.2.1.15 – Provide a clear implementation timeline and recommendation (integrate vs replace) ensuring full deployment by January 1, 2027

The ALiS implementation approach begins with a joint discovery and fit-gap analysis to determine which legacy systems should be integrated and which can be retired. Because ALiS already provides licensing, inspection, payments, and reporting functions out of the box, most programs can migrate by configuration alone. When integration is preferable, the system's API framework supports direct, secure data connections.

A detailed project schedule—with milestones for configuration, testing, user training, and go-live is included in ALiS's standard project-management plan. Similar statewide deployments in Vermont DOE and Colorado DPHE were completed as scheduled for their initial programs. This proven methodology ensures West Virginia meets or exceeds its statutory deadline while maximizing reuse of existing assets.

4.2.1.16 – Provide a "train-the-trainer" program

ALiS's deployment methodology includes a structured **train-the-trainer curriculum**. Core agency staff are trained not only in daily operations but also in configuration skills creating license types, editing workflows, and designing reports so the State maintains long-term self-sufficiency. All sessions combine hands-on exercises, system demonstrations, and guided labs within the sandbox environment.

Graduates of this program become internal subject-matter experts capable of onboarding new users or adjusting processes without vendor assistance. Vermont DOE and Nevada DPBH both leveraged this model to build permanent in-house configuration teams, reducing support dependency significantly. West Virginia will gain the same capability, ensuring knowledge transfer and operational independence.

4.2.1.17 – Provide self-paced learning and on-demand resources for users

The ALiS platform includes a comprehensive **self-paced, on-demand learning ecosystem** designed to ensure rapid and sustainable adoption across all user groups agency staff, administrators, reviewers, inspectors, finance teams, and external applicants. ALiS elevates the State's readiness through a blended learning model that mirrors best practices from our statewide deployments.

4.2.1.18 – Integrate with Google and Microsoft productivity tools

ALiS's open integration layer allows seamless connectivity with **Google Workspace** and **Microsoft 365** environments. Through standardized APIs and secure OAuth connections,

notifications can be delivered to Outlook or Gmail, calendar invites can synchronize with inspection schedules, and documents can be exchanged with OneDrive or SharePoint repositories.

4.2.1.19 – Ensure scalability to onboard additional agencies and support state growth

ALiS was designed as a **multi-tenant, enterprise-scale platform** capable of supporting dozens of agencies under a single statewide instance. Each agency operates as a configurable "business unit," preserving separate workflows and data schemas while sharing the same infrastructure and security model. The system's horizontal scaling and containerized architecture allow rapid resource expansion without downtime.

This scalability has been validated in Nevada DPBH, where ALiS manages thousands of facility and professional licenses across multiple bureaus. The same architecture enables West Virginia to begin with priority agencies and expand as adoption grows, guaranteeing consistent user experience and centralized administration even as volume increases.

4.2.1.20 – Provide high availability, transparent maintenance windows, and rapid recovery

ALiS's hosting model available in FedRAMP-authorized cloud environments delivers enterprise-grade **availability and disaster-recovery protections.** The platform employs multi-zone redundancy, real-time replication, and automated failover. Scheduled maintenance windows are announced in advance through the system's notification framework, and updates occur during predefined low-usage periods.

Comprehensive monitoring dashboards track performance, uptime, and response metrics in real time. In production, Vermont DOE and Colorado DPHE maintain 99.9 percent uptime with recovery times measured in minutes. West Virginia agencies will benefit from the same resilient infrastructure, ensuring continuous service delivery to citizens and staff.

4.2.1.21 – Describe project-management approach and tools

AGRC follows proven **Hybrid Agile–Waterfall project-management framework** for ALiS implementation tailored for public-sector IT programs. Team conducts iterative configuration sprints with weekly demonstrations and sprint reviews so that State stakeholders can see progress in real time. Jira and Smartsheet are used for backlog tracking, sprint planning, and risk management, while MS Project provides milestone visibility for executive reporting.

Each engagement begins with a detailed implementation roadmap defining phases for discovery, configuration, data migration, testing, and training. This structured yet adaptive approach validate functionality early ensuring schedule adherence and minimizing rework for West Virginia's One-Stop-Shop rollout.

4.2.1.22 – Integrate with the State's Single Sign-On environment

ALiS natively supports **SAML 2.0 Single Sign-On** integration and has successfully connected with multiple state identity-management systems. The configuration allows the client staff to access the application through existing government credentials, eliminating redundant logins and improving security posture. External applicants authenticate through a secure portal account with multi-factor options when required.

This integration centralizes user lifecycle management under the State's control, aligning with cybersecurity standards and reducing administrative overhead. Vermont DOE and Nevada DPBH both operate ALiS under state SSO, achieving seamless access for thousands of users while maintaining strict separation of agency data.

4.2.1.23 – Provide pricing for build-out, milestones, and annual licensing/hosting/maintenance

The ALiS pricing framework is transparent and modular, separating **implementation, licensing, hosting, and support** components. Implementation costs are milestone-based covering discovery, configuration, testing, and go-live while annual fees include software licensing, FedRAMP-certified hosting, and Tier 2/Tier 3 support. This model allows the State to plan budgets confidently over the contract term.

