

State of West Virginia

Board of Medicine

RECEIVED

2025 DEC 11 AM 11:32

WM PURCHASING
DIVISION

Original is in the State of West Virginia Contents

Medical Licensure / Records Database Maintenance System

Request for Proposal

CRFP 0945 BOM2600000001


GL Solutions

555 Corporate Drive, Suite 301
Kalispell, Montana 55901
541-312-3662
glsolutions.com

Date of Submission:
December 17, 2025



Title Page

Proc Folder: 1739608			Reason for Modification: Addendum 05
Doc Description: Medical Licensure / Records Database Maintenance System			
Proc Type: Central Master Agreement			
Date Issued	Solicitation Closes	Solicitation No	Version
2025-11-24	2025-12-17 13:30	CRFP 0945 BOM2600000001	6
VENDOR			
Vendor Customer Code		000000186731	
Vendor Name:		GL Suite, Inc. dba GL Solutions	
Address:			
Street:		555 Corporate Drive, Suite 301	
City:		Kalispell	
State: Montana		Country: United States	Zip: 59901
Principal Contact:		William Moseley	
Vendor Contact Phone:		541-312-3662	Ext.
FOR INFORMATION CONTACT THE BUYER			
Larry D McDonnell 304-558-2063 larry.d.mcdonnell@wv.gov			
<div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div> Vendor Signature X  <small>William Moseley (Doc 3, 2025 11:06:46 MST)</small> </div> <div> FEIN# 43-1797439 </div> <div> DATE: 12/03/2025 </div> </div>			

Secondary Point of Contact:

Steve Matzker, Technical Writer

- 541-312-3662
- matzker@glsolutions.com

Amendment Acknowledgement

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: CRFP BOM26*01

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)

<input checked="" type="checkbox"/>	Addendum No. 1	<input type="checkbox"/>	Addendum No. 6
<input checked="" type="checkbox"/>	Addendum No. 2	<input type="checkbox"/>	Addendum No. 7
<input checked="" type="checkbox"/>	Addendum No. 3	<input type="checkbox"/>	Addendum No. 8
<input checked="" type="checkbox"/>	Addendum No. 4	<input type="checkbox"/>	Addendum No. 9
<input checked="" type="checkbox"/>	Addendum No. 5	<input type="checkbox"/>	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 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.

GL Suite, Inc. dba GL Solutions
Company


William Hosley (04/2/2025 11:06:45 MST)

Authorized Signature

12/03/2025 Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

Table of Contents

Contents

Title Page	2
Amendment Acknowledgement.....	3
Table of Contents	4
Project Goals and Proposed Approach.....	6
<i>Executive Summary</i>	6
<i>Goals and Objectives Alignment</i>	8
Licensing and Credentialing	8
Case Management.....	11
Financial Management.....	14
Interfaces	15
User Portal and Website Integration	17
Document Management.....	18
Reporting and Communications	20
Communications	22
Configurability	25
Customization and Branding	27
Approach and Methodology to Goals/Objectives	27
Project Implementation Plan	27
Agency Transformation (AT) Framework.....	29
Implementation	31
Requirements Traceability Matrix (RTM) Overview	34
Design	36
Development	37
Data Conversion	37
Quality Assurance and Performance Testing.....	40
Training.....	43
Go-Live.....	45
Maintenance and Support	46
Approach and Methodology to Compliance with Mandatory Project Requirements.....	51
Security	54

Security, Auditing, and Notifications	56
Database and Technical Requirements	58
Hosting and IT	60
Qualifications and Experience	61
General Vendor Qualifications	61
Similar Projects	62
Staffing Plan and Schedule	62
Relevant Project Experience	83
Exceeding Mandatory Qualification/Experience Requirements	85
Value-Added Services	85

The rest of this page intentionally left blank

Project Goals and Proposed Approach

Executive Summary

GL Solutions is pleased to submit our proposal to modernize WVBOM's licensing and case management systems. We understand that WVBOM is seeking a secure, web-based solution that replaces aging infrastructure, streamlines business processes, improves access for licensees and the public, and ensures compliance with HIPAA, WCAG 2.1 AA, and other applicable security and accessibility standards.

For over 25 years, GL Solutions has delivered configurable, cloud-hosted software solutions to state regulatory boards across the country, including West Virginia's Alcohol Beverage Control Administration. Our SaaS solution, GL Suite, supports professional licensing, enforcement, inspections, complaints, document and financial management, audits, 3rd-party integrations and reporting—through a unified, configurable, and secure platform. GL Suite currently supports 35 agencies in 23 states, including medical boards with requirements and complexity comparable to WVBOM.

Understanding Your Goals

WVBOM's current systems lack essential functionality, including digital applications, self-service portals, comprehensive reporting, and secure, centralized data management. Our proposed solution directly addresses these gaps through a modern, SaaS-based platform that enables WVBOM to:

- Transition all applications and renewals to a mobile-friendly, online portal for both applicants and licensees.
- Streamline staff workflows for licensing, enforcement, and case management using configurable business rules that automate reviews, assignments, and communications.
- Implement robust Role-Based Access Controls (RBAC) to ensure secure access to sensitive information based on user roles and operational need.
- Support seamless integration with external systems, including IMLCC, FSMB, VeriDoc, and the Interstate Medical Licensure Compact.
- Generate custom reports, real-time dashboards, and legally sufficient application archives—without vendor intervention or code changes.

Key Differentiators

- **No-Code Configurability:** GL Suite enables authorized staff to manage business rules, workflows, forms, reports, and documents without custom coding or vendor assistance.
- **Business Rule Engine:** GL Suite supports the configuration of logic-based rules that automate approvals, enforce licensing policy, trigger alerts, and ensure compliance across all modules.
- **Comprehensive Portal Ecosystem:** Credential holders can complete all transactions online, while staff and board members benefit from role-specific dashboards and task queues.
- **Security and Compliance:** GL Solutions is on track to achieve StateRAMP authorization by the end of Q4 2025, demonstrating our commitment to meeting one of the most stringent sets of cloud security controls for public-sector vendors. GL Suite is hosted in the Microsoft Azure Cloud (FedRAMP authorized) and meets HIPAA, WCAG 2.1 AA, and PII handling requirements. Role-based access, encryption, audit trails, and secure communications are standard.



Our Approach

We bring a collaborative and transparent implementation process designed to deliver a fully operational system on time and within budget. Our team works side-by-side with agency stakeholders to configure the system to WVBOM's specifications, perform full legacy data conversion, conduct thorough testing, and deliver tailored training and go-live support. Our hybrid-phased implementation approach ensures minimal disruption while preparing staff for long-term system ownership.

Long-Term Support

Post-implementation, GL Solutions provides responsive U.S.-based support, continuous enhancement releases, and full lifecycle maintenance. Our goal is not just to implement software—but to partner with WVBOM in building a sustainable, efficient, and future-ready regulatory system.

We appreciate the opportunity to support WVBOM's mission and look forward to the opportunity to deliver a transformative solution that improves operations and public service delivery across the Board.

Sincerely,

A handwritten signature in black ink, appearing to read "Bill Moseley".

Bill Moseley
President and CEO

The rest of this page intentionally left blank

Goals and Objectives Alignment

Licensing and Credentialing

GL Suite provides WVBOM with a configurable, automated platform for managing the full licensing lifecycle—including initial applications, renewals, reclassifications, and new credential types. The system supports all current license and credential types and gives WVBOM the flexibility to introduce new ones without custom development or vendor involvement.

Support for All License Types – Current and Future

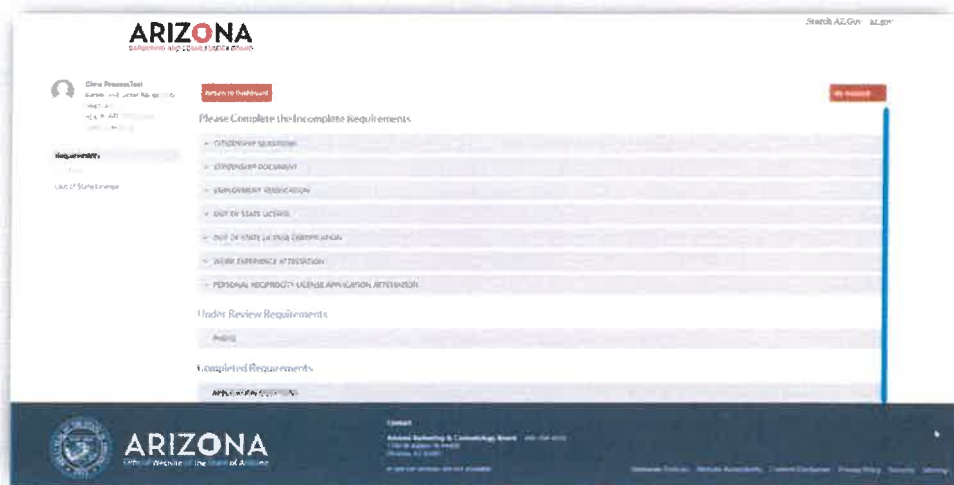
- GL Suite supports all WVBOM member and credential types—including licenses, registrations, permits, and authorizations—and is fully configurable to accommodate new types or subtypes as the Board’s authority expands.
- Staff can define unique workflows, requirements, and communication templates for each license type using intuitive administrative tools.

Integrated Online Application and Renewal System

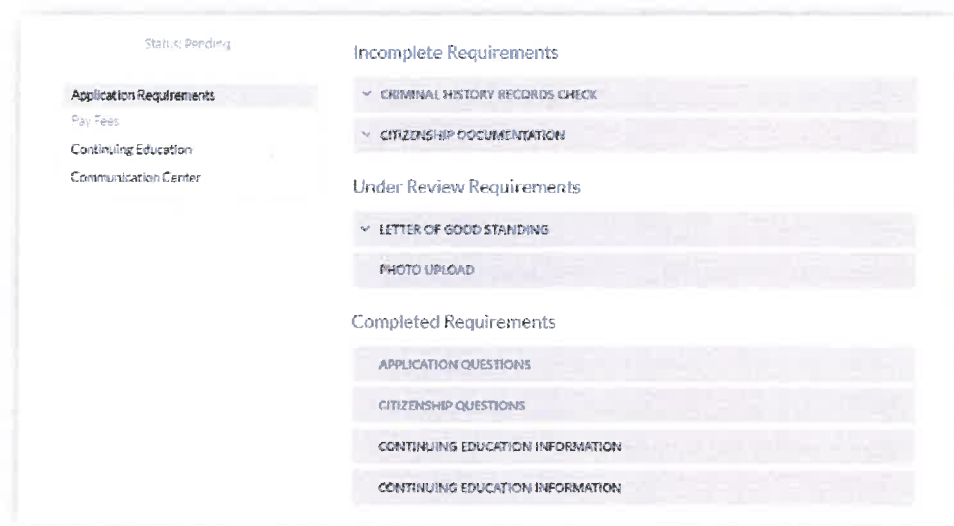
- **Self-Service Portal:** Applicants and credential holders can initiate applications and renewals through a mobile-friendly, secure web portal, available 24/7 through WVBOM’s website.
- **Dynamic Application Workflows:** Application forms and requirements automatically adjust based on member type, reciprocity, or background, presenting only relevant tasks and documents.
- **Real-Time Status Tracking:** Credential holders can view the real-time status of their application or renewal (e.g., incomplete, submitted, under review, approved).
- **Automated Communication:** System-generated emails and portal notifications alert members to outstanding requirements, approvals, or deficiencies.

Renewals, Reclassifications, and Credential Issuance

- **Automated Renewals:** GL Suite auto-generates renewal notices based on configurable timelines and automatically links new renewal records to the member’s history.
- **Auto-Reclassification and Issuance:** Once all renewal requirements are fulfilled, the system updates the license status (e.g., to “Active”) and issues certificates or wallet cards automatically.
- **Delivery Options:** Final credentials can be printed, emailed, or downloaded through the portal, based on WVBOM’s preferences.



Once logged into the self-service portal, Applicants can intuitively navigate to the application requirements menu. can create business rules that mandate all requirements are met before submission.



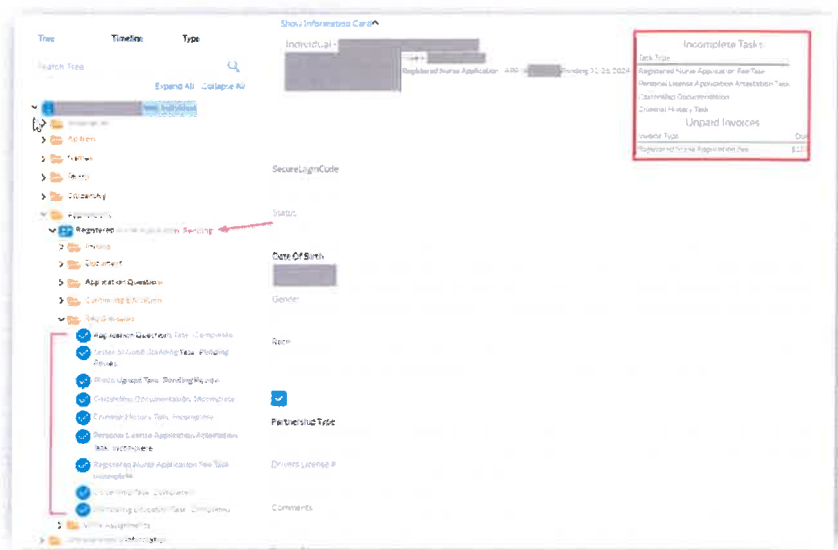
Application requirements shown for a partially completed application on the web.

Document and Requirement Management

- **Custom Checklists:** Application checklists are tailored to license type and agency rules (e.g., background checks, CE hours, verifications).
- **Incremental Document Upload:** Members can upload documents over time, with the system validating and updating task statuses automatically.
- **Master Task Configuration:** WVBOM staff can consolidate requirements into “master tasks” to streamline tracking and simplify the applicant experience.

Back-Office Workflow and Oversight

- **Workflow Automation:** License processing follows configurable rules that prevent credential issuance until all requirements are verified and approved.
- **Duplicate Prevention:** GL Suite applies configurable matching logic to ensure new applications are linked to existing records when appropriate.
- **Renewal Notifications:** The system sends personalized email or SMS reminders based on WVBOM-defined business rules to promote timely renewals and reduce lapses.



Application shown from the backend, displaying the application and each requirement, along with requirement statuses.

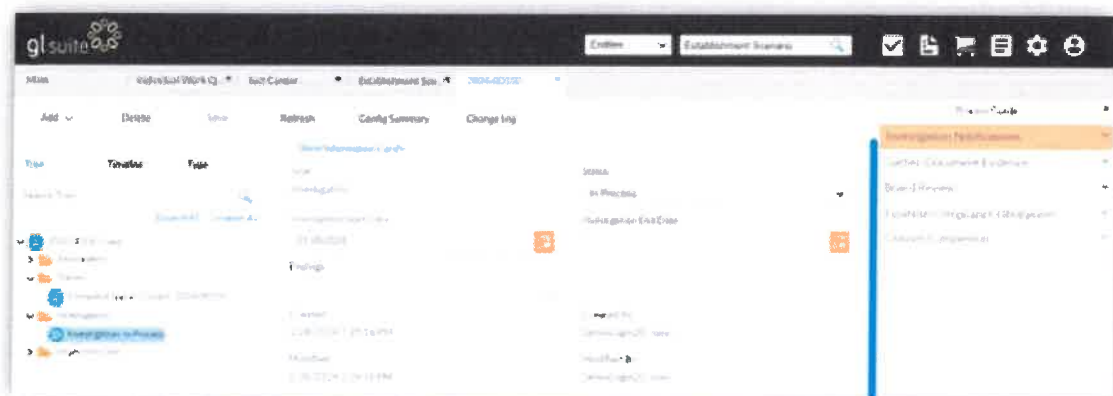
Legally Sufficient Application Archives

- GL Suite generates archival PDFs of completed applications that mirror exactly what the member saw and submitted, including timestamps and digital signatures.
- These archives are saved in the member’s profile, accessible to both staff and the applicant through their respective portals, ensuring regulatory defensibility.

Case Management

GL Suite provides WVBOM with a configurable, secure, and fully integrated platform for managing the entire lifecycle of complaints, investigations, enforcement actions, and disciplinary proceedings. The system ensures traceability, compliance, and transparency while reducing administrative burden and improving public trust.

WVBOM will have the ability to provide the public with an online complaint portal. On the backend, all complaints will be routed to the appropriate staff for review with capabilities to assign the case to additional staff with a single click.



Backend layout of GL Suite, where staff will navigate all workflow related tasks; from case and application intake to running reports and communicating with licensees.

Complaint Intake and Case Tracking

- **Online Complaint Submission:** Members of the public or WVBOM staff can submit complaints via a configurable online intake form. Intake can be automatic or routed for preliminary staff review prior to formal acceptance.
- **Centralized Case Records:** All materials—including complaint forms, notes, correspondence, evidence, and system-generated tasks—are stored in a single case file with full audit trail.
- **RBAC-Driven Access:** Access to case content is restricted based on roles. Staff, attorneys, or external reviewers can be given time-bound, permissioned access as needed.
- **Scalability:** The system supports 500 new complaints per year, or more, with no performance degradation.

Investigations and Case Management

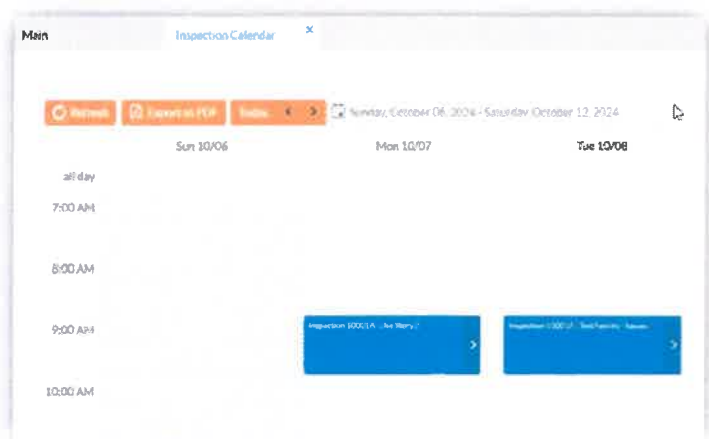
- **Business Rule Automation:** Configurable logic governs case intake, escalation, and closure. GL Suite automatically enforces key steps such as document receipt, status reviews, and stakeholder notification.
- **Assignment & Routing:** Cases can be auto assigned to investigators based on criteria such as type, location, workload, or credential holder role.
- **Task Management:** Required tasks are created based on rules and must be completed before advancing the case. Tasks include deadlines, assignees, and status tracking.
- **Integrated Communications:** Staff can generate templated Microsoft Word letters, store correspondence, and log contact activity—all within the case file.

Litigation and Legal Proceedings

- **Case Escalation:** Complaints can trigger formal case creation through status transitions, with support for many-to-one complaint-to-case associations.
- **Legal Tools:** Assign and manage attorney access, set visibility (internal/public), and manage legal processes including depositions, discovery, hearing scheduling, and evidence management (e.g., Bates stamping).
- **Billing and Cost Tracking:** Record and report time, legal costs, and administrative expenses related to disciplinary actions and legal proceedings.

Enforcement and Compliance Monitoring

- **Enforcement Actions:** Track hearings, corrective actions, and disciplinary decisions. Compliance status and case



Authorized staff will have the ability to schedule and track inspections from GL Suites built-in calendar

outcomes are linked to the member's profile.

- **Automation:** GL Suite sends notifications, generates letters, and updates statuses based on rules—ensuring no step is missed.
- **Ongoing Monitoring:** Post-violation compliance is tracked through auto-generated tasks, audit-ready documentation, and linked historical records.

Evidence and File Management

- **Multimedia Support:** Staff can attach and review documents, audio files, and video files within each case. All files are viewable in-platform without delay or external download.
- **Indefinite Retention:** Historical complaint and disciplinary records are retained indefinitely or according to WVBOM's document retention policy.
- **Audit Trails:** Every action—such as edits, submissions, status changes, and file uploads—is recorded in a transactional audit log, ensuring data integrity and accountability.

Board Meeting Management

GL Suite provides a comprehensive and configurable solution for managing Board of Medicine meetings and related regulatory activities through its Board Meeting Management functionality. Designed specifically for state licensing and enforcement boards, this functionality allows WVBOM to plan, organize, and document board meetings efficiently and in full compliance with record retention and public transparency requirements.

Using GL Suite, WVBOM can plan meetings months in advance, define and manage agenda items, assign presenters or respondents, and dynamically update the agenda as needed. The integrated Board Meeting Manager screen auto-generates the agenda based on selected items, allowing staff to make real-time edits that are immediately reflected in the displayed version.

Board members can access the meeting agenda through secure, role-based portals prior to the meeting to review supporting materials, including applications, disciplinary cases, and enforcement records. If enabled, all associated documents can be downloaded for offline review. During the meeting, authorized users can update agenda item statuses, take notes, record motions and votes, and maintain a live record of proceedings.

Once completed, GL Suite automatically generates Board Meeting Minutes, pulling directly from the agenda and notes captured during the session. This automation saves time, ensures accuracy, and supports compliance with West Virginia's Open Meetings Act and information retention policies. All meeting records are securely retained within GL Suite, supporting internal audits, historical review, and Freedom of Information Act (FOIA) requests.

Key Feature Summary

- Schedule and track Board Meetings, including date, time, and location details.
- Define and manage agenda items, including case reviews, license applications, and disciplinary actions.
- Link enforcement cases, complaints, or licensing records directly to meeting agenda items for contextual review.

- Utilize the Board Meeting Manager to dynamically display agenda items, supporting documents, and notes.
- Automatically generate and post PDF agendas for public viewing (if applicable).
- Allow secure online or offline access to meeting materials for board members.
- Record and update agenda statuses during meetings with real-time visibility.
- Automatically generate meeting minutes and post approved minutes online for public access.
- Support follow-up tracking of post-meeting actions and assignments.
- Maintain complete historical records to support retention policies and FOIA requests.

Financial Management

GL Suite provides a secure, configurable financial management framework fully integrated with WVBOM's licensing and credentialing operations. The system supports real-time payment processing, automated reconciliation, and detailed financial oversight—all in a PCI-DSS-compliant environment designed to meet public-sector standards.

Integration with WV State Treasurer's "E-Gov" System

GL Suite is designed to integrate with the WV State Treasurer's "E-Gov" platform for seamless online payment collection. Our platform's API-ready architecture ensures WVBOM can process credit card and ACH payments through the State's designated gateway with real-time synchronization.

- Payment confirmations are reflected immediately in both systems.
- Licensees receive automated receipts and confirmations via email and portal access.
- WVBOM staff can access complete payment histories directly from the member's profile.

Online Payment Processing and Self-Service

- **Shopping Cart Functionality:** Applicants and credential holders can combine multiple fees (e.g., application, exam, renewal) into a single transaction.
- **Flexible Payment Options:** Supports full, partial, split, and batch payments.
- **Self-Service Portal:** Licensees can view pending fees, submit payments, and receive receipts without staff intervention.

The screenshot displays a 'Checkout' page with a progress bar at the top indicating 'Checkout' as the current step. Below the progress bar, there are sections for 'Customer Information' and 'Payment Information'. The 'Customer Information' section includes fields for First Name, Last Name, Country, Address 1, Address 2, City, State, ZIP/Postal Code, and Phone Number. The 'Payment Information' section includes fields for Payment Method, Payment Type, and Payment Amount. On the right side of the page, there is a 'Log Payments' section with a table showing payment details and a 'Total' of \$100.00. The page also features a 'Checkout' button and a 'Cancel' button.

WVBOM staff can enter payment information for numerous licenses, events, exams, etc. from one screen

Automated Financial Workflows via Business Rules

GL Suite leverages WVBOM-configured business rules to automate financial policy enforcement:

- **Late Fees and Collections:** Automatically applied based on due dates and triggers.
- **Refund Processing:** Refunds and credits are issued based on rule-defined scenarios.
- **Dynamic Fee Calculations:** Fee totals adjust in real time based on applicant status, license type, or submission timing.

Daily Reporting and Record Reconciliation

- **Scheduled Reconciliation Reports:** Automatically generated on a daily, weekly, or monthly basis to support WVBOM's reconciliation with State finance teams.
- **Real-Time Reporting:** Enables staff to pull current revenue reports filtered by credential type, date, or fee category.
- **Manual and Automated Oversight:** Staff can review, override, or audit transactions as needed for compliance and accuracy.

Comprehensive Fee Tracking

GL Suite tracks all financial activity at the member level, including:

- Initial and renewal fees
- Refunds and billing corrections
- Adjustments and credits
- Installment or partial payment plans

All financial records are linked to member accounts and available via export for accounting systems or external audits.

Interfaces

GL Suite is built to support secure, standards-based integration with WVBOM's third-party systems, ensuring seamless interoperability, reliable data exchange, and long-term flexibility. Our no-code interface engine enables WVBOM staff or GL Solutions to configure and maintain interfaces without custom development, reducing costs and turnaround time.

Supported Standards and Protocols

GL Suite supports modern, secure data exchange formats and methods, including:

- **Protocols:** REST, SOAP, SFTP
- **Data Formats:** JSON, XML, flat files (CSV, TXT)
- **Security:** FIPS 140-3 compliant encryption; HTTPS, TLS, VPN tunnels

These protocols allow GL Suite to push, pull, or exchange data bidirectionally with a variety of regulatory, credentialing, financial, and document systems.

Proven Integration Examples

GL Suite has successfully integrated with systems used by state medical and licensing boards, including:

- **FSMB** – Federation of State Medical Boards (Uniform Application, FCVS)
- **VeriDoc** – Credential verification and license transfer
- **Interstate Medical Licensure Compact (IMLCC)**
- **NABP / Bamboo Health** – License data reporting and pharmacy monitoring
- **State Payment Gateways** – e.g., WV State Treasurer’s “E-Gov”
- **Document Management Systems** – FileDirector, Laserfiche

Configurable Interface Engine

Interfaces are configured using reusable, no-code logic components. Key features:

- **Scheduled or Event-Driven Jobs:** Interfaces can run on a set schedule or be triggered by events (e.g., license issued).
- **Data Mapping:** Field-level data mapping is fully configurable to accommodate third-party requirements.
- **Transport Control:** File transfer methods and API endpoints are managed through interface configuration tools, not source code.

Secure and Auditable Connectivity

- **Encryption in Transit and at Rest:** All interface data is secured end-to-end.
- **Audit Logging:** All interface activities are logged, including file transfers, payload content, status, timestamps, and user/system triggers.
- **Alerts and Exception Handling:** Failures are logged in an exception table and generate real-time alerts to designated WVBOM staff via email or SMS.

Collaborative Interface Implementation

GL Solutions partners with WVBOM and third-party vendors to:

- Define use cases and data flows
- Establish secure connection parameters
- Validate test transactions
- Finalize integration before production use

Each interface is tracked and documented in the project plan, tested before go-live, and included in change management procedures post-launch.

Developer Access and API Enablement

To support advanced integration needs, GL Suite can publish secure APIs to authorized third parties. These services allow:

- External systems to submit, retrieve, or update records
- Triggering of WVBOM-defined workflows
- Integration with portal-based data exchange (e.g., FSMB to member record)

Role-Based Interface Access

Interfaces are protected using RBAC, ensuring that only authorized staff or systems can initiate or receive transactions. WVBOM can control access at the user, role, or system level

User Portal and Website Integration

GL Suite provides a fully integrated, secure, and configurable Self-Service Portal tailored to meet the specific needs of WVBOM, its licensees, business entities, continuing education providers, and the public. This portal is accessible through WVBOM's website and is fully mobile responsive and WCAG 2.1 Level AA compliant, ensuring usability across devices and by all users.

Integrated Public and Staff-Facing Portal

GL Suite's Self-Service Portal is built directly into the licensing database, ensuring real-time data synchronization and eliminating the need for duplicate data entry or third-party syncing. The system allows WVBOM staff and credential holders to interact through the same unified platform, streamlining operations and enhancing transparency.

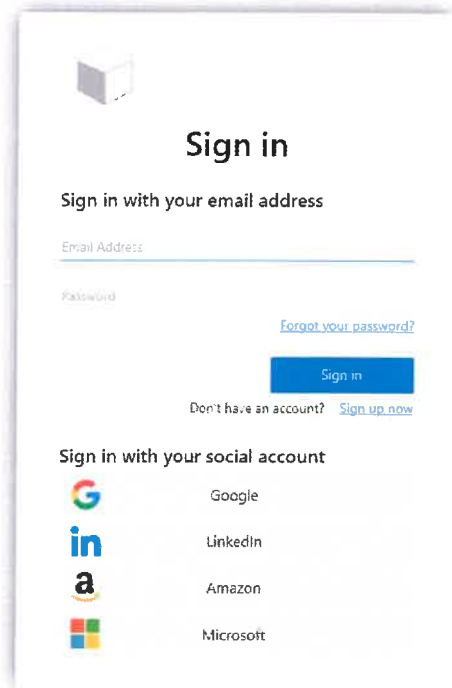
Licensee, Business and Provider Portals

GL Suite offers secure, role-based Self-Service Portals tailored to the needs of individual licensees, business entities, and continuing education (CE) providers. These portals are accessible 24/7 and empower external users to manage their regulatory interactions independently and efficiently.

Licensee Portal

WVBOM licensees, including MDs, PAs, DPMs, and permit holders—access a personalized dashboard where they can:

- Submit new license, permit, and exam applications, selecting from customized pathways (e.g., examination, reciprocity, endorsement).
- Complete renewals and upload supporting documentation (e.g., CE verification, malpractice records).
- Track application and renewal status in real-time.
- Receive system-generated reminders and status updates via email, SMS, or portal notifications.
- Securely communicate with WVBOM staff through a built-in messaging system.
- Download or print licenses, permits, wallet cards, and official communications.
- Update personal information and manage their accounts, including MFA setup and password resets.



Business Portal

For Medical Corporations and PLLCs, GL Suite offers a dedicated portal that enables:

- Submission and renewal of business licenses or registrations.
- Oversight of affiliated licensees, including expiration tracking.

- Upload of corporate documents (e.g., articles of incorporation).
- Direct communication with WVBOM staff and access to compliance documents or inspection results, if applicable.

Public License Verification

Members of the public can perform real-time verification of license and permit statuses—including disciplinary history, license types, and work addresses—through a searchable, mobile-friendly interface embedded into WVBOM’s website. This information is pulled directly from the live GL Suite database to ensure accuracy.

