

AI-Powered Workflow Mapping & Analytics Services

MASTER AGREEMENT

This Master Agreement (“Master Agreement”) is between Procurement Professionals Alliance, an Arizona-based non-profit corporation, on behalf of its RFXPremier cooperative contracting division (“PPA/RFXP”), and Klarity Intelligence, Inc., whose primary business address is 55 2nd Street, Floor 23, San Francisco, CA 94105 (“Contractor”). PPA/RFXP and Contractor may each be referred to as a “Party” and collectively as “Parties.”

BACKGROUND

- A. PPA/RFXP seeks to establish a cooperative contracting relationship with Contractor to provide goods and services to non-profit, private, and public purchasing entities.
- B. This Master Agreement sets forth the terms and conditions under which Contractor will supply such goods and services to these entities through the PPA/RFXP program.

The Parties agree as follows:

I. Term of Agreement

- 1.1 **Effective Date.** This Master Agreement is effective upon the date of last signature.
- 1.2 **End Date.** This Master Agreement will continue for a period of two years, unless otherwise terminated by either Party in writing.
- 1.3 **Termination.** Either Party may terminate this Master Agreement upon breach by the other party, subject to thirty (30) days’ written notice and opportunity to cure. Notwithstanding the expiration or termination of this Master Agreement, each Party shall perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination.

II. Cooperative Purchasing Mechanism

- 2.1 **Marketing and Administration.** PPA/RFXP shall market and administer this Master Agreement as a convenient and cost-effective contracting vehicle for use by states, territories, counties, cities, and other political subdivisions,

higher education, K-12, healthcare, tribal, and nonprofit organizations (“Eligible Entities”).

2.2 Annual Contract Performance Review. Contractor shall participate in an annual contract performance review with PPA/RFXP.

2.3 Logo Use. The PPA/RFXP logos may not be used by Contractor in sales and marketing until a separate logo use agreement is executed with PPA/RFXP.

2.4 No Representations. The Contractor shall not make any representations concerning PPA/RFXP or any purchaser as to the quality or effectiveness of the goods or services provided herein, without prior written consent.

III. Purchasing and Contract Administration

3.1 Goods and Services. Contractor will provide the goods and services to Eligible Entities as set forth in Exhibit B, as attached and incorporated herein.

3.2 Pricing. The prices contained in Exhibit B represent the not-to-exceed price Offered by Contractor. All prices and rates must be guaranteed for the initial term of the Master Agreement.

3.3 Shipping. Any physical deliveries will be F.O.B. destination. All shipping costs must be clearly set forth in the purchase order and pre-approved by Buyer.

3.4 Purchase Orders. Contractor shall require all nonprofit, private, or public entities purchasing under this Master Agreement (“Buyers”) to include the following language in each purchase order: “Buyer shall hold Procurement Professionals Alliance harmless and, to the extent permitted by law, shall indemnify Procurement Professionals Alliance and RFXPremier from all third-party claims or causes of action, arising from goods and services acquired under this Purchase Order.”

3.5 Applicability of Master Agreement. RFXPremier Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. Any such alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the

consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g., purchase order or contract) used by the Purchasing Entity to place the Order.

3.6 Administrative Fee. Contractor shall pay PPA a fee for management and marketing of the Master Agreement (“Administrative Fee”) equal to one percent (1% or 0.01) of each sale of products or services under this Master Agreement no later than sixty (60) days following the end of each calendar quarter. The Administrative Fee applies to the cost of the goods and services, less any charges for taxes or shipping. The PPA/RFxP Administrative Fee is not negotiable and must be included in the overall cost provided to the Buyer and not shown as a separate line item.

3.7 Sales Data Reporting. Contractor shall report to PPA/RFxP all sales made under this Master Agreement which Contractor has invoiced and received payment for, including orders for personal use, if applicable (“Sales Data”).

3.7.1 Summary Sales. Contractor shall provide a summary of the Sales Data (“Summary Sales Data”) using a reporting tool or template provided by PPA/RFxP. Contractor shall provide PPA/RFxP with Summary Sales Data each calendar year quarter, no later than thirty (30) days following the end of the quarter. If Contractor has no reportable Sales Data for the quarter Contractor shall submit a zero-sales report.