Because ALiS is low-code and configuration-driven, future enhancements or new-agency onboarding typically incur configuration rather than development costs. This cost

predictability was a decisive factor for Vermont DOE and Colorado DPHE, both of which expanded usage without renegotiating core licensing terms.

4.2.1.24 – Ensure all work is performed in the U.S. and excludes tools from federally banned countries

All ALiS implementation, support, and hosting services are performed **entirely within the United States**. Development, configuration, and help-desk operations are staffed by U.S.-based personnel who hold appropriate background clearances. The hosting environment resides in U.S. data centers operated by FedRAMP-authorized providers, ensuring compliance with federal and state procurement restrictions.

4.2.1.25 – Provide a digital wallet for payments, refunds, and license management

ALiS features an integrated **financial and payment-tracking module** that acts as a digital wallet for each applicant. Users can store payment methods, review invoices, request refunds, and view the balance of fees across multiple permits all from a unified dashboard. Transactions flow through state-approved payment gateways, and reconciliation data is available to treasury staff in real time.

Every financial event is tokenized and auditable, ensuring compliance while giving citizens a modern, retail-like payment experience.

4.2.2. Mandatory Project Requirements:

4.2.2.1 – Provide a solution to develop the One-Stop-Shop Permitting Portal

The ALiS platform delivers a comprehensive, enterprise-grade foundation for developing and operating West Virginia's One-Stop-Shop Permitting Portal. Built specifically for government licensing and regulatory programs, ALiS unifies all permitting activities including application intake, review, inspection, compliance, and renewal within a

configurable, low-code environment. The platform's modular design allows the State to create a shared ecosystem serving multiple agencies while preserving each agency's autonomy over its workflows, data, and branding.

From a technical standpoint, ALiS uses a multi-tenant, business-unit architecture that supports numerous departments under one statewide instance. Each business unit (e.g., Commerce, DEP, OEHS, Revenue, Tourism, Transportation, Secretary of State) can configure its own license types, fee structures, and approval chains without vendor coding. The solution's drag-and-drop form builder, workflow designer, and notification engine allow authorized State administrators to tailor processes dynamically reducing implementation time.

The public-facing portal provides a single point of entry for citizens and businesses to discover, apply for, and track permits across agencies. Using ALiS's built-in service catalog and search engine, users can answer guided questions that direct them to the correct permit type. The same portal provides dashboards for applicants and agency staff, giving transparent visibility into submission status, payment history, inspections, and renewal dates. These dashboards are fully configurable through the low-code interface, requiring no custom development.

ALiS's underlying infrastructure supports RESTful APIs, secure SSO (SAML 2.0), and FedRAMP-authorized hosting, enabling seamless integration with existing State systems such as financial services, GIS, or document management. The platform meets NIST 800-53 and FIPS 140-3 encryption standards, ensuring that all data at rest and in transit remain secure within U.S.-based data centers.

This approach has already proven successful in Vermont DOE where ALiS powered the Educator Licensing Portal consolidating several workflows into one low-code platform, and in Colorado DPHE where multiple permitting programs were unified into a single web application with real-time status tracking. For West Virginia, the same architecture enables rapid configuration, centralized visibility, and a modern digital experience aligned with the State's mission to simplify public access and streamline agency operations.

4.2.2.2 – Provide a structured, transparent, and collaborative methodology ensuring timeliness, alignment, and quality assurance

ALiS implementations follow a **structured and transparent Agile delivery methodology** refined through multiple statewide digital transformation projects. The approach combines Scrum-based configuration cycles with formal governance and quality assurance checkpoints, ensuring that every deliverable meets State expectations and contractual timelines. The methodology is anchored by three guiding principles: collaboration, visibility, and accountability.

At project initiation, the project team conducts a **Joint Application Design (JAD) and Fit-Gap Analysis** workshop with all participating agencies. These sessions map existing business processes, identify pain points, and align them with the ALiS modules Licensing, Inspections, Complaints, Payments, and Reporting. The outcome is a detailed Configuration Blueprint and Sprint Plan that prioritizes requirements into manageable increments. This early alignment minimizes rework and guarantees that agency priorities drive the configuration sequence.

Each sprint typically runs for two to three weeks and concludes with a **Sprint Review and Stakeholder Demonstration**, during which the State team can see and test completed configurations in the sandbox environment. Feedback is logged in Jira or Smartsheet for transparent tracking, with every issue assigned a responsible owner and expected resolution date. Daily stand-ups and weekly progress meetings between the project manager, State PMO, and technical leads ensure that potential delays or scope concerns are addressed immediately.

We employ a **hybrid Agile–Waterfall governance model** to align iterative development with the State's formal procurement and oversight processes. High-level milestones requirements sign-off, user acceptance testing (UAT), and production release are defined in the Master Schedule, while Agile ceremonies provide iterative visibility and validation between those milestones. This ensures predictable delivery without sacrificing flexibility.

