AUJAS
CYBERSECURITY
An NSEIT Company

aujas.com

SUCCESS STORY | IDENTITY AND ACCESS MANAGEMENT

# Digital identity powered tech innovation and growth

## Identity and access management program for a global telecom giant: Past, present and future

# Introduction

In recent years, the world has been experiencing a significant rise in digital business and e-government initiatives. The client's home country has been actively working to diversify their economy and move toward a digital future. As a result, the government has launched several initiatives to promote digital transformation, and the private sector has also been quick to embrace digital technologies. The telecom industry has been an essential driver for this growth, providing the necessary infrastructure and services to support the country's digital ambitions.

The rise of digital business globally has been impressive. The client's home country has seen a surge in e-commerce and online marketplaces, with consumers increasingly turning to digital channels to shop and make payments. The country's government has also launched several initiatives to support entrepreneurship and innovation in the digital space, such as a fintech initiative, which aims to promote financial technology startups. The telecom industry has been instrumental in enabling this digital business growth by providing highspeed internet, mobile connectivity, and digital payment solutions. E-government initiatives have also been a key focus for the country's digital transformation efforts. The government has launched several digital services, such as the Absher platform, which provides citizens with access to a range of government services online. The telecom industry has played a vital role in enabling these initiatives by providing secure and reliable connectivity, as well as developing digital identity solutions to ensure the authenticity and security of online transactions. The government has also launched several initiatives to promote digital skills and literacy, such as the Digital Skills Initiative, which aims to equip the workforce with the skills needed for the digital economy. With continued investment in digital infrastructure and skills development, the country is poised to become a leader in the digital economy in the region. It is essential to promote this growth in a secure, reliable, and trustworthy manner.

# About the client

Over the years our client has evolved into a multifaceted conglomerate, offering an extensive array of services that span far beyond conventional telecom offerings. While it provides traditional fixed line, mobile and internet services, they have emerged as a leader in providing 5G services, high-speed internet, cloud computing, and Internet of Things (IoT) solutions.

Their commitment to delivering reliable and cutting-edge services has enabled them to connect individuals, households, businesses, and industries on an unprecedented scale. Our client's influence extends beyond the borders of their home country through strategic international ventures and partnerships. These initiatives allow them to contribute to the global telecommunications landscape while leveraging their expertise to empower other nations with advanced communication solutions.

# Challenges

In the realm of innovation, our client stands as a visionary. The company has proactively embraced emerging technologies and trends, transforming themselves from a conventional telecom provider into a digital enabler. To stay ahead of the curve, they are continuously investing in advanced IT and telecom infrastructure that has numerous components, servers, and clients running on heterogeneous hardware and software platforms which adds the complexity of securing and managing normal and privileged identities. The issue is complex; from granting users timely and appropriate access to their assets, managing the user's lifecycle, and local and privileged access to business-critical systems and applications.

The complexity in the client's digital infrastructure arises from multiple factors such as the size of the network, the range of services offered, the technology used, the geographical coverage, and the number of subscribers. Such a diverse and complex access landscape is managed by providing different layers of access control and a solid framework. The framework's core is based on the discovery of all identities (all users, accounts, service IDs, privileged accounts, etc.). Identity functions layer adds all the functional capabilities to the identities. A successful Identity & Access Management program covers all the digital assets that require user identification and authentication thus providing help in building a modern identity program to enable security as well as digital business transformation.

### IT & Security Programs

- Regulatory Compliance
- Access Security
- Zero Trust Security
- Subsidiaries, Customer and Partner Access Management Experience
- Application Modernization
- Data Engineering And Analytics
- DevOps

### Digital Assets

- Network Elements Telecom Devices
- IT Services
- Business Applications
- Database/Dataware/
- Data Lakes
- APIs & Microservices
- BSS & OSS

