# The Airitos Strategic Imperative: Navigating Azure Migration and Automating Identity Management with Key Talent Acquisition

This eBook outlines the critical security and identity management challenges confronting Airitos.com, a global organization with 50 offices, as it undergoes a significant strategic migration from AWS to the Microsoft Azure ecosystem.

# Airitos.com's Strategic Imperative: Navigating Azure Migration and Automating Identity Management with Key Talent Acquisition

## Executive Summary

This eBook outlines the critical security and identity management challenges confronting Airitos.com, a global organization with 50 offices, as it undergoes a significant strategic migration from AWS to the Microsoft Azure ecosystem. The core issues revolve around a severe talent gap in security engineering and architecture, a highly manual and complex Identity and Access Management (IAM) operation, and the burden of untangling legacy systems. Airitos.com is actively seeking external expertise and skilled personnel to accelerate its transition to Microsoft Entra ID, Sentinel, and Purview, aiming for enhanced automation, compliance, and operational efficiency. This report details the specific pain points, the strategic rationale behind the Azure pivot, the precise talent requirements, and a proposed iterative engagement model designed to deliver tangible value and mitigate past frustrations with large-scale consulting engagements.

## 1. Introduction: Airitos.com's Security & Identity Transformation Journey

Airitos.com, under Bill's ownership, is currently navigating a pivotal phase in its operational and security landscape. The organization manages 50 offices globally, with direct responsibility for physical security and access control in 20 of these locations.[1] This extensive footprint necessitates a robust and adaptable security posture, a need that has rapidly intensified due to recent, unplanned security requirements.[1] The sudden emergence of these critical needs suggests that the organization is now in a reactive mode, striving to catch up with evolving security demands. This reactive genesis for current security initiatives often translates into urgent, high-pressure demands for immediate and effective solutions, which in turn influences the preference for agile, iterative approaches over protracted, traditional assessments.

The overarching strategic direction for Airitos.com involves a comprehensive migration of its applications and security infrastructure from Amazon Web Services (AWS) to the Microsoft Azure cloud platform.[1] This strategic pivot encompasses the adoption of key Microsoft security services, including Microsoft Entra ID for identity management, Sentinel for security information and event management (SIEM), and Purview for data

governance and compliance. This transformation is not merely an IT upgrade; it is critical for maintaining operational integrity and meeting stringent regulatory demands. Airitos.com serves a client base that includes high-security entities such as countries, states, and banks, which act as de facto regulators for the organization.[1] The stringent compliance requirements from these clients are a fundamental driver for the entire security transformation. This imperative directly influences the selection of enterprise-grade technology solutions, such as the comprehensive Microsoft E5 suite, and dictates the specific requirements for talent acquisition, emphasizing professionals experienced in regulated environments who can ensure adherence to compliance standards. Security, in this context, transcends mere IT hygiene, becoming a critical business enabler for client retention and growth, thereby elevating the stakes of the entire transformation.

## 2. The Unfolding Challenges: A Deep Dive into Airitos.com's Security Landscape

Airitos.com faces a multifaceted array of security and operational challenges, primarily concentrated within its Identity and Access Management (IAM) domain and its overall security engineering capabilities. These challenges are deeply intertwined with legacy systems and a significant technical debt, creating a complex environment that demands immediate and strategic intervention.

### 2.1. The Manual Maze of Identity & Access Management (IAM)

The current state of Airitos.com's identity operations is characterized by a high degree of manual intervention, managed by a substantial team of 50 individuals located in India.[1] This manual approach is described as burdensome and inefficient.[1] A significant portion of this manual effort is dedicated to the complex process of provisioning identities for both Airitos.com's internal employees and its diverse customer employees into critical enterprise systems, notably SAP and Workday.[1] This "cross-boundary" provisioning is particularly intricate and deviates from typical IAM solutions, which are primarily designed for internal workforces.[1]

The fundamental cause of this manual burden lies in the absence or "thinness" of robust middleware solutions that would enable automated provisioning and deprovisioning processes.[1] The consequences of this manual system are substantial: for instance, when 10,000 employees are provisioned into a system like Workday, approximately 5,000 of those identities may be "messed up," necessitating extensive manual remediation by the identity team.[1] This indicates a substantial operational inefficiency and a hidden cost that extends far beyond the salaries of the 50-person

team, encompassing delays in onboarding and offboarding, potential security vulnerabilities due to incorrect or lingering access, and a degraded user experience. Automating IAM is therefore not just a cost-cutting measure but a critical investment in improving operational accuracy, strengthening the security posture, and enhancing overall business agility and compliance.