Quality assurance is embedded throughout the lifecycle. Each sprint undergoes peer code review (for configurations), automated regression testing, and business acceptance testing before promotion to staging.

4.2.2.3 – Meet West Virginia Office of Technology (WVOT) data security requirements across all stages of the project

Security is foundational to ALiS's architecture, hosting model, and implementation approach. The platform is designed to fully align with the West Virginia Office of Technology (WVOT) security framework, as well as federal security requirements including NIST SP 800-53 Rev5, and FedRAMP Moderate/High baselines.

The system operates in a FedRAMP-authorized cloud environment that provides hardened infrastructure, continuous monitoring, and documented security controls. ALiS enforces **AES-256 encryption at rest, TLS 1.2+ in transit**, secure key management in HSM-backed KMS services, and strict role-based access control. All security-relevant events authentication, data exports, configuration changes, and administrative actions are recorded in immutable audit logs with long-term retention.

ALiS uses continuous monitoring tools, automated vulnerability scanning, privileged-access logging, and configuration-drift detection to ensure ongoing compliance.

4.2.2.4 – Ensure the solution meets FedRAMP requirements

The **ALiS platform** is deployed in **FedRAMP-authorized cloud environments**, ensuring that client inherits the same rigorous security controls, monitoring, and compliance standards used by federal agencies. FedRAMP provides a government-wide baseline for security assessment, authorization, and continuous monitoring, and ALiS's hosting model meets or exceeds those standards, depending on agency data classifications.

From an architectural perspective, ALiS leverages **FedRAMP-certified Infrastructure-as-a-Service (IaaS)** providers such as Amazon Web Services GovCloud or Microsoft Azure Government where data is housed exclusively in **U.S.-based data centers**. This ensures compliance with federal requirements and aligns directly with client's data residency policies.

At the **application level**, ALiS implements security controls aligned to **NIST SP 800-53 Revision 5**, covering access control (AC), audit and accountability (AU), configuration management (CM), incident response (IR), and system integrity (SI). The solution enforces **encryption at rest (AES-256)** and **encryption in transit (TLS 1.2 or higher)**, supported by FedRAMP-validated cryptographic modules compliant with **FIPS 140-3**. Continuous monitoring dashboards capture and report compliance metrics to both the vendor and State security officers, ensuring traceability of any deviations or incident responses.

Before deployment, each update passes through a formal **Change Control Board (CCB)** review, and all associated risk assessments are documented in the project's Configuration Management Database (CMDB). Audit evidence including vulnerability scan reports, patch logs, and compliance certificates is made available to the State for verification.

4.2.2.5 – Encrypt State data at rest and in transit (FIPS 140-3)

The **ALiS platform** employs a comprehensive encryption and key-management framework to ensure that all State data remains protected both **at rest** and **in transit**, in full compliance with **FIPS 140-3** and aligned with client's security standards. Encryption is embedded natively within the product architecture covering databases, file storage, backups, message queues, and network connections to safeguard sensitive licensing, inspection, and financial data throughout its lifecycle.

At rest, every database table, document repository, and backup file is encrypted using **Advanced Encryption Standard (AES) 256-bit** algorithms validated under FIPS 140-3. Within the application, individual fields containing personally identifiable information (PII) such as names, addresses, Social Security numbers, and payment tokens are encrypted separately from the broader database layer to prevent exposure even to privileged administrators.

In transit, ALiS enforces **Transport Layer Security (TLS) 1.2 or higher** across every network connection, including portal access, API calls, data-exchange integrations, and administrator consoles. Certificate management follows strict lifecycle controls: certificates are issued by trusted certificate authorities, renewed automatically, and revoked immediately if compromise is suspected.

For data interchange, ALiS's **Data Exchange Platform** enforces end-to-end encryption and digital signing for all import/export activities. Files transferred via SFTP use ephemeral encryption keys, and API payloads are signed using SHA-256 or higher.

4.2.2.6 – Ensure Subcontractor compliance, notification to WVOT, and restrictions on transfer or subcontracting without consent

Advanced GRC doesn't do subcontracting.

4.2.2.7 – Security controls aligned to NIST 800-53.

ALiS implements a comprehensive security control framework fully aligned to NIST 800-53 Rev5. Controls are derived from the underlying FedRAMP Moderate/High authorization of the hosting environment and extended through ALiS's application-level safeguards, operational procedures, and organizational security policies.

Key control coverage includes:

- Access Control (AC): Role-based access, least privilege, MFA, SSO integration
- Audit & Accountability (AU): Immutable logs, log retention, automated monitoring
- Configuration Management (CM): Baseline configuration, version control, change governance
- Incident Response (IR): IR procedures, escalation timelines
- System & Communications Protection (SC): Network segmentation, encryption, data isolation
- Risk Assessment (RA): Vulnerability scoring, mitigation planning
- Contingency Planning (CP): Backup, DR, failover testing

4.2.2.8 – Implement a proactive and transparent security program with vulnerability scanning and routine reports to WVOT.