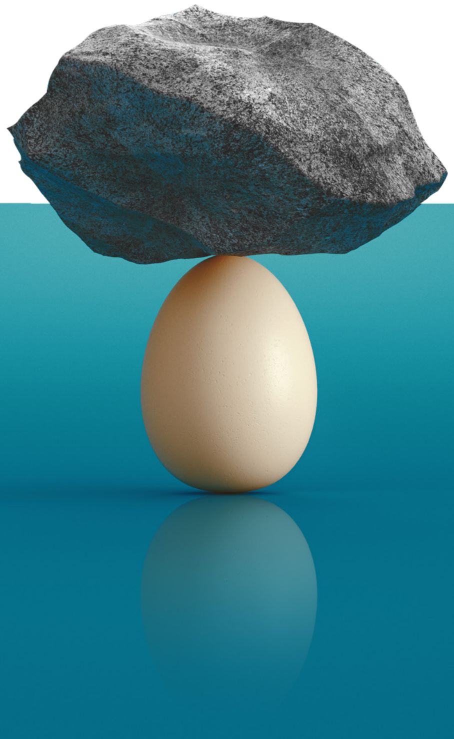
### Identity Core

Identity

- Employee
- Partners
- Clients
- Bot ID

### IT & Security Programs

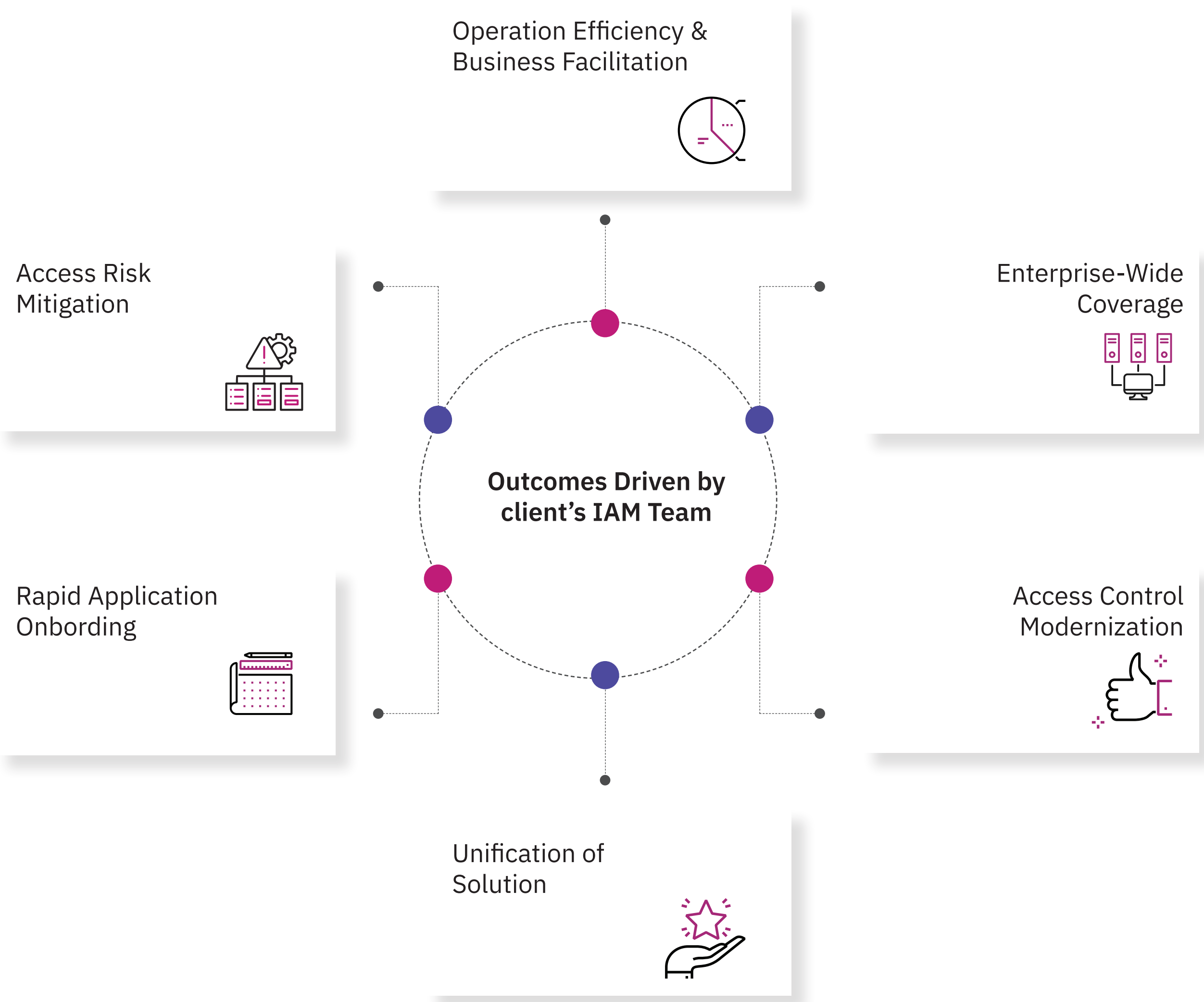
- Authentication
- Authorization
- Account Management
- Access Governance
- Federated Access
- Key Vaulting
- Directory Services



## The client's identity and access management (IAM) landscape

In the realm of innovation, our client stands as a visionary. The company has proactively embraced emerging technologies and trends, transforming themselves from a conventional telecom provider into a digital enabler. To stay ahead of the curve, they are continuously investing in advanced IT and telecom infrastructure that has numerous components, servers, and clients running on heterogeneous hardware and software platforms which add the complexity of securing and managing normal and privileged identities. The issue is complex; from granting users timely and appropriate access to their assets, managing the user's lifecycle, and local and privileged access to business-critical systems and applications.

The complexity in the client's digital infrastructure arises from multiple factors such as the size of the network, the range of services offered, the technology used, the geographical coverage, and the number of subscribers. Such a diverse and complex access landscape is managed by providing different layers of access control and a solid framework. The framework's core is based on the discovery of all identities (all users, accounts, service IDs, privileged accounts, etc.). Identity functions layer adds all the functional capabilities to the identities. A successful Identity & Access Management program covers all the digital assets that require user identification and authentication thus providing help in building a modern identity program to enable security as well as digital business transformation.


