Digital Identity and Access Management Assessment

IAM Strategy and Associated Program Maturity Assessment **with Focus on Azure**

AdNovum

About AdNovum IT Consulting

AdNovum is among the elite Swiss IT companies able to realize complex and demanding projects. AdNovum is a full-service provider of software and security systems for customers with considerable technical and commercial requirements. Renowned organizations from a variety of fields and the public sector trust AdNovum's competence and the strength of its IT service offering as well as its innovative products and solutions.

AdNovum's solutions combine standard products of renowned vendors with open-source software and open standards. Modular in nature, they seamlessly blend in with existing system environments and can be easily extended. This results in sustainable high-performance reference projects.

www.adnovum.ch

Zero Trust Model for Cyber Security

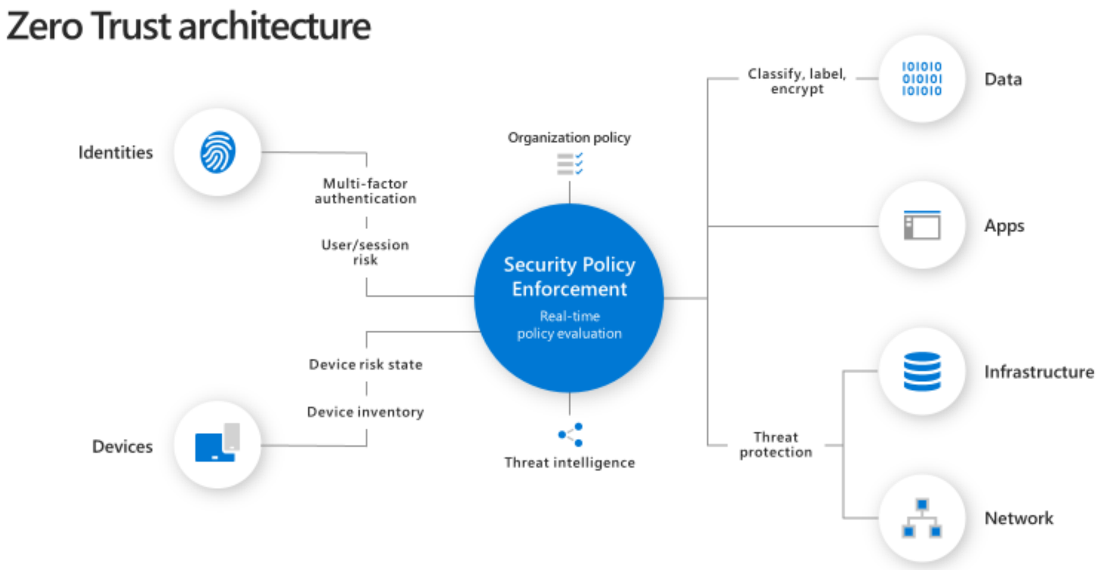
Collaboration today is changing at a rapid pace – the workforce is no longer tied to a particular location. Expectations in terms of efficiency are high, and confidential information circulates outside the corporate network in a continually evolving environment.

In this context, companies need a new security model that allows them to handle technological and operational changes, protect their user identities, company data, mobile devices, infrastructure, and business applications.

The Zero Trust model is an agile approach resulting from the collaboration between leaders in cyber security, based on three pillars: "Verify explicitly", "Use least privileged access", and "Assume breach".

Microsoft Approach to Zero Trust

The Microsoft technologies allow to implement a state-of-the art Zero Trust architecture, with a full coverage of digital assets and solutions.



The pillars of the Microsoft architecture are:

- **Identities:** Whether they represent people, services, or IOT devices – define the Zero Trust control plane. When an identity attempts to access a resource, we need to verify that identity with strong authentication, ensure access is compliant and typical for that identity, and follows least privilege access principles.
- **Data:** Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Data should be classified, labeled, and encrypted, and access restricted based on those attributes.
- **Apps:** Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lift-and-shifted to cloud workloads, or modern SaaS applications. Controls and technologies should be applied to discover Shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control of user actions, and validate secure configuration options
- **Devices:** Once an identity has been granted access to a resource, data can flow to a variety of different devices – from IoT devices to smartphones, BYOD to partner managed devices, and on-premises workloads to cloud hosted servers. This diversity creates a massive attack surface area, requiring we monitor and enforce device health and compliance for secure access.

