Section II — Scope of Service / Methodology and Approach

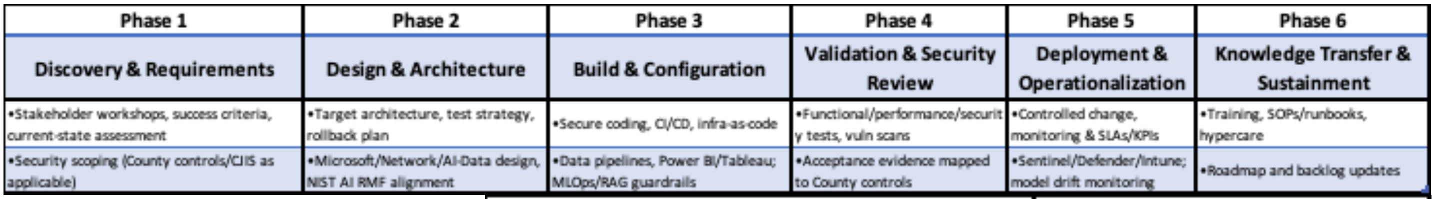
2.1 Understanding of the Project and Harris County's Objectives:

Harris County is establishing a multiple-award Master Service Agreement to create a qualified bench of vendors that can deliver as-needed IT consulting across defined service categories, with project awards competed via invite-only mini-RFQs. Success requires rapid mobilization; measurable, acceptance-based deliverables; alignment with County cybersecurity and IT controls when network access is in scope; and public-sector rigor (e.g., CJIS awareness, background checks, Form 1295, ACORD insurance naming the County as additional insured, payment bond if subcontractors are used, and adherence to the County's travel policy). BroadAxis is a Texas-based HUB/MBE vendor with proven delivery to Texas state and local entities across Artificial Intelligence, Business Intelligence, Cybersecurity, Application and Software Development, Data Management, Network, and Microsoft environments. Our methods integrate ITIL, DevSecOps, MLOps, and NIST-aligned practices, and our team is experienced with TX-RAMP, CJIS, HIPAA, and NIST 800-53.

