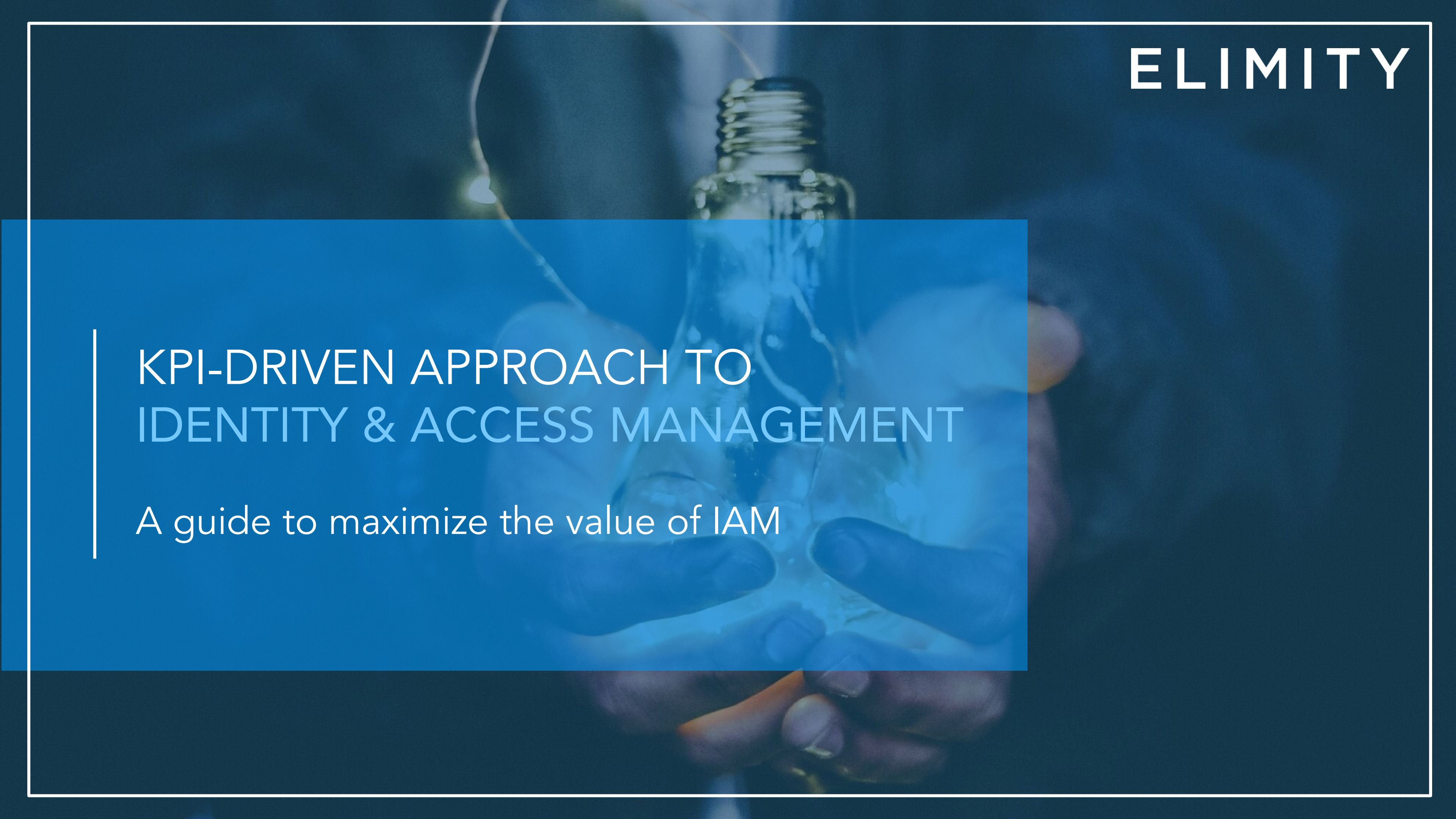


ELIMITY

KPI-DRIVEN APPROACH TO IDENTITY & ACCESS MANAGEMENT

A guide to maximize the value of IAM

TABLE OF CONTENTS

1 Executive summary

2 Conventions & Introduction

3 KPI-driven IAM & the right choice of KPIs

4 KPIs guide: risk reduction & improvement of process and data quality

5 Closed-loop model

6 Conclusion

This paper is written for CISOs, IAM professionals, and IT security experts. The contents of this paper are not limited to any organizational size, structure or industry. Nevertheless, the premise is that the organization has already deployed and is currently using an identity & access management (IAM) system or program. This can range from custom-built solutions to dedicated IAM solutions such as SailPoint and SAP IdM. This, however, does not mean that companies just starting with IAM cannot benefit from this paper. The problem statement and examples are just not focused on that situation.

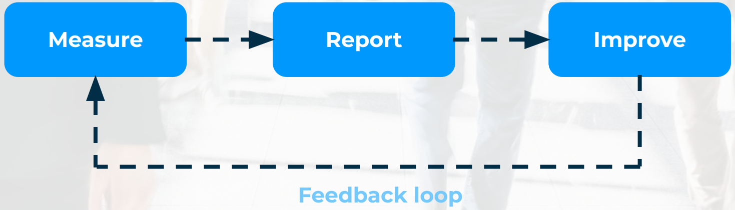
In this paper we propose a closed-loop model to get started on using KPIs to improve IAM effectiveness. Moreover, we bundled a comprehensive set of KPIs that have proven to be applicable to the majority of organizations. Read on to learn more about the closed-loop model, the right metrics and what impact being KPI-driven can have on your organization.