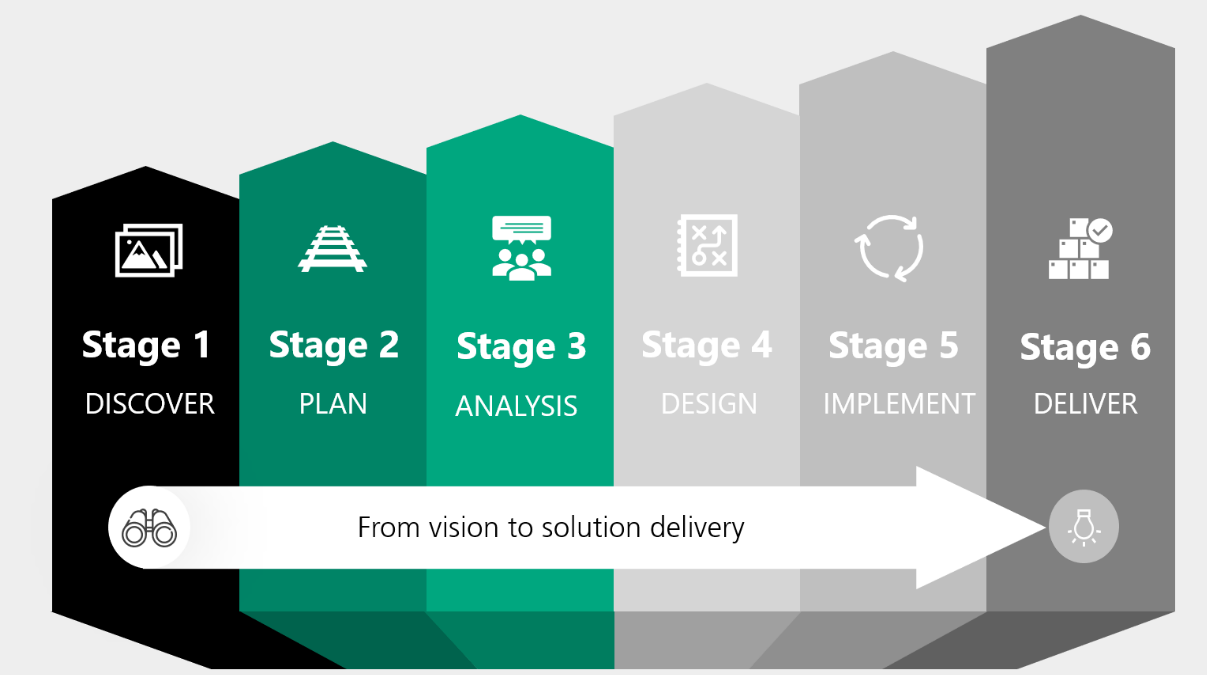
- **Infrastructure:** Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services) represents a critical threat vector. Assess for version, configuration, and JIT access to harden defense, use telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.
- **Network:** All data is ultimately accessed over network infrastructure. Networking controls can provide critical "in pipe" controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in-network micro segmentation) and real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

Microsoft Cloud and on-premises Identity and Access Management solutions allows to unify security of digital identities across hybrid-cloud infrastructures. It creates an ecosystem of Trust between your employees, customers (B2C), partners (B2B) allowing confident and efficient collaboration.

AdNovum Offering in Identity and Access Management

With the adoption of Hybrid-Cloud, the Information Security, previously covering the network security and operations, was extended with the Identity Security Perimeter. This evolution is bringing clear benefits in terms of operational efficiency, drastically improves security and mitigates cyber risks. Many organizations are currently undergoing a profound transformation of Identity and Access Management practices, as well as Identity Governance to align their digital infrastructures and assets to new practices and the modern technology stack. While this transformation is a necessity, the technology landscape is highly complex and, to be addressed properly, requires a forward-thinking cyber security vision and establishment of a detailed IAM strategy and roadmap.

At AdNovum we are specializing in the security of digital identities since 1988. By leveraging our experience on projects for customers in Financial, Insurance, Industrial, Retail, Public, and other sectors, we created a versatile methodology around Identity and Access Management with key stages shown on the figure below.



Thanks to our IAM methodology and associated toolbox, we are capable to guide your company through all IAM program stages.

Azure offers a large set of powerful security tools, extending enterprise Identity and Access Management solutions to the Cloud and allowing a safe and efficient adoption of other Microsoft Cloud offerings such as Office 365 SaaS.

The following non-exhaustive list of Azure capabilities can extend your modern IAM strategy:

- **Conditional Access** is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.
- **Identity Governance** allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.
- **Device Management (with Intune)** helps to maintain an inventory and manage user devices, ensuring their compliance with corporate security standards. It allows to create and enforce policies that help keep your organization data safe on organization-owned and personal devices (BYOD).
- **Privileged Identity Management (PIM)** is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization.
- **Identity Protection** is a tool that allows organizations to accomplish three key tasks:
  - Automate the detection and remediation of identity-based risks.
  - Investigate risks using data in the portal.
  - Export risk detection data to third-party utilities for further analysis.
- **Azure Security Center:** Azure Security Center is a unified infrastructure security management system that strengthens your security posture and provides advanced threat protection across your hybrid workloads in the cloud as well as on premises. It also covers the Identity Security perimeter and complements your SIEM with insight on security incidents in the Cloud.

IAM Strategy and Associated Program Maturity Assessment

AdNovum is pleased to offer you a consulting package allowing to assess the maturity of your IAM strategy with a special focus on Azure environments and associated capabilities.