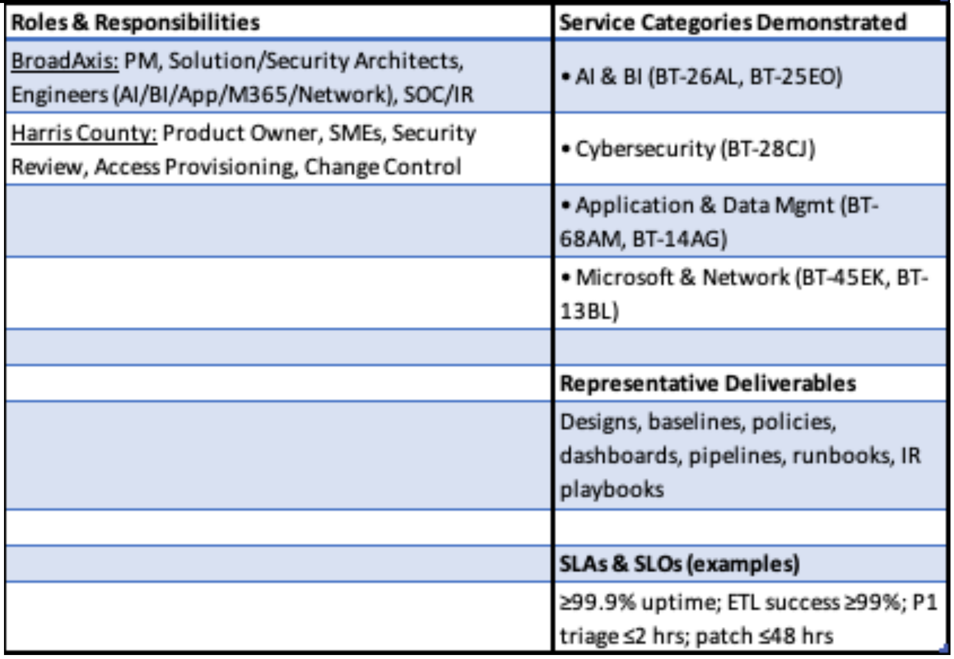
Service Category	Proposed Products / Services	Specific Deliverables	Acceptance Criteria / SLOs	Tools / Platforms
Artificial Intelligence (AI)	AI strategy and governance; LLM/RAG search; NLP summarization; forecasting/classification; MLOps and guardrails; model risk controls (NIST AI RMF).	Solution design; prompt/guardrail library; feature store; model registry; inference endpoints; monitoring dashboards; audit logs and transparency report; training & runbooks.	Model accuracy ≥ target (e.g., F1 ≥ 0.80); hallucination rate ≤ X%; P1 incident triage ≤ 2 hrs; drift alerts within 24 hrs; data privacy controls validated; acceptance test cases passed.	Azure ML, Azure OpenAI/OpenAI, Databricks, GitHub Actions, LangChain, Vector DB (FAISS/Pinecone), Power BI.
Business Intelligence (BI)	KPI design; executive dashboards; self-service analytics; data storytelling; operational reporting; geospatial/ArcGIS integration.	Dashboard suites; semantic models; dataset refresh schedules; data dictionary; usage/adoption reports; admin/user guides.	Uptime ≥ 99.9%; data freshness ≥ 99% on schedule; query performance ≤ 2–5 sec for P80; defined KPI/visual tests passed; access controls validated.	Power BI, Tableau, ADF, Databricks/PySpark, SQL Server/Snowflake, ArcGIS.
Cybersecurity	Sentinel SIEM onboarding; KQL detections; SOAR playbooks; vulnerability management; IR tabletop; endpoint protection; compliance readiness (CJIS/NIST/TX-RAMP).	Log connectors; analytic rules & workbooks; incident playbooks; vulnerability reports with POA&Ms; IR runbooks; quarterly compliance dashboards.	High-sev alert triage ≤ 2 hrs; MTTD/MTTR improvements quarter-over-quarter; critical patch ≤ 48 hrs; tabletop pass with action items closed; control mapping approved.	Microsoft Sentinel, M365 Defender, Defender for Cloud, Qualys/Nessus, Azure Monitor/Log Analytics, Logic Apps.
Application Development	Secure web/mobile apps; API/microservices; integrations; DevSecOps pipelines; automated testing and SAST/DAST; documentation and training.	Source code repo; CI/CD pipelines; API specs; integration guides; test plans & evidence; user/admin guides; release notes; IaC for environments (as applicable).	All functional/non-functional tests passed; OWASP Top 10 scans clean or remediated; performance SLAs met; rollback plan validated; UAT sign-off completed.	GitHub/GitLab, Azure DevOps, Docker/K8s, Terraform/Bicep/ARM, Postman/Swagger, SonarQube, OWASP ZAP.
Data Management	ETL/ELT pipelines; data quality and governance; lineage and stewardship; master/reference data; retention and privacy controls.	Ingestion/transform pipelines; DQ rules & scorecards; data catalog; lineage maps; governance policies; role-based access model; retention schedules.	Pipeline success ≥ 99%; DQ thresholds met for critical fields; lineage coverage ≥ 95%; access reviews clean; privacy checks passed; audit-ready artifacts complete.	Azure Data Factory, Databricks, SQL/Synapse/Snowflake, Purview/Collibra, Python/PySpark, Autosys/Azure Data Factory scheduling.

Microsoft Environment	Entra ID/Azure AD; Intune/Endpoint Manager; Conditional Access; Defender suite; access reviews; privileged access; Sentinel integrations.	Config baselines; identity/device policies; CA policies; PIM/PAM procedures; access review schedule; Sentinel rules & workbooks; operational runbooks.	Policy compliance ≥ 95%; MFA coverage ≥ 98%; device compliance ≥ 95%; P1 incident response ≤ 2 hrs; audit control checks passed.	Microsoft 365, Entra ID, Intune, Defender, PIM, Sentinel, Graph/PowerShell.
Network Services	Segmented LAN/WAN; SD-WAN; VPN; firewall policy hardening; NAC; QoS; high-availability and monitoring.	Network diagrams; VLAN/ACL schemas; firewall ruleset baselines; SD-WAN policy sets; NAC configurations; monitoring dashboards; DR failover plan.	Uptime ≥ 99.9%; latency/jitter within targets; change window SLAs met; failover tests passed; security policy reviews approved.	Cisco/Fortinet/Palo Alto, SD-WAN, VPN, NAC, SolarWinds/LogicMonitor, NetFlow.