EXECUTIVE SUMMARY

Over the past decades, many organizations have - rightfully so - introduced proper IAM to securely manage its ever increasing digital identities and their accesses. Still today, new challenges emerge and new layers are added. Hence, IAM systems should be continuously improved to meet today's and tomorrow's increasing demands. In practice identifying potential inefficiencies or gaps and measuring IAM effectiveness remain a challenge. Applying a KPI-driven approach to IAM is (one of) the solutions to identity areas for improvement as well as areas of success.

In this paper we bundled a comprehensive set of KPIs that have proven to be applicable to and complete for the majority of the organizations that strive for risk reduction and/or improvement of process and data quality. These KPIs are derived from the ISO 27001 based identity wheel (see page 9) which presents eight essential KPI sets.

Don't forget, however, that KPIs in itself are just KPIs. IAM effectiveness can only be improved if those KPIs are actually used to drive decisions, actions and their prioritization. The proposed closed-loop model, that consists of 3 steps - measure, report and improve - and a feedback loop, enables you to do exactly that.



CONVENTIONS

💡 Additional information and insights

👉 Tips & tricks

💻 Screenshots and explanation of how certain things can be done with Elimity Insights, Elimity’s Identity Intelligence SaaS platform.

Some clarifications before you continue reading this ebook:

- The words ‘entitlements’, ‘permissions’ and ‘privileges’ are used interchangeably throughout the text. Whichever of these is used depends on the IAM system that is deployed. Nevertheless, the meaning is similar.
- ‘Access rights’ should be understood as a collection of specific permissions that user accounts are entitled with directly or because they are assigned to one or more roles.
- The words ‘KPI’ and ‘metric’ are used interchangeably throughout the text. Even though it is often stated that a KPI consists of several specific metrics, we will not make that difference in this paper.
- The difference between a Key Performance Indicator (KPI) and a Key Risk Indicator (KRI) is what each of them measures. A KPI measures performance (i.e. the achievement of identified goals) while a KRI measures risk exposure (i.e. an early warning to identify a potential threat). One of the main goals of an IAM system is, however, reducing risk. As a result, there is not always a clear and strict line between a KPI and KRI within IAM. To avoid confusion, only the word ‘KPI’ will be used in this text. Remember, however, that this could also refer to an indicator that in fact measures risk exposure.

INTRODUCTION

Over the past years proper identity management has become business-critical and today's challenge to secure access is more complicated than ever before. Think about the immense increase in (on-prem and cloud) applications that are being used, the trend of hyper-outsourcing and non-linear career paths, agile transformations resulting in cross-functional jobs and the rapid shift to a virtual workforce. As a result, many companies have introduced IAM systems in order to get complex IT infrastructures comprising tens or even hundreds of systems and applications, and thousands of accounts and access rights under control. Once introduced, however, identifying potential inefficiencies or gaps and measuring IAM effectiveness remain a challenge.

In order to achieve transparent and efficient management of a growing - both in complexity and volume - digital identity base, using key performance indicators (KPIs) is essential. Being KPI-driven will enable you to efficiently identify areas for improvement, prioritize efforts and future investments, and align all parties involved.

Companies that don't know the overall performance state of their IAM - here defined as the current state compared to the desired state - could potentially take flawed decisions when it comes to priorities and future IAM investments. On top of that, getting a firm grip on your IAM system is crucial to make identity management manageable.

In this paper, we provide an approach towards sustainable IAM maintenance. Whether you currently use SailPoint IdentityIQ, SAP IdM, Oracle IdM, OneIdentity Manager, another identity management solution or a custom-built solution, ensuring the success of your IAM system should be a top priority.

KPI-DRIVEN IAM

KPIs are a means of measuring IAM performance in order to keep track of and understand IAM effectiveness, and identify potential areas for improvement. Remember that once identified, more in-depth information and action-oriented insights are required to actually improve the identified issue.

EXAMPLE

In many organizations, the number of unassigned roles increases rapidly due to an ever changing access landscape. Once this is identified as an issue, whether for security or operational reasons, role managers should have the right information available to decide whether such an unassigned role is only temporary unassigned or whether it can be deleted.

THE RIGHT CHOICE OF KPIs

Which KPIs are relevant to measure and follow-up is derived from the overall IAM goals. In many organizations the main goal or combination of goals of IAM can differ. In strongly regulated organizations for example, *regulatory compliance* is obviously (one of) the main goal(s). Other commonly stated goals of IAM are *risk reduction*, *improvement of process and data quality*, and *business facilitation* [1]. Even within an organization different people can be responsible for different goals of the IAM system. As a result, the relevant KPIs for each of these people will often slightly differ. Understanding who will use the KPIs and how is thus key to choose the right metrics. Certain KPIs can of course be relevant to measure the success of multiple goals at the same time.

Once the goal(s) are determined, you should ask yourself the following: "Which questions define the goal(s) more precisely?".

The relevant metrics are then - often simply - the answers to those questions. By following this approach, the KPIs will be aligned with the IAM strategy and in turn contribute to the accomplishment of the goal(s).

It's important, however, to understand that the choice of KPIs is not set in stone for all time. There are several factors that could influence the set of relevant KPIs. Think about strategies and goals that develop over time, more information that becomes available, changes in the regulatory landscape, etcetera. In order to continuously ensure that the right set of KPIs is measured, it should be revisited once in a while. Also note that there's no ideal number of KPIs that you should have.