A critical internal skill gap exists in identity architecture, specifically concerning the configuration and ongoing management of Microsoft Entra ID, Entra B2C, and Entra B2B.[1] While external contractors are currently assisting with the migration efforts, Airitos.com lacks full-time employees (FTEs) to manage the long-term architectural design and operational oversight of these critical identity components. Furthermore, the re-certification of access for users who do not originate from the primary HR system—such as external customer employees—presents a significant hurdle. Most standard IAM tools assume the HR system as the definitive system of record, making it challenging to manage and re-certify access for non-standard users.[1] This implies a labor-intensive process to ensure continuous compliance and security for these unique user populations.

Adding to the complexity, the identity environment is deeply "interweave and intertangled" with legacy NGA systems, a direct consequence of a past merger.[1] This legacy system, described as a "can that's been kicked down the road for 15 years," has become a significant source of complexity and manual effort, requiring specialized expertise to untangle and integrate with modern solutions.[1] The use of strong language, such as "mess we have," to describe the current state of identity management, along with the observation of a disconnect between internal stakeholders regarding responsibilities, suggests that the challenges are not purely technical. They also stem from a lack of clear ownership, inconsistent strategic direction, or a series of short-term fixes that have accumulated into an unmanageable state. Addressing these underlying organizational factors, alongside implementing new technology and acquiring talent, is essential for achieving sustainable improvements.

Rick's ultimate objective is to automate these manual processes, aiming to reduce the 50-person identity team to a "handful of people".[1] He seeks a clear "right path" to integrate the diverse client requirements and legacy systems with the new Entra ID stack. The following table summarizes the current challenges and the desired future state for Airitos.com's IAM:

**Table 1: Current State vs. Desired State: Airitos.com's Identity & Access**

### Management Transformation

| IAM Aspect | Current State (Pain Points) | Desired State (Benefits of Automation) |
|---|---|---|
| **Identity Operations Team** | 50 people in India, "pain in the ass to manage" [1] | "Handful of people," reduced operational overhead [1] |
| **Provisioning Process** | "Very manual" for SAP & Workday, "no like middleware or if there is middleware it's kind of thin" [1] | Automated, API-driven provisioning [1] |
| **Deployment Accuracy** | Up to 50% of employees "messed up" during provisioning, requiring manual fixes [1] | Accurate, error-free deployments (Inferred from automation goal) |
| **Deprovisioning** | Manual deprovisioning by Ralph [1] | Automated, immediate deprovisioning upon employee departure [1] |
| **Identity Architecture** | No internal FTEs for Entra ID, B2C, B2B architecture [1] | Dedicated internal identity architects [1] |
| **Legacy Systems** | "Interweave and intertangled" legacy NGA, "kicked down the road for 15 years" [1] | Untangled, integrated with modern Entra ID stack [1] |
| **Compliance/Re-certification** | Complex re-certification for non-HR system users [1] | Streamlined, automated re-certification processes (Inferred from automation goal) |

This table clearly articulates the business case for investment in automation and skilled talent, serving as a quick reference for understanding the scope and impact of the IAM challenge.

### 2.2. Bridging the Security Engineering & Architecture Gap

Beyond identity management, Airitos.com faces an urgent and significant shortage of

security engineering and architecture talent. This is identified as "probably the biggest gap" within the organization.[1] There is an immediate need for hands-on engineers who can "get a hands on keyboard, help us configure stuff" to address pressing operational requirements and support the ongoing Azure migration.[1]

In addition to hands-on configuration, strategic architectural expertise is crucial. Airitos.com requires security architects capable of designing the overall tool stack and integration strategy for the new Azure environment.[1] While Rick has one existing engineer/architect, additional support is needed to allow this individual to focus on the engineering stack, while Rick oversees the broader architecture and application integration. A major undertaking involves migrating and replatforming over 20 applications from AWS to Azure, a process that demands substantial engineering effort.[1] This migration is subject to impending deadlines, specifically by September, for the configuration and setup of all new security tools, including Sentinel, as part of the Transitional Services Agreement (TSA) exit.[1] This hard deadline means that the acquisition of security engineers and architects is not a long-term strategic goal that can be phased in leisurely; it is an immediate, critical operational imperative. Delays in talent acquisition or the configuration of new security tools could lead to non-compliance with TSA exit requirements, potentially resulting in significant penalties, extended costs, or operational disruptions. This adds a layer of time-sensitive pressure to both talent acquisition and project execution. Finally, Rick notes a current lack of product security resources, although efforts are underway to address this with a potential candidate.[1]