Security and Accessibility

- Multi-Factor Authentication (MFA) and Single Sign-On (SSO) via the State’s Digital Citizen Portal ensure secure, seamless access.
- Role-Based Access Control (RBAC) ensures each user type—licensee, business representative, CE provider, or WVBOM staff—only sees information relevant to their role.
- All user data is protected with end-to-end encryption and hosted in a CJIS- and HIPAA-compliant cloud infrastructure.
- The system meets or exceeds WCAG 2.1 Level AA for accessibility and is fully responsive across modern mobile and desktop browsers.



Both licensees and WVBOM staff can access the functionalities of GL Suite across devices.

Document Management

GL Suite provides a secure, integrated, and cloud-based document management solution specifically aligned with the needs of WVBOM. The system ensures that all application materials, supporting documentation, disciplinary files, and historical records are efficiently managed, easily accessible, and protected in accordance with HIPAA and other applicable data security standards.

Secure, Centralized Document Storage

GL Suite replaces WVBOM’s legacy document handling processes with a fully digital repository capable of storing all file types, including:

- PDFs, DOC/DOCX, XLSX, JPG/PNG
- Audio and video files (e.g., MP4, MOV)
- Historical and legacy files from prior systems

Documents are automatically linked to the relevant records—whether licensee, case, or credential type—ensuring that WVBOM staff can locate and act on information with minimal effort.

Automatic Updates and Status Tracking

Documents uploaded by licensees or staff are:

- Automatically date/time-stamped
- Logged with uploader identity
- Associated with corresponding requirements or checklist items
- Marked as “Complete” for fulfillment of document-driven conditions

This automation accelerates WVBOM’s processing timelines, reduces manual effort, and ensures accountability.

Granular Access and Viewing Controls

The system allows WVBOM administrators to define access permissions by user role or individual user, ensuring compliance with need-to-know and least privilege principles. Features include:

- Role-Based Access Control (RBAC)
- Document-specific security settings
- No download or print permissions (if restricted)
- View-only access for sensitive records

Board members and third parties can securely view documents within their accounts through protected web portals. Staff can assign, revoke, or adjust access in real time.

Secure Document Exchange

WVBOM staff and Board members can share documents with third parties—such as external investigators, legal counsel, or credentialing partners—through secure, access-controlled portals. Staff can restrict access by document, folder, or user and manage expiration dates and audit logs for all shared content.

Public Document Flags

GL Suite allows WVBOM to flag select documents (e.g., final orders, public disciplinary actions) for online publication. These documents are searchable and accessible via the public license lookup on WVBOM’s website, promoting transparency and reducing staff burden for records requests.

Compliance, Security, and Redundancy

GL Suite's infrastructure is designed to meet rigorous data protection and confidentiality standards:

- End-to-end encryption at rest and in transit
- Full compliance with HIPAA and WCAG 2.1 Level AA
- ISO 17799-aligned information security practices
- Redundant cloud infrastructure and automated daily backups

Key Benefits for WVBOM

- **Efficiency:** Tasks that once took weeks—like gathering supporting documentation—can now be completed in hours.
- **Scalability:** Unlimited document storage capacity supports WVBOM's projected growth to over 40,000 records.
- **Security:** Audit trails, access logs, and encryption ensure full traceability and data protection.
- **Staff Control:** WVBOM administrators manage document structure, security, and retention policies without needing vendor intervention.

GL Suite's document management capabilities will help WVBOM eliminate paper-based workflows, preserve institutional knowledge, and confidently manage records through the full lifecycle of licensure, discipline, and compliance.

Reporting and Communications

GL Suite provides WVBOM with an integrated and intuitive reporting and communications framework that empowers both technical and non-technical staff to access, analyze, and act on live data. The system fulfills WVBOM's stated need for dynamic reporting without requiring SQL expertise and supports advanced data exploration through dashboard visualizations, public transparency, and audit-ready communication archiving.

Ad Hoc and Operational Reporting

GL Suite's embedded reporting engine, GLS Report, enables WVBOM staff to generate real-time, customized reports directly from the system without IT involvement.

- **No-Code Report Building:** Staff select filters such as license type, complaint status, or renewal due date to create on-demand reports with a few clicks.
- **Reusable Templates:** Frequently used reports (e.g., expiring licenses, pending applications, CE compliance) can be saved, cloned, and adapted by staff across departments.
- **Real-Time Data:** Reports are generated from live records to ensure accuracy for audits, public information requests, and board meetings.
- **Multiple Output Options:** Staff can view reports in-browser, export to Excel, print to PDF, or push data to dashboards or the public portal.

Advanced Business Intelligence and Dashboards

For supervisory and executive-level users, GL Suite integrates with Microsoft Power BI to deliver advanced business intelligence and visual reporting tools.

- **Custom Dashboards:** Dashboards can be configured for licensing trends, renewal rates, open disciplinary cases, and backlogs across all credential types.
- **KPI Monitoring:** WVBOM may define and track Key Performance Indicators by board function (e.g., licensing, enforcement, support), enabling data-driven policy and staffing decisions.
- **Drill-Down Navigation:** Staff can interact with dashboards to move from high-level metrics into specific licensee records or complaint files for detailed review.

Query Management and Scheduling

For advanced users and data analysts within WVBOM, GL Suite supports robust query-building and scheduling capabilities.

- **Custom SQL Queries:** Subject matter experts can create and save custom queries to extract precise datasets, such as licensees with overdue disciplinary compliance or applications missing documentation.
- **Parameterized Filtering:** Input prompts allow staff to run reports by date range, license type, CE provider, or status.
- **Scheduled Reports:** Frequently used queries (e.g., daily revenue summaries, monthly licensee exports) can be automated and emailed to defined recipients on a set schedule.

Mass and Targeted Communications

GL Suite supports both mass and individual messaging via email, SMS, and portal notifications—all logged within the system to create a permanent audit trail.

- **Mass Messaging:** Staff can send batch messages to specific cohorts (e.g., all PAs due for renewal, MDs missing CE, or PLLCs with expiring registrations).
- **Automated Notifications:** Built-in workflows trigger messages based on status changes or due dates (e.g., application receipt, renewal reminders).
- **Secure Messaging:** Licensees can initiate or respond to messages securely through the portal; WVBOM staff manage threads within the licensee's record.

Email Archiving and Legal Sufficiency

All outbound and inbound communications, whether system-generated or staff-created—are:

- Archived within the licensee's or case record.
- Timestamped and attributed to the sender/recipient.
- Stored in compliance with HIPAA, PII, and WVBOM record retention policies.
- Retrievable for audits, legal proceedings, and public records requests.

Public-Facing Reports

To support transparency and reduce staff burden, GL Suite allows WVBOM to securely publish selected data sets directly to the public portal, including:

- Current licensee rosters by credential type.
- Approved continuing education course lists (if applicable).
- Summaries of enforcement activity or complaint statistics.

Access to public reports is managed through role-based controls, ensuring only pre-approved data is displayed.

Communications

GL Suite provides WVBOM with robust communication capabilities, ensuring efficient interaction with applicants, licensees, and internal staff throughout the lifecycle of licensing, enforcement, and case management activities.

Communication Center (Internal System Use)

GL Suite's Communication Center centralizes all incoming and outgoing communications and document uploads associated with an individual record—whether for an applicant, licensee, or respondent. This built-in module enhances efficiency by capturing every touchpoint in a single, easily accessible view.

Key Features:

- **Complete Recordkeeping:** Automatically logs all email and SMS communications sent or received through the system, providing a traceable, legally sufficient history.
- **Integrated Document Tracking:** All uploaded or system-generated documents are stored and linked to their associated records with metadata, improving auditability and retrieval.
- **Direct Response and Navigation:** Staff can reply to messages or navigate directly to associated records, documents, or fees using the built-in “Go To” feature.
- **Customizable View Filters:** Users can filter communication history by license type, status (e.g., active vs. expired), or communication category.
- **Batch Correspondence:** Send letters, notices, or bulk emails to groups of licensees or applicants with merged fields for personalization.
- **Built-in Payment and Certificate Tools:**
 - Licensees can pay fees via a secure shopping cart within the portal.
 - Certificates and verifications (including QR codes) can be printed or downloaded by staff or licensees.

Public-Facing Communications via the Portal

GL Suite's configurable Self-Service Portal enables WVBOM to maintain high-quality digital engagement with licensees, providers, and the public:

- Dynamic dashboards tailored by role (e.g., licensee, medical corporation, academic faculty)
- In-portal messaging and notification history
- Integrated help text and editable FAQs to assist users in common processes like submitting applications, uploading CE documentation, or renewing credentials

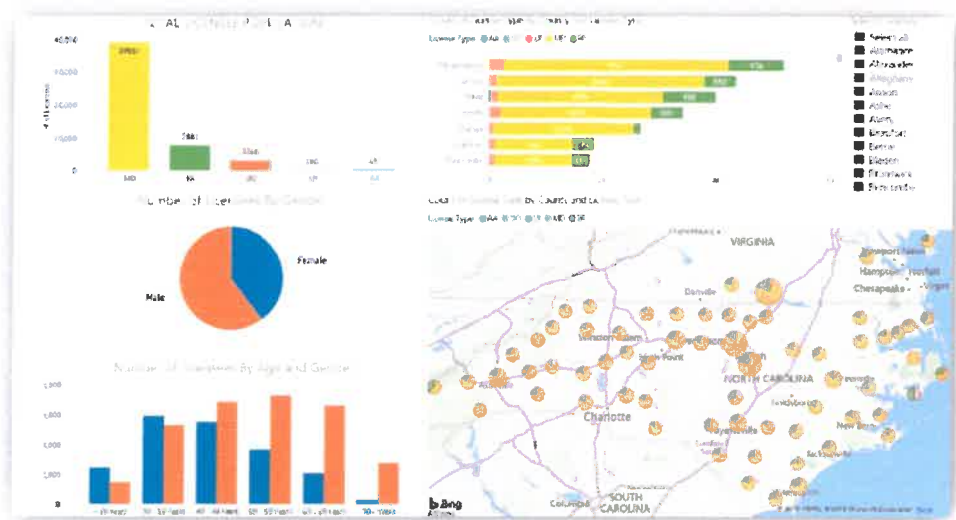
Project Collaboration via the GL Portal

Separate from the operational system used by WVBOM staff, the GL Portal serves as a centralized project management and support platform during implementation and beyond. It facilitates task tracking, defect management, and communication between WVBOM and GL Solutions personnel.

Key Features of the GL Portal:

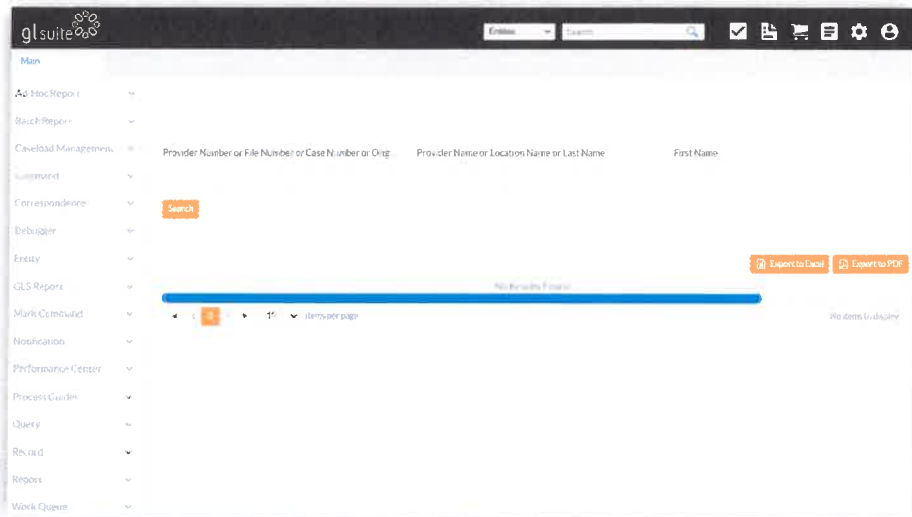
- **Structured Task Tracking:** View the status of configuration tasks, enhancements, defects, and change requests.
- **Issue Reporting and Resolution Monitoring:** Submit issues directly, monitor resolution progress, and validate completion.
- **Power BI Dashboards:** Real-time performance metrics, including outstanding tasks, project progress, and upcoming milestones.
- **Integrated Calendar:** Tracks meetings, deadlines, and deliverables.
- **Direct Messaging:** Communicate with your GL Solutions Project Manager (during implementation) and Agency Partner (post-Go-Live) in real time.

Example of Power BIs visually reporting capabilities, in this case licensing metrics for a current North Carolina client.

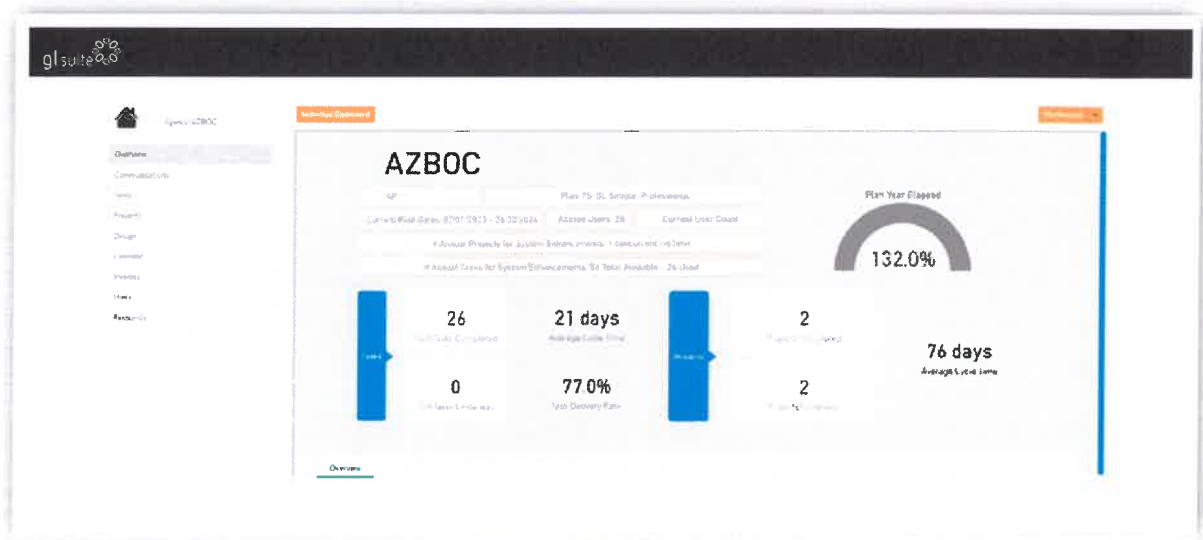


Example of KPI reporting capabilities designed for a client, in this case used in conjunction with reporting capabilities configured specifically for a report entitled: Initial Application Elapsed Time

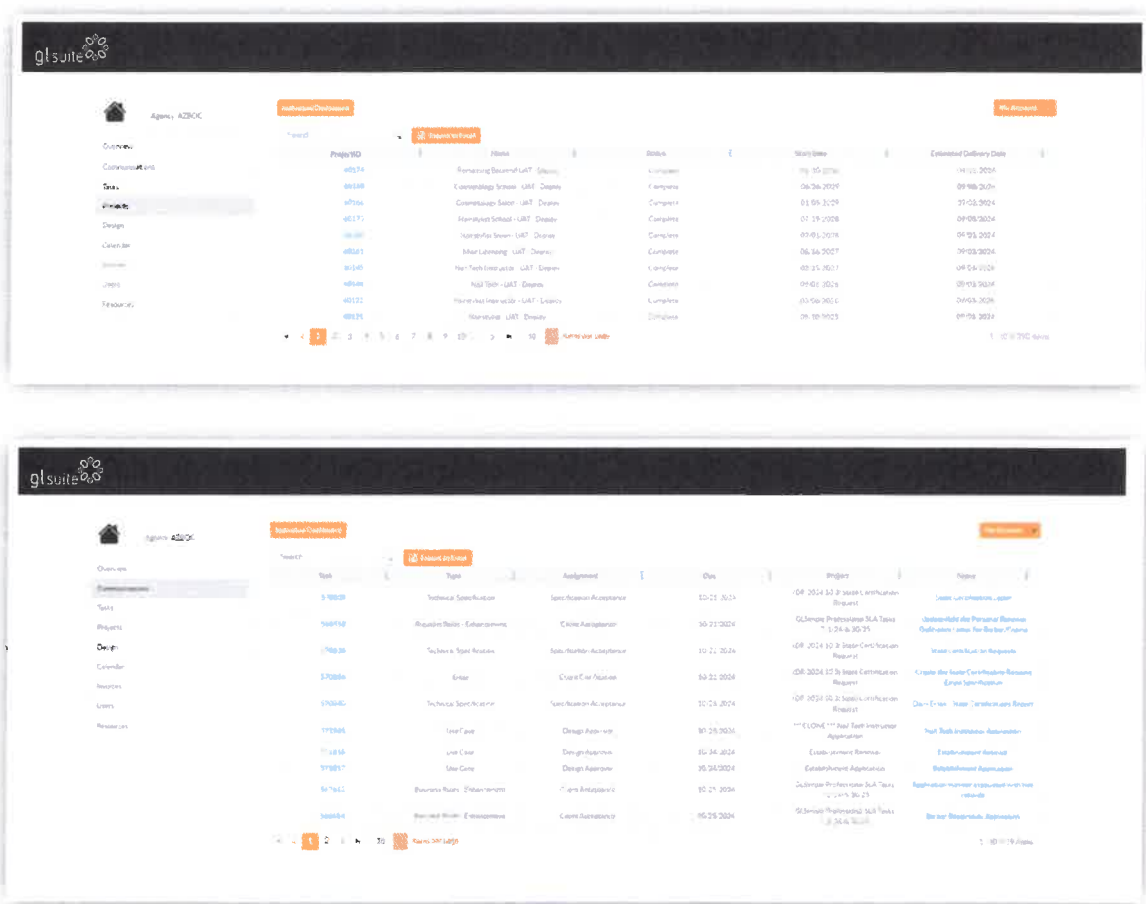




A typical user Dashboard with standard query features, configurable to the needs of WVBOM.



Example of a GL Portal dashboard for a current client. The configurable nature of the dashboard will allow WVBOM to display relevant metrics, e.g., during implementation



GL Portals offers a Project Workflow dashboard where WVBOM and GLS staff can monitor the progress of projects, status and delivery date. Users can drill down into project details as well.

Configurability

GL Suite is designed to empower agencies like WVBOM with a configurable, no-code platform that adapts to evolving business processes, regulatory requirements, and operational preferences—without the need for vendor intervention or custom code development. Through built-in administrative tools and a highly flexible Business Rules Engine (BRE), agency staff can easily modify workflows, forms, data validation, and user permissions in-house.

No-Code Configuration Tools

GL Suite's no-code environment allows WVBOM administrators to make system changes directly through an intuitive interface. These tools enable agency staff to configure:

- **Workflows:** Define and modify the steps required for license applications, renewals, investigations, inspections, and more.

- **Forms and Fields:** Add, remove, or update data fields, form layouts, and associated business logic.
- **Communications:** Customize templates for letters, emails, and portal messages using Microsoft Word-based merge fields and logic-based triggers.
- **Notifications and Alerts:** Create automated system alerts, email messages, or dashboard reminders triggered by specific events or data changes.
- **Dashboards and Views:** Configure role-based dashboards and data views to tailor system experiences to staff responsibilities.

Configurable Web and Self-Service Portals

GL Suite provides a Configurable Web platform that enables WVBOM to manage its public-facing website and integrated backend processes through a single, streamlined solution. Unlike traditional web portals that require custom overlays and separate development efforts, GL Suite allows the agency to configure and maintain web functionality directly within the administrative system—promoting consistency, accuracy, and faster deployment.

Key functionalities include:

- **Configurable Web Architecture** – Allows agency staff to create, deploy, and maintain online services (e.g., applications, renewals, verifications) through administrative configuration rather than custom code. This approach reduces defects and accelerates release cycles by up to 60%.
- **Bi-Directional Communication** – Facilitates seamless interaction between agency personnel and the public via structured workflows, ensuring real-time data exchange and process visibility.
- **Self-Service Access** – Licensees, applicants, and public users can securely log in to perform key tasks, including applying for licensure, renewing licenses, uploading documents, managing profiles, and checking the status of their records—all without agency intervention.
- **24/7 Availability** – Portals provide continuous access to critical services such as application status tracking, fee payment, and licensure verification.

GL Suite’s portal framework enforces strict data security via role-based access and Azure B2C authentication. The system supports multiple sign-in options, including integration with major identity providers such as Google, Facebook, and LinkedIn, and complies with standard authentication protocols like OAuth 2.0 and OpenID Connect.

Public-Facing Features Include:

- Secure dashboards tailored by user role.
- Integrated payment functionality
- Automated password resets, expiration notices, and security prompts
- Public licensee look-up and online verification services

Conversational UI

To further enhance user engagement and streamline communication, GL Suite incorporates a Conversational UI—a built-in, real-time messaging feature embedded within the stakeholder portal. This tool serves as a centralized, user-friendly interface where licensees and agency staff can communicate directly within the system.

Key features include:

- **Interactive Messaging** – Enables two-way conversation between users and staff, replacing fragmented communication via email or postal mail.
- **Guided Deficiency Resolution** – Staff can immediately notify users of missing or incorrect items in their submissions and provide step-by-step instructions for remediation.
- **Centralized Communication Hub** – All messaging is stored within the platform and associated with the relevant licensee or application, ensuring continuity and ease of access.
- **User-Centric Design** – An intuitive layout promotes a seamless experience for stakeholders and improves agency efficiency.
- **Automated Retention** – Messages are saved and accessible for future reference to support transparency and continuity.

Together, the Configurable Web and Conversational UI enable WVBOM to offer an intuitive, secure, and modern digital experience for licensees and applicants, while minimizing administrative burden and optimizing internal workflows.

Customization and Branding

GL Solutions can design WVBOM's websites and public-facing portals to meet all State and Board branding requirements, including adherence to official color palettes, typography, and logo usage guidelines. Our design process incorporates WVBOM brand identity across all interfaces—public websites, licensee portals, and internal dashboards—ensuring a consistent and professional appearance.

To reinforce a seamless user experience, GL Solutions applies the same branding to system-generated documents, email templates, and portal notifications, so that every communication—from online applications to automated renewal reminders—presents a consistent, trusted look and feel.

Approach and Methodology to Goals/Objectives

Project Implementation Plan

GL Solutions employs a proven, structured, collaborative and supportive project management approach tailored to meet the unique needs of WVBOM's modernization initiative. Grounded in the Project Management Institute's PMBOK framework and refined through more than two decades of government implementations, our methodology integrates the clarity of a Waterfall structure with the adaptability of Agile sprints. This hybrid model ensures alignment with WVBOM's timeline, regulatory requirements, and change management needs while enabling continuous feedback, stakeholder engagement, and flexibility.

Hybrid Waterfall/Agile Framework

GL Solutions applies a hybrid methodology that leverages the strengths of both Waterfall and Agile frameworks. Waterfall ensures clear milestones, traceability, and compliance documentation—while Agile enables flexibility, iteration, and responsiveness. This approach allows us to execute structured project phases while incorporating early demonstrations and stakeholder input to reduce rework and improve system alignment.

Phased Execution with Agile Sprints

Each core implementation phase—Requirements Gathering, Design, Configuration, Testing, Deployment, and Post-Go-Live Support—is managed using Agile-informed cycles. Tasks are broken into sprints with short-term goals and regular touchpoints, allowing staff to engage, validate work, and request refinements while maintaining forward progress.

Milestone-Based Deliverables

Project progress is organized around clearly defined milestones tied to contractual deliverables and acceptance criteria. Each milestone includes formal deliverable reviews and quality assurance checkpoints. Agile sprint reviews and demonstrations provide early visibility into how workflows, forms, and portals are taking shape.

Collaborative Governance and Communication

GL Solutions will establish a joint governance structure – JAD and JAR - with that includes agency leadership, subject matter experts, and project stakeholders. We will hold regular status meetings, sprint reviews, steering committee updates, and retrospectives to promote transparency and stay aligned with evolving goals.

Project Management Tools and Transparency

We use industry-standard tools like Microsoft Project and GL Portal, our secure client workspace, to manage schedules, user stories, test cases, risks, issues, and documents. These tools offer real-time visibility into progress, assignments, and issue tracking for all project stakeholders.

Risk and Change Management

Our Risk Management Plan outlines how project risks—such as staffing gaps, policy shifts, or third-party delays—are identified, tracked, and mitigated. A formal Change Management Plan ensures that any adjustments to scope, requirements, or schedule are reviewed and approved through structured procedures that protect WVBOM’s timeline and budget.

Training, Readiness, and Knowledge Transfer

GL Solutions emphasizes staff readiness throughout the project lifecycle. Our comprehensive training plan includes role-based training, user guides, help content, and hands-on workshops. We ensure that staff are confident using, administering, and supporting GL Suite before go-live.

This hybrid methodology, backed by our Agency Transformation framework and aligned with PMBOK principles—equips WVBOM with the tools, structure, and flexibility needed to implement a secure, modern system on time and within budget.

Standard Project Management Deliverables

GL Solutions delivers a comprehensive set of project management artifacts throughout the engagement. These deliverables promote accountability, visibility, and alignment, and are maintained in GL Portal for continuous access and review:

- **Project Management Plan (PMP):** Defines the execution, monitoring, and control strategy, including scope, roles, deliverables, and timeline.
- **Goals and Scope Document:** Outlines high-level objectives, agency priorities, and the regulatory and business outcomes the system must achieve.
- **Communication Management Plan:** Establishes meeting cadence, stakeholder engagement strategies, and reporting protocols.
- **Risk Management Plan:** Identifies, evaluates, and tracks risks, along with mitigation strategies and escalation procedures.
- **Service Level Agreement (SLA):** Documents support tiers, performance expectations, and resolution targets for system maintenance and operations.
- **Disaster Recovery and Incident Response Plans (DRP/IRP):** Provide business continuity and incident handling strategies to ensure uptime and data protection.
- **Project Schedule:** A living project schedule with task dependencies, milestones, and resource assignments, regularly updated and shared with WVBOM.
- **Change Management Plan:** Governs how changes to scope, requirements, or timing are proposed, evaluated, and documented to preserve project integrity.

Each document is version-controlled, collaboratively reviewed, and aligned with WVBOM's implementation goals, ensuring consistency, clarity, and control across the entire project.

Agency Transformation (AT) Framework

At GL Solutions, we recognize that the successful implementation of a new system requires a comprehensive approach that combines effective project management with a deep understanding of organizational needs during times of transformation. Our framework, *Agency Transformation (AT)*, is designed to facilitate a smooth transition from legacy systems to GL Suite while aligning with the best practices outlined in the Project Management Body of Knowledge (PMBOK) methodology.



Refined from twenty-five years of implementation experience, GL Solution's *AT* is structured around five distinct phases that provide a roadmap for implementing 's new system while minimizing disruption, fostering a culture of change, staying on schedule and on budget. Each phase is meticulously crafted to address WBOM's specific objectives, ensuring that the transformation aligns with 's modernization goals. *AT* acknowledges the inherent challenges of organizational and regulatory change, enabling staff to gradually acclimate to the new processes through comprehensive training and support.

Incorporating PMBOK principles into our *AT* framework enhances our methodology's effectiveness. The PMBOK provides a robust set of guidelines for project management, emphasizing stakeholder engagement, risk assessment and a structured project lifecycle. By leveraging these principles, we ensure

that each phase of the AT process is executed with precision, focusing on clear objectives, effective communication, timeline adherence and proactive risk management.

Agency Transformation consists of five distinct phases, designed to implement 's new system on schedule and within budget. We understand that organizational change can be challenging for many, which is why our phased methodology is particularly effective in minimizing disruption. This approach allows staff to gradually transition into the new system, learning and adapting at a comfortable pace, supported by our comprehensive training and educational materials. While the specific details may be subject to change, GL Solutions is committed to guiding WVBOM through each phase outlined below:

Phase 1: Capacity Building

- Establishes the budget, scope and managerial capacity necessary to initiate agency transformation.
- Through GL Suite's scalable, configurable platform, WVBOM can streamline budget planning, monitor expenditures and allocate resources to support modernization efforts. This phase also involves preparing staff with appropriate tools and training to manage the transition effectively.

Phase 2: Process Standardization

- Develops and executes well-defined work processes/use cases and policy frameworks.
- GL Suite helps standardize licensing and enforcement workflows, minimizing redundancies and improving operational consistency. This includes improving licensing application business processes while adding incident management functionalities, while ensuring that staff can efficiently manage caseloads through updated training processes.
- Configurable workflows and a zero-code business rules engine will reduce manual intervention, minimize errors and accelerate regulatory tasks.
- External WVBOM stakeholders will benefit from mobile access and automated notifications for license renewals and updates, providing real-time access to critical information.

Phase 3: Customer Service

- Enables self-service capabilities, i.e., portals and dashboards, for external stakeholders, reducing the administrative burden on agency staff.
- GL Suite provides self-service portals for licensees, enabling them to submit applications, renew licenses and track statuses online. GL Suite will also allow the public to issues complaints via a dedicated portal that routes directly to staff. This phase empowers users to manage their own processes, reducing manual intervention and speeding up service delivery.

Phase 4: Integrated Service

- Facilitates communication, workflow and document integration among agency staff and external entities.
- With GL Suite's integrated document and workflow management, WVBOM will have a unified system for real-time data sharing, allowing staff to collaborate seamlessly and access critical information quickly.
- Integration with external systems via APIs ensures that data bi-directionally flows smoothly across departments and partners, such as law enforcement or other regulatory bodies.

Phase 5: Model Agency

- Builds a culture of continuous improvement, supported by data-driven tools that enhance operational efficiency and supports decision-making.
- GL Suite's KPI tracking and reporting tools will help monitor performance and identify areas for improvement.
- With continuous performance tracking and data-driven insights via Power BI dashboards and ad-hoc reporting tools, WVBOM can measure its success and continuously refine its operations. GL Solutions will also provide ongoing support through regular updates, ensuring WVBOM remains ahead of regulatory technology.