ALiS maintains a proactive security and vulnerability-management program supported by continuous scanning, automated alerting, and transparent reporting to the State. Vulnerability detection occurs across infrastructure, application components, APIs, containers, and dependencies using certified tools.

All findings are assigned severity ratings based on CVSS scoring, logged into a ticketing system , and remediated according to documented SLAs. Remediation progress is tracked.

Additionally, ALiS performs periodic code scans, dependency checks, container image scanning, penetration testing, and configuration drift detection. This transparent, collaborative program ensures WVOT retains continuous visibility into the platform's security posture and remediation performance.

4.2.2.9 – Define timeframes for remediation of critical vulnerabilities according to industry and State standards.

ALiS enforces strict, measurable remediation timelines aligned with industry best practices, CIS Controls, FedRAMP Continuous Monitoring, and State standards. Required

timeframes include:

- Critical vulnerabilities (CVSS 9.0–10.0): Remediated within 72 hours
- High vulnerabilities (CVSS 7.0–8.9): Remediated within 5 business days
- Medium vulnerabilities (CVSS 4.0–6.9): Remediated within 10 business days
- Low vulnerabilities: Addressed in normal release cycles (≤30 days)

When a critical vulnerability is detected, ALiS immediately initiates the incident-response process, notifies WVOT, and applies interim mitigations until a full patch is deployed. All remediation actions, test validations, and closure evidence are documented.

4.2.2.10 – Provide a resilient and secure backup/disaster recovery strategy aligned with SLA requirements

AGRC support Disaster Recovery and share Disaster Recovery Policy if asked.

4.2.2.11 – Ensure the ability to migrate the solution into an existing State cloud tenant after build

The ALiS platform is architected from inception for portability and cloud-tenant neutrality, enabling clients to migrate the full solution including applications, configurations, and data into the State's existing cloud tenant if required after initial implementation.

Architecture designed for portability:
ALiS runs on a modular, three-tier architecture comprising web, application, and data layers orchestrated through scripts that can be redeployed within the State's existing AWS GovCloud, Azure Government, or other compliant infrastructure. All dependencies, configuration parameters, and environment variables are defined through parameterized templates, allowing the complete environment to be instantiated through automation. This ensures the system can be lifted and shifted into the State's cloud tenant.

Data migration and synchronization approach:
ALiS supports exportable and auditable data formats (JSON, XML, CSV) and exposes secure RESTful APIs for data exchange, ensuring full transparency during migration. The platform's Data Exchange Engine automates incremental data synchronization between the vendor-hosted environment and the State's designated tenant until cutover. This process involves near-real-time replication of all licensing, inspection, and payment data, verified through checksum validation and record counts. File attachments, document

repositories, and user configurations are transferred using encrypted pipelines (TLS 1.2 or higher), and all transfers are logged with unique transaction identifiers for traceability.

Governance and transition planning:
The migration process is governed by a Formal Transition Plan developed jointly by the ALiS project team and the client. This plan includes detailed timelines, pre-migration validation steps, rollback procedures, and post-migration testing. Prior to transition, Advanced GRC will conduct an environment readiness assessment to verify resource sizing, IAM configuration, and networking compatibility within the State tenant. The migration will then occur in three controlled stages:
1. Environment Provisioning and Baseline Deployment – ALiS containers and databases are instantiated in the State's tenant.
2. Data Synchronization and Validation – Data sets are mirrored and verified for integrity.
3. Production Cutover and Post-Migration Testing – Final switchover occurs with live transaction verification, followed by user acceptance testing (UAT).

All documentation, scripts, and automation artifacts used during migration are provided to the client to maintain complete transparency and enable future redeployments without vendor assistance.

Security and compliance continuity:
Throughout the migration, the system remains compliant with FedRAMP Moderate/High, NIST 800-53, and FIPS 140-3 controls. Encryption keys, certificates, and secrets are securely transferred using Hardware Security Modules (HSMs) and rotated upon deployment in the new environment. Audit logs, access controls, and monitoring configurations are retained and seamlessly integrated into the State's existing security tooling and SIEM systems.

Operational validation:
After migration, ALiS conducts a comprehensive Operational Readiness Review (ORR) in partnership with client to confirm system stability, user access, and data fidelity. This includes penetration testing, failover validation, and end-to-end functional testing. Any issues identified are documented in the Migration Validation Report, with remediation steps implemented before formal acceptance.

4.2.2.12 – Make the project management interface accessible to the State team at no cost

AGRC **project management framework** is built around the principle of **transparency, collaboration, and shared visibility**, ensuring that the client can monitor schedules, progress, deliverables, risks, and action items in real time without incurring any additional licensing or access fees. The State will have access to the same project management interface, dashboards, and collaboration tools used by the ALiS implementation team, enabling a unified and accountable project governance structure.