### 2.3. Untangling Legacy Systems and Technical Debt

A significant portion of Airitos.com's operational complexity and manual effort stems from its inherited legacy systems. The NGA system, a remnant from a past merger with ALight, has remained largely intact for 15 years, becoming a considerable hurdle in the current transformation.[1] This system is described as "interweave and intertangled," necessitating specialized expertise to disentangle it and integrate it with modern solutions.[1] The legacy NGA system directly contributes to the manual nature of IAM operations, particularly impacting corporate identity management and potentially extending to customer identity processes.[1] Addressing this technical debt is paramount for achieving the desired level of automation and efficiency within the new Azure ecosystem.

## 3. A Strategic Pivot: Embracing the Microsoft Azure Ecosystem

Airitos.com's strategic decision to migrate to the Microsoft Azure ecosystem represents a significant shift towards a more consolidated, modern, and efficient

security and identity management infrastructure. This pivot is driven by both existing investments and the evolving maturity of Microsoft's cloud offerings.

### 3.1. The Power of Entra ID: Modernizing Identity & Access

The migration to Azure positions Microsoft Entra ID (formerly Azure Active Directory) as the central pillar of Airitos.com's identity management strategy.[1] This choice is underpinned by Entra ID's comprehensive capabilities, which are well-suited to Airitos.com's complex requirements. These capabilities include robust features such as passwordless and multifactor authentication (MFA), Conditional Access policies for granular control, Identity Protection to block real-time identity attacks, Privileged Identity Management (PIM) for securing high-privilege accounts, and end-user self-service portals.[2] These features are essential for ensuring secure adaptive access and proactively safeguarding identities.

A critical aspect of Airitos.com's strategy involves the explicit inclusion of Entra B2C (Business-to-Consumer) and Entra B2B (Business-to-Business) solutions.[1] Entra B2C is designed for customer-facing applications, allowing customers to use their preferred social, enterprise, or local accounts for single sign-on (SSO) access. It offers extensive customization for branding and user flows, and supports integration with external user stores.[4] This is particularly crucial for Airitos.com's diverse client base, especially given the experience with B2C implementations involving millions of users globally.[1] Entra B2B, conversely, facilitates secure collaboration with external partners and guests, enabling them to use their own credentials without Airitos.com needing to manage external accounts or passwords.[6] This capability is vital for efficiently managing customer employees within Airitos.com's systems.

Airitos.com is actively migrating away from its existing Identity and Access Management (IAM) tools, such as SailPoint, Okta, and Ping, with the clear objective of consolidating all identity operations under Entra ID.[1] While CyberArk, a Privileged Access Management (PAM) solution, will be temporarily retained for some servers, the overarching strategic direction is a clear shift towards Microsoft's integrated offerings.[1]

The rationale behind this strategic technology choice is multifaceted. Rick acknowledges the significant maturation of Entra ID in recent years, noting that it has evolved to handle complex implementations, including large-scale B2C scenarios, a capability he would have doubted five years prior.[1] The organization's existing E5 license is a significant enabler, providing access to a comprehensive suite of Microsoft security and identity features.[1] This license reduces vendor sprawl, minimizes integration complexity, and eliminates the need for new procurement cycles, allowing

Airitos.com to maximize its existing investment and making the Azure pivot a logical and economically sound strategic move. Furthermore, the move to Entra ID is anticipated to be more cost-effective than maintaining some of the "pure play" identity solutions.[1] Its broad integration capabilities, spanning from on-premises legacy applications to thousands of Software-as-a-Service (SaaS) applications, are also key to achieving a unified identity platform.[2]

The unique challenge of managing identities for both internal employees and customer employees across systems like SAP and Workday, a "rare" use case, highlights the complexity involved.[1] The need to integrate into Entra ID "across all of our different clients, all our different requirements" further amplifies this complexity.[1] While Entra ID's B2C and B2B features offer robust capabilities for external identities, the sheer volume of users and the "interwoven" nature of legacy systems necessitate sophisticated architectural design and implementation. This complex scenario underscores the critical need for high-caliber identity architects who can design solutions that ensure compliance, a seamless user experience for both internal and external stakeholders, and effective integration with the legacy environment, ultimately ensuring the success of this pivotal transition.

