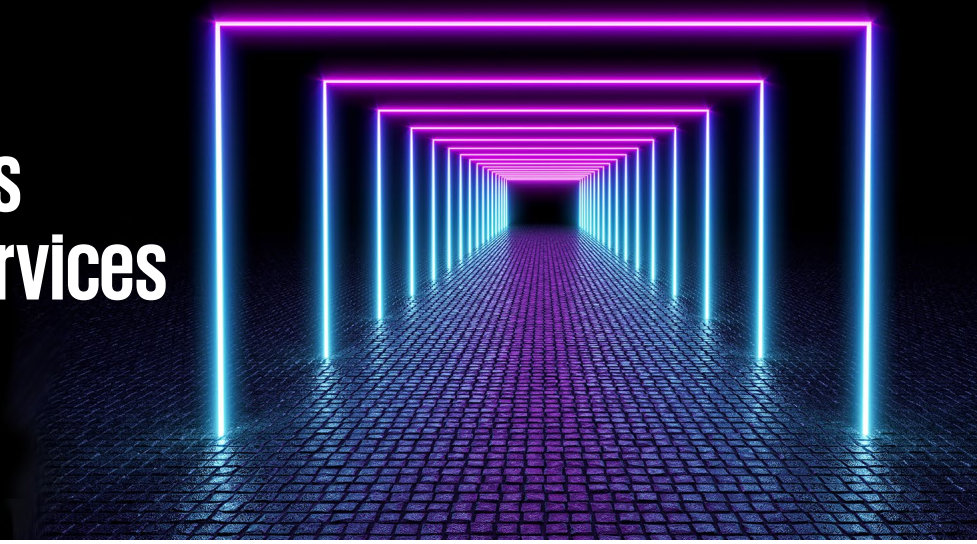
KPMG

Identity & Access Management Services

Cyber Security Advisory

KPMG Advisory Ltd.



Whether you would like to improve your existing IAM processes or are thinking about implementing an IDM system, we can provide services in both – and much more.

It is becoming more widely accepted that Identity and Access Management (IAM) is the gateway to information security processes. It regulates the access level to resources, supports risk management processes and manages the entire employee lifecycle, thereby greatly contributing to meet various industry and legal requirements. Thus, the perception that IAM processes should be strictly at the level of entitlement and access management is getting more and more outdated.

As the requirements for IAM processes become more complex, the focus is shifting to the Identity Management (IDM; IGA) systems that can serve these needs:

- Basic identity and access management processes
- Access level management
- Privileged user and access management
- Zero-trust
- Employee lifecycle management
- Ensuring industry and legal compliance
- Governance and risk management
- IT audit support

Based on our experience, the implementation of an IDM system is far from straightforward. The following obstacles are the most common:

- Incomplete or outdated access management policies serve the basis for IDM implementation
- Outdated, poorly designed identity and access management processes
- Lack of IAM strategy

This shows that the first challenges will be more strategic than technical. If these steps are not taken, the implementation of the IDM system could be delayed by technical problems that could have been solved in the strategic or preparatory phase.

How can we help?

See the below summary of our main services and the areas where we can provide expert support.

IAM strategy planning

Identity and Access Management (IAM) is the set of rules that enables the right individuals to access the right resources at the right times, with the right justification. Nowadays, it aims to address the problem of how to grant access rights to users in diverse technological environments, while complying industry-specific rules and regulations. In this endeavor, it is of utmost importance that upon designing IAM strategy, we do not only approach the issue from a technical perspective, but also seek to address business needs. Companies that define and implement their IAM strategy in the appropriate way will reduce their expenditure on manual activities and be able to support business objectives in an agile way. In many cases, the issue of measurability, i.e., how the company can measure the usefulness of the established entitlement management processes, arises in the context of IAM strategic planning. In this case as well, there are several options available. If you require assistance during the planning process, our experts are ready to support you with your IAM strategy.

Assessment, design, and development of current and future state identity and access management processes

When implementing an IDM system, it is crucial to understand the level of maturity of your organization's identity and access management processes. During the assessment of the current processes, we aim to gain a full picture of current workflows, which will help us to develop the future state operating model and workflows. Based on the results of the survey, we will make recommendations on actions to be taken to address gaps and ensure possible industry and legal compliance. In designing the future state processes, we will seek to align the identity and access management processes with an IDM system that follows industry best practices. In addition to that, our experts can also provide effective support in the development of existing IDM processes.

Feasibility study creation

In preparing the feasibility study, we aim to choose the right framework to achieve the objectives set in the IAM strategy. This consists of the following subtasks:

- Capturing current processes
- Design and development of future state processes
- GAP analysis
- Developing role structure
  - Assessing the current status
  - Role structure concept
  - Proposed methodology for the management of roles and role incompatibilities (SoD)
- Overview of source and target systems
- Definition of functional requirements for IDM systems

Developing IDM entitlement concept

A basic expectation for an IDM system is to provide the highest possible value to the end-user beyond the mandatory information security functionality. At the center of this is a well-structured and maintained product catalogue. As highlighted in the case of strategy planning, it is key to develop an entitlement concept that simultaneously meets business needs and satisfies various regulatory criteria.

Our service covers the following activities:

- Mapping the current entitlement structure
- Recommendations on what changes need to be made to ensure industry and/or legal compliance
- Role design
- Defining SoD rules
- Establishing access review and attestation rules

Creation of complex functional and non-functional requirement list for IDM products

Within this service, we will draw up a complex plan that includes the functional and non-functional requirements of the IDM product and the technological criteria that the IDM system must meet. This plan can be used for tender evaluation and as a guide for the system integrator to demonstrate in a POC (proof-of-concept) whether the IDM product meets the previously established requirements.

If required, our colleagues can support the POC process:

- Preparation of a test plan
- Support for testing activities
- Documentation

Support for system integration projects

Using data analytics, our experts can support your organization in the integration of existing applications access management processes into your IDM systems. What does this involve?

- Full mapping of the entitlement structure in the system – user and access right mappings and review of existing roles, review of compliance with SoD rules, review of access hierarchy
- Support for data cleansing activities– identify unused users, access rights and roles
- Creating access roles – assigning single access rights to composite roles, assigning roles to users based on SoD criteria
- Technical support for the integration – user and access rights/role assignment, preparation of data transfer packages, target system monitoring and control

Contact

Kornél Lukács
Partner

T: +36 1 887 7472
E: kornel.lukacs@kpmg.hu

kpmg.com/socialmedia

kpmg.hu