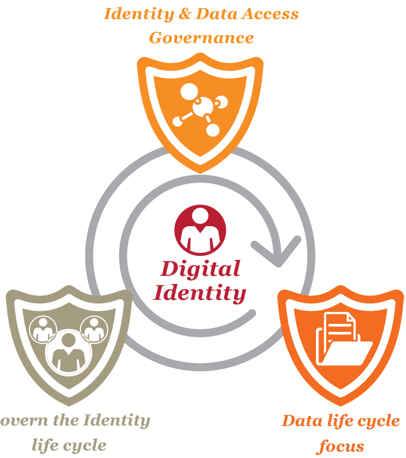
Identity & Data Access Governance

Our formula's

Success factors

Our toolkit


Identity & Data Access Governance
Digital Identity
Govern the Identity life cycle
Data life cycle focus

Our three core formulas to manage the digital identity

The *Identity & Data Access Governance* Formula

PwC has over 20 years of experience in the field of Identity Access Management (IAM) from strategy to execution. We have seen drivers for IAM change, following market, privacy and information security trends. What remains unchanged however, is that (y)our digital identity is still at the core of digitalization. Spurred by digital transformation and requirements for GDPR compliance, the importance of the digital identity in combination with access to data and processing of personal data has increased exponentially. However, managing the digital identity and access to data in a secure and effective way is complex and can have large impact on organizations. With this document, we provide guidance in the form of our key formulas.

Identity & Data Access Governance

Enable the organization to secure, monitor, measure, and continuously improve access to information within the identity and data life cycle.

The goal of Identity & Data Access Governance is to define what the organization needs to focus on in relation to identities and access to data. It addresses the structure of the organization's governance with the goal to continuously secure, measure, monitor and improve access to identity and data assets. Core drivers are risk mitigation, reducing operational costs, and / or increasing user experience. This depends on corporate strategy, business objectives, and regulatory obligations. The organization should focus on questions like '*is privacy a key selling point for us?*' or '*how important is the protection of intellectual property for business continuity?*' This defines the way an organization needs to implement Identity & Data Access Governance and what stakeholders to involve.

Core components

Strategy, business drivers, and corporate objectives

+

Policies, Governance Risk and Compliance (GRC) framework

+

Target Operating Model

Identity & Data Access Governance

Description of the core components of our formula.

Strategy, business drivers, and corporate objectives

Define the external and internal business drivers to manage access to identity and data assets. Align to the corporate and IT strategy and vision. Ensure you involve key stakeholders from business to IT, to identify concerns, focus areas, and to define a shared vision on managing access to identity and data assets.

Policies and Governance Risk and Compliance (GRC) framework

Align the organization’s information security and privacy policies and standards (e.g. IAM policy, Access Governance policy, Access Control policy, etc.) to the identity and data life-cycle processes. In addition, ensure that risks are evaluated and controls are implemented into your GRC framework.

Target Operating Model

Evaluate what is required to operationalize measure, monitor and control the identity and data life cycle on both a tactical and operational level. Focus on the current and to-be governance structure (ownership), core processes, business objectives and strategy, and GRC requirements. Determine the gap and prioritize improvement activities.

Govern the Identity life cycle

Implement an automated Identity & Access Management solution with a closed loop remediation process that aligns to company policies and processes.

Identities need to have access to IT or information asset to perform their work and / or to fulfil a certain task. The type of asset that is required often depends on where the identity is in their life cycle. Think about the phases of a new joiner, when they receive promotion (move), or leave the organization. Different types of identities follow somewhat the same phases; think about employees, contractors, or customers. The organization needs to focus on how access to information assets can be achieved in a way that is secure, effective and efficient. This requires that processes need to be formalized and access to systems is automatically managed and secured conform organizations policies. Combine access monitoring and evaluation with periodical reviews and automatic notifications.

Core components

User application data and provisioning + Application authorization matrix (Soll) and business rules + Identity access processes and workflow

Govern the Identity life cycle

Description of the core components of our formula.

