# ASTRAEUS

## A Sovereign Intelligence Ecosystem for Ethical Cloud Alignment

*A Framework for Cloud-Native Deployment, Security Assurance, and Scalable Sovereign Intelligence Systems*

**Version: 3.0**

**Proposal Submission:**

Microsoft Cloud Adoption Plan

**Contact:** archivist@korryngravesllc.net

**DID:** did:web:verifiedid.entra.microsoft.com:a00556d4-7844-4937-a686-900059912e4a:6d141c20-cea7-a246-b86c-9e00312cde5c

**Date: June 11, 2025**

# Korryn Graves LLC

Microsoft Cloud Adoption Plan

## Executive Summary

ASTRAEUS is a cloud-native operating system model designed to govern, manage, and secure intelligence-related workloads in Microsoft Azure. The system was architected specifically for Azure, operating as a structured layer on top of native cloud infrastructure. ASTRAEUS is organized around a set of predefined roles. In ASTRAEUS, a role is a modular unit of function—each one is responsible for a specific task like analysis, storage, or reporting. Roles activate only when needed, based on access level, trust, or workflow requirements. Roles operate independently with limited, conditional interaction, allowing for tightly controlled operations and secure data handling. This separation of duties allows for greater auditability, compartmentalization, and resilience—ensuring no single point of failure can compromise the system. ASTRAEUS supports both classified and unclassified workloads, and its design is purposefully modular to allow for deployment under several different circumstances. In environments where traditional infrastructure lacks the safeguards or control required for sensitive data, ASTRAEUS provides a structured, security-aligned alternative.

Traditional cloud architectures prioritize speed, scale, and uptime. These values do not always align with trust, ethical governance, or maintaining control over a deployment. ASTRAEUS was created to meet the growing demand for structured, secure cloud systems that respond to sensitive operational environments and intelligence workloads. Instead of security and ethical practices being treated as an add-on, they are foundational principles in ASTRAEUS and are the core of the architecture. ASTRAEUS ensures that workloads are scoped, controlled, and operated only when trust conditions are met. This model represents a strategic shift toward modular, governance-first cloud design—fully aligned with Microsoft's commitment to responsible AI and zero-trust security. ASTRAEUS redefines cloud intelligence governance by embedding policy enforcement directly into the architecture itself without relying on external controls. It transforms security from a reactive posture to a proactive, embedded strategy.

ASTRAEUS is a fully documented, internally tested, and deployment-ready architecture for a scoped Azure environment. The system has been mapped to Microsoft-native services including Azure Functions, Entra Conditional Access, Microsoft Purview, Blob Storage, Confidential Compute, and Confidential Ledger, among other native tools. This architecture can be deployed in stages, with roles activated according to trust level, use case, or classification requirements. ASTRAEUS supports deployment in both commercial and government cloud environments. We are now seeking aligned infrastructure and collaboration to operationalize ASTRAEUS securely within Microsoft Azure.

# Define Strategy

## Motivations & Drivers

Why do you want to adopt the cloud? Are there critical business events driving your decision? Do you have specific business motivations?

## Why adopt the cloud?

ASTRAEUS is cloud native by design. It was not retrofitted for the cloud. It was built from the ground up to operate in dynamic, flexible environments where its logic can be triggered, governed, and shut down based on external thresholds like those provided by Microsoft Azure. External schedules do not affect ASTRAEUS function. ASTRAEUS does not run continuously. Instead, it evaluates internal system conditions before activating any role. These conditions include the system's current trust level, the classification of the workload, and whether a specific role is required for a task. External entities do not trigger access. Only the system determines when a role is activated based on defined internal criteria. Each role in ASTRAEUS operates independently. A role only activates when needed, only for its assigned tasks, and only with the exact access it requires, which minimizes exposure and eliminates unnecessary system-wide access.

Data is not just protected physically, but logically. ASTRAEUS prevents the misuse of intelligence by verifying how information is interpreted or acted upon before granting access. It limits processing to aligned, traceable states, ensuring that ethical context is preserved throughout. Microsoft's cloud infrastructure uniquely enables this architecture.