Implementation

Within the five phases of Agency Transformation, GL Solutions adheres to the project lifecycle of a well-structured Project Management Plan. The following is a high-level outline of the Project Milestones that WVBOM can anticipate participating during implementation:

Project Milestones	Overview
Project Initiation	<ul style="list-style-type: none"> • Initiation Meeting • Project Analysis • Goals and Scope documents • Management Plan • Use case development • RTM Initial creation
Design	<ul style="list-style-type: none"> • Business Process Design <ul style="list-style-type: none"> ○ Solutions Analysis ○ RTM ○ Design ○ Design Review ○ Design Approval • Security • Report, Correspondence, and Subform Designs • External Interfaces and Customized Functionality Design (if included) • Public Website Design
Development and Testing	<ul style="list-style-type: none"> • Configure Rules and Web Sites • Develop Custom Functionality • Unit Testing • System Testing • Interface Development
Data Conversion/Migration	<ul style="list-style-type: none"> • Conversion Design • Conversion Development

	<ul style="list-style-type: none"> • Conversion Testing
User Acceptance Testing (UAT)	<ul style="list-style-type: none"> • Confirms/tests user requirements • Identifies final adjustments • Ensures readiness for launch
Training & Go-Live	<ul style="list-style-type: none"> • Final Conversion • Migrate to Production • Training

Project Initiation

Project initiation is intended to identify how the software will be implemented. This phase ensures all parties agree on the methodology and all other areas of implementation. Project initiation is the first milestone in the project lifecycle.

Initiation Meeting

The Initiation Meeting includes an introduction of the project team, the project overview, the roles and responsibilities, the goals for the project, and any next steps. GL Solutions will dedicate a Project Manager to the life of the implementation. Additionally, GL Solutions will assign business analysis, development, configuration, and testing team resources as needed. WVBOM will dedicate a primary contact for the project that will be expected to make decisions for the project. WVBOM will also assign appropriate SMEs for business requirements gathering, design approval, specification acceptance and UAT. UAT is the responsibility of SMEs. Any change in dedicated resources will be communicated between GL Solutions and WVBOM in writing.

Project Analysis

Project Analysis includes pre-implementation project activities such as the business process definition interview and creating a project scope of work that will be incorporated into the Goals and Scope document. Products of this process include:

- Breakdown of work in project steps
- Develop use case
- Basis for the Goals and Scope document

Management Plan

The Management Plan defines how GL Solutions and WVBOM will collaborate throughout the lifecycle of the implementation. It provides the foundation for the working relationship, clearly documenting roles, responsibilities, expectations, methods, and deliverables. The Management Plan serves as the central framework guiding the configuration, deployment, and support of GL Suite and includes the following components:

1. Goals and Scope

This component establishes the mutually agreed-upon business objectives and boundaries for the project. GL Solutions will:

- Identify and document high-level business processes to be configured.
- Break down processes into discrete functions aligned with GL Suite's configuration methodology.
- Adjust or consolidate processes as needed—with approval from WVBOM.

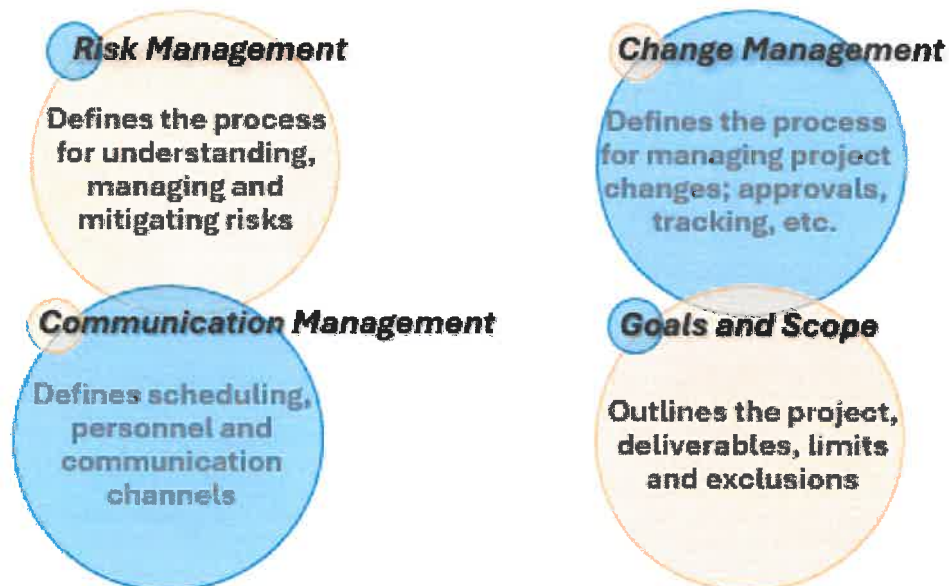
The **Goals and Scope Document** is essential for scope control and change tracking. It forms the foundation for subsequent deliverables such as Use Cases, configuration specifications, and testing criteria.

Use Cases

Use Cases will be developed to represent detailed scenarios of user interactions with the system. These include:

- Step-by-step sequences for each business process
- Exception and alternate flows
- Clear actor definitions (user, system, external party)
- Traceability to functional requirements and system behavior

Use Cases will be used to drive design decisions, test planning, and user training.



2. Risk Management

Risk Management is a core part of the Management Plan. GL Solutions maintains a Risk and Issues Log that is reviewed jointly with agency leadership during regular project meetings. This includes:

- Risk identification and classification
- Mitigation and contingency planning
- Assigned ownership for monitoring and response

- Escalation paths

3. Change Management

To ensure transparency and accountability for any modifications to scope, schedule, or deliverables, GL Solutions follows a structured Change Management Process, including:

- Initiation and documentation through a Change Order Request Form (CORF)
- Internal feasibility review and impact assessment
- Client review and formal approval
- Schedule and scope updates post-approval

No changes are billed or implemented without formal agreement, and all changes are tracked against original project baselines.

4. Communication Management

Clear and consistent communication is critical to project success. The Management Plan defines:

- Communication protocols and escalation paths
- Meeting cadences (e.g., weekly project meetings, steering committee check-ins)
- Communication channels (e.g., GL Portal, email, project documentation)
- Roles and responsibilities for stakeholder engagement

GL Portal serves as the centralized hub for communication, issue tracking, and document exchange between GL Solutions and WVBOM.

5. Schedule and Work Areas

The plan also includes a project schedule using Microsoft Project, developed in collaboration with WVBOM and broken down by functional work areas. This includes:

- Major milestones
- Key deliverables and deadlines
- Interdependencies
- Go-live planning and cutover timing

Schedule updates are managed through change control and reflected in project status reports and Steering Committee meetings.

Requirements Traceability Matrix (RTM) Overview

GL Solutions' RTM process ensures complete alignment between project requirements and deliverables throughout the system implementation lifecycle. The RTM serves as a structured framework that connects documented business and technical requirements to their corresponding specifications, configurations, testing protocols, and final deployments. This process supports accountability, facilitates quality assurance, and ensures that every contractual obligation is fulfilled.

Requirements are first established during project initiation through the development of the Goals and Scope document, which serves as a definitive statement of work. This document refines and formalizes the agency's objectives and lists all business processes to be configured. It also establishes the baseline against which all requirements will be traced and validated.

Each requirement is tracked across the following stages:

- Specification and documentation
- Client review and approval
- Configuration within GL Suite
- Validation through multiple levels of testing (Preliminary, Integration, and System Testing)
- Client acceptance of configured features
- Deployment through test and production environments

The RTM is continuously updated and cross-referenced during these phases to confirm that all functionalities have been developed and tested to meet client needs.

GL Solutions also integrates its Gap Analysis and Product Solution processes into the traceability framework. These mechanisms capture and resolve requirements that are not addressed by standard GL Suite functionality or that present technical uncertainties. Once a solution is identified, the associated work is broken into tasks, assigned to teams, and integrated into the RTM to maintain end-to-end traceability.

In cases of evolving project needs, GL Solutions applies a structured change management process to assess and document any updates to scope. Approved changes are reflected in updated requirements and incorporated into the RTM to maintain traceability and ensure alignment with project goals. By systematically linking requirements to their corresponding deliverables and incorporating client input throughout the project, GL Solutions' RTM process delivers transparency, ensures scope compliance, and supports successful system implementations.

Standard Usability Requirements – Provided by GL Solutions

GL Solutions has included the following standard usability requirements as part of this project. These design requirements are based on our experience in designing GL Suite to ensure that it will be as easy to use as possible. The wording of these requirements is standard and is not open for input. However, agencies can and should enter defects against these requirements if they find the design has not adequately met them.

1 Reference ID	2 Description of the Design Requirement	3 Description for How the Design Meets the Requirement	4 QA: Confirm Requirement Is met? (Y/N - Initials)		5 QA Comments
			Design	Dev	
BP1	Business process meets the standard requirements for all business processes	This Requirement is met by adhering to all of the standard requirements for the Business Process			
BP2	If the client has a pre-application process - record information/line submitted by applicant in support of a request for an application packet	This Requirement does not apply as Client does not use a Pre-Application process.			
BP3	All application requirements are tracked within the system.	This Requirement is met by ensuring the use of Work Assignments that allow a requirement to be tracked and assigned to both Staff and Supplier seamlessly			
BP4	User can add an XXXX application to the Individual/Business record and it appends with all requirements tasks and the Invoice.	This Requirement is met by ensuring that an individual with access to the Configurable Website/Access is granted through creating an account, is able to request a new Application, have it append, and simultaneously append all Requirements, Invoices, and History/Documents			
BP5	User can enter information about an applicant and an application using a one screen	This Requirement is met by utilizing a MultiSOF for the Requirements Page. A MultiSOF allows for all Information, Documents, and Forms to be Completed/Submitted from a single screen.			
BP6	User can create system outputs (for example, the license certificate, approval letter, and incomplete application letter) related to an applicant or groups of applicants according to client business requirements.	This Requirement is met by utilizing Scheduled Jobs to send out Communications and Notifications to the Applicant. The Applicant is also able to produce a License Certificate via the Print Certificates Page			
BP7	User can log payment for the application	This Requirement is met by utilizing a Pay Invoices Page where the Applicant is able to see all unpaid invoices that exist as a child of the application and allow them to submit Credit Card payment via a 3rd party Payment Processing Interface.			

BP8	Upon approval of the application, the system creates an initial license with the correct expiration date.	This Requirement is met by ensuring that on update of the Application to Approved, to then append the License to the record. The License is granted and appended with all dates. DataRuleID 363354 On Append of Initial License, Set Dates & Status. ObjectID 1720 Aesthetic License			
BP9	Validation rules exist, preventing Business until all application requirements have been met.	This Requirement is met by ensuring the use of Validation rules on both the License and all of the Child Tasks of the Application. These Validation rules will prevent the update of the Application Status if all of the Child Requirements of the Application DO NOT have a Status of Completed or Waived.			
BP10	PAI license requirements/tasks to be completed by the applicant include a deficient status with automation to notify the applicant that the requirement is deficient.	This Requirement is met by ensuring the use of Deficient/Not Accepted statuses for tasks and their corresponding documents or forms. When set to Not Accepted/Deficient, the System will send out a Deficiency notice to the Applicant via a Scheduled Job.			
BP11	Application and license statuses are set by business rules and only upper level staff have access to manually change the status.	This Requirement is met by ensuring that the Application Status is only updated via Business Rules and only Administrative Level Staff have the ability to update Application Status			
BP12	Strict Certificate/Card number assignment and tracking ensures no gaps in license numbers.	This Requirement is met by utilizing a Business Rule that produces an application number on append of the Application. The Application Numbers do not use a shared table and therefore are Application/License specific. This Business Rule prevents any gaps in Application/License Number by incrementing by 1 each time			
BP13	Confirm that all essential commands required to automate the application process have been created where the need is implied by GL Suite software, not a client business requirement, e.g. missing market as printed commands.	This Requirement is met by adhering to the Functionality Catalogs best practice section for the Object. In question, in this case, all Commands and Command rules have been specified and implemented.			
BP14	The client-defined Application Number format and numbering sequence has been identified and included in the design if client utilizes an application number.	This Requirement is met by utilizing the already in place Application Number format used in all other Application Processes. This is a 9 digit number preceded by the prefix "APP-".			

An example of a standard RTM WVBOM can anticipate during implementation.

Design

The following is a high-level overview of GL Solution's Design phase.

The Design phase initiates after the agency approves each Use Case. During this phase, GL Solutions' Business Analysts configure GL Suite to meet agency-specific requirements by aligning with the Project Management Plan's "Goals and Scope Document", adhering to established use cases and following GL Solutions' SaaS architecture and best practices. This configuration avoids software customization, emphasizing instead the adaptability of the highly configurable GL Suite application.

Key components of the Design phase include:

- **Solutions Analysis:** Analysts assess the suitability of GL Suite's capabilities in meeting the agency's requirements. This step includes a fit-gap analysis to identify areas needing configuration or enhancement, the validation of high-level requirements, and recommendations for aligning the solution with business objectives.
- **Business Process Design:** Analysts create detailed process flows, configure screens and fields, and define security settings to ensure each process aligns with documented requirements.
- **Prototype Development:** An initial prototype covering 80% of the functionality is built, along with supporting documents such as process guides and technical specifications (Self-Documenting Specification).
 - **Prototype Videos:** Provides SMEs an additional opportunity to address any questions or concerns about the design documents and use case prototypes.
- **Design Review and Approval:** The agency reviews the prototype and associated documentation, providing written feedback to ensure alignment with project requirements. Final approval is granted once the design meets all specified standards.
- **Design Adaptation for Outputs and Interfaces:** Specifications for reports, interfaces, and public website elements are defined to meet both agency needs and technical requirements.

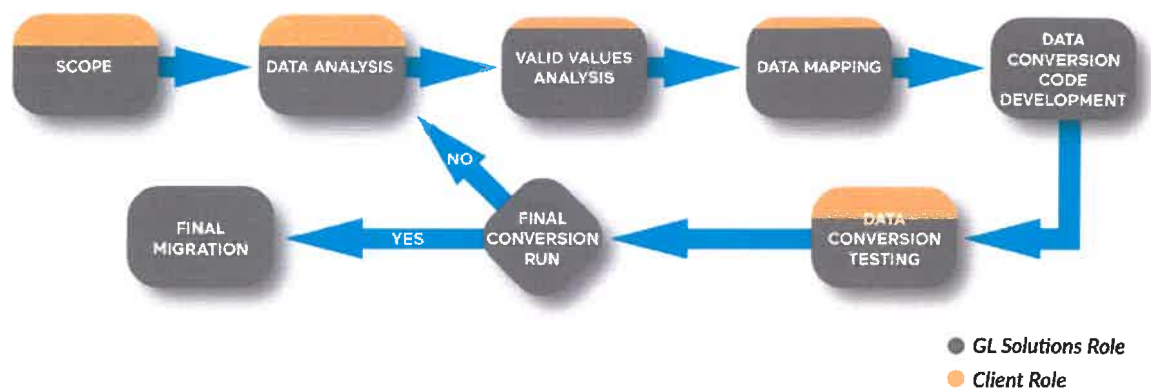
Throughout, GL Solutions applies SaaS best practices, enhancing design stability and scalability, with flexibility for defect correction, at no cost, and change requests that may or may not fall within the scope of work.

Development

After approval of the design, GL Solutions will complete the configuration and development of the system. This includes any business rules, commands, reports, correspondences, etc. described in the detailed functional specifications. This work is completed according to the accepted specification. Development and configuration are performed in the Development (DEV) environment.

Data Conversion

GL Solutions delivers a structured and iterative data conversion process to ensure legacy data is accurately and meaningfully transitioned into GL Suite. This process is executed in four tightly coordinated phases: Conversion Design, Conversion Development, Conversion Testing, and Client Validation (Screen Review). Each phase is built to ensure technical accuracy, compliance with business rules, and agency satisfaction.



The table below identifies GL Solutions and WVBOM personnel expectations and responsibilities during the data conversion and legacy migration phase.

Owner	Role & Named Individual (where applicable)	Responsibilities
GL Solutions	Project Manager	<ul style="list-style-type: none"> • Provide FTP site information for data transfer • Facilitate meetings as needed for technical resources • Conduct conversion testing with the agency (screen to screen review)
GL Solutions	Business Analyst	<ul style="list-style-type: none"> • Produce mockup of conversion records • Produce conversion technical specification (crosswalk) • Set up conversion testing records

GL Solutions	Development Team	<ul style="list-style-type: none"> Convert legacy data to GL Suite Produce conversion exception reports
GL Solutions	Quality Assurance Team	<ul style="list-style-type: none"> Test converted data according to the conversion crosswalk
Agency	Project Manager	<ul style="list-style-type: none"> Participate in screen-to-screen conversion testing Approve conversion exception reports Identify legacy records for conversion testing Approve all data identified to not convert
Agency	Subject Matter Experts	<ul style="list-style-type: none"> Participate in screen-to-screen conversion testing
Agency	IT	<ul style="list-style-type: none"> Produce legacy system data Answer technical data questions

Conversion Design

GL Solutions begins by specifying and developing the functionality needed to migrate data from the agency's legacy system into GL Suite. The primary artifact for this work is the Conversion Crosswalk—a detailed, Excel-based mapping document that identifies how each data field in the legacy system translates to its counterpart in GL Suite.

The **Conversion Crosswalk** includes:

- A listing of every legacy data field to be converted.
- The data type and source table location of each field.
- The destination field in GL Suite including its object and screen location.
- Any required transformation logic or conditional actions to be applied prior to loading the data.

To develop the crosswalk, GL Solutions meets with the agency to review their legacy system screens and business processes. The agency provides screen shares, screenshots, and representative datasets to facilitate accurate mapping. Business Analysts annotate screenshots using image editing tools to indicate the fields to be converted.

tblContact	ProviderIDText	varchar(4)				R
tblContact	ServiceIDText	varchar(2)				R
tblContact	ProgramIDText	varchar(3)				R
tblContact	Filename	varchar(15)			The first name - CED	Y
tblContact	MInitial	varchar(2)			The middle initial - CED	Y
tblContact	LName	varchar(20)			The last name - CED	Y
tblContact	TitleID	int(10)			The title of the contact - CED	Y
tblContact	Phone	varchar(15)			Phone number - CED	Y
tblContact	Cell	varchar(15)			Cell Phone number - CED	Y
tblContact	Fax	varchar(15)			Fax Phone Number	Y
tblContact	PhysicalAddress1	varchar(75)			Physical Address Street 1 - CED	Y
tblContact	PhysicalAddress2	varchar(75)			Physical Address Street 2 - CED	Y
tblContact	PhysicalCity	varchar(30)			Physical City - CED	Y
tblContact	PhysicalState	varchar(2)			Physical State - CED	Y
tblContact	PhysicalPostalCode	varchar(15)			Physical Postal code - CED	Y
tblContact	PhysicalPISCode	int(10)			Physical PIS code - CED	Y
tblContact	MailingAddress1	varchar(75)			Mailing Address Street 1 - CED	Y
tblContact	MailingAddress2	varchar(75)			Mailing Address Street 2 - CED	Y
tblContact	MailingCity	varchar(30)			Mailing City - CED	Y
tblContact	MailingState	varchar(2)			Mailing State - CED	Y
tblContact	MailingPostalCode	varchar(15)			Mailing Postal code - CED	Y
tblContact	email	varchar(100)			Email address - CED	Y
tblContact	CloseDate	datetime			The date the contact entry was closed - CED	Y
tblContact	DateCreated	datetime				Y
tblContact	LastModifiedStartID	int(10)				N
tblContact	LastModifiedDate	datetime				N
tblContact	CheckedOut	bit				N
tblContact	CheckedOutStartID	int(10)				N
tblContact	CheckedOutDate	datetime				N
tblContact	Deleted	bit				N
tblContact	DeletedByUserID	int(10)			This field is used as primary keys for linking to other tables in the database - CED	R
tblContact	DeletedByUserText	varchar(4)				R
tblContact	ServiceIDText	varchar(2)				R
tblContact	ProgramIDText	varchar(3)				R
tblContact	InvestigationID	int(10)				R

WVBOM will receive detailed Conversion Crosswalk documentation like the one above.

These annotated images serve as visual references for mapping each field and applying conversion rules.

The agency must provide the following artifacts early in the project to support successful design:

- An initial dataset exported from the legacy system (SQL, Oracle, or equivalent format).
- A database schema, if available.
- Screenshots of business process screens in the legacy system.
- Identification of any data or tables to be excluded from conversion.

Important: All data delivered for conversion—across all rounds—must retain a consistent structure and format. If the structure changes, those changes are not included in the original scope of work.

Conversion Development

Using the approved crosswalk, GL Solutions proceeds with the technical aspects of conversion. The Configuration Specialist (CS) team is responsible for building and executing the conversion routines.

Key steps in this phase include:

1. Importing the source data into a secure SQL-based conversion environment.
2. Reviewing the legacy data structure and identifying anomalies or inconsistencies.
3. Organizing the data into logical groupings to simplify mapping and development.
4. Writing and executing the conversion code using crosswalk specifications.
5. Importing attachments or associated child records, if applicable.
6. Generating a suite of validation reports, including:
 - Exception Reports to highlight anomalies or transformation issues.
 - Record Count Reports to validate totals between source and target.
 - Reconciliation Reports to ensure logical and numerical consistency.

GL Solutions does not use Visio; instead, the BA and CS teams rely on Microsoft tools (Excel, SQL Server, and image editors) to prepare, document, and execute the conversion.

This phase may include multiple rounds of conversion to accommodate ongoing changes in the legacy system (e.g., newly entered applications or renewals). Each round builds on the previous to ensure full and accurate data capture.

Conversion Testing

Following each round of data migration, GL Solutions performs internal testing to ensure:

- Records have been successfully migrated.
- Data appears in the correct locations within GL Suite.
- Any defined business rules or conversion logic have been properly applied.

Once internal testing is complete, GL Solutions conducts screen-to-screen comparison reviews with agency stakeholders. During these sessions, the CS team presents the legacy and GL Suite systems side-by-side, confirming field-level accuracy.

This iterative process typically includes two or more conversion rounds, each followed by screen review and data reconciliation. Reports generated in each round help verify completeness and identify any necessary corrections.

Agency participation during this phase is critical and includes:

- Reviewing exception reports and confirming how anomalies should be handled.
- Comparing legacy and GL Suite reports for consistency in records, licenses, payments, and other core data.
- Validating that the system reflects all required data accurately and that no meaningful information has been lost.
- Normalizing or cleaning up source data prior to each round (GL Solutions does not provide data cleanup services).

Client Validation / Screen Review

The final step in each conversion round is the Conversion Screen Review—a structured validation session with the agency to confirm the successful outcome of the data load. The CS team demonstrates how legacy records appear within GL Suite and discusses any identified gaps or errors.

Client validation culminates in either:

- **Approval to proceed** to the next round (if additional conversion is required), or
- **Final acceptance** of the converted dataset for Go-Live.

Following final validation, the CS team executes the final conversion based on the latest version of the source data and approved crosswalk. The system is then prepared for production deployment.

The agency is strongly encouraged to conduct additional validation during User Acceptance Testing (UAT) and immediately after Go-Live. This includes:

- Performing screen-to-screen reviews across various record types.
- Reviewing exception reports and signing off on final disposition.
- Comparing system reports to verify data accuracy and completeness.

Quality Assurance and Performance Testing

GL Solutions is committed to delivering high-quality software that meets detailed technical specifications to support WVBOM's operations. Quality is defined not only as functioning software but as software that performs exactly as specified in mutually understood and documented requirements. This ensures that expectations are clear, testable and aligned with WVBOM's needs.

- **Quality Assurance Approach:** GL Solutions' dedicated Quality Assurance (QA) team is involved from design through warranty stages. Each functionality is rigorously reviewed and tested to meet the use cases and specifications before release. Quality is achieved through detailed specifications, best practices, quality control checkpoints, software prototypes and clear documentation to minimize discrepancies. Change requests may be made if specifications evolve or are reinterpreted.
- **Testing Process:** User Acceptance Testing (UAT) criteria define acceptable quality levels for project completion, balancing effort and functionality. This allows for the system to Go-Live even

with minor variations from the original specifications, enabling smooth operation with the flexibility for incremental adjustments post-launch.

- **Performance Testing Services:** GL Solutions provides comprehensive performance testing to ensure that GL Suite functions efficiently under expected loads. Load testing simulates concurrent user access to verify responsiveness and system stability. Performance tests are scheduled one month before Go-Live, with test cases developed to reflect real-world conditions. Any issues found are analyzed for root causes and addressed to meet performance standards.

Testing and Testing Environments

GL Solutions follows a structured configuration and testing process involving **four** distinct environments: Dev (Development), Sys (System Testing), UAT (User Acceptance Testing) and Prod (Production).

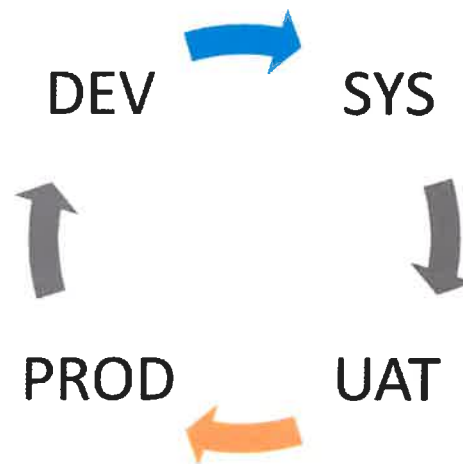
Development Testing

Configuration and development activities occur in the Development (DEV) environment.

During this phase, GL Solutions primarily handles the design and development of the system, including business rules, commands, reports and correspondence based on detailed functional specifications. Within the GL Suite application, configuration changes are tracked seamlessly via task numbers and approved by authorized WVBOM staff.

Unit Testing in System Environment

GL Solutions conducts Unit Testing to determine whether developed or configured functionality performs according to specification. GL Solutions testers use the accepted specifications to verify that the developed functionality meets the specified client requirements. Unit testing occurs as system functionality is designed and developed. Unit testing is performed by GL Solutions in the System (SYS) environment to ensure that system functionality is developed to meet the approved specifications. Integration testing is a form of unit testing to ensure that all inputs and outputs to the client and third-party systems are in place and function according to business process design specifications.



System Testing

GL Solutions conducts system testing to validate that developed functionality meets the expected outcomes documented by the accepted use cases and project specification(s). System testing occurs in the User Acceptance Testing (UAT) environment. Completion of system testing is one of the primary prerequisites for beginning User Acceptance Testing.

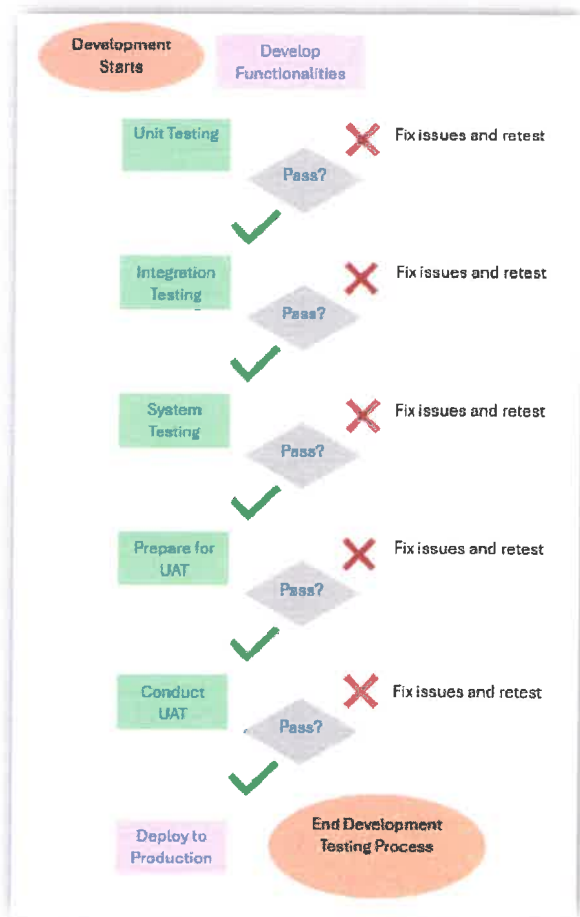
User Acceptance Testing (UAT) UAT is a narrowly defined testing process conducted primarily by identified SMEs as part of the final implementation steps and at the conclusion of all previously noted testing phases. Client testing business process functionality is very important to the success of the project to ensure the client can perform all aspects of the job. Successful agency testing a business process means that the agency can work through the business process using the approved process guide. Additionally, the Agency can help ensure a successful UAT by understanding and meeting these expectations:

- tests using converted (real) data, not test data, to ensure accuracy of the converted data and system functionality.
- tests the system by business process grouped by applicable Use Cases and with GLS provide test cases.

GL Solutions will provide SMEs UAT videos for each use case that needs testing. Prior to the scheduled UAT meeting, SMEs will receive UAT videos to review. This ensures an efficient UAT phase.

It is expected the processes will be tested, defects reported and resolved, and the business process user testing closed to meet the overall project schedule. Once all processes are tested in that manner and the P1 and P2 defects are resolved the project will exit UAT.

Upon successful completion of UAT, the system will be ready for the final rollout to the production environment, provided that required project activities are completed.



Roles and Responsibilities during UAT

Owner	Role	Responsibilities
GL Solutions	Project Manager	<ul style="list-style-type: none"> Resolve conflicts Identify project risks Organize the structured testing schedule
GL Solutions	Business Analyst	<ul style="list-style-type: none"> Create UAT Videos Provide UAT training Facilitate daily UAT meeting Review reported defects identified to be changes to the approved specification with the agency
GL Solutions	Quality Assurance Team	<ul style="list-style-type: none"> Analyze client reported UAT defects Classify issue severity in accordance with the agreed upon definitions Test defect resolution according to the approved specification Provide notification to the agency of defect correction
Agency	Project Manager	<ul style="list-style-type: none"> Attend daily UAT meeting Ensure agency is testing according to the UAT plan
Agency	Subject Matter Experts	<ul style="list-style-type: none"> Review UAT Videos prior to UAT meetings Participate in testing according to the UAT plan

Training

GL Solutions provides hands-on, role-based training, and is aligned with WVBOM's specific licensing processes, credential types, and staff roles. We embed training throughout the project lifecycle—so WVBOM staff build comfort with GL Suite in the context of their actual day-to-day responsibilities, not in a disconnected classroom environment.

Training Methodology

GL Solutions uses a “**show, tell, practice**” model:

1. **Show:** We demonstrate functionality using WVBOM's configured system, applying real examples from WVBOM's business processes.
2. **Tell:** We explain the reasoning behind configuration choices, connecting workflows to regulatory and statutory outcomes.
3. **Practice:** We guide WVBOM staff through real exercises in the live system, reinforcing understanding and readiness.