This assessment includes four interactive workshops involving key IAM program stakeholders:

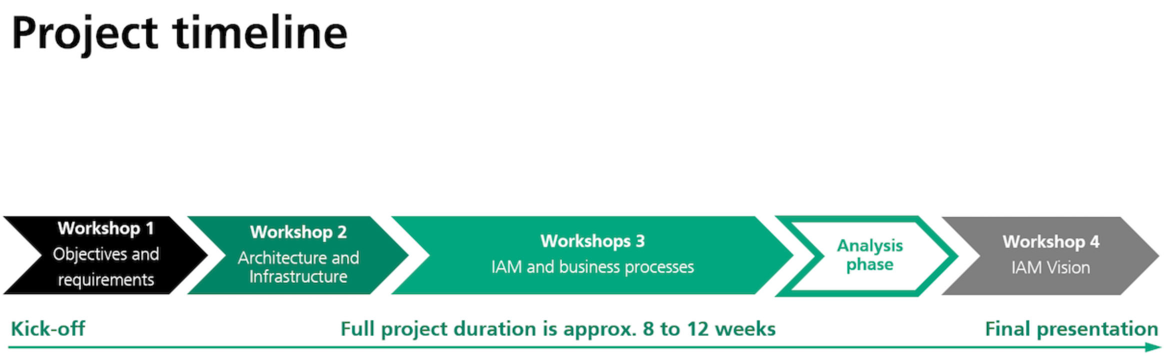
Workshop 1: Objectives and requirements

Workshop 2: Infrastructure and solution architecture discovery

Workshop 3: IAM and business processes

Workshop 4: IAM vision

The timeframe is defined with the customer at the project Kick-off. A typical project will span over approximately 8 to 12 weeks.



Project timeline

Workshop 1
Objectives and requirements

Workshop 2
Architecture and Infrastructure

Workshops 3
IAM and business processes

Analysis phase

Workshop 4
IAM Vision

Kick-off

Full project duration is approx. 8 to 12 weeks

Final presentation

If you are at the inception of your IAM program, our collaboration will allow you to establish a detailed IAM strategy, define a role model fitting your business, create a backlog of capabilities for implementation and associated roadmap.

If you have an established IAM program, the assessment will align your plans with Azure best practices, review and optimize the existing role model, fine-tune IAM workflows and Identity Governance processes, enhance the backlog of future capabilities and refine the IAM implementation roadmap.

Our interactive workshops will allow your internal teams to enhance their skills in Identity and Access Management, cyber security and Azure, thanks to practical experience accumulated by AdNovum experts. We will be pleased to create a personalized offering for your organization and are looking forward to becoming your long-term technology partner.

Example of deliverables

The list of deliverables varies depending on the maturity of existing customer IAM program and may include the following elements:

- IAM strategy.
  - Objectives, requirements, priorities.
  - Mission's definition.
  - Scope, methodology, stakeholders.
- Analysis of the current situation.
  - Systems and architecture.
  - IAM processes and organization.
  - Infrastructures.
  - SWOT analysis.
- Analysis of needs.
  - Current challenges.
  - IAM - SSO solution requirements.
- Vision.
  - Target solution architecture and workflows (B2B, B2E).
  - Prioritized backlog and Roadmap.
  - Complexity estimation.
- Added value to organization.
  - Benefits, RoI, risk mitigation measures.

Management Standards

At AdNovum, we have a project-based organization. Our project managers are educated and experienced in using project management best practices – worldwide and especially in Switzerland. From traditional methodologies and standards such as Waterfall or V to Agile frameworks such as Scrum or Kanban, we have certified managers from recognized associations such as PMI, Prince2, IPMA, Scrum.org, Scrum Alliance, SAFe or Hermes. Continuous education is a baseline for every AdNovum employee. Knowledge sharing about software engineering best practices is actualized efficiently with clear and simple internal documentation, coaching sessions, and video conferencing.

For our projects in Switzerland, we propose a large pool of IAM experts capable to handle on-site assignments of any complexity across the country.

AdNovum Zurich

Headquarter

AdNovum Informatik AG
Roentgenstrasse 22, CH-8005 Zurich
Phone: +41 44 272 6111
E-mail: info@adnovum.ch

AdNovum Bern

AdNovum Informatik AG
Brueckfeldstrasse 16, CH-3012 Bern
Phone: +41 31 952 5858
E-mail: info@adnovum.ch

AdNovum Suisse Romande

AdNovum Informatique SA
Avenue de l'Avant-Poste 4, CH-1005 Lausanne
Phone: +41 31 952 5858
E-mail: info@adnovum.ch

AdNovum Hungary

AdNovum Hungary Kft.
Bókay János utca 44-46, H-1083 Budapest
Phone: +36 1 701 0670
E-mail: info@adnovum.hu

AdNovum Portugal

AdNovum Portugal, Unipessoal Lda.
Campo Grande 378, 1700-097 Lisbon
Phone: +351 211 207 300
E-mail: info@adnovum.pt

AdNovum Singapore

AdNovum Singapore Pte. Ltd.
3 Shenton Way, #23-03 Shenton House
SG-068805 Singapore
Phone: +65 6536 0668
E-mail: info@adnovum.sg

AdNovum Vietnam

AdNovum Vietnam LLC
e.town 2 · 5th floor
364 Cong Hoa Street · Tan Binh District
Ho Chi Minh City
Phone: +84 28 3816 8200
E-mail: info@adnovum.vn