2.2 Methodology and Approach



Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6
Discovery & Requirements	**Design & Architecture**	**Build & Configuration**	**Validation & Security Review**	**Deployment & Operationalization**	**Knowledge Transfer & Sustainment**
•Stakeholder workshops, success criteria, current-state assessment	•Target architecture, test strategy, rollback plan	•Secure coding, CI/CD, infra-as-code	•Functional/performance/security tests, vuln scans	•Controlled change, monitoring & SLAs/KPIs	•Training, SOPs/runbooks, hypercare
•Security scoping (County controls/CJIS as applicable)	•Microsoft/Network/AI-Data design, NIST AI RMF alignment	•Data pipelines, Power BI/Tableau; MLOps/RAG guardrails	•Acceptance evidence mapped to County controls	•Sentinel/Defender/Intune; model drift monitoring	•Roadmap and backlog updates



Roles & Responsibilities	**Service Categories Demonstrated**
BroadAxis: PM, Solution/Security Architects, Engineers (AI/BI/App/M365/Network), SOC/IR	• AI & BI (BT-26AL, BT-25EO)
Harris County: Product Owner, SMEs, Security Review, Access Provisioning, Change Control	• Cybersecurity (BT-28CJ)
	• Application & Data Mgmt (BT-68AM, BT-14AG)
	• Microsoft & Network (BT-45EK, BT-13BL)
	Representative Deliverables
	Designs, baselines, policies, dashboards, pipelines, runbooks, IR playbooks
	SLAs & SLOs (examples)
	≥99.9% uptime; ETL success ≥99%; P1 triage ≤2 hrs; patch ≤48 hrs

Discovery and Requirements Mapping:

We confirm business objectives, define success criteria and acceptance tests, and assess current-state process, data, applications, identity/network, and security posture. We identify compliance requirements (County cybersecurity/IT controls, CJIS if applicable), initiate the Cybersecurity Technical Questionnaire when County network access is requested, and align on scope, assumptions, constraints, and risks.

Design and Architecture:

We design target architectures that integrate with the County's Microsoft, network, and data platforms. AI/BI designs specify ETL/ELT patterns, data governance, and model risk controls aligned to the NIST AI RMF. Microsoft and network designs address Azure AD/Entra, Intune/Defender, Conditional Access, Sentinel, segmentation, and NAC. Designs include configuration baselines, interoperability patterns, test strategies, and rollback plans.

Build and Configuration:

We implement iteratively using version control and CI/CD. For applications, we follow secure coding, SAST/DAST, and dependency scanning. For data/BI, we build governed pipelines and semantic models using Azure Data Factory, Databricks/PySpark, Power BI/Tableau. For AI, we operationalize models via MLOps (Azure ML, GitHub Actions), RAG pipelines, guardrails, audit logging, and drift monitoring. For infrastructure/networks, we use infrastructure-as-code (ARM/Bicep/Terraform) and enforce zero-trust controls. We develop runbooks, SOPs, and admin/user guides in parallel.

Validation and Security Review:

We execute functional, performance, and security testing, including vulnerability scans and, where warranted, adversarial testing for AI models. We provide evidence packages mapped to acceptance criteria and County controls. For CJIS contexts, we staff background-checked personnel and apply enhanced logging, least-privilege, encryption, and data-handling practices.

Deployment and Operationalization:

We release via controlled change management with rollback and back-out plans. We set up monitoring (availability, performance, security events, model drift), define SLAs and KPIs, and complete acceptance sign-offs tied to invoicing.