3.7.2 Detailed Sales. Within sixty (60) days following the end of each calendar year quarter, Contractor shall provide PPA/RFxP with detailed sales Data, including but not limited to customer information, Order information, and line-item ordering detail (“Detailed Sales Data”). PPA/RFxP will work collaboratively with Contractor to determine the appropriate data and means of reporting.

IV. Indemnification, Limitation of Liability and Insurance

4.1 General Indemnification. The Contractor shall defend, indemnify and hold harmless PPA and PPA/RFxP along with their officers and employees, from and against any third-party claims, damages, or causes of action, including reasonable attorneys’ fees and related costs, for any death, injury, or damage to tangible property arising from the sale or use of any product or service sold under this Master Agreement.

4.2 Insurance. Contractor shall, during the term of this Master Agreement, maintain in full force and effect, commercial insurance sufficient to cover its obligations, including indemnity, contained in this Master Agreement.

4.3 Limitation of Liability. In no event will either party be liable for any consequential, indirect, special, or incidental damages such as damages for lost profits, business failure or loss, arising out of this Master Agreement, whether or not such party has been advised of the possibility of such damages. Except with respect to Contractor's indemnification obligations, Contractor's entire liability shall be limited to and shall not exceed two (2) times the amount paid to Contractor by the purchasing entity in the 12 months preceding the act or omission giving rise to the claim, or \$2,000,000, whichever is greater. With respect to Contractor's indemnification obligations including under Exhibit A (AI Solutions Addendum), Contractor's entire liability shall be limited to and shall not exceed four (4) times the amount paid to Contractor by the purchasing entity in the 12 months preceding the act or omission giving rise to the claim, or \$10,000,000, whichever is greater. Notwithstanding the foregoing, the limitations set forth in this Section shall not apply to: (i) Contractor's fraud, gross negligence, or willful misconduct; (ii) Contractor's knowing or intentional misuse of purchasing entity data; or (iii) amounts that cannot be limited under applicable law.

V. General Provisions

5.1 Confidentiality. Parties may have access to information that is confidential, proprietary, or trade secret, including information provided by the other Party, as well as by Buyers, which may also include information on individuals ("Confidential Information"). Parties acknowledge that any unauthorized disclosure or use of the Confidential Information may cause irreparable harm and loss to the disclosing party or other individuals. Therefore, Parties shall (a) use Confidential Information for the sole purpose of performing under this Agreement, (b) limit dissemination of Confidential Information to only those employees and representatives who have a need to know the Confidential Information, and (c) not disclose the Confidential Information to any other person or entity without the approval of disclosing Party or Buyer, if applicable.

5.2 Amendments. This Agreement may only be amended or modified in writing upon agreement by both Parties.

5.3 Assignment. Neither Party may assign its rights or delegate its duties under this Agreement without the prior written consent of the other Party.

5.4 Notice. All notices concerning enforcement, modification, amendment, interpretation, or dispute resolution of this Agreement must be in writing and be delivered to the other Party's signatory to this Agreement.

5.5 Dispute Resolution. In the event of a dispute concerning this Agreement, Parties shall attempt to resolve the dispute in good faith through non-binding mediation prior to any formal legal action.

5.6 Severability. If any provision of this Agreement is deemed to be invalid or unenforceable, the remainder of this Agreement will not be affected and will be enforced to the greatest extent permitted by law.

5.7 Waiver. The waiver of either Party of a breach, default, delay, or omission of any of the provisions of this Agreement by the other Party shall not be construed as a waiver of any subsequent breach of the same or other provisions.

5.8 Governing Law, Jurisdiction, and Venue. Any claim or cause of action must be brought in a court of competent jurisdiction within the Commonwealth of Kentucky, Fayette County, and will be subject to Kentucky law, without regard to its choice of law provisions.

5.9 Warranties. Contractor warrants for a period of one year from the date of acceptance that: (a) the Product performs according to all specific claims that Contractor made in its response to the solicitation, (b) the Product is designed and manufactured in a commercially reasonable manner, and (c) the Product is free of material defects.