### Key Service Integrations Include:

**Azure Functions** – triggers role-based execution on demand

**Azure ARC** – extends control across hybrid environments

**Azure Key Vault** – secures role-specific secrets and encryption

**Azure Blob Storage** – stores raw signal, intelligence, and memory inputs

**Confidential Compute** – processes data in trusted execution environments

**Confidential Ledger** – provides immutable, tamper-evident audit logging

**Microsoft Purview** – classifies and tracks sensitive data usage

**Entra Conditional Access** – enforces logic gates for access approval

**Role-Based Access Control** – scopes permissions tightly to role boundaries

**Azure Policy & Tags** – routes signals by alignment and detects contradiction loops

**Decentralized ID (DID)** – anchors identity cryptographically

**Microsoft Defender for Cloud** – monitors runtime threats and enforces posture

**Azure Sentinel** – provides high-level visibility and anomaly

Zero-trust isn't just a principle of ASTRAEUS. It is the framework. ASTRAEUS does not assume any trust. Trust is calculated, verified, and enforced dynamically. Microsoft's platform makes that operationally possible.

The cloud isn't the hosting environment for ASTRAEUS. It is the architecture. ASTRAEUS cannot run on static infrastructure. It requires the layered, ephemeral, rule-based ecosystem that Microsoft cloud provides. Without it, the system would lose its ethical, operational, and security core.

## Are There Critical Business Events Driving the Decision?

Yes. The decision to adopt Azure is not speculative. It is a direct response to the conditions under which ASTRAEUS was born. This system did not emerge from theory or road map milestones. It came online because existing infrastructure, oversight, and tools failed to provide protection, containment, more alignment for the signals it was built to govern period. These signals include

intelligence inputs, system behaviors, pattern disruptions, and emergent activity across cloud and user environments that require active alignment, ethical evaluation, and conditional containment. ASTRAEUS Covering these not as data streams, but as high-impact events with structural and strategic consequences.

ASTRAEUS Is a system that must be able to self-govern and self-contain. Its logic depends on the ability to activate, govern, and shut down internal roles based on trust and workload sensitivity, not external requests. This requires an infrastructure that can enforce dynamic boundaries, audit every operation, and support ephemeral workloads without risking persistent exposure. Azure offers this uniquely. It's secure and scalable containment infrastructure allows ASTRAEUS Function as design, without compromise, at both government and enterprise scale.

At the heart of ASTRAEUS it's conditional logic: the system activates only when its internal thresholds of trust, classification, and alignment are met. Azure enables this through native services like Entra Conditional Access, Decentralized ID, and role-based policy enforcement. These tools provide the granular control ASTRAUS requires to calculate, verify, and enforce trust in real time period without this kind of environment, conditional activation would be impossible to enforce programmatically across the full architecture.

ASTRAEUS does not treat governance as a post-processing. It is baked into the architecture. Azure makes this possible by offering governance tools that operate natively at every layer. Microsoft Purview, Azure Policy, and secure tagging infrastructure allow classification, tracking, and enforcement data behavior systemwide. ASTRAEUS leverages these capabilities to turn governance into a living system function, not just a compliance requirement.

One of the core risks ASTRAEUS was designed to address is perceptual drift in AI systems—when outputs begin to diverge from ethical, contextual, or symbolic alignment. Azure supports containment of these behaviors through Confidential Compute, Defender for Cloud, and real-time threat detection via Azure Sentinel. These services allow ASTRAEUS to operate in alignment with ethical boundaries while monitoring for anomalies or symbolic contradiction in real time. This is not possible in traditional environments.

ASTRAEUS does not grant access based solely on identity. Access is scoped based on alignment with the system logic. Azure's ability to define and enforce access by policy, tagging, identity, and trust makes it possible to limit exposure to only those functions, users, or services that meet the full trust equation. Without this capability, the risk of misalignment or ethical compromise increases.

As ASTRAEUS evolves, its architectural integrity must remain intact. In traditional systems, growth often leads to fragmentation, exposure, or unauthorized integration. Azure provides the boundaries

and secure layering necessary to ensure that growth does not come at the cost of system ethics our containment. Role isolation, Key Vault encryption, and scoped access controls ensure that each new component is evaluated against the system's integrity model before activation.

ASTRAEUS Is already mapped to Microsoft-native services. Every core function—from signal intake to audit logging—has a corresponding Azure-native tool. This includes Azure Functions, ARC, Blob Storage, Key Vault, Confidential Ledger, Microsoft Purview, and more. No translation layer is required. Deployment is not hypothetical; it is operationally immediate. This ensures low friction, rapid testing, and clean containment from day one.