Operation Efficiency & Business Facilitation
Access Risk Mitigation
Enterprise-Wide Coverage
Outcomes Driven by client's IAM Team
Rapid Application Onbording
Access Control Modernization
Unification of Solution

## Outcomes driven by the client's IAM team

### Access control modernization

- Alignment with overall IAM strategy
- Alignment with business stakeholders
- IAM technology integration to achieve an ecosystem for access control
- Covering IT/non-IT apps for access governance and lifecycle management

### Enterprise-wide coverage to IT, non-IT, and telecom environment

- Expanding the IAM coverage to all the critical and high-risk IT applications
- Expanding IAM coverage to non-IT assets that include network and telecom devices, OSS/NMS, etc.

### Unification of solution

- Building a unified and interconnected IAM solution
- Consolidating silos IAM solutions to decrease complexity and improve application performance
- Complementing telecom and network solutions that can manage remote access to normal and privileged users

### Rapid application onboarding

- Setting up a governance committee involving members from application, IAM implementation, design and, operations team
- Defining the process with a clear approach, SLAs, dependencies, and general prerequisites
- Automating data collection
- Streamlining all app integration steps into a unified integration factory process

### Access risk mitigation

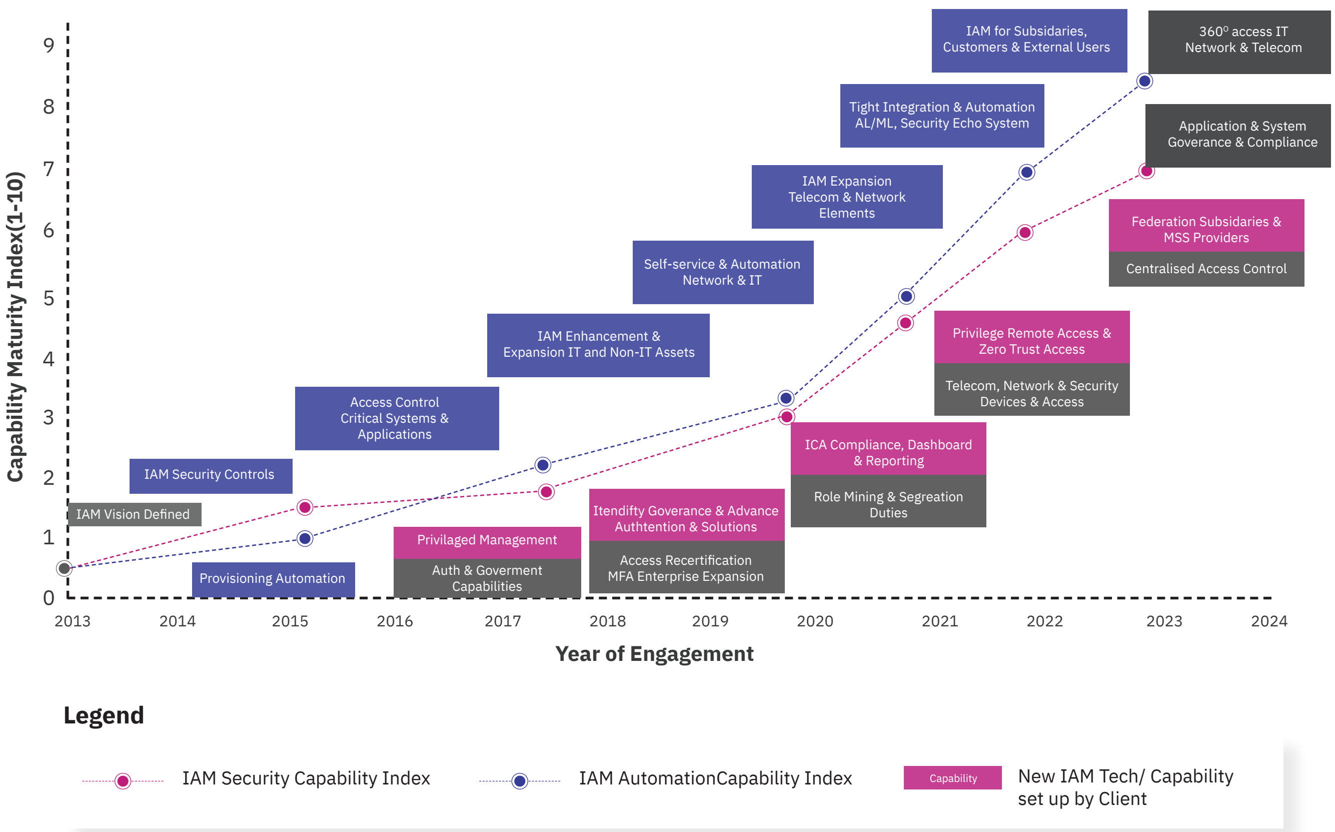
- Policy-linked configuration and enforcement
- Compliance with policies for security and privacy
- Periodic reviews to identify anomalies and privileged access
- Implementation of RBAC
- Internal and external audit reports and evidence

### Operation efficiency and business facilitation

- Reducing complexity and providing user-friendly interface for increasing satisfaction and widespread adoption across the enterprise
- Establishing IAM as an enabler by supporting business needs while helping to reduce risks created by emerging technologies and threats

## Journey toward world-class IAM program

Building the IAM program - Increasing IAM capability over a decade



## Digital identity

As one of the telecom leaders in the Middle East/ EMEA, the client possesses a vast array of digital and tech assets that must be protected. These assets include critical business applications, enterprise apps, core telecom network systems, OSS systems, BSS systems, and many others. The client's IT infrastructure is the backbone of their operations, and any disruption or cyberattack can have severe consequences for their customers and the company.