Notwithstanding the warranties set forth above, Contractor does not warrant that any AI-enabled features or outputs generated through the Product will be error-free or will achieve any specific result or outcome. Except as expressly set forth in this Master Agreement, Contractor makes no additional warranties with respect to AI-generated outputs, including warranties of accuracy, completeness, or fitness for a particular purpose; provided, however, that nothing in this section shall be construed to limit or disclaim Contractor's express warranties regarding Product performance, workmanship, or freedom from defects as set forth in this Agreement.

5.10 Survivability. Survivability. Sections 3.6, 3.7, 4.1, 4.3, 5.1, 5.4, 5.5, 5.6, 5.7, 5.9 and 5.10 will survive expiration or termination of this Agreement.

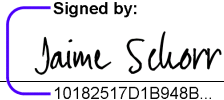
REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

The Parties accept the terms of this Agreement as of the dates set forth below.

For PPA:

Name: Jaime Schorr

Title: Chief Growth Officer

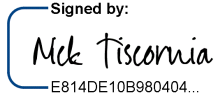
Signature:  Signed by:
Jaime Schorr
10182517D1B948B...

Date: 3/5/2026

For Contractor:

Name: Nick Tiscornia

Title: Chief Business Officer

Signature:  Signed by:
Nick Tiscornia
E814DE10B980404...

Date: 2/24/2026

Exhibit A: Terms and Conditions for AI Solutions

This Addendum defines special requirements agreed to by RFXPremier and Contractor regarding the AI system and/or subsystem provided as part of the Contract.

This Addendum governs over any contrary license terms and RFXPremier will not agree to any terms that conflict with the Addendum. Failure of the Contractor to comply with the terms of this Addendum shall constitute a material breach of the Contract.

1. Definition of AI System

This Contract defines “artificial intelligence” or “AI” to be a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. ¹ AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

This Contract defines an “AI system” to be any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

2. Risk Mitigation

The Contractor represents that the AI system performs substantially in accordance with its documentation and according to all specific claims that the Contractor made in its response to the solicitation and has been developed and will perform in a manner that is in compliance with all applicable laws and regulations.

The Contractor shall maintain and implement a Risk Management Plan that complies with accepted risk management frameworks, such as the NIST AI Risk Management Framework², ISO 42001³, or SOC 2 Type II. Upon reasonable request, Contractor shall provide sufficient documentation or attestations to demonstrate compliance, without disclosure of confidential, proprietary, or security-sensitive information.

The Contractor shall work with the Eligible Entity to evaluate and minimize risks posed by the AI system.

AI Incident Response

In the event of an AI incident, at the request of the Eligible Entity, the Contractor shall thoroughly investigate their systems of any suspected AI incident and promptly report findings to the Agency. An “AI incident” is an alleged or reasonably suspected harm or near

harm event to people, property, reputation, technical integrity of the environment where an AI system is implicated. Examples of AI incidents include providing false information, copyright infringement, generating harmful bias, system misuse, exposure of sensitive information, and liability risk.

Remediation

At the Eligible Entity's request, the Contractor will without undue delay discontinue the use of any AI system involved in providing services to the Eligible Entity. If (i) the Eligible Entity reasonably determines that the AI system is in violation of one or more of the requirements enumerated in Section 3: Requirements for Contractors when Operating AI System(s), or (ii) the Contractor does not promptly resolve an AI incident, then the Eligible Entity will provide the Contractor with notice that they have 30 calendar days to promptly assess and resolve the issue. Potential methods to address such issues include, without limitation, changing the behavior of the AI system or subsystem; supplementing the system or subsystem to achieve the necessary outcomes; replacing the system with a non-AI system that meets the Eligible Entity's needs; or limiting the function of the AI system or subsystem. After 30 calendar days, the Contractor must provide evidence that the AI system is adequately fixed and ready for re-deployment, or that the AI system is not suitable for use.

Indemnification

Contractor agrees to indemnify, defend, and hold harmless RFXPremier and/or Eligible Entities regarding any third-party action rising out of or related to (1) any breach of any representation, warranty, or obligation of Contractor contained in this Addendum; (2) any act or omission of the Contractor related to the provision of an AI system; and (3) any actual or alleged infringement or violation of intellectual property rights arising from the AI system or Contractor's software, except to the extent such claim arises solely from Eligible Entity data or modifications not authorized by Contractor. This indemnification obligation applies regardless of whether the relevant claim has merit.