[1] Hummer, M., Groll, S., Kunz, M., Fuchs, L., Pernul, G. (2018). Measuring Identity and Access Management Performance - An Expert Survey on Possible Performance Indicators. *Proceedings of the 4th International Conference on Information System Security and Privacy (ICISSP)*, 233-240.

KPIs GUIDE: risk reduction & improvement of process and data quality

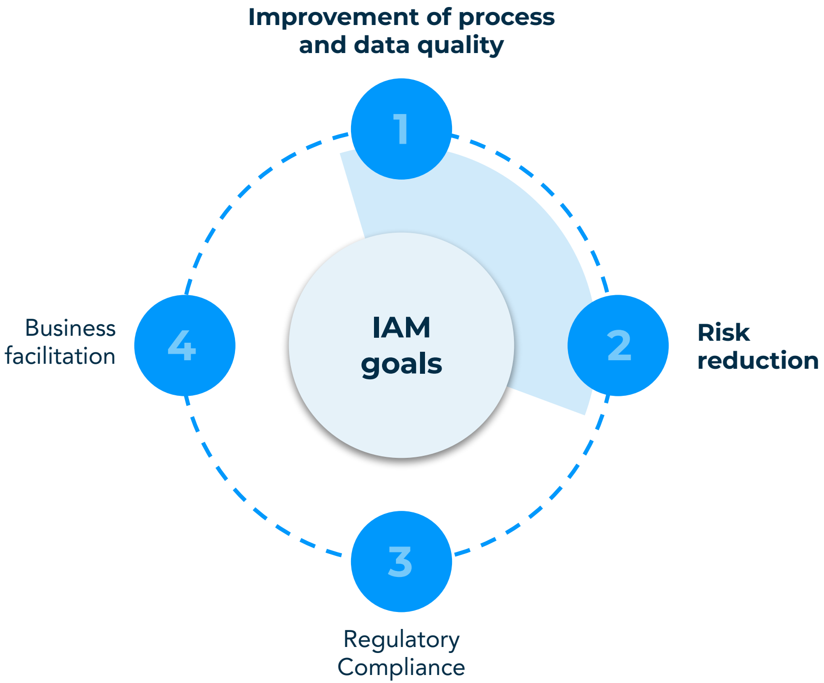


FIGURE: WHEEL OF IAM GOALS

We will cover KPIs particularly focused on the IAM goals *risk reduction* and *improvement of process and data quality* (see figure on the left). The KPIs related to *business facilitation* are more duration-based. Think about the average duration of employee readiness and the average duration of access request processing. Most of the KPIs measuring *regulatory compliance* are regulation-specific and dependent upon audits. Think about the number of compliance violations and the number of successful audits.

Identity wheel: KPI sets

In this chapter we bundled a comprehensive set of KPIs that have proven to be applicable to and complete for the majority of the organizations that strive for risk reduction and/or improvement of process and data quality. The ISO 27001 based identity wheel (see below) shows eight KPI sets, each entailing several specific KPIs.

These KPIs are listed on the following pages. Note that for the KPIs - specifically starting from section 2 - both the quantity and the distribution (e.g. across departments) can be interesting.

Identity assessment

Claim your identity assessment to learn how your organization scores on the identity wheel!

Get in touch

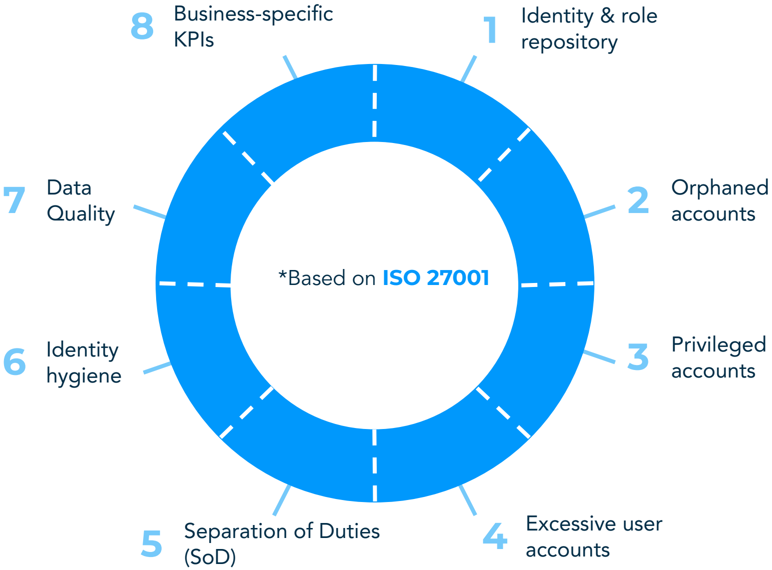


FIGURE: IDENTITY WHEEL

1. Identity & role repository

Even rather simple metrics about the identity and role repository size already enable a first assessment of the quality of the IAM processes. In case the number of users in the IAM system greatly exceeds the number of employees (often found in an HR system), something is probably wrong. Moreover, monitoring how these metrics evolve over time can reveal interesting trends (e.g. growth rates). Think about an almost constant increase in the number of roles. Additionally, the value of ratios should not be underestimated as these provide a good indication of the manageability of the IAM system.

In general, before diving in more complex and detailed metrics, it's important to know what the repository looks like:

- The number of users *(per department or organizational unit, per manager, …)*
- The number of newly created users
- The number of disabled users
- The number of *(organizational, container, IT, business, technical, …)* roles
- The number of entitlements
- The number of applications integrated in the current IAM system
- The number of roles relative to the number of departments
- The number of *IT* roles relative to the number of *business* roles. This can, of course, be done for any type of roles of interest.
- The number of entitlements relative to the number of users
- The number of entitlements relative to the number of roles

RULE OF THUMB

What is the relation between the number of roles and users in your organization?