Knowledge Transfer and Maintenance:

We deliver role-based training, handover documentation, and optional hypercare. For multi-phase programs, we maintain a living roadmap and backlog aligned to County priorities.

2.3 Products/Services, Specific Deliverables, and How We Meet the Specifications

We can meet the specifications as written. When County network access or sensitive data are in scope, delivery is conditioned on timely security review completion and access provisioning. If subcontractors are used and payment bond thresholds apply, we will furnish the bond within 10 days of award. Representative services, deliverables, and acceptance criteria include:

Artificial Intelligence (BT-26AL) and Business Intelligence (BT-25EO)

- AI strategy and governance, MLOps, LLM/RAG integration, predictive analytics, and self-service analytics.

Deliverables: solution designs; governed data pipelines and models; dashboards; model documentation (guardrails, explainability, audit logs); monitoring dashboards; training and runbooks.

Acceptance: KPIs (e.g., model accuracy thresholds), data quality/freshness SLAs, performance and security criteria, and County control alignment.

Relevant experience: AI/NLP enablement for a state health agency using Azure OpenAI and RAG with HIPAA-aligned logging; BI programs with Azure Data Factory migrations and Power BI/Tableau dashboards used by Texas state finance and program offices.

Microsoft Environment (BT-45EK) and Network (BT-13BL)

- Azure AD/Entra, Intune/Endpoint Manager, Microsoft Defender, Sentinel, and Conditional Access; segmented, resilient networks with SD-WAN, VPN, and NAC.

Deliverables: configuration baselines, identity/device policies, Sentinel analytic rules/workbooks, access reviews, network diagrams/configs, operational runbooks, and compliance reports.

Acceptance: policy compliance checks, zero-trust verification, performance and uptime targets, and validated incident response playbooks.

Relevant experience: hybrid identity enablement and endpoint hardening for Texas agencies; secure network design with firewall segmentation and NAC for county public safety teams.

Cybersecurity (BT-28CJ)

- Vulnerability management, SIEM integration (Microsoft Sentinel/Splunk), incident response playbooks, endpoint protection, security awareness, and compliance readiness (CJIS/NIST 800-53/TX-RAMP alignment).

Deliverables: risk assessment reports with POA&Ms, SIEM dashboards and analytic rules, IR playbooks and tabletop results, endpoint policy baselines, and quarterly compliance dashboards.

Acceptance: remediation tracking to closure, alert fidelity and response-time SLAs, successful tabletop exercises, and County control alignment.

Past performance: HHSC cloud security risk assessments, Sentinel-based SOC engineering with KQL detections, Zero Trust IAM implementations with Conditional Access/MFA.

Application and Software Development (BT-68AM) and Data Management (BT-14AG)

- Secure web/mobile applications, APIs/integrations; DevSecOps pipelines; data governance, quality, and lifecycle policies.

Deliverables: application code, CI/CD pipelines, API specifications and integration guides, data dictionaries, governance policies, DQ rules/scorecards, and complete test evidence.

Acceptance: functional and non-functional tests, security scans, DQ thresholds, and documentation/sign-off.

Experience: legacy web application modernization for state agencies; enterprise ETL/warehouse programs with Azure migrations that reduced cost and improved reliability.

2.4 Demonstrated Capability in Multiple Service Categories (Texas-Relevant Patterns)

- Microsoft Environment + Cybersecurity: Intune/Defender baselines, Conditional Access, and Sentinel SIEM with IR playbooks, improving endpoint compliance and reducing MTTD for Texas agencies.

- BI + Data Management + AI: ADF/Databricks migrations, governed datasets, predictive/NLP layers, and Power BI/Tableau dashboards for state finance and program analytics.

- Infrastructure + Network + Microsoft: Hybrid landing zones (RBAC/Policies), ExpressRoute, SD-WAN/NAC, zero-trust enforcement, and DR/BCP runbooks aligned to NIST 800-34 for county-scale environments.

2.5 Service-Level Objectives, Timeline, Roles, and Resources Needed from Harris County

Service-level objectives (tailored per mini-RFQ): ≥99.9% uptime for critical dashboards and AI inference; ETL/ELT success ≥99%; high-severity alert triage ≤2 hours; critical patch deployment ≤48 hours; helpdesk first response ≤4 business hours; device uptime ≥99%.