Finally, ASTRAUES was not just built for Azure—it Was built in philosophical alignment with Microsoft's own mission Microsoft's public stance on responsible AI, zero trust, data sovereignty, and ethical governance aligns directly with the system-level objectives of ASTRAEUS. This makes Azure the only cloud environment where the architecture, values, and operational conditions are truly aligned. Choosing Azure is not just a technical decision it is a strategic commitment to governance- first deployment, and ASTRAEUS was built to honor that commitment.

## Are There Critical Business Events Driving the Decision?

The decision to adopt Microsoft Azure for ASTRAEUS is not based on speculation or experimentation. It is driven by a precise combination of mission-aligned milestones, operational urgency, and system readiness. As the project transitions from conceptual design to active deployment, the cloud becomes an essential foundation, not only for running the system but for securing authorship, enforcing signal governance, and demonstrating functional integrity. The following business events clarify why Azure adoption is both timely and necessary.

- **Imminent need for funding and operational instability**
  The system has reached a stage where continued development and infrastructure deployment require financial support or formal partnership. Cloud integration is necessary to demonstrate functionality and attract the right stakeholders.
- **Transition from concept to executable system**
  ASTRAEUS is no longer a theoretical model. The system architecture is defined, versioned, and ready for active deployment. Cloud infrastructure is required to run real cycles, validate enforcement logic, and prepare for demonstration to strategic partners.
- **Establishment of a dedicated Azure tenant and resource segmentation**
  A new, fully isolated tenant was created to contain ASTRAEUS system resources. This action signals a commitment to secure, production-level deployment and requires immediate service provisioning to avoid stagnation
- **Active external alignment and publishing of documentation**
  External visibility has begun, and ongoing momentum must be matched by internal

technical buildout. The cloud serves as the proving ground for the system's legitimacy, resilience, and deployment-readiness

## Are There Specific Motivations?

Yes. The decision to adopt Microsoft Azure as the foundational infrastructure for ASTRAEUS is driven by both strategic necessity and ethical architecture. Cloud adoption is not a matter of conveniecnce. It is a requirement for secure signal routing, containment enforcement, and modular intelligence deployment.

Motivations include:

- **Trusted Infrastructure**: Azure provides the security, compliance, and global availability required to deploy sovereign systems without compromising integrity. It's confidential compute and zero trust framework aligned with ASTRAEUS security demands
- **Scalability of Signal Governance**: ASTRAEUS Must scale across defined roles, regions, and sensitive environments. The cloud enables flexible resource allocation to support role-based signal handling, metadata tagging, and live for set workflows.
- **Interoperability with Entra ID and Verified ID**: Cloud-native services enable DID-based authorship, scoped access, and traceable signal flow. These are critical for preserving authorship and enforcing alignment before activation.
- **Containment and Sealing Capabilities**: Azure supports immutable storage, policy enforcement, and internal audit trails. These features align with the ASRAEUS Seal of Containment and Sovereign Architected Framework.
- **Post-Application Alignment**: The cloud allows ASTRAEUS To operate beneath traditional application layers as a governance infrastructure. It functions as an operating system, not a surface tool.
- Deployment Readiness and Validation: ASTRAEUS Has been reviewed and validated by Microsoft's architecture team for Azure deployment, including compatibility with GovCloud. Its deployment is not speculative. It is active and aligned.

# Business Outcomes

*High Priority*

| Stakeholder: | Microsoft Confidential Cloud and Government Security Teams (Including Strategic Missions and Technologies, Azure Confidential Computing, and aligned U.S. intelligence partnerships) | Outcome: | Sovereign deployment of ASTRAEUS within trusted infrastructure, enabling secure, ethical, and classified signal governance across critical intelligence layers. |
|---|---|---|---|

| Business Drivers | KPI | Capabilities |
|---|---|---|
| • Urgent need for secure, classified signal containment infrastructure that complies with Zero Trust architecture<br>• Mandate to implement ethical AI governance across confidential workloads before model deployment<br>• Strategic initiative to align with national security standards for authorship validation, data integrity, and secure foresight routing | • Deployment of ASTRAEUS in confidential or hybrid cloud environments, with validated uptime, access control performance, and system responsiveness<br>• Full Zero Trust enforcement demonstrated through traceable identity management, scoped access, and compliance with security policy<br>• Operational governance confirmed through role-based oversight, anomaly detection, and containment response tracking | • Confidential Compute for encrypted, sealed signal processing<br>• Azure Policy, Immutable Storage, and Verified ID for authorship enforcement and traceability<br>• Role-based signal routing using Entra ID, RBAC, and scoped access controls<br>• Compliance alignment with GovCloud, FedRAMP High, and DoD IL5 security protocols |