Shared project management ecosystem:
ALiS implementations leverage an **integrated project management toolset**, which typically includes **Jira Software** for sprint and backlog management, **Smartsheet or MS Project** for milestone and resource tracking, and **Confluence or SharePoint** for centralized documentation.

Governance and reporting:
A shared **Project Management Dashboard** consolidates all key performance indicators (KPIs), deliverable statuses, and upcoming milestones. The dashboard automatically updates as tasks move through the workflow, giving the State immediate visibility into progress across every module licensing, inspections, payments, integrations, and training. Customizable filters allow client to generate reports on project health, pending approvals, and resource utilization without waiting for manual updates.

Weekly and monthly reports are automatically generated and distributed via email, summarizing completed sprints, risks, blockers, and next steps. All documents such as requirements traceability matrices (RTMs), configuration specifications, and test plans are version-controlled and accessible to the State through this same portal. The system also supports e-signature tracking for document approvals, enabling auditable decision-making.

Collaboration and communication model:
The project team fosters a **joint governance structure** that integrates the vendor PMO with the State's project leadership. Regular meetings daily stand-ups, weekly progress reviews, and monthly steering-committee sessions are scheduled within the project management tool. Agendas, minutes, and action items are recorded directly in the system and shared with all stakeholders. Discussion threads and task comments keep communication traceable and eliminate reliance on email for key project decisions.

Training and onboarding:
To ensure full usability, Advanced GRC provides **training and onboarding sessions** for all State project participants on the chosen project management tools. One-on-one walkthroughs, and quick-reference guides are made available. Project Manager and Scrum Master remain available throughout the project to assist State users with dashboard customization, report creation, or troubleshooting.

Security and access control:
State users are authenticated via **Single Sign-On (SSO)** using their official WV credentials, ensuring secure and auditable access. Role-based permissions restrict sensitive internal documents (e.g., proprietary scripts or credentials) while still allowing full visibility into schedules, deliverables, and test evidence. All data within the project management system is encrypted in transit and at rest, consistent with **FIPS 140-3** and **NIST 800-53** requirements.

4.2.2.13 – Provide real-time data exchange

The ALiS platform provides a fully integrated, real-time data-exchange framework that enables seamless interoperability between the State's existing systems, third-party applications, and external regulatory or payment entities. This capability is central to ALiS's low-code architecture—allowing West Virginia to maintain a unified data ecosystem without duplicative entry, inconsistent datasets, or delays in information synchronization.

Standards-based integration framework:
ALiS exposes a comprehensive Application Programming Interface (API) Gateway built on RESTful web services and compliant with open standards such as JSON, XML, and OpenAPI (Swagger) specifications. These APIs allow secure bidirectional data exchange between ALiS and State systems like the financial management system (ERP), GIS mapping tools, document management repositories, identity providers (Active Directory, Okta, Azure AD), and email/SMS gateways. The API layer supports real-time CRUD (Create, Read, Update, Delete) operations, enabling external systems to both push and pull data as transactions occur within ALiS.

Each API endpoint is protected through OAuth 2.0 and API key-based authentication, and all data exchanges occur over TLS 1.2+ encrypted channels. API throttling and rate-limiting controls prevent misuse or denial-of-service attacks, while audit logs capture every request and response for traceability. For bulk data integrations, ALiS also supports secure

SFTP pipelines and message queues (MQ), allowing asynchronous data exchange when real-time operations are not feasible due to bandwidth or scheduling constraints.

Event-driven architecture for real-time updates:
ALiS uses an event-driven architecture (EDA) to broadcast system changes instantly. Each significant transaction such as application submission, fee payment, inspection completion, or license approval triggers an event message published to the integration bus. Subscribed systems (for example, State reporting tools or notification services) receive updates immediately, ensuring the data reflected in external dashboards or analytics tools is current to the second. This architecture also enables seamless synchronization with public portals, ensuring applicants always view the most recent status of their submissions or renewals.

Data quality and schema management:
The ALiS integration engine includes a Data Mapping and Validation Console that allows administrators to define source-to-target mappings, business rules, and transformation logic through configuration rather than custom coding. The platform validates incoming and outgoing payloads against defined schemas, automatically flagging and quarantining records that fail validation for review. This approach ensures that all exchanges maintain referential integrity and conform to the State's master data model.

Scalability and flexibility:
ALiS's API Gateway is cloud-native and scales automatically to support high transaction volumes across multiple agencies. Whether the State needs to integrate a small workflow such as sending automated notifications to a financial gateway or connect a large data warehouse for cross-agency analytics, the integration framework can handle both with consistent performance and zero downtime. This modular approach means West Virginia can continue adding new interfaces as future programs onboard the One-Stop-Shop platform, without requiring redevelopment.

4.2.2.14 – Vendor's solution must be ADA compliant and meet updated federal requirements

The **ALiS platform** is fully designed to comply with **ADA Title II, Section 508 of the Rehabilitation Act**, and **WCAG 2.1 AA** accessibility standards for public-facing digital services. Accessibility compliance is embedded at the architectural, UI/UX, and

configuration levels, ensuring that every applicant regardless of device, ability, or assistive technology can fully engage with the One-Stop-Shop Permitting Portal.