A rule of thumb regarding the number of roles in your IAM system: the total number of roles should be no more than 10% of the total number of users. In many organizations without proper role management this percentage is greatly exceeded. This represents an overly complex role model that is difficult to maintain and can lead to errors and operational inefficiencies.

Struggling with role design or role analytics? We can help!

Get in touch

2. Orphaned accounts

One path to gain access to organization resources, applications or systems is through user and service accounts that are no longer actively used. This applies to both accounts from employees that are leaving and external contractors who finished a project in the organization. Organizations that fail to take the necessary steps to close these entry points leave the door on a jar for attackers.

When an employee leaves the organization or when a contractor's project has ended, their user accounts must be deactivated (i.e. disabled). This should be part of the typical offboarding procedure (often automated by the IAM system) of both employees and contractors. However, in practice, it happens that those accounts are incorrectly deactivated or not deactivated at all. By identifying and cleaning up these accounts risks are reduced significantly. Moreover, by finding out why these accounts were not deactivated, the IAM - offboarding - processes can be improved.

Some metrics regarding orphaned accounts:

- Users that have not logged in for quite some time. Accounts that have not been used for a certain period of time are also known as *dormant accounts*. What that time period should be exactly can differ between organizations. Nevertheless, 90 days is often considered the limit.
    - For certain accounts, such as admin accounts, one might prefer a shorter time period compared to other accounts. Hence, this KPI can be split into several sub-KPIs.
- Users that have never logged in.
- Uncorrelated user accounts, also known as *ghost accounts*. These are accounts that are not linked to an active user or not linked to a user at all.
- User accounts with a status indicating inactivity. What this status is exactly depends upon the IAM system that is used in the organization. Think for example about an employment status 'retired' or an activity status 'inactive'. The clue is to look at the user characteristics in the IAM system that could indicate inactivity of a user.

3. Privileged accounts

Privileged accounts, generally defined as accounts that have significantly more access rights than ordinary accounts, exist in many forms and shapes. However, when not properly managed and monitored, privileged accounts pose significant security risks. These risks could come from all sides: malicious ‘outsiders’ (such as hackers), or careless or disgruntled ‘insiders’. Whoever gains access to these privileged accounts can control organization resources, access sensitive data, or even change or disable (security) systems.

It’s important to know how many and what kind of privileged accounts exist in the organization. Note, however, that some of the below mentioned types of privileged accounts can overlap.

- Administrator accounts, think about Local Admin and Domain Admin.
- Stealthy accounts. These accounts are granted administrative privileges on one or more systems but often exist below the radar as they are not labeled ‘Admin’.
- Privileged service accounts such as Domain Service accounts.
- Non-personal accounts (NPA). These accounts are not directly related to a uniquely identifiable person/employee, nor are they the result of the 'joiner – mover - leaver' HR processes in an organization. Such accounts are often quite powerful (e.g. admin or root account) but difficult to detect. On top of that, login with the account doesn’t leave an audit trace showing which person has actually used it. In other words, there is not a specific person that can be held accountable.
- Privileged data user accounts. Even though these users are not typical privileged accounts, they should be considered privileged anyway, because of the sensitive data they can access. Think about the accountant who has access to financial data of his customers, an HR employee with access to sensitive employee data or a doctor who has access to patient information.
- Privileged role-based accounts. Depending on the role model, certain roles can be considered privileged. Therefore, we should consider users assigned to one or more of these roles as privileged accounts.

YOU CAN’T PROTECT WHAT YOU CAN’T SEE

4. Users with excessive access rights

The difference with privileged accounts and users with excessive access rights is that the former focuses on users who should have (many) sensitive access rights by definition while the latter focuses on users who accidentally have (too) many access rights.

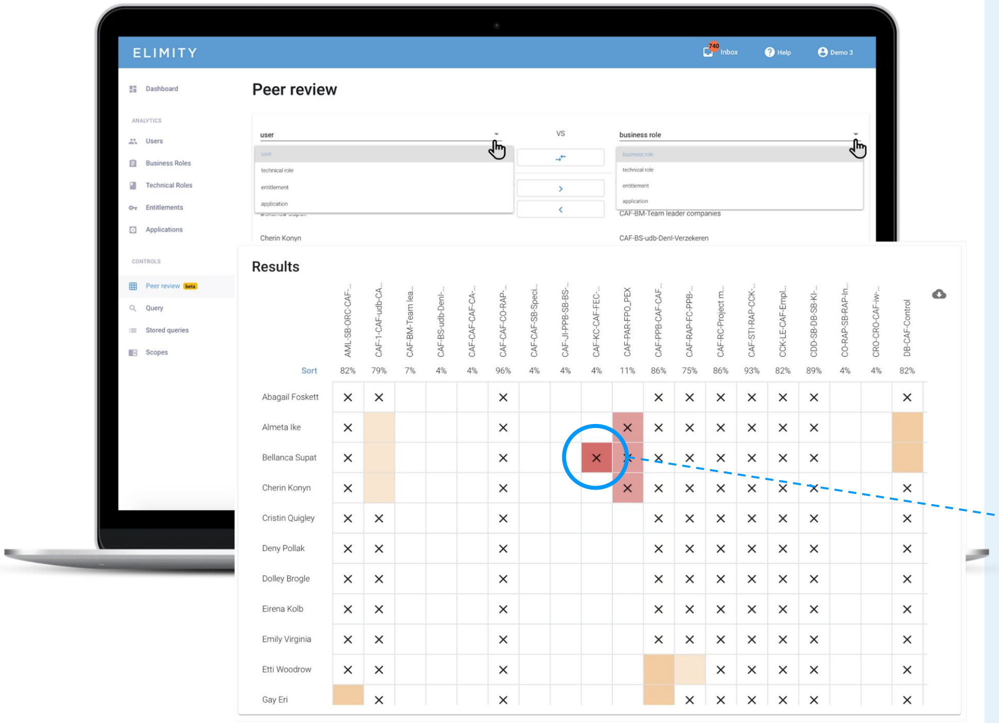
One of the most important principles in information security is the principle of least privilege (PoLP). This principle is the practice of limiting access rights for users to the bare minimum they need to perform their intended work. It is a common misconception to only think about malicious employees when considering using the least privilege principle. The thing is that employees can also accidentally leak data due to phishing, a lost laptop, etc. But whether it's on purpose or not, the less data your employees can leak, the better.