3. Requirements for Contractors AI System(s)

To the extent permissible by law, the Contractor shall adhere to the following requirements in the course of doing business with or for RFXPremier and/or the Eligible Entity:

1 Definition from 15 U.S.C. 9401(3)

2 <https://www.nist.gov/itl/ai-risk-management-framework>

3 <https://www.iso.org/standard/81230.html>

1. Updates: Contractor attests that the previously completed AI FactSheet accurately represents the AI system (See Exhibit C A: AI FactSheet). Contractor shall provide prior notice for system upgrades that substantially impact the services provided to the Eligible Entity. Contractor commits to update the AI FactSheet upon request on an annual basis and within 30 calendar days of any change to the AI system that substantially impacts the services provided to the Eligible Entity. Example of a substantial impact includes, but is not limited to, changes to: sensitive or protected information used in the system, compatibility with the Eligible Entity's other systems, or decisions that impact the rights or safety of individuals. In the event of a change with a substantial impact, vendor will provide the Eligible Entity an opportunity to stay on the existing system version at the Eligible Entity's request. Any updates made to the AI system that render the AI system unserviceable to the Eligible Entity to provide services defined in the Contract, as reasonably determined by the Eligible Entity, may be cause for termination by the Eligible Entity.

2. Data ownership: The Eligible Entity retains ownership of any data it provides to the Contractor, as well as data collected or generated specifically on behalf of the Eligible Entity during the course of the Contract. The Contractor retains ownership of all other data it collects or generates, including data created for the Contractor's general business purposes. The Eligible Entity has the unrestricted right to use its owned data for any purpose. Ownership of such data shall not be transferred to the Contractor or any third party without prior written consent from the Eligible Entity.

3. Data portability: At the Eligible Entity's request, and at no additional cost, the Contractor shall provide all data owned by the Eligible Entity in a format that is easily usable by the Eligible Entity and, to the extent technically feasible, in a structured, commonly used, machine-readable format. The Contractor is not obligated to provide such data more than twice in a 12-month period.

4. Authorized use: Data owned by the Eligible Entity cannot be used for other commercial applications without written consent from the Eligible Entity.

5. Data rights: Data owned by the Eligible Entity that contains sensitive or protected information must be able to be deleted, edited, or anonymized at the request of the Eligible Entity or the data subject.

6. Performance: Provide the Eligible Entity or entity working on behalf of the Eligible Entity with the means to monitor the performance, including the accuracy, of the AI system it uses and report this accuracy to the Eligible Entity.

7. Algorithmic bias: Contractor will provide the Eligible Entity with evidence that demonstrates that bias present in the AI system is effectively managed for the context in

which it will be deployed. Contractor shall provide information describing in detail how bias is assessed.

8. Human oversight: Provide the Eligible Entity the means for a human to evaluate and override outputs of the AI system. The human evaluator must be able to override the outputs of the AI system and take precedence over all outputs.

9. Explainability: Provide the Eligible Entity with an explanation of how the AI system generates outputs, including what factors influence the system's decisions, rule-based logic, training data sources, and probability-based decisions, at a level sufficient for transparency and accountability and without requiring disclosure of source code, proprietary algorithms, or model weights. The Eligible Entity holds the right to communicate its general usage of the AI system and explain its decision-making processes to the public.

10. Notice: If required by the Eligible Entity, provide written notice of the usage of the AI system to data subjects and/or end-users, preferably at the point of service.

11. Process: Contractor shall comply with existing local, state, and federal law for data access and decision appeals related to the use or operation of the system.

12. Ongoing Monitoring: Contractor shall regularly monitor the performance of the AI system to detect and rectify system behavior that violates any of the requirements in this section. Contractor shall promptly communicate the discovery of system behavior that violates any of the requirements in this section to the Eligible Entity, including the potential impact to services.

