ELIMITY | Customer Case

Large organization speeds up and de-risks deployment of a new IGA suite

Industry

Government

Region

Europe

Applications

HR

A large governmental organization with over 26,000 employees faced a critical need to upgrade their identity governance and administration capabilities. As a result, the organization embarked on a multi-year transition from a homegrown, legacy access management system to a full-fledged Identity Governance and Administration (IGA) suite.

26.000	**Employees**
35.000	**Entitlements**
10.000	**Roles**
1.200	**Applications**

Early on, the organization realized that it needed data insights into user accounts and access flows during multiple phases of the IGA deployment to ensure project success. This "visibility before automation" approach allowed the organization to improve the current process before automating it with the IGA suite.

Challenges during IGA roll-out

- Before rolling out the IGA suite, the organization had to clean up and classify current users and their accesses (e.g., Active Directory (AD) groups). Examples of specific data questions included:
  - Which groups should still exist?
  - Which employees should be in which groups?
  - What the owners of these groups should be?
  - Which descriptions these groups should have? And many others.
- As part of rolling out the IGA suite, the organization had to define a role model that specified which types of users receive which accesses. The size of the IAM team required an efficient approach.
- The small IAM team was burdened with numerous manual repetitive analyses that also provided limited identity data and insights.
- The organization had multiple groups of people that all wanted information on their users and their accesses. The new IGA tool was not the platform to achieve this.

> "
> We realised that we needed data insights into our existing users and permissions during multiple phases of our IGA deployment. Elimity provided us with this visibility and context within days."
>
> **Director IAM**

Solution

The organization deployed the Elimity Insights platform and rapidly integrated it with over 10 applications, including the legacy IGA, the newly deployed IGA suite, Active Directory, Azure AD and a custom-built HR application. Elimity Insights then linked all of this data and enabled everyone in the IAM team to easily perform the analyses they needed in their day-to-day jobs on a complete and always up-to-date set of identity data.

Key Results

- ✓ First visibility of existing users and accesses within 2 days.
- ✓ Always-up-to-date comprehensive view of all important IAM data sources within 2 weeks.
- ✓ User-friendly and instantaneous self-service analytics for everyone involved with IAM.
- ✓ Identity analytics used in several projects, including role design.
- ✓ Automated monitoring of KPIs over time, such as entitlements that are still provided directly.
- ✓ The ability to easily include line managers and application owners through access reviews.

Benefits

Accelerated and de-risked the IGA deployment project

Ensured timely delivery of the IGA deployment project

Vastly improved productivity of the IGA team

Lowered the license cost of the IGA suite by removing unneeded accounts up-front

Ensured visibility and governance of systems not connected to the IGA suite after the IGA deployment

> "
> Previously, it took our IAM team up to 3 weeks to create an overview of the accesses of everyone in a specific team. Since implementing the Elimity platform, the process has become just one click away, reducing the workload for the team significantly.
>
> **Director Identity and Access Management**

Customer Case in Numbers

2	Days until first visibility of existing users and their accesses.
10	Sources connected to the platform after 2 weeks
2	Weeks to get to an always-up-to-date overview of over 10 IAM sources
3	Seconds to analyse the accesses of everyone in a team, compared to 3 weeks before
30	Out-of-the-box security controls and automated security KPIs
50	Queries deployed on IAM data, compared to 5 manual queries prior to Elimity
300	Employees with the ability to perform IAM analyses compared to 5 SMEs before

Featured Capabilities of Elimity Insights

1 Data Collection

- Built-in connectors pull data from sources automatically
- File upload connectors for manual data input in LDIF format
- CSV file acceptance for easy data export from custom sources

2 Understanding and Visibility

- Inventory of the users and their access across applications in scope
- List of user access risks and anomalies
- Out-of-the-box security controls
- Peer Group analysis and risks controls