This approach is repeated during configuration, User Acceptance Testing (UAT), Go-Live, and post-Go-Live periods to ensure sustained adoption.

We also support a **train-the-trainer** model. WVBOM may designate Super Users or Subject Matter Experts (SMEs) by program area (e.g., physician licensing, disciplinary actions). These individuals receive

additional training and support, enabling them to lead internal onboarding, answer staff questions, and reduce reliance on external support over time.

Integrated Training Phases

Training is embedded across each project milestone:

1. Design and Configuration Phase:

- Guided demos and video walkthroughs of your system as it's configured.
- Business process discussions tied directly to WVBOM's workflows.

2. User Acceptance Testing (UAT):

- Structured hands-on practice using configured workflows, checklists, and licensing scenarios.
- Identification of knowledge gaps and adjustments to training focus.

3. Go-Live:

- One week of onsite training is included in the cost proposal.
- GL Solutions' Training Lead, Project Manager, or Analyst provides real-time floor support as WVBOM transitions to production.

4. Post-Go-Live Support:

- Follow-up remote or onsite training (available upon request) for new users, system refreshers, or additional topics.

Training Materials and Tools

GL Suite's training is supported by editable documentation tailored to WVBOM's configuration:

- **Process Guides:** Step-by-step user manuals covering licensing, renewal, complaints, and more.
- **Self-Documenting Specifications (SDS):** Auto-generated technical documentation showing screen fields, business rules, and data relationships.
- **Video Walkthroughs:** Short clips created by your assigned Business Analyst, explaining system functions in WVBOM's terminology.
- **Role-Based Exercises:** Completed during UAT and Go-Live to ensure job-specific understanding.
- **Training Records:** Track individual user participation, readiness, and gaps.

All materials are delivered in editable Word or digital formats, with printed copies available if requested.

Training for Public Users

GL Suite's public portal includes:

- Embedded FAQs, help text, and step-by-step prompts for tasks like submitting applications or uploading documentation.

- These tools are configurable by WVBOM staff to reflect the Board's terminology, policies, and license types.
- Public-facing instructions can be updated over time without vendor intervention.



Process Guides



Training Guides



Lesson Plans



Hands-On
Exercises



Individual
Training Records



Skills Activities
List

Go-Live

Following completion of User Acceptance Testing (UAT), the system will be deployed into the production environment for full use by WVBOM. GL Solutions will provide simple instructions, production site credentials, and direct assistance to support the transition.

WVBOM Responsibilities During Go-Live:

- Notify staff of system launch and workflow changes.
- Provide license and case sequencing numbers.
- Deliver final data exports at designated intervals.
- Cease data entry in the legacy system once final data is submitted.
- Confirm data conversion accuracy within the live environment.
- Test all system interfaces and scheduled jobs in the live environment.
- Update desktop shortcuts and login instructions for staff.

GL Solutions' Responsibilities During Go-Live:

- Deploy the live environment and validate production readiness.
- Provide real-time Go-Live assistance, including onsite or remote support.
- Supply conversion reports and documentation for recordkeeping.
- Support live testing of interfaces and system-generated communications.
- Establish processes to ensure a smooth transition into the 90-day stabilization phase.

Maintenance and Support

GL Simple

GL Solutions understands that successful implementation is only the beginning. Ongoing, responsive, and expert support is critical to ensuring that your system continues to serve your mission effectively. That's why we offer GL Simple, our all-inclusive maintenance and support model designed to help agencies like WVBOM sustain operational excellence—without surprises or complexity.

GL Simple provides unlimited access to our expert support team, hosting (if desired), and all software updates and enhancements for a single, fixed rate. It empowers agencies to evolve incrementally, prioritize new capabilities year to year, and receive dedicated support every step of the way.

Warranty

Upon going live, a three-month stabilization (warranty) period will commence, ensuring all project scope items are functioning correctly. This phase marks a transition from the fast-paced installation to a more moderated technical support environment. During stabilization, interaction between GL Solutions and WVBOM will shift focus toward technical support tasks and enhancements. The GLSimple support plan includes monthly meetings with the Project Manager, allowing for ongoing communication about project progress and support needs. staff can reach out to the Project Manager at any time for inquiries or concerns. GL Suite's Communication Center will provide a real-time vehicle for authorized administrators to communicate issues, monitor tasks and projects, and directly communicate with GL Solutions personnel.

Issue Reporting and Workflow Management

GL Solutions employs a work management system to categorize user-reported issues as defects or enhancements based on accepted specifications. All comments and requests for modifications, including those from WVBOM testers, will be routed through the GL Portal. This ensures that issues are addressed efficiently within our workflow management system. If reported defects are identified as enhancements requiring changes to accepted specifications, the Project Manager will validate the assessment and prioritize work, accordingly, ensuring the most critical tasks are addressed first.

Post-Go-Live Support

- **Comprehensive support** will continue after the warranty period, focusing on defect resolution and change request management.
- **Regular updates and patches** will be applied at no additional cost, ensuring ongoing security and reliability.
- **Performance measurements and continuous improvement processes** will be implemented to optimize system performance and enhance agency effectiveness.

Transition to Maintenance and Operations Support: During the 90-day stabilization period, GL Solutions will conduct an audit to ensure the system meets defined requirements and objectives. Defects reported during this time will be corrected at no additional cost. After stabilization, the project will transition to ongoing maintenance and support. The Project Manager will step back from day-to-day involvement as GL Solutions' dedicated Agency Partner (AP) assumes the primary point of contact role. The AP will



manage ongoing support, address issues, and coordinate with other GL Solutions departments as needed.

System Enhancements Management: Enhancements and non-critical issues will be prioritized based on severity. Clients can prioritize tasks, ensuring that issues are resolved in a timely manner according to their impact on operations. Our internal workflow guarantees that tasks are directed to the appropriate teams for resolution, with final confirmations sought from WVBOM.

Patch and Upgrade Support Services: GL Solutions provides comprehensive patch and upgrade support to ensure high-quality release management, including timely application of patches, point upgrades, and major releases. Our release strategy involves scheduled updates (e.g., quarterly for patches, annually for major upgrades) while accommodating WVBOM's preferences for timing and implementation.

Dedicated Agency Partner Support

At GL Solutions, every client is assigned a dedicated Agency Partner (AP), a highly engaged team member whose role is to ensure your success through proactive relationship management, strategic guidance, and responsive support. The AP is more than a point of contact; they are a problem-solver, a communicator, and your trusted advocate within GL Solutions.

The AP supports by:

- Monitoring your agency calendar and preparing for high-volume periods, such as renewals and inspections
- Responding to requests with urgency and professionalism, escalating critical items through GL Solutions' standard resolution processes
- Coordinating cross-functional teams to resolve issues, implement improvements, and drive continued success.
- Leading your staff through GL Solutions' Project Management Methodology (PMM), helping ensure business processes are executed consistently and effectively.
- Listening deeply, identifying future opportunities, and guiding your team toward long-term growth and adaptability

Responsive, Around-the-Clock Support

- **24x7 Emergency Support** for critical system issues.
- **Standard support hours** for non-urgent questions and troubleshooting.
- **Timely Responses**—we respond to all service requests within 24 hours.
- **Continuous Resolution Effort**—high-priority items remain active until fully resolved.

All reported issues are entered into our task routing system within GL Portal and assigned to appropriate teams for resolution, testing, and confirmation. You stay informed at every step.

Empowered End Users

staff should feel confident and supported using GL Suite. That's why GL Solutions offers:

- **Interactive Process Guides** that walk users step-by-step through every business process. These guides track progress, enable status updates, and ensure consistency across roles.



- **On-Demand Training Videos**, supported by guided walk-throughs led by the business analysts who designed your specific processes.
- **Live Training Courses**, covering configurations, reporting, rules, and more.
- **Role-Based Training** for onboarding new staff or refreshing existing users—customized to how your agency does business.

Technical Support and Configuration Assistance

Whether your team is hands-on with configuration or prefers support, GL Solutions offers flexible assistance:

- **Configuration Troubleshooting**—we guide your staff through modifying screens, rules, and workflows.
- **Developer-to-Developer Support**—direct access to GL developers for integrations, custom GUI development, or web services.
- **Remote Desktop Support**—with permission, we provide real-time troubleshooting by interacting directly with your system.
- **Documentation and Reporting Tools**—we help you produce ad hoc and scheduled reports using GL Suite’s powerful reporting engine.

Change Notification Protocols

GL Solutions implements a transparent, structured change management process to maintain alignment and accountability:

- **Raising and Framing Changes:** Changes originate from the Agency Partner, Project Manager, or technical stakeholders, and are evaluated for scope impact. Minor changes are documented in project meetings; significant changes require formal Change Requests (CR) or Change Order Request Forms (CORF).
- **Change Request Process:** Initiation, internal review, client review and approval, and execution phases ensure thorough assessment and client buy-in before billing.
- **Scope Control:** Change Orders manage work beyond the initial agreement, detailing scope, roles, costs, and schedule impact.
- **Risk Management:** Risks and issues related to changes are logged, reviewed weekly, and escalated as agreed.
- **Scope Protection:** Changes are managed separately from core deliverables with distinct approval and funding paths, ensuring original project scope stability.

Table 1—Project Points of Contact and Responsibilities				
Organization	Title and Responsibility	Name	Phone Number	Email Address
SDDL	Project Sponsor			
SDDL	Project Manager			
SDDL	Technical SME; Hardware			
SDDL	Technical SME; Software			
SDDL	Technical SME; Data transmission			
SDDL	Contract Administrator			
SDDL	Contract Monitor			
Organization	Title and Responsibility	Name	Phone Number	Email Address
Contractor	Relationship Representative			
Contractor	Project Manager			
Contractor	Programmer			
Contractor	DBA			
Contractor	Technical SME; Hardware			
Contractor	Technical SME; Software			

Table 2—Project Specific Roles and Responsibilities		
Roles and Responsibilities	Contractor	DOS
Project requirement and dependency #1		
Project requirement and dependency #2		
*primary (P)		

Table 3—Project Schedule			
No.	Deliverable Description	Due Date	Comments

Table 4—Pricing				
Deliverable Description	Service Category and Description (e.g., Programmer) and Employee Name	Quantity of Hours	Hourly Rate in Contract	Cost Extension

A standard CORF will include the above tables.

Change Management Approach

Recognizing the organizational impact of software implementations, GL Solutions provides a structured Change Management Service to:

- Build buy-in through clear communication of vision and business drivers
- Prepare managers to lead teams through change
- Support sponsors in maintaining momentum and modeling commitment
- Engage end users for feedback, expectation-setting, and targeted support

Change management roles are shared among project sponsors, managers, agency staff, and GL Solutions personnel. Activities begin ideally before project kickoff, with ongoing reinforcement during design, testing, and deployment phases to ensure successful adoption.

Support Escalation Paths

Issue resolution is prioritized by severity and business impact. Reported issues generate tasks routed internally to the appropriate teams. Upon resolution, tasks are returned to the Agency Partner for client confirmation.

Timeline

P1	P2	P3	Enhancements/ Changes
24 x 7 x 365	≈ 5 business days	≈ 14 business days	≈ 5 business days

Stakeholder Communication Processes

GL Suite's GL Portal provides a secure, centralized platform for communication and collaboration between WVBOM staff and GL Solutions personnel. It supports notifications, task tracking, issue reporting, training access, and project coordination.

Key features include:

- Structured tracking of tasks and projects with lifecycle visibility
- Power BI dashboards presenting real-time system metrics
- Issue submission and resolution monitoring
- Calendar tools for meetings and deadlines
- Real-time direct communication with Project Manager (installation) and Agency Partner (support)

GL Portal delivers a seamless, transparent communication environment that enhances collaboration and accelerates issue resolution.

Approach and Methodology to Compliance with Mandatory Project Requirements

GL Solutions ensures full alignment with WVBOM’s mandatory requirements through a secure, scalable, and fully configurable platform built specifically for regulatory agencies. GL Suite complies with state and federal standards for data privacy, uptime, accessibility, disaster recovery, auditability, and user access management. Our Software-as-a-Service (SaaS) solution, hosted in Microsoft Azure Government Cloud, provides a secure foundation with robust role-based access controls, audit tracking, automated alerts, and system performance safeguards.

This section outlines how GL Suite complies with each mandatory requirement listed in the RFP and highlights key areas where the solution exceeds those requirements. Detailed technical and procedural information is provided in the subsections that follow.

Compliance Mapping Table

Mandatory Requirement	GL Suite Response	Reference Section
HIPAA and PII Compliance	Encrypted data in transit and at rest, role-based access, audit trails	Security and Access Control Compliance
WCAG 2.1 AA Accessibility	Configurable portals with embedded help text, fully accessible per WCAG 2.1 AA	Accessibility and Usability Standards
99.9% System Uptime	Azure-hosted architecture with automatic scaling and failover	Hosting and Availability Compliance
Role-Based Access and SSO/MFA	Fine-grained access via RBAC, optional MFA, SSO with Active Directory or Okta	Security and Access Control Compliance
Audit Logging and Historical Recordkeeping	Transactional audit logs, record change history, timestamped capture logs	Data Integrity and Auditability
Secure Public and Internal Notifications	Rules-based notifications, multi-channel delivery, configurable triggers and escalation workflows	Notifications and Escalations
Disaster Recovery and Data Backup	Daily encrypted backups, quarterly restoration testing, documented RTO/RPO	Backup and Disaster Recovery
Browser and Device Compatibility	Fully web-based, supports Chrome, Edge, Firefox—no desktop installs required	Browser/Device Compatibility
Compliance with State/Federal Standards (e.g., StateRAMP, NIST)	Azure compliance, encryption standards, StateRAMP “In Process” status	Compliance with State/Federal Digital Standards



Each of the above areas is described in more detail in the pages that follow, organized by compliance topic.

Security and Access Control Compliance

GL Suite is designed with a defense-in-depth security posture to protect WVBOM's sensitive data and system access. We implement robust Role-Based Access Control (RBAC) to ensure staff and external users only access authorized data and functionality. System access is further secured by optional Multi-Factor Authentication (MFA) and Single Sign-On (SSO) integration with identity providers such as Microsoft Active Directory and Okta.

All system activity is logged and auditable. Audit trails, session tracking, and change histories ensure transparency and accountability, meeting WVBOM's needs for data governance and forensic readiness.

Highlights

- RBAC tailored to license types, user roles, and regulatory functions
- Optional MFA and SSO for enhanced access security
- Segregated production, test, and training environments
- Audit logging for all transactions, access attempts, and data changes

Hosting and Availability Compliance

GL Suite is hosted in the Microsoft Azure Cloud, ensuring WVBOM receives enterprise-grade security, high availability, and elastic scalability. With the appropriate GL Simple support plan, the system architecture supports 99.9% uptime, excluding scheduled maintenance, with automated scaling to accommodate increased demand.

Hosting Environment Features

- Geo-redundant data centers with automatic failover
- Load balancing and persistent session management
- Continuous performance monitoring and alerting
- FedRAMP infrastructure with government-specific compliance layers

GL Solutions guarantees responsive uptime, supported by Azure's infrastructure and our own service monitoring protocols.

Data Integrity and Auditability

GL Suite maintains full data integrity and audit trails across all entities and transactions. Every user action—whether editing a record, submitting a form, or generating a time-stamped letter and associated with a user ID. This includes changes to names, addresses, statuses, and license history.

Our Capture Log allows granular tracking of system use, enabling administrators to audit even non-data-changing actions such as button clicks or document views. Finalized communications and documents are versioned and retrievable indefinitely.

Key Features

- Full lifecycle audit history of all data and workflow transactions
- Capture logs for user actions and interface interaction
- Record histories visible in licensee, case, and organization views
- Configurable audit reporting for compliance, QA, and legal review

Notifications and Escalations

GL Suite includes a powerful rules-based notification engine configured to WVBOM's workflows. Automated alerts notify staff, applicants, licensees, or third parties of time-sensitive events, such as license expiration, incomplete applications, or complaint escalations.

Notifications are configured during implementation using GL Suite's business rules engine and can be modified by WVBOM administrators as policies evolve.

Examples

- Licensees receive renewal reminders at 30, 15, and 5 days before expiration
- Investigators receive alerts when a new complaint is assigned
- Supervisors are notified when tasks age beyond acceptable thresholds
- Public users receive portal, email, and optional SMS updates simultaneously

Accessibility and Usability Standards

GL Suite is fully compliant with WCAG 2.1 AA accessibility standards, ensuring that all applicants, licensees, and the public can interact with WVBOM's self-service portals regardless of ability.

Features such as keyboard navigation, color contrast, scalable fonts, and screen-reader compatibility are embedded throughout the public-facing user experience. Contextual help and tooltips guide users through each form and process, reducing friction and increasing user satisfaction.

Browser/Device Compatibility

GL Suite is a web-based system, accessible on modern browsers (Edge, Chrome, Firefox) and fully compatible with mobile, tablet, and desktop devices. No local software installation or plugins are required for end users or agency staff.

Supported Platforms

- Browsers: Chrome, Edge, Firefox
- Operating Systems: Windows, macOS, iOS, Android
- Devices: Desktop, tablet, and smartphone

Back-office users benefit from Microsoft Office integration (optional), but GL Suite functions effectively with alternate office suites upon coordination.

Backup and Disaster Recovery

GL Suite includes a complete Disaster Recovery Plan (DRP) with daily encrypted backups, stored in geographically separated regions. Backups are validated quarterly through full restoration tests to ensure data integrity and recoverability.

Recovery Objectives

- Recovery Point Objective (RPO): 4 hours
- Recovery Time Objective (RTO): 24 hours
- Quarterly recovery testing and documented procedures
- Transparent failover coordination with WVBOM during activation

Compliance with State and Federal Digital Standards

GL Solutions maintains alignment with all relevant state and federal digital compliance frameworks. Hosting on Azure Government Cloud ensures compliance with FedRAMP, NIST, HIPAA, PCI-DSS, and StateRAMP (in-process).

In addition, our internal security program includes annual Information Protection Assessments, vulnerability testing, developer training, and documented security conventions across all operational tools and environments

Security

GL Solutions takes a comprehensive, defense-in-depth approach to security, ensuring that all WVBOM data, including sensitive Personally Identifiable Information (PII) and protected health data—is protected through encryption, access controls, real-time monitoring, and full compliance with applicable security and accessibility standards.

Secure, Scalable, Cloud-Hosted Architecture

GL Suite is hosted in the Microsoft Azure Cloud, a FedRAMP-authorized environment that provides a secure, scalable foundation for WVBOM’s licensing and case management operations. The platform’s n-tier software architecture isolates sensitive data from user-facing components, reducing exposure and improving resilience.

Role-Based Access Control (RBAC)

GL Suite includes a robust Role-Based Access Control (RBAC) framework that enables WVBOM to define fine-grained access by user role, license type, or operational function. Staff and board members access only what is needed to perform their duties, supporting both data protection and operational efficiency.

Compliance with HIPAA, PII, and WCAG 2.1 AA

GL Suite meets the following compliance standards:

- **HIPAA:** All protected health data is stored and transmitted securely using industry-standard encryption.

- **PII Handling:** Access controls, encryption, and audit trails ensure WVBOM's compliance with state and federal data privacy rules.
- **WCAG 2.1 AA:** All user-facing portals meet accessibility guidelines to ensure equitable service to all stakeholders.

StateRAMP Status

GL Solutions is on track to achieve StateRAMP authorization by the end of Q4 2025, demonstrating our commitment to meeting one of the most rigorous cybersecurity frameworks for state and local government cloud vendors. Our solution is currently listed as "In Process" on the StateRAMP/GovRAMP progressing product list.

Continuous Monitoring and Threat Response

GL Suite is continuously monitored through integrated security tools, including:

- **Azure Sentinel (SIEM):** For system-wide threat detection and incident response.
- **Azure Defender:** For behavioral analytics and infrastructure threat prevention.
- **Redgate SQL Monitor:** For database-level performance and security alerts.



Internal Security Policies and Oversight

GL Solutions maintains a comprehensive internal governance framework to enforce and monitor security across all systems:

- **Security Authorization and Conventions Policies:** Define user roles, permission boundaries, and system configuration requirements across Active Directory, AlienVault, and related tools.
- **Information Protection Assessment:** Applies secure development standards and mandates annual secure coding training for all software developers.
- **Security Testing and Remediation:** Includes routine vulnerability assessments, penetration testing, and tracked remediation cycles to ensure continuous platform hardening and compliance.

Staff Training and Vetting

- **Mandatory Security Training:** All GL Solutions personnel complete annual training on information security, PII handling, and regulatory compliance.
- **Background Checks:** All employees undergo background screening upon hire and annually thereafter, with enhanced checks for those with elevated access privileges.

Security, Auditing, and Notifications

Security, Auditing, and Notifications

GL Suite is built to support WVBOM's need for a highly secure, compliant, and responsive system that protects sensitive information, maintains audit trails, and ensures timely communication with internal and external stakeholders.

Role-Based Security and Access Management

GL Suite ensures only authorized users access sensitive data and system functionality through robust role-based controls and authentication mechanisms.

Key Features:

- **Role-Based Access Control (RBAC):** Users are assigned permissions based on their roles, ensuring appropriate access across licensing, case, and enforcement modules.
- **Single Sign-On (SSO):** Supports integration with Active Directory, Okta, or similar identity providers for seamless and secure user access.
- **Multi-Factor Authentication (MFA):** An optional security enhancement requiring a second form of authentication at login.
- **Environment Isolation:** Production, testing, and training environments are kept separate to minimize risk.

Audit Logging and Historical Tracking

GL Suite provides comprehensive audit capabilities to ensure system integrity, user accountability, and historical recordkeeping.

Key Capabilities:

- **Transactional Audit Logs:** Every system interaction—logins, data edits, button clicks, document views—is logged with timestamps and user IDs.
- **Record Change History:** The system retains full historical data for changes to names, license statuses, addresses, and more.
- **Capture Logs:** Tracks granular user actions, including clicks, downloads, field edits, and workflow steps.
- **Audit Reports:** Staff can generate detailed reports showing the lifecycle of records and user interactions for legal, compliance, and troubleshooting purposes.
- **Correspondence Archiving:** Finalized communications are linked to records and stored for long-term retrieval and reprinting.

Notification and Alerting System

GL Suite includes a powerful, rules-based notification engine that automates internal task alerts and external communications to licensees, applicants, and stakeholders.

Internal Notifications (Staff-Facing)

- **Configurable Triggers:** Based on business rules, e.g., a status change, due date, new submission, or pending task.
- **Work Assignment Integration:** Tasks are routed automatically to the appropriate staff user's task drawer (queue).
- **Escalation Workflows:** Items that remain incomplete beyond defined timeframes are routed to supervisors.
- **Examples:**
 - Notify enforcement if a facility under investigation attempts to renew.
 - Alert managers if a complaint remains unreviewed after 30 days.
 - Alert users when a related application is withdrawn.

External Notifications (Licensee/Public-Facing)

- **Multi-Channel Delivery:** Email, SMS (opt-in), and portal inbox messaging.
- **Event-Driven Alerts:**
 - Application receipt, status changes, or deficiencies.
 - License approval and issuance.
 - Renewal reminders at 30, 15, and 5 days before expiration.
- **Web and Email Synchronization:** Portal-based alerts are paired with email/SMS to ensure licensees are aware of pending tasks.

Batch Communications

- **Bulk Email/SMS Tools:** GL Suite supports batch communications to applicants, licensees, or defined groups, allowing WVBOM to send targeted reminders, updates, or policy notices efficiently.

Business Process Messaging

- Automated, context-specific messages guide licensees and applicants throughout each workflow stage (e.g., "Your application is approved," or "Deficiency flagged—please correct and resubmit").

Database and Technical Requirements

GL Suite is a Commercial Off-The-Shelf (COTS), Software-as-a-Service (SaaS) solution hosted in the Microsoft Azure cloud environment. The system supports WVBOM's complex licensing, enforcement, and case management needs through a no-code, configurable relational database and scalable infrastructure. GL Suite's architecture enables secure access, high availability, and flexible configuration without custom development.

Technical Overview

- **Architecture:** N-tiered design (Presentation, Business Logic, and Data layers) to ensure modularity and scalability
- **Database:** Microsoft SQL Server with RAID-enabled storage for performance and data integrity
- **Hosting:** Microsoft Azure Government Cloud (U.S. region), supporting full redundancy and high availability
- **Network:** Encrypted HTTP/S traffic with customizable SQL port access, firewall-protected environment
- **Application Framework:** ASP.NET and IIS 7+ on Windows OS

System Uptime and Performance

Based on the support plan selected, GL Solutions guarantees 99.9% uptime excluding planned maintenance, supported by Azure's redundant infrastructure, automated monitoring, and alerting. Real-time performance metrics and proactive system monitoring ensure system responsiveness and continuity of operations. System capacity scales automatically to accommodate increased user load or data growth.

Disaster Recovery and Backup

GL Suite includes a complete disaster recovery plan with:

- Daily encrypted backups stored in geographically separated regions
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) within 24 and 4 hours respectively
- Quarterly restoration tests and audit logs to validate recovery capability
- Transparent failover procedures and incident response coordination with WVBOM if activated

Software Requirements

Client Devices:

- Web browser: Chrome, Edge, or Firefox (no local install required)
- Office software: Microsoft Office preferred for back-office functions (other suites compatible with prior coordination)

Third-Party Components:

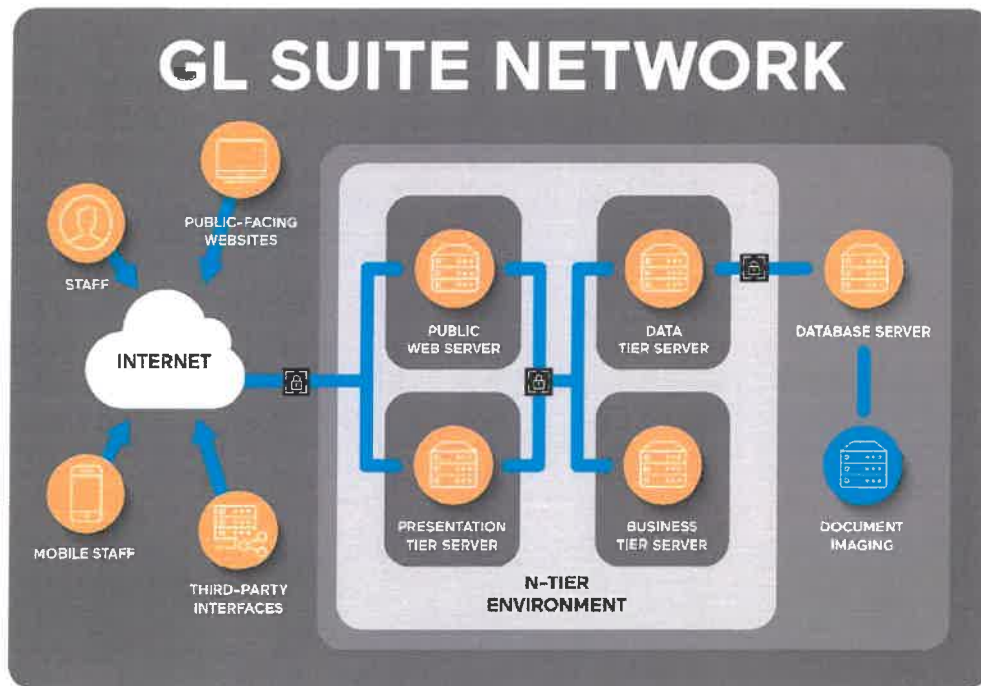
GL Suite operates with a minimal set of reliable third-party components, including:

- Microsoft Windows OS
- Microsoft Office (optional)

- Microsoft IIS and .NET Framework
- Telerik (UI components)
- Abbyy FineReader (OCR engine) or equivalent
- Standard modern browsers

Core Modules

1. **Licensing:** Configurable workflows supporting new applications, renewals, CE tracking, and reciprocity
2. **Case Management:** Tracks complaint intake, investigations, discipline, and enforcement actions
3. **Reporting:** Ad hoc and scheduled reports with Power BI integration
4. **Financials:** Secure, PCI-DSS-compliant fee tracking, invoicing, and online payments
5. **Document Management:** Cloud storage with indexing, tagging, and role-based access control





Hosting and IT

Hosting Infrastructure

GL Suite is hosted within the FedRAMP-certified Microsoft Azure cloud environment, ensuring high availability, security and scalability. GL Suite is designed to handle growing demands while minimizing disruptions, providing a reliable, secure infrastructure for state and vendor needs.

Technical Environment

Azure's cloud infrastructure supports a highly scalable and reliable environment, offering several key capabilities:

- **Load Balancing:** Azure Application Gateway ensures efficient distribution of traffic, providing SSL offloading, session persistence, and failover mechanisms to maintain optimal performance and minimize disruptions.
- **Geo-Redundant Hosting:** Data is replicated across multiple US-based, geographic regions, ensuring high availability. In the event of regional disruption, services are automatically rerouted to another region, preventing downtime.
- **Disaster Recovery:** Azure's disaster recovery capabilities, including multi-region replication and automatic failover, ensure minimal downtime and business continuity.
- **Persistent Session Management:** Azure App Services maintains user sessions during scaling events or maintenance, ensuring a seamless experience for users even during system updates or changes.

Compliance and Security

Azure's compliance with industry standards such as HIPAA, NIST, PCI-DSS, and StateRAMP ensures that data is handled securely. Key security features include:

- **Encryption:** Data is encrypted in transit and at rest using TLS and AES-256 encryption standards, safeguarding sensitive information.

- **Role-Based Access Control (RBAC):** Ensures that only authorized users have access to specific data and functionalities, adding an additional layer of security.
- **Continuous Monitoring:** Tools like Azure Sentinel and SQL Monitor provide real-time threat detection and continuous monitoring to ensure compliance with security standards.

Scalability and Reliability

The use of Azure's virtualized infrastructure ensures that GL Suite can scale both vertically and horizontally to meet the evolving needs of the system. Vertical scaling allows for on-demand increases in resources like CPU and memory, while horizontal scaling adds additional instances of GL Suite services across multiple virtual machines, ensuring consistent performance even during periods of high demand.

Benefits to West Virginia

Reducing Application Processing Time

GL Suite significantly accelerates the application processing lifecycle for state agencies. By automating workflows, document management, and data entry, agencies can reduce processing times from months to days or weeks. Configurable business rules and automated document status updates ensure faster decisions and allow agency staff to focus on critical regulatory tasks rather than manual paperwork. This efficiency is especially crucial for agencies that manage complex licensing processes, like health and safety departments.