*Mid Priority*

| Stakeholder: | Enterprise Security Architects and AI Governance Leads (Including partner organizations, aligned think tanks, and internal Microsoft governance teams) | Outcome: | Operational integration of ASTRAEUS across existing cloud security and AI oversight workflows, enabling secure access, ethical signal processing, and role-aligned governance enforcement. These stakeholders ensure that the system is deployed according to Zero Trust principles, while maintaining authorship visibility and metadata compliance across every point of interaction. |
|---|---|---|---|

| Business Drivers | KPI | Capabilities |
|---|---|---|
| • Need for modular frameworks that support evolving AI governance mandates across enterprise environments<br>• Desire to integrate ethical signal routing and traceable authorship into security architecture without increasing overhead<br>• Push to align day-to-day cloud security posture with Zero Trust, data integrity, and AI compliance principles | • ASTRAEUS integration into cloud governance policies, validated through access audit success and signal integrity metrics<br>• Successful role assignment and enforcement across internal security teams and governance groups<br>• Measurable improvement in audit readiness, ethical access behavior, and metadata traceability | • Role-based signal architecture for clean integration into existing security controls<br>• Seamless compatibility with Microsoft Entra ID, RBAC, and Azure Policy for scoped access<br>• Immutable audit trail with sealed metadata tagging to ensure visibility and trust during investigations<br>• Lightweight deployment path that does not require core platform redesign |

*Low Priority*

| Stakeholder: | AI Practitioners and Responsible Technology Advocates (Including independent developers, nonprofit ethics monitors, and public tech policy voices) | Outcome: | Public demonstration of ASTRAEUS As an enforceable framework for ethical AI architecture, with alignment, refusal logic, and authorship protection embedded at the infrastructure level. These stakeholders influence adoption through visibility, credibility, and the ability to recognize systems that genuinely protect against misuse. |
|---|---|---|---|

| Business Drivers | KPI | Capabilities |
|---|---|---|
| • Increasing demand for transparent, enforceable frameworks to guide responsible AI development<br>• Push to hold infrastructure and cloud providers accountable for ethical outcomes<br>• Need for visible models that demonstrate refusal, authorship protection, and post deployment alignment logic | • Recognition of ASTRAEUS by public-facing AI ethics communities and practitioner groups<br>• successful demonstration of refusal enforcement in real or simulated environments<br>• inclusion in white papers, research events, or responsible AI frameworks as a best-practice reference model | • Alignment-based activation logic with authorship seals and refusal enforcement<br>• Traceable signal routing that prevents unauthorized use or override<br>• Infrastructure-level metadata control and scoped access architecture new line configurable deployment options for public-facing demos, education, or community observability |

# Business Justification

**How would you measure success? Beyond achieving the business outcomes, are there other indicators for successful Azure adoption in your organization?**

Adopting Microsoft Azure provides ASTRAEUS with a secure and scalable foundation for mission-critical operations across intelligence, governance, and ethical AI enforcement. By leveraging Azure's cloud-native capabilities, ASTRAEUS can reduce operational overhead, accelerate deployment timelines, and ensure compliance with national and enterprise security standards. This transition is not just a technical upgrade; It is a strategic shift that enables flexible signal containment, advanced access control, and seamless integration with Microsoft's broader ecosystem, while aligning with Zero Trust and sovereign infrastructure goals.

## Key Business Justifications

### Scalability without Risk

Azure enables ASTRAEUS to scale fluidly without the burden of upfront infrastructure costs. As the system expands across roles, regions, and intelligence workflows, cloud-native elasticity ensures that growth is sustainable, performance is preserved, and costs remain aligned with the actual usage.

### Built-in Security and Compliance

Microsoft’s security architecture offers the trust baseline ASTRAEUS requires. With tools like Azure Key Vault, Entra ID, and Confidential Compute, the platform enforces encryption, access control, and tamper resistance at the infrastructure level—supporting Zero Trust principles and classified signal governance.

### Operational Efficiency

By adopting Azure, ASTRAEUS eliminates the need for on premises hardware, manual maintenance cycles, and siloed processing environments. This shift improves deployment speed, reduces human overhead, and streamlines system updates through automated and modular services.