It's a fact that the cumulated access rights and permissions of all your users together determine the attack surface size of your organization, which of course should be kept as small as possible. Unfortunately, there's often a gap between granted access rights and used access rights. This indicates that users have too many access rights, unnecessarily enlarging your attack surface.

- Outliers. These can be defined as users that have more access rights (i.e. are assigned more roles or have more privileges) than their peers. Often this is the result of employees changing departments or functions without the former - and now unnecessary - access rights were deprovisioned.
    - Another way of finding outliers is by comparing them to an ideal role-profile. Depending on the job function a certain employee has, a certain set of roles might be appropriate. This, however, is only applicable to organizations working with such role-profiles.
- Users assigned with a high number of roles or permissions. What is considered as 'high' depends on the role model and organizational context.

RULE OF THUMB

A rule of thumb about when a user can be identified as having a high number of roles or permissions: the total number of roles or permissions exceeds twice the average *(see section 1: the number of roles/permissions relative to the number of users).*



Peer review

user VS business role

user / technical role / entitlement / application

business role / technical role / entitlement / application

Cherin Konyn — CAF-BM-Team leader companies — CAF-BS-udb-Denl-Verzekeren

Results

Sort	AML-SB-ORC-CAF-...	CAF-1-CAF-udb-CA...	CAF-BM-Team lea...	CAF-BS-udb-Denl-...	CAF-CAF-CAF-CA-...	CAF-CAF-CO-RAP-...	CAF-CAF-SB-Speci...	CAF-JI-PPB-SB-BS-...	CAF-KC-CAF-FEC-...	CAF-PAR-FPO_PEX	CAF-PPB-CAF-CAF...	CAF-RAP-FC-PPB-...	CAF-RC-Project m...	CAF-STI-RAP-CCK-...	CCK-LE-CAF-Empl...	CDD-SB-DB-SB-KI-...	CO-RAP-SB-RAP-In...	CRO-CRO-CAF-iw-...	DB-CAF-Control
	82%	79%	7%	4%	4%	96%	4%	4%	4%	11%	86%	75%	86%	93%	82%	89%	4%	4%	82%
Abagail Foskett	×	×				×					×	×	×	×	×	×			×
Almeta Ike	×					×				×	×	×	×	×	×	×			
Bellanca Supat	×					×			×	×	×	×	×	×	×	×			
Cherin Konyn	×					×				×	×	×	×	×	×	×			×
Cristin Quigley	×	×				×					×	×	×	×	×	×			×
Deny Pollak	×	×				×					×	×	×	×	×	×			×
Dolley Brogle	×	×				×					×	×	×	×	×	×			×
Eirena Kolb	×	×				×					×	×	×	×	×	×			×
Emily Virginia	×	×				×					×	×	×	×	×	×			×
Etti Woodrow	×	×				×							×	×	×	×			×
Gay Eri		×				×						×	×	×	×	×			×

FIGURE: ELIMITY INSIGHTS
Screenshot of peer review interface

ELIMITY INSIGHTS: PEER REVIEW TO DETECT OUTLIERS

Within identity management, an ‘outlier’ can be understood as someone (or something) that has more access rights than necessary. One - quite intuitive - method to detect outliers is by comparing their access rights to those of their peers.

Think about scenarios such as team member that should have similar access rights (i.e. have assigned the same roles or entitlements). Elimity Insights visualizes these kind of situations in an easy-to-digest matrix and automatically colour codes potential outliers. This **automated risk indication** enables you to detect outliers in no time.

In the figure it can easily be seen that Bellanca Supat is the only one who is assigned a certain role.

Get in touch

5. Separation of Duties (SoD)

Separation of duties, also known as segregation of duties, is considered as one of the most difficult and often costly identity controls to implement properly. The objective is to disseminate the tasks and associated permissions among multiple people. That way it is much more difficult to commit fraud since at least two people must work together to do so. However, the objective is no longer limited to fraud prevention, but also includes security and privacy. If properly designed and implemented correctly SoD ensures that employees don't have conflicting responsibilities or interests. For example, you don't want the person defining a policy to have the ability to approve its execution. Apart from the SoD controls itself, the metrics to see how you are doing:

- SoD violations. Besides the total number of SoD violations, it can also be interesting to look at the number of specific SoD violations to identify those toxic combinations that seem the hardest to resist. For these violations, a tactical clean-up will probably not do the trick. A strategic redesign (see info on the right), however, might improve the situation.
- Undecided access rights combinations. These are the combinations of roles, entitlements or applications for which it's not clear whether they are considered 'toxic' or not. If such a combination occurs in practice, it's important to know whether it's allowed or not in order to take appropriate action (if required).