**Table 2: Key Microsoft Entra ID Capabilities and Their Strategic Value for Airitos.com**

| Entra ID Capability | Description | Strategic Value for Airitos.com |
|---|---|---|
| **Passwordless & MFA** | Safeguard access to data and apps with strong authentication [2] | Enhances security posture, reduces reliance on passwords, potentially eliminates password help desk [1] |
| **Conditional Access** | Apply risk-based access controls to strengthen security [2] | Enforces granular access policies for diverse internal and high-security external users, crucial for compliance [1] |
| **Identity Protection** | Protect identities and block identity attacks in real-time [2] | Provides proactive defense against compromised identities, critical for maintaining trust with |

| | | |
|---|---|---|
| | | regulated clients [1] |
| **Privileged Identity Management (PIM)** | Strengthen security of privileged accounts [2] | Secures administrative access to critical systems like SAP/Workday, especially important given current manual processes [1] |
| **Entra B2C** | Customer-facing identity solution for SSO access to applications and APIs [4] | Streamlines customer employee provisioning, centralizes identity for diverse client requirements, handles millions of users [1] |
| **Entra B2B** | Secure collaboration with external partners using their own identities [6] | Simplifies management of external customer employees, reduces administrative overhead and credential management [1] |
| **App Integrations & SSO** | Connect workforce to all apps from any location, using any device [2] | Consolidates access, improves user experience across disparate applications, reduces complexity of managing multiple identity silos [1] |

This table serves as a powerful visual aid, directly mapping the features of Microsoft Entra ID to the specific challenges and strategic goals outlined by Rick. By articulating why each capability is valuable to Airitos.com, it clearly communicates the business case for the technology adoption. This helps stakeholders understand the strategic implications of the Azure pivot and how Entra ID specifically addresses their unique, complex identity management needs, from reducing manual effort to enhancing compliance.

### 3.2. Leveraging Sentinel for Unified Security Operations

As part of its comprehensive Azure strategy, Airitos.com plans to implement Microsoft Sentinel. This signifies a move towards a cloud-native Security Information and Event Management (SIEM) and Security Orchestration Automated Response (SOAR) solution.[1] Sentinel offers a robust set of capabilities for modern security operations. These include extensive data collection and integration from various sources,

including Azure, AWS, and Google Cloud Platform (GCP), providing a unified view of security events. Its advanced threat detection and analytics leverage the Kusto Query Language (KQL) for customized alerting, while AI-powered investigation tools and automated incident response playbooks streamline threat management.[8] Notably, Sentinel also provides a specific solution for monitoring SAP applications [8], which is highly pertinent given Airitos.com's extensive use of SAP for identity management and other critical business functions.

### 3.3. Ensuring Data Governance with Purview

Airitos.com's interest in "the Microsoft stack for defenders the perviews" indicates an intention to leverage Microsoft Purview for comprehensive data governance and compliance.[1] Microsoft Purview is designed to help organizations mitigate data risk through unified data security, governance, and compliance solutions. Its core functions enable organizations to secure data throughout its lifecycle, understand and activate data for analytics, and ensure compliance with privacy regulations.[9] Purview's capabilities span Information Protection, Data Loss Prevention, Insider Risk Management, Data Governance, Audit, and eDiscovery.[9] Given Airitos.com's highly regulated client base, Purview's ability to streamline multi-cloud and regulatory compliance through templates and guided processes is a critical component of its overall security and operational strategy.[1]

## 4. Building the Future: Strategic Talent Acquisition & Engagement

Airitos.com's ambitious security and identity transformation hinges on acquiring the right talent and establishing an effective engagement framework with external partners. The organization's past experiences and unique operational context heavily influence its preferences for staffing and collaboration.