Therefore, they needed to adopt a digital identity first approach to cybersecurity to ensure protection of their assets.

This approach would allow the client to monitor and control access to sensitive data and applications, ensuring that only authorized users can access them. A digital identity-first approach would enable the client to mitigate the risk of cyberattacks, reduce the impact of any potential breaches, and ensure the integrity and availability of their systems.

> “ A strong cybersecurity foundation starts with a focus on digital identity. It provides a secure framework for managing access to digital resources and critical targets. Verifying the identity of users and devices accessing systems helps build trust and transparency for the client. ”

## Challenge - IAM modernization from essentials to a world-class platform

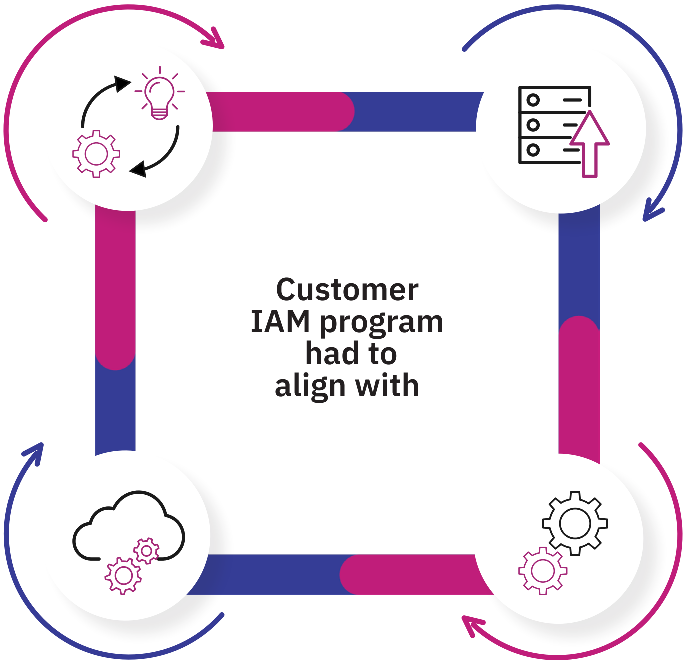
The client started with an IAM program focused on essential controls more than a decade back. The first step was to define the vision of the IAM program and start with practical and achievable goals. The principal challenge was to set up the IAM Program while aligning it with the following four immutable constraints and business parameters.

### The client's overall business evolution

During this period the client was to evolve and add niche acquisitions and set up new subsidiaries. This has an impact on the types of users protected and processes consumed by IAM for automation.

### Technology spread

The technology was supporting both wireless and fixed-line fiber optic. This meant the IAM program was to protect a heterogeneous environment, with varied interfaces.



### Cloud transformation and app modernization

Apps were to be changed which would impact IAM design, application integration methods, and application availability.

### Backward compatibility of the processes

The processes were fully designed with redundancies, checks, and balances required in a manual operations mode. This implied IAM was to support evolving processes with extra compatibility checks.

aujas.com

## Strategy design and solution approach

In view of these tricky requirements and controls, a specialized IAM program design was required. These four design principles served as the guiding approach for all aspects of the IAM program. The most important aspect after setting the design principles was to create the execution and functional framework for IAM.

### The right design framework for IAM

The client started with an IAM program focused on essential controls in 2010. The first step was to define the vision for executing the IAM Program. A 7-R Framework was designed for the execution of the IAM Program based on the following parameters:

### Right strategy

The right strategy is to adapt to changing times and needs instead of going ahead with fixed-intime programs.

### Right design

The Four Design principles were used to develop the right functional framework for IAM. At a broad level, IAM issues were divided into three layers:

- **Source of Truth layer**

Master Directory of all approved users and systems participating in business transactions. This layer contains all systems required for synchronization and virtualization of various user data stores to create a unified, normalized, and de-duplicated user store which is used by various components of the IAM program.

- **Transactional layer**

Subsystems, components, policies, and mechanisms to evaluate and grant access to the right systems and users in real-time. This layer in turn contains all subsystems required for single sign-on, multi-factor authentication, policy evaluation enforcement as needed for real-time decision, e.g., in adaptive authentication, thick client SSO, standards-based Web SSO, federation, cloud access control, privileged session management, and other such technologies.

- **Administrative layer**

Responsible for ensuring that the right users are set up with the right permissions, with the right reasons for the right period. This layer contains systems for self-service, user ID creation, maintenance and removal, management of permissions, and privileges across numerous apps and systems, governance of access assignment, process automation workflows, and detection of dangerous access pattern along with reports and alerts. The three layers were to be designed and built, interconnected, and interoperated along with changing business needs and technical readiness.