REMEDIATION OR MITIGATION?

Remediation: permanently delete the conflict. There are two options to achieve this:

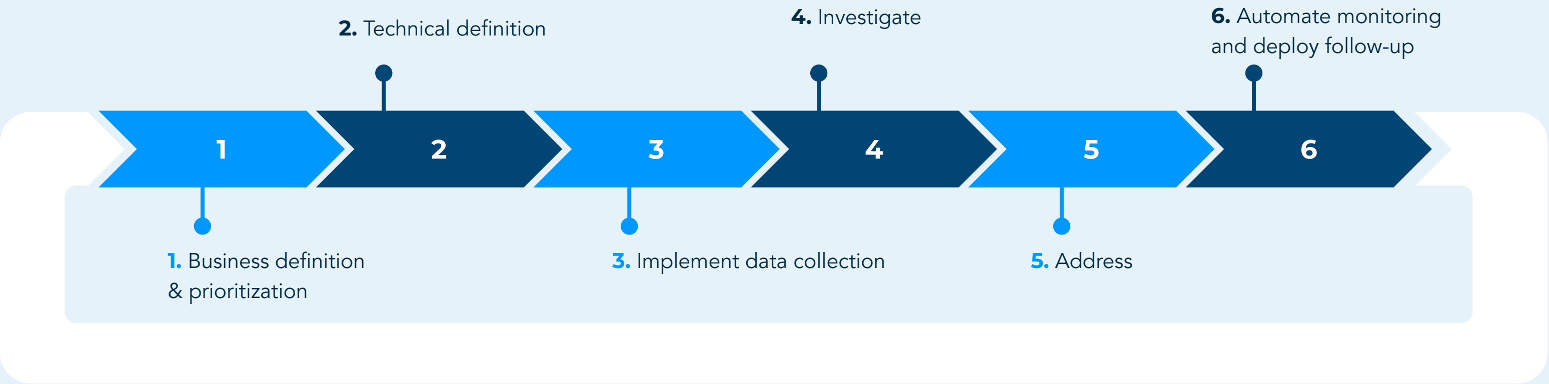
- **Tactical clean-up:** revoke a group, delete the user account, …
- **Strategic redesign:** redesign certain groups or processes

Mitigation: accept the risk, but put controls into place to lower the risk. For example by lowering the impact by defining a max amount for an invoice without additional approval.

DON'T KNOW HOW TO START IMPLEMENTING SOD CONTROLS?

Implementing a proper SoD control set starts with defining 'toxic' combinations of access rights (roles, entitlements, applications, ...). In case users are found who have access rights combinations that are considered toxic, this should be mitigated or remediated. Manually controlling for SoD violations, however, is very time-consuming and error prone. Therefore, the key to actually lower the risk lies in automating the identification of SoD conflicts using an agile approach.

Elimity's agile approach



2. Technical definition
4. Investigate
6. Automate monitoring and deploy follow-up
1
2
3
4
5
6
1. Business definition & prioritization
3. Implement data collection
5. Address

FIGURE: ELIIMITY'S AGILE APPROACH

Struggling with SoD? We can help!

Get in touch

6. Identity hygiene

It is important to realize that identity hygiene (i.e. proper maintenance of the repository) and information security are strongly interconnected: a well-maintained IT environment is better protected against information security risks. Applying good practice to users, roles and entitlements not only helps to prevent risks, but it's also a lot easier and needs considerably less effort compared with a situation where you periodically have to clean up the mess. In other words: prevention is better than cure.

Some metrics to measure how well you're doing regarding user hygiene:

- Users that have no roles or entitlements assigned.
- Users that have no access to any applications.
- User accounts that have not been changed for a certain period of time. What that time period should be exactly can differ between organizations.
- User accounts with direct entitlements, not assigned through roles.
- Users accounts for testing purposes (i.e. *test accounts*).
- Users (and more specifically their access rights) that are not reviewed in a certain period of time. Again, what that time period should be exactly can differ between organizations and often depends on the frequency of (re)certification campaigns.
    - This KPI can also be set up for specific types of accounts, such as admin accounts.
- In case the organization enforces a password expiration policy: user accounts with expired passwords.

Some metrics to measure role hygiene. Note that these KPIs can be split into sub-KPIs for specific types of roles such as IT or business roles:

- Roles that do not consist of other roles or entitlements, also known as *empty roles*.
- Roles that are not assigned to any user, also known as *unassigned roles*.
- Roles that are (not) reviewed in a certain period of time. Again, the exact time period depends on the frequency of (re)certification of roles in the organization.
- Roles with an additional approver.

Some metrics to measure entitlement hygiene:

- Entitlements that are (not) assigned via a role.
- Entitlements that are not assigned to any user.
- Entitlements with an additional approver.

7. Data quality

In order to get accurate results from all of the controls mentioned above, it's crucial that all relevant data ('attribute values') are entered correctly. The KPIs will only reflect the actual state if the data in the IAM system is accurate, complete and up to date. Many of the processes such as onboarding, offboarding and in general changing data, are automated with the help of IAM systems. As a result, finding inaccuracies or blank fields is also an opportunity to improve these processes. Simply solving specific data issues without considering the root cause is like fighting a running battle.

