IAM Strategy Assessment

Identify and close IAM security gaps to reduce your threat landscape

Atos IAM Strategy Assessment Offering

Compromised credentials and excessive access continue to be major contributors to the risks faced by organizations today.

According to the 2022 DBIR Report (Data Breach Investigations Report) 82% of breaches involved the human element and 63% of the data compromised is credentials

Organizations today need to invest in modern IAM technologies to transform their IAM program for the following reasons:

- Respond to emerging cybersecurity threats, mitigate risks
- Increase visibility into who has access to what, why they have the access, and how they are using the access
- Speed up compliance in the face of a rapidly evolving regulatory landscape
- Manage an increasing volume of identities requiring access to resources
- Improve user experience and enable secure digital transformation

Identity and Access Management (IAM) programs enable secure, fast, and efficient access to resources and data for humans and non-humans.

When you choose our IAM assessment services, you will gain a proven, practical, and repeatable way to identify and close IAM security gaps against leading industry standards - and you will create a clear picture of what you must do to transform and modernize your IAM program.

Comprehensive approach. Successful outcome.

We provide an approach to assessing your IAM program maturity to understand the current state of your IAM program, identify priorities, provide actionable recommendations, and define a clear roadmap.
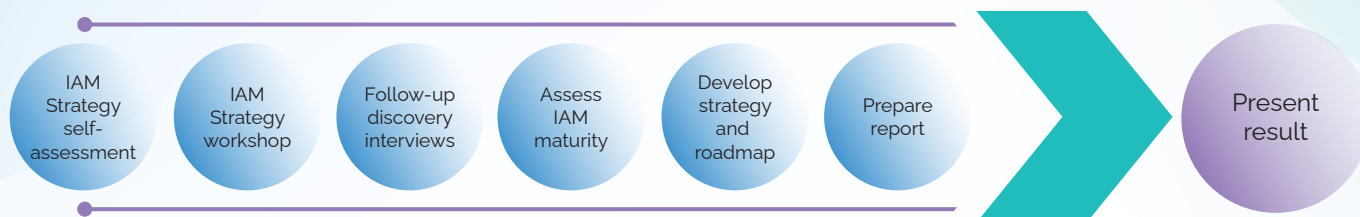
Our methodology is structured around a few simple but proven steps to ensure that our world-class security experts understand your goals, deliver the desired outcomes, and ensure that you have a clear plan on how you will proceed with your IAM strategy.

The assessment includes a review of the following:

- » The top CIO / CISO priorities for the next 12 – 18 months
- » IAM business processes (onboarding, offboarding, transfers, access requests, access reviews)
- » IAM-related security policies and compliance controls (access control, privileged accounts, authentication, passwords, segregation of duty)
- » Current IAM architecture, processes, and tooling

We perform a "deep dive" on every detail of your IAM security:

- We conduct joint workshops to define your IAM ambition and establish the scope of the assessment. To quickly start the engagement, we ask you to complete a self-assessment questionnaire followed by discovery interviews.
- We analyze your existing environment to identify gaps and assess the tooling, policies, and processes to determine the current level of maturity of the workforce IAM program.
- We assess the state of workflows, evaluate Interdependence between systems and look at the regulatory compliance requirements.
- We determine priorities based on a business aligned approach, establish a clear strategy, and deliver an organized step-by-step roadmap including possible quick wins. We also document findings discovered along with actionable recommendations for remediation.

IAM Strategy self-assessment → IAM Strategy workshop → Follow-up discovery interviews → Assess IAM maturity → Develop strategy and roadmap → Prepare report → Present result

Atos

Every IAM consulting service:

- Follows a proven step-by-step approach that aligns with industry standards.

- It is built and delivered by experienced, front-line IAM security consultants.

- Deploys non-invasive processes that do not interfere with business operations.

- Provides both executive-ready reports and precise technical recommendations.

- Gives you an IAM roadmap to improve your security rapidly and seamlessly.

Powerful analysis. Clear next steps

At the end of every IAM assessment, we will provide a well-defined suite of deliverables that crystalize our assessment in a series of actionable strategies and next steps. Our deliverables include a detailed IAM strategy assessment report and presentations to the project sponsors and key personnel.

- Structured, executive-level briefing, report and next steps.
- A baseline view of the current state maturity of the IAM program based on a standard IT maturity framework.
- Detailed findings with specific actionable recommendations for remediation. The information provided can be factored into an overall Cybersecurity risk profile.
- Recommended strategy and 24-month roadmap that can form the basis for a business plan and will answer the question, "Where do I start?".

What you get: key outcomes

Program evaluation

Detailed report outlining your assessment's scope, the methodology we followed, and all our findings organized by security domain.

Roadmap

Clear, visual representation of your short and long-term recommendations for transformation. They will be placed on a timeline to project when you should execute each recommendation.

Improvements

A prioritized list of every technical and organizational finding we uncovered along with actionable recommendations for remediation.

Great benefits

By partnering with Atos for your IAM Strategy Assessment, you will receive guidance on building a fundamentally more secure, and agile environment for your organization.

Compliance readiness

Find out how your IAM program complies with specific standards.

Security domains

Get a specific analysis on dedicated security domains, as an example you can understand how your IAM policies work for non-human identities.

Why Atos

We provide end-to-end IAM services capability from consulting and advisory to technology implementation and integration and operational managed services including an "as a Service" delivery model!

We are recognized globally as a leader in cybersecurity services and the #1 MSSP (Managed Security Services Provider) by revenue according to Gartner.

Atos has been delivering complex and multi-national IAM solutions for 25+ years.

Take the next step

Contact us to schedule your IAM Strategy Assessment today. We will rapidly structure your engagement and help you take the right next steps to identify and close IAM security gaps in your organization!