### 4.1. The Imperative for Hands-On, Independent Expertise

Airitos.com is actively seeking "very technical people" who are "independent thinkers" and possess the ability to "figure it out" without requiring constant supervision.[1] The immediate operational needs necessitate individuals who can "get a hands on keyboard, help us configure stuff".[1] The emphasis is placed on demonstrated capability and independence rather than a strict adherence to "years of experience," as Rick has observed that individuals with fewer years but more impactful project experience can outperform those with longer, less productive careers.[1] This approach allows for a focus on individuals who have successfully tackled complex challenges, referred to as "gnarly projects".[1]

The specific roles in demand include:

- **Security Engineers:** These are the most pressing need, responsible for hands-on configuration and setup of critical security tools within the Microsoft stack, including Defender, Sentinel, Purview, and Entra ID.[1] While Microsoft stack expertise is primary, some experience with external email security solutions like Abnormal or Proofpoint is considered beneficial.[1]
- **Security Architects:** These roles are crucial for designing the overall security infrastructure and integration strategies. They are expected to work collaboratively with Rick's existing architect/engineer.[1] These positions typically require more senior experience due to their strategic design responsibilities.[1]
- **Identity Architects & Engineers:** These specialists are needed to build and operate the new Entra ID stack, partnering with external consultants on the comprehensive IAM transformation, and managing post-deployment operational tasks.[1] Specific expertise in SAP identity and Microsoft Entra ID is considered crucial for these roles.[1]

A clear directive is that these roles are "not business facing people at all" and are expected to "just get it done," indicating a focus on technical execution rather than client interaction or high-level strategic advisory.[1] Given Airitos.com's client base, which includes highly regulated entities, candidates must possess experience managing environments that demand strict compliance with various regulations, change control processes, and rigorous testing protocols.[1] The organization explicitly seeks to avoid "cowboys" from startup environments who may be accustomed to less structured approaches; instead, it prefers individuals who embody a "medium" between narrowly focused enterprise specialists and broad startup generalists.[1] This mandate reflects a strategic move away from ad-hoc, rapid-prototyping approaches towards a more structured, disciplined, and mature operational model. It underscores the increasing importance of governance, compliance, and controlled change within Airitos.com, driven by their highly regulated client base. The talent acquisition strategy must therefore filter for individuals who thrive in such environments and can contribute to building robust, auditable processes, ensuring that new solutions are not only effective but also sustainable and compliant.

**Table 3: Airitos.com's Ideal Talent Profile: Security & Identity Roles**

| Role Category | Specific Roles | Key Technical Skills | Desired Characteristics | Preferred Engagement Model |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **Security Engineering** | Security Engineer, Security Architect | Microsoft Stack (Defender, Sentinel, Purview, Entra ID), Hands-on configuration, Tool setup [1] | Very technical, Independent thinkers, Problem-solvers, Experience in compliant environments, Not business-facing [1] | Contract-to-Hire, Perm, Contractor [1] |
| **Identity & Access Management (IAM)** | Identity Engineer, Identity Architect | Microsoft Entra ID (AD, B2C, B2B), SAP Identity, Workday (understanding) [1] | Very technical, Design capabilities, Institutional knowledge retention, Experience in compliant environments, Not business-facing [1] | Contract-to-Hire, Perm, Contractor [1] |

This table provides a concise, at-a-glance summary of Airitos.com's specific talent needs, breaking down the requirements by role category, key technical skills, and crucial behavioral/operational characteristics. This is highly valuable for both Airitos.com (as a reference for their own internal hiring) and for potential external partners (to quickly identify and screen suitable candidates). It consolidates information scattered throughout the transcript into an easily digestible format, emphasizing the unique blend of technical depth and operational maturity required for successful engagement.

### 4.2. Strategic Staffing: The Contract-to-Hire Advantage

The contract-to-hire model is highly favored by Airitos.com, particularly for engineering roles.[1] This approach allows the organization to rigorously evaluate a candidate's performance, technical proficiency, and cultural fit during the critical migration phase before making a commitment to a full-time hire.[1] This model serves as a strategic de-risking mechanism for Airitos.com, especially given past negative experiences with large consulting firms, including a significant financial loss.[1] By allowing for a "cut" if a contractor proves unsuitable, it mitigates the risk associated with substantial, upfront investments in unsuccessful engagements.[1] This approach

fosters a trust-based relationship, where the external partner must consistently demonstrate value to secure continued engagement and potential conversion, effectively shifting the burden of proof to the partner.