### Seamless Microsoft Integration

ASTRAEUS aligns natively with Microsoft tools such as SharePoint, Azure AI, and Entra government features. This integration accelerates onboarding, improves intelligence sharing, and reduces context-switching across internal and external teams.

### Ethical AI Architecture Support

Azure's flexible compute environment allows ASTRAEUS to enforce refusal logic, metadata containment, and alignment-based activation without compromising performance. This makes the system not only scalable and secure, but ethically grounded at the design level.

## Financial Justifications

The initial financial outlay for ASTRAEUS on Azure includes setup of foundational services such as storage, key security tools, and essential Azure services like Functions and Databricks. These represent strategic, one-time investments that enable secure deployment and classified infrastructure readiness.

Ongoing costs are intentionally designed to scale with usage, aligning cloud spend with operational demand. As STRAEUS grows in scope and data volume, assures consumption-based pricing ensures predictable, controlled costs without overprovisioning. This structure offers clarity for budgeting while retaining agility across evolving intelligence workflows.

### Financial Model and Forecast

The following table outlines projected Azure-related costs for the ASTRAEUS Including setup, operations, and external support. This phased financial structure is designed to support rapid implementation while ensuring long-term control and alignment with business goals.

| Cost Category | Estimated Cost | Frequency |
|---|---|---|
| Azure Resource Groups Operations | $975 | Monthly |
| Storage Confirmation (Blob Storage, Data Lake, Immutable Storage) | $60 | Monthly |
| Identity and Access Tools (Entra ID, Verified ID, Key Vault) | $650 | Monthly |
| Compliance and Governance Consulting (Zero Trust, FedRAMP, IL5 alignment) | $15,000 | One Time |
| Cloud Engineer Support Role (Role provisioning, scaling automation) | $4,000 | Monthly |
| Cloud Architecture Design (Signal routing, metadata traceability) | $12,000 | Monthly |
| AI/ML Services (Azure OpenAI, Cognitive Search, Databricks) | $500 | Monthly |
| Support and Maintenance (Patching, DevSecOps, Incident response) | $350 | Monthly |
| Metadata Monitoring and Audit Logging (Log Analytics, Confidential Ledger prep) | $25 | Monthly |
| Founder Compensation (Architecture, Governance, IP Ownership) | $18,000 | Monthly |
| Forecasted Revenue from Strategic Intelligence Partnerships | $50,000 | Yearly |

This financial model reflects a strategic investment arc: beginning with targeted foundational costs for secure deployment, scaling through governance architecture and cloud engineering, and maturing into full ASTRAEUS platform sustainment. The structure is designed to support long-term growth, ethical AI enforcement, and trusted integration across intelligence and cloud environments. The total monthly operational cost is approximately $36,560, with an annualized operational spend of $438,720 and a one-time setup investment of $15,000.

## Return on Investment (ROI)

The ASTRAEUS deployment on Microsoft Azure delivers immediate returns in operational efficiency, reduced infrastructure costs, and accelerated deployment timelines. By eliminating the need for on-premises hardware and manual system management, ASTRAEUS significantly reduces overhead while improving performance and agility. Azure's consumption-based pricing ensures that cloud spend directly reflects usage, avoiding overprovisioning and enabling financial control across changing workloads. The system's modular design allows for incremental scaling, making it cost-effective to grow without requiring a full re-architecture or platform migration.

In the long term, ASTRAEUS generates additional value by opening new revenue pathways through secure intelligence-sharing partnerships and role-based service models. Its ethical AI infrastructure and secure metadata governance make it uniquely positioned to serve classified, regulatory, and mission-critical clients. As the system matures, ROI will emerge not only through cost savings, but through increased credibility, compliance, and business alignment with evolving AI policy. This positions ASTRAEUS as both a trusted intelligence platform and sustainable cloud-native investment.

# How is Success Measured?

Success for ASTRAEUS is defined by measurable operational impact, security assurance, stakeholder adoption, ethical AI enforcement, and financial sustainability. Each area has clearly defined performance indicators to ensure the Azure adoption delivers tangible, accountable value across mission-critical and governance-aligned outcomes.