3 Review and Clean Up

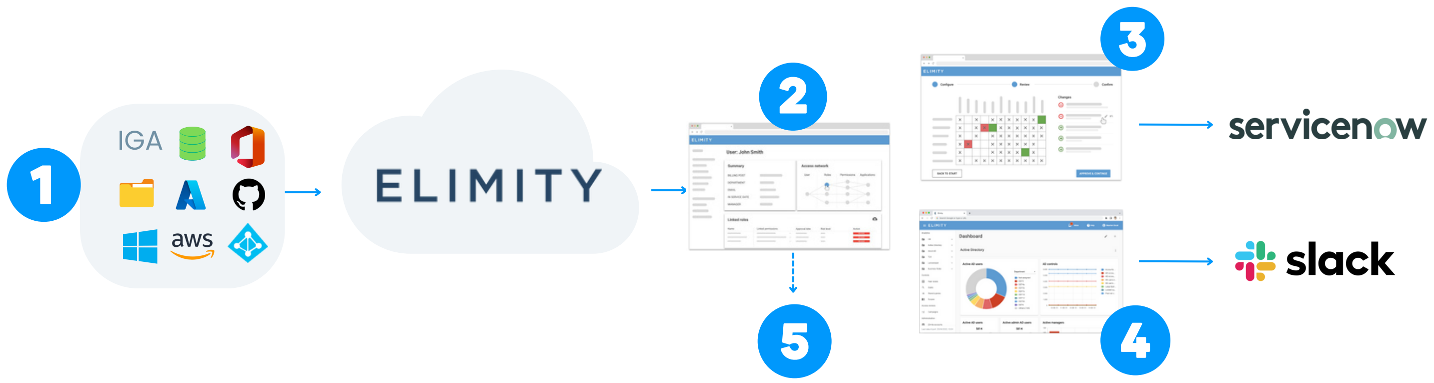
- Streamlined process for account removal and permission revocation
- Access review through analytics or recertification campaigns
- Automated creation of change requests in ITSM

4 Monitoring and Alerting

- Continuous monitoring access risks and tracking reviewer progress
- Automatic alerts on access risks
- Automated reporting on user access governance organization
- Present data in business-friendly language

5 Role Mining

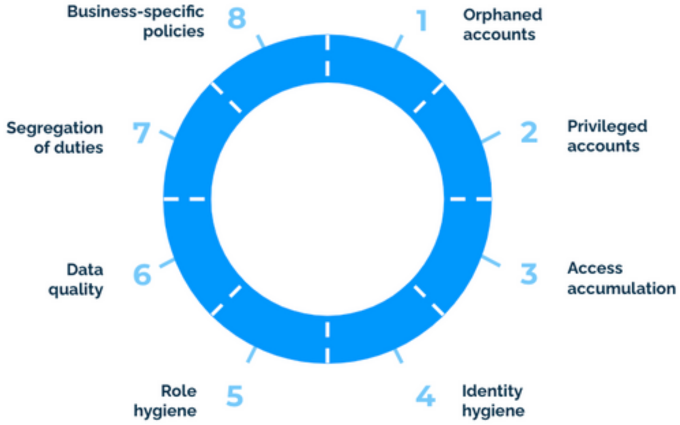
- Cleaning up current group assignments and meta-data
- Classifying current group assignments
- Creating role models



ELIMITY | Solution Brief

IAM Queries and Controls

We use the following eight categories as the basis for the controls to identify key access risks. They exist of a set of out-of-the-box controls, mapped to your scope and organizational context, and can be complemented with custom controls.



Category	Example Queries Performed at Customer	
Orphaned accounts	User accounts for which the last logon timestamp is before 12 months ago.	🟠
Orphaned accounts	User accounts for which the last logon timestamp is not assigned (never logged in).	🟢
Orphaned accounts	User accounts for which the password has expired more than 12 months ago.	🟢
Orphaned accounts	User accounts that are linked to employees for which the end data is in the past.	🟠
Orphaned accounts	User accounts that are linked to employees for which the status is not active anymore.	🟢
Orphaned accounts	User accounts that cannot be linked back to an employee.	🔴
Privileged accounts	Employees that have more than x roles/groups/privileges/...	🟠
Privileged accounts	Use the peer review to look for employees that have far more privileges than their direct peers.	🟢
Access accumulation	Employees that have more than x roles/groups/privileges/...	🟠
Access accumulation	Use the peer review to look for employees that have far more privileges than their direct peers.	🟢
Identity hygiene	User accounts for which the number of groups/roles/privileges/... is 0.	🟠
Identity hygiene	User accounts for which the last modification timestamp is more than 2 years ago.	🔴
Identity hygiene	User accounts for which the timestamp of the last password update is more than 6 months ago.	🟢
Identity hygiene	User accounts for which MFA is not enabled.	🟢
Identity hygiene	User accounts for which the name or description contains "Test", "tst", "temporary" or "tmp".	🔴
Role hygiene	Roles for which the number of linked entitlements or permissions is 0.	🟠
Role hygiene	Roles for which the number of linked user accounts is 0.	🔴
Role hygiene	Entitlements or permissions that are directly assigned to a user account.	🟢
Data quality	User accounts or employees for which an important attribute (e.g., manager) is not assigned.	🟠
Data quality	Roles, entitlements or groups for which the description is empty or not assigned.	🟠
Data quality	User accounts for which an important attribute does not match the needed format.	🟠
Separation of Duties	Employees that are linked to permission A and permission B, in which A and B form a toxic combination.	🔴