ALiS employs a responsive, standards-based design system that adheres to accessible visual hierarchies, proper contrast ratios, keyboard navigation, semantic HTML structure, ARIA labeling, and error-validation cues that support users with cognitive or visual impairments. All form fields, dashboards, and workflow screens created within the low-code form designer inherit these accessibility rules automatically, ensuring consistent compliance across agencies and future permit types.

Before release, all configurations undergo automated accessibility validation using tools such as **WAVE**, and **SiteImprove**, followed by manual testing with screen readers (JAWS, NVDA) and mobile accessibility tools. Remediation of accessibility findings is prioritized in accordance with WCAG guidelines. ALiS UI/UX specialists also receive formal annual training on ADA, Section 508, and WCAG updates.

4.2.2.15 – Vendor must provide 3-tier outage reporting

ALiS provides a structured **3-tier outage reporting framework** that ensures timely communication, transparency, and coordinated response in the event of system degradation or downtime. This multi-tier approach is aligned with industry best practices for incident management.

Tier 1 – Automated System Alerts & Dashboard Status

The platform continuously monitors uptime, latency, API responsiveness, and resource utilization. If thresholds are breached, automated alerts are triggered

Tier 2 – State Notifications & Incident Summaries

For any outage that impacts State users, ALiS generates outbound notifications via email to designated contacts. This notification includes:

- Description of the incident
- Affected components
- Initial impact assessment
- Estimated time to investigate

• Next update window

Tier 3 – Root Cause Analysis (RCA) & Post-Incident Reporting

For outages exceeding SLA thresholds or for repeated incidents, Team provides a formal **Root Cause Analysis** document. This report includes:
• Root cause summary
• Timelines and incident chronology
• Mitigation and corrective-action steps
• Long-term prevention measures

4.2.2.16 – Vendor must provide the State's team with access to a sandbox and production environment early on in the development stage

The ALiS implementation methodology ensures that the State receives **early, continuous, and secure access** to both the **sandbox (UAT) environment** and the **production environment** during the earliest stages of the project. This enables real-time validation, security review, and iterative collaboration between Client, agency SMEs, and the ALiS configuration team.

Sandbox Access Early in Development

Within the first few weeks of project kickoff, ALiS provisions a fully functional sandbox environment that includes:
• Early prototypes of workflows
• Draft forms and dashboards
• Initial configurations for testing
• Configurable data for validation

This enables State SMEs to test features as they are developed, provide feedback during each sprint, and ensure requirements are met before UAT and go-live.

Early Production Environment Provisioning

The production instance is provisioned early for:
• Client's infrastructure/security review

- Penetration testing
- SSO and MFA integration testing
- Network and firewall validation
- Load/performance baseline assessments

This approach reduces risk by resolving all infrastructure and security dependencies well before final deployment.

4.2.2.17 – Vendor must provide a disentanglement plan within 6 months of contract award and maintain compliance with Attachment A

ALiS provides a comprehensive **Disentanglement and Transition Plan** that describes how West Virginia can fully transition away from the solution if required ensuring full portability, data ownership, and operational continuity. This plan is delivered as discussed during contract award and remains continuously updated throughout the project lifecycle.

Key Components of the Disentanglement Plan

1. **Data Export Strategy**
- Complete extraction of all licensing, inspection, financial, document, and audit data.
- Standardized formats (JSON, XML, CSV) with schema documentation.
- Secure transmission procedures and checksum validation.

2. **Technical Architecture Documentation**
- Full environment diagrams
- Integration interface definitions
- Configuration inventories
- API specifications

3. **Knowledge Transfer & Training**
- Administrator training for managing data sets, forms, workflows
- System operation, maintenance, and security procedures
- Configuration-management handover
- Runbook and playbook documentation

4. **Transition Timeline & Roles**
- Sequenced tasks for deactivation
- Joint responsibilities between ALiS and the State
- Contingency measures for maintaining operations during migration

4.2.2.18 – Vendor's solution must include and provide ongoing support and maintenance for the duration of the contract (updates, bug fixes, etc.)

The ALiS platform comes with a comprehensive **Support and Maintenance Program** that ensures continuous operational stability, security, and enhancement throughout the life of the contract. This includes corrective support, preventative maintenance, and platform enhancements.

Ongoing Support Services

- **Tier 1–3 support** for technical issues, user inquiries, workflow questions
- **system monitoring and alerting**
- SLA-driven response and resolution timelines
- Dedicated client success manager and escalation paths

Maintenance & Updates

ALiS provides:

- Regular platform updates
- Security patches
- Bug fixes
- Performance optimizations
- Module improvements
- New features based on State needs

All updates are applied first to sandbox/UAT, validated by the State, and then promoted to production following change-control practices.