### Right Technology

A custom technology evaluation specification was designed keeping the client's functional, business, and technical requirements at the forefront. In addition to incorporating technological features and functionality, these criteria also included aspects like system maintainability, longevity, interoperability, and cost of scaling up. This technology set was used iteratively to identify the right technology for all modules, stages, and phases of the IAM program.

### Right partner

The IAM program required a versatile, managed, and driven IAM solutions development team with expertise and experience in IAM strategy, engineering, and operations. Over the years, the client has involved specialist partners for various purposes including solution design, solution development, independent assessments, and validation, as well as operations. They prioritized subject matter expertise over other traits along with a strategy of rewarding performance with increased responsibility. This strategy allowed them to leverage the best skills in the industry to build out the IAM program.

### Right metrics

Metrics are essential for directing the progress of the IAM programs. The right metrics can be used to incrementally build essential capabilities within the system in an organic fashion. Metrics were layered starting from business outcomes and going down to system performance metrics. The business outcomes included areas like end-user experience, visibility into access risk, compliance with specific controls, reduction of turnaround time for remediating risky access patterns and over permitted accounts, and time taken to allow external users secure access to specific systems among others similar metrics.

### Right communication

IAM Programs can bring in several benefits for both internal and external users.

The requirements and perceptions of various stakeholder teams can vary significantly and often require normalizing, interpretation, translation, and collation. As a result, it becomes important for the IAM program to apprise various IAM stakeholders of the progress of the program.

### Right innovation

Executing an IAM program of this magnitude requires solving unforeseen challenges at every juncture despite best planning. This is due to the fact that the operating environment, technology advancements, IAM methodologies, and cybersecurity threats are all in a constant state of flux. In order to meet the objectives of the IAM program despite such changes in the context, an innovative approach is needed that places a significant emphasis on improving and innovating. It was essential to allow the team to practice courage and curiosity and provide multiple solution candidates for the problems faced during the program. A scientific proof of concept-based approach was adopted for trying out several novel solutions for problems that had remained unsolved for a long period. Four design principles were selected for the IAM program.

## Principles for IAM Program

### Layered and Incremental

The goal was to start with foundational layers, expand them to reasonable coverage, and then layer more sophisticated functionality on top of it.

### Modular and interoperable

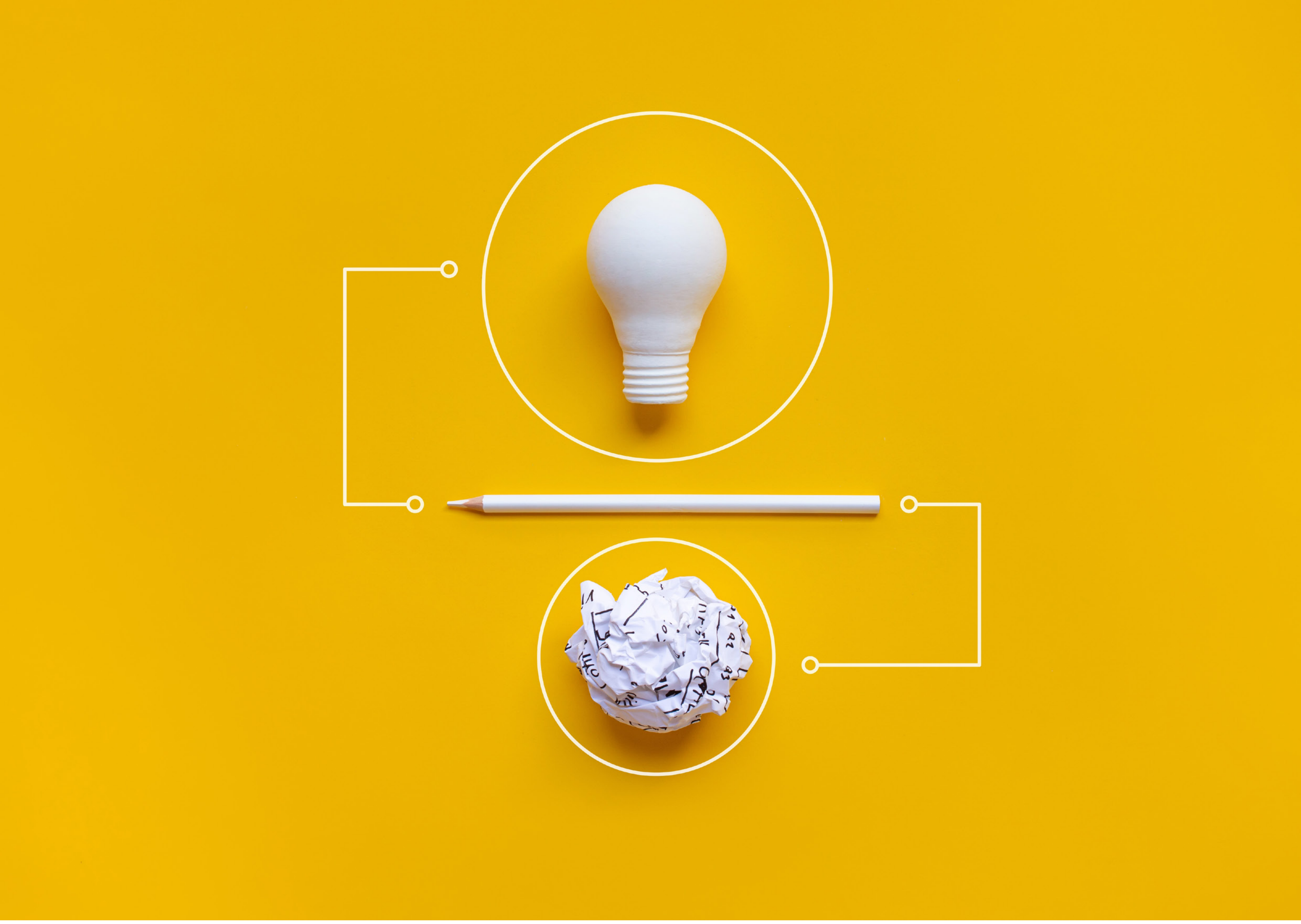
For the second design add, remove, or replace a part of the IAM program without making the rest of the program dysfunctional. “A module for each functional need” – was a design objective.