An initial contract length of six to nine months is proposed, complemented by a nine-month no-fee conversion period offered by the external partner.[1] This duration provides ample time for comprehensive evaluation and integration into the team. Rick has also indicated considerable budget flexibility for these approved positions, particularly for contract-to-hire roles, which enables immediate staffing without the delays often associated with securing full-time employee (FTE) box approvals.[1] Furthermore, the contract-to-hire strategy is designed not just for immediate staffing but also to build enduring internal capability. The success of this model hinges on the external talent's ability to effectively transfer knowledge to Airitos.com's existing team and integrate into their operational processes, ensuring long-term sustainability of the implemented solutions. This implies an expectation for the external partner to actively facilitate knowledge sharing and team integration, contributing to Airitos.com's self-sufficiency over time.

### 4.3. Geographical & Logistical Considerations for a Global Team

Airitos.com operates with a remote-first approach for all new positions, as there is no physical office space available to accommodate additional personnel.[1] This flexibility in location is, however, accompanied by specific geographical preferences. Rick expresses a strong preference against resources located in India or Malaysia, citing significant time zone differences and past management challenges with his existing team in those regions.[1] The preferred locations for talent are Europe (specifically Europe West) or the United States.[1] While US West Coast candidates are acceptable, a preference exists for individuals located east of New York to better align with the time zone of the majority of the company's operations.[1]

### 4.4. Streamlining Contractual Engagements

The initiation of deeper engagement and talent sourcing is contingent upon the timely execution of key contractual agreements. The Non-Disclosure Agreement (NDA) is a critical prerequisite that must be signed before any detailed discussions can occur with key internal stakeholders like Austin Endo or Ralph.[1] The Master Services Agreement (MSA) is also pending, with Rick prioritizing the NDA's completion first.[1] The external partner has expressed willingness to work in parallel, commencing candidate sourcing activities while the contractual agreements are being finalized. This pragmatic approach acknowledges that the availability of strong candidates can

often accelerate the contractual review process.[1]

A streamlined candidate screening process is envisioned. Airitos.com expects the external partner to conduct the initial technical and cultural fit screenings.[1] Rick's team will then perform a final "Quality Control (QC) check," which typically involves two interviews: a technical screen (conducted by Florian for engineering roles and potentially Austin for IAM roles) and a culture fit assessment (conducted by Rick).[1] Collaboration on job descriptions is also a key logistical element. Rick possesses some existing job descriptions and can quickly develop others, with the external partner offering to provide samples to assist in this process.[1] The bureaucratic hurdles in legal and finance, which have caused delays with the NDA and MSA, are directly impeding Airitos.com's ability to address critical security and identity gaps. While Rick is eager to move quickly operationally, the absence of signed agreements prevents external partners from engaging deeply and sharing sensitive information, thereby delaying the very solutions Airitos.com urgently needs. This highlights a critical internal organizational challenge that, if not actively managed and expedited, could significantly derail the entire transformation timeline and potentially incur further costs or risks. The external partner's willingness to work in parallel is a pragmatic response to this internal bottleneck.

## 5. The Path Forward: An Iterative Approach to Transformation

Airitos.com's strategy for addressing its complex security and identity challenges is firmly rooted in an iterative project approach, a direct response to past negative experiences with large-scale, traditional assessments.

### 5.1. Beyond Assessments: Focused Discovery and Action

Rick expresses a strong aversion to traditional, extensive, and costly assessments that historically have yielded minimal tangible progress.[1] He cites a significant financial loss from a prior engagement with a large consulting firm, which merely identified problems without providing actionable solutions.[1] This experience has shaped his preference for a "very pointed," "iterative approach" that involves "a little bit of digging" to understand specific issues before proposing targeted solutions.[1] The objective is to deliver "small things, give you a deliverable, get called back," emphasizing tangible, actionable outcomes in shorter cycles.[1]

This iterative model is also designed to minimize disruption to Airitos.com's internal teams, who are currently "full boore like migrate" and cannot accommodate extensive, time-consuming assessments.[1] The approach aims to be less intrusive and more focused on immediate, actionable insights. Furthermore, the iterative model serves as

a mechanism for Airitos.com to validate the external partner's capabilities and experience on smaller, lower-risk projects before committing to larger engagements.[1] This approach is a strategic mechanism for the external partner to rebuild trust and demonstrate tangible value in smaller, digestible increments. This allows Airitos.com to validate the partner's expertise and commitment without significant upfront financial risk, fostering a collaborative relationship based on proven results rather than promises. This approach shifts the burden of proof to the consulting partner to deliver early and often, which is crucial for a client with past negative experiences.