Continuous Improvement

The State receives:

- Quarterly product roadmaps
- Release notes
- Enhancement workshops
- Opportunities to join multi-state steering committees for ALiS roadmap input

4.3.1 Qualification and Experience Information — Detailed Responses

4.3.1.1 – Proven track record designing, deploying, and supporting permitting platforms for state or local agencies

Our team has an established multi-state track record delivering modern, cloud-based permitting, licensing, inspection, and case-management platforms for government agencies. The ALiS (Aithent Licensing Information System) platform has been successfully deployed across multiple jurisdictions, supporting complex regulatory programs, multi-agency workflows, and large public user populations.

Examples include:
• Vermont Agency of Education (DOE) – Modernized the statewide Educator Licensing and Renewal System, digitizing 80+ workflows, integrating background checks, and reducing processing times through automated reviews.
• Colorado Department of Public Health & Environment (DPHE)
• Nevada Division of Public & Behavioral Health (DPBH) – Deployed ALiS to manage statewide professional and facility licensing, case tracking, inspections, and enforcement actions.

Across these implementations, ALiS has demonstrated scalability, configurability, and the ability to unify previously siloed regulatory systems, providing States with streamlined operations, transparent public services, and secure, compliant modernization outcomes.

4.3.1.2 – Experience integrating with legacy systems, portals, and third-party tools using APIs and secure data-exchange protocols

ALiS includes a robust Integration Hub that supports real-time and batch exchange with legacy and third-party systems through REST APIs, secure SFTP, message queues, and middleware connectors. We have integrated ALiS with:

- State SSO platforms (Azure AD, ADFS, Okta)
- State payment gateways (NIC, PayPort, PayPal Gov, Payeezy)
- Background check systems (fingerprint/criminal history)
- GIS mapping services
- Enterprise document repositories (SharePoint, OnBase, Google Drive API)
- State ERP systems for fee reconciliation
- External data-validation authoritative sources

Our team brings extensive experience analyzing legacy data structures, mapping schema differences, and building secure translation layers to support incremental modernization. These integrations ensure that ALiS becomes part of the State's broader digital ecosystem rather than a standalone product.

4.3.1.3 – Familiarity with scalable, secure cloud platforms (Azure, AWS, Google Cloud) and disaster-recovery best practices

ALiS is deployed in FedRAMP-authorized AWS GovCloud or Azure Government environments, depending on State preference. Our engineering and DevOps teams are certified in:

- AWS Solutions Architecture (Associate/Professional)
- Azure Administrator / Architect Expert
- Google Cloud Digital Leader

We design ALiS environments using cloud-native services including auto-scaling clusters, multi-region redundancy, encrypted data stores, and continuous monitoring. Disaster recovery is supported through:

- Multi-AZ failover
- Hourly/daily encrypted backups
- RPOs under 1 hour
- RTOs under 4 hours
- Quarterly disaster-recovery drills

This deep cloud expertise ensures the State receives a resilient, secure, and scalable

solution designed for sustained growth and 24/7 availability.

4.3.1.4 – Experience managing sensitive data with encryption, access controls, and audit trails

ALiS is built from the ground up to manage regulated and sensitive information collected across licensing and permitting programs. The platform supports:

- FIPS 140-3 validated AES-256 encryption at rest
- TLS 1.2+ encryption in transit
- Granular role-based access control (RBAC)
- Immutable audit logs of every user and system event
- Column-level encryption for PII and financial data
- Automated access review and certification cycles

4.3.1.5 – Experience training in NIST, CIS, FedRAMP, and state-specific security standards, including vulnerability scanning and incident response

Our security and DevOps staff receive formal, ongoing training covering:

- NIST 800-53 and NIST 800-37 (Risk Management Framework)
- NIST 800-171 (Controlled Unclassified Information)
- CIS Critical Security Controls
- FedRAMP Moderate/High controls
- State cybersecurity & privacy standards
- Vulnerability scanning and secure development practices
- Incident-response coordination, detection, containment, and remediation

These trainings ensure that ALiS remains aligned to evolving cybersecurity requirements and that our team maintains readiness to support State security audits, penetration tests, vulnerability assessments, and compliance reviews.

4.3.1.6 – Ability to tailor project management approach using tools like Jira, Smartsheet, or MS Project

We follow a hybrid Agile–Waterfall approach tailored to State governance processes and procurement expectations. Our project-management toolkit includes:
- Jira for sprint management, backlog refinement, and defect tracking
- Smartsheet or MS Project for milestone/schedule visibility and executive reporting
- Confluence / SharePoint for document control, design artifacts, and decisions
- Weekly demos, sprint reviews, and steering-committee meetings

This approach ensures transparency, traceability, risk management, and predictable delivery proven effective in all previous statewide deployments of ALiS.