GARBAGE IN IS GARBAGE OUT

There are many KPIs that help to measure this. Think about all the different data attributes in the IAM system that could be left blank. However, it's important to focus effort on those attributes that are crucial for other KPIs or to take action to improve identified issues. Remember that more in-depth information and action-oriented insights are required to actually improve identified issues. Without the right information, it's almost impossible to decide whether a certain user account or role can be disabled/revoked or not.

Some metrics that are essential for the majority of organizations:

- Users without a manager, department, or email.
- Roles without a (proper and clear) description or owner.
- Entitlements without a (proper and clear) description and owner.
- Applications without a (proper and clear) description and owner.

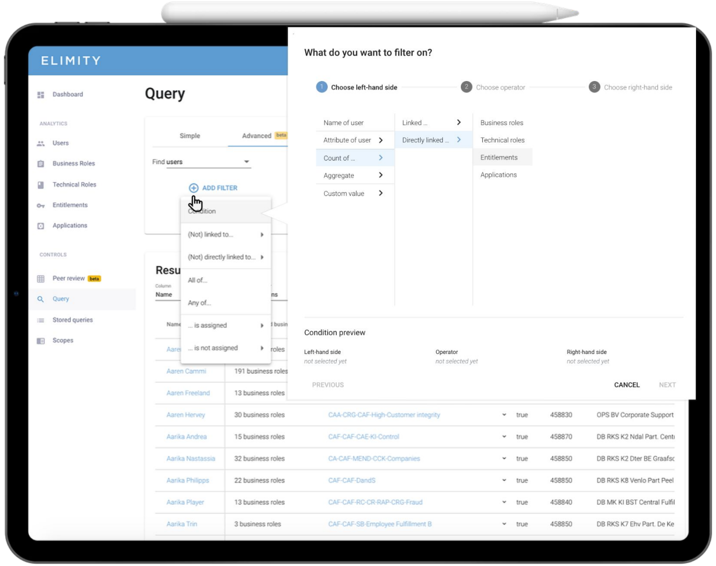
8. Business-specific KPIs

Next to the more general KPIs mentioned in the previous sets, it’s important to enhance these KPI sets with business-specific metrics. In financial institutions, for example, it’s often the case that an employee needs the proper certification/training to perform a certain action. Hence, the number of employees who do have the permissions to execute that action, but don’t have the proper certification could be such a business-specific KPIs. Another frequently seen situation is when companies focus on security awareness training and want to measure for whom such training has been too long, especially if these users have a lot of privileges.

ELIMITY INSIGHTS: ADVANCED IDENTITY INTELLIGENCE

Gain 360-degree insights with the most powerful identity analytics engine ever built and easily automate the KPIs mentioned in this guide. Think of privileged and overly privileged users, unassigned roles, toxic combinations of roles or entitlements, and many more.

Moreover, the purpose-built query language and and user-friendly interface allow anyone - ranging from business to IT - to automate and follow-up almost any (business-specific) KPI.



Find users

Left-hand side: not selected yet
Operator: not selected yet
Right-hand side: not selected yet

Aaren Cammi	191 business roles				
Aaren Freeland	13 business roles				
Aaren Hervey	30 business roles	CAA-CRG-CAF-High-Customer integrity	true	458830	OPS BV Corporate Support
Aarika Andrea	15 business roles	CAF-CAF-CAE-KI-Control	true	458870	DB RKS K2 Ndal Part. Centr
Aarika Nastassia	32 business roles	CA-CAF-MEND-CCK-Companies	true	458850	DB RKS K2 Dter BE Graafsc
Aarika Philipps	22 business roles	CAF-CAF-DandS	true	458850	DB RKS K8 Venlo Part Peel
Aarika Player	13 business roles	CAF-CAF-RC-CR-RAP-CRG-Fraud	true	458840	DB MK KI BST Central Fulfil
Aarika Trin	3 business roles	CAF-CAF-SB-Employee Fulfillment B	true	458850	DB RKS K7 Ehv Part. De Ke

FIGURE: ELIMITY INSIGHTS
Screenshot of creating a KPI

CLOSED-LOOP MODEL

Obviously, KPIs in itself are just KPIs. IAM effectiveness can only be improved if those KPIs are actually used to drive decisions, actions and their prioritization. Following the closed-loop model, shown below, will enable you to do exactly that.

Moreover, remember that in order to maximize the value of your existing IAM system, it's crucial to know (1) where you are now, (2) where you are going and (3) where you want to be. Combining those three will enable you to timely identify areas for improvement so as to ensure effective and efficient IAM.

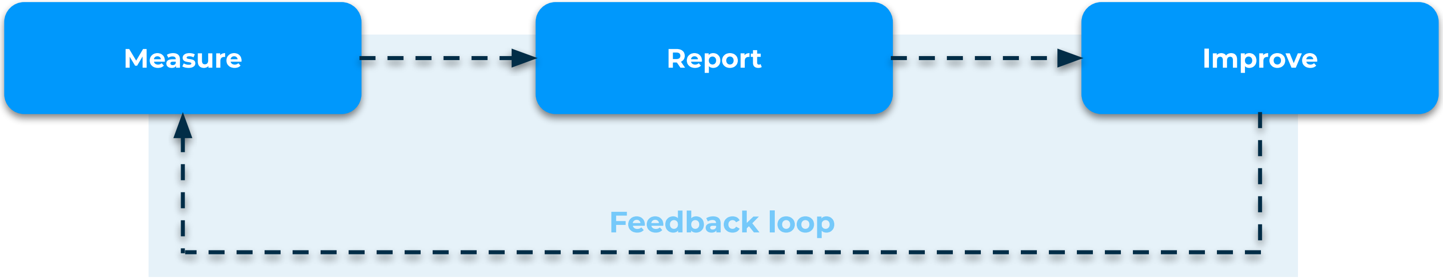


FIGURE: CLOSED-LOOP MODEL

Measure

All organizations could benefit from a metrics-based approach to IAM. Measuring performance is crucial to make timely and informed decisions about short and long term activity focused on increasing the ROI of IAM. It provides hard evidence - numbers don't lie if calculated correctly - that can support decision making, create awareness and simply help you to make your case. On top of that, KPIs allow you to benchmark against peers in order to understand the relative IAM performance. It enables you to understand whether the total number of roles in your type of organization (industry, size, etc.) is below or above average, for instance.