Scalability for Growing Demands

As the state's population or regulatory needs grow, GL Suite's cloud infrastructure scales seamlessly to handle increased volumes. Whether managing hundreds or thousands of applications, GL Suite can scale horizontally, supporting high-demand periods without performance degradation. This scalability ensures that the system can accommodate future growth and evolving regulatory requirements, making it a long-term solution for the state.

Handling Complex Regulatory Processes

GL Suite excels in managing complex, regulated workflows, supporting a wide variety of license types and compliance needs. From healthcare facility inspections to firearm licensing, the system adapts to the specific rules and regulations of each agency, ensuring compliance while streamlining processes. Its ability to enforce strict business rules and integrate with external databases ensures data accuracy and regulatory integrity, providing government agencies with a tool capable of managing even the most complicated compliance tasks.

Qualifications and Experience

General Vendor Qualifications

Company Overview

GL Solutions is a 25-year-old technology company with 91 employees, specializing in providing comprehensive licensing and regulatory solutions for professional boards and state agencies. Our flagship product, GL Suite, is in its seventh version and has been refined over decades to meet the evolving needs of regulatory agencies. Our expertise spans healthcare-related boards, including medicine, pharmacy, dentistry, and health departments, where we support complex licensure, compliance, and enforcement workflows with secure, scalable technology.

Similar Projects

Relevant Client Experience

- **Wyoming Board of Medicine - *current client***
We have been a trusted partner of the Wyoming Board of Medicine for 15 years, delivering and supporting a system closely aligned with the requirements and scope of WVBOM's needs.
- **Arkansas Board of Pharmacy & Wyoming Board of Pharmacy - *current client***
GL Solutions implemented and currently supports licensure systems for these pharmacy boards, managing intricate licensing, compliance, and enforcement processes using GL Suite.
- **Arizona Medical Board - *current client***
We partnered with the Arizona Board of Medical Examiners (AZBOM) to implement a comprehensive licensing and enforcement platform. This system supports online license application and renewal for physicians and physician assistants, complaint and investigation management, compliance and enforcement workflows, and public access to board documents. In 2023, we migrated AZBOM to GL Suite 7 and are actively enhancing performance, including migration to Microsoft Azure and adding Board Meeting management tools.

Experience with Other State Regulatory Agencies

- **West Virginia Alcohol Beverage Control Administration - *current client***
Our implementation of GL Suite supports licensing, permitting, and enforcement activities aligned with WVABC's mission. The platform streamlines online retailer permits and transportation licenses, improves transparency and compliance, and offers robust reporting capabilities.
- **Nevada Board of Alcohol, Drug and Gambling Counselors - *current client***
GL Suite modernization efforts facilitated the migration of key workflows online, including application renewals and automated communications. The public-facing portal enhances licensure verification and overall regulatory transparency.
- **Arizona Board of Cosmetology & Barbering - *current client***
We provide IT licensing and compliance solutions that have generated significant efficiencies and cost savings, such as \$50,000 annually in postage savings through online license delivery. Recent upgrades include migration to GL Suite 7 and advanced features like QR code license issuance.

Staffing Plan and Schedule

GL Solutions takes a collaborative, cross-functional approach to project delivery. A dedicated Project Manager and Business Analyst will be assigned to WVBOM and remain consistent throughout the project. After go-live, a dedicated Agency Partner will serve as your long-term point of contact through maintenance and support. Behind them stands the full strength of our company, ensuring the success of your implementation and continued operations.

Rather than assigning siloed project teams, GL Solutions draws on the expertise of each department at the right time:

- **Operations** – supporting your project from discovery through design, development, testing, and deployment.
- **Administration** – managing system security, licensing, and billing.

- **Business Solutions** – overseeing executive relationships, training, project management, and long-term support.

This flexible, scalable model allows us to deliver high-quality results while maintaining continuity and responsiveness. WVBOM will always have access to experienced professionals who understand your regulatory environment, goals, and priorities—every step of the way:

- Implementation team and support staff roles.
- Resources available for training, support, and system evolution.

GL Solutions proposes a structured and collaborative project approach spanning 331 **business** days from kickoff to go-live – January 12, 2026, to April 19, 2027. (**NOTE:** *This schedule is based on all metrics provided by WVBOM, assumptions made by GL Solutions and typical implementation timelines for a system like this*). The following sections outline how each deliverable and service will be completed, with details on project management techniques, staffing, task durations, deliverables, dates, dependencies, required agency participation, and training.

Task Breakdown with Estimated Hours, Deliverables, Task Dependencies, and Elapsed Dates

WBS	Task Name	Dependencies	Duration	Start	Finish	Resource Names
	West Virginia Board of Medicine		331 days	Mon 1/12/26 8:00 AM	Mon 4/19/27 5:00 PM	
1	Project Initiation		51 days	Mon 1/12/26 8:00 AM	Mon 3/23/26 5:00 PM	
1.1	Project Manager - Initial Contact		1 day	Mon 1/12/26 8:00 AM	Mon 1/12/26 5:00 PM	GLS
1.2	Kickoff meeting	2FS+7 days	1 day	Thu 1/22/26 8:00 AM	Thu 1/22/26 5:00 PM	GLS,Agency
1.3	GL Solutions Request Legacy Data	2	5 days	Tue 1/13/26 8:00 AM	Mon 1/19/26 5:00 PM	GLS,Agency[50%]
/	Project Details		50 days	Tue 1/13/26 8:00 AM	Mon 3/23/26 5:00 PM	
1.4.1	Management Plan	2	10 days	Tue 1/13/26 8:00 AM	Mon 1/26/26 5:00 PM	GLS,Agency[50%]
1.4.2	Acceptance of Management Plan	6	10 days	Tue 1/27/26 8:00 AM	Mon 2/9/26 5:00 PM	Agency

1.4.3	Assessments Complete	7	10 days	Tue 2/10/26 8:00 AM	Mon 2/23/26 5:00 PM	GLS,Agency[50%]
1.4.4	Goals and Scope Document	8	10 days	Tue 2/24/26 8:00 AM	Mon 3/9/26 5:00 PM	GLS,Agency[50%]
1.4.5	Acceptance of Goals and Scope Document	9	10 days	Tue 3/10/26 8:00 AM	Mon 3/23/26 5:00 PM	Agency
2	Software Design and Development		150 days	Tue 3/24/26 8:00 AM	Mon 10/19/26 5:00 PM	
2.1	Use Case Design and Approval		40 days	Tue 3/24/26 8:00 AM	Mon 5/18/26 5:00 PM	
2.1.1	Use Case Design	10	40 days	Tue 3/24/26 8:00 AM	Mon 5/18/26 5:00 PM	GLS
2.1.2	Use Case Approval	13SS+10 days	30 days	Tue 4/7/26 8:00 AM	Mon 5/18/26 5:00 PM	GLS,Agency[50%]
2.2	System Design Upgrade and Configuration		55 days	Tue 5/19/26 8:00 AM	Mon 8/3/26 5:00 PM	
2.2.1	Detailed Specifications	14	50 days	Tue 5/19/26 8:00 AM	Mon 7/27/26 5:00 PM	GLS,Agency[50%]
2.2.2	Acceptance of Specifications	16SS+10 days	45 days	Tue 6/2/26 8:00 AM	Mon 8/3/26 5:00 PM	Agency
2.3	Automation and Rule Development by GL Solutions		55 days	Tue 8/4/26 8:00 AM	Mon 10/19/26 5:00 PM	
2.3.1	Development	17	30 days	Tue 8/4/26 8:00 AM	Mon 9/14/26 5:00 PM	GLS
2.3.2	Unit Testing	19	25 days	Tue 9/15/26 8:00 AM	Mon 10/19/26 5:00 PM	GLS
3	Data Conversion		95 days	Tue 8/4/26 8:00 AM	Mon 12/14/26 5:00 PM	
3.1	Conversion Development	17	30 days	Tue 8/4/26 8:00 AM	Mon 9/14/26 5:00 PM	GLS

3.2	Conversion Round 1	22	15 days	Tue 9/15/26 8:00 AM	Mon 10/5/26 5:00 PM	GLS
3.3	Screen Reviews Round 1	23	10 days	Tue 10/6/26 8:00 AM	Mon 10/19/26 5:00 PM	GLS,Agency[50%]
3.4	Conversion Defect Correction	24	10 days	Tue 10/20/26 8:00 AM	Mon 11/2/26 5:00 PM	GLS
3.5	Conversion Round 2	25	10 days	Tue 11/3/26 8:00 AM	Mon 11/16/26 5:00 PM	GLS
3.6	Screen Reviews Round 2	26	10 days	Tue 11/17/26 8:00 AM	Mon 11/30/26 5:00 PM	GLS,Agency[50%]
3.7	Conversion Defect Correction	27	10 days	Tue 12/1/26 8:00 AM	Mon 12/14/26 5:00 PM	GLS
4	GLS System Testing		25 days	Tue 12/15/26 8:00 AM	Mon 1/18/27 5:00 PM	
4.1	GLS System Testing and Resulting Changes	28	25 days	Tue 12/15/26 8:00 AM	Mon 1/18/27 5:00 PM	GLS
5	User Acceptance Testing (UAT)		55 days	Tue 1/19/27 8:00 AM	Mon 4/5/27 5:00 PM	
5.1	UAT Prep	30	10 days	Tue 1/19/27 8:00 AM	Mon 2/1/27 5:00 PM	GLS
5.2	UAT	32	35 days	Tue 2/2/27 8:00 AM	Mon 3/22/27 5:00 PM	GLS,Agency
5.3	Defect Corrections	33	10 days	Tue 3/23/27 8:00 AM	Mon 4/5/27 5:00 PM	GLS,Agency[50%]
6	Training		15 days	Tue 1/19/27 8:00 AM	Mon 2/8/27 5:00 PM	GLS,Agency[50%]
6.1	Training Plan Finalization	30	5 days	Tue 1/19/27 8:00 AM	Mon 1/25/27 5:00 PM	GLS,Agency[50%]
6.2	Training Preparation	36	5 days	Tue 1/26/27 8:00 AM	Mon 2/1/27 5:00 PM	GLS,Agency[50%]

6.3	Onsite Training	37	5 days	Tue 2/2/27 8:00 AM	Mon 2/8/27 5:00 PM	GLS, Agency[50%]
7	Go Live		65 days	Tue 1/19/27 8:00 AM	Mon 4/19/27 5:00 PM	
7.1	Go Live Implementation Plan	30	20 days	Tue 1/19/27 8:00 AM	Mon 2/15/27 5:00 PM	GLS, Agency[50%]
7.2	GL Suite Go Live - including final conversion	34	10 days	Tue 4/6/27 8:00 AM	Mon 4/19/27 5:00 PM	Agency, GLS

Project Management Techniques:

We apply a hybrid project management approach using:

- **Structured Waterfall** methodology for major phases (e.g., Data Conversion, UAT).
- **Agile principles** (e.g., iterative design, feedback loops, collaborative sprint-style reviews).
- **Weekly status meetings** and issue tracking through our client portal.

Staffing and Resource Planning:

Key GLS Personnel and Roles

Role	Function / Responsibility	% on Project	% on Tasks
Senior Project Manager	POC with WVBOM. Provides leadership, communication, schedule management, risk escalation, training coordination.	100%	N/A
Workflow Manager	Manages scope, schedule, risk, and billing change processes	50%	As needed
Solutions Architect Lead	Use case development, requirements traceability, high-level deliverables	75%	75%
Senior Business Analysts	Requirements gathering, specifications, configuration	75%	75%
Quality Assurance Manager	Leads teams that perform defect triage and UAT defect response,	40%	40%
Training Lead	Develops and delivers training materials	100%	As needed

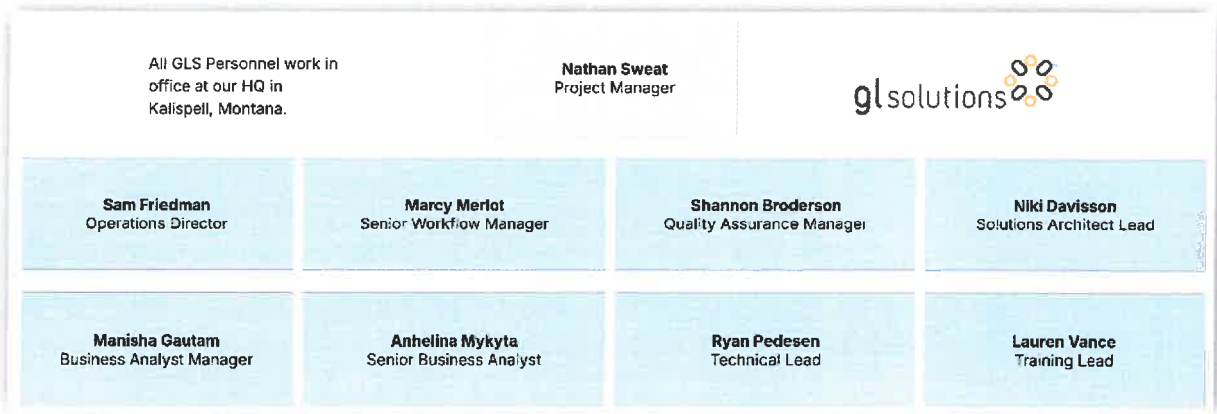
Role	Function / Responsibility	% on Project	% on Tasks
Configuration/Development Manger	Leads teams that configures and develops GL Suite, oversees data conversion	40%	40%
CEO, VPs (Ops, Strategy, Admin, Business Solutions)	Conflict resolution, oversight, security compliance, risk management	As needed	N/A

Required Personnel and Roles:

Role	Function / Responsibility
Executive Sponsor	Drives executive alignment, resolves conflicts, supports agency-wide adoption
Project Manager	Oversees day-to-day participation and status reporting
Program Project Manager	Compiles reports, forms, and supporting documentation
SMEs (Board Representatives)	Validate business processes, approve design/specs
IT Staff	Provide legacy data and support technical integration

The rest of this page intentionally left blank

Project Organization Chart



Staff Resumes and References



Shannon Broderson
Quality Assurance Manager

broderson@glsolutions.com
541-312-3662
555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Leads quality assurance efforts for WVBOM's-specific solution, dedicating 40% of time to the project. Manages testing activities, ensures adherence to GL Suite standards, and coordinates with cross-functional teams to validate system functionality, performance, and stability during all phases of implementation.

Work Experience

Quality Assurance Manager

GL Solutions – 2024 to Present

- Leads a team of QA engineers, developers, and analysts to uphold high-quality standards across projects.

- Directs testing for large-scale client installations, including web portals, back-office systems, and interfaces.
- Assists in back-office setup and system stabilization phases.
- Supports business analysis, QA, and project management teams.
- Developed streamlined QA processes to improve testing efficiency and issue resolution.
- Collaborates closely with project managers to align QA activities with project objectives.

Quality Assurance Specialist

GL Solutions – 2021 to 2024

RFP Experience

Wisconsin Department of Health

- Oversaw QA testing of business processes; ensured system performance and quality compliance.

Kansas Department of Health and Environment

- Led QA testing throughout all implementation phases.

Illinois Office of the State Fire Marshal

- Directed QA efforts for mobile inspection features and system integrations.

North Dakota Department of Health and Human Services

- Managed UAT and post-launch stabilization across all system modules.

Alabama Board of Cosmetology

- Oversaw QA in end-to-end installation, including web and back-office systems.

Nevada Board of Accountancy

- Currently managing QA for website development aligned with agency transformation goals.

Technical Skills

GL Suite Software | Microsoft DevOps | SQL | Microsoft Office Suite | Jira | Agile Methodologies



Niki Davisson

Solutions Architect Lead

davisson@glsolutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Works closely with WVBOM to develop use cases that inform system design. Dedicates 75% of time to this project.

Work Experience

Business Architect

GL Solutions – 2023 to Present

- Collaborates with Workflow Architects to understand and document client requests.
- Translates complex regulatory requirements into detailed, solution-oriented documentation.
- Leads the creation of comprehensive use cases following scope approvals.
- Facilitates handoffs to Business Analyst teams and supports cross-functional delivery.
- Applies expertise in government processes to support scalable and compliant system design.

Business Analysis Manager

GL Solutions – 2016 to 2023

- Managed business analyst team responsible for client software design.
- Designed solutions to meet installation and technical support requirements.
- Tested installation documents and development specifications.
- Developed internal business processes and contributed to policy improvements.

Agency Partner

GL Solutions – 2010 to 2016

- Managed business analysis efforts for system design and client implementation.
- Oversaw testing of installation and specification documents.
- Led internal process design for improved operational efficiency.

RFP Experience

Virginia Department of Behavioral Health & Developmental Services

- Led requirements gathering, business process design, interface design, UAT, and training.

New Mexico Children, Youth & Families Department

- Managed business analysts and provided design leadership for conversion and interface efforts.

Connecticut Department of Emergency Services and Public Protection

- Led conversion and interface design, ensuring a smooth system transition.

Nevada State Contractors Board

- Oversaw business process design, interface development, and data conversions.

New Mexico Environment Department

- Led design for optimized business processes and interface integration.

North Dakota Real Estate Appraiser Qualifications and Ethics Board

- Led interface and conversion design for licensing system implementation.

Nevada Housing Division

- Directed business process and interface design for efficient regulatory operations.

Education

Bachelor of Science in Business Administration

Eastern Oregon University – La Grande, Oregon

Associate of Arts in Business Administration

Central Oregon Community College – Bend, Oregon

Technical Skills

Environments: DOS, Windows

Software: GL Suite (XML-based), Microsoft Office, Microsoft Project



Sam Friedman

Operations Director

friedman@glsolutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Oversees the team responsible for configuring and developing WVBOM's-specific solution, dedicating 40% of time to the project.

Work Experience

Operations Director

GL Solutions –2022 to Present

- Manages a team of configuration specialists delivering regulatory software solutions.
- Oversees project planning, configuration, and delivery aligned with client expectations.
- Provides subject matter expertise in GL Suite configuration and leads internal development initiatives.

Senior Configuration Specialist

GL Solutions –2021 to 2022

- Directed data conversion and system configuration for regulatory clients.
- Collaborated cross-functionally to deliver client-specific licensing solutions.
- Provided advanced technical support and design customization.

Quality Assurance Specialist

GL Solutions –2020 to 2021

- Executed test plans and regression testing to ensure system reliability.
- Identified and documented software defects, ensuring timely resolution and release quality.
- Ensured client-specific requirements were met through comprehensive QA processes.

RFP Experience

Wisconsin Department of Health Services

- Supported licensing system configuration and reporting enhancements to strengthen regulatory oversight and client service delivery.

Kansas Department of Health and Environment

- Led the configuration and deployment of GL Suite's licensing and regulatory system.
- Ensured successful integration with state health systems and adherence to regulatory processes.

Illinois Department of Public Health – ENV and EMS

- Managed system configurations for environmental and EMS programs, meeting regulatory compliance and operational needs.
- Led QA testing to validate workflows specific to environmental health and emergency services.

Virginia Department of Behavioral Health & Developmental Services

- Directed development of bi-directional data interfaces to support statewide data exchange.
- Assisted with system update implementation, ensuring continued regulatory compliance.

Arkansas Board of Pharmacy

- Managed project delivery for pharmacy licensing software, focusing on seamless integration and user-friendly interface design.

Connecticut Department of Emergency Services and Public Protection

- Contributed to the successful migration of legacy systems to a cloud-based platform.
- Supported data integration and system stabilization with minimal downtime.

Education

Bachelor of Science in Kinesiology

University of Maryland, College Park, MA

Meta Front-End Developer Professional Certificate

Technical Skills

T-SQL, Java, C++, HTML/CSS, SQL, SASS, SCSS, LESS, PHP, Webflow

Microsoft Azure | GL Suite Configuration and Deployment



Manisha Gautam

Business Analyst Manager

gautam@glsolutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Leads the Business Analyst team that gathers business requirements, creates business and technical specifications for WVBOM's-specific solution. Dedicates 75% of time to the project.

Work Experience

Business Analyst Manager

GL Solutions – 2023 to Present

- Leads business analyst teams for major state agency projects, including Illinois Office of the State Fire Marshal and Illinois Department of Public Health.
- Designs and delivers training for new permitting software, improving staff adoption and operational workflows.
- Partners with stakeholders to develop business cases that align system features with regulatory and organizational needs.

Business Analysis Specialist

GL Solutions – 2022 to 2023

- Applied systems analysis to improve implementation outcomes for agencies such as VADBHDS, AKCCED, and ND Health and Human Services.
- Translated requirements into technical documentation, ensuring clarity and alignment between business and development teams.
- Authored security requirement documents including background check protocols.

Quality Assurance Specialist

GL Solutions – 2021 to 2022

- Reported and tracked software defects, collaborating with development to ensure timely resolution.
- Built testing programs including regression and usability testing, supporting system compliance.
- Performed compatibility testing across varied platforms to ensure reliability.

RFP Experience

Wisconsin Department of Health

- Provided UAT walkthroughs for client teams to validate system functionality.

Illinois Office of the State Fire Marshal

- Led development of business cases and trained staff on new permitting systems to support regulatory compliance.

Illinois Department of Public Health

- Designed business processes supporting environmental and EMS programs.

Connecticut Department of Social Services

- Managed firearm permitting software design, integrations, and compliance.

Virginia Department of Behavioral Health & Developmental Services

- Oversaw business process and conversion design, led UAT, and conducted end-user training.

New Mexico Children, Youth & Families Department

- Directed interface and conversion design, supporting analyst teams throughout implementation.

Nevada State Contractors Board

- Led process design and interface development to align with agency requirements.

New Mexico Environment Department

- Designed business processes and interfaces for system modernization.

North Dakota Real Estate Appraiser Qualifications and Ethics Board

- Managed business process design and system integration.

Nevada Housing Division

- Oversaw all business process and interface design activities during system conversion.

Education

Master of Arts in Anthropology

Panjab University, Chandigarh, India

Bachelor of Science

Himachal Pradesh University, Shimla, Himachal Pradesh, India

Technical Skills

GL Suite Software | Microsoft Office Suite | Business Process Modeling | User Acceptance Testing (UAT) | Systems Analysis | Agile Methodologies



Marcy Merlot

Senior Workflow Manager

merlot@glsolutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Manages project scope, schedule, risk, and change management processes for WVBOM's-specific solution. Collaborates closely with the Project Manager to ensure project alignment and successful

delivery. Dedicates 50% of time to the project.

Work Experience

Senior Workflow Architect

GL Solutions – 2022 to Present

- Collaborates closely with the Project Manager to manage risks, ensure project scope alignment, and maintain project timelines, ensuring seamless delivery to clients.
- Translates client needs into tailored solutions by leveraging a deep understanding of client systems and GL Solutions processes.
- Oversees delivery by managing project scope, risks, and schedules, matching client requests to appropriate GL Solutions services and pricing.
- Tasks out and schedules work post-scope approval, ensuring efficient workflow through the GL Solutions delivery process.
- Handles exceptional and complex work through a risk management process, ensuring successful project completion for both GL Solutions and clients.

Service Delivery Manager

GL Solutions – 2013 to 2022

- Led account management team.
- Responsible for individual development and all operational duties of account management team.
- Supervised the installation management and technical support for GL Solutions clients.

Project Coordinator Manager

GL Solutions – 2011 to 2013

- Led project coordination team.
- Responsible for individual development and all operational duties of project team.
- Provided installation management and technical project support for GL Solutions clients.

Business Analysis Manager

GL Solutions – 2010 to 2011

- Led business analysis team.
- Responsible for individual development and all operational duties of business analysis team.
- Provided technical support for GL Solutions clients.

Business Analyst

GL Solutions – 2008 to 2010

- Conducted process analysis for existing clients to enhance system efficiency.
- Worked with clients to analyze and address issues.
- Conducted requirements gathering and business process analysis for new installation clients.
- Designed and configured system screens and business rules for installation clients.
- Specified data conversions, interfaces and all forms or outputs for installation projects.

RFP Experience

Nevada State Contractors Board

- Managed the end-to-end installation, overseeing website development, back-office systems, and interfaces.

Connecticut Department of Safety and Emergency Services

- Led the team through user acceptance testing (UAT) and go-live phases, ensuring all system functionalities met agency requirements.

Virginia Department of Criminal Justice Services

- Directed the business analysis and project teams during installation, focusing on regulatory compliance and automated workflows.

New Mexico Environmental Department

- Supervised system installation and integration of diverse environmental compliance modules.

Idaho Board of Pharmacy

- As Agency Partner Manager, guided the client relationship, ensuring smooth system operation and user satisfaction during post-go-live phases.

Wyoming Board of Pharmacy

- Managed the system installation and data migration process, ensuring compliance with Wyoming's regulatory needs.

Wyoming Real Estate Commission

- Led project teams through system implementation, focusing on database management and licensing processes.

Arizona Board of Medicine

- Directed the integration of licensing systems, ensuring a seamless transition to the GL Suite platform during the installation phase.

Education

Associate of Applied Sciences in Business Administration: Accounting
Central Oregon Community College – Bend, Oregon

Software

GL Suite, MS Word, MS Excel, MS Visio, MS Publisher, MS Project, Adobe InDesign, QuickBooks



Anhelina Mykyta
Senior Business Analyst

mykyta@glsolutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Leads the Business Analyst team that gathers business requirements, creates business and technical specifications for WVBOM's-specific solution. Dedicates 75% of time to the project.

Work Experience

Business Analyst Manager

GL Solutions – 2023 to Present

- Leads a team of business analysts in developing and implementing business processes for various state agency projects, including Illinois Office of the State Fire Marshal and Illinois Department of Public Health.
- Designs and executes training programs for staff on new permitting software, ensuring seamless transitions and improved operational efficiency.
- Collaborates with stakeholders to build comprehensive business cases that align technology solutions with organizational goals.

Business Analysis Specialist

GL Solutions – 2022 to 2023

- Utilized systems analysis to enhance project outcomes, ensuring effective solutions for state agencies such as VADHHS, AKCCED, and ND Health and Human Services for Child Care Licensing.
- Translated client requirements into standardized specifications, documenting needs alongside technical specifications for clarity and compliance.
- Engaged in developing security requirement documents, providing comprehensive background checks to meet agency regulations.

Quality Assurance Specialist

GL Solutions – 2021 to 2022

- Documented software defects and collaborated closely with development teams to troubleshoot and resolve issues efficiently.
- Developed testing programs, including regression testing and usability testing, ensuring adherence to compliance standards and best practices.
- Executed thorough compatibility tests across various hardware and software environments, enhancing system performance and reliability.

RFP Experience

Wisconsin Department of Health

- Provides UAT walkthroughs for client stakeholders.

Illinois Office of the State Fire Marshal

- Developed business cases and trained staff for new permitting software, ensuring compliance and smooth implementation.

Illinois Department of Public Health

- Designed business processes for environmental and emergency medical services systems and led user training.

Connecticut Department of Social Services

- Oversaw the development of firearm permitting software, managing integrations and regulatory compliance.

Virginia Department of Behavioral Health & Developmental Services

- Gathered requirements, oversaw business process design, conversion and interface design, led UAT, and conducted training sessions.

New Mexico Children, Youth & Families Department

- Provided design guidance for business analysts, overseeing conversion and interface efforts.

Nevada State Contractors Board

- Oversaw business process designs, interfaces, and conversion efforts.

New Mexico Environment Department

- Directed business process and interface design.

North Dakota Real Estate Appraiser Qualifications and Ethics Board

- Led business process design, conversion, and interface development.

Nevada Housing Division

- Oversaw business process design and supported system conversion and interface deployment.

Education

Bachelor's Degree in Sociology and Law

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute,"

Software

SQL, HTML, CSS, TestRail, Jira

Methodologies: SDLC, STLC, Agile, Waterfall

Testing Techniques: Black Box Testing, Exploratory Testing, Regression Testing, Test Case Design



Ryan Pedersen

Technical Lead

pedersen@gl solutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Oversees the Strategy Department support of WVBOM'S-specific solution. Provides senior technical guidance on interface development, conversion design, and data architecture. Dedicates 30% of time to the project.

Work Experience

Vice President for Strategy

GL Solutions – 2022 to Present

- Leads, plans, and manages the Strategy Department.
- Ensures the Strategy Department produces work according to every subprocess within the department.



Development Manager

GL Solutions – 2010 to 2022

- Provided development management for GL Solutions clients.
- Managed team of software developers and configuration specialists responsible for the configuration and development of client software.

Software Developer

GL Solutions – 2009 to 2010

- Completed data conversions for more than 30 GL Solutions clients.
- Completed third-party interfaces for numerous GL Solutions clients.
- Developed expertise in SQL Server database architecture, implementation, data structures, and administration.
- Developed expertise in .NET software development, including VB.NET and Java-based applications.
- Developed expertise in Microsoft Windows Server and client operating systems.
- Developed and supported all aspects of GL Suite software.

Lead Developer

EDS Government Solutions – 2007 to 2009

- Participated in all aspects of development for VTDrives, a redesign of Vermont's DMV technology.
- Developed software using .NET 3.0 technologies, VB.NET, T-SQL, and XML.
- Planned and tracked tasks using scrum methodologies.
- Hosted classes on application framework and DevX UI development for new hires.
- Analyzed new requirements and planned integration with existing platform.
- Worked on UI design, client-server-database communication/integration using .NET 3.0 and WCF, business logic, internal and third-party interfaces, relational database design, SQL queries, performance testing/tuning, unit and end-to-end testing, data reporting, and framework design.

RFP Experience

Virginia Department of Behavioral Health & Developmental Services

- Led bi-directional data interface development and software updates, ensuring seamless integration with existing systems and processes.

North Dakota Department of Health & Human Services

- Managed software updates and integration, providing ongoing support for system authentication and functionality enhancements.

Arizona Board of Medicine

- Implemented bi-directional interfaces, performed system integration, and led website updates to ensure compliance with regulatory standards.

Education

BA in Computer Software Engineering/Minor in Business Management, Oregon Institute of Technology

Software

GL Suite Software (XML based), .NET Framework, C++, C#, VB, XML, XPath, XSLT, Ruby, SQL, T-SQL, MySQL, DevX, ASP, ASPX, HTML, Visual Studio 2kX, SQL Server Studio, Team Foundation Server, MS Visual Source Safe, Crystal Reports, MS Reporting, MS Office Suite



Nathan Sweat

Project Manager

sweat@glsolutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Leads project management efforts for WVBOM's-specific solution, overseeing project scope, schedule, risks, and client communication. Serves as the primary point of contact for project coordination and delivery. Dedicates 100% of time to the project.