User application data and provisioning

To mitigate the risk of unauthorized access, your solution must be able to evaluate the actual access rights and user account data (also known as IST or As-Is) of connected systems across the IT landscape. The IST data need to include information about users, accounts, and access rights. Process access requests and provisioning actions through a 'central source of truth solution' throughout your IT landscape as much as possible.

Application authorization matrix and logic

Ensure that there is an overview of the target (Soll) situation per application: which users (or user types) need to receive what kind of access rights at what time. There must be an overview of what the application access rights or authorizations provide in business language.

Identity Access processes and workflow

Identify how different type of identities receive access to IT assets for each of the life-cycle phases. Design and automate processes and business logic (segregation of duty). Include remediation processes, like performing access reviews and certification activities. Ensure the processes can be measured, monitored, and are aligned to the GRC controls.

Focus on the Data life cycle

Discover (over)exposed sensitive data, manage and monitor access to (un)structured data within the data life cycle to reduce the risk of data breaches.

The identity life cycle focuses on when identities need specific access to information. In relation to this context, the data access life-cycle perspective focuses on what, how and when specific data is used. Think about the phases of creation, storage, use, archiving and destruction. Identifying what type of data is processed within your organization, defining what data requires additional security (access) controls is an important element within data access governance. The goal of governing the data access life cycle in the context of identities is to minimize the risk that sensitive (un)structured data, e.g. documents that are stored on shares and file collaboration systems, are disclosed to unauthorized persons.

Core components

Discover, evaluate and classify (sensitive) data

+

Evaluate and manage access rights and ownership structure

+

Data processes and workflows

Focus on the Data life-cycle

Description of the core components of our formula.

Discover, evaluate and classify (sensitive) data

Discover data and evaluate whether the data needs to be archived or deleted. Identify sensitive unstructured data by performing data classifications on for example document attributes, sensitive keywords, or specific patterns. With this information, the organization can enforce access policies on specific types of data.

Evaluate and manage access rights and ownership structure

From a business perspective, there are specific rules that define who is allowed to access sensitive information, or whether specific activities can be classified as suspicious behavior. To enforce these policies, insights are required of where specific type of data resides, who should have access to it, and who should be responsible (ownership).

Processes and workflows

Data discovery and classification processes need to be aligned to the current data life-cycle processes within the organization. Think about requesting access to data, and identification and notification of data owners when specific actions on data occur. This requires the implementation of workflows and reporting functionalities.

Critical ***success*** factors

Selling the vision

Planning

Planning for success certainly holds true for Identity, Data, and Access Governance projects: *success depends on defining what is required and who should be involved, before the project actually starts.* Remember that Identity is not a project, it is a program.

Multi-disciplinary team

Identity, Data and Access Governance projects typically require expertise from a variety of domains such as HR, Risk and IT. These projects will affect the entire organization when they go-live. As such, these projects require broad support beyond the immediate project team in order to be successful.

Shared mind-set

In order to obtain and retain this support throughout the project, sell your vision and create a shared mind-set so that everybody is working towards that same goal from start to execution.

Business design alignment

Business involvement

Since Identity, Data and Access Governance is about ensuring that the right people have the right access to the right systems and data, at the end of the day much of it - *if not all* - should be a business decision. This means that next to IT and application owners, you have to engage with the business lines, teams and relevant business process owners. To ensure involvement it’s key to have a sound communication plan, perform stakeholder analysis, and have a clear business translation and goals at hand.

Processes, responsibilities and tasks

Continuous involvement and support of business and IT stakeholders is required in the design and execution of your identity and data access governance processes and associated key content. This requires clear definition of roles, responsibilities, accountabilities, and tasks for each stakeholder.

Line carrying forward

Measure effectiveness

We measure the effectiveness and success of our Identity, Data and Access Governance project implementations during and long after we have left. To PwC it is important that end-users embrace the solution and that the organization is able to carry the results forward without further support if required.

Involve client staff in project

For this reason, we ideally form a PwC led project team composed of PwC subject matter experts and key staff from the client that will continue to play an active role in managing “the run”. This approach facilitates knowledge sharing and learning on the job, benefiting both the project phase as well as operations after go-live.