13. Training: Ensure that appropriate training is available to Eligible Entity staff who may operate the AI system, which may include how to:

1. Protect sensitive or personal information;
2. Mitigate harmful algorithmic bias;
3. Promote optimal performance;
4. Report system errors; and
5. Maintain service delivery if the AI system fails, to the extent possible.

14. Auditing: The Eligible Entity retains the right to observe, assess, or audit any relevant work processes, services, or documents in the course of doing business with the Eligible Entity to confirm that the Contractor (and any relevant sub-contractors) is complying with this Policy. Contractor shall provide access to information, documentation, and personnel

required to complete this audit at no additional cost to the Eligible Entity, during normal business hours and upon reasonable prior notice.

Exhibit B – Scope of Work

Klarity Architect™ 4.0 provides a configurable and scalable AI-powered platform that fully meets and exceeds the Scope of Work requirements for AI-Powered Workflow Mapping and Analytics Services.

Digital Process Mapping

Klarity Architect™ 4.0 enables rapid creation of dynamic, visual process maps that capture how work is actually performed across departments and functions. The platform supports both “as-is” and “to-be” workflows, allowing organizations to document current operations, design future-state improvements, and maintain version-controlled process documentation over time.

Workflow Automation

While Klarity does not replace core transactional systems, it enables workflow automation through standardized process definitions, structured handoffs, and governance controls. Klarity identifies automation opportunities, eliminates manual inefficiencies, and supports orchestration of workflows by aligning people, systems, and policies without requiring complex system reengineering.

Enterprise-Wide Data Capture

Klarity Architect™ 4.0 captures enterprise-wide workflow data through guided user inputs, structured metadata, and optional data imports. This approach enables broad participation across roles and departments while maintaining data consistency, governance, and traceability. The platform scales from individual departments to enterprise-wide deployments across multiple entities.

Secure Documentation

The platform provides centralized, secure creation and storage of process documentation, workflows, and analytics outputs. Role-based access controls, encryption at rest and in transit, and detailed audit logs ensure that documentation is protected and accessible only to authorized users, supporting public-sector security and compliance requirements.

Audit Trail Generation

Klarity Architect™ 4.0 automatically generates audit-ready records that track workflow versions, changes, approvals, and ownership. These audit trails support internal audits, external reviews, compliance reporting, and governance oversight by providing clear, traceable documentation of how processes are defined and managed.

Flexible Deployment

Klarity Architect™ 4.0 is delivered as a cloud-based solution designed for rapid deployment without deep IT integrations. The platform supports flexible configuration to accommodate organizations of varying size, complexity, and maturity. Deployment can be scaled incrementally, enabling participating entities to start small and expand as needs evolve.

Real-Time Analytics

The platform includes real-time analytics dashboards that provide visibility into workflow performance, bottlenecks, handoffs, and risk indicators. These analytics support data-driven decision-making and continuous improvement initiatives across the organization.

Compliance and Risk Management Tools

Klarity Architect™ 4.0 is purpose-built to support governance, compliance, and risk management. The platform highlights control gaps, process risks, and compliance dependencies while enabling transparent documentation aligned with regulatory and policy requirements. Explainable AI ensures insights are understandable and defensible in audit and oversight contexts.

Support for Evolving Requirements

Klarity Architect™ 4.0 is highly configurable and designed to adapt to changing business, regulatory, and operational requirements. Workflows, governance rules, and reporting can be updated without custom development, ensuring long-term flexibility and sustainability.

Cost

Category	Description	Proposed Cost	Metric / Definition
Platform License / Subscription	Annual per-user or per-entity platform license fees, including hosting and updates	up to 100 = \$175,000 101 - <u>250</u> = \$275,000 251 - 400 = \$375,000 401 - 600 = \$450,000 600 + = to be negotiated between both parties	Klarity pricing is based on <u>the Number</u> of people in the department or function being transformed. For example, Finance <u>org</u> at Financial Institution (~200 people) Note: per use pricing is available for those organizations with a Transformation Center of Excellence.
Implementation and Configuration	One-time cost for onboarding, customization, training, and migration	Included in subscription	See below for more details on our implementation, training and value realization managed services.
Support and Maintenance	Annual Maintenance, help desk, updates	Included in subscription	
Value-added Services	Hourly rate for <u>professional</u> services for consulting, training or expansion.	\$25,000-\$75,000 annually depending on project scope	See below for more <u>detail</u> related to our Value Realization Managed Service offering.
TOTAL			

Note: Pricing reflects Not to Exceed pricing. Specific end customer pricing to be negotiated based on customer specific scoping and appropriate sizing.