Work Experience

Project Manager

GL Solutions – 2023 to Present

- Led project management efforts for complex regulatory licensing software implementation and Agency Transformation projects.
- Managed project lifecycle progress, risks, and issues, implementing corrective actions to meet project requirements, quality, schedule, and budget.
- Fostered strong client relationships with government agency partners, serving as a trusted advisor throughout all project phases.
- Provided leadership and facilitated team communication to ensure successful project completion.

Project Manager

Integrated Security Solutions – 2022 to 2023

- Managed proposal and contract operations, directing government and private contracts and deploying teams worldwide.

- Led multi-million-dollar projects from proposal through execution, exceeding timeline and budget goals.
- Applied agile methodology for project development, scheduling, and evaluation.
- Oversaw project deliverables, ensuring successful submission and implementation.

Service Line Director/Project Manager

Logan Healthcare System – 2014 to 2021

- Managed technical, administrative, and operational projects, including electronic medical record implementation and COVID-19 healthcare projects.
- Directed healthcare and IT projects, surpassing timeline and budget metrics.
- Developed project proposals, managed deployment, and ensured successful completion of project deliverables.

RFP Experience

Kansas Department of Health and Environment

- Current implementation project manager

Illinois Office of State Fire Marshal

- Current implementation project manager

Wisconsin Department of Health

- Current implementation project manager

Arizona Barbering & Cosmetology Board

- Led the Agency Transformation implementation

Education

Bachelor of Science in Health Care Management, **Southern Illinois University**

Master of Business Administration, **Syracuse University**

Master of Science in Project Management, **Liberty University**

Surface Warfare Medical Institute, Independent Duty Corpsman - NPI #1588908891



Lauren Vance

Training Lead

vance@glsolutions.com

541-312-3662

555 Corporate Drive, Kalispell, Mont.

Project Responsibilities

Leads analysis and training for WVBOM's-specific solution, including business requirements gathering, technical specification development, and training program delivery. Translates clients' training needs into quantifiable training outputs. Dedicates 75% of time to the project.

Related Experience

Senior Business Analyst | Training Lead

GL Solutions – 2023 to Present

- Analyzed client needs to create designs that adhere to company best practices, ensuring alignment with technical requirements.
- Communicates effectively with clients in non-technical language, translating their needs into technical documentation and designs.
- Designs and modifies technical specifications for reports, queries, correspondences, emails, data rules, and interfaces.
- Creates unit and system test plans to validate functionality and performance of software solutions.

Business Analyst

GL Solutions – 2022 to 2023

- Collaborated with state agencies including VADBHDS and Arkansas Board of Pharmacy, ensuring successful implementation of solutions that meet regulatory requirements.
- Facilitated discussions with stakeholders to identify needs and translate them into actionable technical specifications.
- Engaged in quality assurance processes, contributing to the development of security requirement documents and maintaining compliance with agency regulations.

Seasonal Data Processor

Wildfire Defense Systems – 2021 to 2022

- Quality-checked shift tickets and approved time and expenses, streamlining the operational workflow.
- Developed Python programs that automated data processing tasks, saving the department significant time and improving accuracy in quality checks.
- Assembled and cleaned data from multiple sources to support product development and inform decision-making across departments

Experience

Illinois Department of Public Health – Environmental and Emergency Medical Services

- Analyzed and designed business processes, enhanced system functionality and user training.

Illinois Office of the State Fire Marshal

- Developed and implemented training materials for new software solutions, ensuring compliance with state regulations.

Kansas Department of Health and Environment

- Collaborated on system integration, creating documentation that facilitated seamless transitions.

Virginia Department of Behavioral Health and Developmental Services

- Translated client requirements into technical designs, improving service delivery and regulatory compliance.

Arizona Board of Medicine

- Supported data management initiatives, contributing to efficient workflow and quality assurance processes.

North Dakota Department of Health and Human Services

- Developed training programs for staff on new licensing systems, enhancing operational effectiveness.

Education

Bachelor of Science in Applied Mathematics, Montana State University

Major in Computer Science, Flathead Valley Community College – Kalispell, Montana

Technical Skills

Languages: Python, Java, SQL

Tools: Microsoft Excel, Pandas, SharePoint, Microsoft Teams, Google Colab

Data Analysis: Machine Learning, Data Cleaning, Quality Assurance

Relevant Project Experience

GL Solutions meets and exceeds all requirements for relevant experience, including:

- Deployment of licensing and regulatory systems within the last three years.
- A minimum of three years of support and maintenance.
- Successful data migration from legacy systems.
- Full ownership and authorization of GL Suite, the proposed software.

*Project Reference #1: Wisconsin Department of Health Services – Division of Quality Assurance (DQA)***Project Description:**

GL Solutions implemented GL Suite to consolidate licensing and enforcement for over 40 regulatory programs. The system streamlined inspections, automated high-volume renewals, and supported inter-agency coordination and background check processing.

Responsibilities and Outcomes:

- Delivered licensing, inspections, complaints, and enforcement configuration.
- Migrated legacy data and implemented 35+ external interfaces.
- Deployed GL Suite to support 176 license types and 14,000 providers.
- Enabled automated enforcement and real-time public data sharing.
- Managed milestone-based planning and steering committee oversight.
- Completed project within scope despite high complexity and interface volume.

Notable Constraints Addressed:

Extensive inspection requirements, short deployment timeline, and complex multi-program integration. GL Suite's flexibility allowed tailored workflows without custom development.

Project Reference #2: Office of the Illinois State Fire Marshal (OSFM)

Project Description:

GL Solutions implemented a unified licensing and inspection system across three divisions. The platform replaced fragmented legacy processes with mobile inspection forms, online renewals, and public transparency tools.

Responsibilities and Outcomes:

- Configured licensing, inspection, and renewal workflows across divisions.
- Delivered over 30 license types and supported 10,000+ annual inspections.
- Integrated with Illinois ePay and document management systems.
- Managed dynamic form development and multi-agency compliance tracking.
- Project completed with full scope and functionality.

Notable Constraints Addressed:

Cross-divisional statutory differences, ongoing rule changes, and complex inspection variants. GL Suite accommodated these with configuration alone, avoiding delays or rework.

Project Reference #3: Arkansas State Board of Pharmacy

Project Description:

GL Suite replaced the board's legacy licensing and enforcement system, enabling secure online applications, complaint submissions, and real-time verification.

Responsibilities and Outcomes:

- Delivered licensing and complaint workflows for 20+ license types.
- Migrated legacy data with zero downtime or loss.
- Integrated with payment processors and laid groundwork for digital license cards.
- Delivered on schedule, aligned with licensing renewal cycles.

Notable Constraints Addressed:

Strict deadlines, data integrity requirements, and phased Go-Live timing. GL Solutions ensured continuity while completing early UAT and fallback planning.

Project Reference #4: Alabama Board of Cosmetology

Project Description:

This engagement transitioned the Board from a legacy report database to GL Suite 7, supporting renewals, payments, inspections, and CE tracking.

Responsibilities and Outcomes:

- Full migration from a discontinued system.
- Configured workflows for 20+ license types and enabled public portal access.
- Delivered renewal automation and internal reporting tools.
- Achieved deployment with no data loss or workflow disruption.

Notable Constraints Addressed:

Complex renewal logic and legacy data limitations. The project succeeded without requiring system customization, demonstrating GL Suite's adaptability.

Exceeding Mandatory Qualification/Experience Requirements

Value-Added Services

GL Solutions will deliver value beyond WVBOM's mandatory requirements, providing tools and capabilities that improve efficiency, enhance transparency, and support modernized service. Our work with the [West Virginia Alcohol Beverage Control Commission](#), the [Arizona Board of Medicine](#), and the [Wyoming Board of Medicine](#) demonstrates our ability to deliver these advanced capabilities in diverse regulatory environments, ensuring proven value and familiarity with both state-level compliance and board-specific operational challenges.

Website Creation, Hosting, and Domain Support

GL Solutions can create, host, and maintain secure, ADA-compliant public websites and portals on behalf of WVBOM. This includes domain management, SSL certificates, and ongoing updates to ensure consistent branding, accessibility, and regulatory alignment.

A key differentiator is GL Suite's Configurable Web, which enables WVBOM to maintain accuracy, consistency, and efficiency across all public-facing forms and workflows. Rather than relying on static web pages, Configurable Web allows logic, questions, and rules to be updated once and automatically applied across all relevant forms. This ensures that renewal processes, attestation questions, and other online interactions remain consistent, accurate, and aligned with policy changes—without introducing duplication or risk of error.

All public-facing components are designed in compliance with WCAG 2.1 AA, Section 508, and ADA requirements, ensuring accessibility for all users.

Enhanced Data Migration Capabilities

Our migration tools exceed industry standards by validating, cleansing, and reconciling data during migration. This ensures accuracy while minimizing disruption and maintaining full historical records from legacy systems.

Extended Document Retention Options

GL Suite supports configurable retention rules, long-term secure archiving, and automatic destruction protocols aligned with state statutes and FOIA requirements. Agencies retain control over retention schedules and compliance safeguards.

Custom Form, Report, and Workflow Builders (No Code)

WVBOM staff can independently create and modify forms, dashboards, reports, and workflows using GL Suite's intuitive, no-code tools. This reduces reliance on vendor support and empowers staff to adapt processes quickly as policies change.

Board Meeting Management

GL Suite simplifies and enhances the entire lifecycle of Board Meeting Management through a fully integrated, user-friendly business process. This functionality enables WVBOM to efficiently plan, conduct, and document board meetings while maintaining compliance with retention policies and public transparency requirements.

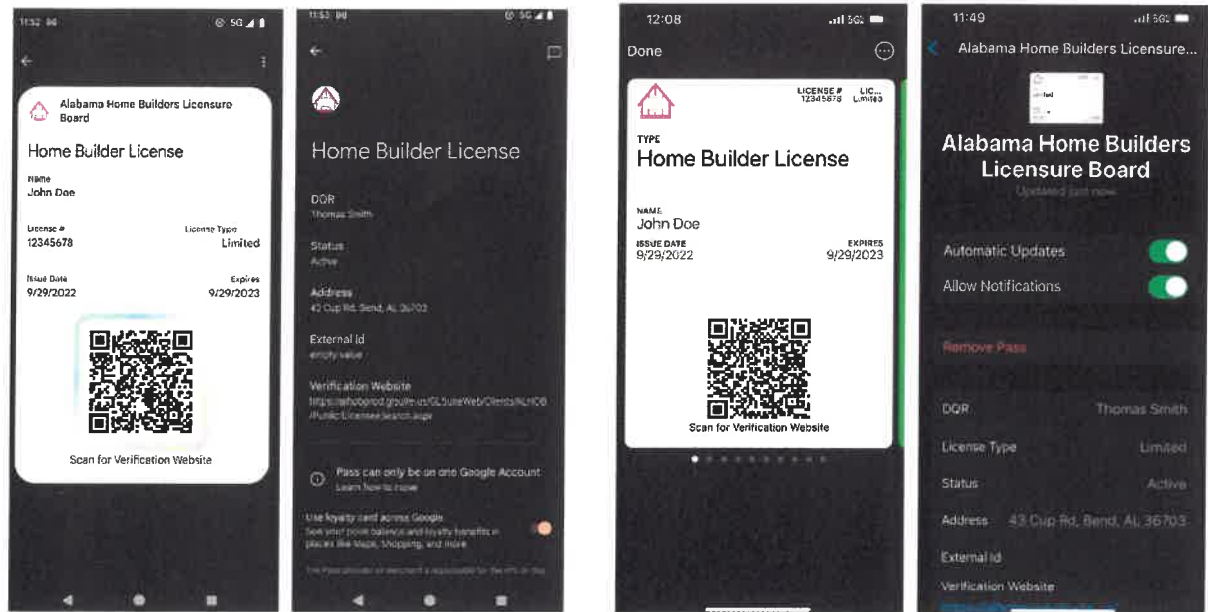
Key Features:

- **Meeting Scheduling and Management:** Easily schedule meetings with full control over dates, locations, and detailed agenda planning.
- **Agenda Creation and Organization:** Create, reorder, and update agenda items flexibly, associating each item with related records such as license applications for seamless data linkage.
- **Participant Assignment:** Assign presenters, witnesses, respondents, and other participants directly to agenda items to coordinate involvement effectively.
- **Dynamic Board Meeting Manager:** Staff can generate and modify agendas in real time, with live access to associated documents for both internal users and board members.
- **Public Access and Offline Review:** Publish agendas as downloadable PDFs online for public transparency, with options for offline document export to facilitate board member preparation.
- **Real-Time Meeting Support:** During meetings, update agenda statuses, add notes, and enable internal communication to keep proceedings organized and on track.
- **Automated Minutes Generation:** Automatically create meeting minutes from agendas and notes entered, ensuring accuracy and saving administrative time.
- **Post-Meeting Follow-Up:** Track and manage action items arising from meetings efficiently.
- **Secure History and Compliance:** Maintain a complete, secure archive of board meeting records to satisfy information retention policies and FOIA requirements.

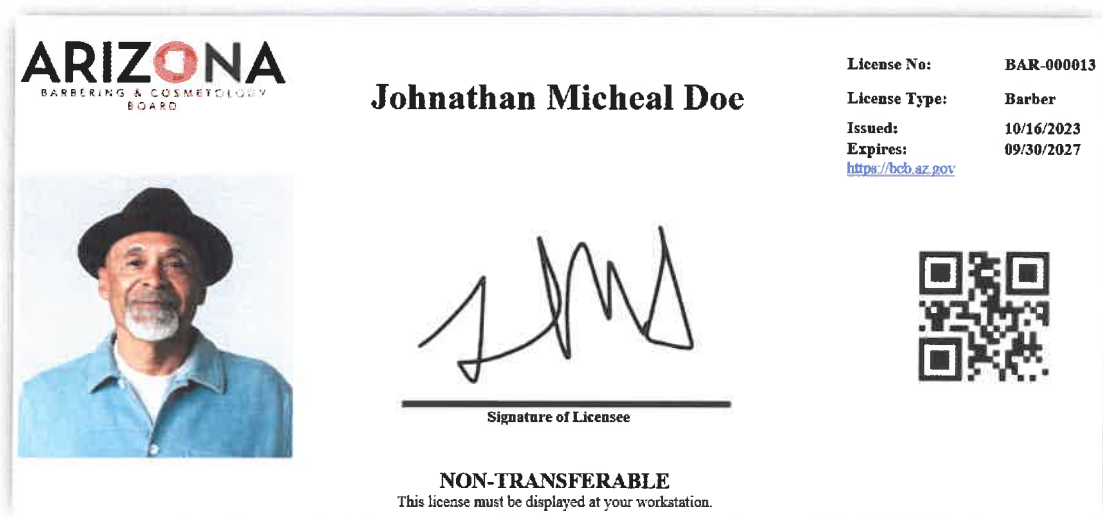
QR Codes, Digital Wallets and Certificates

GL Suite simplifies document printing and management for items like Wallet Cards, Wall Certificates and Licenses. The ability for licensees to print from the self-service portal will reduce the workload for staff. If WVBOM desires to manage distribution, documents like certificates, badges and licenses can be printed and mailed individually or in batches, either manually or automatically.

GL Suite also supports paperless offices by enabling digital wallet cards for licenses, which can be added to Apple Wallet or Google Wallet. These digital cards display critical license information and include QR codes that link to the agency's license verification website. The cards automatically expire upon license expiration and can be resent at any time, either individually or in bulk. In addition, to prevent falsification and limit unauthorized downloads, each downloaded certificate automatically voids the previous version.



Screenshots of Digital Wallet IDs developed for Alabama's Builders Licensure Board, both for iOS and Android respectively.



Example of a standard Certificate with photo and QR Code developed for Arizona.



GL Solutions thanks the West Virginia Board of Medicine for the opportunity to submit this proposal for the Medical Licensure / Records Database Maintenance System (**CRFP 0945 BOM2600000001**). We value the chance to share information about our SaaS solution, GL Suite, and our 25 years of experience supporting state regulatory boards. We respectfully submit this proposal for your review and consideration.






CRFP 0945 BOM2600000001_Technical Response_GL Solutions

Final Audit Report

2025-12-03

Created:	2025-12-03
By:	Steve Matzker (matzker@glsolutions.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAArJVadwuACOCheWnCJEtgwgK1RHyg1cCu

"CRFP 0945 BOM2600000001_Technical Response_GL Solutions" History

-  Document created by Steve Matzker (matzker@glsolutions.com)
2025-12-03 - 5:40:52 PM GMT
-  Document emailed to William Moseley (moseley@glsolutions.com) for signature
2025-12-03 - 5:41:06 PM GMT
-  Email viewed by William Moseley (moseley@glsolutions.com)
2025-12-03 - 6:06:01 PM GMT
-  Document e-signed by William Moseley (moseley@glsolutions.com)
Signature Date: 2025-12-03 - 6:06:46 PM GMT - Time Source: server
-  Agreement completed.
2025-12-03 - 6:06:46 PM GMT



Adobe Acrobat Sign

Attachment 1: Disaster Recovery Plan

Objectives & Policies

The principal objective of GL Solutions' disaster recovery program is to develop, test, and document a well-structured and easily understood plan to help GL Solutions recover from a disaster or emergency that interrupts information systems and business operations as quickly and effectively as possible. Additional objectives include the following:

- Ensuring that all employees fully understand their duties in executing the DRP
- Ensuring that operational policies are adhered to within all planned activities
- Ensuring that proposed contingency arrangements are cost-effective
- Considering how our customers' activities will be affected
- Determining disaster recovery capabilities with respect to key customers, vendors, and others

Plan Modifications

Updates to the DRP will follow GL Solutions' customary procedures for policy updates, which include provisions for document control, versioning, training, implementation, and stakeholder input. The Administration Manager is the policy owner and will employ the expertise and advice of the Systems Administrator and external consultants in the ongoing development of the DRP. Suggested DRP modifications must be fully tested in a simulated environment before the change is formally adopted.

Executive Summary

GL Solutions' strategy is to have a disaster recovery plan in place, to return to normal after the disaster has struck as soon as possible. For an agency, a disaster means abrupt disruption of all or part of its business operations, which may directly result in revenue loss.

Every business disaster has one or more causes and effects. The causes can be natural or human or mechanical in origin, ranging from events such as a tiny hardware or software component's malfunctioning to universally recognized events such as earthquakes, fire, and flood. Effects of disasters range from small interruptions to total business shutdown for days or months, even fatal damage to the business.

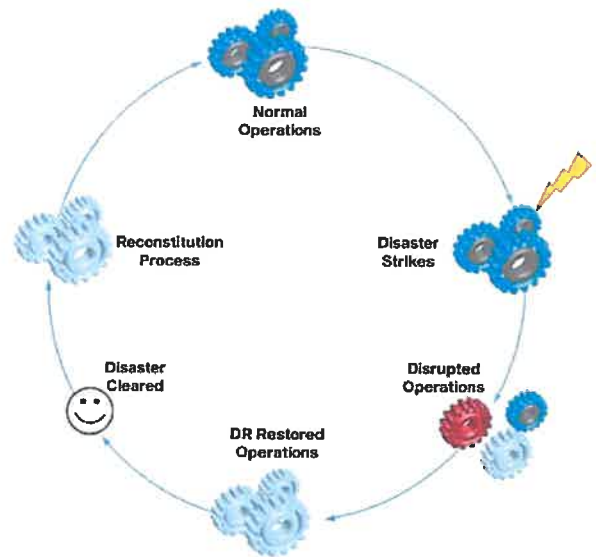
The process of preparing a disaster recovery plan begins with GL Solutions working with our client to identify these causes and effects, analyzing their likelihood and severity, and ranking them in terms of their business priority. The ultimate results are a formal assessment of risk, a disaster recovery plan that includes all available recovery mechanisms, and a formalized Disaster Recovery team that has responsibility for rehearsing, carrying out, and improving the disaster recovery plan.

When a disaster strikes, the normal operations of the enterprise are suspended and replaced with operations spelled out in the disaster recovery plan. Figure 1 depicts the cycle of stages that lead through a disaster back to a state of

normalcy.

It takes time to assess the exact effects of the disaster. Only when these are assessed, and the affected systems are identified can a recovery process begin. The disaster recovery system cannot replace the normal working system forever, but only supports it for a short period of time. At the earliest possible time, the disaster recovery process must be decommissioned and the business should return to normalcy.

The disaster recovery plan does not stop at defining the resources or processes that need to be in place to recover from a disaster. The plan should also define how to restore operations to a normal state once the disaster's effects are mitigated. Finally, ongoing procedures for testing and improving the effectiveness of the disaster recovery system are part of a good disaster recovery plan.



In summary, GL Solutions works with the client to define a disaster recovery plan that (1) identifies and classifies the threats/risks that may lead to disasters, (2) defines the resources and processes that ensure business continuity during the disaster, and (3) defines the reconstitution mechanism to get the business back to normal from the disaster recovery state, after the effects of the disaster are mitigated.

Plan Documentation Storage

Each member of the Emergency Recovery Team (see below) will be issued a CD and hardcopy of the DRP. A master protected copy will be stored on GL Solutions' intranet. Copies of this Plan—CD and hardcopy—will be stored in at least the following secure locations:

- Encrypted portable media distributed to all DR participants
- Intranet Site on Microsoft Azure

DRP Activation

GL Solutions provides for both automated and human initiated activation of the DRP execution.

System Component Alerts

Most GL Solutions system components provide automated internal error sensors. When an error occurs, the system component automatically sends an email to a specified external email address. Upon receipt of the email, a service calls GL Solution's initial responders and escalated responders if there is no response.

The system component alert activates the DRP execution in response to moderately severe, single system component failures which do not destroy the system component's ability to generate alerts. Examples include:

- Server system events such as loss of connectivity to a storage.
- Scheduled job failures
- High priority tasks raised by staff in LOKI

The system component activation includes system components, namely the IDPS and firewall, which monitors for suspicious security activity.

Health Monitor

GL Solutions utilizes an external health monitor application that calls an API at GL Solution's hosting facility every two minutes. The API returns end-to-end system component health data for all system components that support GL Solutions' client software. If the health status is critical, the system initiates a service that calls GL Solution's initial responders and escalated responders if there is no response.

Emergency Hotline

GL Solutions utilizes an external, redundant phone system which supports an emergency support extension. Call: (971) 337-2660. If there is no immediate response, call (503) 449-0898.

When called, the phone system calls GL Solution's initial responders and escalated responders if there is no response.

The emergency hotline may be activated by:

- Client experiencing an outage
- GL Solutions employees observing an event
- Hosting facility personnel, who continuously monitor the facility for environmental events
- Emergency responders and vendors alerted to event such as a fire

Event Classifications

GL Solutions' DRP recognizes and prescribes responses to events based on the expected duration and magnitude of the business interruption. We distinguish and categorize events as either Singular or Major Incidents. Singular Incidents are events with a short-term impact on a single system or client. Major Incidents are events that affect multiple systems or clients and those of a longer duration. The DRP attends to both event types.

GL Solutions maintains an Information Systems Catalog which includes content for predetermined mitigation steps for previous and likely events.

Singular Incident Events

Singular Incident events involve a service or business interruption for a single client or a single company application for a limited duration (typically less than 4 hours). Examples of such events include:

- Single production web or database server hardware failure
- Software defect causing a production outage for a single client
- Single company-used application outage
- DNS interruption for a single client
- SSL certificate errors

Response to Singular Incidents

If a Singular Incident event occurs, GL Solutions technical staff will receive notice of a Singular Incident by email, text and/or IP-based phone system. The phone system is programmed to alert 10 key staff in a predetermined order of escalation until the call is answered. The phone system is tested monthly to ensure that the escalation occurs as programmed and that staff respond appropriately.

In the event of a Singular Incident, the phone system will call staff repeatedly in the following order until it successfully delivers notice that an event has occurred:

- On-call Operations developers
- Off-duty Operations developers
- Development Manager
- Systems Administrator
- VP for Operations
- VP for Business Solutions
- CEO

Most Singular Incident events are correctable through hardware configuration or software defect corrections. During a Singular Incident, our goal is to restore service in the fastest possible time and to diagnose event causes for use in future remediation planning.

Process flow for Singular Incident Responses (IT Service Request and System Events)



Major Incident Events (Disasters)

Major Incident events 1) affect multiple clients or company-used services or 2) involve outages for periods longer than 8 hours. Numerous events can potentially disrupt the normal business processes of GL Solutions and/or our clients at any time. GL Solutions plans, mitigates and practices major incident responses at least annual for identified potential major incidents based upon the probability of occurring, an impact rating, and the potential consequences. Preventative actions are addressed when appropriate through that risk assessment process. The focus here is on the level of business disruption that could arise from each type of disaster.

Response to Major Incidents

GL Solutions has identified an Emergency Recovery Team (ERT) that has been charged to act in the event of a major incident. The ERT is responsible for activating the Disaster Recovery Plan and orchestrating and documenting all recovery events. The team is responsible for activating the DRP for all disasters identified in the DRP and for any other event affecting GL Solutions' ability to maintain normal operations. The team will assesses GL Solutions' response and recovery after business has returned to normal to ensure that all disaster related activities are optimal.

GL Solutions' Major Incident disaster response relies principally on key members of management, who will provide the technical and managerial skills necessary to achieve a smooth recovery of technology and business operations. ERT members include:

- Administration VP
- CEO
- Strategy VP
- Operations VP
- Product Development Manager
- Product Manager
- System Administrator
- Business Solutions VP
- IT Support Specialist
- AMR Coordinator

GL Solutions responds to Major Incidents as follows:

1. In case of emergency (fire, flood, tornado, act of sabotage), dial 911.
2. Notify Emergency Response Team. All GL Solutions employees are issued a Quick Reference card containing ERT contact details to use in the event of a disaster.

Upon activation of the DRP and determination that the event exceeds the scope of a Singular Incident (IT Service Request or System Event) the ERT receives a phone or text notification. The notification system simultaneously calls all ERT members until notification of the event is successfully delivered.

The notification will advise ERT members to assemble virtually or at a safe location. The team may contact and utilize additional employees, responders, and/or vendors as needed to respond to the incident.

In the event of a Major Incident, the ERT will act to accomplish the following goals, listed in order of priority:

- Protect the health and safety of employees
- Minimize the risk of loss to customer data
- Coordinate activities within the ERT and with first responders, etc.
- Establish facilities for an emergency level of service within 2 business hours of the incident
- Restore key services within 4 business hours of the incident
- Recover client systems to functional state within 8 to 24 hours after the incident
- Recover to business as usual within 8 to 24 hours after the incident
- Minimize the risk of legal, financial, and other consequences on the company

The ERT will respond to Major Incidents in the following manner:

1. Respond immediately to a potential disaster and call emergency services if not already contacted
2. Call ERT to action to maintain vital services and restore normal operations
3. Gather Information to determine the extent of the disaster and its impact on employees, the business, clients, the data center, etc. using the *Damage Assessment Form*
4. Utilize *Appendix A – Disaster Recovery by System* to determine which elements of the DRP should be activated
5. Determine additional or alternate actions required by the circumstances (detailed below)
6. Document the activities to be undertaken, and log all activities in the *Event Log*
7. Ensure that employees are notified, allocate responsibilities and activities as required, and record in the *Management of DR Activities Form*
8. Monitor DRP activity to completion in the *Progress Monitoring Form*
9. Assess recovery of each business process utilizing the *Business Recovery Report*
10. Resume normal operations once the *Business Recovery Report* describes all systems as functional
11. Assess disaster response using the *Disaster Recovery Report*

During the disaster recovery process, all activities will adhere to the processes detailed in *Appendix A – Disaster Recovery by System* for each potential type of incident. In addition to the system response activities detailed in *Appendix A*, the ERT may need to take other actions such as those described below.

Gather Information

The IT Support Specialist or whoever receives the initial event report immediately conducts the following steps:

1. Gather information which enables you to determine the potential scope of the issue.
 - a. Is there a facility problem? Does the problem require emergency responders? Have they been contacted?
 - b. Is there an event at the data center? Are employees able to access systems remotely? Are clients able to access hosted applications?
 - c. Are employees exposed to physical risk? How do you know? What is the nature of the risk? Environmental condition? Contagion?
 - d. What other external or internal parties are aware of the event?
 - e. When did the event begin?
2. If the event involves a situation requiring emergency responders, dial 911.
3. Correlate the event to one or more system event plans. See: How To: [System Component Event](#)
4. If the event appears correlated to a single system event, escalate to the system event leader, e.g. the System Administrator
5. Alternately, escalate to the disaster event leader if any of the following are true:
 - a. the event is indeterminate or uncorrelated to a system event
 - b. multiple system events apply,
 - c. there is a risk to the health of employees
 - d. there is a significant risk to company property, or
 - e. the event risks violating our recovery point or recovery time goals.

The remainder of this disaster plan applies only to disaster events, not single system events. The Administration\Infrastructure\Network Administration\System Events subprocess responds to system events.

DRP Remediation Actions

Urgent Actions

Assembly Points

In the event that the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

Primary – *Deleted from document to protect sensitive information
Alternate – *Deleted from document to protect sensitive information

Staffing

Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

Returning Recovered Business Operations to Business Unit Leadership

Once normal business operations have been restored, responsibility for specific operations will need to be returned to the appropriate business unit leader. This process should be formalized to ensure that all parties understand the change in responsibility and the transition to business-as-usual.

Communications

During emergency recovery, affected persons and organizations must be kept up-to-date and informed. The information provided to involved parties must be accurate and timely. In particular, any estimate of the timing for a return to normal operations should be announced with care. It is also vital that only authorized personnel deal with media queries. The ERT will assign a media representative to be responsible for all communications activities. S/he will track all such interactions on the *Communications Form*.

Recorded Messages/Updates

Clients and staff members will be notified with the latest information on the disaster and GL Solutions' response via our phone system. The system will call each staff member and leave a recorded message about the nature of the disaster, assembly sites, and updates on work resumption. An "All Employee" disaster update and an "All Client" disaster update have been set up for this purpose.

Contact with Employees

When communication with employees other than the ERT is required, ERT members will contact managers, who will serve as focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and GL Solutions' immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information about the disaster.