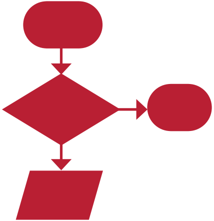
Toolkit *accelerator*

Our toolkit

During our 19 years of IAM and Data Access Governance experience we have created a large knowledge base of reusable blueprints and content that we leverage in projects for the benefit our clients.

- **IAM process templates**
- **Communication & training**
- **Target Operating Model standard**
- **Monitoring dashboard**
- **Authorization modeling guide**
- **Application on-boarding**

IAM process templates



IAM process design is a fundamental part of every Identity and Data Access Governance implementation project. It is crucial to understand who, when and how tooling and functionalities will be used to make any technology implementation a success.

Examples of IAM process templates in our toolkit are:

- Life cycle management (joiner, mover, leaver);
- Authorization management (roles and rules for Segregation of Duties);
- Access request management (request, approval and fulfilment);
- Access review (also known as certification or attestation);
- IT change management.

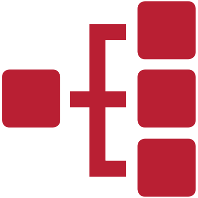
Target operating model standard

With the implementation of Identity, Data and Access Governance, new management processes often introduce new roles and responsibilities. This concerns both a tactical and operational level to ensure lasting success. This may vary from an IAM officer to set and monitor IAM process KPI's to a team of people tasked with maintaining the role model, on boarding of new applications or scheduling access review campaigns.

Our operating model standard provides an overview of common Identity, Data and Access Governance management processes, roles and associated responsibilities. In addition, it provides guidance on how to join up with other important related processes such as IT change management.

Role modelling guide

PwC developed a standardized approach for the design of role based authorization models, also referred to as RBAC. This approach guides the designer step-by-step in three phases:



1. Business process and supporting system(s) analysis
2. Segregation of duty (SoD) analysis
3. Process task and function based design

This delivers an authorization model consisting of:

- A role model expressing desired state of access rights
- Business rules to monitor SoD conflicts
- A business glossary to supporting business decisions
- Ownership to ensure continuity

Communication and training

Organizational wide impact

Identity, Data and Access Governance needs to be made operational throughout all levels of the organization. This means it has significant impact on a variety of stakeholders within your organization. As the subject matter is complex, providing an understandable and practical explanation of business drivers, scope and the actual implementation should not be underestimated.

Communication & training

Our communication and training approach facilitates the process of stakeholder discovery and mapping stakeholder involvement to (existing) communication and training channels. Execution of the resulting plan leverages our standardized communication and training content in all phases from project initiation to go-live.

Monitoring dashboard

Monitoring progress is complex

Identity, Data and Access Governance implementations are often supported by tooling to support (cost) effective risk management. We support our customers to identify what processes and supporting systems are potential candidates for (semi)automation. However, implementing supporting tooling can be complex and understanding progress and status can be challenging.

Monitoring dashboard

To address this, we use our standardized IDAG monitoring dashboard that supports project managers and business stakeholders in understanding the status and progress of the project. Our dashboards contains around 26 activities from analysis and design to process dry-run phases. These activities relate to milestones to improve planning, management and communication within our projects.

Application on-boarding

Typically, a significant number of business critical applications are in scope of your Identity, Data and Access Governance project to mitigate key risks. In order for the project to scale, we have created an application on-boarding approach and toolkit that enables quick and easy on-boarding of applications.

Some of the key content includes:

- Step-by-step script and checklist for on-boarding
- Guide for identifying and involving right stakeholders
- Questionnaire to discover key information for on-boarding (such as account life cycle, business rules, role model and integration characteristics)
- Templates for data loading (including authorization model and business glossary)

Want to know more? Contact www.pwc.es/bss

Andrés Diego Hontiveros

PwC Spain
Socio responsable Identity & Data Governance
+34 915 685 363
andres.diego.hontiveros@pwc.com

making identity ***matter***