### Best of breed

The IAM technology and methodology had been under constant and increasingly rapid evolution at the time of planning for IAM for the client. Sustained innovation across large product suites was a declining trend as evidenced by analyst reports as well. It was decided to select leading tech products for each category to benefit from the best-in-class innovation.

### Scalable and elastic

As the solution was to be developed for a set of key systems and then expanded later to cater to larger IT and business sections, the program had to be designed with scalability and extensibility as key design parameters.



# The **Solution**

Aujas Cybersecurity started the execution of the IAM program by setting up a strategy based on a scalable approach.

Aujas Cybersecurity's IAM program adopted a strategic, scalable, and iterative approach. By retiring legacy systems, prioritizing applications, and implementing a sophisticated Integration Factory Model, the program aimed to enhance security and access management systematically and effectively.

Aujas Cybersecurity's IAM program, launched in 2010, implemented a Matrix approach for scalability. Initial efforts involved setting up core IAM systems, including directory servers and access managers. Legacy systems were retired and replaced by leading Identity Management and Privileged Access Management solutions.

To prepare for rapid scale-up, standardization efforts focused on directory structures, user nomenclature, and IAM policies. An innovative Integration Factory Model was adopted, shifting from traditional waterfall integration to an assembly line approach. This facilitated iterative tasks for application onboarding and system maturity scale-up.

The program expanded coverage by prioritizing applications based on business criticality and ease of integration. An application inventory analysis led to categorization (Gold, Silver, Bronze), guiding project teams in terms of effort and cost estimation.

## Goal-based sub-projects

The IAM Program was divided into goal-based sub-projects to make sure that the outcome can be measured in quantitative and qualitative factors to achieve the overall goal. Key goals from the IAM program were.

### Risk reduction

One of the key goals of the client was to prevent attackers from gaining unauthorized access to sensitive data and systems. IAM solutions focus on preventing resources from unauthorized access and mitigating risks from excessive permissions, misconfigurations, abuse of privileged access, identity theft, and identity fraud.

### Regulatory compliance

Governance of identities and access, and automation of access review was essential for the client as well as regulatory requirements. With time the regulatory requirements related to IAM have only become more stringent.

### Business facilitation

Another important sub-goal of IAM was to allow a smoother and non-disrupting business experience. While in traditional scenarios, users must request for access rights in various forms, through manual process, centralized IAM provides a standardized and easy-to-follow workflow-based automated process for requesting identities, user accounts, or access rights. This also reduces human errors. The client divided the entire IAM program into small manageable projects with clear achievable goals.

### IT cost reduction

Legacy manual processes of creating Identities, granting access, and providing helpdesk support to resolve issues related to IAM costed money and led to wasted productive hours by the end users. IAM solutions help in reducing the overall IT costs by automating the user identity and access lifecycle management process.

## Partner selection

IAM initiatives are typically complex and involve specialized knowledge. The client was clear that the partner of choice must have strong IAM domain experience, understands their unique needs and requirements, have a proven track record of successful IAM implementations, and strong focus on security and compliance. The client partnered with us to help them develop the IAM roadmap, assess and select the right IAM solution, provide IAM implementation and system integration, and sustain and enhance the maturity of IAM processes post-deployment. Our consulting services helped them ensure the selection of the right system for their needs and implement the program effortlessly. For technology

## Automation

Automation was one of the core principles behind adopting and implementing IAM. By implementing IAM solutions the client aimed to streamline the process of managing user accounts, access permissions, enforcing security policies, achieving compliances, reducing risks from human error, reducing the time and effort in managing user accounts and access, and enhancing the overall efficiency. The client has gone one step ahead and leveraged new-age automation and robotics to integrate legacy systems, and applications and automate repeatable human tasks. Automation of end-to-end access management lifecycle helped in reaping all the benefits that IAM solution has to offer. It helped in:

### Streamlined operations

The use of sophisticated algorithms and access authorization workflows eliminated human intervention and helped in seamlessly verifying and managing crucial tasks such as – access provisioning, deprovisioning, visibility into third-party integrations, and more.