Additional Information

Implementation Resources:

Klarity Implementation Services are provided to ensure optimal time to value realization (TTVR). As part of the deployment, customers have access to an AI Delivery Lead and an AI Solution Specialist.

The AI Delivery lead is a subject matter expert in deploying Architect™ 4.0. They are accountable for aligning on value targets and realization. They are responsible for the customer relationship both during and after implementation.

The AI Solution Specialist drives the value realization plan and project management coordination. They're responsible for translating customer requirements into Architect-ready templates and prompts.

As part of the implementation, customers will also have access to our library of training assets.

No migration services are anticipated or included for our deployments.

Exhibit C – AI FactSheet

Vendor Name	Klarity Intelligence Inc
Product Name	Klarity Architect™ 4.0
Overview	Klarity Architect™ 4.0 is an AI-powered workflow mapping and analytics platform designed to help organizations understand, document, analyze, and improve how work is actually performed. The platform supports governance, compliance readiness, operational efficiency, and continuous improvement by combining structured process capture with explainable AI-driven insights.
Purpose	<p>Klarity Architect™ 4.0 enables organizations to:</p> <ul style="list-style-type: none"> • Capture and document “as-is” and “to-be” workflows • Identify inefficiencies, bottlenecks, handoff delays, and risk points • Support audit readiness, compliance, and transparency • Enable data-driven process optimization and governance <p>AI functionality supports analysis and insight generation; all final decisions remain under human control. Configurable features include workflow structure, analytics views, permissions, governance rules, and reporting outputs.</p>
Intended Domain	In addition to our private sector customers, Klarity has a focus on public sector, education, healthcare, nonprofit, and other regulated or governance-driven environments requiring transparency, auditability, and risk management.
Training Data	<p>Klarity Architect™ 4.0 uses a combination of:</p> <ul style="list-style-type: none"> • Proprietary, curated process data models • Aggregated, de-identified workflow metadata • Rule-based and supervised learning approaches <p>No customer-owned or sensitive data is used to train models without explicit authorization.</p>
Test Data	System performance is tested using controlled, representative workflow scenarios, synthetic datasets, and anonymized operational metadata. Testing includes validation across varying process complexities, organizational sizes, and governance contexts to ensure reliability, consistency, and explainability.
Model Information	<p>Klarity Architect™ 4.0 employs a combination of:</p> <ul style="list-style-type: none"> • Supervised learning models • Rule-based logic • Statistical and pattern-recognition techniques <p>Klarity Architect™ 4.0 integrates enterprise-grade foundation models from providers such as OpenAI, Anthropic, and Google within Klarity-</p>

	<p>controlled workflows that apply customer-specific logic, pattern recognition, and validation to ensure reliable outputs.</p> <p>All model usage is governed through Klarity’s AI Management System (AIMS), enforcing contractual controls for data protection, zero data retention, and restrictions on model training using customer data.</p>
<p>Update Procedure</p>	<p>Models and platform components are updated on a controlled, periodic basis. Customers are notified in advance of updates that materially impact functionality or outputs. Documentation is provided for each release, and customers may request to remain on a prior version if an update introduces substantial changes affecting governance or operations.</p>
<p>Inputs & Outputs</p>	<p>Inputs:</p> <ul style="list-style-type: none"> • User-defined workflow steps and metadata • Organizational role and handoff information • Optional imported documentation or datasets <p>Outputs:</p> <ul style="list-style-type: none"> • Dynamic process maps • Analytics dashboards • Identified bottlenecks, risks, and improvement opportunities • Audit-ready documentation and reports <p>The platform supports data import/export and lightweight integrations with commonly used enterprise tools.</p>
<p>Performance Metrics</p>	<p>Performance is measured using:</p> <ul style="list-style-type: none"> • Workflow completeness and consistency • Identification accuracy of bottlenecks and handoffs • User validation and acceptance rates • System responsiveness and availability <p>Users can monitor performance through dashboards and reports and validate or override AI-generated insights.</p>
<p>Bias</p>	<p>Klarity Architect™ 4.0 is designed in alignment with recognized best practices for algorithmic bias detection and mitigation, such as those described in the Brookings Institution’s framework for algorithmic bias mitigation. This framework recommends proactive identification of bias sources, bias impact assessments, inclusive design, and cross-functional mitigation practices. Brookings+1</p> <p>Our bias strategy for Klarity Architect™ 4.0 reflects these principles:</p> <ul style="list-style-type: none"> • Bias Awareness and Definitions: We recognize that bias can arise from data representativeness, unanticipated use cases, or model design assumptions. While Klarity predominantly analyzes structured workflow and operational data (not sensitive demographic traits), we nonetheless design processes to detect