Personnel and Family Notification

If the incident has resulted in a situation that would cause concern to an employee's immediate family, such as hospitalization of injured persons, they must be notified as quickly as possible. When feasible, an ERT team member will notify the family by phone. When phone contact is not possible, the ERT team member will leave messages and await contact by the family.

Media Contact

The ERT leader will assign a representative to coordinate with the media, working according to previously approved guidelines for dealing with post-disaster communications. Only the media representative is permitted direct contact with the media. Anyone else contacted should refer callers or in-person members of the media to the media representative. Objectives for media contact include:

- Do not interfere with emergency responders
- Avoid adverse publicity for the company and clients
- Answer only essential questions about incident and response activities

Facilities

Alternate Collocation Facilities

In the event of a disaster that affects the collocation facility, GL Solutions will restore data from backups to standby equipment already established at a different location. The equipment will then be moved to a designated substitute collocation facility.

Alternate Work Facilities

In the event of a disaster affecting the GL Solutions office, the company will resume operations via VPN and remote connections until a permanent solution can be identified. The ERT will assemble at the office and then choose an alternate temporary Hot Site location for managing the disaster. Notification will be delivered via recorded messages or communications with managers. Hot Site staffing will consist of members of the ERT only for the first 24 hours with other staff members joining at the Hot Site as necessary.

Data Protecting and Backup

Key business processes and the backup strategy for each process are listed below. The strategy entails a Warm Recovery at a specified location and plans to implement a full recovery Hot Site in the future. This plan involves maintenance of a Warm Recovery site that will enable complete backup restores from two separate locations.

*Details of this section have been removed to protect sensitive information.

Financial and Legal Resources

Financial Assessment

The ERT will prepare an initial assessment of the incident and its impact on GL Solutions' financial affairs. The assessment will consider:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.

- Loss of cash
- Cost of replacement equipment, furniture, etc.

GL Solutions' immediate financial needs must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

Insurance

A number of insurance policies have been put in place as part of GL Solutions' disaster recovery and business continuity strategies. These include Errors and Omissions, Directors & Officers Liability, General Liability, and Business Interruption Insurance.

*Details of this section have been removed to protect sensitive information.

Legal Actions

The ERT may contact GL Solutions' legal counsel to review and discuss legal requirements and recommendations for mitigating the liabilities associated with an incident.

Disaster Recovery Forms

DAMAGE ASSESSMENT FORM: The ERT leader will document the impact of the disaster within the *Damage Assessment Form*. Information detailed in the form includes:

- Key business process affected
- Description of problem
- Extent of damage

MANAGEMENT OF DR ACTIVITIES FORM: The ERT leader will use the *Management of DR Activities Form* to track and manage all activities involved in a disaster. The form includes the following information:

- Recovery Activity
- Commencement date/time
- Completion date/time
- Resources involved
- Person in charge

EVENT LOG: The ERT leader will maintain a log of all key events that occur during disaster recovery. The ERT will initiate the *Event Log* at the start of an emergency. The log details the following information:

- Actions taken by ERT
- Date/Time of activity

- Outcome of activity
- Follow-up action required

COMMUNICATIONS FORM: The *Communications Form* provides a place for the ERT leader and other team members to track all communication activities associated with the event. It includes the following information:

- Group affected (e.g. Customers, Management & Staff, Suppliers, Media, Stakeholders)
- Contact information
- Contact details

PROGRESS MONITORING FORM: The progress of technology and business recovery tasks will be closely monitored using the *Progress Monitoring Form*. Since difficulties experienced by one group could significantly affect other dependent tasks, it is important that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated.

DISASTER RECOVERY REPORT: On completion of the initial disaster recovery response, the ERT leader will prepare a *Disaster Recovery Report* describing the activities undertaken in response to the disaster. The *Disaster Recovery Report* includes:

- A description of the emergency or incident
- Those notified of the emergency (including dates)
- Action taken by members of the ERT
- Outcomes arising from actions taken
- An assessment of the impact on normal business operations
- Assessment of the effectiveness of the DRP
- Lessons learned

BUSINESS RECOVERY REPORT: The ERT leader will maintain a *Business Recovery Report* to document the activities undertaken and completed for each disrupted business process and to mark the completion of each recovered business process. The *Business Recovery Report* includes:

- A description of the incident
- People notified of the emergency (including dates)
- Actions taken by the ERT
- Outcomes arising from actions taken
- An assessment of the impact on normal business operations
- Status of disrupted business process
- Identification of any issues identified in the disaster recovery process
- Suggestions for enhancing the disaster recovery and/or business continuity plan
- Lessons learned

DRP Exercises

Disaster Recovery Plan exercises are an essential part of the plan development process. When

disasters occur, successful DRPs launch smoothly and effectively. This can only happen when everyone with a role to play in the plan has rehearsed disaster scenarios at least once. Exercising the DRP ensures that members of the ERT are familiar with their assignments and, more importantly, confident in their capabilities. Moreover, DRP exercises help team members identify what elements of the DRP need improvement and how improvements can be achieved.

Testing

GL Solutions requires the Systems Administrator to exercise all plans documented in *Appendix A – Disaster Recovery by System* at least once a year. As plan defects surface, modifications will be made to the plan.

Backup & Recovery

The GL Suite application creates primary and remote backup data to achieve designated recovery point and recovery time objectives. The backup process encompasses data stored in every location in the system, including: Transactional Data, Report Data, Document Repository, Correspondence Templates, Reports, Persisted Customizations, Automated Database Jobs, Interface Applications, Files.

Moreover, GL Solutions maintains a secure, offsite backup repository. We backup data to this facility to meet recovery time and recovery point objectives in the event that the primary backup is unavailable. Daily monitoring of jobs and tasks to confirm restorability ensures continuous protection of data from unnecessary loss. GL Solutions relies upon Azure redundant, replacement failover equipment to monitor and minimize downtime caused by any hardware failure. In the event of a disaster or hardware failure, data can be recovered within minutes.

Your data is safeguarded in an environment that minimizes the risk of irretrievable loss of data and/or configuration settings. The following are GL Solutions' most common strategies for data protection:

- Replication of data to a secondary location.
- High availability systems keep the data and the system replicated, enabling continuous access to systems and data.
- Wide Area Network Optimization technology improves disaster recovery capabilities and increases network response times. This technology also ensures that data continues to move through the network even when it is down.
- Enterprise-level backup, colocation and cloud computing solutions.
- Complete disaster recovery plan to ensure your IT infrastructure will stay up and running during virtually any disaster.

Disaster Recovery Environment

GL Solutions incorporates commercial Azure hosting as part of its disaster recovery plan to ensure high availability and data protection. Azure regions are designed to offer protection against local disasters with availability zones, providing organizations with both high availability and protection from large- scale phenomena and regional disasters.

GL Solutions leverages Azure's cross- region replication feature, which asynchronously replicates applications and data across multiple Azure regions for disaster recovery protection. This replication strategy helps ensure business continuity and protects against data loss. Azure's storage solutions, such as georedundant storage (GRS), automatically replicate data to a secondary region, further enhancing data availability.

The secondary back location is the Azure US East region.

By hosting GL Suite on secure Microsoft Azure servers, GL Solutions benefits from Azure's high compliance offerings, including FedRamp. GL Solutions is also AZRamp certified, further enhancing the security and integrity of the hosted client environments. Azure's infrastructure maintenance, patch management, malware protection, system monitoring, and backup and retention services contribute to the overall reliability and resilience of the hosting environment.

United States

Azure Data Center Region	Location
Central US	Iowa
East US	Virginia
East US 2	Virginia
North Central US	Illinois
South Central US	Texas
West US	California
West US 2	Washington
West Central US	Wyoming

Attachment 2: Incident Response Plan

An Incident Response Plan (IRP) is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. The Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team (IRT) is responsible for putting the plan into action throughout the preparation, detection and analysis, containment, eradication, and recovery of an incident.

This IRP applies to all information system components and all information held by the company. This Incident Response Plan outlines steps GL Solutions will take upon discovery of unauthorized access to Confidential or PII information that could result in harm or inconvenience to the entity such as fraud or identity theft. The entity could be a customer, data stored on behalf of a customer or for GL Solutions, or an employee of GL Solutions.

If an incident has resulted, or will result in downtime, it must be coordinated with the Information System Contingency Plan to determine a logical approach and define objectives for system recovery.

The Incident Response Plan itself is modifiable by the Active Directory groups. For a revision to be permissible, it must be versioned appropriately with accurate descriptions and compliant with GovRAMP Revision 5 and NIST SP 800-34.

The incident response procedure is annually reviewed, tested, and revised to address issues encountered, lessons learned, brought up to date with current system and environment changes, and updated to gain compliance with modifications or additions to the security standards GL Solutions utilizes. An email notification will be sent to relevant staff detailing the IRP change and providing the revision description.

This IRP does not include customer responsibilities, as listed below:

- Safeguarding of account access (Usernames and password)
- Violations of Acceptable Use Policy (AUP) and Rules of Behavior (ROB) impacting customer data

High-Level Incident Response Approach

The incident response process begins when an event is raised, either automatically or manually. The event is routed to the IT Support Specialist or Chief Administrative Officer, who assesses whether notification is necessary after gaining approval from the legal contact. The event is then classified and assigned a severity level. The IT Support Specialist or Chief Administrative Officer escalates the event to the CSO, who activates the Incident Response Team (IRT). If the incident is expected to cause an outage, recovery objectives will be defined according to the Information System Contingency Plan. During the response and resolution phases, the Incident Response Plan (IRP) will be completed with relevant details. Following resolution, the After-Action Report Template will be filled out, and lessons learned will be documented to inform future processes and training.

Raising An Event

If you are the first person that became aware of the potential incident, complete this form and create a P1/HP Net Admin-System Event task. Handoff the task to the IT Support Specialist or in their absence, the Chief Administrative Officer, for event classification.

How and when did you learn of the incident? Paste in any supporting notification information (e.g. email)
Provide Contact Information for Impacted Third Parties (Name, cell phone, email, etc.)
Describe the Incident Paste screen shots if you have them.
What Information Suggests an Incident? Do you have any evidence about the nature of PII or confidential data loss?
Any other information?

Create a P1/HP Net Admin-System Event task.
Handoff the task to the Chief Security Officer (CEO)
Or Call (541) 312-3662 option 8.

When Notification Is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.
- An unauthorized party has broken into database(s) that contain Confidential or PII information.
- Computer equipment such as a workstation, portable device, portable storage, or other electronic media containing data has been lost or stolen.
- A department or unit has not properly disposed of records containing data.
- A third-party service provider has experienced any of the incidents above, affecting the organization's data stored with GL Solutions.

The following incidents may not require individual notification under contractual commitments or applicable laws and regulations, provided GL Solutions can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected entities:

- GL Solutions is able to retrieve Confidential or PII information of an entity that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.
- The organization determines that Confidential or PII information of an entity was improperly disposed of but can establish that the information was not retrieved or used before it was properly destroyed.
- An unauthorized party accessed files that contain only information classified as Public – for example, names and addresses of licensees otherwise available for public use.

A portable device is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device.

Employee and Customer Responsibilities

Employees who come in contact with customers with a vested interest in Confidential/PII information play an active role in the discovery and reporting of any breach or suspected breach of data.

All employees and customers must report any suspected or confirmed breach of Confidential/PII information to the CSO immediately upon discovery. This includes notification received from any third-party service providers or other business partners with whom the organization shares Confidential/PII information. The CSO will notify the Chief Privacy Officer (CPO) and data owners whenever a breach or suspected breach of information affects their business area.

Note: For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, the IT Support Specialist, contacted via the emergency support line, will act as a central point of contact for reaching the CSO and CPO.

The CSO will determine whether the event warrants investigation as a possible incident full incident response plan activation (See “Incident Response” section.) The data owner will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the CPO, CSO, Legal or other Incident Response Team members throughout the investigation.

Good faith acquisition of information by an employee or agent of our company for business purposes is typically not an incident, provided that the information is not used or subject to further unauthorized disclosure.

GL Solutions Team Manager Responsibilities

Team managers are responsible for ensuring all employees in their unit are aware of policies and procedures for protecting personal information.

If a breach or suspected breach of personal information occurs in their supervision area, the team manager must notify the IT Support Specialist immediately and open an incident report. (See “Incident Response” Section, IT Support Specialist).

Note: Education and awareness communication will be directed annually to all employees informing them of the proper procedures for reporting a suspected breach of Confidential/PII information.

Automated Events

GL Solutions leverages automated tools which raise event alerts:

- Microsoft Sentinel: collects, indexes and analyzes information from information system component logs including the firewall, application gateway, servers and other components. Identifies threats and potential vulnerabilities.
- Microsoft Defender for Cloud and Endpoint: Detects potential vulnerabilities and security alerts on networks, servers and desktops.
- Microsoft Intune: Provides mobile device management and mobile threat detection technologies for staff accessing company resources on personal devices.
- Azure Security Center: Monitors for threats and generates security alerts based on advanced threat detections.
- Azure Service Health: Provides notifications about security advisories, warnings, and informational alerts related to the health of Azure services.
- Azure Active Directory: Generates security notifications related to identity and access management, such as suspicious sign-in attempts, risky users, and conditional access policies.

Automated alerts should be examined as an event and classified accordingly.

Event Notification

The IT Support Specialist will be the central point of contact for reporting computer events and incidents. Upon notification, the IT Support Specialist will classify the event as indicated below. If there is any indication of a severity 1 or 2 event, the IT Support Specialist will immediately notify the Chief Security Officer (CSO), or when unavailable, the first listed member of the IRT. The CSO will conduct a preliminary analysis of the events and determine whether Incident Response Team activation is appropriate.

If the event does not suggest a severity 3 or lower event, the IT Support specialist will process in accordance with the applicable System Event in the Information Systems Catalog. Notification to the System Security Administrator may be required by the System Event.

Event and Incident Severity

Reported events, and incident investigations thereof, classify events by severity to ensure that the event receives the resource level attention relative to the incident priority. This document uses the terms below to establish consistent communications. For the purposes of this document, their definitions are defined in the table below:

SEVERITY LEVEL	DEFINITION
1	<ul style="list-style-type: none">• <i>Unauthorized access, disclosure, or destruction of PII or confidential information or data</i>• <i>Intentional disruption of client GL Suite systems that prevents or impairs customer access to the system (such as a denial-of-service attack)</i>
2	<ul style="list-style-type: none">• <i>System, application, or component experiencing an outage that impacts the customer's ability to use GL Suite and therefore causes customer pain.</i>

	<ul style="list-style-type: none"> • <i>Suspicious files or malicious code identified on any server within the production environment</i> • <i>Automated high or critical severity event notifications for information system components.</i> • <i>Simultaneous logins by the same user from different IP addresses</i>
3	<ul style="list-style-type: none"> • <i>Improper usage, such as a violation of the Rules of Behavior, or any unauthorized scanning or probing activities</i> • <i>Security vulnerabilities or bugs in GL Suite code or software applications used within the production environment that has the potential to be exploited</i> • <i>Automated high or critical severity vulnerability notifications for information system components.</i>
4	<ul style="list-style-type: none"> • <i>Any other type of incident not included above</i>

Classifications

All computer security events are classified to assist company management in determining the severity and criticality of the security event and ensure that the event receives the resource level attention relative to the incident priority. This document uses the terms below to establish consistent communications. For the purposes of this document, their definitions are defined in the table below.

CLASSIFICATION	DEFINITION
<i>Attack Vector</i>	<i>The method or means by which a hacker or unauthorized user can gain access to computer systems or data, such as via email, removable media, web applications, etc.</i>
<i>Event</i>	<i>An occurrence suspected or confirmed not yet assessed, in an information system, network or application that may negatively affect an information system, network, or process, but has not been determined to be an incident</i>
<i>Incident</i>	<i>An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.</i>
<i>Security Incident</i>	<i>An incident the includes the unauthorized acquisition of data maintained by GL Solutions that compromises the security, confidentiality, or integrity of confidential or PII information.</i>
<i>Indicators of Compromise</i>	<i>A sign that an incident may have occurred or may be currently occurring</i>
<i>Significant Incident</i>	<i>An incident involving an information system or administrative-related policy violation that represents a meaningful threat to the business process and requires immediate leadership notification</i>
<i>Minor Incident</i>	<i>A security-related incident that does not represent a significant threat to the business process and does not require immediate leadership notification</i>
<i>Vulnerability</i>	<i>A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source</i>

<i>Threat</i>	<i>Any circumstance, event, or person with the potential to adversely impact operations (including mission, functions, image, or reputation), organizational assets, or personnel</i>
<i>Threat Source</i>	<i>The intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger vulnerability. Synonymous with threat agent</i>

IRT Activation

The CSO shall activate the IRT upon suspicion of a severity 1 event.

Incident Response Team

An Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. The Incident Response Team's mission is to prevent a serious loss of business operability or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Chief Security Officer will coordinate these investigations.

The Incident Response Team will subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents. Further, a backup and copy of this Incident Response Plan will be distributed monthly to members of the Disaster Recovery Team during the Disaster Recovery Repository backup process.

Incident Response Team Members

Each of the following areas will have a primary and alternate member:

- CEO (Chief Security Officer)
- Chief Administrative Officer (Chief Privacy Officer)
- System Security Administrator
- Chief Technology Officer
- CFO
- IT Support Specialist

Incident Response Team Roles and Responsibilities

Chief Security Officer

- Determines the nature and scope of the incident

- Contacts qualified IT Support Specialists and System Security Administrators for advice as needed
- Contacts members of the Incident Response Team
- Determines which Incident Response Team members play an active role in the investigation
- Provides proper training on incident handling
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate
- Prepares a written summary of the incident and corrective action taken

Chief Privacy Officer

- Coordinates activities with the Chief Security Officer
- Documents the types of personal information that may have been breached
- Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information
- Assists in developing appropriate communication to impacted parties
- Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach

System Security Administrator

- Central point of contact for all computer incidents
- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
- Looks for signs of a firewall breach
- Collects pertinent information regarding the incident at the request of the Chief Information Security Office

IT Support Specialist

- Responds to automated and manual alerts of suspicious activity
- Notifies Chief Security Officer to activate computer incident response team
- Monitors business applications and services for signs of attack
- Contacts System Security Administrator for assistance in handling the incident
- Takes actions necessary to block traffic from suspected intruder
- Ensures all service packs and patches are current on mission-critical computers
- Ensures backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity
- Reviews audit logs of mission-critical servers for signs of suspicious activity

Information Technology Auditor

- Reviews systems to ensure compliance with information security policy and controls
- Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
- Reports any system control gaps to management for corrective action

Common Incident Classifications

The Information Systems Catalog describes common incidents and typical resolution steps. Charted below are the types retrieved from the catalog and the attributed severity.

Incident Type	Severity Level
Brute Force Attack	2
Denial of Service Attack	1
Phishing Attack	3
Ransomware Attack	1
SQL Injection Attack	1
Account Compromise	2
XSS Attack	3

Event and Incident Documentation

Staff, including all members of the IRT, associated with the classification and response to an event or incident must keep accurate notes on all actions taken, by whom, and the exact time and date. Event and severity 2 or lower event notes are tracked in LOKI. Severity 1 events and incidents are tracked in line in this IRP. Post-incident, the lessons learned are incorporated and implemented into both training material and the applicable documentation.

Each person involved in the investigation must record his or her own actions.

IT Support Specialist

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. The IT Support Specialist will serve as a central point of contact for reporting any suspected or confirmed event.

IT Support Specialist contact information: (541) 312-3662 option 8

2. After documenting the facts presented by the caller and verifying that an event or suspected event occurred, the IT Support Specialist will open a High Priority task.
3. The IT Support Specialist will then immediately contact the Chief Security Officer for any event with a Severity 1 or higher. The Chief Security Officer analyzes the facts and confirms whether the event warrants incident response team activation.

4. The IT Support Specialist will process Severity 2 and lower events in accordance with process identified in the System Events section of the information systems catalog.

Chief Security Officer

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. Create a copy of this master Incident Response Plan. Save locally until the response is complete. Within the IRP, take notes inline until all the response is complete.
2. When notified by the IT Support Specialist, the CSO performs a preliminary analysis of the facts and assesses the situation to determine the nature and scope of the incident. If this is an obvious security incident, immediately contact the IT Support Specialist and request that the appropriate System Event be executed on a P1/HP basis.
3. Informs the Legal Department and the Chief Privacy Officer that a possible privacy breach has been reported and provides them with an overview of the situation.
4. Contact the individual who reported the problem.
5. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of Confidential/PII information. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).
6. Reviews the preliminary details with the Legal Department and the Chief Privacy Officer.
7. If a privacy breach affecting Confidential/PII information is confirmed, Incident Response Team activation is warranted.
8. Notify GovRAMP PMO if the information is within the GovRAMP authorization boundary.
9. Engage the IT Support Specialist to take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third-party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.
 - Change all applicable passwords for IDs that have access to Confidential/PII information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the unauthorized party, disable the account.
 - Do not access or alter the compromised system.
 - Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable) and/or disable the access method that allowed the breach (i.e., turn off the website).
10. Containment is important to limit the impact of an incident and prevent increased damage. Upon identification of impacted assets, the assets will be removed from the production VNETs and into a secured group for continued analysis, eliminating the affected machine's ability to

communicate with other systems in the production stack. Additional information can be found in the below "Containment & Eradication" table.

11. Notify the Chief Privacy Officer of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.
12. The Chief Security Officer is responsible for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.
13. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.
14. If the investigation suggests that a data loss or breach may reasonably have occurred and is potentially ongoing, contact the IT Support Specialist and System Security Administrator for emergency assistance in gathering additional information.
15. Contact appropriate Incident Response Team members.
16. Identify and contact the appropriate Data Owner affected by the breach. In coordination with the Legal Department, Chief Privacy Officer and Data Owner, determine additional notification requirements (e.g., Human Resources, external parties).
17. If the breach occurred at a third-party location, determine if a legal contract exists. Work with the Legal Department, Chief Privacy Officer and Data Owner to review contract terms and determine the next course of action.
18. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all tests, development and production systems and the number of entities at risk.
19. Determine the type of Confidential/PII information that is at risk, including but not limited to:

Name, Address, Social Security Number, Account number, Financial and identifying information

20. If entity information is involved, have the Data Owner determine who might be affected. Coordinate next steps with the Legal Department and Chief Privacy Officer (e.g., individual notification procedures).
21. Determine if an unauthorized party has exported or deleted any personal information data.
22. Determine where and how the breach occurred.
 - Identify the source of compromise, and the timeframe involved.
 - Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and point-to-point connections. Look at the appropriate system and audit logs for each type of system affected.
 - Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
23. Monitor systems and the network for signs of continued unauthorized party access.
24. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

25. Engage the IT Support Specialist to modify the retention schedule for backups to preserve back up records until otherwise directed.
26. Notify the CPO in coordination with the Legal Department as appropriate. Provide a summary of confirmed findings, and of the steps taken to mitigate the situation.
27. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager for disciplinary action and possible termination. In the case of contractors, temporary workers, or other third-party personnel, ensure discontinuation of the user's service agreement with the company and revoke security/permissions.
28. Notify the System Security Administrator to perform an After-Action Report analysis of the event in order to revise security policies and procedures.

After-Action Report Template

OBJECTIVE

The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

CORE CAPABILITY STRENGTHS

The [full or partial] capability level can be attributed to the following strengths:

Strength 1:

Strength 2:

Strength 3:

AREAS FOR IMPROVEMENT

The following areas require improvement to achieve the full capability level:

AREA FOR IMPROVEMENT 1:

[Observation statement. This should clearly state the problem or gap; it should not include a recommendation or corrective action, as those will be documented in the Improvement Plan.]

REFERENCE:

[List relevant plans, policies, procedures, laws, and regulations, or sections that apply. If no references apply to the observation, it is acceptable to simply list "Not Applicable."]

1. *[Name of the task and the applicable plans, policies, procedures, laws, and regulations and 1–2 sentences describing their relation to the task.]*
2. *[Name of the task and the applicable plans, policies, procedures, laws, and regulations and 1–2 sentences describing their relation to the task.]*

ANALYSIS:

[The analysis section should be the most detailed section of an Observation. Include a description of the behavior or actions at the core of the observation, as well as a brief description of what was discussed, and the implications/consequence(s) noted. If a strength was identified, include any relevant innovative approaches discussed by the exercise participants.]

Notifications

Security incidents involving client information or information systems within the GovRAMP authorization boundary must be reported to the GovRAMP PMO and agencies within 60 minutes.

The information described below is required when notifying a customer agency of a security incident:

1. Current level of impact on functions or services (Functional Impact). See table below for a list of Functional Impact categories. Specific thresholds for loss-of-service availability (e.g., all, subset, loss of efficiency) must be defined by the reporting organization.
2. Type of information lost, compromised, or corrupted (Information Impact). See table below for a list of Information Impact categories.
3. Estimate of the scope of time and resources needed to recover from the incident (Recoverability). See table below for a list of Recoverability categories.
4. When the activity was first detected.
5. Number of systems, records, and users impacted.
6. Network location of the observed activity.
7. Point of contact information for additional follow-up.

Important: Do not add sensitive personally identifiable information (PII) to incident submissions.

In some cases, it may not be feasible to have complete and validated information prior to reporting. The company will provide the best available estimate at the time of notification and report updated information as it becomes available.

CATEGORY	DESCRIPTION
Denial of Critical Services/Loss of Control	A critical system has been rendered unavailable.
Significant Impact to Critical Services	A critical system has a significant impact, such as local administrative account compromise.
Denial of Non-Critical Services	A non-critical system is denied or destroyed.
Significant Impact to Non-Critical Services	A non-critical service or system has a significant impact.
Minimal Impact to Critical Services	Minimal impact but to a critical system or service, such as email or active directory.
Minimal Impact to Non-Critical Services	Some small level of impact to non-critical systems and services.
No Impact to Services	Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
No Impact	Event has no impact.

Functional Impact Levels

Note: Incidents may affect multiple types of data; therefore, you may select multiple options when identifying the information impact.

CATEGORY	DESCRIPTION
Destruction of Critical System	Destructive techniques, such as MBR overwrite; have been used against a critical system

CATEGORY	DESCRIPTION
Core Credential Compromise	Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated
Critical Systems Data Breach	Data pertaining to a critical system has been exfiltrated
Destruction of Non-Critical Systems	Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system
Proprietary Information Breach	The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCI), intellectual property, or trade secrets was compromised.
Privacy Data Breach	The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised
Suspected but not Identified	A data loss or impact to availability is suspected, but no direct confirmation exists
No Impact	No known data impact

Information Impact Levels

RECOVERABILITY LEVEL	DESCRIPTION
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly)
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Supplemented	Time to recovery is predictable with additional resources
Regular	Time to recovery is predictable with existing resources

Recoverability Levels

The following information should also be included if known at the time of submission:

- Attack vector(s) that led to the incident.
- Any indicators of compromise, including signatures or detection measures developed in relationship to the incident.
- Any mitigation activities undertaken in response to the incident.

ATTACK VECTOR	DESCRIPTION	EXAMPLE
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.

ATTACK VECTOR	DESCRIPTION	EXAMPLE
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email/Phishing	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected flash drive.
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack method does not fit into any other vector	Miscellaneous

Legal

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

Ongoing:

1. Monitor relevant privacy-related legislation, provide input as appropriate, and communicate to our clients the effect that any enacted legislation may have on them.
2. Be cognizant of major contracts which the organization enters that may have an impact or effect on our customers, employees, and other data.
3. Be aware of other companies' privacy policies that may affect GL Solutions and affiliates.

When a Privacy Breach Occurs:

1. After confirmation that a breach of personal information on individuals has occurred, notify external legal counsel

2. Coordinate activities between business areas and other departments (e.g., Human Resources, if necessary).
3. If necessary, notify the appropriate authorities.
4. Coordinate public relations efforts on the timing and content of notification to individuals.
5. If the Chief Security Officer determines that the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.
6. Notification to individuals may be delayed until the CSO is assured that necessary measures have been taken to determine the scope of the breach and that it has been properly investigated.
7. Follow approved procedures for any notice of unauthorized access to Confidential/PII information. Notification to entities should be timely, conspicuous, and delivered in any manner that will ensure the individual receives it. Notice should be consistent with laws and regulations the organization is subject to.

Appropriate delivery methods include written notice, email notice, and conspicuous posting of the notice on the customer website.

Human Resources

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. If notified of a privacy breach affecting employee personal information, open an incident request with the IT Support Specialist to activate the Incident Response Plan for suspected privacy breach.
2. When notified by the Information Security Office that the privacy breach incident response plan has been activated for a breach of information on an individual, perform a preliminary analysis of the facts and assess the situation to determine the nature of the incident.
3. Work with the IT Support Specialist, CSO, CPO and business area to identify the extent of the breach.
4. If appropriate, notify the business area that a breach has been reported and is under investigation.
5. Work with the business area to ensure there is no further exposure to privacy breaches.

6. Work with the CSO, CPO and Legal Department to determine if the incident warrants further action.

System Security Administrator

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. When notified by the CSO that the privacy breach Incident Response Plan is activated, provide assistance as determined by the details of the potential breach.
2. Review firewall logs for correlating evidence of unauthorized access.
3. Provide technical escalation and expertise to the IT Support Specialist and CSO.
4. Implement firewall rules and other network configuration changes as needed to close any exposures identified during the investigation.

Public Relations

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

Ongoing:

1. Monitor consumer privacy issues and practices of other companies.
2. Monitor consumer privacy breaches of other companies and how they respond.
3. Keep generic/situational talking points current.

When Privacy Breach Occurs:

1. After confirmation that a breach of personal information about individuals has occurred, notify the Chief Privacy Officer.

2. Coordinate with the CPO and Legal on the timing, content and method of notification. Prepare and issue press release or statement, if needed.

Vehicles for communicating include:

- a. GL Solutions Website
 - b. Internal Website – If appropriate for breach of employee information
 - c. E-mail
 - d. News conference – If privacy breach should reach a national and/or crisis level, coordinate brief news conference at headquarters or appropriate location.
 - i. Appoint appropriate spokesperson
 - ii. Prepare statement and, if necessary, potential Q & A.
 - iii. Coach spokesperson on statement and potential Q & A.
 - iv. Invite select media to attend and cover organization's proactive message.
 - v. Use conference as a platform for communicating who the breach involves, what the organization is doing to correct breach, how it happened and the organization's apology but reassurance of its privacy policies
3. Prepare appropriate response to media, customer, and/or employee; and have the CPO and Legal Department approve prior to distribution.
 4. Proactively respond to media inquiries, if necessary.
 5. Monitor media coverage and circulate accordingly.