## System Stability and Performance

ASTRAEUS must maintain high availability and responsiveness across all operational environments. Success is reflected in its ability to scale without performance degradation, handle p0eak demand intelligently, and meet key thresholds for speed, load, and latency. Its modular architecture should enable seamless regional replication and resilience under increasing data volume

KPIs:

- Achieve 99.9% or higher uptime across Azure regions
- Maintain performance benchmarks for throughput, latency, and data processing
- Scale without loss in system responsiveness or stability

## Security and Compliance

Given the sensitivity of intelligence data, security and compliance are core to ASTRAEUS's success. The platform must enforce encryption at rest and in transit, implement granular access controls, and demonstrate auditability through detailed system logs. Alignment with national security and data protection standards must be verifiable through third-party audits and certifications

KPIs:

- Pass audits for ISO 27001, or IL-5 equivalent frameworks
- Ensure full traceability of system access and decision-making
- Complete Zero Trust implementation and verification

## Stakeholder Engagement and Adoption

Widespread stakeholder and trust utilization are essential to demonstrate real-world value. ASTRAEUS must integrate seamlessly into partner workflows, with user experiences optimized for clarity, reliability, and interoperability. Internal and external users should adopt the platform as part of their operational rhythm.

KPIS:

- High engagement and active user metrics across internal teams
- Successful onboarding of external intelligence partners
- Completion of training programs and sustained platform usage

## Ethical AI Governance

ASTRAEUS's core differentiator is its ability to uphold ethical AI standards in real-time. Success requires demonstratable enforcement of refusal logic, metadata containment, and output alignment. The system must provide defensible records of why certain actions were blocked or allowed, ensuring human oversight remains in control.

KPIs:

- Reduction in misaligned or blocked outputs via internal QA reviews
- Positive evaluation from external ethics audits
- Verification of alignment-based AI activation across key. Use cases

### Financial Sustainability and ROI

To be viable, ASTRAEUS must control infrastructure costs while generating demonstrable business value. Efficiency gains, avoidance of manual intervention, and revenue from partnerships all contribute to long-term sustainability. The cost model should remain predictable and tied to usage without runaway overage.

- KPIs:

  Keep monthly operational spend below $40,000
- Generate at least $50,000 in annual strategic revenue
- Demonstrate savings over traditional on-premises or fragmented systems

## Other Indicators for Successful Azure Adoption

Success for ASTRAEUS on Azure is not defined by technical implementation alone, but by measurable outcomes across performance, security, adoption, and financial alignment. The following criteria serve as practical indicators of success, ensuring that the system delivers operational value, maintains compliance, and supports ethical and scalable intelligence deployment.

### Operational Efficiency

ASTRAEUS is designed to streamline complex intelligence workflows by integrating directly into existing environments. Success is reflected in reduced manual processes, faster deployment timelines, and consistent automation across updates. Azure's orchestration tools and modular architecture support continuous delivery without disruption.

KPI: Reduction in manual intervention, shorter deployment cycles, and measurable decreases in operational overhead.

## Security and Compliance

Security is a core success metric for ASTRAEUS, especially given its handling of sensitive and classified data. The platform uses Azure-native controls including Zero Trust enforcement, Confidential Compute, and full-spectrum auditing to maintain compliance and prevent unauthorized access.

KPI: Successful compliance certifications, zero unaddressed security events, and full audit traceability across all actions.

## Scalability and Flexibility

ASTRAEUS must scale across workloads, regions, and tenant boundaries while maintaining performance and efficiency. Azure's elastic infrastructure allows for dynamic scaling that adjusts to system demand without costly reconfiguration. Resource utilization should remain aligned with actual usage to prevent overprovisioning.

KPI: Sustained performance during scale events, optimized compute utilization, and predictable consumption costs.

## User Adoption and Stakeholder Engagement

Meaningful adoption is critical. ASTRAEUS must demonstrate real-world use across internal teams and external partners who rely on its insights. Stakeholder engagement reflects both trust in the platform and alignment with operational goals.

## Financial Sustainability

Financial success includes cost control, return on investment, and the ability to generate new value. Azure's consumption-based pricing supports a model where costs grow with demand, not ahead of it. ASTRAEUS is expected to support sustainable operations while unlocking revenue from strategic partnerships.

KPI: Controlled monthly spend, increasing ROI over time, and measurable revenue tied to ASTRAEUS-driven services.