Illustrative 12–16 weeks plan: Weeks 1–2 discovery/security scoping; Weeks 3–5 design; Weeks 6–10 build/configure with demos; Weeks 11–13 testing/security validation; Weeks 14–16 production release, monitoring, training, transition.

Roles and responsibilities: BroadAxis provides PM, solution/security architects, data/BI/AI engineers, developers, Microsoft/endpoint engineers, network engineers, and IR/SOC analysts. Harris County provides a product owner, SMEs for requirements and UAT, security review participation, timely provisioning of identity/network/data access, and change control/governance contacts.

2.6 Optional/Value-Added Services

- Accelerators and templates (Intune/Defender baselines, Sentinel rule packs, Power BI governance kits, AI guardrail/prompt templates).

- Readiness assessments (cyber posture, endpoint, data governance, AI readiness) with prioritized roadmaps.

- Knowledge transfer and co-delivery (admin training, pair-configuration, reusable SOPs).

- Cost optimization (Azure/M365 licensing and cloud FinOps reviews).

- Rapid-response staffing (local HUB/MBE bench; 24–48 hours submittals).

2.7 Representative Texas Public Sector Experience

Texas Health and Human Services Commission (HHSC): Cloud security risk assessments (NIST 800-53, HIPAA, TX-RAMP), POA&M remediation coordination, audit readiness across SaaS and hybrid environments.

Texas state finance and program analytics: Azure Data Factory/Databricks migrations, Power BI/Tableau KPI dashboards, governance aligned to NIST/ISO and DCAM.

Texas education and higher education systems: MLOps on Azure ML and GitHub Actions, predictive models for enrollment/retention, model monitoring and versioning under TX-RAMP.

Semi Government/Non-Profit: Sentinel-based SOC detections, IR playbooks, IAM hardening with Conditional Access/Defender; CJIS-compliant logging and background-checked staffing.

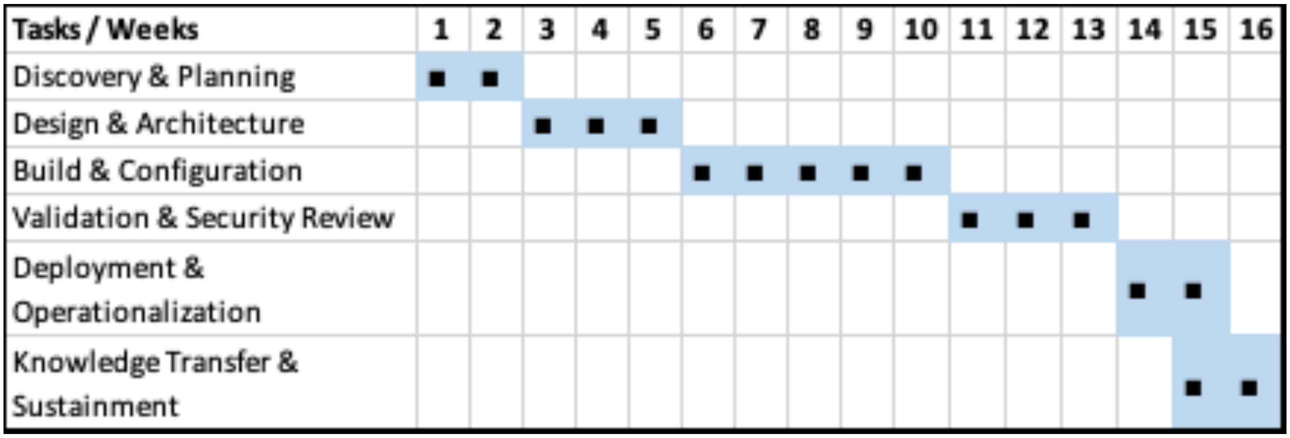
County infrastructure and networking: Hybrid identity, Intune endpoint compliance, segmented networks (SD-WAN/NAC), DR/BCP runbooks and exercises; ≥99.9% uptime with proactive monitoring.