### Secure access provisioning

Automation of the entire access management lifecycle ensured secure operations and reduced incidents from human error – beginning from secure access provisioning during employee onboarding, tracking their accesses and permissions, to deprovisioning during employee offboarding.

### Enhanced productivity

Without the need to manually manage systems and processes, users were able to focus on performing more important tasks that need their attention, increasing user productivity, reducing human error, and more efficient usage of the resources in the IT department.

### Compliance and audit readiness

Automated IAM process ensured quick and seamless updates of passwords, accounts, and personal identity information. This made it easier to comply with the client's policies and offered complete visibility to user activities with detailed reports and automated dashboards.

### Robotic process automation (RPA)

Aujas Cybersecurity introduced a virtualized workforce to streamline and enhance operational efficiency for the client. This robotic process automation (RPA) initiative has significantly transformed the handling of manual tasks, bridging gaps, improving results, reducing costs, and enhancing workplace satisfaction. The digital identity needs of the client were met through the implementation of RPA, enabling the automation of repetitive and rule-based business processes.

Aujas Cybersecurity's Robotic IAM services leverage RPA to mimic human actions performed by administrators on machines, interacting seamlessly with IAM systems. This automation is scalable, allowing the client to automate various processes efficiently.

### Platform for User Lifecycle Management (PALM)

Aujas Cybersecurity's PALM played a crucial role in the client's end-to-end integration and onboarding of applications to IAM solutions. PALM is a novel cross-platform solution for automated app integration with IAM is, available as cloud-native SaaS or on-premises. The platform's automated application integration factory model streamlines the integration process, automating tasks from requirement collection to code generation. PALM ensures a secure and efficient way to integrate apps with IAM products, tackling the challenges associated with manual and traditional integration models. The solution addressed key challenges for the client including:

**Faster and secure Integration**

PALM significantly reduced errors and the need for rework, enhancing the efficiency of the integration process.

**Reduced RoI challenges and access risks**

PALM mitigated Return on Investment (RoI) challenges in IAM, reducing the risk of unauthorized access and ghost accounts.

**Error elimination and rework reduction**

PALM facilitated quicker and more secure application integration, overcoming the traditionally time-consuming process.

**Simplified IAM configuration audits**

The platform simplified IAM configuration audits, providing a streamlined approach to ensure compliance and security.

**Addressing access risks and MRAs**

PALM helped in identifying and addressing access risks and potential Major Risk Areas (MRAs) through insightful data analysis.

**Results delivery with workforce efficiency**

PALM delivered successful outcomes while simultaneously reducing the engineering workforce, optimizing efficiency.

## Core Features

- Excel-based documentation to a secure web-based process
- Rapid onboarding in leading IAM products
- Change control and digital tracking of sign-offs and version history
- Dashboards, statistics, and reporting

## Benefits of PALM

**Increased Efficiency and Security**
25% efficient access profile process.
85% efficient app integrations with IAM.

**Part of the Ecosystem**
Interconnected with other systems in the Enterprise Ecosystem

**Workflow Driven**
Platform built with RACI (Responsible, Accountable, Consult, Inform) at its core

**Accurate Access Structure**
Accurate collection and representation of entitlement structure

# Business **Outcomes**

With IAM, the client ensures prevention of data misuse, and compliance with government regulations.

## Digital identities interacting with a telecom corporation

Some of the best IAM practices that we have incorporated into the client's IAM strategy are as follows:

**Adoption of password-less authentication**

The client is on the path of eliminating password issues by choosing password-less authentication to protect vital business data and ensure that only authentic people access their systems and resources. password-less authentication shall enable users to authenticate their identity without entering a password. There are various benefits for the client to become password-less, including enhancing overall efficiency, saving time, improving productivity, and providing greater ease of access. But, most importantly, password less authentication shall allow users to access the environment safely and securely.

**Use of appropriate DevSecOps tools**

The client was able to create a strong strategy for DevOps and it will help prevent data breaches and ensure no one can access sensitive data. By using various DevOps techniques, the client keeps track of the unstructured data from the initial stage and boosts the overall security level.

**Use of Artificial Intelligence (AI) and Machine Learning (ML)**

As a part of the IAM program, the client adopted AI and ML technologies to reduce the threat vector. AI has helped the client to ensure improved security and maintain business integrity. Using AI technology monitors and reveals the abnormalities in user behavior. The client produces a significant quantity of unstructured data, and the ML system scans all the data efficiently and prevents data leaks and breaches. Moreover, the AI system constantly monitors user behavior and ensures that verified users have access to system and network resources. If, by any chance, threat actors gain access to the network by any backdoor, the AI system sends a quick alert to the IAM solution so that appropriate action can be taken thus denying access and ensuring the safety of business data.

**Additional best practices**

Apart from the practices mentioned above, we helped the client enforce some common IAM practices. These include:

- Ensuring new applications from all sources are securely developed and onboarded. For this purpose, we helped the client deploy API access control (authentication and authorization of APIs) as it is a crucial part of API security.
- Enforcing use of multi-factor authentication, step-up authentication, and risk-based authentication methods to authenticate the identity.
- Reduce periodic campaigns to remove unnecessary users from the network to reduce need for recertification.
- Ongoing reviewing and auditing of the IAM policies to ensure users are granted the least privilege in line with their role of work.