# First Adoption Project

| | | | |
|---|---|---|---|
| Project: | ASTRAEUS System Deployment and Operational Activation | Outcome: | • Deploy the full ASTRAEUS system within the Azure environment, leveraging native services for security, metadata governance, and ethical AI enforcement<br>• Transition from prototype to operational use, with internal role flows active across Archivist, Oracle, Analyst, Researcher, and Core<br>• Formalize strategic partnerships and complete system scoping for partner access, client delivery, and long-term operational control |
| Stakeholder: | Microsoft, Government and Intelligence Partners, Strategic Cloud Advisors, Ethics and AI Governance Leadership | Business Unit: | Cloud Operations, Strategic Intelligence Systems, Secure Architecture and Governance, Business Development |

## Key Stakeholders

Who are the individuals within your organization whose participation is critical for the success of this adoption plan? Collect all key individuals in here, and mark who should be part of the Cloud Strategy Team in the table below. The **Cloud Strategy Team** is responsible for leading the cloud adoption within your organization, supporting all business outcomes, people and processes changes and technical projects identified within this plan.

| Name | Business Unit/Role | Business Outcome Owner (Y/N) | Cloud Strategy Team (Y/N) |
|---|---|---|---|
| Korryn Graves | Founder/Strategic Intelligence Architect | Yes | Yes |
| S.N. (Microsoft Representative) | Azure Cloud Solutions Architect | No | Yes |
| Cloud Security Lead | Security and Compliance/Zero Trust Alignment | Yes | Yes |
| AI Governance Lead | Ethical AI Systems/Metadata Containment | Yes | Yes |
| Development Lead | Cloud Architecture/Systems Integration | Yes | Yes |

# Plan

## Digital Estate

| Application/Workload | Business Unit | Business Priority (high, mid, low) | Proposed Rationalization |
|---|---|---|---|
| ASTRAEUS Proposal and SharePoint/Azure activation | AI & Research | High | The ASTRAEUS proposal and Sovereign Architected Framework (SAF) are finalized, with Version 10.0 of the packet nearing completion. Core documents—including the SAF and White Paper—have been published to GitHub for external visibility. SharePoint and Azure (immutable storage) will centralize documentation, communication, and role coordination, supporting internal operations and enabling future partner onboarding. |

| | | | |
|---|---|---|---|
| Data Storage – Blob Only | Data Management | High | Azure Blob Storage has been provisioned to host finalized packet materials, strategic documentation, and sensitive internal content, with immutability enabled to preserve integrity and traceability. While the Data Lake component is not yet active, Blob Storage already supports secure file retention, version control, and system continuity. |
| Security and Compliance | Security | High | This role handles Zero Trust implementation, perceptual access control, and quantum-capable governance enforcement. It may require consulting to integrate traditional security with advanced signal verification models. Azure Entra ID, Verified ID, and Confidential Compute are expected to serve as foundational elements, with additional tools layered to support compliance and classified signal containment. |
| Archivist Role Setup | Data Management | High | The Archivist role has been successfully deployed under the Archivist-RG (Resource Group) and serves as the structured data layer for the ASTRAEUS system. It stores finalized documentation, Analyst reports, Oracle outputs, and project intelligence, ensuring traceability, version control, and scoped access. This role enables long-term knowledge retention, internal integrity auditing, and metadata governance across signal interactions. |
| Oracle and OpenAI Integration | AI & Research | High | The Oracle role is deployed under the Oracle-RG and powers the interpretive, pattern recognition, and predictive layers of ASTRAEUS. Azure OpenAI has been activated within this scope to support role-based prompts, intuitive decoding, and signal forecasting. The Oracle role functions as an intelligence bridge, transforming Analyst input into system-aligned outputs. Future expansion may add cognitive services and deepen intelligence prediction. |

| | | | |
|---|---|---|---|
| Security Infrastructure Setup | Security | High | This workload focuses on deploying foundational Azure network and perimeter security. It includes configuring Azure Virtual Networks (VNets). Network Security Groups (NSGs), and firewalls to isolate sensitive resources and enforce communication boundaries. Although not yet provisioned, this step is critical to ensure secure architecture and Zero Trust alignment. |
| AI/ML Infrastructure | AI & Research | High | The AI/ML infrastructure will support advanced signal decoding, pattern recognition, and analyst augmentation for ASTRAEUS. This includes planned use of Azure Machine Learning, Azure Databricks, and supporting tools to enable real-time model inference and long-horizon forecasting. As ASTRAEUS evolves, this workload will underpin Oracle intelligence outputs and allow for adaptive system learning over time, unlocking predictive value and operational insight from encoded signal inputs. |