4.3.1.7 – History of successful train-the-trainer programs and self-paced training portals

Our team has delivered structured train-the-trainer (TtT) programs for agencies adopting ALiS. These sessions equip selected State staff to:
- Configure workflows, forms, and business rules
- Train new internal staff after go-live
- Manage user roles, permissions, and onboarding
- Troubleshoot common system questions
- Create and maintain internal training materials

4.3.1.8 – Familiarity with uptime guarantees, RTO/RPO metrics, and SLA reporting

ALiS supports enterprise-grade uptime and continuity standards including:
- 99.9% availability SLAs

- Near-real-time replication for critical components
- daily encrypted backups
- RTO < 4 hours
- RPO < 1 hour

Our operational dashboards provide SLA metrics, uptime reports, incident logs, and performance analytics that can be shared with the State weekly, monthly, or quarterly. These standards exceed typical state permitting system requirements.

4.3.1.9 – Experience working with multi-agency teams, gathering requirements, and managing change

ALiS was built for **multi-agency statewide permitting modernization**. Our team has led requirement-gathering and change-management efforts involving:

- Regulatory agencies
- IT and cybersecurity offices
- Facility inspectors
- Licensing boards
- Finance/treasury units
- Public user groups
- Interdepartmental stakeholders

Through structured JAD workshops, user story mapping, cross-agency governance committees, and Agile sprint cycles, we ensure needs across diverse programs are understood, harmonized, and implemented successfully.

4.3.2 – Mandatory Qualification/Experience Requirements

4.3.2.1 – Vendor's employees must have security training, and the Vendor must provide records of such training upon request

AGRC maintains a comprehensive Security Awareness and Compliance Training Program that is mandatory for all employees, subcontractors, and project resources supporting the ALiS platform. The training curriculum aligns with industry-accepted frameworks such as NIST 800-53, NIST 800-171, FedRAMP Moderate/High, and State cybersecurity standards. Courses include modules on secure development practices, data-handling protocols, phishing prevention, encryption standards, incident reporting, and role-based access responsibilities.

All personnel assigned to the West Virginia project will be required to complete annual security certification, with additional quarterly refresher modules covering emerging threats and State-specific requirements. All training records including completion logs, certificates, curricula, and employee attestations are centrally maintained and can be provided to state upon request. For personnel with elevated privileges (e.g., system administrators or DevOps engineers), enhanced training covering secure configuration, vulnerability management, and cloud-security operations is also mandatory.

This disciplined training approach ensures that every ALiS project team member understands their responsibility in safeguarding State data and aligns with the same practices

4.3.2.2 – Vendor must highlight training in WCAG 2.1 and Section 508 compliance for public-facing digital services

All ALiS implementation personnel including UX designers, business analysts, configuration specialists, and testers receive formal accessibility training focused on WCAG 2.1 AA and Section 508 compliance. This training covers accessible form design, keyboard navigation, contrast requirements, error handling, assistive-technology compatibility (screen readers, magnifiers), and alternative text usage. The ALiS design framework itself follows these standards out of the box.

The ALiS low-code form designer includes built-in guidance and automated checks that encourage accessible field layouts, labels, and instructions. This ensures every public-facing portal page from permit applications to dashboards to notifications is developed in alignment with federal accessibility requirements. Before any configuration is released, ALiS applies automated accessibility followed by human review using assistive

technologies.

4.3.2.3 – Vendor must show experience aligning solutions with state IT policies, privacy laws, and accessibility mandates

The ALiS platform is specifically engineered for **state-level regulation, licensing, and inspection programs**, enabling seamless alignment with State IT governance frameworks, privacy regulations, and accessibility mandates. AGRC has successfully adapted ALiS to the unique compliance requirements of multiple states, including data-classification policies, statewide identity-management standards, public-records statutes, retention policies, and open-data requirements.

ALiS supports configurable **data-retention schedules, role-based access control (RBAC)**, audit logging, and full encryption in accordance with privacy and security statutes. The platform integrates with State Single Sign-On solutions and adheres to State standards for cybersecurity, records management, and digital accessibility.

4.3.2.4 – Vendor must demonstrate experience with vulnerability scanning and reporting, disaster-recovery planning and drills, encryption standards (e.g., AES-256), and RBAC

AGRC maintains an enterprise-level **Security Operations Program** that supports the ALiS platform through continuous vulnerability scanning, penetration testing, and detailed reporting aligned to **NIST, FedRAMP**, and State standards. Automated scans are conducted weekly using industry tools such as **Nessus** and **Qualys**, with findings categorized by severity and tracked through a structured remediation workflow. Reports including vulnerability summaries, CVSS scoring, and remediation evidence can be shared with client as part of ongoing oversight.

ALiS also includes a fully documented **Disaster Recovery (DR) and Business Continuity (BCP)** program that outlines roles, recovery steps, backup schedules, and communication procedures. DR exercises are conducted quarterly, with results logged and available to the State upon request. If needed, our **formal DR policy** is provided to clients under NDA.

Encryption is enforced across the platform using **AES-256 encryption at rest, TLS 1.2+**

encryption in transit, and **FIPS 140-3 validated cryptographic modules**. Sensitive fields, including PII and payment tokens, are encrypted at the column level in addition to full-disk encryption. Access is governed by ALiS's granular **Role-Based Access Control (RBAC)** system, which ensures least-privilege access across agencies, reviewers, inspectors, financial officers, and system administrators.