Moreover, depending upon the goals of IAM in the organization and the specific IAM responsibilities of someone, not only the type of KPIs (*see The right choice of KPIs*) but also the importance of those right KPIs will differ. Hence, it's important to assign 'weights' to the sets of KPIs or specific KPIs in order to focus efforts and get a correct image of the IAM system's effectiveness. It could, for example, be possible that empty roles are prominent in the organization, but that they are not a priority right now. Ensuring that the focus is correctly distributed across the different KPIs enables you to set up a long-term, focused plan.

Report

Just measuring KPIs will not enable you to get the most out of your IAM system. Reporting about those KPIs, however, provides context which allows to better understand where you are now and identify areas of success and areas to improve in order to get where you want to go. For that reason, it's important to look at the KPIs over time in order to detect trends and correlations. Imagine, for example, that the number of roles has been steadily increasing over time and that the same trend can be seen with unused roles (e.g. *unassigned* or *empty roles*). In that case, evaluating those unused roles - and deciding whether they can be deleted - could help to avoid a 'role bloat'.

Unfortunately, the majority of applications that are currently being used for reporting about IAM KPIs are not specifically built for it. A common 'gap' is that you can only see the numbers of the KPIs but not what's behind it. It is possible to see that there are for example 100 unassigned roles, but it's not possible to click through to find out which roles are involved.

Improve

Being KPI-driven is only as valuable as the value of the actions that result from it. Hence, I can only suggest using KPIs to drive prioritization of both the most valuable short term and long term activities and investments.

There are several activities in which you can maximize the value of IAM for your organization. An obvious one: clean-up. We've already talked about cleaning up roles to avoid a 'role bloat'. Besides unassigned and empty roles, think about cleaning up incorrect access rights and inactive accounts. Also here prioritization is key. Which issues to clean up first depends on the relative importance and current state of the corresponding KPIs. It's important to remember that a 'clean' identity and role repository makes identity management a lot more manageable.

Need help with prioritization or implementing the closed-loop model in practice? We can help!

Get in touch

Moreover, it's not only important to clean up identified issues but also to find out whether there is a bigger root cause that can be solved. Think about 'joiner - mover - leaver' HR processes that should be updated.

Feedback loop

Once actions are taken, this will - hopefully - be reflected in the KPIs. Tracking progress enables you to evaluate the success of a certain activity in improving IAM effectiveness. Those experiences and knowledge allows for better prioritization of next actions. It's a process of continuous improvement. Not only focused on the output but also on the means of getting there.

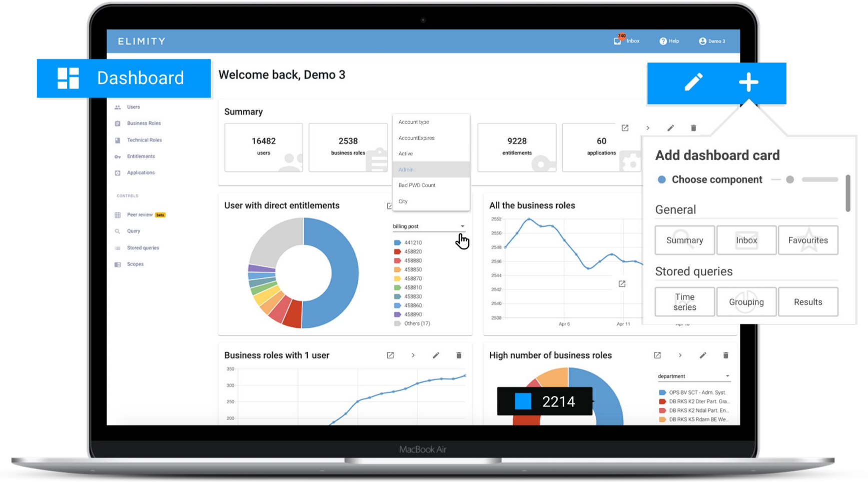
CONCLUSION

Using key metrics does not only enable an organization to understand how its existing IAM system is performing but also helps to better plan for maximizing its value for the organization. It's crucial - now more than ever - to understand what is needed to increase the success of these solutions to ensure efficient and secure management of all identities and their accesses.

Main takeaways:

- Measure how you are doing. Choose a set of KPIs based on the organization's IAM goals and your specific responsibility within IAM. But remember that KPIs in itself are just KPIs.
- Report on KPIs over time in order to detect trends and areas for improvement. Allow for dynamic reporting that can actually be used by various stakeholders.
- Improve the current state by cleaning up accounts, roles, entitlements and other objects that don't belong in the identity repository anymore.
- Track progress over time and learn continuously.

ELIMITY INSIGHTS FOR IAM



Get a demo!

Want to discover
Elimity Insights for IAM?

Get in touch

Need more information? We are happy to answer your questions!

MAARTEN DECAT
Solution Architect
maarten@elimity.com

ELIMITY