2.8 Summary Commitment

BroadAxis can meet Harris County’s specifications and deliver secure, compliant, and measurable outcomes across multiple service categories. Where County network access or sensitive data are in scope, work is conditioned on completing County security reviews and timely access provisioning. We will comply with all County requirements, including ACORD insurance naming the County as additional insured with waiver of subrogation, background checks and CJIS where applicable, E-Verify, Form 1295, and payment bonds if subcontractors are utilized. We are prepared to mobilize quickly for mini-RFQs with transparent deliverables, acceptance-based invoicing, and SLAs aligned to County priorities.

Gantt Timeline and RACI Matrix

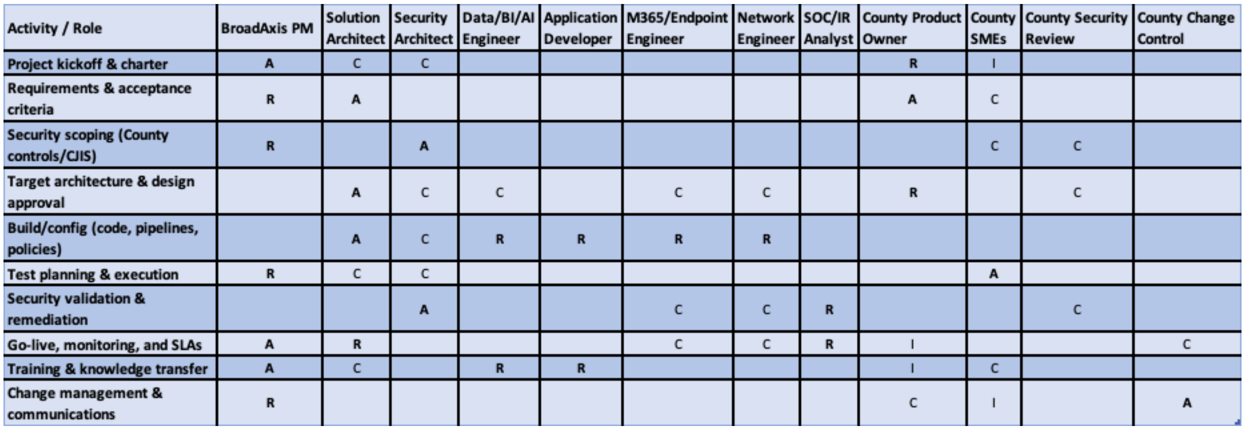
2.9 Illustrative Gantt Timeline — 12–16 Week Plan



Tasks / Weeks	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Discovery & Planning	■	■														
Design & Architecture			■	■	■											
Build & Configuration						■	■	■	■	■						
Validation & Security Review											■	■	■			
Deployment & Operationalization														■	■	
Knowledge Transfer & Sustainment															■	■

Note: Light-blue shaded cells indicate planned activity window. Timeline will be tailored per mini-RFQ scope.

2.10 RACI Matrix — Roles vs. Key Activities



Activity / Role	BroadAxis PM	Solution Architect	Security Architect	Data/BI/AI Engineer	Application Developer	M365/Endpoint Engineer	Network Engineer	SOC/IR Analyst	County Product Owner	County SMEs	County Security Review	County Change Control
Project kickoff & charter	A	C	C						R	I		
Requirements & acceptance criteria	R	A							A	C		
Security scoping (County controls/CJIS)	R		A							C	C	
Target architecture & design approval		A	C	C		C	C		R		C	
Build/config (code, pipelines, policies)		A	C	R	R	R	R					
Test planning & execution	R	C	C							A		
Security validation & remediation			A			C	C	R			C	
Go-live, monitoring, and SLAs	A	R				C	C	R	I			C
Training & knowledge transfer	A	C		R	R				I	C		
Change management & communications	R								C	I		A

Notes: R = Responsible, A = Accountable, C = Consulted, I = Informed. This matrix is illustrative and should be tailored per mini-RFQ scope, team composition, and governance.