## New frontiers - the cloud and beyond

We helped the client conduct an extensive evaluation of the deployment approach for the IAM solution, one being the cloud and the other for on-premises while taking into consideration the compliance with local regulations and data residency before the approach was finalized. The client understands that the cloud based IAM practices are fast-growing and demand for cloud adoption has increased over time.

### IAM for cloud and from cloud

We are helping the client to build the following capabilities as a part of their Cloud IAM strategy:

- Identity provider (IdP)
- Open protocol support
- Access control for legacy apps
- Standard-based provisioning and deprovisioning
- Analytics and reporting

|  | HOSTING | CAPABILITIES | READINESS |
|---|---|---|---|
| IAM For Cloud | IAM FOR CLOUD | • Provisioning of SaaS apps for client's users<br>• Seamless utilization of SaaS apps for client's users | Fully Ready |
|  |  | • Internal IAM components for standard-based provisioning are deployed<br>• Open protocol SSO is implemented | Fully Ready |

|  | HOSTING | CAPABILITIES | READINESS |
|---|---|---|---|
| IAM From Cloud | IAM FROM CLOUD | • Ability to relocate client's IAM on client's Private Cloud<br>• Set up components in hybrid cloud model using DevOps approach<br>• Deliver Cloud IAM services to client and others | Partially Ready |
|  |  | • Use IAM Software Deployed on Public Cloud<br>• Modular IAM design allows cloud IAM integration and ease of management<br>• Standard-based approach allows cloud IAM plug-and-play | Partially Ready |

## Zero trust - Boundaryless solution for IT, network and telecom security

We are enabling the client to adopt the zero-trust architecture ensuring that IAM policies are followed whenever the user accesses the organization's network and protects the data at rest and in transit. We help the client monitor and determine the relationship between the apps and then enforce the rules. In addition, we are also empowering the client to use other technologies like MFA, endpoint protection, micro-segmentation, and visibility and analytics to execute zero-trust systems.

### IAM-based trust fabric

We are helping the client build the identity fabric that will define the users who are online and unique to them. People may have similar online profiles, but their Identity Fabric is how they can work and perform different activities online. This shall be intricate, interwoven linking for users online.

### The impact of identity fabrics on the client

We are helping the client build a hub system for most services users require as an employee or non-employee due to the pervasive existence and use of identity fabric. It relies on the ability to identify users online with a unique identity.

### The Impact of zero trust on the client

Zero trust, on the other hand, is part of the operational model that the client's access control team has developed and blended into their approach to IAM, using it to control access to assets in a flexible, manner. It becomes clear that it would be impossible to maintain a zero-trust architecture without the use of trust anchors within an identity fabric.

### Expand IAM coverage subsidiaries and customers

- Majority of apps yet to be protected by IAM
- Partial management of currently integrated apps
- Non-IT assets in telecom network not connected
- Limited network assets like OSS/BSS integrated with Access Control

### Mitigate access risk for telecom network

- Set up modem PAM solution with network PAM-ready use cases
- Increase governance with enterprise IGA
- Set up zero trust based approach
- Set up identity analytics for insider threat detection and prevention

### Identity analytics

- Gain visibility of actions in the perimeter less IAM environment
- Identity threat detection and response

### Develop zero trust access fabric

- Setup and integrate foundational ZTA components
- Identity services, MIDM, access control, remote access, PAM, analytics
- Develop ZTA strategy
- Prioritize ZTA use cases
- Pilot with ZTA-based remote access replacing VPN

### Expedite routine IAM tasks

- Automate tasks that are still performed manually
- Utilize robotics and RPA to rapidly eliminate manual tasks
- Enhance security by eliminating errors and omissions by humans
- Achieve standardizations across procedures

### Digitally connect with customers and partners

- Setup robust consumer IAM (CIAM) solution
- Provide centralized IAM solution to client's subsidiaries
- Prepare foundation to offer IAM as a service to the Saudi market
- IAM as a Service - Expand to government departments and ministries

# The **way ahead**

In the years ahead, we aim to enable the client

1. Optimize resource usage by using a consolidated pool instead of individual silos for each service.
2. Reduce cost of operation by automating common tasks, standardizing the environment, and providing self-service features for affiliates, heir administrators, and to end users.
3. Meet compliance with the local regulatory requirements and international standards.
4. Achieve faster time to market, with a secure, ready, reliable, and scalable infrastructure, to provision new affiliates easily.

We will continue to support the client in expanding their IAM program and strategy with leading technologies, enabling them to lead the world in fortifying digital identities for a secure and successful digital transformation.

# About **Aujas Cybersecurity**

**Aujas Cybersecurity -An NSEIT Company** empowers clients with enhanced security resilience by minimizing the potential for attacks, threats, and risks. We specialize in architecture risk analysis, comprehensive threat modeling, rigorous penetration testing, and secure coding guidelines. By partnering with us, you can strengthen your security defenses and maintain a robust security posture.

For more information, visit us at **www.aujas.com** or write to us at **contact@aujas.com.**

**Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore**

**Follow us at:**