	<p>potential patterns that may systematically disadvantage groups, functions, or outcomes.</p> <ul style="list-style-type: none"> • Human-in-the-Loop Oversight: All AI-generated insights and analytics outputs are reviewed and interpreted by subject matter experts, ensuring human accountability and judgment. This human-centered review aligns with recommended bias mitigation practices that place oversight and decision authority with trained users. • Cross-Functional Review: Bias assessment and mitigation involve cross-functional teams during design, testing, and deployment phases, consistent with self-regulatory best practices that advocate inclusive participation and process review. Silicon Flatirons • Transparency and Explainability: Klarity provides transparent, explainable outputs and decision logic that allow users to understand how analytics were derived and to identify any patterns that could indicate bias. • Continuous Monitoring and Feedback: We incorporate ongoing monitoring of outputs to identify anomalies or patterns that could reflect bias in results, combined with mechanisms for users to provide feedback and correct flagged issues. <p>Klarity does not use protected class attributes (e.g., race, gender, etc.) in its analytics models, and it does not make autonomous decisions about individuals or groups. Where any analytic patterns might intersect with sensitive data (e.g., imported data from customer systems), customers are responsible for managing data governance and ensuring compliance with applicable laws and policies. Through these design principles and ongoing governance processes, Klarity aligns with the Brookings best practices for algorithmic bias detection, mitigation, and reporting.</p>
Robustness	The system handles outliers by flagging anomalous workflows or data patterns for human review rather than making automated determinations. User overrides and corrections are incorporated to refine future system behavior and improve analytical accuracy.
Optimal Conditions	The model performs best when workflows are clearly defined with sufficient process detail and participation from subject matter experts. Accuracy improves as more validated workflow data is captured over time.
Poor Conditions	Performance may be limited when workflows are incomplete, inconsistently defined, or lack stakeholder input. The system does not generate autonomous decisions and may surface incomplete insights if provided data is insufficient.
Explanation	Klarity Architect™ 4.0 provides explainable outputs through visual process maps, annotated analytics, and clear descriptions of contributing factors. Outputs are designed to be understandable by

	business users, auditors, compliance professionals, and leadership.
Data Protection	Klarity complies with recognized data protection frameworks and best practices, including alignment with NIST security principles. Controls include encryption at rest and in transit, role-based access, audit logging, and U.S.-based data hosting.
Ongoing Monitoring	System performance is continuously monitored to detect errors, anomalies, or unintended behavior. Users can override AI-generated insights, and such overrides are used to improve future system performance and reliability.
Independent Evaluation	Internal validation and testing are conducted to assess accuracy, consistency, and reliability. Documentation is available upon request. Klarity supports customer-led or third-party reviews as required by participating entities.
Accessibility	Klarity Architect™ 4.0 is designed to support accessibility best practices, including intuitive navigation, readable interfaces, and compatibility with assistive technologies where applicable.
Responsible AI Strategy	<p>Klarity maintains a responsible AI strategy grounded in transparency, human oversight, strong data stewardship, and risk-based controls including formal governance of third-party AI services used within the platform.</p> <p>This strategy is operationalized through Klarity’s AI Management System (AIMS), which is designed in alignment with the NIST AI Risk Management Framework (NIST AI RMF) and maps AI governance, risk identification, measurement, and mitigation practices across the full AI lifecycle.</p>