The immediate next steps for initiating the IAM project work are clearly defined. The Non-Disclosure Agreement (NDA) must be executed as a prerequisite for any deeper engagement.[1] Once the NDA is in place, Rick will facilitate targeted introductions between the external partner and key internal stakeholders: Austin Endo, the AHEAD team's security/identity lead, and potentially Ralph, Airitos.com's identity specialist.[1] The purpose of these initial discussions is to gain a foundational understanding of the current landscape and for the external partner to ascertain their capacity to assist.[1] Following these calls, the external partner is expected to provide a concise "one pager" summarizing their understanding and initial recommendations.[1]

### 5.2. Recommendations for Accelerated Progress

To accelerate Airitos.com's transformation journey and maximize the effectiveness of external engagement, several key actions are recommended:

- **Expedite Contractual Agreements:** Prioritizing the swift signing of both the NDA and MSA is paramount. These legal frameworks are essential to enable immediate and deeper engagement, facilitating the sharing of sensitive information and the formal commencement of project work and candidate sourcing.
- **Leverage Iterative Discovery for IAM:** The proposed iterative approach should be fully embraced for the IAM transformation. This involves initiating with the planned introductory calls and a small, focused project aimed at exploring specific automation opportunities within SAP identity management, an area where Rick already has existing plans and quotes.[1]
- **Parallel Talent Sourcing:** Concurrently with the IAM project discussions, active sourcing of candidates for security engineering and identity roles (utilizing the contract-to-hire model) should proceed. This strategy should leverage the agreed-upon remote work flexibility and preferred geographical locations to identify and onboard critical talent swiftly.
- **Collaborate on Job Descriptions:** Close collaboration with Rick to refine or develop comprehensive job descriptions is essential. This ensures that the descriptions accurately reflect the specific need for hands-on, independent, and

compliant-environment-experienced talent, streamlining the recruitment process.

## Conclusion: Charting a Course for Secure and Automated Growth

Airitos.com stands at a pivotal juncture, poised to transform its security and identity landscape through a strategic migration to the Microsoft Azure stack. The challenges are significant—a complex, manual IAM environment, a critical talent deficit, and the burden of legacy systems—but the vision for an automated, compliant, and efficient future is clear. The organization's past experiences with large, unproductive consulting engagements have instilled a preference for a de-risked, iterative approach to transformation, emphasizing tangible deliverables and a focus on building trust through demonstrated value.

By strategically acquiring hands-on, independent expertise through a flexible contract-to-hire model, Airitos.com can accelerate its Azure migration and untangle its intricate identity management issues. The successful execution of this transformation hinges on expediting foundational contractual agreements, initiating focused, iterative discovery projects in IAM, and maintaining a proactive approach to talent acquisition. This strategic imperative will not only significantly enhance Airitos.com's security posture and operational efficiency but also strengthen its position with its high-security clients, charting a clear course for secure and automated growth in a complex global landscape.

**Works cited**


1. Bill and Rick - Jan 8, 2025.pdf
2. Microsoft Entra ID (formerly Azure Active Directory) | Microsoft Security, accessed May 30, 2025, https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id
3. What is Microsoft Entra ID? | Azure Docs, accessed May 30, 2025, https://docs.azure.cn/en-us/entra/fundamentals/whatis
4. What is Azure Active Directory B2C? | Microsoft Learn, accessed May 30, 2025, https://learn.microsoft.com/en-us/azure/active-directory-b2c/overview
5. Technical and feature overview - Azure Active Directory B2C | Microsoft Learn, accessed May 30, 2025, https://learn.microsoft.com/en-us/azure/active-directory-b2c/technical-overview
6. Overview: B2B collaboration with external guests for your workforce, accessed May 30, 2025, https://docs.azure.cn/en-us/entra/external-id/what-is-b2b
7. What is Microsoft Entra B2B Collaboration? - YouTube, accessed May 30, 2025, https://www.youtube.com/watch?v=1TWxB4VYdJc

8. Microsoft Sentinel: 5 Key Features, Limitations & Alternatives - Exabeam, accessed May 30, 2025, https://www.exabeam.com/explainers/microsoft-sentinel/microsoft-sentinel-5-key-features-limitations-and-alternatives/
9. Microsoft Purview: Data Security and Governance, accessed May 30, 2025, https://www.microsoft.com/en-us/security/business/microsoft-purview
10. Microsoft Purview Data Governance | Microsoft Security, accessed May 30, 2025, https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-data-governance


www.airitos.com