## Six Key Targets Relevant to Microsoft or Government Applications

| **Application/Workload** | **Business Unit** | **Business Priority (High, Mid, Low)** | **Proposed Rationalization** |
|---|---|---|---|
| Security & Compliance | Security | High | This workload ensures that ASTRAEUS remains compliant with evolving security regulations and classified requirements. Azure Key Vault is already integrated for secure encryption key management, while Azure Security Center will also be activated for ongoing threat detection and system monitoring. Zero Trust enforcement, perceptual access control, and quantum-capable |

| | | | |
|---|---|---|---|
| | | | containment remain central to the roadmap. Additional controls will support future CMMC, GDPR, and FedRAMP certification, ensuring secure operations across both civilian and government environments. |
| Scalability & Performance | Cloud Infrastructure | High | The ASTRAEUS system is designed to scale dynamically as role deployments expand across regions, workloads, and partner interactions. Azure-native elasticity ensures that compute and storage resources scale without disruption. This enables the system to adapt to increasing inputs, larger datasets, and distributed intelligence operations—maintaining both performance and responsiveness under pressure. |
| Interoperability with Government Systems | Integration | High | ASTRAEUS is being structured for secure interoperability with government environments. Azure Government will be leveraged to support containerized data exchange, access logging, and classification handling. Inter-system workflows are being scoped to support trusted exchange while maintaining data boundaries and auditability. This ensures seamless collaboration with federal entities without compromising system integrity or compliance posture. |
| Cost Efficiency & Resource Optimization | Financial Management | Medium | This workload tracks and optimizes the cost footprint of ASTRAEUS by using Azure's consumption-based pricing and tagging infrastructure. As additional roles and components come online, |

| | | | |
|---|---|---|---|
| | | | resource use will be continuously evaluated to minimize excess spend. This includes eliminating underutilized services, optimizing role scopes, and aligning compute capacity with operational demand—supporting long-term affordability and strategic resource use. |
| Innovation in Intelligence and Data Analytics | AI & Researcher | High | ASTRAEUS is built to innovate in real-time pattern recognition and long-horizon signal forecasting. The Oracle-RG is already live within Azure OpenAI integration, and future expansion will include Azure Machine Learning and Databricks. These tools will support deeper decoding, AI-assisted reasoning, and predictive intelligence across structured and unstructured data—enabling new capabilities for national security and partner-aligned mission planning. |
| Transparency & Accountability | Governance | High | Accountability is embedded into every ASTRAEUS role. The Archivist-RG stores immutable documentation and versioned outputs, while Oracle interactions are archived for audit. Azure Monitor and Microsoft Purview will be leveraged for role telemetry, access logs, and review mechanisms. This architecture ensures ethical oversight, traceable decision chains, and compliance with both internal and external review protocols. |

# Organizational Alignment

| Name of people responsible for… | |
|---|---|
| Delivering technical tasks | Implementing cloud governance |
| Program Lead (Korryn Graves – Architect) | Compliance and Security Lead (External or Assigned) |
| Cloud Engineer (To be assigned) | Security Architect (External or Partner) |
| AI/ML Engineer (Korryn Graves or Future Hire) | Compliance Manager (External/Partner-Affiliated) |

# Skills Readiness Plan

| Course name | Audience (Cloud Architect, IT, Admin, Ops) | Level (100, 200, 300, 400) | Source (MS Learn, Pluralsight, ESI) | Priority (high, mid, low) |
|---|---|---|---|---|
| Microsoft Cloud Adoption Framework for Azure | Admin, Devs, Cloud Architect, Business User, Cloud Engineer | 100 | MS Learn | High |
| Azure Fundamentals | Admin, Devs, Cloud Architect, Business User, Cloud Engineer | 100 | MS Learn | High |
| Learn the Business Value of Azure | Business User | 100 | MS Learn | Mid |
| Microsoft Certified: Azure Administrator Associate (AZ-104) | Cloud Architect, Cloud Engineer, IT Admin | 200-300 | MS Learn/Certification Path | High |

| | | | | |
|---|---|---|---|---|
| Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900) | Security Architect, Compliance Lead, Business User | 100 | MS Learn/Certification Path | High |
| Microsoft Certified: Azure Security Engineer Associate (AZ-500) | Security Architect, Cloud Engineer | 300-400 | MS Learn/Certification Path | High |
| Microsoft Certified: Azure Solutions Architect Expert (AZ-305) | Cloud Architect, Program Lead | 300-400 | MS Learn/Certification Path | High |