Attachment 3: Service Level Agreement (SLA)

GL Suite End User License Agreement

Contract

1. Parties. Parties to this GL Suite End User License Agreement ("Contract") include GL Suite, Inc. (dba GL Solutions), a Montana corporation ("Provider"), and _____ an agency of the State of _____ ("Customer").

2. Contract Incorporation. This Contract may be executed in any number of counterparts, including this contract, Provider's offer and, optionally, Customer's request for offers, each of which shall be deemed to be an original and all of which shall constitute one agreement which is binding upon all the parties hereto, notwithstanding that all parties are not signatories to the same counterpart. If this Contract was submitted with the Provider's offer in response to Customer's request for offers, Provider intends for the offer to be contingent upon acceptance by Customer of the terms of this Contract.

3. Order of Precedence. When determining software functionality required by this contract, the following documents shall have precedence in the order listed:

- (a) Specifications which include detailed design documents including Self-Documenting Specifications, output and web page specifications, and other specifications;
- (b) Process guides or process flow diagrams;
- (c) Goal and Scope Document
- (d) Change Requests
- (e) This contract, as amended
- (f) Provider's Offer, as amended, if any
- (g) Customer's RFP, as amended, if any

4. Applicability. Some Customers have a separate agreement with GL Suite, Inc. (dba GL Solutions) which covers the use of the software and services. In such cases, the terms of that agreement supersede and replace this contract. If you have a written software license agreement with GL Solutions, please disregard this notice.

Scope of Permitted Use

5. Software License. The purpose of this contract is to provide Customer with a regulatory business process automation software application known as GL Suite, including related setup, access, and support services. GL Suite is a software application designed to automate business processes in government regulatory agencies (the "Software"). The Provider grants Customer a non-exclusive, non-transferable, revocable, limited right to access and use the Software as a Service (SaaS) during the Term of this Agreement, solely for the Customer's internal business purposes and in accordance with Provider documentation of the same. Provider offers this SaaS contract along with licensing, customer service and support for Software in annual support plans referred to herein as "GL Simple plans".

6. User Licenses. Customer may authorize up to the number of named users specified in a purchase order or other contract document to access and use the SaaS. Customer is responsible for ensuring that all users comply with the terms and conditions of this contract.

7. Third-Party Users. Customer may not sublicense, resell, lease, rent, or otherwise make the SaaS available to any third party, except to entities not employed by the agency in conjunction with the Customer's regulatory activities such as applications, renewals, complaints, investigations,

inspections and other regulatory activities carried out by Customer. Customer may also connect third-party software to the Software through Provider provided interfaces to support the use identified in this paragraph.

8. License Limitations. Customer may not use the SaaS for any unlawful, fraudulent, or malicious purposes, or in any manner that violates any applicable laws, regulations, or industry standards. Customer may not use the SaaS to interfere with or disrupt the operation of the Provider's systems or networks, or attempt to gain unauthorized access to the Provider's systems or networks. Customer may not modify, reverse engineer, decompile, disassemble, or create derivative works of the SaaS or any part thereof.

9. Updates. The license granted by this contract is limited to the most current and immediately prior version of the Software. Provider shall determine the functionality of the Software, which may be configured to meet Customer's specific business requirements. Provider shall take reasonable efforts to notify Customer at least thirty (30) days prior to of any planned change(s) or update(s) to the Software; its functionality; security architecture, features or settings. The planned changes or updates include any change(s) that would potentially impact the secure and efficient use of the Software, as understood and agreed to between Provider and Customer.

10. Confidentiality. Customer agrees to maintain the confidentiality of the Software including all concepts, documentation, methods, processes and ideas, and the structure, sequence, and organization, designs, data models, tables and set-ups, and interfaces embodied, or expressed therein and to use same only as expressly authorized in this License.

Term and Termination

11. Contract Term. This Contract shall be effective during the term of any GL Simple Plan. ("Term of this Agreement")

12. Contract Renewal. Upon the expiration of any annual term, the GL Simple plan tier then in effect for Customer shall be automatically renewed for an additional annual term, unless Customer has provided Provider 90-day's written notice of non-renewal or request to change GL Simple plan tier prior to the date of current GL Simple plan expiration. Customer's right to purchase a GL Simple plan from Provider expires five years from execution of this Contract, unless otherwise extended by mutual agreement between the parties. GL Simple plans must be purchased for consecutive time periods. Failure by Customer to purchase a GL Simple plan for any period of time terminates Customer's right to purchase a GL Simple plan under this Contract.

13. Termination without Cause. Either party may terminate this Contract without cause by providing notice 90 days prior to the expiration of the current GL Simple plan.

14. Termination for Cause. Either party may terminate this Contract after a cure period for a material breach of the Contract terms. The party alleging breach shall provide a 30-day written notice to cure (cure period), detailing each instance of breach, including the facts and provisions of the contract breached, and the remedy sought. The party alleging breach shall provide a good-faith opportunity to cure. The remedy sought must be reasonably intended to allow the parties to fulfill the material provisions of the contract and waiving remedies for prior breaches.

15. Transition Upon Termination. Provider shall provide services under a GL Simple plan for an effective and efficient transition of service with minimal disruption to the Customer including

cooperation and assistance to ensure that all Customer data is securely transferred to Customer. Customer data includes transactional data and images, but not data about the configuration of Software. Customer Data will be transferred in Microsoft SQL Server Database Backup or native image format via a SFTP site specified by Customer or through other media as required by the size of the data. Within 90 days following termination, Provider will provide a written certificate to Customer stating that all Customer data has been transferred or deleted or disposed of as directed by the Customer.

16. Provider's Remedies. In the event Provider terminates the Contract for breach by Customer, Provider shall have the right to exercise any one or more of the following remedies:

- (a) To sue for and recover all payments, then due or thereafter accruing hereunder;
- (b) To immediately terminate all performance of GL Simple plan services;
- (c) To bring an action in a court with jurisdiction over Customer seeking injunctive relief mandating removal and surrender of the Software;
- (d) To terminate the license as to any or all items of the Software; and
- (e) To pursue any other remedy available at law or in equity.

The foregoing remedies are cumulative and not exclusive or sequential.

17. Customer's Remedies. In no event shall Provider's liability for breach of contract exceed the sum of all funds previously received from Customer by Provider during the prior twelve months. This remedy is Customer's sole and exclusive remedy for any non-conformities, defects or errors and all performance or non-performance problems related to the Contract including without limitation any breach of warranty by Provider. The parties intend for this limitation of liability to supersede any other provision in conflict within this contract, whether those provisions be contained in a document with precedence or not.

18. Attorney Fees. Neither party shall be entitled to costs or expenses in exercising any of its rights or remedies in enforcing any of the terms, conditions or provisions hereof. In the event this provision is determined not to be enforceable, both parties shall reimburse the other party in proportion of their liability for reasonable costs and expenses, including attorneys' fees, costs and disbursement incurred by Provider in exercising any of its rights or remedies in enforcing any of the terms, conditions or provisions hereof.

19. Waiver. The waiver by either party, or the failure by either party, to claim a breach, or give notice with respect thereto, of any provision of this Contract shall not be, or be held to be, a waiver of any subsequent breach, or as affecting in any way the effectiveness, of such provision.

Data Ownership and Security

20. Customer Data. Transactional data entered by Customer or authorized third parties belongs to the Customer. Customer provided domain names, file uploads, and graphics belong to the customer. These data and files are collectively referred to as "Customer Data." Customer Data does not include meta data, proprietary to the business rules engine of the Software.

21. Use of Customer Data. Provider may collect Customer Data only as necessary to provide services authorized under the Contract. No Customer Data shall be disclosed, provided, rented or sold to any third party for any reason unless authorized by Customer, required by law or regulation or by an order of a court of competent jurisdiction.

22. Security. The Software subject to this SaaS contract shall be provide by Provider in a secure environment. Provider shall provide good faith efforts to meet applicable SOC I and SOC II standards to prevent unauthorized access to and use or modification of, and to protect, the Software and Customer data.

(a) Provider shall implement user identification and access controls designed to limit access to users in accordance with the principles of least privilege.

(b) Provider shall ensure that all personnel with physical or logical access to the Software will receive industry standard annual security awareness training.

(c) Provider shall ensure that the Software is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.

(d) Provider shall ensure that the Software employs automated mechanisms to centrally review, analyze and correlate audit and log records from multiple components of the Software to support organizational processes for investigation, alerting and response to suspicious activities.

(e) Provider shall ensure that the Software supports exporting of log files to the Customer for review and analysis.

(f) Provider shall provide evidence of a comprehensive continuous monitoring program encompassing all systems with access to Customer data.

(g) Provider shall ensure that all changes to proposed Software or Hosting services are authorized according to change management policies.

(h) Provider shall provide and maintain a backup of Software and Customer data that can be recovered in an orderly and timely manner within a predefined frequency consistent with recovery time and recovery point objectives. Provider shall store a backup of Content, at least daily, located within the continental United States, maintaining the security of the Software and Customer data.

(i) Provider shall implement a contingency plan designed to maintain the access to the Software and to prevent the unintended destruction or loss of Content. This plan should provide a predefined frequency, consistent with recovery time and recovery point objectives for disaster recovery and archival purposes of Software at a secure facility located within the continental United States.

(j) Provider shall maintain an incident response program that implements incident handling for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery processes. Incident response must have the capability to support automated mechanisms for supporting incident handling processes.

(k) Provider shall perform quarterly scans using an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

(l) Provider shall support physical security measures, including securing Software on a secure server, in locked data cabinets within a secure facility located within the continental United States.

(m) Provider shall ensure that access to facilities housing Software are restricted to only allow access to Provider's personnel and agents who have a need to know in connection with operation and support of the Software.

(n) Provider shall ensure that the Software, operating systems, middleware, applications, and interfaces will be scanned for vulnerabilities every 30 days.

(o) Provider shall conduct monthly vulnerability scans against all public-facing interfaces with access to the Software.

(p) Provider shall ensure that Software is stored, processed and maintained within the continental United States at all times.

(q) Provider shall, at all times, remain compliant with the privacy and security requirements mandated by federal, state and local laws and regulations.

(r) Provider shall ensure performance of a security audit at least once annually of the Software.

(s) Provider shall ensure that external connections incorporated into the Software have appropriate security controls including industry standard intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the firewall maintained by Provider.

(t) Provider shall ensure that the Software will utilize industry standard firewalls regulating all data entering the internal data network from any external source which will enforce secure connections between internal and external systems and will permit only authorized data to pass through.

(u) Provider shall ensure that the Software will use industry standard encryption techniques to protect Content that is transmitted or stored on behalf of the Customer.

(v) Provider shall utilize industry standard malware protection, incorporating both signature and non-signature-based detection mechanisms, on all systems with access to Software. Provider shall ensure that malware protection will be centrally managed and receive regular automatic updates to malicious code protection mechanisms and data files from the software vendor.

23. Premium Security. Requirements for GovRAMP compliance for the Software at the “Ready” or “Authorized” levels are available to agencies for an additional fee denoted as “Premium Security” in the Pricing Addendum.

Pricing and Payments

24. Due Dates. Payment for Setup Services and Escalated Projects are due upon Acceptance of the deliverables or Escalated Project. Payment for Escalated Tasks are due when ordered by Customer. Payment for GL Simple Plans are due prior to the first day of the GL Simple plan term. Annual GL Simple plans may be paid for in quarterly installments or in increments that coincide with the end of Customer’s fiscal year. Irrespective of any language on or accompanying a payment, Provider shall apply all payments received to the oldest invoice due.

25. Price Increases. Provider may increase the cost of GL Simple Plans, Escalated Project and Escalated Tasks, but not Setup Services by a percentage not to exceed the consumer price index for urban dwellers of the most recent twelve-month period reported by the United States Department of Labor. Provider shall notify Customer not less than three months prior to any price change.

26. Payment Obligation Absolute. Customer's obligations under this Contract, including the obligation to pay license fees unabated, shall continue in full force and effect regardless of any inability of Customer to use the Software because of war, governmental regulations, or strikes, unless for breach of contract or warranty.

27. Late Payments. Should Customer fail to pay any amount required hereunder to be paid by Customer to Provider, within thirty (30) days after the due date thereof, Customer shall pay the Provider interest on the unpaid amount of such delinquent payment at the rate of eight percent (8%) per annum from the date such payment was due until it is paid in full, or, in the event such rate exceeds that which is permitted by applicable law, the highest permissible rate.

28. Non-Refundable. GL Simple plan fees are non-refundable. Customer's obligation to pay GL Simple plan fees for the full duration of the annual plan period shall survive the termination of this Contract.

Setup Services

29. Setup Services. To enable Customer specific uses of the Software, Provider shall provide the services described in the Setup Services – Statement of Work attached for the fees specified.

30. Project Management. Within 30 days following contract execution and annually thereafter, Customer and Provider shall agree to a Management Plan, which describes the project management methodology including scope, schedule, change, risk, deliverable review and

communication management activities. Provider and Customer shall perform project scope, schedule, change, conflict, risk, deliverable review, and communication management activities consistent with the Management Plan.

31. Project Management Tools. Provider and Customer agree to use GL Portal, an online, web-based project management system developed by Provider to store project deliverables, communicate schedules, provide Acceptance of specifications and other deliverables, answer clarifications, report defects, and provide notifications. Provider will issue Customer a unique login and access to GL Portal for each person authorized by Customer. Customer will authorize Provider to grant GL Portal access only to Customer agents with authority to act on behalf of Customer. Provider shall utilize Microsoft Word, Excel, PowerPoint and Visio to develop written project documents. Provider shall provide project management forms for acceptance, deliverable review reporting defects, etc. No other project management software or forms shall be used.

32. Conversion. Customer shall produce legacy data along with documentation that describes the Legacy Data structure, relationships, fields and tables in detail sufficient to enable Provider to convert the data to a format utilized by Software. Provider will transfer legacy data from delimited or fixed length ASCII text files or an ODBC compliant data source to the Software. Transfer of data means the manipulation of data from a data source to the table structure utilized by Software. Conversion Services does not include the identification or correction of data-entry or normalization errors present in legacy systems.

33. Requirements Refinement. Software functionality required by this contract shall be clarified through a process of refinement. The refinement begins with the adoption of a Goal and Scope Document which describes the business processes, interfaces, outputs and legacy data sources required prior to production use of the software. A Goal and Scope document shall be adopted for each GL Simple Project as required to modify, add or delete Customer business process functionality.

34. Configuration. Customer shall provide all necessary staff required by Provider to assist Provider with the design, review deliverables, and answer clarifying business requirement questions. Staff shall possess subject matter expertise on Customer's operations and business requirements. Provider shall gather business requirements from Customer and create designs and specifications that describe the Software requirements functionality that accomplishes the business requirements gathered. Provider shall configure the Software to operate in accordance to Customer Accepted specifications. Provider shall perform unit and system tests to ensure the development conforms to the Accepted specifications.

35. Deliverable Review. Provider shall create specifications and other documentation, such as project management documents, training, and software documentation, to support the Goal and Scope Document. Provider shall submit specifications and documentation to Customer for Acceptance using GL Portal. Provider shall specify which contract requirements are met by the specification or documentation. Customer shall review the specification or documentation to determine whether the document, if developed per the specification, fulfills the contract requirement specified by Provider. Customer shall respond to Provider's request for approval by:

- (a) Accepting the submitted specification or documentation within seven calendar days,
- (b) Rejecting the specification or documentation within seven calendar days, or
- (c) Not responding to the Acceptance request within seven calendar days. Not responding to the Acceptance request within seven calendar days constitutes Customer's Acceptance of the specification or documentation.

If the specification or documentation does not conform to the Contract, Customer shall notify Provider using GL Portal specifying the specific contract exceptions which cause the specification or

documentation to be unacceptable. All such deficiencies within the specification or documentation must be noted during Customer's initial review of the specification or documentation.

Provider shall correct the deficiencies and resubmit the specification or documentation within seven calendar days from the receipt of the rejection. Customer shall have seven calendar days to re-inspect, test and reevaluate the resubmitted specification or documentation to determine whether deficiencies initially noted are corrected. Additional cycles may be added until all deficiencies initially noted are corrected.

Acceptance of a specification or documentation constitutes Acceptance that Provider's configuration and implementation of the Software according to the specification or documentation satisfies Provider's performance obligations with respect to the corresponding contract requirement identified. Acceptance of a software deliverable constitutes Acceptance that the Software performs as specified.

36. Training. Provider shall provide end user training on how to use the configured Software as described in Accepted specifications. Customer shall require training attendance and participation by Software users. Customer shall provide one or more employees with responsibility for retraining users and providing personal direction to employees requiring additional assistance.

37. UAT. No later than 30 days prior to the planned commencement of User Acceptance Testing for the initial product usage of the Software, Customer and Provider shall adopt a UAT Plan, which describes the objective, measurable criteria for beginning and successfully exiting UAT. Successful performance of the UAT exit criteria constitutes Acceptance of setup services and customer's direction deliver the Software to the production environment. Customer shall conduct UAT testing of the configured Software exclusively by following process guides in the Software detailing each Customer business process.

38. Timeliness. Provider and Customer timely and effective cooperation is essential to the provision of setup and support services in this contract. Delay by Customer waives any requirement for Provider's timely performance; waives Customer's rights to liquidated damages, if any; may cause delay in the production use of the software and subsequent delivery of support services.

39. Acceptance. Any the following conditions constitute acceptance ("Acceptance") of a project document, specification, software, Software, sub-deliverable or deliverable by Customer, in the form delivered by Provider:

(a) Written acceptance by Customer;

(b) Production use of the Software in a live environment; or

(a) Failure to test, inspect and report specific defects regarding the Software or any contract deliverable within seven calendar days after delivery by Provider to Customer.

GL Simple Plan

40. GL Simple. GL Simple plans include the SaaS licensing and following the execution of setup services, certain support services. The annual cost of a GL Simple plan is based on the tier and number of named Customer employees with access to the Software whether or not such usage is concurrent as shown in the Pricing Addendum.

41. Tasks and Projects. Provider offers additional services to Customer in the form of Tasks or Projects.

(a) Projects – A project includes a request for a service with any of the following characteristics: 1) functionality requests that require coordination between Provider and a third-party; 2) functionality requests with three or more finite deliverables which must be delivered in a specific sequence to meet the Customer's business requirements; 3) functionality which may impact other aspects of the configured Software and therefore require a system test of an entire business process; or 4) service or functionality which requires the presence of a Provider employee onsite at Customer's place of business.

(b) Tasks – A task is a single request for a service except requests that are a project.

(c) At the Provider's sole discretion, Provider may establish and modify reasonable policies affecting the definition of services, the concurrency of item fulfillment, the definition of projects and tasks, and the request timing required to perform requests within a GL Simple plan.

42. GL Simple Plan Tiers. GL Simple plans are offered in three tiers: Standard, Professional and Enterprise. Provider shall provide “Tasks” and “Projects” specified for each tier as follows:

GL Simple Tier	Tasks for Services	Projects for Services
Standard	None included	None included
Professional	2 tasks/user/year or 24 tasks per year, whichever is greater; max 200	One concurrent project, no limit on total
Enterprise	4 tasks/user/year or 48 tasks per year, whichever is greater; max 400	Three concurrent projects, no limit on total

(a) Customers purchasing the Standard tier must purchase GL Simple for a minimum of 25 named Customer employees or contractors with access to the Software.

(b) Customers purchasing the Professional tier must purchase GL Simple for a minimum of 8 named Customer employees or contractors with access to the Software.

(c) Customers purchasing the Enterprise tier must purchase GL Simple for a minimum of 3 named Customer employees or contractors with access to the Software.

(d) Customer may incrementally increase the number of Tasks or concurrent Projects in a GL Simple tier by paying an “Escalation Fee” in the amount applicable for each task or project pursuant to the Pricing Addendum.

43. Support Services. Provider offers GL Simple services as labeled in the first row in the GL Simple Service table below. The columns to the right of the service determine whether the service is offered to the GL Simple plan tier.

i. Services with a “\$” mark are available to the tier through escalated Tasks and/or Projects only.

ii. Services with a check mark without the symbol “\$” are provided without limitation.

iii. Services noted with the symbol “\$” utilize a Task or Project.

iv. Services without any mark for the tier are not available to that tier.

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise
Account Management			
Schedule Management	✓	✓	✓
Scope Management	✓	✓	✓
Risk Management	✓	✓	✓
Communication Management	✓	✓	✓
Client Engagement	✓	✓	✓
Project Initiation	✓	✓	✓
Change Management	✓	✓	✓
Critical Project Monitoring		✓	✓
Critical Task Prioritization		✓	✓
Technical Support			
Emergency Support (24 X 7 X 365)	3 hr response ✓	1 hr response ✓	15 min response ✓
User Questions	✓	✓	✓
Design Review	✓	✓	✓
Developer Support	\$	✓ t	✓ t
Hardware, Network and Security Support	\$	✓ t	✓ t
Architecture and Best Practice Guidance		✓ t	✓ t
Training and Documentation			
Design Training	✓	✓	✓
User Training	✓	✓	✓
Configuration and Developer Training Group Courses	\$	✓ t	✓ t
Administrator Training	\$	✓ t	✓ t
Administrator Documentation	✓	✓	✓
Software Patches and Releases for Core Software			
Software Releases	✓	✓	✓
Software Patches	✓	✓	✓

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise
Software Release Installation	\$	✓ _†	✓ _†
Software Patch Installation	✓	✓	✓
Warranty and Enhancements			
Lifetime Defect Correction	✓	✓	✓
Configuration and Customization	\$	✓ _†	✓ _†
Security			
Compliance Audit (PCI, NIST, HIPAA)	✓ _†	✓ _†	✓ _†
Configuration Management (Tiered Environments: Dev, Sys, UAT and Prod)	✓	✓	✓
Security Assessment		✓ _†	✓ _†
Custom Network Isolation and Management		✓ _†	✓ _†
Multi-Factor Authentication			✓
Uptime Guarantee		98%	99.9%
Disaster Recovery			
Data Export Service	\$	✓ _†	✓ _†
Automated Job and Interface Monitoring/Response			✓
Automated Site Monitoring/Response			✓
Backups	7 days	14 days	3 months
Disaster Recovery	within 14 days	within 3 days	within 1 hour
Mobile Inspections			
Mobile Inspection Service – per device	\$	\$	\$
Mobile Inspection Form Development		✓ _†	✓ _†
Mobile Inspection Dispatch Service		✓ _†	✓ _†
On-Premise Mobile Dispatch and Synchronization DB		✓ _†	✓ _†
Business Intelligence			
Power BI - Visual and interactive reports and dashboards for business analytics	\$	✓ _†	✓ _†
Communication Services			
Text and email messaging, including read receipts and email bounce reports	Number of Individuals in System X \$0.09		
Self-Service Administration (by Customer)			
User Security Administration	✓	✓	✓

GL Simple Service	GL Simple Standard	GL Simple Professional	GL Simple Enterprise
Ticket and Project Tracking Portal	✓	✓	✓
Automated Task and Project Promotion Between Environments	✓	✓	✓
Business Rule Configuration	✓	✓	✓
Output Modification	✓	✓	✓
Access your data using alternative tools (e.g. SQL Server Management Studio)		✓ t	✓ t
Power BI Professional license for authoring and publishing			✓ t

Service Level Agreement

44. Availability. The Software will be available to Customer twenty-four (24) hours a day, seven (7) days a week (“Uptime”) less Excusable Downtime for at least the percentage of time indicated for the “Uptime Guarantee” corresponding to Customer’s GL Simple plan tier in the GL Simple Service Table. Available means the software is generally accessible and usable, though certain functionalities may or may contain defects. Provider is not responsible for Customer’s equipment or connectivity.

45. Downtime. For the purposes of this Contract, “Excusable Downtime” is defined as that period of time when the Licensed Services are not available to Customer due to scheduled network, hardware or service maintenance and/or upgrades. Except in cases of emergency, Customer shall be provided a two (2) business day advance notification of such maintenance and/or upgrade. In cases of emergency, Provider will use its best efforts to notify Customer of a planned Downtime as soon as practicable. Maintenance or upgrades shall not occur Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Eastern Time.

46. Geo Redundant, Failover Hosting. Customer requirements for geographically redundant environments with failover Software support are available for an additional fee denoted as “Geo Redundant, Failover Hosting” in the Pricing Addendum. Geo redundant, failover hosting is required for any uptime guarantee greater than 99.9% uptime or uptime during Excusable Downtime.

47. Penalties. Provider shall credit Customer applicable GL Simple charges in proportion of excess downtime in a month. For example, if the Uptime Guarantee is 98%, but the actual uptime was 95%, a credit equal to 3% of the GL Simple plan fees due for that month shall apply.

Warranty

48. Intellectual Warranties. Provider warrants that Provider has the full power and authority to grant the rights granted Customer hereunder with respect to the SaaS, and neither the license or use by Customer of the Software, as permitted under this License, will in any way constitute an infringement or other violation of any copyright, patent, trade secret, trademark or any other intellectual property right of any third party.

49. Government Mandates. In the event Software requires updating due to Federal, State statutory or regulatory requirements affecting Customer, the Provider’s Software development

department shall give its highest priority to the implementation of such updates, but Provider does not warrant that all such updates will be completed, or that any updates will be completed by a certain time.

50. Setup and Services Warranty. During any GL Simple plan, Provider warrants that the Software configuration will perform in material conformity with Accepted specifications. Provider will cure all breaches of the foregoing warranty reported in GL Portal by Customer during a GL Simple plan.

51. Hosting Service Warranty. Customer assumes total responsibility for Customer's use and users' use of the Software. Customer understands and agrees further that the Internet is accessible by persons who may attempt to breach the security of Provider and/or Customer's networks. Provider has no control over and expressly disclaims any liability or responsibility whatsoever for such actions and Customer and Customer's end users access the service at Customer's own risk.

52. Warranty and Remedy Limitations. EXCEPT AS EXPRESSLY SET FORTH IN THIS CONTRACT, PROVIDER MAKES NO OTHER WARRANTIES OF ANY KIND, AND EXPRESSLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, AS TO ANY MATTER WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THE SUITABILITY OR THE CONDITION OF THE SOFTWARE, OR ITS FITNESS OR SAFETY FOR ANY PARTICULAR PURPOSE OR USE, OR AS TO ITS MERCHANTABILITY. PROVIDER MAKES NO WARRANTY REGARDING THE USABILITY OR CONVERTIBILITY OF ANY OF CUSTOMER'S DATA, THE SUITABILITY OF THE SOFTWARE FOR CUSTOMER'S NEEDS, OR ANY PERFORMANCE PROBLEM, CLAIM OF INFRINGEMENT OR OTHER MATTER ATTRIBUTABLE TO ANY USE OR MODIFICATION OF THE SOFTWARE, OR COMBINATION OF THE SOFTWARE WITH ANY OTHER SOFTWARE OR COMPUTER PROGRAM OR COMMUNICATIONS DEVICE, NOT EXPRESSLY AUTHORIZED BY PROVIDER IN WRITING. PROVIDER SHALL NOT BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING LIABILITY IN TORT, STRICT OR OTHERWISE) DAMAGES ARISING DIRECTLY OR INDIRECTLY FROM THE SOFTWARE, THE USE, MISUSE, LOSS OF USE OR SALE THEREOF OR THE DELAY OR FAILURE OF DELIVERY OF THE SOFTWARE OR FROM ANY OTHER CAUSE WHATSOEVER EVEN IF IT HAS BEEN ADVISED OF SUCH POSSIBILITY. THE LIMITATIONS, EXCLUSIONS AND DISCLAIMERS IN THIS CONTRACT SHALL APPLY IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND OR ACTION BY CUSTOMER, INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT OR ANY OTHER LEGAL THEORY, AND REGARDLESS OF THE SUCCESS OR EFFECT OF OTHER REMEDIES. IN NO EVENT WILL THE AGGREGATE LIABILITY OF PROVIDER TO CUSTOMER UNDER THIS CONTRACT FOR DAMAGES, COSTS, ATTORNEY'S FEES, EXPENSES OR INDEMNITY EXCEED THE TOTAL FEES PAID BY CUSTOMER IN THE LAST TWELVE MONTHS TO PROVIDER HEREUNDER. CUSTOMER HEREBY WAIVES ANY CLAIM THAT THESE EXCLUSIONS DEPRIVE IT OF AN ADEQUATE REMEDY OR CAUSE THIS CONTRACT TO FAIL OF ITS ESSENTIAL PURPOSE.

Miscellaneous

53. Interpretations. This Contract and all rights and obligations of the parties hereunder and all rights and obligations of the parties shall be governed by, and construed and interpreted in accordance with, the laws of the State of Montana applicable to agreements made and to be performed entirely within such State, including all matters of enforcement, validity and performance.

54. Amendments. This Contract may only be amended in a written agreement executed by authorized representatives of both parties hereto.

55. Assignments by Provider. Any and all rights and interests of Provider under this Contract may be assigned, either in whole or in part, without notice to Customer, and Customer agrees that its rights under this Contract are expressly subject and subordinate to any and all security interests which may now or hereafter be placed by Provider or its assigns upon the Software. All references in this subparagraph to assignment shall be deemed also to include any pledge, mortgage, transfer or other disposition. Subject always to the foregoing provisions of this section, this Contract shall inure to the benefit of, and shall be binding upon, the successors and assigns of the parties hereto and, where appropriate, their heirs, legatees and personal representatives. The Provider will provide Customer with no less than a ninety (90) calendar day notice of impending cessation of its business.

56. Notices. Any and all notices ("Notices") which either party hereto may desire to give to the other party hereunder shall be deemed to be duly given if and only if mailed by registered or certified mail, postage prepaid, addressed to the other party at its address as set forth below or at such other address as such party may designate to the other party in writing from time to time. Notification by any other means shall be considered a service request and a waiver of any related breach of contract dispute until such time as the party provides notice in accordance with this paragraph.

If to Provider: GL Suite, Inc.
PO Box 595
Kalispell, MT 59903

If to Customer: Mailing address identified by Customer
on Customer's public web site.

57. Execution. This contract is executed by any of the following methods:
(a) Acceptance of an offer from Provider and incorporation as a counterpart into a contract executed by the parties, or
(b) Use of the Software without another superseding contract between the parties, or
(c) Issuance of a purchase order for a GL Simple plan, or
(d) The execution of this contract below:

GL Suite, Inc.

By _____

Signature, Title

Date

Customer

By _____

Signature, Title

Date